Thomas-Gabriel Rüdiger
Petra Saskia Bayerl *Hrsg.*

Cyberkriminologie

Kriminologie für das digitale Zeitalter

Springer VS

Cyberkriminologie

Thomas-Gabriel Rüdiger ·
Petra Saskia Bayerl
(Hrsg.)

Cyberkriminologie

Kriminologie für das digitale Zeitalter

Springer VS

Hrsg.
Thomas-Gabriel Rüdiger
Institut für Polizeiwissenschaft
Hochschule der Polizei des Landes
Brandenburg
Oranienburg, Deutschland

Petra Saskia Bayerl
Centre of Excellence in Terrorism,
Resilience, Intelligence and Organised
Crime Research (CENTRIC)
Sheffield Hallam University
Sheffield, UK

ISBN 978-3-658-28506-7 ISBN 978-3-658-28507-4 (eBook)
https://doi.org/10.1007/978-3-658-28507-4

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020
Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.
Die Wiedergabe von allgemein beschreibenden Bezeichnungen, Marken, Unternehmensnamen etc. in diesem Werk bedeutet nicht, dass diese frei durch jedermann benutzt werden dürfen. Die Berechtigung zur Benutzung unterliegt, auch ohne gesonderten Hinweis hierzu, den Regeln des Markenrechts. Die Rechte des jeweiligen Zeicheninhabers sind zu beachten.
Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag, noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Planung/Lektorat: Cori Antonia Mackrodt

Springer VS ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Inhaltsverzeichnis

Grundlagen der Cyberkriminologie

Cyberkriminologie 3
Thomas-Gabriel Rüdiger und Petra Saskia Bayerl

Ist der Begriff „Cyberkriminalität“ in Forschung und Praxis hinreichend konturiert und somit adäquater (Sozial-)Kontrolle zugänglich? 13
Holger Plank

Der digitale Raum ist kein (grund-)rechtsfreier Raum 71
Roland Hoheisel-Gruler

Problematik der Hell- und Dunkelfeldanalyse im Bereich Cybercrime 109
Edith Huber und Bettina Pospisil

Strafverfolgung digital 135
Dirk Kunze

Defensible Digital Space 151
Cindy Ehlert und Thomas-Gabriel Rüdiger

Phänomenologie von Kriminalität im digitalen Raum

Darknet – die dunkle Seite des Internets? 175
Tim Henkel

Terrorismus und die Nutzung des Internet 193
Holger Nitsch

Wie Cyberterrorismus stattfindet – und warum wir ihn nicht sehen 217
Sebastian Enghofer, Daniel Müller und Alessandro Parrino

Liebesschwindel im Cyberspace 241
Christian Thiel

Hate Speech in der Computerspielkultur 269
Sonja Gabriel

Von der Straße ins Netz 289
Geert Slabbekoorn, Charlotte Colman, Noel Klima und Maud De Meyer

Cyberangriffe gegen private Internetnutzer*innen 319
Arne Dreißigacker, Bennet von Skarczinski, Marie Christine Bergmann und Gina Rosa Wollinger

Cyber-Viktimisierung von Unternehmen 345
Selma Lamprecht und Gergana Vladova

Posterboys und Terrorpropaganda 373
Astrid Bötticher

Wired Drug War 397
Julia Jaroschewski und Sonja Peteranderl

Phänomenologie von digitalen Delikten 425
Christoph Einzinger

Identitätsbildung im digitalen Zeitalter 449
Martina Althoff, Wytske van der Wagen und René van Swaaningen

Grooming-Umgebungen von pädophilen und hebephilen Männern in Deutschland 475
Daniela Stelzmann, Till Amelung und Laura F. Kuhle

Normenkontrolle und digitale Polizeiarbeit

Kriminalität und Unsicherheit im virtuellen Raum 489
Stefan Piasecki und Dorothee Dienstbühl

Strafbedürfnis und Kriminalitätsfurcht im Cyberspace 507
Stefanie Kemme und Maximilian Querbach

Digitaler Vigilantismus 547
Kerrin-Sina Arfsten

Digitale Rechtsdurchsetzung 611
Claudia Otto

Alter Wein in Neuen Medien? 625
Daniel Wagner, Lara vom Feld und Thomas Görgen

Vorhersage von Gruppendynamiken auf der Grundlage von Daten aus Sozialen Netzwerken 653
Michael Spranger und Dirk Labudde

GIS und Geoinformatik bei der Polizei 685
Roman Povalej und Dirk Volkmann

Warum automatische Verfahren bei der Detektion von Hate Speech nur die halbe Miete sind 707
Konstanze Marx

Cyborgs bei der Polizei? 727
Viktoria Pawlowski

Autorenverzeichnis

Prof. Martina Althoff ist Associate Professor für Kriminologie an der Rijksuniversiteit Groningen, Niederlande. Ihre Forschung richtet sich auf die Diskurse und öffentliche Meinung über Kriminalität und Strafe, gesellschaftliche Reaktionen auf Kriminalität und Gewalt, das Zusammenspiel von Gender, Gewalt und Migration sowie auf geschlechtsspezifische Aspekte von Kriminalität. 1997 promovierte sie an der Universität Bremen mit „Die soziale Konstruktion von Fremdenfeindlichkeit“ (Springer VS). Althoff ist Mitherausgeberin des *Kriminologischen Journals* und Mitglied der Redaktion von *Tijdschrift over Cultuur en Criminaliteit.*

Dr. Till Amelung ist Assistenzarzt an der Charité – Universitätsmedizin Berlin, wo er seine Weiterbildung zum Psychiater ableistet. Seine 2016 abgeschlossene Promotion untersuchte Diagnostik und Therapie von Pädophilie im Dunkelfeld. Er ist als Verhaltenstherapeut und Sexualtherapeut ausgebildet. In seiner Arbeit als Arzt und Therapeut am Institut für Sexualwissenschaft und Sexualmedizin und der Klinik für Psychiatrie und Psychotherapie der Charité – Universitätsmedizin Berlin arbeitet er mit Patienten mit psychiatrischen und sexuellen Störungen. Seit 2009 umfasste diese Arbeit auch Männer mit pädophiler Störung, die im Rahmen des Präventionsprojektes und -netzwerks Dunkelfeld (www.kein-taeter-werden.de) im Institut für Sexualwissenschaft und Sexualmedizin vorstellig wurden. Von 2012 bis 2016 war er als wissenschaftlicher Mitarbeiter im Forschungsnetzwerk NeMUP tätig (www.nemup.de), das der Untersuchung neurobiologischer Grundlagen von Pädophilie und sexuellem Kindesmissbrauch gewidmet war.

Dr. Kerrin-Sina Arfsten ist Soziologin und Kriminologin. Im Juni 2019 hat sie ihre Promotion zum Thema „Under Watchful Eyes: Public Vigilance in the

Post-9/11 United States“ an der *International Research School on Retaliation, Mediation, and Punishment* (REMEP) des Max-Planck-Instituts für Internationales und Ausländisches Strafrecht, Freiburg, erfolgreich abgeschlossen. Ihr Forschungsinteresse gilt insbesondere dem (digitalen) Vigilantismus, der visuellen Kriminologie, sowie der Privatisierung von staatlichen Sicherheitsaufgaben im Rahmen der US-amerikanischen Heimatschutzpolitik.

Prof. Dr. Petra Saskia Bayerl ist Professorin für Digitale Kommunikation und Sicherheit am Centre of Excellence for Terrorism, Resilience, Intelligence and Organised Crime Research (CENTRIC) an der Sheffield Hallam University, UK. Sie studierte Psychologie, Informatik und Computerlinguistik (Dipl.-Psych., M.A.) in der Justus-Liebig Universität Giessen, Organisationsdynamik (M.A.) an der University of Oklahoma (USA) und promovierte im Fachbereich Industrielles Design an der Technischen Universität Delft (Niederlande). Ihre derzeitige Forschung untersucht die sozialen Folgen neuer Technologien im Sicherheitsbereich mit Schwerpunkt auf sozialen Medien, Automatisierung und Privacy.

Marie Christine Bergmann studierte Sozialwissenschaften in Hannover und Sociology and Social Research in Utrecht, Niederlande. 2012 erhielt sie ein Promotionsstipendium am Kriminologischen Forschungsinstitut Niedersachsen e. V. (KFN) und ist dort seit 2014 wissenschaftliche Mitarbeiterin. Seit 2019 leitet sie ein von Prof. Dr. Wollinger und ihr initiiertes Projekt zu Cybercrime gegen Privatnutzer. Ihre Forschungsschwerpunkte sind Kriminalität und Devianz von Jugendlichen online und offline, sowie Cyberkriminalität.

Dr. Astrid Bötticher promovierte an der niederländischen Universität Leiden unter der Leitung der weltbekannten Terroristenexperten Alex P. Schmid und Edwin Bakker. Dr. Astrid Bötticher hat zusammen mit Miroslav Mareš das Lehrbuch „Extremismus – Theorien, Konzepte, Formen“ veröffentlicht, das 2012 im Oldenbourg Verlag erschienen ist. Zusammen mit Hans-Jürgen Lange hat sie den Sammelband „Cybersicherheit“ herausgegeben, der 2015 im Springer Verlag erschienen ist. Sie bloggt für die London School of Economics and Political Science und ist Dozentin an der Berlin School of Economics and Law. Als Expertin ist sie Teil des Netzwerkes der EU Kommission Radicalisation Awareness Network und des BKA European Expert Network on Terrorism Issues.

Prof. Dr. Charlotte Colman ist Professorin für Kriminologie. Sie unterrichtet unter anderem Drogenpolitik, Kriminologie der Strafjustiz und Rechtssoziologie.

Seit 2007 leitet und koordiniert sie internationale, EU- und nationale Forschungsprojekte zu den verschiedenen Aspekten des Drogenphänomens. Ihre (Forschungs-)Expertise konzentriert sich auf die Bewertung der Drogenpolitik, die Märkte für das Drogenangebot, einschließlich der Kryptomärkte, Alternativen zur Bestrafung und Entwicklungen bei Straffälligen- und Drogenkonsumentenkarrieren.

Prof. Dr. Dorothee Dienstbühl lehrt an der FHöV NRW seit 2016 im Fachbereich Polizei, Kriminologie und Soziologie und ist Mitglied im Institut für Polizei- und Kriminalwissenschaften (IPK). Zuvor war sie als Leiterin des Bedrohungsmanagements an der Hochschule Darmstadt (h_da), in Jobcentern und in der Forensischen Psychiatrie tätig. Ihre Forschungsschwerpunkte sind Terrorismus, Organisierte Kriminalität, politischer Extremismus, Radikalisierungsprozesse junger Menschen, sowie spezielle Gewaltphänomene wie Hasskriminalität, Amok und zielgerichtete Gewalt an Schulen, Ehrgewalt und patriarchalische Familienstrukturen.

Arne Dreißigacker studierte an der Fachhochschule für Verwaltung- und Rechtspflege Berlin und war zwischen 2001 und 2004 im gehobenen Dienst der Berliner Polizei tätig. Anschließend studierte er Soziologie an der Martin-Luther-Universität Halle (Saale), erhielt 2013 ein Promotionsstipendium am Kriminologischen Forschungsinstitut Niedersachsen e. V. (KFN) und ist dort seit 2015 wissenschaftlicher Mitarbeiter. Zu seinen Forschungsschwerpunkten gehören das Kriminalitätsdunkelfeld, Wohnungseinbruchdiebstahl, Vorurteilskriminalität und Cyberkriminalität.

Cindy Ehlert ist Polizeihauptkommissarin und studierte Kriminologin (M.A.) und ist als solche als Dozentin für Kriminologie an der Hochschule der Polizei des Landes Brandenburg beschäftigt. Als Vorstandsvorsitzende des Fördervereins der Hochschule setzt sie sich insbesondere für den Bildungs- und Forschungsauftrag ein. Ein besonderes Interesse ihrerseits liegt auf der Erforschung von Delikten im schulischen Bereich.

Christoph Einzinger geboren 1989, ist seit 2012 Polizeibeamter des Landes Rheinland-Pfalz. 2016 wurde er zum Landeskriminalamt versetzt und arbeitet dort im Bereich Cybercrime. Im Jahr 2019 erwarb er seinen Master of Science in digitaler Forensik. Bereits seit 2009 beschäftigt er sich mit IT-Sicherheit bzw. der Thematik „Hacking“.

Sebastian Enghofer arbeitet als wissenschaftlicher Mitarbeiter am Lehrstuhl für Vergleichende Politikwissenschaft (Schwerpunkt Westeuropa) der Universität Regensburg. Nach dem Studium der Kriminologie und Gewaltforschung sowie Demokratiewissenschaft promoviert er derzeit zu verhaltensbasierten Policy-Instrumenten (Nudging). In seiner Forschung beschäftigt er sich dabei vor allem mit der Transformation von Gewalt und der interdisziplinären Betrachtung von politischem Extremismus aus psychologischer, kriminologischer und politikwissenschaftlicher Perspektive.

Lara vom Feld ist Soziologin (M.A.) und wissenschaftliche Mitarbeiterin im Fachgebiet Kriminologie und interdisziplinäre Kriminalprävention an der Deutschen Hochschule der Polizei in Münster. Ihre Schwerpunkte sind Arbeitssoziologie und Soziologie abweichenden Verhaltens und sozialer Kontrolle.

Prof. Dr. Sonja Gabriel arbeitet als Hochschulprofessorin für Mediendidaktik und Medienpädagogik an der KPH Wien/Krems, wo sie in der Aus-, Fort- und Weiterbildung von Lehrer*innen und Kindergartenpädagog*innen tätig ist. Ihr Forschungsfokus liegt vor allem auf Digital Game-Based Learning, Gamification und dem Einsatz von Serious Games zum Lehren und Lernen sowie auf der Evaluation unterschiedlicher Projekte rund um das Lehren und Lernen mit digitalen Medien, digitalen Spielen und Game-Design Ansätzen. Sie studierte Deutsch und Englisch auf Lehramt an der Universität Wien und arbeitete für zehn Jahre in einer berufsbildenden höheren Schule in Niederösterreich. Zudem absolvierte sie zwei Masterlehrgänge zu Educational Media (Universität Duisburg/Essen) und Applied Game Studies (Donau-Universität Krems). In ihrer Dissertation an der PH Weingarten beschäftigte sie sich mit Wissensmanagement an höheren Schulen.

Prof. Dr. Thomas Görgen ist Psychologe und Leiter des Fachgebiets Kriminologie und interdisziplinäre Kriminalprävention an der Deutschen Hochschule der Polizei in Münster.

Tim Henkel ist Kriminalbeamter des Landes Rheinland-Pfalz. Seit dem Jahr 2013 verrichtet er seinen Dienst im Landeskriminalamt Rheinland-Pfalz als kriminalpolizeilicher Sachbearbeiter im Ermittlungsbereich. Über seine anfängliche Tätigkeit im Bereich der Rauschgiftermittlungen und die damit verbundenen Ermittlungstätigkeiten innerhalb des Darknets wechselte er vor wenigen Jahren in den Bereich der Cybercrime-Ermittlungen. Seine Erfahrungen im Bereich des Darknets konnte er bei weiteren projektbezogenen Verwendungen beim Bundeskriminalamt in Wiesbaden, sowie bei einer dreimonatigen Hospitation bei EUROPOL in Den Haag ausweiten.

Roland Hoheisel-Gruler ist Dipl. Forstwirt (univ.) und Jurist. Schon während des Studiums der Rechtswissenschaften bewegte er sich in den Weiten der digitalen Welt und erkundete schon im ausgehenden letzten Jahrtausend die frühen Möglichkeiten von Chatrooms sowie Diskussionsboards in Foren und Mailing-Listen mit Hilfe eines Modems und eines kleinen PCs – und erlebte schon in der Frühzeit des damals so genannten Web 2.0 nicht nur die ungeahnten Möglichkeiten, sondern auch die Problemfelder, die sich im Miteinander im digitalen Umfeld auftun, wenn die Regeln hierfür nicht existierten oder mühsam erarbeitet werden mussten und der Erfahrungsschatz aus der analogen, mit Regeln, Gesetzen und Sanktionsmöglichkeiten durchsetzten Welt nicht oder nur eingeschränkt möglich waren. Die Themen der Konfliktbewältigung und Konfliktbearbeitung im Kontext von Kommunikation sowohl im Anoalogen als auch im Digitalen begleitete ihn sein weiteres berufliches Leben, zunächst als Rechtsanwalt, später als zertifizierter Mediator und Fachanwalt für Familienrecht. Seit 2017 arbeitet er als Hauptamtlich Lehrender an der Hochschule des Bundes für öffentliche Verwaltung am Fachbereich Kriminalpolizei in Wiesbaden und unterrichtet dort vornehmlich Eingriffsrecht und Internationale Rechtshilfe.

Mag. Dr. Edith Huber studierte an der sozialwissenschaftlichen Fakultät der Universität Wien und ist seit 2006 an der Donau-Universität Krems beschäftigt. Fachlich spezialisierte sie sich auf den Bereich Cybercrime, Rechts- und Kriminalsoziologie und Sicherheitsforschung. 2009 wurde sie für ihre Forschungsarbeit im Sicherheitsprojekt für das Projekt „Schutz kritischer Infrastrukturen bei Großveranstaltungen“ mit dem KIRAS Sicherheitspreis des BMVIT, für das KIRAS Projekt „Cyberstalking – Österreichweite Studie über das Cyberstalking-Verhalten“ mit dem Dr. Maria Schaumayer Preis sowie für das KIRAS Projekt „CERT-Kommunikation II“ mit dem NÖ-Innovationspreis der Donau-Universität Krems ausgezeichnet. Sie kann auf zahlreiche Forschungs- und Lehrarbeiten aus dem Bereich der Sicherheitsforschung zurückgreifen.

Julia Jaroschewski ist Investigativjournalistin, Politikwissenschaftlerin (M.A.) und Dozentin für Sicherheits- und Drogenpolitik. Sie studierte Politikwissenschaft, Soziologie und Kommunikationswissenschaften an der Freien Universität Berlin und der Universidade de Coimbra. Als freie Auslandskorrespondentin hat sie in den vergangenen zehn Jahren für Medien wie DER SPIEGEL, WIRED oder DIE WELT aus Lateinamerika, USA, Indien und Afrika berichtet, mit Fokus auf Internationaler Politik, Organisierter Kriminalität/Drogenkrieg und Sicherheitspolitik. Sie ist zudem Gründerin des Think Tank BuzzingCities Lab, der erforscht, wie Digitalisierung Sicherheit und kriminelle Organisationen in Brennpunkten urbaner Gewalt wie Favelas in Brasilien beeinflusst.

Prof. Dr. iur. Stefanie Kemme ist seit 2015 Professorin für Kriminologie und Strafrecht an der Hochschule in der Akademie der Polizei Hamburg. Sie studierte Psychologie und Rechtswissenschaften an der Freien Universität und an der Humboldt-Universität in Berlin sowie an der Università Degli Studi Roma Tre. Nach einem Jahr in Frankreich trat sie an der Justus-Liebig-Universität in Gießen eine Stelle als wissenschaftliche Mitarbeiterin am Lehrstuhl für Kriminologie, Jugendstrafrecht und Strafvollzugsrecht bei Prof. Dr. Kreuzer an. Sie promovierte 2007 in den Rechtswissenschaften. Nach dem Referendariat am Kammergericht Berlin (Auswärtiges Amt in Berlin, Anwaltskanzlei SCP d'Avocats Germani, Nizza) arbeitete sie zunächst als Rechtsanwältin für die Wirtschaftskanzlei Heuking Kühn Lüer Wojtek. 2009 begann sie ihre Tätigkeit als Projektleiterin am Kriminologischen Forschungsinstitut Niedersachsen (KFN) und von 2011 bis 2015 war sie Juniorprofessorin für Strafrecht an der Universität Hamburg.

Dr. Noel Klima ist Forschungskoordinator des interdisziplinären IDC-Konsortium Crime, Criminology & Criminal Policy der Universität Gent und Postdoc am Institute for International Research on Criminal Policy (IRCP). Er ist Mitglied des Institutes PIXLES – Datenschutz, Informationsaustausch, Strafverfolgung und Überwachung, UGent-Abgeordneter für das Forschungsprogramm Horizon 2020 SC7 Sichere Gesellschaften und war Mitglied des wissenschaftlichen Beirates für die 2019 Konferenz der Europäischen Gesellschaft für Kriminologie. Zuvor war er unter anderem am Interregionalen Institut für Kriminalitäts- und Justizforschung der Vereinten Nationen (UNICRI), im belgischen Föderalen Öffentlichen Dienst Inneres und im Europäischem Netzwerk für Kriminalprävention (EUCPN) tätig. Noel Klima ist Doktor der Kriminologie, Master in europäischer Kriminologie und Strafrechtssystemen (UGent) und studierte Rechtswissenschaften an der Westfälischen Wilhelms-Universität Münster, der Universität Reims Champagne-Ardenne und der Radboud-Universität Nijmegen.

Dr. Laura F. Kuhle arbeitet als Sexualtherapeutin und Wissenschaftliche Mitarbeiterin am Institut für Sexualwissenschaft und Sexualmedizin an der Charité – Universitätsmedizin Berlin. Dort koordiniert sie den Berliner Standort des Kein-Täter-werden Netzwerkes und arbeitet klinisch in der Diagnostik und Therapie von Menschen mit sexuellen Präferenzstörungen. Sie hat zum Thema „Risk of child sexual abuse image offending in undetected pedophiles and hebephiles" promoviert und forscht gegenwärtig zu den Themen sexueller Kindesmissbrauch in digitalen Medien und deren Präventionsmöglichkeiten, sowie Risikodiagnostik und Therapie von Menschen mit einer sexuellen Präferenz für Kinder. National und international ist sie als Dozentin und Referentin im Bereich der sexuellen Störungen tätig.

Dirk Kunze ist seit 1992 Polizist in Nordrhein-Westfalen. Er gehörte zu den ersten in seinem Land, die Internetermittlungen nicht als Spezialistenaufgabe sahen, sondern diese und die umfassende Auswertung digitaler Spuren als Standardwerkzeug kriminalpolizeilicher Ermittlungen in seiner täglichen Arbeit einsetzte. Seine erworbenen Kenntnisse vermittelte er seit 2006 beim zentralen Fortbildungsträger der Polizei NRW. Nach seinem erneuten Studium übernahm er 2015 den Aufbau und die Leitung des Ermittlungsdezernats des Cybercrimekompetenzzentrums des LKA NRW und der Zentralen Internetrecherche. In den Jahren 2016 und 2017 erarbeitete er konzeptionell die Voraussetzungen für die Schaffung des neuen Cyber-Recherche- und Fahndungszentrums und war verantwortlich für dessen Einführung und Umsetzung. Derzeit leitet er das Landesprojekt Datenbankübergreifende Analyse und Recherche – DAR.

Prof. Dr. Dirk Labudde Nach dem Studium der Theoretischen Physik und Medizin forschte und lehrte Professor Labudde an verschiedenen Universitäten, bevor er 2009 zum Professor für Bioinformatik und Forensik an der Fachhochschule in Mittweida berufen wurde. Insgesamt war er Co-Autor von acht Forschungsbüchern und mehr als 135 Publikationen im Bereich der Bioinformatik und Forensik. Insbesondere interessiert er sich für strukturbasierte Systembiologie, Anwendungen der nächsten Generation für die Analyse biologischer Spuren, wissensbasierte Systeme zur Unterstützung der digitalen Forensik und Resilienztechnik. Darüber hinaus sind die Ergebnisse seiner Forschung für die Industrie, die Regierung und verschiedene Unternehmen von großem Interesse. So gewann er 2009 mit Nanometis, einem innovativen Biotech-Startup, den Science4Life and Venture Cup. Professor Labudde wurde als Hauptredner zu mehreren internationalen Konferenzen eingeladen und ist Berater der Polizei und der Staatsanwaltschaft. Er hält auch Vorlesungen an der Deutschen Polizeiuniversität und der Technischen Universität Bergakademie Freiberg. Für seine hervorragende Lehrtätigkeit erhielt Professor Labudde mehrere Auszeichnungen, darunter den Helmut-Lindner-Preis und den Sächsischen Lehrpreis. Darüber hinaus gründete er 2014 den ersten Bachelor-Studiengang für Allgemeine und Digitale Forensik in Deutschland und ist seit Anfang 2017 Teil des Fraunhofer-Instituts für Sicherheit in der Informationstechnik (SIT).

Selma Lamprecht ist Doktorandin am Fraunhofer Forschungsinstitut für Offene Kommunikationssysteme (FOKUS) und Mitglied der Gruppe ‚Digitalisierung und vernetzte Sicherheit' am Weizenbaum Institut für die Vernetzte Gesellschaft in Berlin. 2017 beendete sie ihren Master in Internationalen Kriminologie in Hamburg und beschäftigt sich heute mit polizeilicher Öffentlichkeitsarbeit und IT-Security-Awareness.

Prof. Dr. Konstanze Marx ist Professorin am Institut für Deutsche Philologie der Universität Greifswald. Sie leitet hier den Arbeitsbereich Germanistische Sprachwissenschaft. Ihre Forschungsschwerpunkte liegen in der Internetlinguistik, der Diskurs- und Textlinguistik, der Erforschung des Zusammenhangs zwischen Sprache-Kognition-Emotion, der Genderlinguistik und der medienlinguistischen Prävention.

Maud De Meyer hat einen BA in Kriminologie und einen MA in Kriminologie an der Universität Gent erworben. 2019 absolvierte sie ein Praktikum am Institute for International Research on Criminal Policy (IRCP) unter der Leitung von Prof. Dr. Colman.

Daniel Müller ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Strafrecht und Kriminologie, Jugendstrafrecht und Strafprozessrecht der Universität Regensburg. Nach dem Studium der Politikwissenschaft, Kriminologie und Gewaltforschung promoviert Daniel Müller aktuell an der Universität Regensburg zum Thema Mechanismen der Radikalisierung. Seine Forschungsschwerpunkte liegen interdisziplinär verortet im Bereich der Extremismus- und Terrorismusforschung.

Dr. rer. pol. Holger Nitsch leitet das Fachgebiet für Gesellschaftswissenschaften an der Hochschule für den öffentlichen Dienst in Bayern, Fachbereich Polizei. Seine Forschungsschwerpunkte sind Extremismus, Radikalisierung, illegaler Menschenhandel und Korruption. Darüber hinaus ist er verantwortlich für internationale Forschungsprojekte und die internationalen Beziehungen des Fachbereichs. Nach seinem Studium an der LMU in München mit den Schwerpunkten internationale Beziehungen und Terrorismus arbeitete er am Flughafen München im Bereich der Bekämpfung der illegalen Migration und des Terrorismus. Er hat mehrere Veröffentlichungen zum Thema Extremismus und hält international Vorträge zu seinen Themenschwerpunkten. Zudem ist er Mitglied in der Foreign Affairs Association und im Advisory Board von CENTRIC.

Claudia Otto ist seit 2012 Rechtsanwältin, seit Dezember 2019 Sozia der Rechtsanwaltskanzlei Dentons Europe LLP, Frankfurt am Main und seit 2017 Herausgeberin der interdisziplinären Fachzeitschrift Recht innovativ (Ri). Sie forscht und berät in Sachen Digitalisierung sowie sich hieraus ergebenden Rechtsfragen. Vor ihrer Tätigkeit für Dentons war sie über drei Jahre selbstständige Rechtsanwältin mit der Kanzlei COT Legal, Frankfurt am Main.

Alessandro Parrino ist externer Doktorand bei Prof. Dr. Alexander Straßner an der Universität Regensburg. Er studierte Politikwissenschaft, Philosophie und Demokratiewissenschaft mit dem Schwerpunkt der Extremismus- und

Terrorismusforschung. Aktuell promoviert er zum Themenkomplex der Cybersicherheit und entwickelt in Kooperation mit wirtschaftlichen und zivilgesellschaftlichen Partnern Lösungsstrategien für eine geordnete digitale Transformation. Insbesondere untersucht er deviante Cyber-Phänomene und die Proliferations- und Nivellierungsmechanismen, welche im virtuellen Raum wirken.

Viktoria Pawlowski Jahrgang 1983, lebt in Hamburg und schloss hier 2003 ihre Ausbildung zur IT-Systemkauffrau ab. An der Universität Hamburg studierte sie Soziologie sowie Slavistik (B.A., 2016) und Internationale Kriminologie (M.A., 2018). Sie arbeitet seit 2013 als Interviewerin für sozialwissenschaftliche Umfragen, absolvierte 2016 ein Praktikum an der Hochschule der Polizei des Landes Brandenburg zum Thema Cyberkriminologie und wirkte 2017 am Forschungsprojekt „From Polygraph to Brain Scan – On the continuous attractivity and socio-technical reconfiguration of lie detection“ an der Universität Hamburg mit. Ihre interdisziplinären Forschungsschwerpunkte liegen im Bereich der Cyberkriminalität, Cyborgisierung sowie der Polizeiarbeit.

Sonja Peteranderl ist SPIEGEL-Redakteurin im Ressort Netzwelt und Gründerin des BuzzingCities Lab. Sie berichtet über Sicherheitspolitik, Organisierte Kriminalität und Technologie. Sie hat zuvor als Redakteurin für das WIRED Magazin gearbeitet und unter anderem aus Lateinamerika, China und USA über Überwachung, Grenzpolitik, Drogenkrieg und Waffenhandel berichtet. Im Rahmen des Kellen Fellowship des American Council on Germany forscht sie zu Predictive Policing und algorithmischen Entscheidungssystemen in Polizeiarbeit/Sicherheit in den USA und Deutschland.

Prof. Dr. Stefan Piasecki lehrt seit 2018 an der FHöV NRW die Fächer Soziologie und Politik (Fachbereiche Verwaltung und Polizei). Zuvor war er an der CVJM-Hochschule in Kassel als Professor tätig und lehrte dort Soziale Arbeit und Medienpädagogik. Er ist habilitierter Religionspädagoge (Uni Kassel) und Jugendmedienschutzprüfer bei der Freiwilligen Selbstkontrolle der Filmwirtschaft (FSK) in Wiesbaden. Zu seinen Forschungsschwerpunkten gehören Formen religiösen und politischen Extremismus, medieninduzierte Devianzphänomene sowie interreligiöse und interkulturelle Problemlagen.

Dr. iur. Holger Plank, M.A., ist Leitender Kriminaldirektor, Leiter des Sachgebietes E3 (Verbrechensbekämpfung) beim Polizeipräsidium Mittelfranken in Nürnberg, Lehrbeauftragter an der Ruhr-Universität Bochum, Masterstudiengang Kriminologie, Kriminalistik und Polizeiwissenschaft und Gastdozent an der FAU Erlangen (jeweils im Nebenamt).

Bettina Pospisil, M.A., absolvierte 2017 den Master of Arts am Department für Soziologie an der Universität Wien. Als Junior Researcher arbeitete sie bereits an der Alpen Adria Universität Klagenfurt sowie an der Wirtschaftsuniversität Wien. Im Rahmen der Beschäftigung an der Donau-Universität Krems wirkte sie in mehreren geförderten Projekten (u. a. ÖAW, FFG, Land NÖ) zum Thema Cybersicherheit mit. Beispiele dafür sind die Projekte „CERT-Komm I“, „CERT-Komm II“ und „Cyber Sicherheit für zukünftige Verkehrssysteme“. Für das Projekt CERT-Komm II erhielt Bettina Pospisil zusammen mit Edith Huber den Niederösterreichischen Innovationspreis 2017 der Donau-Universität Krems. Im Rahmen ihrer Arbeit veröffentlichte Pospisil mehrere Zeitschriftenartikel sowie Beiträge in Tagungsbänden und hielt Vorträge bei verschiedenen kriminologischen, technischen und wirtschaftlichen Konferenzen (z. B. KrimG, ARES, IRIS). Auch ist Bettina Pospisil Mitherausgeberin des Buches „Die Cyber-Kriminellen in Wien“ (Huber, Pospisil 2018) sowie Mitautorin des Buches „Sicherheit in Cyber-Netzwerken“ (Huber 2015). Ihr Forschungsschwerpunkt liegt in den Themen Cyberkriminalität sowie Kriminal- und Techniksoziologie.

Dr. Roman Povalej ist seit Juli 2015 an der Polizeiakademie Niedersachsen (PA) als Professor für Informations- und Kommunikationstechnik (IuK) und Cybercrime (CC) tätig. Seit 2004 betreut er Studierende und hält seit 2006 regelmäßig Informatik-Vorlesungen mit starkem Praxisbezug an diversen Hochschulen und Weiterbildungsinstituten. Er engagiert sich in mehreren Gremien und Arbeitsgruppen bei den Polizeien. Ein besonderes Anliegen von Dr. Povalej ist das Voranbringen der Polizei-Informatik. Die jährliche Fachtagungsreihe Polizei-Informatik wurde als die erste Fachtagung für Lehrende und/oder Forschende in der Informatik an Hochschulen und Akademien der Polizeien ins Leben gerufen.

Maximilian Querbach ist seit 2019 wissenschaftlicher Mitarbeiter beim Landeskriminalamt Niedersachsen und arbeitet dort im EU-Projekt „Cutting Crime Impact“ an der Erarbeitung kriminalpräventiver Ansätze und Maßnahmen zur Verminderung von Alltagskriminalität sowie der Stärkung des öffentlichen Sicherheitsgefühls. Er studierte Soziologie und Erziehungswissenschaften an der Universität Trier und Internationale Kriminologie an der Universität Hamburg.

Thomas-Gabriel Rüdiger ist studierter Kriminologe (M.A.) und forscht als akademischer Rat am Institut für Polizeiwissenschaft an der Hochschule der Polizei in Oranienburg zu Themen der Cyberkriminologie. Seine Themenschwerpunkte liegen dabei auf der Erforschung digitaler Straftaten und Polizeiarbeit sowie den Ursachen und Erklärungsansätzen für digitale Normenbrüche.

Neben der Veröffentlichung einer Vielzahl von Fachpublikationen vertritt er die Fachdisziplin der Cyberkriminologie als Experte und Interviewpartner in unterschiedlichen Medienformaten. Zudem wird er regelmäßig als Experte zu Gesetzesvorhaben zu digitalen Themen auf Landes- und Bundesebene angehört.

Bennet von Skarczinski studierte Betriebswirtschaftslehre an der Hochschule Hannover und arbeitet seit 2015 bei PricewaterhouseCoopers (PwC) in Hannover. Seit Dezember 2017 ist er zudem assoziierter Mitarbeiter am Kriminologischen Forschungsinstitut Niedersachsen e. V. (KFN) im Projekt Cyberangriffe gegen Unternehmen und promoviert als externer Doktorand am Lehrstuhl für Unternehmensrechnung und Wirtschaftsinformatik der Universität Osnabrück. Zu seinen Schwerpunkten gehören das Management von Informationssicherheit in Unternehmen und Cyber-Economics.

Geert Slabbekoorn erwarb einen B.A. in Philosophie und einen M.A. in Europastudien. Derzeit ist er zusätzlich aktiv im MSc-Programm Statistik an der KU Leuven. Er ist seit März 2019 an der Universität Gent tätig. Derzeit arbeitet er als Hauptforscher am CRYPTODRUG-Projekt unter der Leitung von Prof. Dr. Charlotte Colman, wo er und das CRYPTODRUG-Team Umfragen, Interviews und umfangreiche Webdatenanalysen benutzen, um die belgische Beteiligung am Drogenhandel im Internet zu erfassen.

Michael Spranger Nach dem Studium der Wirtschaftsinformatik und Informatik arbeitete Herr Spranger als Softwareentwickler im Bereich Systemintegration. 2012 wurde er wissenschaftlicher Mitarbeiter im Projekt Digitale Forensik an der Fachhochschule Mittweida und war Mitverfasser eines Forschungsbuchs und zahlreicher Veröffentlichungen auf dem Gebiet der forensischen Datenanalyse. Seit 2015 ist Herr Spranger Dozent für Forensik und maschinelles Lernen zur Analyse von strukturierten und unstrukturierten Daten in den Bachelor-Studiengängen „Allgemeine und Digitale Forensik“ sowie „IT-Forensik/Cybercrime“. Daneben führt er Kurse im Weiterbildungsprogramm für Staatsanwälte und Ermittler durch. Er interessiert sich insbesondere für wissensbasierte Systeme zur Unterstützung der Forensik und des Resilienz-Engineerings.

Daniela Stelzmann, M.A., hat an der Johannes Gutenberg-Universität Mainz Publizistik und Psychologie studiert. Seit 2016 ist sie als wissenschaftliche Mitarbeiterin an der Freien Universität Berlin (Institut für Publizistik- und Kommunikationswissenschaft) tätig. In ihrer Forschung beschäftigt sie sich mit den Zusammenhängen zwischen psychischen Erkrankungen und Medien. Zu ihren Forschungsschwerpunkten gehören dabei die mediale Stigmatisierung von

psychisch Erkranken und deren Konsequenzen, sexueller Kindesmissbrauch in digitalen Medien durch Präferenztäter, sowie die Nutzung und Wirkung sozialer Medien auf depressive Menschen. Ihre Forschungsprojekte sind interdisziplinär angelegt und finden in Kooperation mit Wissenschaftler*innen der Charité Universitätsmedizin Berlin statt.

Prof. Dr. René van Swaaningen ist Professor für Kriminologie an der Erasmus Universität Rotterdam (EUR) und Leiter des kriminologischen Instituts der Erasmus School of Law. Seine Forschungsinteressen orientieren sich an internationalen kriminologischen Themen, insbesondere dem Zusammenhang zwischen kulturellen und sozialen Entwicklungen und der Kriminalitäts- und Unsicherheitspolitik in europäischen Städten, den Strafvollzugssystemen und der globalen Kriminologie. Er promovierte 1995 mit einer Umfrage und theoretischen Neubewertung der europäischen kritischen Kriminologie an der Erasmus Universität Rotterdam. Seine Antrittsvorlesung als ordentlicher Professor von 2007 trug den Titel „Towards a Cosmopolitan Criminology“. Van Swaaningen ist Mitglied von Redaktionen bzw. Beirat in verschiedenen (inter-)nationalen Zeitschriften.

Dr. Christian Thiel ist wissenschaftliche Mitarbeiter an der Universität Augsburg und leitet derzeit das DFG-Forschungsprojekt „Zur Herstellung von Täuschung und Vertrauen beim Betrug“. Er studierte Soziologie, Psychologie und Kommunikationswissenschaften und wurde 2010 mit einer geldsoziologischen Arbeit an der Universität Augsburg promoviert. Seine Lehr- und Forschungsschwerpunkte sind Kriminalsoziologie, Geldsoziologie und Kultursoziologie.

Dr. Gergana Vladova ist Postdoktorandin am Lehrstuhl für Wirtschaftsinformatik, insb. Prozesse und Systeme an der Universität Potsdam und Leiterin der Forschungsgruppe „Bildung und Weiterbildung“ in der digitalen Gesellschaft am Weizenbaum Institut für die Vernetzte Gesellschaft in Berlin. Seit 2008 forscht und lehrt sie zu den Themen Kompetenzentwicklung im Kontext der Digitalisierung, Wissens- und Innovationsmanagement und Produktpiraterie.

Dirk Volkmann ist Polizeioberkommissar und Dozent für Kriminalwissenschaften an der Polizeiakademie Niedersachsen (PA). Seit 2005 ist er Fachreferent für Gewässer/Boden/Luft, Luft-/Satellitenbildauswertung und GIS-Analyse, seit 2008 Gutachter für Umweltschutz und seit 2011 als Dozent für die Fächer Mathematik, Abfallwirtschaft/Recycling und Erneuerbare Energien nebenamtlich tätig. Für Dirk Volkmann nimmt das Thema GIS bei den Polizeien, vor allem in der Einsatzleitung und Einsatzplanung sowie Kriminalanalyse, eine wichtige Rolle ein. Entsprechend fördert er die Entwicklung und den Einsatz für die tägliche Polizeiarbeit.

Dr. Wytske van der Wagen arbeitet als Assistenzprofessorin an der Erasmus-Universität Rotterdam (Abteilung Kriminologie). In dieser Funktion forscht sie über Cyberkriminalität, Cyberkriminelle und Interventionen. Ihr besonderes Interesse gilt der Frage, wie sich Kriminalität im Zeitalter von Cyber und Künstlicher Intelligenz verändert und wie sich diese Transformationen auf die Anwendbarkeit kriminologischer Theorien auswirken. Diese Frage hat sie auch in ihrem Dissertationsprojekt „From cybercrime to cyborg crime: an exploration of high-tech cybercrime, offenders and victims through the lens of actor-network theory" (University of Groningen, 2018) behandelt.

Daniel Wagner ist Soziologe/Politikwissenschaftler (M.A.) und wissenschaftlicher Mitarbeiter im Fachgebiet Kriminologie und interdisziplinäre Kriminalprävention an der Deutschen Hochschule der Polizei in Münster. Seine Schwerpunkte sind politische Soziologie und Kommunikationsforschung, Jugendsoziologie und Soziologie abweichenden Verhaltens und sozialer Kontrolle.

Prof. Dr. Gina Rosa Wollinger studierte Soziologie in Leipzig und promovierte 2018 an der dortigen Fakultät für Sozialwissenschaften und Philosophie. Zwischen 2012 und 2018 arbeitete sie am Kriminologischen Forschungsinstitut Niedersachsen e. V. (KFN) und leitete seit Dezember 2017 das von ihr initiierte Forschungsprojekt Cybercrime gegen Unternehmen bevor sie im Oktober 2018 eine Professur für Soziologie und Kriminologie an der Fachhochschule für öffentliche Verwaltung NRW antrat. Zu Ihren Forschungsschwerpunkten zählen Wohnungseinbruchdiebstahl, Cyberkriminalität und die Viktimologie.

Grundlagen der Cyberkriminologie

Cyberkriminologie

Braucht die Kriminologie ein digitales Upgrade?

Thomas-Gabriel Rüdiger und Petra Saskia Bayerl

Vermutlich seitdem es den denkenden Menschen gibt, hat es Normen als Regelwerke des gesellschaftlichen Miteinanders gegeben. Mit jeder Norm stellte – und stellt sich noch immer – auch die Frage der Durchsetzung der Gültigkeit dieser Regeln, da es immer wieder zu Normenbrüchen kommt. Im Laufe der Zeit entwickelten sich hieraus Begriffe wie *Kriminalität, Verbrechen* und *Strafrecht.* In den letzten zwei Jahrhunderten hat sich dabei die Erkenntnis durchgesetzt, dass Kriminalität primär ein gesellschaftlich konstruiertes und bestimmtes Phänomen ist (Bock 2008, S. 4 f.; Kunz und Singelnstein 2016, S. 9 f.). Erst ab diesem Zeitpunkt begann die Menschheit tatsächlich und empirisch basiert Kenntnisse über Kriminalität, normenabweichendes Verhalten, aber auch der Normenkontrolle als solches zu erheben. Hieraus entwickelte sich mit der Kriminologie eine eigenständige Wissenschaft, die sich jedoch erst mit der Zeit von den Rechts- und den Sozialwissenschaften emanzipieren konnte (Bock 2008, S. 10 f.; Kunz und Singelnstein 2016, S. 38 f.).

Die wechselnden Definitionen von „normenabweichendem Verhalten“ – in der Ausprägung der durch die jeweilige Gesellschaftsform als „Kriminalität“ definierten Verhaltensweisen – basierte dabei weitestgehend auf einer ähnlichen

T.-G. Rüdiger (✉)
Institut für Polizeiwissenschaft, Hochschule der Polizei des Landes Brandenburg, Oranienburg, Deutschland
E-Mail: thomas.ruediger@hpolbb.de

P. S. Bayerl
Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research (CENTRIC), Sheffield Hallam University, Sheffield, UK
E-Mail: p.s.bayerl@shu.ac.uk

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

T.-G. Rüdiger und P. S. Bayerl (Hrsg.), *Cyberkriminologie,*
https://doi.org/10.1007/978-3-658-28507-4_1

Grundprämisse: Es handelt sich um soziale Handlungen in einem durch eine jeweilige Gesellschaft klar definierten Rechtsraum. Dieser Rechtsrahmen konnte für die Menschen auch optisch durch tatsächlich wahrnehmbare Staats-, Stadt- oder anderweitige Formen von Grenzen wie beispielsweise Sprach- und Kulturgrenzen fixiert werden. Auch die Kriminologie neigt dazu, eine wissenschaftliche Auseinandersetzung an den Strafrechtsnormen des jeweiligen Landes festzumachen, sich also an staatlichen Legalitätsgrenzen zu orientieren. Eine Studie zu einem Diebstahl in Russland wird vermutlich ganz selbstverständlich das dortige Rechtsverständnis eines Diebstahles zugrunde legen, was aber nicht vergleichbar sein muss mit dem Rechtsverständnis etwa in Deutschland. Ein allgemeiner Vergleich von Kriminalität zwischen Staaten wird auch dadurch erschwert, dass im Bereich der sog. „Delicta male mere prohibita", also Delikten, die nicht einem allgemeingültigen Unrechtsbewusstsein unterliegen (wie etwa Brandstiftung), jeder Staat selbst bestimmt, welche Verhaltensweisen er unter Strafe stellt und damit zur Kriminalität erklärt (Kunz und Singelnstein 2016, S. 11). Entsprechend ist es noch nicht gelungen, Gesetzesmäßigkeiten zu erarbeiten, die frei von diesen Beschränkungen sind, auch wenn dies als ein Ziel der Kriminologie definiert werden kann.

Dies liegt auch daran, dass soziale Normen und damit auch Verbrechensphänomene immer im Kontext der jeweiligen Zeit und Region gesehen werden müssen. Verändernde soziale Räume bringen neue oder zumindest angepasste soziale Erwartungen mit sich und damit auch sich wandelnde Räume, in denen sich kriminelle Energie entfalten kann. Die fraglos größte Umwälzung der letzten Jahrzehnte ist die Etablierung des Internet als neuer sozialer Raum auf globaler Ebene. Mit dem Internet – und vor allem der Entstehung Sozialer Medien – ist ein Kommunikationsraum entstanden, in dem Menschen jeglichen Alters weltweit ohne wahrnehmbare physische Grenzen miteinander interagieren. Bereits im Jahr 2018 sollen weltweit 4 Mrd. Menschen das Internet nutzen (Bouwman 2018). Alleine 2,3 Mrd. Menschen sollen im Jahr 2019 Facebook genutzt haben, 1,5 Mrd. Menschen sogar täglich (Roth 2019). Gemäß der ARD/ZDF Onlinestudie nutzten in Deutschland im Jahr 2018 90,3 % der Bevölkerung ab 14 Jahren zumindest gelegentlich das Internet, 77 % sogar täglich (Frees und Koch 2018, S. 399). Insgesamt 19 % der Bevölkerung in Deutschland nutzen Facebook täglich, weitere 9 % Instagram, 10 % spielen Onlinegames und ganze 37 % nutzen Messenger wie Whatsapp (Frees und Koch 2018, S. 407). Diese verschiedenen Formen Sozialer Medien – neben dem inzwischen fast traditionell anmutenden Kommunikationkanal Email – unterstützen Kommunikation und Interaktion über Grenzen hinweg.

Im Rahmen solch potenziell grenzenloser Kommunikationsmöglichkeiten entstehen fast selbstverständlich auch Handlungsweisen, die nach deutschem

Rechtsverständnis als Kriminalität verstanden werden können. Dabei kann es sich um Kriminalitätsformen handeln, die aus dem offline Milieu bekannt sind, jedoch andere Formen annehmen, wie etwa illegaler Handel mit Drogen über Darknets (s. Kap. „Darknet – die dunkle Seite des Internets?“ und „Von der Straße ins Netz“), sogenannte Romancescams (s. Kap. „Liebesschwindel im Cyberspace“) oder terroristische Phänomene (s. Kap. „Terrorismus und die Nutzung des Internet“, „Wie Cyberterrorismus stattfindet – und warum wir ihn nicht sehen“ und „Posterboys und Terrorpropaganda“). Auf der anderen Seite stehen Phänomene, die in enger Weise mit dem Internet verbunden sind; z. B. Cyber-angriffe auf Bürger und Unternehmen (s. Kap. „Cyberangriffe gegen private Internetnutzer*innen“ und „Cyber-Viktimisierung von Unternehmen“) oder Online-Grooming (s. Kap. „Posterboys und Terrorpropaganda“ und „Grooming-Umgebungen von pädophilen und hebephilen Männern in Deutschland“).

Die kriminologische Betrachtung dieser Erscheinungen ist bisher recht analog geblieben und hat die kriminologischen Besonderheiten des digitalen Raumes als gigantischem Kriminalitätsraum nur bedingt berücksichtigt. Oftmals werden bisherige kriminologische Ansätze ohne weitere Anpassung auf den digitalen Raum transferiert. Dabei gibt es – neben der physischen Grenzfreiheit – durchaus kriminologisch relevante Besonderheiten im Internet. So ist vor allem in den Sozialen Medien, aber auch in anderen onlinebasierten Bereichen, eine Art „fixierte Kriminalitätstransparenz“ feststellbar, d. h. dass Menschen fast täglich mit wahrnehmbarer Kriminalität konfrontiert werden, die über lange Zeit sichtbar, also „fixiert“, bleibt. Beispiele hierfür sind Phishing-Emails, aber auch Beleidigungen und andere Meinungsäußerungsdelikte in Kommentaren oder Blogs, sowie sexuelle Belästigungen in Sozialen Medien (Rüdiger 2019, S. 18 f.). Hier herrscht ein Unterschied zum physischen oder analogen Raum, in dem Normenüberschreitungen oder gar Kriminalität zumeist nur temporär sichtbar sind: Wenn beispielsweise jemand einen Tag später am Ort eines Vermögens-, Sexual- oder auch Gewaltdeliktes vorbeikommt, ist meist nicht mehr ersichtlich, dass hier eine Normenabweichung stattgefunden hat. Online bleiben Kommentare oder Material wie Bilder und Videos oft über lange Zeit erhalten. Dies ist insofern relevant, als dass nach den von Popitz aufgestellten Annahmen, das Nichtwissen um Kriminalität eine Präventivwirkung für andere Normenüberschreitungen entfaltet (Popitz 2016, S. 36 f.). Vereinfacht dargestellt: Wenn Menschen stetig mit sichtbaren Normenüberschreitungen konfrontiert würden, ohne dass eine (korrigierende) Reaktion erfolgt, würde dies letztlich zu einer Senkung ihrer eigenen Hemmschwelle führen, weil der Eindruck entsteht, dass die formelle sowie informelle Normenkontrolle nicht wirksam ist.

Im Internet tritt genau diese Transparenzsituation ein. So werden viele Menschen regelmäßig mit Spam-Emails oder dubiosen Anfragen über Soziale Medien

konfrontiert, die nicht selten als versuchte Straftaten gewertet werden können, ohne dass Ahndungen oder Konsequenzen für die Sender ersichtlich sind. Als konkretes Beispiel gaben im Rahmen der U-25 Studie des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI) 1/3 der befragten jungen Internetnutzer von 14–24 Jahren an, aufgrund einer „Beleidigungskultur" im Internet sich dort nicht zu äußern (Borgstedt et al. 2018, S. 66 f.). Dies deutet darauf hin, dass Beleidigungen und andere entsprechende Delikte im Netz faktisch zeitlich unbefristet fixiert werden, was die Wahrnehmbarkeit von Normenüberschreitungen exponentiell steigert und letztlich auch zu der häufig verwendeten Bezeichnung eines „rechtsfreien Raumes" verleitet (s. Diskussion dazu in Kap. „Der digitale Raum ist kein (grund-)rechtsfreier Raum"). Als ein etwaiges Gegengewicht ist die Normenkontrolle beispielsweise in Form von sichtbaren virtuellen Polizeistreifen oder Ähnlichem zwar denkbar, aber derzeit kaum wahrnehmbar (Rüdiger 2019).

Bisher hat sich – sicher im deutschsprachigen Raum – die Kriminologie noch kaum auf diese besonderen Situationen eingestellt. Dabei erscheint es naheliegend, dass das Verschwimmen von Grenzen und die Schaffung eines globalen digitalen Kriminalitätsraumes mit der dargestellten Kriminalitätstransparenz auch eine angepasste Kriminologie erfordert. Ähnlich wie sich Sozialwissenschaften wie die Psychologie und Anthropologie im Rahmen einer „Cyberpsychologie" und „Cyberanthropologie" mit menschlichem Verhalten im digital Raum befassen (Budka 2014; Kothgassner und Felnhofer 2018), scheint eine Ausweitung kriminologischer Betrachtungen sinnvoll und zweckführend.

Dabei ist der Begriff bzw. die Notwendigkeit einer eigenen „Cyberkriminologie" nicht gänzlich unbekannt. Mit der „Space Transition Theory" definierte Jaishankar für den englischsprachigen Raum bereits 2007 die Notwendigkeit einer eigenen Theorie zur Erklärung von Cybercrime-Delikten und etablierte mit dem *International Journal of Cyber Criminology* eine englischsprachige Fachzeitung (Jaishankar 2007, S. 7 f.). Jaishankar formulierte sieben Grundannahmen, inwiefern sich Täter im digitalen Raum anders verhalten als im physischen Raum und damit eigene kriminologische Theorien notwendig machen. Im Jahr 2018 veröffentlichte Jaishankar einen englischsprachigen Sammelband zur *Cyber Criminology* (Jahankhani 2018).

Im deutschsprachigen Raum fehlt es bisher hingegen an einer grundlegenden Aufarbeitung der Materie. Zwar findet sich der Begriff der Cyberkriminologie in unterschiedlichen Schreibweisen auch vereinzelnd in deutschsprachigen Publikationen (Brodowski 2015, S. 252–254; Meier 2016, S. 232; Rüdiger 2018b; Shaw 2018, S. 115 f.), jedoch handelt es sich meist nur um die Erkenntnis, dass eine solche eigenständige Disziplin notwendig wäre. Eine gewisse Popularität

in diesem noch jungen Feld hat dabei die Übertragbarkeit des *Routine Activity Ansatzes* von Cohen und Felson (1979, S. 588 f.) erlangt (Bässmann 2015, S. 65 f.; Rüdiger 2018a, S. 259 f.). Die Übertragbarkeit weiterer Theorien, der Entwicklung eigener Theorien nur für diesen digitalen Raum oder auch die Frage, welche kriminologischen Methodiken bei der Untersuchung digitaler oder digitalisierter Kriminalitätsphänomene zur Anwendung kommen können, stand bisher kaum im Fokus der kriminologischen Auseinandersetzung.

Der vorliegende Sammelband soll dabei helfen, diese Lücke an fehlenden kriminologischen Ansätzen und Erkenntnisse für den deutschsprachigen Raum zu schließen. Zudem soll dieser Band dabei helfen, die Cyberkriminologie als eigene wissenschaftliche Disziplin im deutschsprachigen Raum zu etablieren.

In **Teil I** „Grundlagen der Cyberkriminologie" behandeln die Beiträge die Grundlagen einer deutschsprachigen Cyberkriminologie. Plank thematisiert in seinem Beitrag die Frage, inwiefern der Begriff der „Cyberkriminalität" sowohl in der Forschung als auch in der Praxis hinreichend bestimmt und ausgestaltet ist (Kap. „Ist der Begriff „Cyberkriminalität" in Forschung und Praxis hinreichend konturiert und somit adäquater (Sozial-)Kontrolle zugänglich?"). Diese Frage ist umso relevanter, als dass der digitale Raum ohne physisch wahrnehmbare Grenzen auch eine Art Kriminalitätsraum aller Gesellschaften bildet, in denen gerade auch die Definition der Untersuchungsgegenstände einer hohen Bedeutung beigemessen werden muss. Die Frage, ob der digitale Raum daher auch ein (grund-)rechtsfreier Raum sei, thematisiert Hoheisel-Gruler in seinem Beitrag, wobei er vor allem anspricht, welche Rolle die staatliche Ordnung in diesem Konstrukt überhaupt einnehmen kann (Kap. „Der digitale Raum ist kein (grund-)rechtsfreier Raum"). Die Frage, ob das Internet als rechtsfrei empfunden wird, kann hierbei u. a. entlang der Strafverfolgungswahrscheinlichkeit – gemessen an der Dunkelzifferrelation – thematisiert werden (Rüdiger 2019, S. 18 f.). Welche Besonderheiten, Probleme aber auch Möglichkeiten bei der Analyse des Hell- und Dunkelfeldes von Cybercrime-Delikten bestehen, haben Huber und Pospisil in ihrem Beitrag betrachtet (Kap. „Problematik der Hell- und Dunkelfeldanalyse im Bereich Cybercrime"). Die Grundlagen der digitalen Polizeiarbeit in Bezug auf die Bekämpfung von Cybercrime als eine Form der Normenkontrolle auch im digitalen Raum hat Kunze beschrieben (Kap. „Strafverfolgung digital"). Ehlert und Rüdiger haben sich der Frage gewidmet, ob der Ansatz der „Defensible Space Theory" von Newman als kriminalitätsminimierender Faktor auf Soziale Medien sowie auf eine Meta-Ebene des digitalen Raumes als solcher übertragen werden kann (Kap. „Defensible Digital Space").

Einen besonderen Schwerpunkt in diesem Sammelband bildet die Betrachtung der Phänomenologie von Normenüberschreitungen und Kriminalität im

digitalen Raum. Auch wenn hierbei eine Betrachtung aus Sicht des deutschen Rechtsverständnisses überwiegt, so sind auch Beiträge aus dem Blickwinkel anderer Staaten vertreten. Der erste Abschnitt von **Teil II** betrachtet dabei die Modi Operandi neuer, aber auch klassischer digitaler Delikte und deren Rahmenbedingungen. Henkel problematisiert zunächst das Darknet als ein Ort, der in der gesellschaftlichen Debatte häufig als ein Ort mit hoher Kriminalitätsbelastung wahrgenommen wird (Kap. „Darknet – die dunkle Seite des Internets?“). Nitsch diskutiert die Online-Komponente modernen Extremismuss und Terrorismus (Kap. „Terrorismus und die Nutzung des Internet“). Enghofer, Müller und Parrino setzen sich hingegen mit der Frage auseinander, was unter dem Begriff „Cyberterrorismus“ verstanden werden kann und ob sich dieser auch durch eine reine virtuelle Gewalt manifestiert (Kap. „Wie Cyberterrorismus stattfindet – und warum wir ihn nicht sehen“). Mit dem Aufbau, den Modi Operandi und dem Forschungsstand von vorgetäuschten virtuellen Liebesbeziehungen, dem sog. Romance- oder auch Bridescaming, setzt sich Thiel in Kap. „Liebesschwindel im Cyberspace“ auseinander.

Der digitale Raum setzt sich nicht nur aus klassischen Sozialen Medien wie Facebook, Twitter oder Instagram zusammen. Nicht selten wird in der Diskussion übersehen, dass auch Onlinespiele zu den sozialen Medien gezählt werden müssen und es auch in Onlinespielen zu kriminellen Handlungen kommen kann, wobei besonders Kinder betroffen sind (Rüdiger 2016). Diesen Aspekt greift Gabriel in Kap. „Hate Speech in der Computerspielkultur“ auf und thematisiert das Phänomen von Hate speech in Onlinespielen und im Zusammenhang mit der Gamingkultur im Allgemeinen. Slabbekoorn, Colman, Klima und De Meyer beschäftigten sich mit dem onlinebasierten Drogenhandel, sowie dessen Struktur und Aufbau, und stellen hierzu Forschungsergebnisse zu belgischen Konsumenten vor (Kap. „Von der Straße ins Netz“).

Eine viktimologische Perspektive nehmen die Beiträge im zweiten Abschnitt von **Teil II** ein. So setzen sich Dreißigacker, von Skarczinski, Bergmann und Wollinger mit der Wahrscheinlichkeit von digitalen Angriffe auf private Internetnutzer auseinander (Kap. „Cyberangriffe gegen private Internetnutzer*innen“). Lambrecht und Vladova betrachten in ihrem Beitrag die Viktimisierung von Unternehmen durch Cyberangriffe und die Wirtschaft als zweite große Opfergruppe, die von digitalen Delikten betroffen ist (Kap. „Cyber-Viktimisierung von Unternehmen“). Einen gänzlich anderen Blickwinkel schlägt hingegen Bötticher ein, die sich damit auseinandersetzt, inwiefern sog. „Posterboys“ Mechanismen des Cybergroomings – ein Begriff, der die onlinebasierte Anbahnung des sexuellen Missbrauches eines Kindes beschreibt – nutzen, um Frauen für den

ISIS anzuwerben. Bötticher thematisiert dabei sowohl die Opfer- als auch die Täterperspektive (Kap. „Posterboys und Terrorpropaganda“).

Einen dezidierten Blick auf die Täterperspektive liefern Beiträge des letzten Abschnittes in **Teil II.** So setzen sich Jaroschewski und Peteranderl damit auseinander, wie lateinamerikanische Drogenkartelle ihre Aktivitäten digitalisieren und welche Schlussfolgerungen daraus gezogen werden können (Kap. „Wired Drug War“). Einzinger befasst sich hingegen explizit sowohl mit der Vorgehensweise als auch mit der Einordnung von sog. „Hackern“ als eine Form digitaler Täter (Kap. „Phänomenologie von digitalen Delikten“). Die Frage, inwiefern sog. Hacker ein gesellschaftliches Label – also ein Etikett – verliehen wird und welche Bedeutung dies für die Täter selbst spielt, wird von Althoff, v. d. Wagen und Swaaningen diskutiert (Kap. „Identitätsbildung im digitalen Zeitalter“). Relativ wenige Erkenntnisse liegen im Forschungsbereich auch zu den Profilen von Online- bzw. Cybergrooming-Tätern vor. Stelzmann, Amelung und Kuhle nehmen sich dieses Feldes anhand der Ergebnisse qualitativer Interviews mit Grooming-Tätern an (Kap. „Grooming-Umgebungen von pädophilen und hebephilen Männern in Deutschland“).

Teil III betrachtet die Mechanismen der Normenkontrolle sowie die Rolle bzw. Möglichkeiten digitaler Polizeiarbeit. Im ersten Abschnitt dieses Teils setzen sich Dienstbühl und Piasecki mit dem generellen Sicherheitsempfinden der Nutzer in sozialen Netzwerken auseinander und welche Bewältigungsstrategien diesen bei der Konfrontation mit Cybercrime anwenden bzw. ihnen zur Verfügung stehen (Kap. „Kriminalität und Unsicherheit im virtuellen Raum“). Einen ähnlichen Ansatz haben auch Kemme und Querbach gewählt, die die Betrachtung einerseits um den Aspekt der Punitivität erweitern und andererseits, basierend auf einer an der Universität Hamburg durchgeführten Dunkelfeldbefragung, Schlussfolgerungen bisheriger Dunkelfelderkenntnisse zur Kriminalitätsfurcht im digitalen Raum hinterfragen (Kap. „Strafbedürfnis und Kriminalitätsfurcht im Cyberspace“). Nicht selten wird hinterfragt, ob der digitale Raum ein rechtsfreier Raum sei. Arfsten entwickelt diesen Gedanken weiter, indem sie Formen des digitalen Vigilantismus in Sozialen Medien – beispielsweise das öffentliche Posten von „Fahndungsaufrufen“ durch Privatpersonen – beschreibt und thematisiert (Kap. „Digitaler Vigilantismus“). Eine gänzlich andere Perspektive wird von Otto eingenommen. Sie betrachtet in ihrem Beitrag die Frage, inwiefern KI (Künstliche Intelligenz) gestützte Rechtsverfahren von sog. „Legal Tech“ Firmen in der Lage sind, die Rechtsdurchsetzung im digitalen Raum zu revolutionieren und welche Risiken sich hieraus ergeben (Kap. „Digitale Rechtsdurchsetzung“).

Die Polizei ist neben der Justiz das vermutlich zentralste Organ der formellen Normenkontrolle. Dabei stehen zwei Gedanken im Vordergrund: zum einen

die Frage, wie sich die Polizei im digitalen Raum selbst verortet, welche Risiken sich hieraus ergeben (Rüdiger 2019; Rüdiger und Bayerl 2018) und wie die Polizei in ihrer Rolle der Normenkontrolle durch Digitalisierungsaspekte verändert oder unterstützt wird. In diesem Kontext hinterfragen Wagner, vom Feld und Görgen zunächst wie eine moderne Kriminalprävention im Rahmen der polizeilichen Kommunikation über Soziale Medien gestaltet werden kann und welche Effekte hierbei ggf. sichtbar sein können (Kap. „Alter Wein in Neuen Medien?“). Einen weiteren, ebenfalls präventiven Blickwinkel werfen Spranger und Labudde auf die Nutzung Sozialer Medien. Sie stellen in ihrem Beitrag in Kap. „Vorhersage von Gruppendynamiken auf der Grundlage von Daten aus Sozialen Netzwerken“ dar, wie gruppendynamische Prozesse anhand Sozialer Netzwerke vorhergesagt werden können und welche Relevanz dies für eine digitale Polizei haben kann. Eine Vielzahl an Informationen im digitalen Raum, aber auch in behördlichen Systemen, können für die polizeiliche Arbeit eine hohe Relevanz entfalten. Povalej und Volkmann thematisieren dabei, inwiefern die Informationen aus Geografischen Informationssystemen (GIS) durch die Polizei im Rahmen von Ermittlung genutzt werden können (Kap. „GIS und Geoinformatik bei der Polizei Chancen und Potenziale für Ermittlungen“). Dass automatisierte Verfahren bei der Bekämpfung und Identifikation von digitaler Kriminalität nicht alleine stehen können, zeigt Marx in ihrem Beitrag in Kap. „Warum automatische Verfahren bei der Detektion von Hate Speech nur die halbe Miete sind“. Sie beschäftigt sich damit, mit welchen Mechanismen sog. Hatespeech – also Hasskriminalität im digitalen Raum – auch über andere Prozesse erkannt und identifiziert werden kann. Die Verschmelzung von Mensch und Maschine bei der Polizei und deren soziotechnischen und digitalen Auswirkungen stehen im Mittelpunkt des Beitrages von Pawlowski (Kap. „Cyborgs bei der Polizei?“).

An der Vielzahl an unterschiedlichen Beiträge und Themengebiete wird ersichtlich, dass auch für die Cyberkriminologie ähnliche Grundsätze gelten wie für die klassische Kriminologie: Es gibt keine singulären Theorien zur Erklärung von normenabweichendem Verhalten und es gibt auch keine einfachen Lösungsansätze. Vielmehr müssen auch hier die unterschiedlichen gesellschaftlichen, rechtlichen und politischen Rahmenbedingungen von Normenabweichungen und Normenkontrolle beachtet werden. In unserer Perspektive wird sich aus diesem Grund eine Cyberkriminologie ebenso differenziert gestalten wie die klassischen Themengebiete der Kriminologie. Unsere Autoren in diesem Sammelband versuchen einen ersten Ansatz zu bieten, diesen Aspekten und einer kriminologischen (Sub)Disziplin „Cyberkriminologie“ einen strukturellen Rahmen zu bieten.

Literatur

Bässmann, J. (2015). *Täter im Bereich Cybercrime*. Wiesbaden: Bundeskriminalamt.

Bock, M. (2008). Grundlagen und Methoden. In M. Bock (Hrsg.), *Kriminologie* (6., vollständig neu bearbeitete u. erweiterte Aufl., S. 1–62). München: Beck.

Borgstedt, S., Borchard, I., Jurczok, F., & Javakhishvili, I. R. (2018). DIVSI U25-Studie. Euphorie war gesteren. https://www.divsi.de/wp-content/uploads/2018/11/DIVSI-U25-Studie-euphorie.pdf.

Bouwman, V. (2018). Digital in 2018. Die Anzahl der Internetnutzer weltweit knackt die 4 Milliarden Marke. https://wearesocial.com/de/blog/2018/01/global-digital-report-2018.

Brodowski, D. (2015). Cybersicherheit durch Cyber-Strafrecht? Über die strafrechtliche Regulierung des Internets. In H.-J. Lange & A. Bötticher (Hrsg.), *Cyber-Sicherheit: Bd. 18. Studien zur Inneren Sicherheit* (S. 249–277). Wiesbaden: Springer VS.

Budka, P. (2014). Von „Cyber Anthropologie" zu „Digitaler Anthropologie". kultur- und sozialanthropologische Beiträge zur Erforschung digitaler Medientechnologien. http://www.philbu.net/blog/wp-content/uploads/2014/01/budka_cyber_digitale_anthropologie.pdf.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588. https://doi.org/10.2307/2094589.

Frees, B., & Koch, W. (2018). ARD/ZDF-Onlinestudie 2018. Zuwachs bei medialer Internetnutzung und Kommunikation. *Media Perspektiven, 9,* 398–413.

Jahankhani, H. (Hrsg.). (2018). *Cyber criminology* (Advanced sciences and technologies for security applications). Cham: Springer.

Jaishankar, K. (2007). Establishing a theory of cyber crimes. *Interntational Journal of Cyber Criminology, 1*(2), 7–9.

Kothgassner, O. D., & Felnhofer, A. (Hrsg.). (2018). *Klinische Cyberpsychologie und Cybertherapie: Bd. 4894. UTB Psychologie* (1. Aufl.). Wien: Facultas.

Kunz, K.-L., & Singelnstein, T. (2016). *Kriminologie. Eine Grundlegung: Bd. 1758. utb-studi-e-book* (7., grundlege. überarbeitete Aufl.). Bern: Haupt.

Meier, B.-D. (2016). Risikofaktoren der Onlinekriminalität. In F. Neubacher & N. Bögelein (Hrsg.), *Krise – Kriminalität – Kriminologie: Bd. 116. Neue kriminologische Schriftenreihe* (S. 231–245). Mönchengladbach: Forum Verlag Godesberg GmbH.

Popitz, H. (2016). Über die Präventivwirkung des Nichtwissens. Dunkelziffer, Norm und Strafe. In D. Klimke & A. Legnaro (Hrsg.), *Kriminologische Grundlagentexte* (1. Aufl., S. 33–46). Wiesbaden: Springer VS.

Roth, P. (2019). Nutzerzahlen. Facebook, Instagram, Messenger und WhatsApp, Highlights, Umsätze, uvm. https://allfacebook.de/toll/state-of-facebook.

Rüdiger, T.-G. (2016). Onlinespiele – Ein kritisches Spielfeld für Kinder und Erwachsene? Eine kriminologische Betrachtung auf das alterslose Zusammenspiel in Onlinespielen. In T. Junge & D. Clausen (Hrsg.), *Digitale Spiele im Diskurs*. https://ub-deposit.fernuni-hagen.de/receive/mir_mods_00000562.

Rüdiger, T.-G. (2018a). Das Broken Web: Herausforderung für die Polizeipräsenz im digitalen Raum. In T.-G. Rüdiger & P. S. Bayerl (Hrsg.), *Digitale Polizeiarbeit. Herausforderungen und Chancen (Research)* (S. 259–299). Wiesbaden: Springer VS.

Rüdiger, T.-G. (2018b). Kriminologie, Kriminalistik und Cyber-Kriminologie? Was ist das und worin unterscheiden sie sich? https://utopiensammlerin.com/2018/04/11/kriminologie-kriminalistik-und-cyber-kriminalitaet-was-ist-das-und-worin-unterscheiden-sie-sich/.

Rüdiger, T.-G. (2019). Polizei im digitalen Raum. *Aus Politik und Zeitgeschichte, 69* (21–23), 18–23. http://www.bpb.de/shop/zeitschriften/apuz/291195/polizei.

Rüdiger, T.-G., & Bayerl, P. S. (Hrsg.). (2018). *Digitale Polizeiarbeit. Herausforderungen und Chancen (Research)*. Wiesbaden: Springer VS.

Shaw, J. (2018). *Böse. Die Psychologie unserer Abgründe* (1. Aufl.). München: Hanser.

Ist der Begriff „Cyberkriminalität“ in Forschung und Praxis hinreichend konturiert und somit adäquater (Sozial-)Kontrolle zugänglich?

Eine Betrachtung aus der Perspektive einer „Gesamten Strafrechtswissenschaft“

Holger Plank

1 Präliminarien

> „Digitalisierung ist mit dem Versuch gleichzusetzen, einen neuen Kontinent zu entdecken.“[1]

Digitalisierung ist ein Schlüsselthema der Zukunft. Sie fordert trotz „scheinbar“ umfassend vorhandener Daten und Fakten neuerdings wieder den Humboldt’schen Entdeckergeist heraus. Das ist die Herausforderung, auf die das Eingangszitat eines anerkannten Experten auf diesem Gebiet implizit verweist. Digitalisierung umfasst alle Lebensbereiche – und zwar umfassend und tief greifend – und ist in Ausmaß, Tiefe und Wirkung auf unsere arbeitsteilig organisierte

[1]So wird Christoph Meinel vom Hasso Plattner Institut (HPI) in Potsdam in einem Beitrag von Stefan Braun in der Süddeutschen Zeitung (SZ) vom 21. August 2018 unter dem Titel: „Die Kanzlerin betritt das Neuland“, vgl. https://www.sueddeutsche.de/politik/digitalisierung-die-kanzlerin-betritt-das-neuland-1.4099214, zitiert, in dem auch der durch das Kabinett auf Vorschlag der Kanzlerin berufene „Digitalrat“ thematisiert wird.

H. Plank (✉)
Lehrstuhl für Kriminologie, Ruhr-Universität Bochum, Lehraufträge, Deutschland
E-Mail: holgerplank@t-online.de

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

T.-G. Rüdiger und P. S. Bayerl (Hrsg.), *Cyberkriminologie,*
https://doi.org/10.1007/978-3-658-28507-4_2

Gesellschaft „überkomplex“[2] (Leisterer 2018, S. 1). Insofern ist es „alternativlos“, dass die Bundesregierung die Digitalisierung zu einem der Top-Themen der 19. Legislaturperiode gemacht hat. Sie will das darin liegende umfassende Potenzial als „Rohstoff“ bergen, um diesen in naher Zukunft möglichst veredeln zu können.

> „So, cyberspace is real. And so are the risks that come with it. It's the great irony of our Information Age – the very technologies that empower us to create and to build also empower those who would disrupt and destroy.“ (Barack Obama 2009, Vorstellung der Cyber-Sicherheitsstrategie der USA)

Wie steht es also abseits des Nutzens dieser Schlüsseltechnologie mit dem Bewusstsein um die Gefahren, mit der Bereitschaft zu einer umfassenden Cyber-Sicherheitsstrategie? Welche Schritte sind bereits zurückgelegt und welche müssen noch gegangen werden? Das sind Fragen, denen sich dieser Beitrag zum vorliegenden Sammelband „Cyberkriminologie“ aus kriminologischer, kriminalistischer, rechtswissenschaftlicher und kriminalpolitischer Perspektive anzunähern versucht.[3]

Dabei wird schon angesichts dieser Perspektive deutlich, dass selbst ein solch verschwindend kleiner Ausschnitt des komplexen Leitthemas „Digitalisierung“ in dem Beitrag nur kursorisch behandelt werden kann. Ein kurzer Blick auf einen Beitrag von Bundeskanzlerin Angela Merkel sei einleitend erlaubt. Sie scheint sich auch der „janusköpfigen“ Gefahren dieser Schlüsseltechnologie durchaus bewusst zu sein. Jedenfalls wird sie im oben erwähnten Beitrag der SZ anlässlich eines Staatsbesuchs in China zur chinesischen Strategie beim Ausbau der Digitalisierung mit den Worten zitiert, dass *„George Orwells ‚1984‘-Fantasien gegen die chinesische Realität ein laues Lüftchen seien. Europa und Deutschland drohten im Verhältnis zu China zu einem ‚schönen Museum‘ zu verkommen.“* Dieses Zitat spiegelt die ungeheure Dynamik wie auch die Risiken dieses Teilthemas sehr eindrucksvoll, aber eben nur in einer kleinen Facette des Oberthemas Digitalisierung, wider.

Zur Eingrenzung und Konturierung der Fragestellungen bediene ich mich ganz bewusst des Modells einer *„Gesamten Strafrechtswissenschaft“*. Was ist

---

[2] *„Alle wesentlichen Bereiche und Funktionen in heutigen Gesellschaften sind abhängig von der Informations- und Kommunikationstechnologie Internet. […] Das Funktionieren des Internet hat mittlerweile essenzielle Bedeutung für den Einzelnen, die Gesellschaft, die Wertschöpfungsketten und die öffentliche Aufgabenerfüllung“*.

[3] Stand des Beitrags: Februar 2019.

unter diesem Begriff zu verstehen und welchen zusätzlichen repressiven wie auch präventiven Erkenntnisgewinn darf man sich von diesem Ansatz mit Blick auf potenzielle Risiken im Cyberraum erwarten?

Die Strafrechtswissenschaft ist eine normative Disziplin. Sie untersucht, streng formalisiert mittels juristischer Methodenlehre, rechtstatsächliche Lebenssachverhalte auf deren strafrechtliche Relevanz. Dieser enge, „materiellrechtliche Ansatz", hier kriminalpolitisch durch das sogenannte „Cyber-Strafrecht" als wesentlicher Marker für die aktuelle Bedrohungslage eingegrenzt, bedarf jedoch zweifellos der interdisziplinären empirischen Erweiterung, um relevante Problemstellungen weitergehend und faktenbasiert zu durchdringen. Abgeleitet von diesem Liszt'schen Leitbegriff[4] der „Gesamten Strafrechtswissenschaft"[5] können damit sozialwissenschaftliche, kriminologische und kriminalpolitische Impulse auf das Strafrecht, welches derzeit die „Cyberkriminalität" gemessen an den statistischen Ausgangsbedingungen im Vergleich zum angenommenen Dunkelfeld wohl nur unzureichend im Fokus zu haben scheint[6], gesetzt werden. Obgleich in weiten Teilen der Strafrechtswissenschaft nach wie vor kritisch „beäugt", ist die „Gesamte Strafrechtswissenschaft" m. E. aber gut geeignet, die Erkenntnisse normativer und empirischer wissenschaftlicher Disziplinen zu einem Gesamtbild zu vereinen. So eignet sich das Modell, um nicht nur Straf- und Gefahrenabwehrrecht methodisch und fachlich mittels evidenzbasierter,

---

[4]Als Begründer dieses Begriffs darf zurecht Franz von Liszt gelten. Mithilfe seiner Theorien *„formierten sich (mit der) Kriminologie (wie auch mit der anfangs nur schwer von ihr zu unterscheidenden Kriminalistik) in den letzten beiden Jahrzehnten des 19. Jahrhunderts interdisziplinäre Fächer, die sich methodisch gegen die Tradition der als zu normativ ausgerichteten Strafrechtswissenschaft abgrenzten"* (Vec 2009, S. 413).

[5]Die Kriminologie steht heute nicht nur hinsichtlich des Phänomens „Cyberkriminalität" am Scheideweg. Will sie sich, nachdem sie zweifellos als selbstständige Erfahrungswissenschaft konstituiert ist, weiterhin in diese Richtung entwickeln und ggf. phänomenbezogene disziplinäre Subkategorien ausprägen, oder soll sie ein Anhängsel des Strafrechts mit entsprechend einseitigeren Forschungen bleiben? Letzteres widerspricht der ursprünglichen Absicht v. Liszts, der durch die Einbeziehung der „strafrechtlichen Hilfswissenschaften" die „Konturen einer erweiterten, vervollständigten Strafrechtswissenschaft" sichtbar machen wollte. Mit der Zusammenführung verschiedener Gegenstandsbereiche unter dem Dach der Strafrechtswissenschaft sollte die Wissenschaft vom Strafrecht insgesamt gefördert werden, wobei die „strafrechtlichen Hilfswissenschaften" mit ihrer erfahrungswissenschaftlichen Perspektive die *„Wissenschaft vom Strafrecht modernisieren und zu dessen durchgängiger Verwissenschaftlichung beitragen sollten"* (v. Liszt und Dochow 1881, S. 1; ergänzend hierzu Galassi 2004, S. 247 f.).

[6]Schon hierdurch werden die durch unterschiedliche Faktoren beeinflussten Risiken einer z. T. evidenten Symbolik des „Cyberstrafrechts" gewahr.

rationaler Wegweisungen fortzuentwickeln, sondern auch im kriminalpolitischen Beratungszyklus wahrnehmbare Zeichen zu setzen. Die Gelegenheit einer solchen Annäherung ist zudem günstig, hat sich die Große Koalition in der 19. Legislaturperiode doch „vertraglich“ eine „evidenzbasierte Kriminalpolitik“[7] verordnet. Das sollte bei der Strafrechtswissenschaft, der Kriminologie und den übrigen relevanten Sozialwissenschaften durchaus Wachstums- bzw. Fortentwicklungsanreize hervorrufen können. Disziplinär darf sich die Kriminologie jedenfalls diese einmalige Chance, die dieses „Bekenntnis“ der Kriminalpolitik implizit in sich birgt, keinesfalls entgehen lassen.

Die Kriminologie spielt also aus dem Betrachtungswinkel einer „Gesamten Strafrechtswissenschaft“ bei der Problemlösung eine signifikante (empirische) Rolle, unabhängig von der im Rahmen des Sammelbandes aufgeworfenen Frage, ob sie hierfür einer eigenen Subkategorie mit dem Präfix „Cyber-“bedarf. Obgleich hierfür in der Literatur und Praxis vereinzelt durchaus gute Gründe genannt werden[8], eine interessante Argumentation bezieht sich z. B. auf das „Zwei-Welten-Theorem“ (vgl. Fn. 34), sollten schon heute Wissenschaft (insbesondere natürlich die Kriminologie) und Sicherheitsbehörden eigentlich zum Phänomen Cybercrime zu profunden Schlussfolgerungen kommen können! Das Phänomen ist jedenfalls nicht neu, aber, angesichts der derzeitigen Erkenntnislage drängen sich verschiedene strukturelle Fragen geradezu auf. Gibt es überhaupt ein einheitliches Begriffsverständnis von ‚Cyberkriminalität‘ (Abschn. 2)? Welche konzertierten Maßnahmen sind in Wissenschaft und Praxis strukturell,

[7]Koalitionsvertrag zwischen CDU/CSU und SPD, *„Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land“,* vom 12. März 2018, S. 133, Zeilen 6282 ff.

[8]Die deutschsprachige Kriminologie habe sich noch nicht ausreichend tief greifend mit webbasierten Kriminalitätsformen und deren Kontrolle beschäftigt (Meier 2015a, S. 94). Hinsichtlich der einzelnen Erscheinungsformen der Internetkriminalität gebe es zwar einige wenige deskriptive Studien (Grabosky 2009), die sich mit der Phänomenologie der Delikte und Fragen der Häufigkeit und Verteilung beschäftigen, aber nur wenig erfahrungswissenschaftlich fundierte Analysen (Meier 2012, S. 212). Unter dieser jedenfalls im deutschsprachigen Raum relativ neuen, nach wie vor aber fachwissenschaftlich nicht reliabel „durchwirkten“ kriminologischen Subkategorie firmiert z. B. der Mitherausgeber dieses Sammelbandes und Kriminologe am Institut für Polizeiwissenschaft an der Fachhochschule der Polizei Brandenburg, Thomas-Gabriel Rüdiger und bietet unter der Bezeichnung „Cyber-Kriminologie“ auch spezifische Fachseminare am „Institut für Gewaltprävention und angewandte Kriminologie“ in Berlin an (http://www.igak.org/cyber-kriminologie.html). Geht man dem Begriff international nach, so ist – inzwischen im 11. Jahrgang auf dem Markt – auch das *International Journal of Cyber Criminology* zu nennen. Ansonsten halten sich auch dort die Nachweise dieser Subkategorie „eher in Grenzen“.

institutionell, planerisch und strategisch-legislativ erforderlich, um die Erkenntnis zum Gegenstand adäquat auszuweiten (Abschn. 3 und 4)?

Was können eine interdisziplinär verortete „Gesamte Strafrechtswissenschaft" – und hierbei insbesondere die Kriminologie mit ihrer empirischen Kopfnote im normativen Kontext – sowie die Sicherheitsbehörden auf dem Feld der Polizeiforschung und -wissenschaft tun, um ihre phänomenologischen/ätiologischen Erkenntnisse im Hinblick auf den schier grenzenlos erweiterten „Cyber-Raum" auszubauen bzw. vorhandenes Wissen zu validieren?

2 Phänomenologie ‚Cybercrime' – ein Versuch der Annäherung

> „Wir fühlen, dass selbst, wenn alle möglichen wissenschaftlichen Fragen beantwortet sind, unsere Lebensprobleme noch gar nicht berührt sind. Freilich bleibt dann eben keine Frage mehr; und eben dies ist die Antwort." (Ludwig Wittgenstein 1922, Tractatus logico-philosophicus, These 6.52)

Wissen wir aktuell überhaupt genau, worüber wir reden, wenn wir den Begriff „Cybercrime" verwenden? Nicht nur die „Internetsicherheit" ist wohl in erster Linie ein „Wissensproblem" (Leisterer 2018, S. 1 ff.). Nach wie vor werden *„Computer- und Internetdelikte weder juristisch noch kriminologisch einheitlich definiert"* (Selzer 2019, S. 221 ff.). Namhafte Experten und Praktiker mahnen gar seit geraumer Zeit die *„Erforderlichkeit einer umfassenden Reform des Internetstrafrechts"* an (Fünfsinn und Krause 2019, S. 652 f. u. a. unter Berufung auf den Beschluss Nr. I.3 des 69. Deutschen Juristentages 2012[9]). In Anlehnung an die einleitende Wittgenstein'sche Sentenz zielt meine Frage an dieser Stelle also keinesfalls bereits auf die wissenschaftliche „Wahrheitsfrage" ab. Sie ist vielmehr eine „Geltungsfrage" im Bereich der praktischen Lebensführung der betroffenen Menschen, für Anbieter und Nutzer des Mediums gleichermaßen wie für die Strafverfolger im beruflichen Kontext, deren Aufgabe im repressiven wie im präventiven Sinne die Minimierung aktueller Risiken durch Aufklärung und Verhütung umfasst. Der Soziologe und Münchner Hochschullehrer Armin Nassehi

[9]Dort heißt es: *„Im Hinblick auf die zahlreichen erforderlichen Reformen im Bereich des Internetstrafrechts sollte wegen der Komplexität der Materie, der schnellen technischen Entwicklungen, der vielfältigen internationalen Verflechtungen sowie des unerlässlichen kriminologischen Forschungsbedarfs eine interdisziplinär besetzte Sachverständigenkommission eingesetzt werden, die dem Gesetzgeber beratend zur Seite steht."*

(2017) hat zu dieser interessanten Ambivalenz von „Wahrheit“ im Zusammenhang mit „überkomplexen Sachverhalten“, z. B. im Rahmen eines sehr lesenswerten Buches „Kritik an der komplexitäts*vergessenen* Vernunft“ geübt.

Wollen wir uns also aufmachen und zunächst die indifferente Ausgangslage, wie sie sich uns derzeit *kriminalstatistisch* belegbar darstellt, aufzuklären versuchen, auch wenn sich dabei das dichte Datengestrüpp, welches den Blick auf das Phänomen verdeckt, derzeit wohl bestenfalls ein klein wenig lichten lässt.

2.1 Lage – kriminalstatistische Konturierung

Statistisch kursieren einige für den Laien nur schwer auseinanderzuhaltende Begriffe, die noch dazu in den Lagebildern wie auch im innerpolizeilichen Sprachgebrauch strukturell-organisatorisch differieren. Kriminalstatistisch und somit öffentlich einigermaßen seriös vergleichbar sind hierbei die definierten Kategorien „Straftaten mit dem Tatmittel Internet“, der „Summenschlüssel Computerkriminalität“ sowie ein eigener „Summenschlüssel Computerbetrug“ (Unterschiede zw. den beiden Kategorien, vgl. BKA, PKS 2017b, Übersicht Summenschlüssel, S. 6) und schließlich noch ein weiterer Summenschlüssel (980100) „Cybercrime im engeren Sinne“ (BKA, PKS 2017b, Übersicht Summenschlüssel, S. 13), der allerdings in den PKS-Jahrbüchern des BKA nicht in einer eigenen Tabelle dargestellt ist.

Die Polizei unternimmt durchaus beträchtliche Bemühungen, sowohl die quantitative als auch die qualitative Bedeutung der durch die Digitalisierung entstandenen neuen Kriminalitätsformen einer größeren (Fach-)Öffentlichkeit bekannt zu machen und mit diesen Erkenntnissen auch zielgerichtet vor potenziellen Gefahren zu warnen. So gibt es eine bereits im Jahr 2004 eingeführte und seit dem Jahr 2010 sämtliche Bundesländer umfassende Tabelle 5[10], die in der richtliniengestützt bundesweit einheitlich geführten Polizeilichen Kriminalstatistik (PKS) die Straftaten mit dem „Tatmittel Internet“[11] ausweist. Diese Deliktskategorie kann man durchaus als *eine* relevante „Obergruppe“ des Phänomens bezeichnen.

[10]Vgl. Erläuterungen des BKA zu den Standardtabellen, zuletzt veröffentlicht zur PKS des Jahres 2017 auf der Website des BKA. Grafik aus dem Jahrbuch Band 1 zur PKS 2017 entnommen.

[11]Bedient man sich bei diesem Phänomen hinreichend verbreiteter Definitionsansätze, so sind darunter Straftaten zu verstehen, bei denen Informationstechnologie zur Planung, Vorbereitung bzw. Ausführung eingesetzt wurde. Das kann grundsätzlich das gesamte

2.1.1 PKS

Das Tortendiagramm in Abb. 1 und Tab. 1 zeigen die deliktische Aufteilung der Straftaten mit dem statistisch erfassten Zusatz „Tatmittel Internet“ = 251.617 Fälle (entnommen aus dem PKS Jahrbuch Band 1, Berichtsjahr 2017, S. 31, Abnahme von 1673 Fällen = 0,7 % im Vergleich zum Jahr 2016).

Dabei ist Tab. 1 (vorletzte Zeile, ebenfalls dem PKS Jahrbuch 2017 entnommen) bereits ein Summenschlüssel „Computerkriminalität“ zu erkennen, welcher jedenfalls zum Teil als „Schnittmenge“ der erfassten Delikte mit dem „Tatmittel Internet“ zu betrachten sein dürfte (hinsichtlich des Summenschlüssels 897.000 sind hierbei jedenfalls anteilig 64.169 Delikte ausgewiesen).

Tab. 2 zeigt die Straftatenuntergruppen, die sich insgesamt hinter dem Summenschlüssel „Computerkriminalität“ und auch dem 2016 eingeführten, modifizierten Summenschlüssel „Computerbetrug“ (897100) vereinen. Letzterer, addiert man die Delikte, muss wiederum integraler Bestandteil des Summenschlüssels „Computerkriminalität“ sein.

2.1.2 Lagebild Cybercrime

Die Begriffsvielfalt und die kriminalstatistische Darlegung sind also mindestens verwirrend. Seit dem Jahr 2010 gibt es darüber hinaus noch ein gemeinsames „Bundeslagebild Cybercrime“ (bis zum Jahr 2009 geführt als Bundeslagebild „IuK-Kriminalität“), das darauf abzielt, ergänzend zur PKS das Gefahren- und Schadenspotenzial der „Computerkriminalität“ (nun aber im offiziellen Sprachgebrauch des BKA im Bundeslagebild als „Cybercrime“ [im engeren Sinne!] gekennzeichnet, vgl. Abb. 2, Seite 1 des Bundeslagebildes 2017) darzustellen und seine Bedeutung für die Kriminalitätslage in Deutschland zu beschreiben.

Um die Leser des Beitrags statistisch vollends zu verwirren, die vergleichbare Grafik im Bundeslagebild Cybercrime des Jahres 2016, in der Kategorie 1 noch

---

Straftatenspektrum des StGB und des Nebenstrafrechts umfassen. Hierbei steht aber das eigentlich geplante Delikt im Vordergrund. Das Internet bzw. deren Komponenten werden zur Tatbegehung als „Werkzeug“ benutzt. Allgemeine, nicht der Computerkriminalität zuzurechnende Straftaten, begangen „mit dem Tatmittel Internet“, können demnach also im weitesten Sinne kriminalstatistisch nicht einfach per se als „Computerkriminalität“ identifiziert werden. Sie werden diesem Komplex alleine durch die notwendige zusätzliche Kennzeichnung mit dem Begleittext „Tatmittel Internet“ im polizeilichen Vorgangsbearbeitungssystem durch den polizeilichen Sachbearbeiter (und auch) erst bei Abgabe an die Staatsanwaltschaft (die PKS ist eine reine *Auslaufstatistik*) zugeordnet und als solche klassifiziert und unterliegen damit der (richtliniengesteuerten) polizeilichen „Deutungshoheit“ (vgl. Abschn. 2.1.2) mit all den damit verbundenen grundsätzlich Unschärfen.

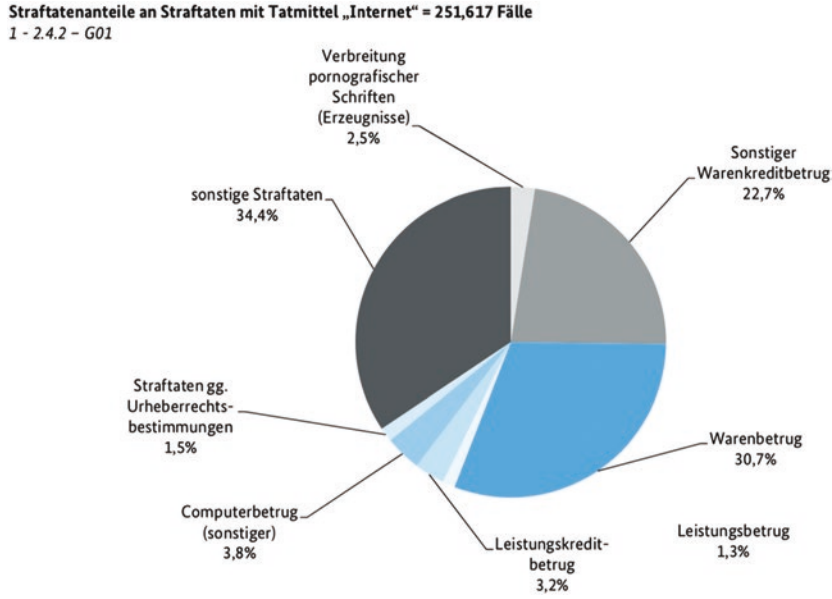


Abb. 1 Strafanteile an Straftaten mit Tatmittel Internet. (Quelle: PKS 2017b)

mit 82.649 Delikten, bezog sich kategorial im PKS-Jahrbuch (Band 1, Berichtsjahr 2016, S. 14) noch auf „IuK-Kriminalität im engeren Sinne“. Dieser Begriff ist im entsprechenden Jahrbuch 2017 nicht mehr enthalten.

Auf der Vollzugsebene arbeitet die Polizei darüber hinaus mit verschiedenen länderspezifischen „Fachfeinkonzepten“ Cybercrime. Diese beinhalten einerseits den strukturell-organisatorischen polizeilichen Bekämpfungsansatz bei der „Kriminalität rund um das Tatmittel Internet“, je nach Deliktskategorie, -schwere, notwendiger fachlicher Spezialisierung und Ausstattung und aufgeteilt zwischen Bearbeitungszuständigkeiten der Schutz- und Kriminalpolizei. Darin werden andererseits aber neben der bekannten und kriminalstatistisch (sofern nach den PKS-Richtlinien erfasst wurde) relativ „eindeutigen“ Kategorie „Tatmittel Internet“ auch noch die kanonisch „unscharfen“ und daher erläuterungsbedürftigen Begriffskategorien „Cybercrime im engeren Sinne“ und „Cybercrime im weiteren Sinne“ verwendet.

Dies führt, diesen ersten phänomenologischen Teilbereich (vorläufig) abschließend, zur vorläufig ersten, dennoch für die weitere Betrachtung nicht ganz unwichtigen Feststellung, dass man kriminalstatistisch, jedenfalls mit den

Tab. 1 Ausgewählte Straftaten/-gruppen mit Tatmittel „Internet". (Quelle: PKS 2017b)

Schlüssel	Ausgewählte Straftaten/-gruppen	Erfasste Fälle insgesamt (Tabelle 01)	Erfasste Fälle mit Tatmittel INTERNET (Tabelle 05)	%uale Verteilung Sp 4	%-Anteil Sp 4 an Sp 3	Aufgekl. Fälle mit Tatmittel INTERNET (Tabelle 05)	AQ	Tatverdächtige mit Tatmittel INTERNET (Tabelle 05)
1	2	3	4	5	6	7	8	9
—	**Straftaten insgesamt**	**5.761.984**	**251.617**	**100,0**	**4,4**	**161.161**	**64,1**	**98.258**
143000	Verbreitung pornographischer Schriften (Erzeugnisse)	10.066	6283	2,5	62,4	5589	89,0	5306
510000	Betrug	910.352	187.100	74,4	20,6	117.844	63,0	61.376
Darunter:								
511200	Sonstiger Warenkreditbetrug	185.032	57.070	22,7	30,8	33.800	59,2	19.674
511300	Warenbetrug	105.792	77.348	30,7	73,1	62.048	80,2	31.857
517100	Leistungsbetrug	20.977	3214	1,3	15,3	1332	41,4	905
517200	Leistungskreditbetrug §§ 263, 263a StGB	33.358	7976	3,2	23,9	2787	34,9	2323

(Fortsetzung)

Tab. 1 (Fortsetzung)

Schlüssel	Ausgewählte Straftaten/-gruppen	Erfasste Fälle insgesamt (Tabelle 01)	Erfasste Fälle mit Tatmittel INTERNET (Tabelle 05)	%uale Verteilung Sp 4	%-Anteil Sp 4 an Sp 3	Aufgekl. Fälle mit Tatmittel INTERNET (Tabelle 05)	AQ	Tatverdächtige mit Tatmittel INTERNET (Tabelle 05)
1	2	3	4	5	6	7	8	9
[a]517500	Computerbetrug (sonstiger)	13.338	9516	3,8	71,3	4161	43,7	2581
518900	Sonstige weitere Betrugsarten	150.026	15.414	6,1	10,3	7784	50,5	5737
715000	Straftaten gg. Urheberrechtsbestimmungen	8085	3655	1,5	45,2	2709	74,1	2699
Summenschlüssel								
897000	Computerkriminalität	108.510	64.169	25,5	59,1	25.024	39,0	14.833
893000	Wirtschaftskriminalität	74.070	5105	2,0	6,9	3373	66,1	1907

[a]Soweit nicht unter den Schlüsseln 511120, 511212, 516300, 516520, 516920, 517220, 517900,518112 bzw. 518302 zu erfassen

Tab. 2 Fallentwicklung und Aufklärung – Computerkriminalität. (Quelle: PKS 2017b)

Schlüssel	Ausgewählte Straftaten/-gruppen	Erfasste Fälle		Veränderung		AQ	
		2017	2016	Absolut	in %	2017	2016
897000	Computerkriminalität	108.510	107.751	759	0,7	39,3	37,7
Davon:							
543000	Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung -§§ 269, 270 StGB-	8352	8158	194	2,4	46,9	51,4
674200	Datenveränderung, Computersabotage-§§ 303a, 303b StGB-	3596	4422	−826	−18,7	25,1	22,1
678000	Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei	9600	10.638	−1038	−9,8	24,9	23,1
715100	Softwarepiraterie (private Anwendung z. B. Computerspiele)	322	319	3	0,9	95,3	94,7
715200	Softwarepiraterie in Form gewerbsmäßigen Handelns	268	154	114	74,0	71,3	91,6
897100	Computerbetrug	86.372	84.060	2312	2,8	40,5	38,8
Darunter:							
511212	Weitere Arten des Warenkreditbetruges	30.584	24.568	6016	24,5	49,7	50,5

(Fortsetzung)

Tab. 2 (Fortsetzung)

Schlüssel	Ausgewählte Straftaten/-gruppen	Erfasste Fälle		Veränderung		AQ	
		2017	2016	Absolut	in %	2017	2016
516300	Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN	21.960	24.629	−2669	−10,8	34,2	33,5
516520	Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten	9065	9982	−917	−9,2	29,7	29,3
516920	Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel	2497	1906	591	31,0	37,6	33,6
517220	Leistungskreditbetrug § 263a StGB	7428	5948	1480	24,9	27,6	29,5
[a]517500	Computerbetrug (sonstiger) § 263a StGB	13.338	14.722	−1.384	−9,4	44,8	39,5
518302	Überweisungsbetrug § 263a StGB	933	1419	−486	−34,2	37,3	32,8

[a]Soweit nicht unter den Schlüsseln 511120, 511212, 516300, 516520, 516920, 517220, 517900, 518112 bzw. 518302 zu erfassen

derzeit öffentlich verfügbaren Daten, das kriminalpolitisch bedeutsame Gesamtphänomen der Cyberkriminalität in allen ihren relevanten Facetten im Gegensatz zu einzelnen Tatbeständen selbst in einem aufwendigen Erhebungsverfahren über die PKS-Tabellen 1, 5 und 7 derzeit nur eingeschränkt kategorial konturieren und weitergehenden Betrachtungen zugänglich machen kann.

Abb. 2 Bundeslagebild „Cybercrime im engeren Sinne“. (Quelle: BKA 2017a)

2.1.3 Definitionen fehlen – das macht die Abgrenzung schwierig

Sucht man weitergehend nach sauber voneinander abgrenzbaren kategorialen Definitionen, wird man damit zwar in der PKS selbst (neben den deliktischen Inhalten der genannten „Summenschlüssel“ sind dies aber eher Erläuterungen zu

den Erfassungsmodalitäten), in darüber hinausgehenden Cybercrime-Lagebildern, in Lehr- und Fachbüchern wie auch in behördlichen Fachfeinkonzepten reichhaltig, aber im Ergebnis inhomogen versorgt.[12] Das ist für eine phänomenologische Betrachtung unter kriminologischen Aspekten nicht sehr ergiebig, vielleicht aber aufgrund der inzwischen beinahe vollständigen „digitalen Sättigung“ unseres Alltags und den dabei implizit eröffneten vielfältigen Tatgelegenheiten und Modi Operandi noch nachvollziehbar. Auch das Internet selbst kann ja als „Tatmittel“ missbraucht und als „virtueller Tatort“ genutzt werden, und das beinahe in jedem Deliktsbereich.

Dennoch bleibt die Ausgangslage strukturell unbefriedigend. Nebenbei bemerkt, kriminalpolizeilich wird also jedes Fachkommissariat, sowohl bei der kriminalistischen Hypothesenbildung als auch bei den sich daraus ergebenden Ermittlungspaketen, fast durchgängig auch mit intensiven „Netzwerkspurenkomplexen“ befasst sein, obgleich sich die eigentlichen Fachleute hierzu (insbesondere auch extern nach Abschluss entsprechender Hochschulstudiengänge gewonnene IT-Forensiker und -Kriminalisten) in eigens eingerichteten „Cyber-Fachkommissariaten“ bei innerbehördlicher Spezialisierung auf Straftaten der Kategorie „Cybercrime im engeren Sinne“ konzentrieren. Das führt in der Praxis durch einen extremen Anstieg der Bildung von kommissariatsübergreifenden Ermittlungs- und Arbeitsgruppen allerdings zu beständiger organisatorisch-struktureller Unruhe. Ganz zu schweigen von der zusätzlichen Notwendigkeit ständig verfügbarer OSINT-Expertise[13] bei Schutz- und Kriminalpolizei, nicht nur zur eigenständigen und möglichst frühzeitigen Detektierung von Gefahrensachverhalten und deren Abwehr, sondern auch ermittlungsbegleitend und -initiierend.

2.1.4 Dunkelfeld – Deutungshoheit

Als Einstieg in dieses Teilkapitel eignen sich die kriminologischen Kategorien des Hell- und Dunkelfeldes. Mithilfe einer Grafik des BKA (Abb. 3; s. a. Kap. „Problematik der Hell- und Dunkelfeldanalyse im Bereich Cybercrime“) lassen sich die in der Literatur verwendeten Begrifflichkeiten *absolutes/relatives*

[12]Immer wieder zitiert wird auch die allgemeine Differenzierung der Europäischen Cybercrime-Konvention vom 23. November 2001.

[13]Open Source Intelligence. Diese erlangt bei der Polizei, auch bei der unmittelbaren Einsatzbewältigung und nicht nur bei der Ermittlungsarbeit z. B. im Rahmen von „SENTINEL-“ oder „INTEL-OFFICER-Projekten“ etwa in Einsatzzentralen immer größere Bedeutung.

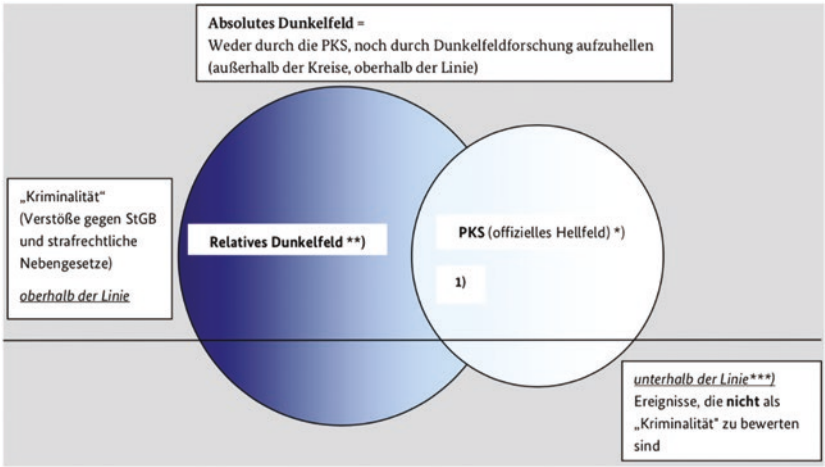


Abb. 3 Aspekte des Hell- und Dunkelfeldes. (Quelle: PKS-Jahrbuch 2016b, Band 1, S. 7)

Dunkelfeld und *Hellfeld* sowie hieraus entstehende „kriminalstatistische Interpretationsspielräume“ gut darlegen.

Aus der Grafik erschließt sich der Begriff des „absoluten“ Dunkelfeldes sehr prägnant. Gründe für ein solches können u. a. folgende sein:

- Eine große Anzahl strafbarer Handlungen im Internet kommt aufgrund zunehmender technischer Sicherungseinrichtungen über das Versuchsstadium nicht hinaus und wird von den Geschädigten gar nicht bemerkt.
- Die betroffenen Personen bemerken lange Zeit oder gar nicht, dass sie Opfer einer Cyber-Straftat geworden sind (z. B. bei Diebstahl ihrer Identität bei einem Online-Shop) bzw. dass von ihnen eingesetzte technische Geräte unbemerkt zur Begehung von Cybercrime-Straftaten missbraucht werden (z. B. Nutzung infizierter PCs oder Router als Teil eines Bot-Netzes zur Ausführung von DDoS-Angriffen).
- Geschädigte erstatten beispielsweise in Erpressungsfällen oftmals nur dann Anzeige, wenn trotz Zahlung eines Lösegeldes keine Dekryptierung des durch die Täterseite zuvor verschlüsselten Systems erfolgt (auch bei anonymisierten Dunkelfeldbefragungen wird aus Scham oder anderen subjektiven Gründen die Viktimisierung nicht benannt). Im letztgenannten Fall würde die PKS-Erfassung auch nicht unter der Kategorie „Cybercrime i.e.S.“ erfolgen.

Vielmehr würde die schwerste Straftat (in diesem Fall i. d. R. nach § 253 StGB, „Erpressung“) in der PKS mit dem spätestens bei Auslauf der Anzeige an die StA händisch erzeugten Sachbearbeiter-Vermerk „Tatmittel Internet“ erfasst werden.

Neben diesem Phänomen lässt sich daneben auch noch ein „relatives“ Dunkelfeld identifizieren. Im Unterschied zum „absoluten“ Dunkelfeld ließe sich, entsprechende Viktimisierungssurveys (siehe Abschn. 2.3) vorausgesetzt, das „relative“ Dunkelfeld deliktisch bei Opfern und Behörden durchaus signifikant validieren und auch strukturell verkleinern. Welche Gründe für ein solches „relatives“ Dunkelfeld lassen sich finden?

- *Geistiges Eigentum:* Downloads von Schriften, Bildern und Musik können unter bestimmten Voraussetzungen urheberrechtliche Verstöße darstellen; häufig haben die Rechteinhaber aber ausschließlich Interesse an einer *zivilrechtlichen Geltendmachung* von Ansprüchen, die sie v. a. im gewerblichen Sektor z. B. über den Auskunftsanspruch ggü. dem Provider nach § 101 Urheberrechtsgesetz (UrhG) gelten machen.
- *UrhG:* Anzeige wird ggf. direkt an die Staatsanwaltschaft versandt; dort, unterhalb einer Bagatellgrenze (i. d. R. bis zu von 50.-EUR), werden sie dem Opportunitätsprinzip folgend ggf. sofort eingestellt, wodurch keine polizeiliche Erfassung in der PKS erfolgt.
- Tatort unbekannt oder im Ausland (sehr häufig bei Computerkriminalität – seit 2014 werden diese Delikte nicht mehr in der PKS erfasst, vgl. Bundeslagebild Cybercrime 2016a, S. 3). Allerdings soll dieser phänomenologisch untragbare Umstand ab 1. Januar 2019 durch eine neben der PKS eigenständig „begleitend geführten“ statistischen Erfassung wieder „geheilt“ werden.
- Erfassungsfehler im Rahmen der Sachbehandlung bei der Polizei und mangelnde Qualitätskontrolle bei der PKS-Freigabe.
- In der PKS gilt das „Prinzip der Einmalerfassung“ (Telekom-Router-Hack im Jahr 2016 mit ca. 1,25 Mio. Geschädigten ist damit kriminalstatistisch i. d. R. immer nur *ein* Fall).
- Straftaten werden durch Geschädigte nicht angezeigt, insbesondere, wenn noch kein finanzieller Schaden entstanden ist (z. B. bloßer Virenfund durch Scanner auf dem PC).
- Geschädigte, insbesondere Firmen und Gewerbetreibende, zeigen erkannte Straftaten nicht an, um bspw. im Kundenkreis die Reputation als „sicherer und zuverlässiger Partner“ nicht zu verlieren. Sie wollen auch nicht, dass über dies und über Firmeninterne ggf. in einer öffentlichen Hauptverhandlung

gesprochen wird. Diese Kategorie könnte demnach grundsätzlich auch im „absoluten Dunkelfeld" verortet werden, da sich Unternehmen hierzu u. U. aus den gleichen Gründen auch bei anonymisierten Umfragen i. d. R. nicht „outen" werden.

- Im Gegensatz zur PKS umfasst der „Sondermeldedienst Cybercrime" (ab 2019 deliktischer Übergang zu PIAV[14]) zusätzlich Auslandstaten und auch Vorgänge, bei denen neben der Cybercrime-Komponente höherwertige Tatbestände verwirklicht wurden (z. B. Erpressungsdelikte – wobei dann kriminalstatistisch nach den PKS-Richtlinien nur das „höherwertige Delikt", hier also die „Erpressung" nach § 253 StGB, s. o., erfasst wird!).[15]
- Meier (2015a, S. 99[16]) spricht darüber hinaus sogar von einer Reduzierung des objektiven Verfolgungsrisikos durch mangelnde Ressourcen bei den Strafverfolgungsbehörden.

Weil der Phänomenbereich Computerkriminalität (inkl. Erfassungsoption „Tatmittel Internet") technisch und deliktisch außerordentlich vielfältig und damit phänomenologisch nur schwer greifbar bleibt, ist auch das derart strukturell bedingte Dunkelfeld exorbitant hoch. Seriöse Angaben hierzu sind aufgrund der vorhandenen, meist regionalen und daher nicht ausreichend repräsentativen Studienergebnisse zwar kaum möglich. Die wenigen kursierenden

[14]Bundesweiter „Polizeilicher Informations- und Analyseverbund" im „Data-Warehouse BKA" (Teil der „Saarbrückener Agenda" der IMK und der daraus folgenden Strategie „Polizei 2020"), welcher weitgehend den Kriminalpolizeilichen Meldedienst (KPMD) bzw. Sondermeldedienste ablöst.

[15]Gerade dieser Umstand führt zu signifikanten *statistischen Unschärfen* bei der PKS, da z. B. *„einzelne relevante Phänomene, wie Erpressungshandlungen im Zusammenhang mit gezielten DDoS-Attacken oder auch mit sogenannter Ransomware (‚Scareware'), in der PKS* nicht *unter dem Begriff ‚Cybercrime im engeren Sinne' erfasst werden, sondern gemäß PKS-Richtlinien unter den PKS-Schlüsseln der schwerwiegenderen bzw. speziellen Tat, z. B. der Erpressung. Derartige Fallkonstellationen können aber dennoch (wenngleich auch nicht spezifisch) aus den Zahlen zum ‚Tatmittel Internet' errechnet werden"* (Bundeslagebild Cybercrime 2016a, S. 4).

[16]Da seit diesem Zeitpunkt bis heute personell, logistisch und auch organisatorisch enorme Anstrengungen unternommen worden sind, müsste man die damalige Argumentationsgrundlage Meiers nochmals überprüfen. Auch hierin läge ein signifikantes kriminologisches/polizeiwissenschaftliches Aufgabenfeld.

Ergebnisse/Schätzungen sind allerdings auch unter diesem Vorbehalt geradezu erschreckend.[17]

Vereinzelt, u. a. hinsichtlich des ersten Punktes auch durch das BKA oder bei Huber (2015), werden über die oben genannten Gründe noch weitere Variablen für statistische Unschärfen genannt, z. B.:

- Mangel an Vertrauen in die (operative) Leistungsfähigkeit der Polizei bei der Aufklärung der Delikte im Cyberraum (was besonders bedenklich wäre und schon deshalb der genaueren polizeiwissenschaftlich begleiteten Untersuchung bedürfte)

[17]Laut einer Studie des Branchenverbandes *bitkom* aus dem Jahr 2016 wurde alleine innerhalb des der Befragung vorangegangenen Jahres *jeder zweite Internet-Nutzer* Opfer von Internetkriminalität. Nach einer Pressemitteilung des Branchenverbandes *bitkom* vom 8. November 2017 haben *„trotz aller Schutzmaßnahmen rund zwei Drittel der Internetnutzer das Gefühl, dass sie es gar nicht merken würden, wenn Fremde ihren Computer oder ihr Smartphone ausspionieren würden. […] Nur jeder Dritte sieht sich selbst in der Lage, seine Geräte ausreichend vor Angriffen durch Cyberkriminelle zu schützen.“* Wenn wir diese Bezugszahlen mit dem Hellfeld in der PKS vergleichen, dann wird die Diskrepanz zu den anzunehmenden tatsächlichen Fallzahlen schon hierdurch offensichtlich. Nach Einschätzung des BKA und unter Bezugnahme auf verschiedene empirische Studien (unter anderem eine sehr aufwendige Untersuchung des DIW aus dem Jahr 2015 und des LKA Niedersachsen aus dem Jahr 2012 und 2016) ist von „einem sehr großen Dunkelfeld auszugehen“ (vgl. hierzu auch Website des BKA, Themenschwerpunkt Internetkriminalität/Cybercrime). So errechnet bspw. das DIW in der o. g. Studie (Riekmann et al. 2015) auf der Basis von Zahlen der Jahre 2012–2014 einen jährlichen Mittelwert von *14,7 Mio. (!) Delikten* im Bereich Cybercrime, wohingegen die PKS in diesem Zeitraum durchschnittlich rund 250.000 Delikte auswies (rechnet man die Delikte „Tatmittel Internet“ mit, entspräche das dann einem durchschnittlichen Dunkelfeld von etwa 1:60!). Sehr aussagekräftige, weil reliable und valide Ergebnisse der weiter oben zitierten regionalen Dunkelfeldstudie des LKA Niedersachsen aus dem Jahr 2012 im Bereich Cybercrime zeigen z. B. bei Betrug mittels Internet ein Dunkelfeld, welches das Vierfache der bei den Strafverfolgungsbehörden durch Anzeige bekanntgewordenen Fälle beträgt; beim Phänomen Phishing wird das Zehnfache und schließlich bei Datenverlusten und finanziellen Verlusten Einbußen durch Viren, Trojaner etc. sogar mehr als das Zwanzigfache errechnet! Diese Zahlen wurden im Übrigen 2016 spezifiziert repliziert. Ein letztes Beispiel hierzu aus der österreichischen Wirtschaft: Die Wirtschaftskammer geht nach einem Bericht vom 20. August 2018 („Wirtschaftskammer rüstet gegen Cyber-Attacken auf“, Online-Zeitschrift trend.at) landesweit von rund 25.000 Cybercrime-Attacken *täglich* alleine gegen Unternehmen und Wirtschaftsbetriebe aus. Die im Jahr 2017 in Österreich bekannt gewordenen Fälle belaufen sich auf rund 17.000 Fälle, woraus sich ein Verhältnis zwischen Hell- und Dunkelfeld von rund 1:536 (!) errechnet. Allesamt verheerende Zahlen für den „Gewaltmonopolisten“ Staat!

- Annahme einer nicht umfänglichen Verfügbarkeit polizeilicher Expertise bei der Erstaufnahme (korrespondiert mit Punkt 1)
- Umständlichkeit der Anzeigeabgabe bei bloßen Bagatellschäden (vgl. Kap. „Digitale Rechtsdurchsetzung“).

Aber, trotz der eingeschränkten Aussagekraft der PKS hinsichtlich der Grundgesamtheit der in Deutschland verübten Cybercrime-Straftaten pro Jahr ist festzuhalten, dass es sich deutschlandweit um die *einzige statistische Datenerhebung* handelt, die auf *Fallzahlen basiert,* welche im Rahmen von polizeilichen Ermittlungen erhoben wurden. Damit liefert die PKS grundsätzlich eine qualitativ und quantitativ standardisierte und grundsätzlich auch qualitätsgesicherte Datenbasis trendprägender Straftaten für das Deliktsspektrum und bildet mindestens die Entwicklung der in Deutschland durch die Polizei erfassten und somit der „Lebenswirklichkeit“ zugänglichen Cybercrime-Delikte ab, auch wenn der kriminologische Aussagewert angesichts des exorbitanten Dunkelfeldes beschränkt bleibt, es sich mit wenigen kasuistischen Ausnahmen eher um eine kategoriale Arbeitsbelastungsstatistik der Polizei handelt (nach der sich allerdings auch die personelle und logistische Bedarfsberechnung orientiert!).

Man muss also zwingend um die genannten statistischen und phänomenologischen Schwachstellen wissen. Mit diesem Ausgangsmaterial lässt sich das Phänomen oder einzelne Segmente hieraus derzeit empirisch nicht valide deuten. Streng genommen wären angesichts des Ausmaßes des angenommenen Dunkelfeldes nicht einmal seriöse Trendaussagen möglich, denn die jährlichen Veränderungen zeigen nur eine unterschiedlich hohe Aufhellung des exorbitanten Dunkelfeldes an, was mitunter Zufälligkeiten geschuldet bleibt.

Die entscheidenden Fragen nach dem kurzen und daher dem Anlass geschuldet kursorischen kriminalstatistischen Ausflug ist: Wer hat auf Grundlage welcher Falldaten die deliktische und damit gleichzeitig eine phänomenologische Deutungshoheit? Kann man alleine aus dem Fallaufkommen seriöse Ableitungen vornehmen und verbindliche kriminal- und personalpolitische oder institutionell-organisatorische Schlussfolgerungen ziehen?

2.2 Täter-Opfer-Spezifika/Viktimisierungssurveys

Aus den oben unter Abschn. 2.1 ausgewählten kriminalstatistischen Tabellen ist schon auf den ersten Blick ersichtlich, dass historisch „analog“ angelegte Modi Operandi, vor allem aus dem 14. („Beleidigung“) und dem 18. Abschnitt („Straftaten gegen die persönliche Freiheit“, hier insbesondere die Tatbestände der „Nachstellung“, „Nötigung“ und „Bedrohung“) im Besonderen Teil (BT) des

StGB überhaupt nicht gelistet sind und i. d. R. noch nicht einmal in der Rubrik „Tatmittel Internet“ der Jahrbände PKS dargestellt werden. Dies ist angesichts der anhaltenden Debatte um „Hate Speech“ (s. a. Kap. „Hate Speech in der Computerspielkultur“) und die lebensweltlich inzwischen immer stärker mit dem Präfix „Cyber-“ versehenen Phänomene „Mobbing“, „Bullying“, „Stalking“, „Grooming“ (Kap. „Posterboys und Terrorpropaganda“ und „Grooming-Umgebungen von pädophilen und hebephilen Männern in Deutschland“) u. a. oder zielgerichteten Radikalisierungsstrategien unterschiedlicher Couleur auf den verschiedensten Social Media-Kanälen und -plattformen[18] einigermaßen erstaunlich.

Das macht eingangs dieses Teilkapitels (und auch nur am Rande) deutlich, dass virtuelle „Täter-Opfer-Beziehungen“ ebenso wie die kriminalstatistischen Daten empirisch nach wie vor undeutlich bleiben und es auch hierbei signifikanten Forschungsbedarf gibt. Nach wie vor gibt es also bis auf wenige, empirisch als belegt geltende Ausnahmen im inhomogenen und mit einem exorbitanten Dunkelfeld umsäumten Phänomenbereich Cybercrime über die Kasuistik hinaus kaum eine objektive und valide Möglichkeit, Delikts-, Täter- oder Opferspezifika auf der Grundlage der verfügbaren, insuffizienten statistischen Datenlage herauszuarbeiten.

Wiederum mit Bezug auf Huber, die als eine der wenigen auf dem Gebiet der phänomenbezogen empirischen Täter-Opfer-Analytik sehr aktiv ist, hier ihre deutliche Beschreibung der zugrunde liegenden Problematik:

> „Es gibt kein einheitliches Profil für Cyberkriminelle und nur in wenigen Fällen für Cyberopfer. Abhängig von der Deliktsart variieren die Merkmale der einzelnen Täterinnen und Täter sowie der Opfer massiv. Dunkelziffer und Prävalenzzahlen sind kaum wissenschaftlich erhoben worden. Eine weitere Problematik ist, dass sich bisherige Forschungen hauptsächlich damit beschäftigt haben, Firmen und Staaten als Opfer zu betrachten, wobei deren wirtschaftlicher Schaden im Vordergrund stand. Cybercrimedelikte richten sich aber auch gegen Privatpersonen, die keine Lobby haben, um als Untersuchungsobjekt der industriellen Forschung infrage zu kommen. Die wissenschaftliche Auseinandersetzung steht daher erst am Anfang und es gilt noch viel zu erforschen.“ (2015, S. 399 ff. und Huber und Pospisil 2018[19])

[18]Ein bedeutsames kriminologisches und kriminalistisch anspruchsvolles Thema, dessen sich der Mitherausgeber dieses Bandes, Thomas-Gabriel Rüdiger, seit geraumer Zeit intensiv angenommen hat, sodass ich dieses Themenfeld über diese, das Teilkapitel einleitende kurze Erwähnung im Fortgang meines Beitrags weitgehend ausblende.

[19]In letztgenannter Studie am Beispiel einer hellfeldorientierten regionalen Wiener Täter-Opfer-Erhebung aus den Jahren 2006–2016.

Das ist einerseits sicher ein Dilemma für die repressive und präventive sicherheitsbehördliche Programmatik. Der operative Bedarf für den hilfesuchenden „Kunden" bleibt undeutlich, aber der Dienstleister investiert gehörig, ja er weitet gerade in jüngster Vergangenheit die Ressourcen für die gezielte Kontrolle des Phänomens signifikant aus! Das ist im Grundsatz angesichts der Dimension des Phänomens, welche man in Bezug auf das bestehende Wissensdefizit auch im übertragenen Sinne als „schwarzes Loch" bezeichnen kann, zwar grundsätzlich lobenswert. Es fehlt aus den genannten Gründen allerdings die Zielgenauigkeit. Hierbei wird dann aber ein Mangel an effektivem und effizientem Einsatz der Ressourcen evident.

Andererseits bietet dieses Dilemma aber auch ein interdisziplinäres wissenschaftliches Forschungsfeld, auf dem es viel „umzugraben" und mit „archäologischer Akribie" zu bergen gäbe. An dieser wissenschaftlichen Schnittstelle stehen aber im Moment wohl deutlich weniger Ressourcen zur Verfügung. Es besteht Anschubfinanzierungsbedarf, bspw. via behördlich veranlasster „Auftragsforschung". So könnte sich – wiederum unabhängig von der Frage der Notwendigkeit einer eigenen disziplinären Subkategorie – aus dem derzeit zarten subkategorialen Pflänzchen phänomenologischer und ätiologischer „Cybercrime-Analytik" und der notwendigen Fortentwicklung kriminalistischer „Cyber-Forensik" innerhalb der kriminologisch-kriminalistischen Forschungslandschaft durchaus Einiges entwickeln.

Es gibt in jüngerer Vergangenheit – jedenfalls im deutschen Sprachraum – nur einige wenige Versuche, literaturgestützt (und dadurch nur mittelbar empirisch gesichert) phänotypische Besonderheiten herauszuarbeiten, die sich in gewisser Hinsicht vielleicht sogar verallgemeinern ließen (vgl. auch Lit.-Hinweise Fn. 10). Eines der wenigen Beispiele hierfür ist die Analyse von Bässmann (2015)[20], der sich in seiner Untersuchung „Täter im Bereich Cybercrime – Eine Literaturanalyse" insbesondere intensiv mit der Phänomenologie von Hackern auseinandergesetzt hat (zudem Kap. „Phänomenologie von digitalen Delikten" und „Identitätsbildung im digitalen Zeitalter"). Eine weitere BKA-Studie von Füllgraf (2016)[21] befasst sich im Anschluss daran wiederum ausschnittsweise und ebenso

[20]Tätig in der „Forschungs- und Beratungsstelle Cybercrime", vormals KI 16, inzwischen IZ 36 des BKA. Obwohl die Digitalisierung sämtliche Bereiche des gesellschaftlichen Lebens durchzieht, hat dies (jedenfalls in der Breite) nicht zum Aufkommen neuer Forschungsfragen geführt (Meier 2016, S. 232).

[21]Ihr zufolge *„grenzt sich das Phänomen deutlich von der profitorientierten Cybercrime, wie z. B. dem Phishing ab, obwohl die Untersuchungsergebnisse zeigen, dass Hacktivisten ähnliche Vorgehensweisen wie Cyberkriminelle an den Tag legen."* Die bevorzugten

auf der Grundlage von Hellfelddaten mit dem spezifischen Phänomen und den Motiven gruppengestützten „Hacktivismus“ (s. Kap. „Phänomenologie von digitalen Delikten“). Ähnliches gilt für eine länderübergreifende englischsprachige Studie, ebenfalls aus dem BKA, zur „Cyber-OK“ (Bulanova-Hristova et al. 2016) mit einigen interessanten hellfeldbasierten Hinweisen zur Täterstruktur.

Empirische Studien sind im deutschen Sprachraum leider ebenso rar (s. Kap. „Phänomenologie von digitalen Delikten“ und „Identitätsbildung im digitalen Zeitalter“). Bspw. hat Meier (2015a, b) auf der Grundlage einer (nach zugänglicher Aktenlage) nur bedingt repräsentativen Stichprobe verschiedene analoge Kriminalitätserklärungstheorien in Bezug auf das Unrechtsbewusstsein und ihre Übertragbarkeit auf den „virtuellen Raum als Tatort“ am Beispiel illegaler Downloads untersucht, dabei insbesondere also Täterspezifika erhoben. Größere Stichproben mit ergänzendem Bezug auf das Phänomen Cyberkriminalität finden derzeit im Rahmen von regionalen, wissenschaftlich (z. B. durch das KfN) begleiteten, repräsentativen Viktimisierungssurveys (z. B. in den Bundesländern Niedersachsen, vgl. Fn. 20, oder Schleswig-Holstein, vgl. Dreißigacker und Riesner 2018[22]) statt. Natürlich sind auch die jährlichen repräsentativen Umfragen oder spezifische Studien der Branchenverbände, bspw. von „bitkom-research“ oder dem „DIW“, mindestens zum Trendsetting bzw. -watching nicht uninteressant, sofern sie täterspezifische oder viktimologische Teilaspekte aufgreifen.

Die kurze und unvollständige Aufzählung zeigt aber auch bei der empirischen Grundlage zu Täter- und Opferspezifika eine signifikante Insuffizienz. Obwohl die Forderungen aus der Wissenschaft für regelmäßige, die PKS und die Strafverfolgungsstatistik ergänzende periodische Dunkelfeldstudien bzw. Viktimisierungsbefragungen seit geraumer Zeit (nicht nur in Deutschland) erhoben werden[23], sind die getroffenen Maßnahmen und die erzielten Ergebnisse

---

strafrechtlich relevanten Vorgehensweisen der Hacktivisten, um im digitalen Raum Protest und/oder Propaganda auszuüben sind „Web-Defacement“, DDoS-Angriffe sowie das Ausspähen und Manipulieren von Daten. Hacktivismus findet überwiegend in und durch Gruppierungen statt, welche üblicherweise aus einem festen Kern bestehen und abhängig von den jeweiligen Aktionen in der Gesamtmitgliederzahl stark schwanken können. In der Mehrzahl beteiligen sich männliche Personen zwischen 16 und 30 Jahren an „hacktivistischen“ Aktionen. Dabei können jedoch auch (erhebliche) materielle Schäden entstehen.

[22]Somit die derzeit jüngste empirische Studie nach dem Erscheinungsdatum, allerdings auf der Grundlage von repräsentativ erhobenen Daten der Jahre 2015, repliziert 2017.

[23]Vgl. hierzu nur den ersten Periodischen Sicherheitsbericht der Bundesregierung, 2001. Im Koalitionsvertrag zw. CDU/CSU und SPD für die 19. Legislaturperiode 2017–2021 (vgl. dort S. 133, Z. 6292 ff.) ist im Übrigen von *„einer zügigen Aktualisierung des Periodischen Sicherheitsberichts“* die Rede.

zwar ein wichtiger erster Schritt, nach wie vor (insbesondere auf dem Gebiet der Computerkriminalität) jedoch „lückenhaft".[24]

Im Übrigen wird dieses Problem nicht nur in Deutschland, sondern auch auf Ebene der EU[25] erkannt. Um die Innen- und Justizpolitik in den Mitgliedstaaten besser aufeinander abstimmen zu können, hat die Europäische Kommission von Eurostat die Schaffung einer zuverlässigen und vergleichbaren Datenbasis für Europa gefordert. In diesem Zusammenhang hat Eurostat eine europaweite Bevölkerungsumfrage über Kriminalität und Sicherheitsempfinden (Viktimisierungsbefragung) vorbereitet. Eine solche Befragung verspricht eher vergleichbare Ergebnisse zum Ausmaß der Kriminalitätsbelastung zu liefern, als dies ein Vergleich der amtlichen Daten zur registrierten Kriminalität derzeit leisten kann, da sich in den Ergebnissen der amtlichen Polizei- und Justizstatistiken vor allem die unterschiedlichen nationalen Rechts- und Justizsysteme in Europa widerspiegeln. Mit der Planung der europäischen Viktimisierungsbefragung *European Safety Survey* (EU-SASU) sowie dem Test einer neuen Welle des *International Crime and Victim Surveys* (ICVS-2) scheint die in den letzten Jahren ins Stocken geratene internationale Dunkelfeldforschung jedoch zu prosperieren (Guzy 2014, S. 149 ff.).

Der deutsche Viktimisierungssurvey 2012[26] (Birkel et al. 2014) ist als ein Kernelement eines umfassenden Projekts zur Erstellung eines Sicherheitsbarometers für Deutschland eingebettet (BASiD, gemeinsam koordiniert durch das BKA und das MPICC in Freiburg). Er ordnet sich ferner in eine europäische und internationale

[24]Einen guten Gesamtüberblick zu diesem Thema bieten die 2015 durch Guzy et al. zusammengestellten und durch das BKA herausgegebenen beiden Bände „Viktimisierungsbefragungen in Deutschland".

[25]Immerhin wurde im Rahmen der supranationalen Fortentwicklung der EU im Vertrag von Amsterdam im Jahre 1997 für den Verbund der Union erstmals das Ziel eines gemeinsamen „Raums der Freiheit, der Sicherheit und des Rechts" erklärt. Bis dato war auf der Grundlage des EUV (alte Fassung) die polizeiliche und justizielle Zusammenarbeit in Strafsachen (PJZS) in der dritten Säule der Europäischen Union geregelt. Die Mitgliedsstaaten arbeiteten in der dritten Säule vor allem intergouvernemental zusammen. Die intergouvernementale Zusammenarbeit findet, im Gegensatz zur supranationalen Zusammenarbeit, vor allem auf zwischenstaatlicher Basis statt. Durch den Vertrag von Lissabon wurde zwar die bisherige Säulenstruktur der Europäischen Union aufgelöst, allerdings bestehen für die Gemeinsame Außen- und Sicherheitspolitik (GASP) und den Raum der Freiheit, der Sicherheit und des Rechts (RFSR), der die PJZS ablöst, weiterhin Sonderregelungen (bspw. für das Vereinigte Königreich, Irland und Dänemark, vgl. Protokoll Nr. 1 zum Vertrag von Lissabon, ABl. 2007 C306/185 ff.), die einen intergouvernementalen Charakter aufweisen (vgl. hierzu Art. 67 Abs. 1 AEUV).

[26]Gemeinsam hrsg. vom BKA und MPICC in Freiburg.

Entwicklung (s. o.) ein, die eine regelmäßige Sicherheitsberichtserstattung nicht bloß auf Analysen der amtlich registrierten Kriminalität stützt. Vielmehr zeigen die Erfahrungen, dass tragfähige Beurteilungen der Sicherheitslage neben den polizeilichen Kriminalstatistiken dringend auf Opferbefragungen angewiesen sind. Dabei steht zwar zuerst das Ausmaß der von polizeilichen Kriminalstatistiken nicht erfassten Kriminalität, also das konventionelle Dunkelfeld, im Mittelpunkt. Daneben finden vor allem aber auch solche Straftaten Aufnahme, die, wie die Cyberkriminalität, wegen ihres Charakters als neue Kriminalität in besonderem Maße von subjektiven Faktoren geprägt werden. Es ist jedoch gleichermaßen von Bedeutung, aus welchen Gründen Anzeigen gestellt oder unterlassen werden, wie die Strafverfolgung wahrgenommen wird und welche Erwartungen und wieviel Vertrauen Polizei und Strafjustiz entgegengebracht werden. Mit dem Deutschen Viktimisierungssurvey 2012 werden durchaus einige dieser Lücken geschlossen und Maßstäbe gesetzt. Der Survey war als nationale Befragung ausgestaltet und umfasste erstmals eine große Stichprobe von etwa 35.000 Befragten.

In Bezug auf die Computerkriminalität finden sich in der Zusammenfassung dieses Surveys allerdings auch nur recht allgemeine statistische Angaben, z. B. über die Anzahl der Nutzer des Internets und ihr Nutzungsverhalten. Ganz vereinzelt und nur ausschnittsweise werden einige zusätzliche Facetten des Phänomens und nur wenige Befunde zur Computerkriminalität aufgegriffen.

2.3 Schadenssummen

Wenn im Abschn. 2.2 im Ergebnis ein strukturell exorbitantes Dunkelfeld als belegt gelten darf, schlägt dies auch auf das Verhältnis zwischen erfassten und tatsächlich vorhandenen, statistisch jedoch nicht ausgewiesenen individuellen wie auch die volkswirtschaftlichen Schäden durch, die durch Cyberkriminalität verursacht werden. Bemerkenswert hierbei ist, dass in den durch das BKA veröffentlichten PKS-Jahrbänden (einschließlich des PK-Exemplars, sogenannte „IMK-Ausgabe“) für das Berichtsjahr 2017 im Unterschied zu den Vorjahren im Rahmen der tabellengestützten phänomenologischen Kurzdarstellung keine kategorialen Schadenssummen für Computerkriminalität ausgewiesen sind. Ein Motiv hierfür könnte die immer wieder kritisierte Diskrepanz zwischen kriminalstatistischen und öffentlich kursierenden Schadenssummen gewesen sein. Für die „Lücke“ gibt es statistische Ursachen (Bundeslagebild Cybercrime 2016a):[27]

[27]Nachfolgend zitierte Aussagen wurden dem Bundeslagebild Cybercrime 2016a, S. 7, entnommen.

> „Schäden im Deliktsbereich Cybercrime werden in polizeilichen Statistiken ausschließlich für Fälle des Computerbetrugs – sofern kategorial ‚Cybercrime im engeren Sinne' – und der missbräuchlichen Nutzung von Telekommunikationsdiensten ausgewiesen. Die für 2016 ausgewiesene Gesamtschadenssumme betrug 51,63 Mio. Euro. Vom erfassten Gesamtschaden entfielen rund 50,9 Mio. Euro (2015: 40,51 Mio. Euro) auf den Bereich Computerbetrug und rund 0,73 Mio. Euro (2015: 4,6 Mio. Euro) auf die missbräuchliche Nutzung von Kommunikationsdiensten. […] Da lediglich zu den genannten Deliktsbereichen des §263a StGB eine statistische Schadenserfassung erfolgt, sind keine belastbaren statistischen Aussagen zum tatsächlichen rein monetären (Gesamt-)Schaden durch Cybercrime möglich. Oft sind finanzielle Schäden eines erfolgreichen Cyber-Angriffes nicht gänzlich bekannt oder können nicht beziffert werden. Reputationsverluste, Imageschäden oder entstehende Wartezeiten und Produktionsausfälle lassen sich in finanzieller Hinsicht kaum seriös darstellen (wären aber durchaus als ‚volkswirtschaftlicher Schaden' relevant). Hinzu kommt, dass je nach Ausgestaltung des Angriffs oft nicht nur ein einzelnes System für einen bestimmten Zeitraum ausfällt, sondern teilweise gesamte Netzwerke lahmgelegt werden. Zur Darstellung des tatsächlichen Schadensausmaßes müssen demnach verschiedene (andere) Faktoren berücksichtigt werden."

Diese statistischen Bemerkungen sind allesamt sachlich nachvollziehbar, dennoch entsteht hierdurch ein „deliktisches Zerrbild", welches in seiner Aussagekraft dem einer „Spiegelstraße im Kuriositätenkabinett" entspricht. Durch seine Verzerrung bis zur Unkenntlichkeit hat es kaum noch etwas mit der Lebenswirklichkeit zu tun. Die aus verschiedenen Quellen gespeisten Zahlen, die über die kriminalstatistisch erfasste Schadenssumme hinausgehen, differieren. Es zeigt sich allerdings eine ähnliche Diskrepanz[28] wie bei den Fallzahlen selbst.

[28]Wieduwilt schreibt in der FAZ vom 21. Juli 2017 („Cyberkriminalität: Teure Rufschädigung durch frustrierte Kollegen") zu mutmaßlichen Schadenssummen, die alleine der deutschen Wirtschaft entstünden: *„Einmal das gesamte Budget des Freistaates Bayern: So viel sollen Datendiebstahl und Sabotage deutsche Unternehmen kosten."* Bitkom bestätigt diese Größenordnung von etwa 55 Mrd. EUR alleine für die deutsche Wirtschaft in einer PM vom 21 Juli 2017. Nach Erhebungen des Portals „statista" sollen es 2017 insgesamt bis zu 109 Mrd. EUR gewesen sein. Im „Norton Cyber Security Insights Report", auf den sich die ZEIT vom 23. Januar 2018 bezieht („Studie: 23 Millionen Opfer von Cyber-Kriminalität in Deutschland"), sei im Jahr 2017 den Opfern ein Schaden von 2,2 Mrd. EUR entstanden. Aus einer Studie des Center for Strategic and International Studies (CSIS), die in Zusammenarbeit mit dem IT-Security-Anbieter McAfee erstellt wurde, ging hervor, dass nirgendwo auf der Welt der Schaden durch Verbrechen unter Ausnutzung von Informations- und Kommunikationstechnik gemessen am Bruttoinlandsprodukt (BIP) so hoch ist wie in Deutschland (vgl. Huber 2015, S. 394). Das CSIS (Studie „Economic Impact of Cybercrime" vom 21.02.2018) berichtet hierzu z. B. 2014 von einer jährlichen Schadenssumme (weltweit) von 445 Mrd. US$ und steigert diese Schadensannahme im Jahr 2017 sogar auf rund 600 Mrd. US$, eine Steigerung von knapp 35 % in 3 Jahren! Dies entspräche ca. einem Prozent des globalen GDP („gross domestic product").

Vor allem wird aber eine erhebliche Streubreite offenbar, weshalb die Werte zur Abrundung dieses Topos auch „nur“ in die Fußnote „verbannt“ und beispielhaft erwähnt werden sollen.

Welche Wirkungen entstehen angesichts derart „sozialschädlicher“ und in der Höhe „gesellschaftsgefährdender“ Schadenssummen für den Rechtsstaat? Kann eine derartige Diskrepanz amtlicher Berichterstattung im Verhältnis zu öffentlich kursierenden Größenordnungen das dem Rechtsstaat wesenseigene staatliche Gewaltmonopol diskreditieren oder gar gefährden? Wie hoch ist angesichts dieser wenigen statistisch bekannten Rahmendaten im Vergleich zur angenommenen phänomenologischen Realität die Entdeckungs- und Verfolgungswahrscheinlichkeit im „virtuellen Raum“?

Auch hinsichtlich dieser sowohl kriminalistischen wie auch kriminologischen Fragestellungen entsteht komplementär zur dargelegten Problematik der statistischen Fallzahlenanalytik und der damit verbundenen Frage der kriminalstrategischen „Deutungshoheit“ wie auch in Bezug auf das Problem der Täter-Opfer-Analyse ein interdisziplinär bedeutsames (kriminologisches, sozialwissenschaftliches bzw. – mit Blick auf das „Gewaltmonopol“ – ein durch empirische Daten anzureichendes rechtsphilosophisches), aber derzeit weitgehend unbestelltes phänomenologisches Forschungsfeld. Vor allem darf man sich – auch mit Blick auf die Verlässlichkeit der Durchsetzung des staatlichen Gewaltmonopols und Bezug nehmend auf die auch heute, gut 50 Jahre nach der ersten Formulierung durch Heinrich Popitz (1968) noch immer interessante Theorie der „Präventivwirkung des Nichtwissens“[29] – mit einigem Unbehagen die zusätzliche Frage stellen, was würde eigentlich passieren, wenn ein beträchtlicher Teil der Opfer im „relativen“ Dunkelfeld tatsächlich Anzeige erstatten würde?

2.4 Was bleibt, sind vor allem Herausforderungen!

Wir wissen über die Phänomenologie der Computerkriminalität noch viel zu wenig, um tiefer gehende Feststellungen und Ableitungen aus den vorhandenen Fakten vorzunehmen, oder, um es im übertragenen Sinne mit einer Sentenz von Jules Lequier auszudrücken:

[29]Popitz äußerst sich darin dezidiert zur Normstabilisierungsfunktion des Dunkelfeldes und leitet ab, dass *„bei Ahndung aller Normbrüche das Normensystem kollabieren würde“*. Die Theorie ruft bis heute wissenschaftliches Interesse hervor und wird, jedenfalls was die Auswirkung der normstabilisierenden Wirkung der Dunkelziffer betrifft, durch jüngere Forschungsergebnisse (vgl. z. B. nur Diekmann et al. 2011, S. 74–84) validiert.

> „Wenn wir felsenfest glauben, die Wahrheit zu besitzen, müssen wir wissen, dass wir glauben, und nicht glauben, dass wir wissen.“

Jedenfalls kennen wir aber hinsichtlich der Ausgangsfrage zum Zustand der Konturierung des Phänomens inzwischen eine ganze Reihe von Hindernissen, die es künftig Stück für Stück aus dem Weg zu räumen gilt. Huber (2015, S. 400 f.) fasst die Grundprobleme, die gleichzeitig auch die Punkte darstellen, an denen auf diesem Deliktsfeld künftig für eine jeweils passgenaue phänomenologische Lagedarstellung als Grundlage für kriminologische Expertisen und, hierauf gestützt, kriminalpolitische Initiativen gearbeitet werden muss, sehr treffend zusammen. Betrachte man die Entwicklungen der Rechts- und Kriminalsoziologie, zeige sich in den letzten hundert Jahren ein signifikanter Fortschritt in den Methoden der Erhebung der Dunkelfeldzahlen bei den unterschiedlichsten Delikten. Die wissenschaftliche Auseinandersetzung in Bezug auf Opfer im Bereich von Cybercrime stecke hingegen aber noch in den Kinderschuhen, so Huber. Forschungsarbeiten zum besseren Verständnis von Cybercrimeopfern finde man in erster Linie dann, wenn Firmen oder Staaten zu Opfern werden. Diese fokussierten sich vor allem auf technische Produktentwicklungen zur Prävention. Im Falle von Cybercrimedelikten gegen Privatpersonen stehen jedoch Exekutive und Forschung vor einer neuen Herausforderung, da bestehende Methoden hier weniger gut greifen. Gründe hierfür sind u. a.:

- Es gebe *keine strafrechtliche Definition von Cybercrime;* es seien unterschiedliche Delikte unter den Begriff „Cybercrime“ zu subsumieren, d. h. bei der Erfassung von Cybercrime im Hellfeld müsse jedes Delikt gesondert betrachtet werden. Es gebe also unterschiedliche Arten, wie Cybercrime definiert werden könne. Diese seien abhängig von Kategorisierung und Zuordnung (technisch, juristisch, usw.). Dies spiele insofern eine Rolle bei den Opferbefragungen, als eine *Inkongruenz zwischen den Alltagsvorstellungen über Cybercrimedelikte und den technischen sowie juristischen Bedeutungen* bestehe, wenngleich diese Problematik (eingeschränkt) auch andere Kriminalitätsdelikte betreffe. Zentrale Herausforderung für die Erhebung der Opfer im Bereich von Cybercrime sei daher, Umschreibungen zu finden, die sowohl dem technischen und juristischen Verständnis gerecht, als auch durch die Befragten verstanden werden.
- Das *Misstrauen von Opfern in die Exekutive,* die Täterinnen und Täter zu ermitteln, sei offenkundig massiv (Huber bietet eine der wenigen Fundstellen in der Literatur, wo diese bedenkliche Vermutung in dieser Deutlichkeit ausgesprochen wird!) – vor allem wenn die vermeintlichen Täterinnen

und Täter im Ausland sitzen. Dies reduziere die Bereitschaft, Viktimisierung durch Cybercrimeattacken zur Anzeige zu bringen. Bei vielen Delikten gebe es ein Beweisfindungsproblem, um strafrechtliche Schritte zu setzen. Damit sei gemeint, dass viele Opfer (rein faktisch) nicht in der Lage seien (ihre Vermutung) zu beweisen, dass Tatbestände erfüllt sind, um Anzeigen im strafrechtlichen Sinn nachzugehen. Auch dies reduziere die Anzeigebereitschaft von Opfern erheblich.

- Die *Technikentwicklung* verlaufe derart rasant, dass Lösungen stets hinterherhinken. Nationale und europäische Initiativen, die Forschungen zu Cybercrime unterstützen, fördern primär Vorhaben, die eine Technikentwicklung vorsehen, z. B. die Entwicklung eines neuen Anti-Viren-Programms oder neuer Sicherheitstechniken. Daraus folge, dass ein erheblicher Teil der Cybercrimedelikte nicht oder zu spät erkannt werde bzw. im Nachgang nicht mehr nachgewiesen werden könne.
- Viele Personen wissen nicht, dass sie Opfer von Cybercrimeattacken geworden sind und geben ihre individuellen Vorfälle in Opferbefragungen daher nicht an. Diese Tatsache sei allerdings kein Spezifikum von Opferbefragungen, sondern ein allgemeines, vor allem die Arbeit der Exekutive erschwerendes Problem.
- Auch die Umdefinierung von Opfern zu Täterinnen oder Tätern sei ggf. erheblich. Darauf wurde bereits von BloomBecker (1990) hingewiesen. Oft werde den Opfern eine *Mitschuld an der Straftat* unterstellt. Man hätte doch z. B. ein aktuelles Anti-Viren-Programm installieren müssen oder sei selber schuld, wenn man bei einer Phishing-Attacke die Banken-TAN eingäbe. Dies reduziere die Bereitschaft, eine Opferwerdung durch Cybercrime anzugeben.
- Eine weitere Problematik sei die grundsätzlich *geringe Bereitschaft* einzelner Opfer zuzugeben, Ziel eines Angriffs geworden zu sein. Personen geben in der Öffentlichkeit nicht gerne zu, Opfer eines Cyberangriffs geworden zu sein, da sie sich schämen und *Reputationsverlust* fürchten. Diese Entwicklung betreffe nicht nur Privatpersonen. Die meisten Unternehmen, die Opfer werden, geben dies in der Öffentlichkeit selten zu. Das Sprechen über Cybercrimedelikte werde daher oft tabuisiert.

Nicht nur die Sicherheitsbehörden, sondern auch die Wissenschaft stehen also angesichts der empirischen Validierung möglicher Ursachen für das phänomenologische Dunkelfeld vor eminenten Herausforderungen!

Das betrifft nicht nur die Dunkelfeldaufhellung, sondern wohl auch die Qualitätssicherung der vorhandenen Daten, die offenkundig kein valides kriminalstatistisches Bild widerspiegeln. Zu schließen ist das u. a. z. B. aus dem aktuellen

„Bundeslagebild Cybercrime 2017a" des BKA (S. 6). Dort ist nachzulesen, dass 2017 bspw. drei Viertel aller „Cybercrime-Straftaten im engeren Sinne" als Fälle von Computerbetrug registriert worden sind: *„Recherchen in zwei großen Bundesländern führten (allerdings) zu dem Ergebnis, dass die unter den relevanten Schlüsselzahlen des Computerbetrugs erfassten Delikte in den meisten Fällen keine ‚Cybercrime im engeren Sinne' darstellten. In den meisten Fällen wurden (offensichtlich) Sachverhalte hierunter (polizeilich) erfasst, bei denen das Internet lediglich als Tatmittel fungierte."* Das BKA empfiehlt daher – und das ist angesichts der bereits dargelegten Informationen durchaus bemerkenswert – die Fallzahlen der PKS differenziert zu betrachten und zu bewerten!

3 Herausforderungen für die Kriminalpolitik und die Sicherheitsbehörden

> „Wird die Gewährleistung der Internetsicherheit als Wissensproblem aufgefasst, so stellt sich vor allem für den Staat als wissensbasierte Organisation die Frage, wie das Recht mit diesem Problem umgeht." (Leisterer 2018, S. 5)

Derzeit glauben wir wohl, die Gefahren, welche mit der Nutzung global vernetzter, im Kern weitgehend anonymer Informations- und Kommunikationsstrukturen verbunden sind, (wenigstens technisch) relativ gut einschätzen zu können. Jedenfalls sind die Annahmen hierzu in der Literatur vielfältig und zum Teil auch gut belegt. Ferner versorgen zahlreiche Behörden, Agenturen und Institutionen die Öffentlichkeit präventiv mit Informationen zu aktuellen Bedrohungen. Dieses präventive Sicherungsnetz wird lobenswerterweise grundsätzlich auch immer engmaschiger. Kriminologisch betrachtet wissen wir im Moment allerdings kaum etwas wirklich Verlässliches. Weder können wir aufgrund des ungeheuren Dunkelfeldes in Bezug auf die tatsächlichen Fallzahlen und wegen der allgemein geringen Aufklärungsquoten herausarbeiten, wer die „typischen" Täter sind, ob es diese überhaupt gibt oder ob bzw. wie man diese nach ihren Fähigkeiten oder Motiven ggf. sogar kategorisieren könnte? Wir wissen außerdem nicht wirklich verlässlich, wo und wie sie sich mit der notwendigen „Angriffssoftware" ausrüsten/versorgen. Hierbei ist immer nur pauschal vom „Darknet" und von „Cybercrime as a Service" die Rede. Einzelne spektakuläre Kriminalfälle werden hierbei als Beleg der eigenen Annahme präsentiert.

Wir können zudem kaum mit belastbaren Aussagen zu Täter-Opfer-Beziehungen aufwarten. Bspw. wissen wir nicht wirklich, ob die Täter ihre Opfer gezielt auswählen (wofür z. B. einiges im Rahmen gut gemachter „Social

Engineering-Angriffe“ spräche) oder es sich aufgrund des Tatmediums Internet und des grundsätzlich „Distanzverhältnisses“ hierbei überwiegend um eine Zufallsauswahl seitens der Angreifer handelt (s. a. Kap. „Grooming-Umgebungen von pädophilen und hebephilen Männern in Deutschland“). Wir kennen aus den Viktimisierungssurveys einige Gründe, die Opfer dazu veranlassen, z. B. keine Anzeige zu erstatten. Auch hier bleibt uns Genaueres aber derzeit verborgen, denn strukturiert und nachhaltig validiert sind diese selten wirklich repräsentativen Erhebungen kaum. Es handelt sich bestenfalls um einigermaßen seriöse Annahmen.

Zuletzt, der volkswirtschaftliche Schaden und damit die Auswirkung auf unsere Gesellschaft und deren soziale und kohäsive Grundlagen sind, legt man die verschiedenen Schätzungen zugrunde, enorm. Sie bewegen sich in der Spitze in einer Größenordnung von knapp 15 % des aktuellen Bundeshaushaltes! Das individuelle wie auch das gesellschaftliche Bedrohungsniveau dieses Kriminalitätsphänomens ist nicht nur beträchtlich, sondern vielmehr bereits exorbitant zu nennen.

Was lässt sich aus dieser einleitenden Darstellung ableiten? Nach derzeit signifikant ergänzungsbedürftiger objektiver Faktenlage können sich beide Institutionen zwar rechtstatsächlich und daher vornehmlich kasuistisch, aber kaum umfassend kategorial und evidenzbasiert phänomenologisch/ätiologisch mit der Cyberkriminalität auseinandersetzen. Wenn wir glauben, kasuistisch einen gebräuchlichen Modus Operandi kriminalistischem Handwerk zugänglich gemacht zu haben, haben sich die Urheber in den Tiefen des Netzes oftmals bereits wieder Umleitungen gesucht und die „Spur ist kalt“. Überspitzt und mit einer Metapher angereichert formuliert, versuchen wir derzeit „den Auguren gleich, die aktuelle Situation und die erforderlichen Maßnahmen gleichsam aus dem Vogelflug oder den Eingeweiden von Opfertieren zu ergründen.“ Diese in der Zeit vor Christi Geburt in Rom gebräuchliche priesterliche „Empirie“ ist in der Moderne aber wohl kaum geeignet, rationaler, evidenzbasierter Kriminalpolitik objektive Fakten zu liefern, worauf dann die notwendigen rechtlichen, investiven, institutionell-organisatorischen und personellen Entscheidungen gründen sollten. Zunächst bedürfen diese wesentlichen Fragen also einer möglichst interdisziplinären empirischen Aufhellung.

3.1 Kriminalpolitik

Bundes- und Landesregierungen verfügen über tief reichende, vernetzte Cybersicherheitsstrategien, die sich vor allem dem institutionalisierten und operativen

Schutz des Netzes als Wirtschafts- und Kommunikationsraum und insbesondere auch „kritischen Infrastrukturen" widmen. Diese präventiv ausgerichteten Strategien sind operativ mit „Emergency Response Komponenten" („CERT") angereichert. Schon wegen der Ubiquität möglicher Bedrohungen an vielen Anknüpfungspunkten sind diese selbstverständlich im europäischen Kontext (unter der Federführung der Europäischen Kommission und des Europäischen Rates) eng miteinander verknüpft. Diese national und supra-national gestalteten präventiven Komponenten sollen jedoch nur am Rande erwähnt sein und stellen im Fortgang keinen Schwerpunkt dieses Beitrags dar. In wirklich intensive, grundlagen- und anwendungsorientierte interdisziplinäre Forschung über die Nutzung der Chancen des Netzes oder seiner technischen Absicherung hinaus, wird derzeit aber noch zu wenig investiert, obwohl es sich wirtschaftlich wie auch kulturell um eine Schlüsseltechnologie handelt, die unser aller Leben in den nächsten Jahrzehnten nachhaltig verändern wird.

Nationalstaatlich ist üblicherweise die wesentlichste, jedoch nach dem „Ultima-Ratio-Prinzip" letzte kriminalpolitische Handlungsoption die Anpassung bestehenden Rechts „de lege ferenda". Handlungsfelder sind hierbei v. a. das öffentliche Recht (Gefahrenabwehr) und das materielle und formelle Strafrecht. Gleichzeitig hat sich inzwischen aber im Cyber-Raum *„ein Maß an Komplexität und ein Grad an Kopplung desselben mit sozialen Prozessen entwickelt, die sowohl für die Infrastruktur ebenso wie für die Nutzer zur Gefahr werden können"* (Leisterer 2018, S. 1). Die Gefahrenlage ist hierbei aber indifferent und bedarf daher nachhaltiger Analyse. Die Rechtswissenschaft darf dabei *„nicht allein oder vorrangig als normtextorientierte Interpretationswissenschaft verstanden, sondern […] muss als problemlösungsorientierte Handlungs- und Entscheidungswissenschaft konzipiert werden"* (Hoffmann-Riem 2014, S. 138). Aber welche rechtlichen Instrumente können dazu beitragen? Hier ist ein m. E. bedeutendes und daher breites Einfallstor sozialwissenschaftlicher bzw. kriminologischer Empirie zur Strafrechtswissenschaft, z. B. im Rahmen einer derart sich verstehenden „Gesamten Strafrechtswissenschaft" eröffnet. Es sollte angesichts bestehender akuter Wissensdefizite rechts- und kriminalpolitisch auch mutig und konsequent genutzt werden.

3.1.1 Strafrecht

„Auf jeden Fall wird uns aber das Thema ‚Cyberkriminalität' beschäftigen. Hier hat die Realität den Gesetzgeber überholt, und es ließe sich manches optimieren

> im Sinne eines klareren, moderneren und effektiveren Strafrechts. Und genau darin sehen wir unsere Aufgabe.“ (Hoven 2018[30])

Wie schwer sich der Gesetzgeber tut, das dem digitalen Zeitalter eigene, neue Phänomen eines in der Fachwelt diskutierten „Zwei-Welten-Theorems“[31], nämlich einer weitgehenden und eigenständigen Parallelität der „Cyber-Welt“ (oder auch der „Fünften Dimension“, vgl. Lange, Fn. 34) und deren wesenseigenen

[30]Zitat aus einem Interview mit Frau Prof. Dr. Hoven, Universität Köln, Begründerin des „Kriminalpolitischen Kreises“ im „Einspruch Magazin“ der FAZ vom 14.03.2018 („Kriminalpolitik – Besser machen statt Besserwissen“).

[31]Für ein „Theorem“ ist aktuell die Meinungsvielfalt vielleicht noch ein wenig zu unstrukturiert, eine h. M. lässt sich hierbei noch nicht erkennen, denn nicht wenige Kriminologen und Sozialwissenschaftler verneinen nach wie vor eine derart strikte lebensweltliche Trennung mit durchaus guten Gründen. Hierzu z. B. kritisch: Wernert (2018, S. 34), der aus kriminologischer Sicht dem Internet nicht die Bedeutung eines „eigenen Erlebnisraumes“ zubilligt. Ebenso kritisch Meier (2015a, S. 96), der den Gedanken eines *„eigenständigen digitalisierten Raumes (Cyberspace), in dem eine selbstständige, dem Leben in der ‚analogen Welt‘ vergleichbare Daseinsform möglich sei und in dem es dementsprechend ganz eigenständige Handlungs- und Tatmotive geben könne“* vollständig verwirft. Gegenmeinung z. B. Mischkowitz (2013, S. 218; vgl. Zitat zur Kap.-überschrift Abschn. 5); Lange und Böttcher (2015, S. 9): Er spricht in Anlehnung an den von Skala (2011) eingeführten Begriff der „fünften Dimension“, die der Mensch mit dem Cyberspace entwickelt habe, von *„Veränderungen großen Ausmaßes […], die die Digital- und Informationsgesellschaft noch verarbeiten bzw. bearbeiten muss, um diese künstliche Dimension mit der natürlichen Lebenswelt und den darin sich historisch entwickelten Regelungen, Einrichtungen und Einigungen in Einklang zu bringen.“* Hierin ist durchaus die Annahme einer eigenständigen, parallelen „Realität“ zu erkennen. Verbindend Hoffmann-Riem (2018, S. 22): *„Das tägliche Leben ist vielfach weder on- noch offline, sondern beides, so dass sich eine neue Welt – die Onlife-Welt – zu bilden beginnt.“* Vermittelnd aber noch ambivalent Jagoda Marinić in ihrer gelungenen Kolumne unter dem Titel „Zuversicht“ in der Süddeutschen Zeitung, Ausgabe vom 30. Dezember 2017: *„Viele Vordenker der digitalen Welt haben vom Internet als einem sozialen Raum geträumt. Doch die sozialen Medien bringen auch die Schwächen des Gemeinwesens ans Licht. Aus ihnen ist (z. B. auch) die größte Vernetzungsplattform für rechte Kräfte und demokratiefeindlichen Lügen geworden. Es wäre eine Illusion zu glauben, die sozialen Medien hätten das alles verursacht. Es war da, verborgen in diesem Gemeinwesen“,* in der sie im Übrigen durchaus *„zuversichtlich“* fortfährt, dass es möglich sei *„das Gelingende besser sichtbar zu machen und dafür reale und digitale Räume zu finden“,* auch wenn es hierbei in Anlehnung an Martin Buber wieder stärker *„des lebendigen Wortes“* bedürfe. Ebenso Leisterer (2018, S. 1): *„Im Laufe der Entwicklung des Internets haben sich ein Maß an Komplexität und ein Grad an Kopplung desselben mit sozialen Prozessen entwickelt, die für die Infrastruktur ebenso wie für Nutzer zur Gefahr werden könnte.“*

Kriminalitätsphänomenen[32] zur „realen, analogen Welt" sachgerecht materiellrechtlich abzubilden, zeigt sich schon im aktuellen Strafrecht. Im Besonderen Teil (BT) des Strafgesetzbuches (StGB) findet sich das Phänomen, an dieser Stelle wird zunächst der inzwischen bei vielen geläufige bzw. immer noch gebräuchliche (Ober-) Begriff „Internetkriminalität"[33] verwendet, an den verschiedensten Stellen verteilt. Dort tatbestandsorientiert an den bereits vorhandenen, definierten und daher (überkommenen) phänotypischen Abschnitten und zumeist schutzgutbezogen. Das Phänomen tritt nach wie vor an *keiner* Stelle der 30 Abschnitte des Besonderen Teils prominent, etwa durch eine eigenständige Abschnittsüberschrift „Internet- oder Computerkriminalität", zutage.[34]

---

[32]Typische Vokabeln, wenn man so will als Unterkategorien der „Cybercrime im engeren Sinne", sind in diesem Zusammenhang z. B. „Cyber-Aktivisten" (Kochheim 2018, S. 214 ff.), Hacking/Hacktivismus, Computer Assisted Crime, Computer Content Crime, Advanced Persistent Threats („APT", gelten als die „Königsklasse" unter Hackerangriffen; Florian Roth, IT-Sicherheitsforscher der Fa. Nextron Systems, listet inzwischen in einer öffentlichen Excel-Liste weltweit etwa 150 relevante „APT-Gruppen" auf, die im Auftrag von Staaten agieren).

[33]Begründet mit der auf den deutschen-österreichischen Philosophen Ludwig Wittgenstein, „Tractatus logico-philosophicus, 1922", These 5.6, zurückzuführenden Sentenz: *„Die Grenzen meiner Sprache bedeuten die Grenzen meiner Welt",* beginnt hier m. E. schon die Notwendigkeit einer grundlegenden Reform der Begrifflichkeiten, wie im Abschn. 2.1 im Rahmen der kriminalstatistisch belegten unscharfen Semantik dargelegt. Nicht nur kriminalstatistisch, auch in der Fachliteratur wird das Phänomen mit differierenden und daher in Bezug auf die tatsächliche statistische Lage verwirrenden Begrifflichkeiten belegt. Ein kleiner Ausschnitt hierzu findet sich z. B. bei Büchel und Hirsch (2014, S. 3 ff.). Dort werden bspw. unter dem Oberbegriff „Internetkriminalität" die nur eingeschränkt zutreffend kategorisierenden Begrifflichkeiten „Cybercrime", „IuK-Kriminalität", „Computerkriminalität" (diese wird, wie dargelegt, dazu noch in der kriminologischen Literatur und im behördlichen Sprachgebrauch häufig mit den Attributen „im engeren" und „im weiteren Sinn" „verbrämt"), „EDV-Kriminalität", „Kriminalität unter Nutzung des Tatmittels Internet", etc. verwendet.

[34]Und das trotz des Umstandes, dass wenigstens nominell mit dem „41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität und zur Umsetzung des EU-Rahmenbeschlusses über Angriffe auf Informationssysteme" vom 24. Februar 2005 (ersetzt durch die Richtlinie 2013/40/EU vom 12. August 2013) und dem „Übereinkommen des Europarats über Computerkriminalität" vom 23. November 2001 (41. StÄG in Kraft getreten am 11. August 2007, Historie des StÄG und der Übereinkommen nachgewiesen in der hier verlinkten elektronischen Bibliothek „GesMat" [steht für Gesetzesmaterialien] des BGH) unmittelbare strafrechtliche Anknüpfungspunkte hierfür gelegt wurden. Mit dem Inkrafttreten des „Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten" am 18. Dezember 2015, in dem auch ein neuer § 202 d StGB (nachgewiesen in der hier ebenfalls verlinkten elektronischen Bibliothek „GesMat" des BGH), „Datenhehlerei" geregelt wurde, wurde damit der Kanon der Straftaten,

Am *unmittelbarsten* lässt sich der direkte strafrechtliche Bezug im Zusammenhang mit der Nutzung informationstechnischer Systeme und der dabei verarbeiteten Daten noch im „Fünfzehnten Abschnitt des Besonderen Teils StGB – Verletzung des persönlichen Lebens- und Geheimbereichs" (insbesondere bei den §§ 202 a–202 d StGB), im „Zweiundzwanzigsten Abschnitt – Betrug und Untreue" (insbesondere § 263 a) oder im „Siebenundzwanzigsten Abschnitt – Sachbeschädigung" (insbesondere §§ 303a und b – Frage: Sachenbegriff?) deuten.

Mittelbar kann man hingegen zu den allermeisten sonstigen strafrechtlichen Tatbeständen Bezüge hinsichtlich der Nutzung informationstechnischer Systeme und damit zum „Internet als Tatmittel" herstellen. Dies gilt insbesondere für Vorbereitungshandlungen (vorbereitende Absprachen, bspw. im Sinne bereits eigenständig strafbarer Tathandlungen [vgl. nur § 30 StGB, „Versuch der Beteiligung"] oder auch bei der akzessorischen Anstiftung, Beihilfe oder der mittelbaren Täterschaft, etc. zu/bei einer späteren Haupttat), auch wenn es *strafprozessrechtlich* zunächst nur um die entsprechende Sicherung flüchtiger Beweismittel bzw., bei der Abwehr von gegenwärtigen oder „drohenden"[35] *Gefahren,* parallel

---

die üblicherweise neuerdings als „Cybercrime im engeren Sinne" nach dem StGB und im Nebenstrafrecht bezeichnet werden (vgl. hierzu auch Wernert 2018, S. 29 f.), weitgehend geschlossen. Derzeit (Stand 27. März 2019) kursiert jedoch ein RefE eines IT-Sicherheitsgesetzes 2.0 als Artikelgesetz, in dem auch wesentliche Änderungen des StGB und der StPO enthalten sind.

[35]Rechtsdogmatisch neu in die gefahrenabwehrrechtliche Systematik im Rahmen einer Entscheidung des BVerfG integriert (BVerfG, Urteil des Ersten Senats vom 20. April 2016, 1 BvR 966/09 zum BKA-Gesetz, vgl. Rn. 112) und inzwischen im BKA-Gesetz und in einigen Länderpolizeigesetzen (z. B. im bayerischen Polizeiaufgabengesetz) gefahrenabwehrrechtlich statuiert. Nach Vorgaben des BVerfG kann *„eine hinreichend konkretisierte Gefahr in diesem Sinne […] danach schon bestehen, wenn sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, sofern bereits bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Die Tatsachen müssen dafür zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann"* (BVerfGE 120, 274 [328 f.]; 125, 260 [330 f.]). In Bezug auf terroristische Straftaten, die oft durch lang geplante Taten von bisher nicht straffällig gewordenen Einzelnen an nicht vorhersehbaren Orten und in ganz verschiedener Weise verübt werden, können Überwachungsmaßnahmen auch dann erlaubt werden, wenn zwar noch nicht ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, jedoch das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie solche Straftaten in überschaubarer Zukunft begehen wird. Denkbar ist das etwa, wenn eine Person aus einem Ausbildungslager für Terroristen im Ausland in die Bundesrepublik Deutschland einreist.

um die Verhinderung eines i. d. R. jedenfalls hinsichtlich Ort und Zeit nur vage skizzierten Szenarios geht. Im Nebenstrafrecht gibt es natürlich ebenfalls, wie u. a. anhand der Kategorie des „Schutzes des geistigen Eigentums"[36], bspw. der (kunst-) urheberrechtlich relevanten Kategorie der „Softwarepiraterie" oder auch bei sonstigen urheberrechtlichen *Plagiatsfällen* im Zusammenhang mit ausschließlich im Internet bereitgehaltenen Texten deutlich wird, viele *mittelbare* Bezugsfälle zu dem Phänomen.

Das Computerstrafrecht unterlag in jüngerer Vergangenheit umfänglicher Modifizierung (vgl. ausschnittsweise hierzu Fn. 37). Trotzdem wird kriminalpolitisch immer wieder Fortschreibungsbedarf angemahnt.[37] Aus der Wissenschaft sind hierzu durchaus unterschiedliche Stimmen zu vernehmen. Diese können hier aber kaum in allgemeiner Aussage und notwendiger Kürze differenziert genug dargestellt werden, schon weil es „die" Internetkriminalität als homogenen rechtsdogmatischen Betrachtungsgegenstand gar nicht gibt. Allerdings lassen sich durchaus verschiedene „Lager" identifizieren. Die einen sehen schon den bestehenden strafrechtlichen Schutz in Teilen als rechtsdogmatisch zu weitreichend, andere erachten den strafrechtlichen Schutz als angemessen, sehen keinen Anlass für ein „Update", sondern erkennen die Probleme vielmehr bei der Straftatenentdeckung und -verfolgung. Diese sei aufgrund des

[36]Welche Bedeutung und Reichweite solche Vorgänge haben können, zeigt ein Verfahren der „Zentralstelle Cybercrime Bayern" (ZCB) bei der Generalstaatsanwaltschaft Bamberg im Zusammenhang mit einem illegalen Portal zum Download von E-Books, E-Paper und Hörbüchern („lul.to"), welches im Juni 2017 in Zusammenarbeit mit dem „Cybercrime Competence Center" des LKA Sachsen vom Netz genommen werden konnte.

[37]So hat z. B. das Bundesland Hessen (BR-Drs. 338/16 – Gesetzesantrag/BT-Drs. 18/10182 – Gesetzesentwurf) über den Bundesrat die Einführung eines Straftatbestandes der „unbefugten Benutzung informationstechnischer Systeme" („Digitaler Hausfriedensbruch"), gliederungstechnisch in einem neuen § 202 e StGB verortet, also einem neuen Haupt- und einen weiteren Vorbereitungstatbestand für spätere Haupttaten gefordert. Der Bundesrat hat im Übrigen in seiner 965. Sitzung (TOP 5) am 2. März 2018 beschlossen (BR-Drs. 47/18), den o. g. Gesetzesantrag (BR-Drs. 338/16) in der Fassung vom 23. September 2016 erneut in den Deutschen Bundestag (zur Behandlung in der 19. Legislaturperiode) einzubringen. Dabei sei bereits der Begriff, der im Gesetzgebungsverfahren nachvollziehbar bewusst plakativ gewählt wurde, dennoch verfehlt, worauf Golla (2017, S. 166) zurecht hinweist. Schon in der Literatur zu § 202 a StGB (vgl. nur Ernst, NJW 2007, S. 2661; Lenckner und Eisele, in Schönke und Schröder, StGB, 29. Auflage 2014, § 202 a, Rn. 18 m. w. N.) werde dieser nämlich als „elektronischer Hausfriedensbruch" bezeichnet. Der Tatbestand findet sich nun (und trotz Verneinung eines Regelungsbedarfs durch die Bundesregierung in der 18. Legislaturperiode) nun in modifizierter Form im RefE des BMI zu einem IT-Sicherheitsgesetz 2.0 vom 27. März 2019 wieder.

weltumspannenden Netzes und dem zunehmenden Einsatz von Anonymisierungssoftware schwierig. Schon deshalb sei der Ausbau bestehenden Strafrechts mangels erwartbarer Durchsetzbarkeit kritisch zu beurteilen. Wieder andere sehen durchaus *punktuellen* tatbestandlichen, strafmaßrechtlichen oder gesetzlich systematisierenden Anpassungsbedarf, bspw. bei der Abschnittsgliederung des Besonderen Teils des StGB oder auch hinsichtlich der „unbefugten Weitergabe von anvertrauten Daten", da z. B. der 2015 neu eingeführte § 202d StGB nur auf den „Hehler" abstelle. Ferner deshalb, weil sich etwa die besondere Verwerflichkeit von beleidigenden und/oder ehrverletzenden Äußerungen im Internet mit einem fast unbegrenzten Adressatenkreis im (vermeintlichen) Schutz der Anonymität des Netzes nicht ausreichend in der Strafandrohung der ansonsten tatbestandlich adäquaten §§ 185 ff. StGB[38] spiegele. Außerdem beziehen sich diskutierte Anpassungsbedarfe auch auf eine mutmaßliche Strafbarkeitslücke für Einrichtung und Betrieb von Darknet-Handelsplattformen (i. S. der unklaren „Betreibereigenschaft", welche bspw. in Anlehnung an § 2 Nr. 1 Telemediengesetz zu konkretisieren sei). Letztere „Lücke" berücksichtigt der RefE zu einem IT-Sicherheitsgesetz 2.0 (Stand 27. März 2019) mit einem eigenen Straftatbestand § 126a StGB, „Zugänglichmachen von Leistungen zur Begehung von Straftaten". Kritiker (vgl. z. B. nur Oehmichen und Weißenberger 2019; Selzer 2019; Schulze 2019 u. a.) bestreiten hingegen einen Regelungsbedarf bzw. erachten den Entwurf zu § 126a StGB als viel zu weitreichend und damit kriminal- und gesellschaftspolitisch als schädlich.

Nahezu allen Stimmen gemeinsam ist die von Golla (2017, S. 154) dargelegte und evidenzgeleitet nachvollziehbare Einschränkung, es müsse *„erst präzise und mit Blick auf spezifische Gefährdungslagen"* bestehendes „Internetstrafrecht" analysiert werden. Eigentlich eine kriminalpolitische Binsenweisheit, dennoch angesichts des diesbezüglichen gesetzgeberischen „Reformeifers" nicht zu vernachlässigen. Die entscheidende Frage sei dabei also die nach evidenten Schutzlücken. Erst danach stelle sich die Folgefrage, ob diese aus rechtsdogmatischen, rechtssoziologischen, kriminologischen sowie kriminalpolitischen Erwägungen angemessen bzw. zwingend erforderlich mittels des Strafrechts zu schließen

[38]Bleckat (2018) verweist in Anlehnung an Cornelius (2014) darauf, dass typische Erscheinungsformen bzw. Täter-Opfer-Konstellationen des Mobbings und vor allem des „Cybermobbings" zum jetzigen Zeitpunkt strafrechtlich kaum justiziabel seien. Er plädiert daher für einen neuen § 185 a StGB, mit dem die vielfältigen sowohl analogen wie auch insbesondere digitalen Tathandlungen dieses Phänomens zu erfassen wären und verweist beispielhaft auf eine derartige Vorschrift im aktuellen österreichischen Strafgesetzbuches (§ 107c StGB).

seien. Hierzu bedarf es nach Auffassung zahlreicher Experten und Praktiker (vgl. nur Fünfsinn und Krause 2019) allerdings einer grundlegenden Diskussion über das aktuelle Cyberstrafrecht, z. B. im Rahmen einer Reformkommission.

Gleichzeitig weist Golla (2017) noch auf die dem Computerstrafrecht im Besonderen inhärente Gefahr symbolischen Strafrechts[39] hin; es sei nämlich grundsätzlich

> „anzuerkennen, dass ein öffentlichkeitswirksamer Einsatz des Strafrechts durchaus sinnvoll sein kann. Der Staat könne so eine positive Generalprävention bezwecken und das Rechtsbewusstsein stärken, indem er sich durch das Strafrecht zu bestimmten Rechtsgütern bekenne. (Gerade) im Internetstrafrecht bestehe allerdings das Risiko einer übermäßigen symbolischen Ausweitung der Regelungsmaterie."

Schon an der Vielfalt der dargelegten Meinungen lässt sich auch hier der Bedarf einer umfassenden, evidenzbasierten und daher notwendigerweise interdisziplinär strukturierten Aufhellung gut erkennen. Verdeutlichen lässt sich diese Notwendigkeit sehr einprägsam mit einem Zitat von Hassemer (2008, S. 119):

> „Das Strafrecht jenseits einer Gesamten Strafrechtswissenschaft, das nur mit sich selbst in Kontakt stehende Strafrecht, womöglich noch verkürzt auf das materielle Strafrecht […], also ohne ein wissenschaftliches Sensorium für den Prozess und die Erscheinungsformen des Verbrechens, dieses Strafrecht ist ein schmales Wesen, eine anämische Monade."

Hinzu tritt die als grundsätzlich abstrakt belegt geltende allgemeine kriminologische Erkenntnis um die eher geringe allgemeine Steuerungskraft von Gesetzen im strafrechtlichen Kontext (Meier 2004, S. 420). Schon deshalb darf mangels hinreichend fundierter empirischer (kriminalstatistischer) Erfahrungen und Belege über die tatsächliche Wirkung wichtiger Teile des Computerstrafrechts davon ausgegangen werden, dass für die Kriminalpolitik – jedenfalls außerhalb des Kernstrafrechts hierbei – die Symbolik durchaus bedeutsam ist (Sazger 2007, S. 95 u. a.[40]).

---

[39] Vgl. zum Begriff und Wirkung ausführlich Kunz (2010).

[40] Noch differenzierter und daher deutlicher z. B. Albrecht (2004, S. 500), denn, *„die Kriminalpolitik (sei nicht per se deshalb) irrational oder nur symbolisch […], denn sie mag mit einer solchen Ausrichtung (jedenfalls) auf die Unsicherheitsgefühle eine durchaus effiziente Antwort geben. Was allerdings bleibe, sei das Problem der Legitimation."*

3.1.2 Gefahrenabwehrrecht

Das Computerstrafrecht ist bereits bis in die Vorbereitungsphase spezifischer Straftaten hinein ausgedehnt (vgl. hierzu bspw. nur die Tatbestände § 202c StGB oder § 202d StGB). Dadurch entsteht auch die latente Gefahr, dass materielles Strafrecht sich durch Vorverlagerung der Strafbarkeit dem Gefahrenabwehrrecht immer weiter annähert. An einigen Stellen sind bereits signifikante Schnittmengen erkennbar, die nur bedingt sachgerecht nach den Grundsätzen der „Doppelfunktionalität" aufgelöst werden können. Namhafte Kritiker bemängeln diese dogmatische Entwicklung einer in bestimmten Bereichen immer undeutlicher werdenden Grenzziehung zwischen den beiden Rechtssphären daher auch als „Abdriften in das Risiko- oder Präventionsstrafrecht".

Ein ähnlicher Vorwurf wird aktuell für das Gefahrenabwehrrecht, welches weitgehend in unmittelbarer Regelungshoheit der Bundesländer liegt, laut. In der Tat haben einige Bundesländer (z. B. Bayern) und der Bund (BKAG und BundespolizeiG) ihre Polizeigesetze bereits neuen, „digitalen" auftretenden Gefahrenerfordernissen angepasst. Einige Bundesländer stehen kurz davor, entsprechende Gesetzesvorhaben abzuschließen (Niedersachsen, Nordrhein-Westfalen, etc.).[41] Diese Rechtsmaterie, so die Kritiker, sei ohnehin aufgrund einer unserer Lebenswirklichkeit immanenten, rasant wachsenden Anzahl potenzieller Gefahrenlagen nur schwer dogmatisch zu strukturieren und daher schon aktuell notwendigerweise von vielen unbestimmten Rechtsbegriffen durchwirkt. Außerdem sei diese Regelungsmaterie deshalb auch einer unbestimmten Vielzahl von nicht durch typisierte Spezialermächtigungsklauseln geregelten Anwendungsfällen in bedenklicher Weise der „atypischen" Generalermächtigungsklausel zugänglich und werde immer weiter in das Vorfeld hinreichend konkreter Gefahrenlagen[42] bis hin zu verfassungswidrigen Risikoerforschungseingriffen ausgedehnt. Derart erweitert werde insbesondere das „Trennungsgebot" zwischen polizeilicher Gefahrenabwehr und nachrichtendienstlicher Informationserhebung in unzulässiger Weise permeabel. Befürworter und Kritiker weitergehender Regelungen diskutieren auf hohem Niveau, z. T. auch aus sicherer Höhe im wissenschaftlichen Elfenbeinturm. Was ist wirklich zur Prävention von Cybercrime gesetzlich erforderlich, was ist angemessen und geboten, um Vor- und Nachteile

[41] Siehe hierzu die Aufstellung von H. Busch, „Polizeigesetzgebung der Länder", entnommen aus dem Heft Nr. 116 (Juli 2018) des Instituts für Bürgerrechte & öffentliche Sicherheit e. V. (cilip.de).

[42] Vor allem der modifizierte Gefahrenbegriff der „drohenden Gefahr" (vgl. Fn. 38) wird hierbei als Argument verwendet.

prinzipiell grenzenloser IT-Infrastruktur in einem freiheitlich-demokratischen Lot bei hinreichender Sicherheit und bei angemessener Eigenverantwortung der Nutzer auszupendeln?

„Eine erfolgreiche Digitalisierungsstrategie setzt Datensicherheit voraus."[43] Digitalisierung bietet unendlich viele Chancen und Entwicklungsmöglichkeiten, sowohl kommerzieller Natur als auch im Non-Profit-Sektor. Die Bundesregierung hat deshalb im August 2018, wie im Koalitionsvertrag beschlossen, ein externes Beratergremium, den „Digitalrat"[44] ins Leben gerufen, um diesen Schatz aktiv, entschlossen und nachhaltig bergen zu helfen. Neben den Chancen der Digitalisierung besteht natürlich auch eine Vielzahl unspezifischer Gefahren, denen sich verantwortlich handelnde Politik bewusst sein sollte. Die Bundesregierung begegnet diesen Gefahren im Rahmen ihrer Cybersicherheitsstrategie u. a. mit einer ebenfalls im August 2018 ins Leben gerufenen „Agentur für Innovation in der Cybersicherheit"[45] und einem „Nationalen Cybersicherheitsrat"[46], der sich im Unterbau auf institutionelle und operative Strukturen in Bund und Ländern stützt. Bedrohungsszenarien unter Nutzung der IT-Infrastruktur sind allerdings

---

[43]Vergleiche Koalitionsvertrag zwischen CDU/CSU und SPD, „Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land", vom 12. März 2018, S. 125, Zeilen 5869.

[44]Vgl. URL: https://www.bundesregierung.de/Content/DE/Artikel/2018/08/2018-08-21-digitalrat.html. Zugegriffen: 1. Februar 2019.

[45]Vgl. https://www.bundesregierung.de/Content/DE/Artikel/2018/08/2018-08-29-cybersicherheit.html (zugegriffen: 29. August 2018): *„Der Staat müsse in der digitalen Welt seine Schutzfunktion wahrnehmen. Aufgabe der neuen ‚Agentur für Innovation in der Cybersicherheit' wird es sein, den Bedarf des Staates im Bereich der Inneren und Äußeren Cybersicherheit zu decken. Sie soll in gänzlich neu aufkommende Technologien investieren und Ideenträgerinnen und Ideenträger zeitlich befristet fördern. An erster Stelle steht, welche technologischen und digitalen Innovationen es überhaupt gibt und welches Potenzial in ihnen steckt. Die am besten geeigneten Innovationsträger sollen ermittelt werden, um sie mit Forschungsvorhaben beauftragen zu können."* Diese neue Agentur unter gemeinsamer „Trägerschaft" der Bundesministerin für Inneres und für Verteidigung war auch im Koalitionsvertrag vom 12. März 2018, S. 159, Z. 7544 ff., angekündigt.

[46]*„Ein Ziel der am 23. Februar 2011 erstmals verabschiedeten ‚Cyber-Sicherheitsstrategie' für Deutschland war die Einrichtung eines ‚Nationalen Cyber-Sicherheitsrates', der unter dem Vorsitz des Beauftragten der Bundesregierung für Informationstechnik (seit 2007 eingerichtet, derzeit wahrgenommen durch den Staatssekretär im BMI, Klaus Vitt) die Zusammenarbeit innerhalb der Bundesregierung sowie zwischen Staat und Wirtschaft organisiert. […] Der Sicherheitsrat ergänzt und verzahnt die Aufgaben mit der IT-Steuerung Bund und dem IT-Planungsrat im Bereich der Cyber-Sicherheit auf einer politisch-strategischen Ebene."*

vielfältig und erstrecken sich über Eigentums- und Vermögenskriminalität, über die Verbreitung gezielter Indiskretionen, Manipulation von demokratischen Entscheidungen bis hin zum Schüren von Hass und Aufruhr. Im Netz werden Straftaten über Ländergrenzen und Kontinente hinweg verabredet und geplant und „Anschläge“ durchgeführt (z. B. durch gezielte Angriffe auf systemrelevante Infrastrukturen) – die Verteidigungspolitik plant inzwischen sogar „Strike- bzw. Counter-Strike-Fähigkeiten“ (sogenannter „Hackback“) zu entwickeln, um im Anschlagsfall bzw. im potenziellen „Cyber-War“ reaktionsfähig zu sein.

Nun ist *„die Gefahrenabwehr die vornehmste Aufgabe der Polizei“*. So richtig der von Carl Severin, der in der Weimarer Republik preußischer und Reichsinnenminister war, geprägte Satz nach wie vor ist, er wäre überstrapaziert, würde die polizeiliche Gefahrenabwehr immer weiter nach vorne bis hin zu einer allenfalls „allgemeinen, abstrakten Risikovorsorge“ ausgeweitet werden. Das kann niemand wollen. Wie weit dies im Extrem führen könnte, zeigt sich am Beispiel undemokratischer Autokratien, in welchen eine implizit global angelegte und ausgerichtete IT-Infrastruktur zur Kontrolle „der Untertanen“ gleichsam als abgeschirmte „Insellösung“ zurückgebaut ist und jeder Einwahl- und Verteilknoten, einem lückenlos überwachten Hafen gleich, vollständig zu- und ausgangsgesichert bleibt. Platz für die individuelle Entfaltung von Freiheit und emotional konnotiertes Sicherheitsempfinden wären dort bis auf Null reduziert, was mit unserem durch Würde gekennzeichneten Menschenbild des Grundgesetzes völlig unvereinbar ist. Zugleich – und hiermit wird das Spannungsfeld über diese beiden äußeren Pole begrenzt – *„brauchen die Sicherheitsbehörden gleichwertige Befugnisse im Umgang mit dem Internet wie außerhalb des Internets […], ja die Sicherheitsbehörden (bedürfen) bei der Verfolgung und Prävention von Cyberkriminalität durch die Schaffung notwendiger rechtlicher, organisatorischer sowie technischer Rahmenbedingungen der Stärkung.*“[47] Diese allgemeine, programmatische Aussage bleibt ohne potenzielle Anwendungsfälle, die bei den Sicherheitsbehörden zur kriminalpolitischen Beratung in rechtstatsächlichen Sammlungen beim BKA regelmäßig zusammengetragen werden, konturenlos.

Greifen wir nur eines der zahlreichen dort diskutierten Beispiele heraus, die „Pädophilie“ (im Übrigen *kein* klassisches Delikt der „Cybercrime im engeren Sinne“, sondern zumeist kategorisiert mit dem Zusatz „Tatmittel Internet“!), die über weltweit organisierte, gut abgeschirmte und getarnte Netzwerkstrukturen

[47]Vergleiche Koalitionsvertrag zwischen CDU/CSU und SPD, „Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land“, vom 12. März 2018, S. 128, Zeilen 5997 f.

inzwischen einzigartige Verbreitungsmöglichkeiten und „markttypische Vertriebswege" gefunden hat. Bei diesem Phänomen verschmelzen kriminalstrategisch und – jenseits rechtsdogmatischer Diskussionen – in praxi Strafverfolgung und Gefahrenabwehr weitgehend miteinander. Erweiterte Möglichkeiten, ohne im Einzelfall hinreichenden Verdacht einer konkreten Straftat, gefahrenabwehrrechtlich in die strukturelle Erkenntnisgewinnung und damit auch bereits bei „drohender Gefahr" einzusteigen, wären angesichts des gerade bei diesem Phänomen mit unendlichem Leid der missbrauchten Opfer angefüllten Dunkelfeldes natürlich sachgerecht. Derart gewonnene Daten, einerseits streng nach den Regeln der „hypothetischen Datenneuerhebung" ins Strafverfahren einzubringen, anderseits damit aber auch Verbreitungskanäle schnell und nachhaltig generalpräventiv auszutrocknen und damit aktiv und nachhaltig das „Kindeswohl" über Ländergrenzen hinweg zu schützen, das wäre ein rechtsstaatlich gebotenes und lohnendes Ziel, welches man gemeinsam und über dogmatische Grenzen hinweg diskursiv entfalten müsste.

Aber, auch hier gilt das kybernetische Regelkreismodell der Problemlösung: Audits – Strategieentwicklung – Operationalisierung – Evaluation! Am Anfang steht demnach immer die möglichst umfassende Analyse der Ausgangssituation. Nur so sind evidenzbasierte, rationale (kriminal-)politische Entscheidungen möglich. Am Ende steht neben der Rechtsdogmatik die nüchterne Betrachtung der Praktikabilität in Abgrenzung zum Nutzen und Ertrag. In jüngerer Vergangenheit werden bspw. in diesem Zusammenhang in der Literatur, zwar noch nur vereinzelt, bspw. Forderungen zur Einführung eines „Evaluationsrates" (z. B. Schaar 2018, S. 222)[48] in Anlehnung an das bereits bestehende Gremium des „Normenkontrollrats" erhoben, um derart dauerhaft eine möglichst rationale, evidenzbasierte (Kriminal-)Politik zu gewährleisten. Angesichts der Bedeutung des Themas Sicherheit und Freiheit bleibe für „Symbolpolitik" (vgl. Fn. 42) an dieser Stelle kaum wirklich Raum.

3.1.3 Gefahr für das Gewaltmonopol?

> „Staat soll ein politischer Anstaltsbetrieb heißen, wenn und insoweit sein Verwaltungsstab erfolgreich das Monopol legitimen physischen Zwangs für die Durchführung der Ordnung in Anspruch nimmt." (Weber 1976, Kap. I, § 17, S. 39)

[48] Vgl. auch Abschn. 4.3, dort Erweiterung dieser Forderung über den Begriff der „Gesetzgebungslehre" m. w. N.

Zum Abschluss dieses Kapitels noch eine in Frageform konnotierte „Endnote“. Wir diskutieren in diesen Tagen des Spätsommers 2018 öffentlich am Beispiel von unerträglichen tätlichen und verbalen Übergriffen auf „Ausländer“, die über soziale Netzwerke und dort verbreitete Falschmeldungen in bestimmter Absicht und motiviert von einer destabilisierenden Wirkung für den Rechtsstaat mittelbar veranlasst/ausgelöst werden, intensiv über die notwendige Durchsetzung des staatlichen Gewaltmonopols, um staatsfeindlich geübte Selbstjustiz zu unterbinden. Wenn auch nur der geringste öffentliche Eindruck entsteht, der Staat als Gewaltmonopolist sei nicht mehr in der Lage, für die Sicherheit der Menschen zu sorgen, ist die Gefahr des Vertrauensverlustes gegenüber dem Staat mit Ausstrahlungswirkung auf alle staatlich regulierten, gesellschaftlich und sozialen Stabilitätsfaktoren groß. Der Mitherausgeber dieses Bandes, Thomas-Gabriel Rüdiger versucht dies seit einiger Zeit unter der Bezeichnung „Broken-Web“[49] (2018) und die derart erzeugte anomische Wirkung, ausgelöst durch einen Mangel an wahrnehmbarer Polizeipräsenz im Netz, zu thematisieren und diese Wechselwirkung im virtuellen Raum auch empirisch zu belegen.

Man darf, ja man muss sich vielmehr gerade mit Blick auf die der „virtuellen Welt“ immanenten Gefahren die Frage stellen, ob diese tendenziell abstrakte Vulnerabilität der Nutzer und des Netzes im Allgemeinen und im Gegensatz zur (noch nur) vereinzelt in der Literatur (z. B. Huber 2015; Themenseite „Cybercrime“ des BKA) aufgeworfenen Frage, ob Teile der Bevölkerung den Sicherheitsbehörden die nötige (digitale) Problemlösungsfähigkeit aktuell überhaupt zutrauen, im gesellschaftlich-sozialen Klima derartige, von Rüdiger unter Bezugnahme auf Emile Durkheim (1990) und Robert K. Merton (1949) apostrophierte anomische Reize mit schädlichen Wechselwirkungen zwischen der „analogen Welt“ und dem „virtuellen Raum“ hervorrufen könnten?

Allerdings muss man bei diesen Überlegungen wohl auch das auf den ersten Blick nur bedingt erklärbare, ambivalente Handeln von Internet-Nutzern berücksichtigen. Trotz der vielfältig öffentlich verfügbaren und erschreckenden Ergebnisse zahlreicher Viktimisierungssurveys, die das Internet eigentlich zur – im Unterschied zu in der „analogen Welt“ jedenfalls politisch vehement negierten – „No-go-area“ machen würde, steigt seit Jahren statistisch sowohl die Zahl der Nutzer als auch insgesamt die durchschnittliche tägliche Nettozeit, die User im Netz zubringen,

[49]In Anspielung auf die von Wilson und Kelling in den 1980er Jahren entwickelte „Broken-Windows-Theorie“ (vgl.: The Atlantic, March 1982 Issue, passim), deren Funktionalität in jüngerer Vergangenheit in der Wissenschaft vereinzelt allerdings deutlich kritischer betrachtet wird (vgl. z. B. Wolbring und Keuschnigg 2015).

kontinuierlich an. Theoretisch schlüssiger wäre angesichts der immensen latenten Risiken eher ein signifikanter Anstieg des Vermeidungs- und Sicherungsverhaltens (konative Komponente des Sicherheitsempfindens), jedenfalls im privaten Sektor, in dem es im Unterschied zur Wirtschaftswelt derzeit durchaus noch Ausweichmöglichkeiten gäbe (s. a. Kap. „Cyber-Viktimisierung von Unternehmen" und „Kriminalität und Unsicherheit im virtuellen Raum"). Das wirft natürlich auch Fragen zu den gesamtgesellschaftlichen Präventionsstrategien, insbesondere zum Wirkungsgrad der Bemühungen um eine hinreichende Medienkompetenz, möglichst bereits eingebaut in den Schulalltag, fortgesetzt bis hin zur Seniorenarbeit auf. Ohne eine empirisch im Übrigen nicht belegte Absicht lässt sich beim Betrachter dennoch der Eindruck eines ausgeprägten „Defätismus" der Nutzer nicht vermeiden. Liegt es etwa an der den eigenen Alltag durchdringenden ubiquitären Sättigung mit Gefahrenhinweisen und Handlungsaufforderungen, z. B. die aktuelle Virenabwehrsoftware auf allen Geräten im eigenen Haushalt ebenso wie das Betriebssystem ständig aktuell zu halten oder das eigene Password-Management zu überdenken, etc., dass eine Vielzahl von Menschen angesichts der evident unvermeidbaren Gefahren offenbar der Überzeugung sind, man könne sich im Internet ohnehin nicht hinreichend schützen? Es hat sich bei den privaten Nutzern offenbar überwiegend eine Haltung etabliert, die immer wieder mit dem Akronym „Nimby" („Not in my backyard") dem sogenannten Sankt-Florian-Prinzip folgt. Getreu der Schutzbitte an den katholischen Schutzpatron gegen Feuer und Dürre – *„Heiliger Sankt Florian / Verschon' mein Haus / Zünd' and' re an"* – hoffen Nutzer offensichtlich, „Sie werde es schon nicht treffen!" Diese unverständliche und geradezu gefährliche Haltung könnte man „ironisch" mit einem anderen eingängigen Akronym, nämlich „Picnic", kontern, welches für „Problem in chair, not in computer" steht.

4 Herausforderungen für die Wissenschaft

> „Bei der Kriminologie handelt es sich um eine besondere Disziplin, weil sie in ihren Inhalten und Methoden in einer an der Juristischen Fakultät einmaligen Weise die Rechtswissenschaft mit sozialwissenschaftlichen Disziplinen verbindet. Ihr Reiz liegt (daher) in der Interdisziplinarität und auch im Spannungsverhältnis zwischen Theorie und Praxis."[50] (Neubacher 2006, S. 435)

[50]Neubacher spielt hier auf die inzwischen weit überwiegende Verankerung der Kriminologie an Juristischen Fakultäten im deutschen Sprachraum an, sieht aber zum anderen für die Strafrechtswissenschaft die Chance, sich *„jenseits strafrechtlicher Dogmatik mit einer Fülle fesselnder (empirischer) Fragestellungen zu beschäftigen, die eigentlich erst so recht den Grund abgeben, für eine fundierte wissenschaftliche Beschäftigung mit dem Strafrecht."*

Vor allem in der Kriminologie als sozialwissenschaftlicher empirischer „Fruchtstand“ einer „Gesamten Strafrechtswissenschaft“ i. S. des einleitenden Diktums von Neubacher vereinen sich m. E. Verpflichtung und Chance, die anstehenden Herausforderungen anzunehmen. Sie verfügt über das notwendige empirische Know-how, die vorhandenen phänomenologischen Lücken (eigentlich müsste man angesichts des Ausmaßes eher von „Schluchten“ reden) zu verkleinern. Sie verfügt auch über einen – jedenfalls für die „analoge Welt“ – hinreichend gesicherten ätiologischen Erkenntnisstand. Dadurch ergibt sich auch die Chance, letzteren durch Modifikation oder ggf. auch Neuformulierung von Kriminalitätserklärungsmodellen am Beispiel der „virtuellen Welt“ fortzuentwickeln. Aus eigener Kraft und ohne individuelle wissenschaftliche Präferenzen, die sich allerdings „cyberkriminologisch“ nur recht zaghaft entwickeln[51], wird dies ohne Fremdanreize, bspw. durch gezielte staatliche Aufträge im Rahmen angewandter kriminologischer Forschung, nur bedingt gelingen. Die Herausforderungen angesichts der wie bisher dargelegt beachtlichen Wissensdefizite bleiben also groß. Die Chancen einer Fremdmittelförderung für kriminologische Institute und Informatik-Lehrstühle, ggf. sogar im interdisziplinären Verbund, werden mit der Einrichtung einer neuen, durch das BMI und das BMV gemeinsam finanzierten „Agentur für Innovation in der Cybersicherheit“, die im Jahr 2019 ihren Betrieb aufnehmen wird, mutmaßlich steigen. Eine Aufgabe der mit einem Haushaltsvolumen von 200 Mio. EUR für die Jahre 2019–2024 ausgestatteten Bundesagentur besteht nämlich darin, innovative Forschungsvorhaben zu unterstützen. Voraussichtlich wird es sich bei den künftig geförderten Vorhaben im Rahmen der Zielsetzung der Bundesregierung, die für Deutschland bei der Cybersicherheit im europäischen Kontext offenbar einen beträchtlichen Nachholbedarf annimmt, wohl eher um „angewandte“ und weniger um „epistemologische Grundlagenforschung“ handeln.

Die kriminologisch-kriminalistischen Betrachtungsebenen im Cyber-Raum entsprechen kategorial grundsätzlich wohl denen der „analogen Welt“. Neben

[51]Der Mitherausgeber Rüdiger, Kriminologe und Fachhochschullehrer in Brandenburg, firmiert und agiert bereits intensiv unter dem „Label“ Cyberkriminologie. An der Hochschule für Öffentliche Verwaltung in Bremen, Fachbereich Polizei, wurde zum 1. Oktober 2018 eine Vollzeitstelle für Kriminologie mit dem Schwerpunkt Cyber-Kriminologie/IT-Forensik besetzt. Ferner, im deutschsprachigen Raum, z. B. das im Oktober 2018 startende einsemestrige „Certified Program Cybercrime“ an der Donau-Universität Krems in Österreich, die empirischen Ansätze Meiers (2015b) am Beispiel Täter illegaler Downloads oder das strafrechtlich-forensisch ausgerichtete Modul 8 im MA-Studiengang „Kriminologie, Kriminalistik und Polizeiwissenschaft“ an der Ruhr-Universität Bochum etc.

dem einführend dargelegten Aspekt der *Phänomenologie* (v. a. auf den Ebenen *Person* [Täter/Opfer in seinen viktimologischen Bezügen], die spezifisch „virtuelle" *Situation* des Geschehens und Besonderheiten der formellen wie auch informellen *Sozialkontrolle* bei diesem Phänomen mit seiner typischen Distanz, einer i. d. R. allenfalls mittelbaren „virtuellen" Begegnung zwischen Täter und Opfer oder gar die vom Opfer lange Zeit völlig unbemerkte, klandestine Vorgehensweise abseits jeglicher gesellschaftlicher Bezüge im „virtuellen Raum"), sind es insbesondere die *Kriminalätiologie,* also die Suche nach spezifischen Ursachen/Erklärungsmodellen von Computerkriminalität (weniger im kriminalbiologischen als vielmehr im -soziologisch-psychologischen Kontext) sowie die Besonderheiten gesamtgesellschaftlich initiierter und gepflegter (Kriminal-)*Prävention* hierbei, die im Besonderen betrachtenswert bleiben.

4.1 Kriminalphänomenologische Validierung

Hier liegt, wie dargelegt, die zunächst wichtigste Aufgabe, denn ohne ein wirklich valides Fundament an Befunden ist wohl kaum eine spezifische Problemanalyse und schon gar keine sachgerechte kriminalpolitische und, darauf aufbauend, operative und institutionell-operative Planung der Kontrolle des Phänomens möglich. Die Lücken im Erkenntnisbestand sind wie dargestellt jedoch signifikant.[52] Dieser Umstand fordert m. E. geradezu die Fortführung der Diskussion um die Wiederaufnahme einer die PKS ergänzenden, mit kriminologischer Expertise angereicherten periodischen Sicherheitsberichterstattung[53], nicht nur, aber vor allem auch die Computerkriminalität betreffend mit ebenso regelmäßigen integralen Viktimisierungssurveys, auch zu diesem Phänomen.

Weitgehend unkonturiert und noch überwiegend frei von fundierter empirisch strafrechtswissenschaftlicher Untersuchung scheint mit darüber hinaus noch der Bereich der Beleidigung/Belästigung und bewussten Diskreditierung im virtuellen Raum zu sein, „neudeutsch" mit vielen phänomenologischen Anglizismen belegt. Dies ist u. a. verbunden mit der Frage, ob das aktuelle Strafrecht

[52]Die über die einzelnen Delikte hinweg unterschiedlichen Aufklärungsquoten sind erstens weitgehend unterdurchschnittlich und ferner angesichts ihrer Bedeutung in Relation zum jeweiligen Dunkelfeld hinsichtlich ihrer Aussagekraft kaum geeignet, Täter-Opfer-Hypothesen zu erarbeiten und zu validieren.

[53]Wie wir sie mit den beiden ersten Berichten 2001 und 2006 erlebt haben.

derartige Handlungen derzeit parallel zur Meinungsäußerungs- und Kunstfreiheit ausreichend tatbestandlich abdeckt? Im Übrigen auch eine wesentliche Ausgangsfrage im Zentrum des Gegenstandes einer „Gesamten Strafrechtswissenschaft“.

4.2 Kriminalätiologische Ansätze im analogen und im virtuellen Raum

Computer-Kriminalität ist nach all dem, was phänomenologisch bekannt ist, inzwischen zur „Online-Alltagskriminalität“ geworden. An diesen Befund schließt sich natürlich automatisch die Frage nach ausreichend plausiblen (kriminologischen) Kriminalitätserklärungsansätzen an. In der Literatur und auf Internet-Fachportalen[54] werden einige bekannte Modelle[55] immer wieder mit diesem Phänomen verknüpft, v. a. sind dies der/die

- „Routine-Activity-Approach“ nach Cohen/Felson und Clarke
- „General Theory“ nach Gottfredson/Hirschi
- „Neutralisierung“ des Unrechts in Anlehnung an Sykes/Matza[56]
- Begriff der „Internetdissozialität“, modifiziert nach Meier (2015a, S. 103) und neuerdings
- die „Situational-Action-Theory“ (SAT) nach Wikström sowie
- die von Rüdiger umrissene „Broken-Web-These“ mit ihren integralen anomischen Wirkungen

Meier (2012, S. 197) postuliert auf der Basis der noch spärlichen und kaum evaluierten Befunde und weniger tiefer gehender Erkenntnisse hierzu:

---

[54]Vgl. z. B. das von Prof. Dr. Christian Wickert von der FHöV NRW erstellte und gepflegte, sehr übersichtliche Portal „SozTheo“ (vormals „KrimTheo“), https://soztheo.de. Zugegriffen: 30. August 2018.

[55]Die ausschnittsweise Aufzählung (Adaptationsüberlegungen werden derzeit durchaus auch auf der Grundlage der „Subkulturtheorie“ nach Stellin, der „Anomietheorie“ nach Durkheim und Merton oder verschiedener „kontroll- und bindungstheoretischer Ansätze“ bzw. der „Rational-Choice-Theorie“ nach Becker, Cornish und Clarke – insbesondere bezogen auf Tatgelegenheit und Entdeckungsrisiko, angestellt) erhebt an dieser Stelle keinesfalls den Anspruch der Vollständigkeit. Im Übrigen wird auch auf eine Beschreibung der Theorien unter Bezugnahme auf die Besonderheiten der „virtuellen Welt“ aus Gründen der Übersichtlichkeit dieses Beitrags verzichtet.

[56]Die „Neutralisierungsthese“ ist streng betrachtet keine Kriminalitätserklärungstheorie, sie beschreibt vielmehr das „rationalisierende“ Verhalten der Täter nach der begangenen Tat.

> Es gibt „keinen Anlass […] davon auszugehen, dass die Internetkriminalität […] anderen Regelmäßigkeiten folgt als sie aus der allgemeinen Kriminologie bekannt sind. Dazu gehören namentlich das häufigere Auftreten leichter als schwerer Delikte, die höhere Belastung junger Menschen, namentlich von Jugendlichen (‚digital natives'), die höhere Belastung von Männern gegenüber Frauen sowie ein vergleichsweise geringer Anteil von Mehrfach- und Intensivtätern gegenüber einer Dominanz von Einmal- und Gelegenheitstätern. Flächendeckende Untersuchungen liegen zu diesen Fragen allerdings (noch) nicht vor."

Diese eher noch allgemein gehaltene Feststellung kann m. E. nicht vollständig überzeugen, sie greift angesichts der Unbekannten zu kurz. Unter Verweis auf die auf Jaishankar[57] (2008) zurückzuführende „Space Transition Theorie" (STT), auch wenn diese sicher noch nicht „prominent" in die „cyberkriminologische" Forschungslandschaft eingeführt ist, stellt bspw. Bässmann (2015, S. 67 f.) fest, sie sei eine der wenigen, allerdings noch nicht ausreichend kritisch diskutierten und empirisch überprüften Studien zur Kriminalitätserklärung die davon ausgehe, *„dass sich Menschen in der Cyberwelt anders als in der realen Welt verhalten."* Die Theorie, die somit auch entfernt auf die „Zwei-Welten-Problematik" (vgl. Fn. 34) reflektiert, versucht mittels folgender (ausschnittsweiser) Thesen diese Unterschiede bzw. das Verhalten von Menschen „zwischen diesen beiden Welten" zu erklären:

- Menschen, die delinquentes Verhalten in der realen Welt aufgrund von Status und Position unterdrücken, sind geneigt, derartiges Verhalten in der Cyberwelt zu zeigen.
- Flexible Identitäten, eine dissoziative Anonymität und unzureichende Abschreckungsfaktoren in der Cyberwelt eröffnen Chancen der Tatbegehung.
- Wechselnde Unternehmungen von Tätern in den Cyberraum und die dynamisch räumlich-zeitliche Natur des Cyberraumes bieten Chancen der Flucht.
- Der Konflikt von Normen und Werten der realen Welt mit den Normen und Werten der Cyberwelt kann zu Cyberkriminalität führen.

Die weitergehend differenzierungsbedürftige Studie geht ferner davon aus, dass kriminelles Verhalten von Tätern im Cyberraum in die reale Welt importiert werde und umgekehrt.

---

[57]Indischer Kriminologe und Herausgeber des im Übrigen z. Zt. nach meiner Beobachtung einzigen fachkriminologischen Journals („International Journal of Cyber Criminology"), welches schon denominativ explizit auf eine eigene kriminologische Subkategorie hinweist.

Kriminalätiologisch betrachtet zeigt sich, dass die Diskussion zur „Cyber-Kriminalität“ am Beispiel der wenigen angerissenen Themenbereiche nach wie vor erst am Anfang steht. Allerdings zeichnen sich bei kritischer Betrachtung der bisherigen Befunde durchaus Besonderheiten ab, die näherer interdisziplinärer Untersuchung bedürfen. Haben bspw. die sich in der virtuellen Welt entwickelten Spezifika der Sprache, der Verbreitungsgeschwindigkeit von Informationen sowie die weitgehende, im Übrigen den AGB der Social Media Unternehmen widersprechende Pseudonymisierung/Anonymisierung zahlloser Accounts über die Distanz zwischen den handelnden/betroffenen Subjekten hinaus kriminovalente Auswirkungen auf die Gesellschaft im Allgemeinen, etc.?[58]

4.3 Interdisziplinäre Ableitungen?

Ob die bisher genannten Besonderheiten allerdings eine dauerhaft tragfähige Grundlage für eine eigenständige Subkategorie der Disziplin bieten und welchen besonderen Gegenstand sich diese Subkategorie dann geben müsste, der sich von der formgebenden Leitdisziplin deutlich unterscheidet, das sind m. E. noch weitgehend offene Fragen. Angesichts des Wissensdefizites, welches m. E. größtenteils zunächst innerhalb der bereits bestehenden interdisziplinären Strukturen aufgehellt werden könnte, lassen diese sich derzeit noch nicht abschließend beantworten. Der disziplinäre Forschungsunterbau der unter Druck stehenden universitären Kriminologie oder auch ihrer wenigen außeruniversitären Institute ist jedoch fragil und schon im Moment nicht annähernd tragfähig genug, das Wegbrechen eines oder mehrerer substanzieller Stützpfeiler zu verkraften. Deswegen wird die zarte „subkulturelle Substanz“ einiger weniger „Inseln der Cyberkriminologie“ im deutschsprachigen Raum für den Augenblick wohl auch informell kaum exponentiell wachsen können. Dies schon deshalb, da die epistemologische Diskussion zur notwendig diese Subdisziplin begleitenden, in Umfang und Tiefe noch zu definierenden „Grundlagenforschung“ neben wenigen Projekten „angewandter Forschung“ noch nicht einmal begonnen hat. Als Beispiel hierfür mag nur die Problematik einer immer ausgefeilteren, algorithmenbasierten „Big-Data-Analytik“, für die grundsätzlich keine „personenbezogenen

[58]Hier fänden sich neben den soziologischen v. a. sprach-, literatur-, kultur- und medienwissenschaftliche Bezüge als interdisziplinäre Korrelate der Kriminologie und somit auch der „Gesamten Strafrechtswissenschaft“, die v. Liszt bei der Entwicklung des Modells noch gar nicht erkennen konnte.

Daten"[59] im Wortsinn mehr notwendig sind, sondern bereits die Verknüpfung der im Cyber-Raum massenhaft vorhandenen grundsätzlich depersonalisierten Metadaten genügt. Ferner ist der fortschreitende Ausbau und die Wirkung von Künstlicher Intelligenz auf gesellschaftliche Soziotope im Moment noch nicht einmal allgemein verbindlichen ethischen Standards zugänglich, obwohl am Ausbau bis hin zu Kriegsgerät bereits eifrig mit hohem Kapitalaufwand geforscht wird. Können oder müssten diese Versatzstücke dann nicht auch bei der Frage des Gegenstandsbereichs cyberkriminologischer Bestrebungen diskutiert werden? Welcher eigenständigen, besonderen Interdisziplinarität unterlägen derartige Unternehmungen dann und sind diese bereits institutionell-operativ vorhanden? Viele Fragen und derzeit noch zu wenige bzw. allenfalls fragmentarische Antworten darauf!

Doch zurück zur Eingangsfrage: Ehrlicherweise ist diese vielleicht etwas zu fatalistische Feststellung zur Cyberkriminologie auch auf das ebenfalls allenfalls zarte Pflänzchen „Gesamte Strafrechtswissenschaft" mit ihrem jedoch durchaus vorhandenen interdisziplinären Potenzial und Gegenstand, formelle Sozialkontrolle auch im Cyber-Raum rational zu gestalten, grundsätzlich übertragbar. Die Diskussion um diese Disziplin ist aber seit geraumer Zeit entfacht, köchelt allerdings im Moment höchstens auf kleiner Flamme ohne bisher wirklich nennenswerte institutionelle oder operative Folgen gezeitigt zu haben. Man kann es dennoch durchaus als Konsens zwischen allen Fronten dieses nach wie vor aktuellen Diskurses betrachten, dass grundsätzlich eine negativ konnotierte[60], punktuelle strafrechtliche Symbolik evidenzbasierter Notwendigkeit[61] weichen muss.

Um dem Ideal einer möglichst (durchgängig) am Gemeinwohl orientierten, rationalen Gesetzgebung nahe zu kommen, empfiehlt bspw. Rolinski (2009, S. 174) doch z. B. auf die Ergebnisse der (Noll'schen) „Gesetzgebungslehre" zurückzugreifen. Diese versuche *„durch Vorgabe bestimmter Verfahrensregeln auch im komplexen Bereich widerstreitender Partikularinteressen und ideologischer Positionen einen möglichst hohen Grad an Gerechtigkeit zu erreichen"*,

[59]Mit dem europäischen Datenschutzpaket, v. a. der Datenschutzgrundverordnung hat diese Kategorie eine signifikante Ausweitung erfahren.

[60]Kunz, vgl. Fn. 42, beschreibt in seinem sehr lesenswerten Aufsatz durchaus auch das notwendig symbolische Wesen des Strafrechts und die Notwendigkeit dieses Momentums im Rahmen einer funktionalen Sozialkontrolle.

[61]Nicht nur, weil dies denominativ im aktuellen Koalitionsvertrag der 19. Legislaturperiode zwischen CDU/CSU und SPD, S. 133, Z. 6289 ff. explizit ausgewiesen ist.

enthalte demnach also wesentliche Ingredienzen (kriminal-) politikwissenschaftlicher Interessen und Gegenstände. Eine „Gesetzgebungslehre“ sei schon deshalb nützlich, weil sie gegenständlich nach der „Herbeiführung optimaler sozialer Zustände frage“, die Wertfrage also nicht ausklammere. Sie verfügt sicher auch über große Schnittmengen zu einer sich „wissenschaftlich“ verstehenden Kriminalpolitik und ergänzt die Ziele sozialwissenschaftlich begründeter, „praktischer Kriminalpolitik“, was Rolinski sehr anschaulich anhand eines Musters einer „Prüfschablone rationaler Gesetzgebung“[62] verdeutlicht. Eine solche „wissenschaftliche Lehre von der guten Gesetzgebung“, wie sie schon Noll (1973) dezidiert beschrieben und deren Anwendung empfohlen hat, eine solche *„allgemein anerkannte und […] damit verbindliche (wissenschaftliche) Gesetzgebungslehre“* (Schulze-Fielitz 1988, S. 26 ff., 562 ff.) gibt es eigenständig denominativ und gegenständlich-inhaltlich aber ebenso wenig wie eine „wissenschaftliche Kriminalpolitik“ (immer) noch nicht. Hierfür bietet die derzeitige interdisziplinäre Forschungslandschaft, mit wenigen Ausnahmen im Schwerpunkt verortet an den Rechtswissenschaftlichen Fakultäten, dort vereinzelt unterstützt durch kriminologischen, psychologischen und sozialwissenschaftlichen Sachverstand, aber bereits heute prinzipiell sicher ausreichend Substanz. Dennoch, ein Ausbau der kriminologisch-kriminalistischen Komponente, z. B. in Anlehnung – um den begrenzten Ausschnitt der deutschsprachigen Kriminologie zu verlassen – an die anglo-amerikanischen universitären „Criminal-Justice-Modelle“ (vgl. z. B. Jehle 2007, S. 201; Karstedt 2013, S. 127; Lösel 2013, S. 131, die beiden letztgenannten Autoren v. a. am Bsp. Großbritanniens), wäre hierbei mitunter wünschenswert.

5 Epilog

> „Im Hinblick auf das […] Kommunikationsverhalten junger Menschen und die sich bietenden Gelegenheitsstrukturen (wird man) fragen müssen, ob das kriminologische Wissen der ‚analogen Welt‘ auf die ‚digitale‘ ohne Weiteres übertragbar erscheint oder ob es einer Art ‚Cyberkriminologie‘ bedarf, um den uns bekannten Fundus kriminologischen Wissens zu erweitern oder zu ergänzen?“ (Mischkowitz 2013, S. 218)

„Cyberkriminalität“ ist eine eminente Bedrohung der Sicherheit unseres freiheitlich-demokratischen Gesellschaftsentwurfs und *„provoziert daher Antworten*

[62]Plank (2017) verwendet diese Schablone z. B. in etwas modifizierter Form am Beispiel der Genese und Fortentwicklung des Straftatbestandes des § 238 StGB von 2007–2017.

auf die Frage, ob und wieweit die überkommenen (öffentlich-, zivil- und straf-)-rechtlichen Regeln dazu taugen, der veränderten (digitalen) Problemlage gerecht zu werden und die in der Rechts- und Gesellschaftsordnung bisher verankerten oder gar wichtige neue Zielwerte unter den veränderten Bedingungen optimal zu verwirklichen" (Hoffmann-Riem 2018, S. 13). Daher bedarf primär das öffentliche Recht und die (Straf-)Rechtswissenschaft eines empirisch validierten Erkenntnisgewinns, um die gebotene Risiko- und Gefahrenminimierung zu kanonisieren. Ob man der Kriminologie angesichts des dort disziplinär vorhandenen Wissens und der aufgezeigten „Erkenntnislücken" in diesem notwendigen Prozess kategorisch eine neue Subkategorie mit dem Präfix „Cyber-" verordnen möchte, kann im Sinne der Eingangsfrage und der bisherigen Bemerkungen m. E. deshalb jedenfalls für den Moment durchaus noch offen bleiben. In Bezug auf das Phänomen Cybercrime wäre es derzeit jedenfalls sachgerechter, die vorhandenen beträchtlichen Erkenntnislücken – herkömmlich institutionell und wissenschaftlich konservativ-operativ – möglichst zügig zu schließen.

Auf dieser Informationsgrundlage, evidenzbasiert und disziplinübergreifend im Rahmen einer interdisziplinären, im ursprünglichen Liszt'schen Verständnis einer „Gesamten Strafrechtswissenschaft" erzeugt, sollte man zunächst sowohl Straf- als auch Gefahrenabwehrrecht „de lege lata" kritisch auf Wirksamkeit und ggf. evident negativ konnotierte Symbolik[63] analysieren und erst dann evtl. vorhandene Lücken „de lege ferenda" zu schließen versuchen. Hier hat sich die Haltung der empirisch aufgeschlossenen (Straf-)Rechtswissenschaft in den letzten Jahrzehnten, eingerahmt von Jeschecks[64] (damals) progressivem Diktum,

> „die Frage, wie das Strafrecht eingerichtet werden soll, um dem Rechtsfrieden und der öffentlichen Sicherheit am besten dienen zu können, ist zunächst einmal eine Frage der Zweckmäßigkeit, und mit welchen Mitteln die Zwecke des Strafrechts am besten erreicht werden können, sagt uns die Kriminologie" (Jescheck 1980, S. 41[65]),

[63]Fabricius (2006, S. 269, 282 f.), findet hierfür eine schöne Metapher, indem er festhält, eine eher *„generalpräventiv orientierte Rechtspolitik verspräche Erfolg auch dort, wo das Auge des Gesetzes und der Arm der Strafjustiz nur geringe Chancen haben, sich Zutritt zu verschaffen."*

[64]Man darf Jescheck mit gutem Grund als einen der wichtigsten Vertreter des Modells „Strafrecht und Kriminologie unter einem Dach", durch ihn am Max-Planck-Institut für ausländisches und internationales Strafrecht verfeinert, bezeichnen.

[65]Sogar noch viel früher, nämlich im Jahr 1967, formulierte der ausgewiesene Strafrechtler, er sei davon überzeugt, *„dass es die Kriminologie sei, die die Brücke von der Normwissenschaft zur Lebenswirklichkeit schlage und deswegen zur Erklärung und Bewertung juristischer Lösungen ständig gebraucht werde."*

m. E. auch nur wenig verändert, ist also im deutschen Sprachraum trotz ausgeprägter strafrechtlicher Dogmatik gerade in Deutschland durchaus substanziell vorhanden.

Mit der „Gesamten Strafrechtswissenschaft“ ist auf diesem Weg ein durchaus geeigneter Kompass vorhanden. Auch wenn beide Disziplinen, die Strafrechtswissenschaft und die Kriminologie, noch enger zusammenwachsen und bei aller wesenseigenen Unterschiedlichkeit ihren gemeinsamen Gegenstand noch präziser definieren müssen, eint sie die gemeinsame (empirische) Erkenntnis limitierter Steuerungskraft strafrechtlicher Normen. Hillenkamp (2009, S. 320 f.) mahnt daher, die „Gesamte Strafrechtswissenschaft“ müsse ihren Einfluss auf die Kriminalpolitik erweitern, indem sie *„Verläufe mehr als bisher (aktiv) zur Kenntnis nimmt, relevante Vorgänge mit methodischer wie inhaltlicher Reflektion begleitet und die Erfüllung der gesetzgeberischen Pflichten einfordert.“* Hillenkamp sieht deshalb sogar den Gesetzgeber in der Pflicht, *„die ‚gesamte Strafrechtswissenschaft‘ fördernd und fordernd zu begleiten.“* Er begründet dies anhand einer Beobachtungs- und Nachbesserungspflicht (Evaluation!) im Strafrecht, die den Gesetzgeber unmittelbar treffe. Angesichts des *„jeweils zu erwartenden bzw. nicht auszuschließenden Wandels von Erscheinungen und Zusammenhängen sowie Folgen des Regelungsproblems“* habe der Gesetzgeber nämlich die wichtige Aufgabe, *„nach Erlass des Gesetzes neben den Informations- und Aufklärungspflichten hinsichtlich des Zwecks und der Durchführung die Verpflichtung, gegebenenfalls für eine möglichst baldige Überprüfung zu sorgen.“*

Im Sinne dieser „praktischen Vernunft“, die Hassemer im Zusammenspiel von Strafrecht und Kriminologie am Beispiel einer „Gesamten Strafrechtswissenschaft“ immer wieder zurecht eingefordert hat, können beide Disziplinen an einer entscheidenden und im Besonderen der empirischen Evidenz zugänglichen Schnittstelle formeller Sozialkontrolle im Sinne der Eingangsfrage wichtige, interdisziplinär tragfähige Beiträge leisten. Entzieht man die Kriminologie bei der Analyse der Cyberkriminalität und deren derzeit überdies phänomenologisch extrem undeutlichen Konturen ihrer (im Rahmen des Konzepts einer „Gesamten Strafrechtswissenschaft“ implizit angelegten) „Bindung an“ und der damit „gegebenen Kanalisierung auf“ das Strafrecht, läuft ein derartiger Ansatz jedenfalls im Moment Gefahr, *„zu einem verschwommenen unscharfen Gebilde zu diffundieren“* (Kunz 2014, passim).

Tiefergehender, spezifisch „cyberkriminologischer Befunde“ bedarf die Analytik dabei jedenfalls im Augenblick noch nicht unmittelbar. Vielmehr benötigt das noch weitgehend unerforschte phänomenologische Dunkelfeld dringend umfänglicher Aufhellung (mit vorhandenen sozialwissenschaftlich-empirischen Methoden), um künftig – sicher zunächst einseitig anwendungsorientiert

anmutend – rechtzeitig institutionell, organisatorisch und personell die zügig gebotenen investiven Impulse und Grundsatzentscheidungen sowohl auf politischer als auch exekutiver Ebene treffen zu können. Das ist in Bezug auf die disziplinäre, derzeit zwischen den beiden Polen einer „traditionellen", methodisch positivistisch, quantitativ erklärenden Kriminologie, die sich v. a. im Rahmen „angewandter Forschung" der Praxis präventiver/repressiver Kriminalitätskontrolle sowie deren Instrumentarien zuwendet und derart Einfluss auf die politische Praxis zu nehmen versucht, und einer „theoretischen", qualitativ-interpretativen, mit kritischer Distanz zur jeweiligen kriminalpolitischen Formensprache auftretenden Kriminologie, zunächst auch kein dysfunktionaler Ansatz. Schon deshalb nicht, weil sich bei der „Cyberkriminalität" derzeit die „Verbrechenswirklichkeit" noch gar nicht ausreichend oder gar als ontologische Entität konturiert. Ohne eine derartige deutlich umrissene Kontur wäre ein theoretisch-interpretatives Vorgehen, ggf. sogar mit dem Ziel einer eigenen subkategorialen „Cyberkriminologie", allenfalls ein wenig Erfolg versprechendes Fischen im trüben Wasser. Auch im sozialwissenschaftlichen, qualitativ-interpretativen Kontext, bspw. angelehnt an den kriminologischen Interpretationsrahmen Edwin H. Sutherlands (1960, S. 3),

> „criminology is the body of knowledge regarding crime as a social phenomenon. It includes within its scope the process of making laws, of breaking laws, and of reacting toward the breaking of laws"

rekurriert der derzeit kriminologisch relevante Anteil zunächst vor allem auf das „lawbreaking" (i. S. „nature/extent of crime"), dann auf „reaction" („police, courts, corrections") und erst zuletzt auf das „lawmaking" („how laws are created/changed"), was naturgemäß auch Auswirkung auf den Ansatz entfaltet, mit dem man sich der Problemstellung primär annähert.

Literatur

Albrecht, H.-J. (2004). Öffentliche Meinung, Kriminalpolitik und Kriminaljustiz. In M. Walter, H. Kania, & H.-J. Albrecht (Hrsg.), *Alltagsvorstellungen von Kriminalität* (S. 491–520). Münster: LIT.

Birkel, C., Guzy, N., Hummelsheim, D., Oberwittler, D., & Pritsch, J. (Hrsg., durch das MPICC, 2014). *Der deutsche Viktimisierungssurvey 2012. Erste Ergebnisse zu Opferbefragungen, Einstellungen gegenüber der Polizei und Kriminalitätsfurcht*. Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht, Arbeitsbericht A7. Freiburg.

Bitkom. (2016). Studie: Sicherheit und Vertrauen im Internet, Internetquelle. https://www.bitkom.org/Presse/Anhaenge-an-PIs/2016/Oktober/Bitkom-Charts-PK-Vertrauen-und-IT-Sicherheit-13-10-2016-final.pdf. Zugegriffen: 1. Febr. 2019.

Bitkom. (2017). Pressemitteilung: Bürger sehen wachsende Bedrohung durch Cyberkriminelle. https://www.bitkom.org/Presse/Presseinformation/Buerger-sehen-wachsende-Bedrohung-durch-Cyberkriminelle.html. Zugegriffen: 1. Febr. 2019.

BKA (Hrsg.). Periodische Sicherheitsberichte, Teil 1 (2001) und Teil 2 (2006). https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PeriodischerSicherheitsbericht/periodischersicherheitsbericht_node.html. Internetquelle. Zugegriffen: 6. Jan. 2018.

BKA (Hrsg.). (2016a). Cybercrime, Bundeslagebild 2016. Wiesbaden. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2016.html. Zugegriffen: 17. Jan. 2020.

BKA (Hrsg.). (2016b). Polizeiliche Kriminalstatistik, Jahrbuch 2016. Wiesbaden. https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2016/pks2016_node.html. Zugegriffen: 17. Jan. 2020.

BKA (Hrsg.). (2017a). Cybercrime, Bundeslagebild 2017. Wiesbaden. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2017.html. Zugegriffen: 27. Sept. 2017.

BKA (Hrsg.). (2017b). Polizeiliche Kriminalstatistik. Wiesbaden. https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2017/pks2017_node.html. Zugegriffen: 17. Jan. 2020.

BKA (Hrsg.), & Bässmann, J. (2015). *Täter im Bereich Cybercrime. Eine Literaturanalyse. Teil 1: Eine phänomenologische und tätertypologische Betrachtung / Teil 2: Kriminologische Erklärungen und Handlungsmöglichkeiten, Bundeskriminalamt.* Kriminalistisches Institut, Forschungs- und Beratungsstelle Cybercrime KI 16. Wiesbaden.

BKA (Hrsg.), Bulanova-Hristova, G., et al. (2016). *Cyber-OC, Scope and manifestations in selected EU member states: Bd. 50. Polizei + Forschung.* Wiesbaden: BKA.

BKA (Hrsg.), & Füllgraf, W. (2016). *Hacktivisten – Abschlussbericht zum Projektteil der Hellfeldbeforschung*. Wiesbaden: BKA.

Bleckat, A. (2018). Mobbing und Cybermobbing – Eine Strafbarkeitslücke? In Wassermann et al. (Hrsg.), *Recht und Politik (Zeitschrift für deutsche und europäische Rechtspolitik), Berlin* (Beiheft 2, S. 75–82). Vgl. Buchbesprechung hierzu im PNL: http://polizei-newsletter.de/wordpress/?p=911. Zugegriffen: 1. Febr. 2019.

BloomBecker, B. (1990). *Spectacular computer crimes: What they are and how they cost American business half a billion dollars a year!* Homewood: University of Michigan & Dow Jones-Irwin.

Büchel, M., & Hirsch, P. (2014). *Internetkriminalität. Phänomene, Ermittlungshilfen, Prävention*. Heidelberg: Kriminalistik.

Cornelius, K. (2014). Plädoyer für einen Cybermobbing-Straftatbestand. *Zeitschrift für Rechtspolitik (ZRP), 47*(6), 164–167.

Diekmann, A., Przepiorka, W., & Rauhut, H. (2011). Die Präventivwirkung des Nichtwissens im Experiment. *Zeitschrift für Soziologie, 40*(1), 74–84.

DIW (Hrsg.), Riekmann, J., & Kraus, M. (2015). Tatort Internet: Kriminalität verursacht Bürgern Schäden in Milliardenhöhe. Internetquelle, Pressemitteilung. https://www.econstor.eu/handle/10419/108862. Zugegriffen: 1. Febr. 2019. Noch ausführlicher im DIW-Wochenbericht 12-2015, S. 295–301. Zugegriffen: 1. Febr. 2019.

Dreißigacker, A., & Riesner, L. (2018). Private Internetnutzung und Erfahrung mit computerbezogener Kriminalität. Ergebnisse der Dunkelfeldstudien des Landeskriminalamtes Schleswig-Holstein 2015 und 2017. Hannover: KfN (Hrsg.).

Durkheim, E. (1990). *Der Selbstmord*. Frankfurt a. M.: Suhrkamp. (Erstveröffentlichung 1897).

Fabricius, D. (2006). Generalprävention oder: Die beste Kriminalpolitik ist eine gute Rechtspolitik. In T. Feltes, et al. (Hrsg.), *Kriminalpolitik und ihre wissenschaftlichen Grundlagen* (S. 269–287). Heidelberg: Müller.

Fünfsinn, H., & Krause, B. (2019). Plattformen zur Ermöglichung krimineller Handlungen im Internet. In I. Goeckenjan, J. Puscheke, & T. Singelnstein (Hrsg.), *Für die Sache – Kriminalwissenschaften aus unabhängiger Perspektive. Festschrift für Ulrich Eisenberg zum 80. Geburtstag* (S. 641–654). Berlin: Duncker & Humblot.

Galassi, S. (2004). *Kriminologie im Deutschen Kaiserreich. Geschichte einer gebrochenen Verwissenschaftlichung*. Stuttgart: Steiner.

Golla, S. (2017). Risiken und Nebenwirkungen bei der Fortbildung des Internetstrafrechts – Datenhehlerei, Digitaler Hausfriedensbruch und alternative Regelungsansätze. In Hessische Rechtsanwaltschaft (Hrsg.), *Schriftenreihe der Stiftung* (Bd. 8, S. 153–181). Göttingen: Optimus.

Grabosky, P. (2009). High-tech crime: Information and communication related crime. In H. J. Schneider (Hrsg.), *Internationales Handbuch der Kriminologie* (Bd. 2, S. 73–102). Berlin: de Gruyter.

Guzy, N. (2014). International vergleichende Viktimisierungssurveys. Aktuelle Herausforderungen und Ergebnisse des Methodentests „ICVS-2". In S. Eifler, et al. (Hrsg.), *Empirische Forschung über Kriminalität. Methodologische und methodische Grundlagen* (S. 149–182). Wiesbaden: Springer.

Guzy, N., Birkel, C., & Mischkowitz, R. (Hrsg., durch das BKA, 2015). *Viktimisierungsbefragungen in Deutschland. Polizei + Forschung: Bd. 47.1, Erster Teilband – Ziele, Nutzen und Forschungsstand; Bd. 47.2, Zweiter Teilband – Methodik und Methodologie.* Wiesbaden: BKA.

Hassemer, W. (2008). *Strafrecht. Sein Selbstverständnis, seine Welt: Bd. 21. Strafrechtswissenschaft und Strafrechtspolitik*. Berlin: Berliner Wissenschafts-Verlag.

Hillenkamp, T. (2009). Zur Beobachtungs- und Nachbesserungspflicht des Gesetzgebers im Strafrecht. In H. E. Müller, G. Sander, & H. Válková (Hrsg.), *Festschrift für Ulrich Eisenberg zum 70. Geburtstag* (S. 301–320). München: Beck.

Hoffmann-Riem, W. (2014). Regulierungswissen in der Regulierung. In A. Bora, et al. (Hrsg.), *Wissensregulierung und Regulierungswissen* (S. 135–156). Weilerswist: Velbrück.

Hoffmann-Riem, W. (Hrsg.). (2018). *Big Data. Regulative Herausforderungen*. Baden-Baden: Nomos.

Hoven, E. (2018). Besser machen statt besser wissen. In: Frankfurter Allgemeine Zeitung, Einspruch Magazin vom 14. Jan. 2018. https://einspruch.faz.net/einspruch-magazin/2018-03-14/a51d34fff1cfc1299be56e189fc8cb3c/?GEPC=s5. Zugegriffen: 17. Jan. 2020.

Huber, E. (2015). Cybercrime gegen Privatpersonen. In N. L. Guzy, BKA, et al. (Hrsg.), *Viktimisierungsbefragungen in Deutschland: Bd. 47.1, Teilband 1. Polizei + Forschung* (S. 393–420). Wiesbaden: BKA.

Huber, E., & Pospisil, B. (Hrsg.). (2018). *Die Cyber-Kriminellen in Wien. Eine Analyse von 2006–2016*. Krems: Edition Donau-Universität, Zentrum für Infrastrukturelle Sicherheit.

Jaishankar, K. (2008). Space transition theory of cyber crimes. In F. Schmalleger & M. Pittaro (Hrsg.), *Crimes of the internet* (S. 281–283). Upper Saddle River: Prentice Hall.

Jehle, J.-M. (2007). Strafrechtswissenschaft und empirische Kriminologie – Konfrontation, Koexistenz, Integration? In Loos, et al. (Hrsg.), *Bedeutung der Strafrechtswissenschaft in Geschichte und Gegenwart* (S. 191–201). Heidelberg: Müller.

Jescheck, H.-H. (1980). Strafrecht und Kriminologie unter einem Dach. *Freiburger Universitätsblätter* (67), 39–43.

Karstedt, S. (2013). Zur Lage der Kriminologie in Großbritannien: Was können und sollten wir lernen? In H.-J. Albrecht, et al. (Hrsg.), *Zur Lage der Kriminologie in Deutschland, Monatsschrift für Kriminologie und Strafrechtsreform (MschrKrim), 96*(2/3), 127–130.

Kochheim, D. (2018). *Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik* (2. Aufl.). München: Beck.

Kunz, K.-L. (2010). Zur Symbolik des Strafrechts. In D. Dölling, et al. (Hrsg.), *Verbrechen – Strafe – Resozialisierung, Festschrift für Heinz Schöch zum 70ten* (S. 353–367). Berlin: de Gruyter.

Kunz, K.-L. (2014). Die „wissenschaftliche Eigenständigkeit" der Kriminologie. Zur diskursiven Formation einer Disziplin. Konferenzbeitrag „Penal law and criminology". https://www.researchgate.net/publication/316990587_Die_wissenschaftliche_Eigenstandigkeit_der_Kriminologie_Zur_diskursiven_Formation_einer_Disziplin. Internetquelle. Zugegriffen: 1. Sept. 2018.

Landeskriminalamt Niedersachsen. (2016). Dunkelfeldstudie – Befragung zu Sicherheit und Kriminalität in Niedersachsen. 2. Welle der 2012 gestarteten Initiative, Internetquelle. http://www.lka.niedersachsen.de/forschung/dunkelfeldstudie/dunkelfeldstudie-befragung-zu-sicherheit-und-kriminalitaet-in-niedersachsen-109236.html. Zugegriffen: 1. Febr. 2019.

Lange, H.-J., & Böttcher, A. (Hrsg.). (2015). *Cyber-Sicherheit: Bd. 18. Studien zur Inneren Sicherheit*. Wiesbaden: Springer VS.

Leisterer, H. (2018). *Internetsicherheit in Europa*. Reihe: Internet und Gesellschaft, Band 12 der Schriften des Alexander von Humboldt-Instituts für Internet und Gesellschaft an der HU Berlin. Tübingen: Mohr Siebeck.

Lösel, F. (2013). Kriminologie in Großbritannien. *Zur Lage der Kriminologie in Deutschland, Monatsschrift für Kriminologie und Strafrechtsreform (MschrKrim), 96*(2/3), 131–139.

Meier, B.-D. (2004). Restorative Justice – Bericht über Deutschland. In H. Schöch & J. Jehle (Hrsg.), *Angewandte Kriminologie zwischen Freiheit und Sicherheit* (S. 415–428). Mönchengladbach: Forum.

Meier, B.-D. (2012). Neue Kriminalitätsformen: Phänomenologie und Bedingungsfaktoren der Internetkriminalität. In E. Hilgendorf, et al. (Hrsg.), *Festschrift für Wolfgang Heinz* (S. 209–221). Baden-Baden: Nomos.

Meier, B.-D. (2015a). Kriminologie und Internet: Ein ungeklärtes Verhältnis. In S. Beck, et al. (Hrsg.), *Cybercrime und Cyberinvestigations* (S. 93–118). Baden-Baden: Nomos.

Meier, B.-D. (2015b). Illegaler Download: Alltagshandeln ohne Unrechtsbewusstsein. In T. Rotsch, et al. (Hrsg.), *Strafrecht, Jugendstrafrecht, Kriminalprävention in*

Wissenschaft und Praxis. Festschrift für Heribert Ostendorf zum 70. Geburtstag (S. 619–634). Baden-Baden: Nomos.

Meier, B.-D. (2016). Risikofaktoren der Onlinekriminalität. In F. Neubacher, et al. (Hrsg.), *Krise – Kriminalität – Kriminologie: Bd. 116. Neue Kriminologische Schriftenreihe* (S. 231–244). Bad Godesberg: Forum.

Merton, R. K. (1949). *Social theory and social structure. Toward the codification of theory and research*. Glencoe: Free Press.

Mischkowitz, R. (2013). Fragen an die Kriminologie … aus Sicht der Polizei. *MschrKrim, 96*(2/3), 212–221.

Nassehi, A. (2017). *Die letzte Stunde der Wahrheit* (kpl. überarbeitete Neu Aufl.). Hamburg: kursbuch.edition.

Neubacher, F. (2006). Welche Zukunft hat die Kriminologie? Über Kriminalpolitik und Kriminologie in Deutschland. In M. Walter, et al. (Hrsg.), *Neue Wege und Perspektiven der Kriminologie* (S. 403–471). Berlin: LIT.

Noll, P. (1973). *Gesetzgebungslehre: Bd. 37. Rechtswissenschaften*. Reinbek bei Hamburg: Rororo Studium.

Oehmichen, A., & Weißenberger, B. (2019). Digitaloffensive im Strafrecht! Verbesserte Bekämpfung von Cyberkriminalität durch das IT-Sicherheitsgesetz 2.0? In G. Duttge, et al. (Hrsg.), *KriPoZ, 4*(3), 174–182.

Plank, H. (2017). *Gesamte Strafrechtswissenschaft. Ein fallanalytischer Diskurs am Beispiel eines Kriminalromans: Bd. 40. Bochumer Schriften zur Rechtsdogmatik und Kriminalpolitik*. Holzkirchen: Felix.

Popitz, H. (1968). *Über die Präventivwirkung des Nichtwissens*. Berlin: Berliner Wissenschafts-Verlag. (um ein Vorwort von Fritz Sack ergänzte Neuauflage, 2003).

Rolinski, K. (2009). Über rationale und nicht rationale Gesetzgebung. In H. E. Müller, et al. (Hrsg.), *FS für Ulrich Eisenberg* (S. 171–192). München: Beck.

Rüdiger, T.-G. (2018). *Das Broken-Web-Phänomen.* Online-Publikation „Publicus", Teil 1, Ausgabe 3/2018; Teil 2, Ausgabe 4/2018. Stuttgart: Boorberg. Parallel veröffentlicht in: Der Wirtschaftsführer 2017–2018, S. 50–53. Rubrik Jur@ im Netz. Stuttgart: Boorberg.

Sazger, H. (2007). Das europarechtliche Verhältnismäßigkeitsprinzip als Maßstab für eine europäische Kriminalpolitik. *Neue Kriminalpolitik (NK)* (3), 93–98.

Schaar, P. (2018). *Trügerische Sicherheit*. Hamburg: Edition Körber.

Schulze, M. (2019). Kriminalitätsbekämpfung im Dark Net. Neue Ermittlungsansätze statt Verbote. SWP-Aktuell 2019/A 28. https://doi.org/10.18449/2019a28.

Schulze-Fielitz, H. (1988). *Theorie und Praxis parlamentarischer Gesetzgebung*. Berlin: Duncker & Humblot.

Selzer, N. (2019). Bekämpfung der Organisierten Kriminalität in der digitalen Welt – Kritische Betrachtung des RefE zum IT-Sicherheitsgesetz 2.0. In G. Duttge, et al. (Hrsg.), *KriPoZ, 4*(4), 221–230.

Skala, M. (2011). Cyberwarfare – Identifying the opportunities and limits of fighting in the ‚fifth domain'. In M. Majer, R. Ondrejcsák, V. Tarasovic, & T. Valášek (Hrsg.), *Panorama of global security environment* (S. 511–565). Bratislava: Centre for European and North Atlantic Affairs.

Sutherland, E.-H., et al. (1960). *Principles of criminology*. Chicago: Lippincott.

Vec, M. (2009). Sichtbar / Unsichtbar: Entstehung und Scheitern von Kriminologie und Kriminalistik als semiotische Disziplinen. In R. Habermas & G. Schwerhoff (Hrsg.), *Verbrechen im Blick* (S. 383–414). Frankfurt a. M.: Campus.

von Liszt, F., & Dochow, A. (1881). An unsere Leser. Geleitwort der 1. Ausgabe der *Zeitschrift für die gesamte Strafrechtswissenschaft (ZStW), 1*, 1–3.

Weber, M. (1976). *Wirtschaft und Gesellschaft. Grundriss (sic!) der verstehenden Soziologie* (Fünfte, revidierte Aufl.). Tübingen: Mohr Siebeck.

Wernert, M. (2018). *Internetkriminalität. Grundlagenwissen, erste Maßnahmen und polizeiliche Ermittlungen* (3. aktualisierte Aufl.). Stuttgart: Boorberg.

Wolbring, T., & Keuschnigg, M. (2015). Disorder, social capital, and norm violation: Three field experiments on the broken windows thesis. *Rationality and Society, 27,* 96–126.

Der digitale Raum ist kein (grund-)rechtsfreier Raum

Roland Hoheisel-Gruler

Bereits im Jahre 2001, und damit lange bevor das mobile Internet und die Sozialen Medien die moderne Gesellschaft prägen konnten, stellten sich Gerhard Vowe und Martin Emmer die Frage, ob es so etwas wie eine digitale Agora geben können (Vowe und Emmer 2001). Die Agora war im antiken Griechenland nicht nur ein Marktplatz, sondern der zentrale Ort, an dem Meinungen kundgetan und diskutiert wurden. Sie war der Ort, an dem das Zusammenleben in der Polis organisiert und mitgestaltet wurde. Diesen Platz finden wir heute auch in der digitalen Welt.

Eine allgemeingültige Definition für den Begriff „Digitale Welt" sucht man vergebens. Die beste Näherung kann man daher erreichen, wenn man den Zusammenhang mit digitalen Sachverhalten sucht. Dieser weite Begriff umfasst daher die Gesamtheit aller Einzelerscheinungen, die mit Digitalsignalen beschrieben oder von diesen beeinflusst werden können (Berthel 2019). Diese digitale Welt ist aber keine schlichte Adaption der analogen Lebensumgebung. Die fortschreitende Digitalisierung der Lebensbereiche führt auch zu einem Wandel der Alltagsgestaltung und Wahrnehmung der Menschen. Dieser Prozess betrifft neben der Berufs- und Arbeitswelt auch das Privatleben: Mobile Endgeräte sind aus dem Alltag nicht mehr wegzudenken. Damit verändern sich aber auch Informationsbeschaffungsvorgänge ebenso wie das Kommunikationsverhalten. Die digitalen Medien, Werkzeuge und die verschiedensten Kommunikationsmöglichkeiten mit Messenger-Diensten oder über Social Media-Plattformen ermöglichen daher neue mediale Wirklichkeiten (Kultusministerkonferenz 2016). Gleichwohl steht die

R. Hoheisel-Gruler (✉)
Fachbereich Kriminalpolizei, Hochschule des Bundes für öffentliche Verwaltung, Wiesbaden, Deutschland
E-Mail: post@elfstricheins.de

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

T.-G. Rüdiger und P. S. Bayerl (Hrsg.), *Cyberkriminologie,*
https://doi.org/10.1007/978-3-658-28507-4_3

digitale Polizeiarbeit vor dem Dilemma, dass sie es eben nicht mit virtuellen Welten, sondern mit real existierenden Menschen zu tun hat, deren Handeln in der analogen Welt sich im Digitalen auswirkt.

Das Bundeskriminalamt definiert Cybercrime folgendermaßen: *„Cybercrime umfasst die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne) oder die mittels dieser Informationstechnik begangen werden“* (Bundeskriminalamt 2016, S. 2).

In diesem Beitrag soll auf Besonderheiten, die das Internet als Kommunikationsmittel bietet, eingegangen werden. Phänomene der Schwer- und Schwerstkriminalität unter Verwendung des Internets, die Probleme, die sich durch die Verschlüsselung von Kommunikation ergeben, und das Darknet sollen dagegen allenfalls am Rande mit betrachtet werden. Kommerzielle Datenabgriffe und ähnliche Deliktsformen bleiben außen vor. Dies hat seinen Grund darin, dass es sich bei diesen Phänomentypen um kriminelle Handlungen in der realen Welt handelt, die unter Zuhilfenahme digitaler Hilfsmittel erfolgen. Auch Erpressungsversuche mittels Ransomware oder Phishing bleiben hier aus demselben Grunde unbeachtet. Viele Formen von Wirtschaftskriminalität sind ohne digitale Unterstützung kaum denkbar. Zwar wird Handel von Drogen oder Waffen, Menschenhandel oder die Verteilung von Kinderpornografie im Wesentlichen über Online-Plattformen abgewickelt, aber auch hier dienen die digitalen Möglichkeiten im Wesentlichen nur der Erleichterung der Straftatenbegehung und der Erschwerung der Strafverfolgung (s. a. Kap. „Strafverfolgung digital“ und „Darknet – die dunkle Seite des Internets?“).

Auf der anderen Seite gibt es gerade im Kommunikationsbereich Möglichkeiten strafrechtlich relevanten Verhaltens, das eben aufgrund des internetbasierten Austausches zwischen Menschen im virtuellen Raum stattfindet. Diesem kleinen Ausschnitt des Cybercrime, also in der Untergruppe „mittels dieser Informationstechnik begangen“ gelten die folgenden Ausführungen.

1 Das Internet ist kein rechtsfreier Raum

Diese an sich banale Erkenntnis wurde und wird auf den verschiedensten Kanälen so oft und bei jeder sich bietenden Gelegenheit wiederholt, sodass die Frage angebracht sein dürfte, ob dem wirklich so sei.

Zu Beginn lohnt ein Blick in die Geschichte des Internet: Dessen Anfänge basieren auf einer plattformunabhängigen Kommunikationsmöglichkeit zwischen Wissenschaftlern, die zudem schnell und kostengünstig war. Frühzeitig erkannten

zunächst Wirtschaftsunternehmen das Potenzial, das in der Vernetzung von Firmen und Kunden steckte. Während das Web 2.0 die Interaktionsmöglichkeiten entdeckte und nutzbar machte, führte die Entwicklung der mobilen Endgeräte und die Entwicklung von Social Media-Plattformen zu einer weitestgehend alle Lebensbereiche durchdringende Digitalisierung des Privaten. Das Marktvolumen einiger weniger Internetkonzerne beläuft sich auf viele Milliarden US-Dollars. Die rechtlichen Rahmenbedingungen konnten mit den rasanten Entwicklungen der letzten Jahre nicht standhalten. Mit dem Begriff der „Goldgräberstimmung" verbindet sich nicht nur die Erwartung auf die Realisierung von schnellen Gewinnen, sondern eben auch die Chance, das Recht selbst in die Hand zu nehmen und die eigenen Regeln durchzusetzen.

Mit diesem Begriff eng verwoben ist die Vorstellung des kalifornischen Goldrausches 1849/1849. Mehrere hunderttausend Goldsucher kamen innerhalb kürzester Zeit nach Kalifornien (Rawls und Orsi 1999). Damit einher geht auch der Umstand, dass die Entwicklung ziviler Strukturen und rechtsstaatlicher Grundsätze dem Ansturm der Menschenmassen nicht gewachsen war. Daraus folgte zwangsläufig, dass die Menschen gehalten waren, ihr Recht in die eigene Hand zu nehmen. Bereits 1851 entstanden in San Francisco „Committees of Vigilance". Diese als Bürgerwehr auftretende Organsiation verfolgte das Ziel, „das Gesetz in die eigene Hand zu nehmen." (Taniguchi 2016, S. 42; s. a. Kap. „Digitaler Vigilantismus").

Hinzu kommt ein weiteres Moment, das in der US-amerikanischen Kultur tief verwurzelt ist. Bereits Alexis de Tocqueville beschrieb in „Über die Demokratie in Amerika" 1799 die Ideale einer Bürgergesellschaft, die sich selbst organisiert und sich aufgrund des bürgerschaftlichen Engagement von sich heraus entwickelt und kontrolliert (Tocqueville, II. Sect. 2, Kap. 5). Der norwegische Kriminologe Nils Christie beschrieb 1977 die Verdrängung der Bürger aus der Regelung oder Lösung ihrer sie betreffenden Konflikte. Seiner Auffassung zufolge sind Straftaten und andere Konflikte zunächst und vornehmlich Eigentum der betroffenen Bürger (Christie 1977).

Ergänzt wird dies um den zweiten Verfassungszusatz der USA, dessen Inhalt jedem das Recht zuspricht, Waffen zu besitzen und zu tragen. Der Wesensgehalt dieser Grundrechtsgewährleistung wird auch als Beleg dafür genommen, dass ein dem unserem Rechtssystem vertrautes Gewaltmonopol des Staats dem der Vereinigten Staaten fremd ist (Hansen 2012). Hinzu kommt, dass weite Teile der sogenannten Netzgemeinde sich als basisdemokratisch organisierte Selbstverwaltungseinheiten (Rosenkranz und Feddersen 2010) verstehen, die einer öffentlichen Regulierung kritisch gegenüberstehen. Das Recht in die eigene Hand nehmen heißt in diesem Zusammenhang auch: den Einfluss staatlicher Kontrolle und Einflussnahme zurückdrängen soweit dies möglich ist (Kirsch 1988).

Als ein Beispiel für eine Initiative, die im Netz das Recht in die eigene Hand nimmt, könnte das Kollektiv „Anonymous“ gelten. Wiedemann (2012, S. 212) beschreibt diese Gruppe als eine „open collectivity“. Es ist kein Verein, keine Organisation, keine Institution. Auch die Beschreibung als „Hacker-Gruppe“ ist unzureichend. Sie stellt heraus, dass Anonymous selbst der Kampf dafür sei, dass alle Anonymous sein dürften. Es gehe um Teilhabe ohne Beschränkung. Diese beziehe sich sowohl auf den Informationsfluss als auch auf den Informationsaustausch. Sie beschreibt Anonymous daher zutreffend als eine „dauernde Herausforderung und Verschiebung von Herrschaftsverhältnissen und Grenzziehungen“ (Wiedemann 2012, S. 213).

Nahezu die gesamte bundesdeutsche Bevölkerung ist zwischenzeitlich online zu finden: Die Online-Studie von ARD und ZDF aus dem Jahre 2018 stellte fest, dass der Anteil der Internetnutzer sich auf 90,3 % der Gesamtbevölkerung belaufe, bei Jugendlichen zwischen 14 und 19 Jahren liegt der Anteil sogar bei 100 %.[1] Dabei ist der Anteil an der Nutzung von Online-Communities im Vergleich zur Vorjahreserhebung nochmals angestiegen, wobei Facebook als einzige Plattform einen leichten Rückgang hinnehmen musste.[2]

Wenn es nun um Problemkreise geht, in denen die Interaktion zwischen den Internetnutzern zu Konfliktlagen führt, wird die eingangs erwähnte These wie ein Mantra in die Debatte gebracht. Die zentrale Botschaft wurde auch von der Bundeskanzlerin Frau Dr. Angela Merkel wiederholt und zuletzt anlässlich des Safer Internet Day 2018 in ihrem Video-Podcast zum Ausdruck gebracht.[3] Hierbei ist bedeutsam, dass dieses Zitat in unmittelbarem Kontext zu ihren Ausführungen zum NetzDG gefallen ist. Rüdiger (2019) weist darauf hin, dass es nicht allein darauf ankommen kann, ob es einen definierten oder definierbaren Raum gibt, in dem formal-juristisch Gesetze Geltung beanspruchen. Vielmehr sei entscheidend, ob die Chance besteht, dass diese auch mit einer hinreichenden Wahrscheinlichkeit durchgesetzt werden können (Rüdiger 2019). Daran können aber, wenn man die öffentliche Debatte verfolgt, durchaus Zweifel angebracht sein. Hinzu kommt in diesem Zusammenhang auch der Glaube an die Selbstregulierungskräfte im Netz im Zusammenspiel mit einer Wahrnehmung unter den Internetnutzern, wonach Gesetze in der digitalen Welt nicht durchgesetzt

[1] http://www.ard-zdf-onlinestudie.de/ardzdf-onlinestudie-2018/

[2] http://www.ard-zdf-onlinestudie.de/ardzdf-onlinestudie-2018/whatsapponlinecommunities/ zit: Onlinestudie-whatsapp 2018.

[3] https://www.bundeskanzlerin.de/bkin-de/mediathek/die-kanzlerin-direkt/merkel-das-internet-ist-kein-rechtsfreier-raum--1007676

werden können, sondern allenfalls eigene Regeln gelten. Auf der einen Seite und gemäß dem marktliberalen Ansatz der Selbstregulierung ist das Internet zwar kein rechtsfreier Raum, um die Geltung und Einhaltung der in der analogen Welt geltenden Regeln muss aber gerungen werden.

2 Grundrechtsgeltung und das Internet

Die hier näher zu behandelnden Verhaltensweisen betreffen in erster Linie die Menschenwürde, das allgemeine Persönlichkeitsrecht und die Meinungsfreiheit. Immer wieder muss im Einzelfall daher zwischen den berechtigten Interessen der Betroffenen und der Meinungsfreiheit der Akteure abgewogen und ein Ausgleich geschaffen werden. Aufgabe des allgemeinen Persönlichkeitsrechts ist es, wie das Bundesverfassungsgericht schon in der Eppler-Entscheidung ausgeführt hatte, *„im Sinne des obersten Konstitutionsprinzips der ‚Würde des Menschen' (Art. 1 Abs. 1 GG) die engere persönliche Lebenssphäre und die Erhaltung ihrer Grundbedingungen zu gewährleisten"* (BVerfGE 54, 148 (153) – Beschluss vom 3. Juni 1980 – 1 BvR 185/77). Es dient dem Schutz der inneren Elemente und Faktoren der menschlichen Entfaltungsfreiheit, soweit diese nicht schon anderweitig Gegenstand der besonderen Freiheitsgarantien des Grundgesetzes sind. Das allgemeine Persönlichkeitsrecht wird daher verstanden als ein Recht auf Respektierung der Integrität des „Person-Seins". Es hebt sich von der allgemeinen Handlungsfreiheit als dem aktiven, nach außen gerichtetem Element der Persönlichkeitsentfaltung ab. Der Schutzbereich des allgemeinen Persönlichkeitsrechts erfasst nur jene engeren Tatbestände, die die – von der Menschenwürde Art. 1 Abs. 1 GG her verstärkten – wesentlichen Bedingungen personaler Autonomie ausmachen.

Wenn die menschliche Persönlichkeit aufgrund der gesellschaftlichen Entwicklung oder des wissenschaftlich-technischen Fortschritts neuen Gefährdungen ausgesetzt wird, ist der Schutzbereich entsprechend, wie beim Volkszählungsurteil aus 1983, neu zu bestimmen (BVerfGE 65, 1 (41) – BVerfG, Urteil vom 15. Dezember 1983 – 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83). Das hierin erstmals dogmatisch ausformulierte Recht auf informationelle Selbstbestimmung leitet sich aus den oben genannten Grundannahmen ab. Es flankiert den grundrechtlichen Schutz von Verhaltensfreiheit und Privatheit beim Umgang mit personenbezogenen Daten, indem es ihn bereits auf der Ebene der Gefährdung der Persönlichkeit beginnen lässt (BVerfG, Beschluss vom 13. Juni 2007 – 1 BvR 1550/03, 2357/04, 603/05).

Der ehemalige Präsident des Bundesverfassungsgerichts, Papier, stellte die Frage, wie es angesichts der realen Entwicklungen der digitalen Gesellschaft

um die Geltungskraft dieses allgemeinen Persönlichkeitsrechts in seiner Unterausprägung sowohl als Recht auf informationelle Selbstbestimmung wie auch in der Unterausprägung des Rechts auf die Sicherheit und Integrität informationstechnischer Systeme bestellt sei, wobei er auch das Telekommunikationsgeheimnis nach Art. 10 GG mit in die Thematik aufnahm (Papier 2017). Das Bundesverfassungsgericht hatte bereits im Volkszählungsurteil darauf hingewiesen gehabt, dass in Ermangelung einer Datenhoheit des Betroffenen, dieser wesentlich gehemmt werden könnte, aus eigener Selbstbestimmung zu planen und zu entscheiden. Gerade wenn es um den Umgang mit rechtswidrigen Inhalten im Internet geht, weist Papier darauf hin, dass nach der Rechtsprechung des Bundesgerichtshofs und seiner Wechselwirkungslehre sehr strenge Maßstäbe anzulegen seien, wenn es um die Beschränkbarkeit des Art. 5 GG gehe. Die Schranken können demnach nur aufgrund einer Interessenabwägung bestimmt werden, die einerseits der grundlegenden wertsetzenden Bedeutung des Art. 5 Abs. 1 GG Rechnung trägt und andererseits strikt auf den Einzelfall bezogen ist (Papier 2017).

Die Wechselwirkungslehre des Bundesverfassungsgerichts besagt, dass die „allgemeinen Gesetze“, die nach Art. 5 Abs. 2 GG der Meinungsfreiheit eine Schranke setzen, in ihrer das Grundrecht beschränkenden Wirkung ihrerseits im Lichte und in der Bedeutung der Grundrechte gesehen und so interpretiert werden, dass der besondere Wertgehalt der in Art. 5 Abs. 1 GG verankerten Rechte gewahrt bleibt. Dies hat das Gericht bereits im Lüth-Urteil 1958 ausgeführt (Bundesverfassungsgericht Urteil vom 15. Januar 1958, Az.: 1 BvR 400/51). Die gegenseitige Beziehung zwischen Grundrecht und „allgemeinem Gesetz“ bedeutet also nicht nur, dass der Geltungskraft des Grundrechts nur durch diese „allgemeinen Gesetze“ eine einseitige Beschränkung entgegensteht. Es ist stattdessen eine Wechselwirkung zu beobachten, nach der die Schranken setzenden Gesetze ihrerseits aus der Erkenntnis der wertsetzenden Bedeutung dieser Grundrechte im freiheitlich-demokratischen Staat ausgelegt und so „in ihrer die Grundrechte begrenzenden Wirkung selbst wieder eingeschränkt werden“ (Bundesverfassungsgericht Urteil vom 15. Januar 1958, Az.: 1 BvR 400/51). Die Gefahren für das allgemeine Persönlichkeitsrecht in der digitalen Umgebung werden aus diesen Gründen flankiert über die Debatte zur Meinungsfreiheit aus Art. 5 GG.

Bei der Bewertung, ob eine Äußerung vom dem Schutzbereich der Meinungsfreiheit gedeckt ist oder ob in der Abwägung mit dem Schutz des von der Äußerung betroffenen Rechtsgutes diesem der Vorrang zu geben ist, kommt es darauf an, ob die Formulierungen oder die Umstände der Äußerung eine nicht das Persönlichkeitsrecht verletzende Deutung zulassen (Bundesverfassungsgericht

Beschluss vom 25.03.1992, Az.: 1 BvR 514/90). Falls unter mehreren möglichen Deutungen einer Äußerung nur eine zu einer straf- oder zivilrechtlichen Sanktion führen kann, reicht es nicht aus, die hierfür sprechenden Gründe anzugeben. Vielmehr müssen sämtliche anderen Deutungsmöglichkeiten eindeutig ausgeschlossen werden können (Bundesverfassungsgericht Beschluss vom 4. April 2002, Az.: 1 BvR 724/98). Wenn die Äußerung einen Beitrag zur öffentlichen Meinungsbildung leisten soll, spricht eine Vermutung zugunsten der Freiheit der Rede, wie das Bundesverfassungsgericht bereits im Lüth-Urteil ausgesprochen hatte (Bundesverfassungsgericht Urteil vom 15. Januar 1958, Az.: 1 BvR 400/51). Das Bundesverfassungsgericht lässt bei seiner Rechtsprechung die Tendenz erkennen, dass bei Beiträgen zur öffentlichen Debatte im Konflikt zwischen Meinungsfreiheit und Ehrenschutz dem letzteren der Vorrang eingeräumt wird.

Geschützt ist nach Art. 5 GG die Meinung, wobei grundsätzlich ein freier Meinungsbegriff Anwendung findet (Bundesverfassungsgericht Beschluss vom 22. Juni 1982, Az.: 1 BvR 1376/79). Entscheidend wird hier auf das „Element der Stellungnahme, des Dafürhaltens oder Meinens“ abgestellt. Dies kann im Rahmen einer geistigen Auseinandersetzung oder sonstigen sozialen Kommunikation erfolgen. Dabei geht es nur um diese äußeren Faktoren; der Wert, die Richtigkeit, die Rationalität oder die Gefährlichkeit einer Äußerung ist für die Qualifizierung einer Äußerung als Meinung irrelevant (Bundesverfassungsgericht Beschluss vom 4. November 2009, Az.: 1 BvR 2150/08). Allerdings ist durchaus umstritten, ob reine Tatsachenbehauptungen „Meinungen“ darstellen können. Tatsachenbehauptungen werden dadurch gekennzeichnet, dass sie der Überprüfung mit Mitteln des Beweises zugänglich sind (Bundesverfassungsgericht Beschluss vom 13. April 1994, Az.: 1 BvR 23/94 „Auschwitzlüge“). Sie können daher nach Auffassung des Bundesverfassungsgerichts nur soweit in den Schutzbereich des Art. 5 Abs. 1 S. 1 GG fallen, als sie selbst eine Voraussetzung der Bildung von Meinungen darstellen (Bundesverfassungsgericht Beschluss vom 22. Juni 1982, Az.: 1 BvR 1376/79). Bewusst unwahre Tatsachenbehauptungen, falsche Informationen oder unrichtige Zitate fallen nicht unter den Meinungsbegriff, da sie aufgrund ihres unwahren Inhalts nichts zum Meinungsbildungsprozess beitragen können. Die Lüge genießt daher per se keinen Grundrechtsschutz (Bundesverfassungsgericht Beschluss vom 3. Juni 1980, Az.: 1 BvR 797/78 „Heinrich Böll“).

Wenn es im Internet um die Problematik des Sperrens oder Löschen inkriminierter Postings geht, ist in der Debatte schnell der Begriff der Zensur zur Hand. Die Zensur, die mit der Aussage in Art. 5 Abs. 1 S. 3 GG gemeint ist, ist nur die sog. Vor- oder Präventivzensur. Darunter versteht man die präventive Vorschaltung eines behördlichen Verfahrens, welches die Vorprüfung oder

Genehmigung durch eine Behörde in Bezug auf die Abfassung, Herstellung oder Verbreitung eines Werkes zum Gegenstand hat (Bundesverfassungsgericht Beschluss vom 25. April 1972, Az.: 1 BvL 13/67). Der Natur der Sache nach schützt das Zensurverbot daher „nur Akte der Meinungsäußerung und möglicherweise auch der Meinungsverbreitung, mithin den Hersteller und unter Umständen auch den Verbreiter eines Geisteswerkes“, nicht aber die Adressaten der Äußerung (Bundesverfassungsgericht Beschluss vom 14. Oktober 1969, Az.: 1 BvR 30/66). Aus diesen Gründen ist die Begrifflichkeit der „Zensur“ in diesem Zusammenhang falsch und irreführend.

3 Befugniserweiterungen im Digitalen Raum: Online-Durchsuchungen, Quellen-TKÜ

In den vergangenen Jahren lag der Schwerpunkt der strafprozessualen und gefahrenabwehrrechtlichen Debatte auf der Erweiterung der polizeilichen Befugnisse, insbesondere bei verdeckten Maßnahmen im digitalen Bereich. Wenn man die Entwicklung der letzten zehn Jahre betrachtet, ging es insbesondere um technikoffene Regelungen zur Strafverfolgung und Gefahrenabwehr (May 2017). Die von Strafverfolgungsbehörden gewünschte Vorratsdatenspeicherung ist wegen rechtlicher Unsicherheiten bislang zwar Gesetz, wird aber nicht angewendet. Zuletzt sind durch das Gesetz vom 17. August 2017 hier weitreichende Eingriffsbefugnisse geschaffen worden. Zu nennen sind hier an erster Stelle die Schaffung gesetzlicher Grundlagen für Online-Durchsuchungen zur Aufhellung gespeicherter Daten. Daneben war aufgrund der Entwicklungen im Telekommunikationsbereich die Quellen-TKÜ als Maßnahme zur Telekommunikationsüberwachung in die Strafprozessordnung aufgenommen worden. Hier wird eine heimliche Software auf den Kommunikationssystemen installiert, um die dortigen Verschlüsselungen zu umgehen. Dies ist grundsätzlich auf mehreren Wegen denkbar.

Dabei ist zu unterscheiden zwischen einem aktiven Aufspielen durch Hoheitsträger, die das informationstechnische System physisch hierzu in ihren Händen halten müssten, oder durch eine Infektion des betroffenen Systems. Die erste Variante könnte durch ein aktives Aufspielen beispielsweise bei einer Grenzkontrolle oder einem vergleichbaren Anlass erfolgen; zu denken wäre auch ein Aufspielen durch Hoheitsträger nach heimlichem Betreten der Räumlichkeiten, in denen sich das System befindet. Alternativ dazu gäbe es das Ausnutzen der Unaufmerksamkeit des berechtigten Nutzers, etwa indem man ihm einen E-Mail-Anhang mit einem (getarnten) Infektionsprogramm in der Hoffnung

zuspielt, dass er ihn ausführen werde, oder aber das Aufspielen durch Ausnutzen von Sicherheitslücken des genutzten Systems, etwa indem der berechtigte Nutzer zum Aufruf einer speziell präparierten WWW-Seite animiert wird, deren bloße Ansicht aufgrund von Sicherheitslücken zur Infektion des Zielsystems führt (sogenannte drive by downloads).

Das Aufspielen anlässlich einer Kontrolle ist ebenso unbedenklich wie die als kriminalistische List zu bezeichnende Übersendung einer infizierten E-Mail. Beide Varianten tragen aber Nachteile der Entdeckung oder des Scheiterns, beispielsweise durch Nicht-Ausführen des Programmes, in sich. Das Betreten von Räumlichkeiten zum Zwecke der Infektion des informationstechnischen Systems dürfte wegen fehlender Ermächtigungsgrundlage, die einen Eingriff in Art. 13 GG rechtfertigen müsste, nicht zu realisieren sein. Das Ausnutzen von Sicherheitslücken indes stellt, wenn die technischen Voraussetzungen geschaffen sind, deshalb diejenige Möglichkeit dar, die am ehesten als erfolgversprechend einzustufen ist. Damit eine solche Infektion also gelingen kann, müssen Sicherheitslücken, die nicht geschlossen werden, ausgenutzt werden.

Ein Exploit wird definiert als das systematische Ausnutzen von Schwachstellen in informationstechnischen Systemen. Ein Zero-Day-Exploit ist besonders effektiv, da dieser eingesetzt werden kann, bevor die Entwickler einen Patch als Gegenmaßnahme zur Verfügung stellen können. Es bleibt daher keine Zeit – zero days – um das System zu schützen. Komplexe, gezielte Cyber-Angriffe zielen auf Effektivität. Deshalb beruhen sie in der Regel auf dem Ausnutzen solcher Zero-Day-Exploits. Diese können sowohl in der Hardware als auch im Softwarecode der jeweiligen Zielsysteme vorliegen. Das Fehlen von Patches bringt neben der Wirksamkeit aufgrund fehlender Abwehrmöglichkeiten auch mit sich, dass das Entdeckungsrisiko gering ist. Das kompromittierte System hat keine Möglichkeit, die Infektion zu erkennen.

Das als „stockpiling“ bezeichnete Verhalten bezeichnet die Geheimhaltung des Wissens über solche Sicherheitslücken. Aus dem „stockpilling“ folgt zunächst, dass solche Lücken nicht dem Hersteller gemeldet werden und folglich nicht behoben werden. Statt dessen werden diese auf Schwarzmärkten, beispielsweise im Darknet, zu hohen Preisen feilgeboten. Darauf basiert dann die aktive Entwicklung von Tools, die den Angriff auf das Zielsystem unter Ausnutzung dieser Lücken erlauben (Schulze 2019). Als Käufer auf diesen Märkten treten Kriminelle, Black Hat-Hacker, Terroristen ebenso auf wie auch Polizeibehörden, Geheimdienste und Militärs sowohl demokratischer als auch autoritärer Staaten (Ablon et al. 2014).

Die in §§ 100a Abs. 1 Satz 2, 100b StPO geschaffenen Regelungen sind deshalb primär an dem Grundrecht auf Gewährleistung der Vertraulichkeit und

Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG), wie dies das Bundesverfassungsgericht entwickelt hat, (Bundesverfassungsgericht, Urteil vom 27. Februar 2008, Az.: 1 BvR 370/07) zu messen. Diese gesetzgeberischen Maßnahmen stellen die Rechtfertigung eines besonders schwerwiegenden Eingriffs in den Schutzbereich des sogenannten Computergrundrechts dar. Deswegen hat der Gesetzgeber für die Online-Durchsuchung sich bei den Schranken an der akustischen Wohnraumüberwachung orientiert. Allerdings ist hierbei zu beachten, dass bei der Online-Durchsuchung nicht nur Telekommunikationsverbindungen untersucht werden; hier kann eine vollständige Einsicht in die gesamte Kommunikation und über alle Aufenthaltsorte erreicht werden. Damit reichen die erlangten Ergebnisse weiter als bei einem Lauschangriff. Wegen der Schwere des Grundrechtseingriffes sind daher überragende Rechtsgüter wie Leib, Leben, Freiheit von Personen oder Bestand des Staates und seiner Organe in die Abwägung einzustellen. Darüber hinaus erlangt der Schutz des Kernbereichs privater Lebensführung allein aufgrund der Tatsache, dass mobile Endgeräte als permanente Begleiter in der Lage sind, Bewegungsprofile zu tracken sowie intime und private Korrespondenz zu speichern, eine besondere Bedeutung.

Auch im präventivpolizeilichen Bereich sind die Landesgesetzgeber zwischenzeitlich tätig geworden. Nachdem das Bundesverfassungsgericht in seiner Entscheidung zum „Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKAG)“ (Bundesverfassungsgericht, Urteil vom 20. April 2016 – 1 BvR 966/09), die Schranken bei verdeckten Ermittlungsmaßnahmen aufgezeigt hatte, hat sich ein Reigen an Novellierungen durch das Land gezogen. Während im strafprozessualen Rahmen diese neuen Ermächtigungen einer erheblichen Kritik unterzogen wurden und verfassungsrechtliche Bedenken geäußert wurden, könnten die damit verbundenen Grundrechtseingriffe zur Gefahrenabwehr dieser höchstrangigen Rechtsgüter gerechtfertigt werden (Rogan 2018). All diesen Maßnahmen ist aber gemein, dass sie sich im Wesentlichen um das Phänomen des Cybercrime im engeren Sinne kümmern. Für die hier zur Rede stehenden Deliktsfelder der kommunikationsbasierten Kriminalität können Online-Durchsuchung und Quellen-TKÜ nicht angewendet werden. Gerade mit der infrage stehenden Eingriffstiefe solcher Maßnahmen kann daher auf diese nicht zurückgegriffen werden, wenn es um kommunikationsbasierte Straftaten im Netz geht. Hier helfen neue Befugnisse offensichtlich nicht weiter.

4 Abwesenheit staatlicher Präsenz im Netz? Das Broken Web

Rüdiger hat das Erklärungsmodell des Broken Web entwickelt (Rüdiger 2018). Diese Theorie vergleicht die Annahmen der Broken Window Theorie von Wilson und Kelling in die digitale Welt. Die klassische Theorie verwendet das Bild eines eingeschlagenen Fensters, indem dargelegt wird, dass dieser erste sichtbare Normverstoß – wenn hierauf nicht zeitnah durch Wiederherstellung des ursprünglichen Zustandes reagiert wird – weitere Verstöße in Gestalt weiterer eingeschlagener Fenster nach sich ziehen werden. Das zerbrochene Fenster signalisiert mithin dem Außenstehenden die sichtbare Abwesenheit einer regulierenden Ordnungsmacht. Es ist das Sinnbild einer Einladung in einen rechtsfreien Raum. Trotz aller Kritik an diesem Erklärungsansatz in der kriminologischen Literatur (Rüdiger 2018) könne es wegen Überschneidungen in den Grundzügen auf den digitalen Raum Anwendung finden.

Dies ist nachvollziehbar, wenn man die Grundthese der Broken Window Theorie zugrunde legt: Ein Raum, der keiner Normkontrolle unterliegt, generiert weitere Normverstöße unterschiedlichster Art. Damit ist dieser Theorie die Interaktion als Wesenselement zu eigen. Der Raum selbst sendet eine Botschaft – ein Signal – an diejenigen aus, die sich in ihm aufhalten oder diesen betreten. Dieses Signal lautet: „Hier interessieren eingeschlagene Fenster niemanden!“ – „Es kümmert sich keiner um die Wiederherstellung eines ordentlichen Zustandes!“. Dabei kann der Begriff „Raum“ jede für sich abgeschlossene Einheit beschreiben. Es kommt nicht auf eine lokalisierbare, tatsächlich vorhandene Räumlichkeit an. Nach Rüdiger erfüllen auch digitale Räume diese Eigenschaften, gleich ob es sich um Chaträume, Postings in sozialen Medien, Online-Spiele oder Kommentarspalten handelt. Entscheidend ist nur die Botschaft, die von dem jeweiligen Medium an den Nutzer ausgeht. Wenn also die Nutzer bei Betreten eines solchen digitalen Raumes Normüberschreitungen wahrnehmen können, dürfen sie davon ausgehen, dass es keine wirksame Kontrolle gibt. Diese wahrnehmbaren Normüberschreitungen basieren ihrerseits auf dem zweiten für diese Theorie notwendigen Element: Der Chance auf Kommunikation, also der Interaktion zwischen den verschiedenen Nutzern dieses Raumes. Solches findet hier mit den in den jeweiligen Räumen verschiedenen Interaktionsmöglichkeiten statt. Folglich sind die hier zu beschreibenden Normverletzungen im Wesentlichen solche, die ihren Kern in der Kommunikation zwischen den verschiedenen Nutzern haben.

Marx hat Verrohungstendenzen im Internet ausgemacht (Marx 2019). Sie benennt zahlreiche Quellen, die einen Zusammenhang zwischen kommunikationsbasierter Normverletzung und dem Internet nahelegen. Unter Verweis auf den in der Online-Forschung etablierten Enthemmungseffekt beschreibt sie zutreffend Situationen, die als Beleg für die Richtigkeit der Broken Web Theorie herhalten können.

Hierbei ist noch ein weiteres zu beachten: Während die analoge Kommunikation vielschichtig angelegt ist, also Körpersprache, Tonfall, Lautstärke und ähnliches eine wichtige Rolle im Kommunikationsprozess spielen, findet die digitale Kommunikation in der Regel nur schriftlich statt, wenn man von Sprachnachrichten als Kommunikationsmittel einmal absieht. Die hier auch zu beobachtenden Interaktionen durch die Avatare in Online-Games geht zwar über die rein schriftliche Kommunikation hinaus, erreicht bei Weitem aber nicht die Ausdruckstiefe und Vielschichtigkeit wie zwischenmenschliche Interaktion. Diese online zu beobachtenden schriftlichen Äußerungen entbehren die übrigen Merkmale in der analogen Welt. Vermutlich auch aus diesem Defizit sind Emojis in der digitalen Welt so wichtig geworden. Hinzu kommt aber ein weiterer wichtiger Punkt: Diese schriftlichen Äußerungen können nicht mit dem Briefeschreiben in der analogen Welt gleichgesetzt werden. Während auch hier keine Möglichkeit besteht, die nonverbale Kommunikation zu übermitteln, ist im Digitalen eine sprachliche Beschränkung zu beobachten. Gedanken werden in der Regel wenig ausgeführt, sondern präsentiert. Die Begrenzung der Zeichenzahl (etwa in Twitter) verlangt nach Vereinfachung. Differenzierte Auseinandersetzungen mit einem Thema sind daher auf den diversen Plattformen eher selten zu finden. Diese Rahmenbedingungen begünstigen im Zweifelsfalle eher einen Normverstoß, als dass sie ihn verhindern können.

Die fehlende legitimierte Ordnungsmacht im Netz oder zumindest die Erfahrung, dass Fehlverhalten in der Regel nicht hinreichend sanktioniert wird, begünstigt daher die Enthemmung und Verrohung im kommunikativen Miteinander.

5 Die Geschichte von den Selbstregulierungskräften im Netz

Die auch vertretene Meinung „Soziale Medien […] verlangen ein neues Recht der Netzwerke, welches durch Selbstorganisation in den Netzwerken selbst generiert werden muss“ (Ladeur 2018, S. 185) beschränkt den staatlichen Einfluss und die Kontrolle dagegen auf Verfahrensregeln. Die staatlichen Sanktionsmöglichkeiten würden dadurch aber auf die Verstöße gegen diese Verfahrensregeln beschränkt

werden müssen. Sowohl die Opfer wie auch die Täter solcher kommunikationsbasierender Normverletzung wären aber dem direkten Schutz des Staates entzogen. In diesem Falle wäre auch die Legitimation eines solchen Rechtes noch nicht geklärt.

Die DIVSI-Entscheiderstudie 2013 befasste sich mit der Haltung von Vertretern aus Wirtschaft, Politik, Öffentlichem Dienst, Zivilgesellschaft, Medien sowie Wissenschaft und Forschung. Dieser Personengruppe wurden die Eigenschaften einer Meinungsführerschaft und von Führungskräften zugeschrieben. Die Studie erfragte die dort sogenannten „digitalen Lebenswelten in der deutschen Entscheider-Landschaft" und beschrieb die grundlegenden Haltungen der befragten Entscheider gegenüber dem Internet. Erfragt wurden auch deren Anforderungen bezüglich Vertrauen in und Sicherheit im Netz (DIVSI Entscheider-Studie 2013). Im Vorwort hierzu schrieb Herzog:

> „Ich selbst muss wohl – meinem Lebenslauf entsprechend – von den sich aufdrängenden verfassungsrechtlichen Fragen ausgehen. Nicht, weil ich der Meinung wäre, dass ausgerechnet Rechtsfragen im Zentrum unserer Problematik lägen. Aber meine Erfahrungen haben mich gelehrt, dass man den ethischen Fragen, die sich uns heute stellen, sehr gut beikommt, wenn man den Blick immer wieder vergleichend über die verfassungsrechtliche Nachbarschaft schweifen lässt. Ich meine, dass in unserem digitalen Zeitalter Fragen der Ethik einen zunehmend größer werdenden Raum einnehmen. Fragen, an die zu Beginn des Internet-Zeitalters wohl kaum jemand gedacht hat." (Herzog 2013, S. 5)

Bemerkenswert ist hierbei, dass er hier zwar die sich *„aufdrängenden verfassungsrechtlichen Fragen"* anspricht, gleichzeitig aber betont, dass es nicht primär die Rechtsfragen wären, die zu beantworten wären, sondern die der Ethik – auch wenn er seine Antworten hierauf doch verfassungsrechtlich fundieren will. Kritisch geht Herzog mit einem Befund der Studie ins Gericht, wenn er schreibt:

> „Die Digital Souveränen unter den Entscheidern, also die nachwachsende Elite unseres Landes, hat im Vergleich zu anderen Teilnehmern der Studie das geringste Vertrauen in das politische System, ja sogar in unseren Rechtsstaat selbst. Hier könnten Entwicklungen zu einem Abrücken vom Rechtsstaat und vom Staat gegebenen Garantien im Gange sein." (Herzog 2013, S. 7)

Diese von Herzog angesprochenen „Digital Souveränen" bilden ein Cluster in der Untersuchung. Sie werden als die digitale Avantgarde beschrieben, die Individualismus und Unabhängigkeit als Ausgangspunkte ihres Denkens und Handelns sieht. Sie sind überwiegend männlichen Geschlechts und Anfang 40 und vorwiegend leitende Angestellte. Die wesentlichen Ergebnisse der Studie

sehen folgendermaßen aus: Mehr als die Hälfte dieser Gruppe sieht das Internet insgesamt als freies Medium an, welches unter keinen Umständen reglementiert werden sollte. Für diese Menschen ist demnach längst Realität, dass man das Netz ohnehin nicht kontrollieren kann. Es wird die These vertreten, es handele sich um einen Irrglauben, in globalen Kontexten nationale Grenzen und Verbote einziehen zu können (DIVSI Entscheider-Studie 2013).

Entsprechend sehen sie auch die Rolle des Staates als äußerst begrenzt. An rechtliche Rahmenregelungen und Gesetze als Basis für Freiheit im Netz glauben sie deutlich weniger als die anderen Entscheider. Der Staat ist aus ihrer Sicht nicht nur hilflos, sondern sogar ein Risiko, wenn sie eine Überregulierung durch staatliche Kontrolle als Bedrohung sehen. Zwar sehen auch Digital Souveräne Risiken im Internet, hier wird die Gefahr allerdings in dem Handeln von Hackern gesehen. Große globale Internet-Dienstleister oder auch unbedachte Nutzer werden weniger als Bedrohung wahrgenommen als in der Gesamtheit der Entscheider. Auf der anderen Seite schreiben sie den staatlichen Sicherheitsbehörden mehr Risikopotenzial zu und haben ein deutlich geringeres Vertrauen in das deutsche Rechtssystem oder politische Entscheider (DIVSI Entscheider-Studie 2013).

Auch wenn diese Studie zwischenzeitlich in die Jahre gekommen ist, bleiben die hier genannten Grundeinstellungen doch bemerkenswert. Es handelt sich um den digitalen Nachhall der Globalisierung. Diese Haltung ist geprägt von einem Vertrauen in die Selbstregulierungskräfte einerseits und einem damit einhergehenden Misstrauen in staatliche Ordnungsmacht andererseits. Die hierin lauernden Gefahren hat Herzog benannt: Es ist ein Abrücken vom Rechtsstaat und damit einhergehend auch die Ablehnung staatlicher Garantien. Wenn im Vordergrund aber letztlich eigene Erfahrung, Meinungen von Experten und Bildung stehen und der Wissens- und Informationsaustausch über Netzwerke im Vordergrund stehen, dann können sich hieraus Legitimationsprobleme staatlichen Eingreifens ergeben. Die in der Studie genannten Haltungen geben ein kulturelles Phänomen wieder, das nicht nur kurzfristige Meinungen wiedergibt und tagesaktuellen Schwankungen unterworfen ist. Die Idee der Selbstregulierung ist aber auch ansonsten dem deutschen Rechtssystem nicht fremd.

Rechtliche Grundlage für die Selbstregulierung kann in der Vereinigungsfreiheit gesehen werden, wie sie in Art. 9 Abs. 1 GG gewährleistet wird. Historisch betrachtet rührt diese Freiheit aus dem 19. Jahrhundert her, als sich als Folge der Aufklärung die Idee der freien Assoziation freier Individuen durchsetzte, die in der Öffentlichkeit wirksam wird. Das Bundesverfassungsgericht betonte sowohl das „Prinzip freier sozialer Gruppenbildung“ (Bundesverfassungsgericht, Beschluss vom 18. Dezember 1974 – 1 BvR 430/65 und 1 BvR 259/66) als auch

das „Prinzip freier Assoziation und Selbstbestimmung“ (Bundesverfassungsgericht, Urteil vom 1. März 1979 – 1 BvR 532, 533/77, 419/78 und BvL 21/78). Damit einher geht das „prinzipielle Recht zur autonomen gesellschaftlichen Selbstorganisation“ (Scholz 2009, Art. 9 RdNr. 11). Die Vereinigungsfreiheit folgt damit dem Prinzip einer freien sozialen Gruppenbildung.

Die Vereinigungsfreiheit erweist sich schon aufgrund der Tatsache, dass Menschen soziale Kontakte suchen und pflegen, als elementarer Aspekt der Persönlichkeitsentfaltung. Darüber hinaus sind Meinungs- und Willensbildungsprozesse in einem freiheitlich-pluralistisch verfassten Gemeinwesen auf die Bündelung und gleichgerichteter Interessen angewiesen. Diese sind nur durch die Assoziation der Interessierten erreichbar. Damit ergibt sich auch eine für die Gestaltung des sozialen Miteinanders besondere Bedeutung (Stern und Becker 2019, Artikel 9 GG RdNr. 11). Zum Gewährleistungstatbestand von Art. 9 Abs. 1 gehört auch die vereinigungsspezifische Vertragsfreiheit. Art. 9 Abs. 1 GG erfasst damit auch das Recht rechtserhebliche Vereinbarungen zu schließen. Dies bezieht sich sowohl auf die Selbstorganisation als auf die vertragliche Ausgestaltung von Beziehungen mit anderen Rechtssubjekten (Stern und Becker 2019, Artikel 9 GG RdNr. 11).

Unter dem Terminus der regulierten Selbstregulierung wird die Rechtsetzung privater Akteure zur Konkretisierung hoheitlicher Vorgaben verstanden. So wird beispielsweise die Arbeit privater Normierungsgremien wie das Deutsche Institut für Normung (DIN), der Verein Deutscher Ingenieure e. V. (VDI) oder der Verband Deutscher Elektrotechniker (VDE) genannt (Stockhaus 2015, S. 83). § 14 Jugendschutzgesetz (JuSchG) regelt die Kennzeichnung von Filmen und Film- und Spielprogrammen. In Absatz 2 dieser Vorschrift wird diese den obersten Landesbehörden oder einer Organisation der freiwilligen Selbstkontrolle übertragen. Das Verfahren wird in Abs. 6 näher ausgeführt. Die Freiwillige Selbstkontrolle der Filmwirtschaft GmbH (FSK) wird von der Spitzenorganisation der Filmwirtschaft (SPIO) getragen.

In Deutschland besteht, neben Österreich, Frankreich, Spanien und Italien, ein weit gefächertes System von Wirtschafts- und Berufskammern. Als Wirtschaftskammern werden die Industrie- und Handelskammern, die Handwerkskammern und die Landwirtschaftskammern bezeichnet, während die Berufskammern die sogenannten freien Berufe umfassen. Die Besonderheit dieser Institutionen ist, dass sie als Körperschaften des öffentlichen Rechts verfasst sind. Ein wesentlicher Unterschied zu den Vereinen besteht in der Pflichtmitgliedschaft der Berufsträger. Auf dieser Konstruktion gründet sich ein Selbstverwaltungsrecht. Die staatlichen Stellen üben nur eine Rechtsaufsicht aus. Die Kammern verfügen deshalb über eine große Selbstständigkeit gegenüber der unmittelbaren

Staatsverwaltung bei der Wahrnehmung der ihnen zugewiesenen Aufgaben (Kluth 2008). Die Idee hinter dem Kammerwesen resultiert aus der liberalen Gedankenwelt des 19. Jahrhunderts als einer sogenannten Betroffenen-Selbstverwaltung (Kluth 2008).

Als verfassungsrechtliche Grundlage für die Selbstregulierung werden die allgemeine Handlungsfreiheit aus Art. 2 Abs. 1 GG und die Wissenschaftsfreiheit des Art. 5 Abs. 3 GG genannt. Daneben gewährleisten die Wirtschaftsgrundrechte aus den Art. 9, 12 und 14 GG eine staatliche Verpflichtung zur Gewährung von Selbstregulierungsmechanismen (Reip 2002). Selbstregulierung kann daher in wirtschaftlicher Hinsicht auch als eine Form der Entstaatlichung gesehen werden. Hierunter versteht man zunächst die Rückführung des Staates auf seine Kernaufgaben. Im Konkreten beschreibt dieses auch einen Prozess, in dem die staatliche Aufgabenwahrnehmung zusehends mit dem gesellschaftlichen Bereich bei der Aufgabenerfüllung verzahnt wird (Ewald 2005). Problematisch wird in diesem Zusammenhang die Verschiebung der Grundrechtspositionen der Betroffenen zu betrachten sein. Im Verhältnis Bürger-Staat ist der Staat schon über Art. 1 Abs. 3 GG unmittelbar und durch die Gesetzesbindung in Art. 20 Abs. 3 GG mittelbar an die Grundrechte gebunden; der Bürger hat seine Teilhabe- und Abwehrrechte aus seinen Grundrechten gegenüber den staatlichen Akteuren. Sobald nun aber das Schwergewicht auf Selbstregulierungskräfte gelegt wird, ist zu beachten, dass diese ihrerseits eben nicht grundrechtsgebunden sind. Vielmehr kommen diesen eigenständige Grundrechtspositionen zugute. Die Durchsetzung grundrechtlicher Abwehr- oder Leistungsansprüche durch betroffene Dritte kann daher nur bei Annahme einer mittelbaren Drittwirkung der Grundrechte in einer Abwägung der jeweiligen geschützten Positionen stattfinden (Reip 2002).

Das Vertrauen auf die Kräfte der Selbstregulierung haben in Deutschland auch in der analogen Welt eine lange Tradition und gründen sich im Wesentlichen auf das liberale Gedankengut des 19. Jahrhunderts. Aus diesen Gründen ist es auch naheliegend, dass, weil die Digitalisierung der Lebensumwelt mit der Globalisierung des ausgehenden 20. Jahrhunderts einhergeht, diese Ideen eine quasi-vertraute Umgebung vorgefunden haben. Die Globalisierung hat nach Auffassung von marktwirtschaftlich-ökonomischen Denkern durch das Vertrauen auf Marktkräfte bei weitestgehendem Freihandel und Kommunikativer Freiheiten erst den damit einhergehenden Wohlstand möglich gemacht. Der Wettbewerb und nicht staatliche Eingriffe sind die Motoren dieser Entwicklung (Enquete-Kommission 2003). Diese gelebte und erlebte Kultur ist aber durchaus auch als eine Ursache dafür anzusehen, dass das Internet allen Beteuerungen zum Trotz in weiten Räumen als rechtsfreier Raum erlebt wird.

6 Archaische und präzivile Ordnungsmuster?

Das alleinige Vertrauen auf die Selbstregulierungskräfte im Netz verkennt letztlich die unterschiedlichen Interessen, die die Benutzerinnen und Benutzer auf der einen Seite und die Internetkonzerne auf der anderen Seite antreiben. Im Gegensatz zur analogen Welt geht es eben nicht primär um den Austausch von Informationen, Waren und Dienstleistungen. Darüber hinaus wird das eigentliche Geschäftsmodell mit dem Begriff „Big Data“ selbst nur unzureichend beschrieben: Es geht darum, wer unter welchen Umständen wie Daten erheben, verwalten, speichern, verarbeiten und dann zu weiteren Geschäftszwecken gewinnbringend nutzen kann. Ein Vertrauen auf Selbstregulierung indes kann diese Komplexität nicht abbilden. Wegen der Asymmetrie der wechselseitigen Interessen von Nutzern, die zum Beispiel einkaufen, verreisen, sich informieren wollen oder Erfahrungen oder einfach nur Privates austauschen oder letztlich vielleicht auch nur dem Phänomen des „Cybernarzissmus“ frönen wollen, und den Plattformbetreibern, die aufgrund der jeweiligen Geschäftsmodelle mehr an der hinter den Einzelinteressen der Nutzer stehenden Person und deren Vernetzungen als an dem jeweiligen Interesse interessiert sind, kann mangels hinreichender Schnittmengen ein Interessensausgleich auf dieser Ebene kaum oder gar nicht gelingen.

Diese archaischen Ordnungsmuster kann man auch in den Selbstregulierungsversuchen moderierter Foren erkennen, in denen mitunter Ausschlüsse und Sperren einerseits oder Beleidigungen, offenes Cybermobbing oder sexuelle Belästigungen andererseits zu beobachten sind (s. a. Kap. „Hate Speech in der Computerspielkultur“). Letztlich verbleibt der Streit darüber, ob eine solche ausgesprochene Maßnahme rechtens war oder nicht, bei der zivilrechtlichen Auseinandersetzung über das sogenannte digitale Hausrecht. Die Dunkelziffer derer, die sich einer solchen Maßnahme fügen, ohne diese rechtlich überprüfen zu lassen, dürfte hoch sein. Daher sind die Grundlagen der Rechtsprechung zum digitalen Hausrecht, soweit es nicht um die Fragen nach Nutzungsregeln geht, auch in Verfahren gelegt worden, die Urheberrechtsverletzungen beispielsweise auf YouTube oder von Computerspielen zum Inhalt hatten.

Den Betreibern von Internetplattformen steht ein sogenanntes digitales Hausrecht grundsätzlich zu, wie aus einer Vielzahl von zwischenzeitlich ergangenen Urteilen zu entnehmen ist (Elsaß et al. 2017, S. 238, siehe auch z. B. Oberlandesgericht Dresden Beschluss vom 8. August 2018, Az.: 4 W 577/18 mwN., Oberlandesgericht Stuttgart Beschluss vom 6. September 2018, Az.: 4 W 63/18). Im Kern geht es darum, dass diese Plattformen es den Nutzern erlauben, Inhalte

einzustellen und so den anderen Nutzern zugänglich zu machen. Dabei wollen die Betreiber aber sicherstellen, dass sie letztlich darüber entscheiden können, was sie an Veröffentlichungen zu dulden bereit sind. Die Rechtsgrundlage dieses Hausrechts wird unterschiedlich gesehen. Die Verletzung von Nutzungsbedingungen ist auf vertragsrechtlicher Grundlage zu prüfen. Das OLG Dresden hat hierzu ausgeführt, dass Nutzungsbedingungen des Anbieters eines sozialen Netzwerkes eben keine bloßen Leistungsbeschreibungen seien. Diese seien vielmehr als kontrollfähige Allgemeine Geschäftsbedingungen (AGB) zu qualifizieren (OLG Dresden Beschluss vom 8. August 2018, Az.: 4 W 577/18). Daneben kann es auch gesetzliche Gründe für die Herleitung dieses Hausrechts selbst geben. Zu nennen ist hier an erster Stelle die sogenannte Störerhaftung.

Bei Rechtsverletzungen auf Plattformen haben die Geschädigten die Möglichkeit, eine Beseitigung dieser Inhalte im Rahmen des „Notice-and-Takedown"-Verfahrens zu verlangen (Stang 2017). Darüber hinaus kann auch die Einhaltung einer aus der Störerhaftung abgeleiteten, in die Zukunft gerichteten Pflicht zur Verhinderung gleichartiger Rechtsverletzungen verlangt werden (Bundesgerichtshof Urteil vom 12. Juli 2012, Az.: I ZR 18/11 „Alone in the Dark"). Problematisch bei diesem Notice-and-Takedown-Verfahren ist allerdings, dass eine Rechtsverletzung erst dann Folgen zeitigt, wenn der Geschädigte seinerseits sich an den Seitenbetreiber gewandt hat und diesen zur Beseitigung der Verletzung aufgefordert hatte. Die Betreiber agieren auf dieser Basis daher nicht deswegen, weil Rechte Dritter verletzt wurden und sie diese schützen, sondern weil sie sich ansonsten entsprechender Unterlassungs- und Beseitigungsansprüchen ausgesetzt sehen könnten. So führte das OLG Brandenburg aus:

> „Auch im Internet kann der Eigentümer nach §§ 903 Satz 1, 1004 Abs. 1 Satz 1 BGB analog jemanden von der Nutzung seiner Hardware durch das Speichern von Inhalten ausschließen (LG München I, CR 2007, 264 [LG München I 25.10.2006 – 30 O 11973/05]). Das Hausrecht ist Ausdruck der durch Art. 2 Abs. 1 GG gewährleisteten Privatautonomie, die die Selbstbestimmung des Einzelnen im Rechtsleben schützt (vgl. BVerfG, NJW 1994, 36, 38 [BVerfG 19.10.1993 – 1 BvR 567/89] m.w.N.), und hat zur Folge, dass rechtlich erhebliche Willensentscheidungen zu der Frage, ob und in welchem Umfang einem Dritten der Zugang zu einer bestimmten Örtlichkeit – bzw. hier der von der Antragsgegnerin betriebenen Internetplattform – gestattet wird, keiner Rechtfertigung bedürfen (vgl. BGH, NJW 2012, 1725 [BGH 09.03.2012 – V ZR 115/11] Rn. 8)." (Oberlandesgericht Brandenburg Beschluss vom 27. Juli 2018, Az.: 1 W 28/18)

Nicht zuletzt aus den oben genannten Gründen haben sich in der Vergangenheit immer wieder Private daran gemacht, das Vakuum der anscheinenden oder

zumindest gefühlten Gesetzlosigkeit auszufüllen. Die subjektive Wahrnehmung des Internets als rechtsfreier Raum oder – oftmals im Zusammenhang mit der Ausübung eines virtuellen Hausrechts, die als Willkürakt empfunden wird – zumindest eines rechtsstaatsfreien Raumes ruft immer wieder Aktivisten auf den Plan. Als prominenteste Vertreter dürfte hier die Gruppe „Anonymous“ gelten, die immer wieder mit spektakulären Aktionen für Schlagzeilen gesorgt hat. Erklärte Ziele dieses Kollektivs sind das Eintreten für die Redefreiheit, die Unabhängigkeit des Internets und gegen die Beschränkungen des Urheberrechts. Adressaten dieser Aktionen waren Personen, Organisationen, Behörden und Unternehmen, die nach Meinung der Gruppe den Zielen der Gruppe zuwider handelten. Damit handelten sie sich – je nach Standpunkt – schon frühzeitig den Ruf eines digitalen Robin Hood oder einer Online-Terrorgruppe ein (Robertz und Rüdiger 2012). Hieraus wird aber ersichtlich, dass diese Muster wenig geeignet sind, nachhaltig Straftaten zu verhüten oder effektiv an der Aufklärung mitzuwirken.

7 Das Gewaltmonopol des Staates als Zivilisationsfaktor

Max Weber definierte den Staat als einen politischen Anstaltsbetrieb, wenn und insoweit sein Verwaltungsstab erfolgreich das Monopol legitimen physischen Zwanges für die Durchführung der Ordnungen in Anspruch nimmt (Weber 1922, Erster Teil I, § 17). Darunter verstehen wir das staatliche Gewaltmonopol. Rechtsnormen sichern demnach ein geordnetes und friedliches Zusammenleben, der Staat mit seiner Exekutive sorgt für die verlässliche Durchsetzung.

Diese zivilisatorische Leistung ist schon in frühester Zeit erkannt worden: In der germanischen Zeit oblagen viele Aufgaben, insbesondere die der Selbstverwaltung, den Sippenverbänden. Allerdings durchschnitt die sogenannte Friedlosigkeit – die Folge eines Verbrechens gegen höherrangige Rechtsgüter oder bei Taten ehrloser Gesinnung – das Sippenband. Die staatliche Organisation wahrte damit ihre Souveränität gegenüber der Sippe. Sie ist damit also nicht aus dem Familienverband hervorgegangen, sondern entwickelte sich aus dem Kampfe gegen diese. Dies konnte aber nur gelingen, indem darin ein rechtsstaatliches Moment, nämlich die Garantie der Achtung der Rechte, sich entwickeln konnte (Mitteis 1992). Dadurch konnte die zerstörerische Kraft der Rache abgefedert werden. Die Rache zielte auf Vergeltung und Vernichtung des Gegners. Dem konnte die – freilich über Jahrhunderte sich hinziehende – Entwicklung eines staatlichen Gewaltmonopols entgegenwirken. Gewalt, beziehungsweise das

Monopol ihrer Ausübung, meint hier also stets die legale Gewalt im Sinn der *potestas,* das Verfügen-dürfen über andere (Grimm 2002).

Damit das Recht seine Befriedungsfunktion auch tatsächlich ausüben kann, ist es unerlässlich, dass dort, wo andere Motivationen des Normgehorsams versagen, organisatorische Vorsorgen dafür getroffen sind, dass diese Durchsetzung auch zwangsweise getroffen werden kann (Zippelius 1980). Das Gewaltmonopol des Staates dient letztlich dazu, die Anwendung und Androhung privater Gewalt, also der *violencia* zu unterbinden. Dadurch sollen die Rechtsgüter der Bürger vor gegenseitigen Übergriffen geschützt werden. Letztlich wird dadurch angestrebt, durch Androhung der legitimen potestas einen Gesamtzustand der Sicherheit herzustellen (Isensee 2006 § 71 Rn. 76).

Als das Programm Innere Sicherheit 2008/2009 fortgeschrieben wurde, betonten die Innenminister von Bund und Ländern in einem eigenen Abschnitt, dass die Gewährleistung der Inneren Sicherheit eine staatliche Aufgabe sei. Ein Rückzug des Staates aus diesem Kernbereich hoheitlichen Handelns komme daher nicht in Betracht. Weil das Grundgesetz dem Staat das Gewaltmonopol zuweise, könne dieses auch nicht zur Disposition stehen (zit nach: Walter 2012, S. 211). Dieser programmatische Ansatz ist daher, wenn es um die innere Sicherheit in der digitalen Welt geht, zu justieren.

Es ist unerlässlich, dass das Netz nicht seinen Selbstregulierungskräften überlassen wird. Die Vision vom freien Netz als Ort der Selbstregulierung greift daher zu kurz. Es bedarf einer legitimen Begrenzung der allgemeinen Handlungsfreiheiten auch in der digitalen Umgebung. Die Frage nach der Möglichkeit, solches zu erreichen, ist zum einen verbunden mit der Chance, Macht im Sinne der potestas ausüben zu können, zum anderen aber auch mit der realen Möglichkeit der Durchsetzung und gegebenenfalls Sanktionierung. Dies erfordert aber eine Herrschaft im Sinne der Verbindung von Machtausübung und ordnender Durchsetzung. Die Legitimation einer solchen Ordnungsmacht kann auf verschiedene Art und Weise erfolgen.

Max Weber definiert den Begriff „Herrschaft“ als die Chance, für spezifische (oder: für alle) Befehle bei einer angebbaren Gruppe von Menschen Gehorsam zu finden. Dieser geht also über die Begrifflichkeiten von „Macht“ und „Einfluss“ auf andere Menschen hinaus. Herrschaft oder das Synonym der Autorität kann auf den verschiedensten Motiven beruhen, es sind nicht nur zweckrationale Erwägungen in Betracht zu ziehen (Weber 1922, Erster Teil, III.1. § 1). Hierbei unterscheidet er drei grundsätzliche Typen legitimer Herrschaft nach rationalem, traditionalem oder charismatischem Charakter. Hier kommt es nur auf den ersten Typus an: Die legale Herrschaft beruht auf dem Glauben an die Legalität

gesetzter Ordnungen und des Anweisungsrechts der durch sie zur Ausübung der Herrschaft Berufenen (Weber 1922, Erster Teil, III.1. § 2). Nur das staatliche Gewaltmonopol kann diese Voraussetzungen erfüllen, die Durchsetzung dieser zivilisatorischen Befriedungsfunktion zu garantieren. Dazu bedarf es aber auch sichtbarer staatlicher Präsenz im digitalen Raum.

8 Das NetzDG – Privatisierung öffentlicher Aufgaben?

Das Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG) richtet sich gegen rechtswidrige Inhalte auf Internetplattformen. Es legt den Betreibern Compliance-Pflichten auf, die bei Zuwiderhandlungen Geldbußen bis zu 50 Mio. EUR nach sich ziehen können. Die Zielrichtung ist dabei, dass „strafbare Falschnachrichten“ und „Hasskriminalität“ der Boden entzogen werden soll. Dies soll dadurch erreicht werden, dass die Betreiber im Umgang mit Beschwerden die Löschung oder Sperrung binnen kurzer Fristen gewährleisten sollen. Das NetzDG selbst verschafft jedoch den Betroffenen keine eigenen zivilrechtlichen Anspruchsgrundlagen zur Löschung von Inhalten. Vielmehr wird nur ein Verfahren für die Löschung strafbarer Äußerungen vorgegeben (Schöddert 2018).

Hierbei stellt sich zunächst die Frage nach einer Definition der rechtswidrigen Inhalte. § 1 Abs. 3 NetzDG gibt hier die Legaldefinition vor: Rechtswidrige Inhalte sind Inhalte im Sinne des Absatzes 1, die den Tatbestand der §§ 86, 86a, 89a, 91, 100a, 111, 126, 129 bis 129b, 130, 131, 140, 166, 184b in Verbindung mit 184d, 185 bis 187, 201a, 241 oder 269 des Strafgesetzbuchs erfüllen und nicht gerechtfertigt sind. Es handelt sich somit um Normen aus den Bereichen des Schutzes des demokratischen Rechtsstaats, der öffentlichen Ordnung, der persönlichen Ehre, der sexuellen Selbstbestimmung, des persönlichen Lebens- und Geheimbereichs sowie der politischen Verdächtigung und der Fälschung beweiserheblicher Daten.

Die objektiven und subjektiven Tatbestandsmerkmale müssen erfüllt sein. Rechtfertigungsgründe dürfen keine vorliegen. Auf die Schuld kommt es demnach nicht an. § 3 Abs. 2, 3 NetzDG regelt dann die Einzelheiten für das Beschwerdemanagementverfahren. Das Gesetz selbst ist in der Literatur einer starken Kritik ausgesetzt worden (Schiff 2018). Neben verfassungs- und europarechtlichen Bedenken, die sich der Frage der Gesetzgebungszuständigkeit oder der hinreichenden Bestimmtheit ebenso widmeten wie der Dienstleistungsfreiheit oder

dem Herkunftslandprinzip (Zusammenfassend: Liesching 2018), waren es immer wieder zwei Aspekte, die in diesem Zusammenhang hier einer näheren Betrachtung bedürfen. Der eine betrifft die Meinungs- und Informationsfreiheit (Art. 5 Abs. 1 S. 1 GG). Der Schutzbereich dieses Grundrechts ist demnach eröffnet, weil das Gesetz auf die Löschung von Meinungen im Internet abstellt. Die konkrete Umsetzung des Anliegens, dass der Staat seinen ihm zukommenden Schutzauftrag durch Regulierung strafrechtlich relevanter Inhalte in sozialen Medien nachkommt, ist im NetzDG wegen der dadurch einhergehenden Gefahr für die Meinungsfreiheit in der Kritik (Engeler 2018).

Problematisch ist hier, dass Fehleinschätzungen des Plattformbetreibers ebenso zuLasten der Nutzer gehen wie eine im Zweifel intransparente Einzelfallprüfung. Guggenberger weist in diesem Zusammenhang darauf hin, dass im Falle unberechtigter Löschungen nicht nur die Urheber der Postings in ihren Grundrechten betroffen wären, sondern darüber hinaus die anderen Nutzer, die wegen der Löschung aus einem Teil ihres Meinungsbildungsprozesses ausgeschlossen sind (Guggenberger 2017). Neben einem befürchteten „Over Blocking“ (Papier 2017) aus Furcht vor den im Gesetz angedrohten Bußgeldern wird auf der Verhältnismäßigkeitsebene der verfassungsrechtlichen Rechtfertigung auch damit argumentiert, dass das Gesetz selbst keinen eigenen legitimen Zweck verfolgen könne. Dies wird damit begründet, dass es sich zwar bei den zu löschenden Inhalten um solche handele, die tatbestandlich und rechtswidrig ein Strafgesetz aus dem Straftatenkatalog des § 1 Abs. 3 NetzDG verletzen; dabei wird aber darauf verwiesen, dass Strafverfolgung und Strafvollstreckung originäre Aufgaben des Staates sind. Der Versuch, die Verfolgung und Sanktionierung von Straftaten quasi zu privatisieren, entspringt auch der oben dargestellten Idee der Selbstregulierung im Netz. Weil es sich hier aber im Ergebnis darum handelt, dass die Rechtdurchsetzung auf Private verlagert wird, werden die Plattformbetreiber zu Quasi-Hilfspolizisten (Guggenberger 2017).

Die mit dem NetzDG verfolgte Idee, die Betreiber der Plattformen für die Durchsetzung rechtmäßiger Zustände einzusetzen, und zwar dergestalt, dass diese eigenständig über Recht und Unrecht gemeldeter Postings innerhalb kürzester Zeit zu entscheiden haben, ist zwar im Sinne einer Selbstregulierung nachvollziehbar. Sie offenbart aber die Schwächen, die die Abwesenheit staatlicher und damit demokratisch legitimierter Gewalt mit sich bringt. Anstelle des Outsourcings von hoheitlichen Aufgaben durch die Einrichtung eines privaten Nebenstrafrechts für Online-Inhalte wäre an Alternativen wie die Optimierung der weiter unten dargestellten zivil- und strafrechtlichen Möglichkeiten und der Stärkung der Präventivarbeit und Sensibilisierung zu denken.

9 Fußball und das Internet – ein Stadionverbot und seine Folgen

Im Beschluss vom 11. April 2018 hatte sich das Bundesverfassungsgericht mit der Ausstrahlungswirkung des allgemeinen Gleichbehandlungsgebots des Art. 3 Abs. 1 GG in das Zivilrecht befasst (Bundesverfassungsgericht, Beschluss vom 11. April 2018, Az.: 1 BvR 3080/09). Schon bald nach Inkrafttreten des Grundgesetzes wurde in der Rechtswissenschaft die Frage diskutiert, ob und inwieweit die Grundrechte in die Privatrechtsordnung „hineinwirken“: die sogenannte Drittwirkung der Grundrechte (Ipsen 1954, S. 111 f.). Dabei wird die „mittelbare Drittwirkung“ des Grundrechts dadurch bewirkt, dass über die ausfüllungsfähigen Generalklauseln des Privatrechts wie z. B. §§ 138, 242, 826 BGB, der Wesensgehalt des Grundrechts in die Rechtsbeziehung zwischen Privaten hineingetragen wird (Bundesverfassungsgericht Urteil v. 23. April 1986, Az.: 2 BvR 487/80; BVerfG vom 11. Juni 1991 Az.: 1 BvR 239/90 – FamRZ 1991, S. 1037). Das Bundesverfassungsgericht hat diese Auffassung dem Grunde nach bereits seit dem Lüth-Urteil geteilt (Bundesverfassungsgericht, Urteil vom 15. Januar 1958 – 1 BvR 400/51 „Lüth“). In der dortigen Entscheidung führte das Gericht aus: Die Grundrechte sind in erster Linie Abwehrrechte des Bürgers gegen den Staat.

In den Grundrechtsbestimmungen des Grundgesetzes verkörpert sich aber auch eine objektive Wertordnung, die als verfassungsrechtliche Grundentscheidung für alle Bereiche des Rechts gilt. Im bürgerlichen Recht entfaltet sich der Rechtsgehalt der Grundrechte mittelbar durch die privatrechtlichen Vorschriften. Er ergreift vor allem Bestimmungen zwingenden Charakters und ist für den Richter besonders realisierbar durch die Generalklauseln (Bundesverfassungsgericht, Urteil vom 15. Januar 1958 – 1 BvR 400/51 „Lüth“). Eine eigentliche Drittwirkung ergibt sich aufgrund der Tatsache, dass der Gesetzgeber bei der Schaffung zivilrechtlicher Normen über Art. 1 Abs. 3 GG an die Grundrechte gebunden ist, daher nur dann, wenn in privatrechtlichen Rechtsverhältnissen Verhaltensweisen geübt werden, die mit den Grundrechten unvereinbar sind. In solchen Fällen muss aber ein besonderes Augenmerk darauf gerichtet werden, dass sich hier Privatrechtssubjekte einander gegenüberstehen, die ihrerseits selbst grundrechtsberechtigt sind. Bei der Frage nach einer mittelbaren Drittwirkung müssen daher deren Sphären gegeneinander abgegrenzt werden (Stern und Becker 2019, C. RdNr. 65).

Dies ist, wenn es um Fragen von Kommunikation im Internet geht, besonders bedeutsam, weil die Grundrechtspositionen der Internetkonzerne mit denen der

Nutzer in Ausgleich gebracht werden müssen. Die Entscheidung zum Stadionverbot weist in ihren Grundzügen aber Parallelen auf, die auch für die hier zu behandelnde Frage von Bedeutung sein können. Im konkreten Fall ging es um die Verfassungsbeschwerde eines mit einem bundesweiten Stadionverbot belegten Fußballanhängers. Dabei hat das Gericht herausgestellt, dass ein solches Verbot am Gleichbehandlungsgebot des Art. 3 Abs. 1 GG zu messen sei. Zur Begründung hierfür hatte das Gericht zunächst herausgestellt, dass sich zwar auch nach den Grundsätzen der mittelbaren Drittwirkung kein objektives Verfassungsprinzip entnehmen lasse, wonach die Rechtsbeziehungen zwischen Privaten von diesen prinzipiell gleichheitsgerecht zu gestalten wären. Mittelbare Drittwirkung entfaltet nach der Auffassung des Bundesverfassungsgerichts der allgemeine Gleichheitssatz aber dann, wenn einzelne Personen mittels des privatrechtlichen Hausrechts von Veranstaltungen ausgeschlossen werden, die von Privaten aufgrund eigener Entscheidung einem großen Publikum ohne Ansehen der Person geöffnet werden und wenn der Ausschluss für die Betroffenen in erheblichem Umfang über die Teilhabe am gesellschaftlichen Leben entscheide (Bundesverfassungsgericht, Beschluss vom 11. April 2018, Az.: 1 BvR 3080/09).

Bereits in der FRAPORT-Entscheidung hatte das Bundesverfassungsgericht ausgeführt:

> „Wenn heute die Kommunikationsfunktion der öffentlichen Straßen, Wege und Plätze zunehmend durch weitere Foren wie Einkaufszentren, Ladenpassagen oder sonstige Begegnungsstätten ergänzt wird, kann die Versammlungsfreiheit für die Verkehrsflächen solcher Einrichtungen nicht ausgenommen werden, soweit eine unmittelbare Grundrechtsbindung besteht oder Private im Wege der mittelbaren Drittwirkung in Anspruch genommen werden können.“ (BVerfG, Urteil vom 22. Februar 2011 – 1 BvR 699/06 „FRAPORT“)

Das OLG München hat dann unter anderem in Bezugnahme auf diese Stadionverbotsentscheidung des Bundesverfassungsgerichts am 24. August 2018 Facebook im Rahmen des Erlasses einer einstweiligen Verfügung untersagt, einen von der Antragstellerin eingestellten Kommentar zu löschen und die Antragstellerin wegen eines erneuten Einstellens dieses Posts zu sperren (Oberlandesgericht München, Beschluss vom 24. August 2018, Az.: 18 W 1294/18).

Zwischenzeitlich hat dieser digitale Marktplatz – die Agora im Cyberraum – auch das Bundesverfassungsgericht erreicht. Hier klagte eine Partei – zunächst erfolglos durch die Instanzen – wegen eines Postings auf Facebook. Während die ordentlichen Gerichte auf die Regelungen aus dem NetzDG, hier insbesondere auch auf die Folgen einer Nichtlöschung verwiesen, sah das Bundesverfassungsgericht dies anders: Unter Verweis auf seine ständige Rechtsprechung zur mittel-

baren Drittwirkung von Grundrechten stellte das Bundesverfassungsgericht heraus, dass zumindest im Verfahren zum einstweiligen Rechtsschutz die absehbaren Nachteile einer Sperrung für die Partei erheblich schwerer wögen, als die Nachteile, die die Social Media-Plattform erleiden müsse, wenn die Sperrung sich im Nachhinein als zulässig herausstellen würde, hier aber bis zur Klärung im Hauptsacheverfahren vorerst aufgehoben werden würde (Bundesverfassungsgericht, Beschluss vom 22. Mai 2019 – 1 BvQ 42/19). Hier hatte das Gericht sich ausdrücklich auf die Entscheidung zum Stadionverbot bezogen.

Werte und Rechte, die offline Geltung beanspruchen, können also auf die virtuellen Realitäten übertragen werden. So sind die Argumente des Bundesverfassungsgerichts in der Stadionverbot-Entscheidung für soziale Plattformen zutreffend. Das strukturelle Verhältnis zwischen den Social Media-Plattformen und dem Benutzer folgt diesem Muster: Es besteht ein erhebliches Ungleichgewicht zwischen beiden Parteien. Eine individuelle Möglichkeit, das Vertragsverhältnis auszugestalten, ist faktisch nicht vorhanden: Die AGB der Betreiber sind gesetzt, die Möglichkeiten, Einstellungen vornehmen zu können, ändert nichts am Grundverhältnis. Social Media-Plattformen haben – legt man die Maßstäbe des Bundesverfassungsgerichts an diese Voraussetzungen an – deshalb eine Stellung als Monopol inne. Zumindest ist ihnen eine strukturelle Überlegenheit zu Eigen. Wer sich vernetzen oder online engagieren will, ist auf wenige Anbieter beschränkt, die die Spielregeln vorgeben.

Darüber hinaus ist aber im Wesentlichen die gesellschaftliche Bedeutung bestimmter Leistungen zu beachten. Die moderne Informationsgesellschaft ist ohne diese nicht mehr zu denken. Daraus folgt aber dann, dass unter Berücksichtigung dieser Rechtsprechung das allgemeine Gleichbehandlungsgebot aus Artikel 3 GG im Verhältnis zwischen den Plattformbetreibern und den Bürgerinnen und Bürgern diese mittelbare Drittwirkung zur Entfaltung gebracht wird (Weinzierl 2018). Daraus folgt nun aber in der Zusammenschau, dass nochmals ein Blick auf die Funktion der Grundrechte lohnt: Diese und ihre Gewährleistungen sollen ein Gegengewicht zu dem Gewaltmonopol des Staates bilden: *„Die Friedenspflicht der Bürger und das Gewaltmonopol des Staates daher sind gleichsam zwei Seiten einer Medaille: Dem Gewaltmonopol des Staates entspricht der Verzicht seiner Bürger auf Selbstjustiz; der Staat übernimmt die Sicherheit seiner Bürger und ahndet sie im Falle der Verletzung“* (Hopfauf in Schmidt und Bleibtreu: Vorbemerkung zu Art. 92 GG 2017).

Daraus folgt aber auch zwingend, dass Private wie die Plattformbetreiber nicht unmittelbar auf die Grundrechte verpflichtbar sind. Eine unmittelbare Grundrechtsbindung der Internetkonzerne würde im Ergebnis nur die Aufgabe des staatlichen Gewaltmonopols gegenüber diesen Mächten bedeuten (Engeler 2018).

Somit lässt sich als daher festhalten, dass es geboten ist, das Gewaltmonopol auch den Digitalkonzernen gegenüber durch eine kluge und angemessene Regulierung effektiv durchzusetzen (Engeler 2018).

10 Klarnamenpflicht und Lösungsmöglichkeiten

Eine besondere Schwierigkeit bei der Verfolgung von Straftaten im Internet stellt der Umstand dar, dass die Täter häufig nicht mit Klarnamen auftreten. Deswegen wird mitunter gefordert, dass eine Klarnamenpflicht eingeführt werden solle. Vergleiche werden hier gerne zur analogen Welt gezogen: Im realen Leben müsse man sich auch mit Haut und Haaren der Debatte stellen. Den Befürwortern geht es um die Debattenkultur: So sollen Soziale Netzwerke, Zeitungen und andere Intermediäre unterstützt und ermutigt werden, eine Klarnamenpflicht einzufordern.

Dabei wird auch darauf verwiesen, dass diese gegebenenfalls angehalten werden sollten, kraft ihrer Privatautonomie also im Rahmen der AGB und Nutzungsbedingungen auf Klarnamen zu bestehen. Die öffentliche und demokratische Diskussionskultur vertrage sich nicht mit Nicknames. Der Gesetzgeber sei aber dann gefordert, wenn es um den Schutz besonderer Interessen, insbesondere von Kindern oder Kranken gehe. Auch sei die Klarnamenpflicht ein geeignetes Mittel, wenn es um Betrug und Abzocke im Internet gehe (Krings: DRiZ 6/2019, S. 214). Auf der Gegenseite wird bemängelt, dass der Generalverdacht im Digitalen mehr und mehr zum Normalzustand werde. Im deutschen Telemediengesetz ist das Recht verankert, Telemedienangebote auch anonym nutzen zu können. Dem § 13 Abs. 6 TMG komme demnach eine zentrale Schutzfunktion für die Nutzer zu. Die Verfolgung von strafbaren Handlungen könne auf anderem Wege besser und zielgerichteter erfolgen (Notz. DRiZ 6/2019, S. 215).

In Österreich war noch vor dem Ende der Regierungskoalition im April des Jahres 2019 ein Gesetz eingebracht worden, um gegen den Hass im Netz vorzugehen. Unter Anspielung auf das aus dem Versammlungsrecht bekannte Verbot, sich bei Demonstrationen zu maskieren, spricht die dortige Regierung von einem „digitalen Vermummungsverbot“ (Gesetzentwurf Österreich). Zur Begründung heißt es, dass eine wirksame Authentifizierung zur Bestätigung der Nutzerdaten dabei unumgänglich sei. Damit soll es unmöglich werden – jedenfalls in Fällen, in denen Straftaten begangen werden – sich in der Anonymität des Internets verstecken zu können (134/ME XXVI. GP – Ministerialentwurf, Erläuterungen, S. 1). Auch in Deutschland wird unter Bezugnahme auf die österreichische Initiative verstärkt eine Klarnamenpflicht gefordert. Forciert wurde diese Debatte durch „Shit-

storms“ gegen Politikerinnen und Politiker oder Personen des öffentlichen Lebens (Amann et al. 2019). Sascha Lobo schrieb dazu auf Spiegel Online: *„Anonymität im Netz bedeutet in allererster Linie Schutz, und zwar gerade für Menschen, die sich ansonsten nicht nur im Internet, sondern auch in der Kohlenstoffwelt angreifbar machen würden“* (Lobo 2019).

Hier wird ein Kernelement der digitalen Arbeit sichtbar: Es geht nicht nur um die Verfolgung und Verfolgbarkeit von Straftaten und damit einhergehend um die leichtere Identifizierung von Tätern, sondern es geht auch und gerade in erster Linie um Rechtsgüterschutz. Diesen Rechtsgüterschutz sollen aber nicht nur die (potenziellen) Täter in Anspruch nehmen können, sondern alle Nutzerinnen und Nutzer. Hier wird der Kernbereich des Rechts auf informationelle Selbstbestimmung aller berührt. Die angesprochene Schutzbedürftigkeit verlangt nach staatlichen Schutzpflichten.

Einen Ausweg aus diesem Dilemma hat nun Buermeyer in die Debatte eingebracht. Er nennt seinen Vorschlag ein „digitales Gewaltschutzgesetz“ (Buermeyer 2019). Das zum 1. Januar 2002 in Kraft getretene Gesetz zum zivilrechtlichen Schutz vor Gewalttaten und Nachstellungen – Gewaltschutzgesetz – vom 11. Dezember 2001 dient dem präventiven zivilrechtlichen Schutz derjenigen Personen, die Opfer von Gewalttaten, Bedrohungen oder Nachstellungen geworden sind. Über den sozialen Nahbereich hinaus bietet das Gesetz aber auch Opfern von Belästigungen wie dem so genannten „Stalking“ Schutz (§ 1 Abs. 2 Satz 1 Nr. 2b; Kaßing und Weinreich 2018 RdNr. 373). Dies wird dadurch erreicht, dass ein Katalog an zu missbilligenden Verhaltensweisen gerichtliche Schutzmaßnahmen auslösen kann: Das Gesetz folgt der Konzeption, dass durch die Schaffung von Distanz, insbesondere auch von räumlichem Abstand, zwischen Täter/Täterin und Opfer, weitere Gewalt verhindert werden könne (Schumacher: FamRZ 2002, S. 645).

Seine hierfür vorgebrachte Begründung liest sich einfach: *„Weil die Identität der virtuellen Schlägertypen nicht in jedem Fall zu klären ist, sollte er sich auf ihre Schlagstöcke konzentrieren – nämlich die Accounts, mit denen sie verbale Gewalttaten begehen“* (Buermeyer 2019). Übertragen in die digitale Welt bedeutet dies nun, dass gerichtliche Verfahren eingeführt werden sollen, mit denen Sperrungen von solchen Accounts, die für rechtswidrige Äußerungen benutzt werden, beantragt werden können. Antragsberechtigt könnten nach dem Vorschlag sowohl Betroffene als auch Opferorganisationen sein. Wie das Gewaltschutzgesetz also Täter vor die Türe setzt, sollen die Nutzer der Accounts ausgeschlossen werden können. Dabei hätte das Gericht durchaus die Chance, über die Dauer der Sperre auch die Schwere der Rechtsgutverletzung hinreichend zu berücksichtigen. Als Vorteil eines solchen Verfahrens wird genannt, dass es

wegen der Antragsgegnerschaft aufseiten der Betreiber auf die konkrete Identität des Täters nicht mehr ankomme. Es wäre daher unerheblich, ob dieser unter seinem Klarnamen oder einem Pseudonym auftritt oder ob dieser aus Deutschland oder dem vermeintlich sicheren Ausland agiert.

Soweit hiergegen angeführt wird, dass sich die Schutzhöhe der Betroffenen gegenüber dem NetzDG nicht wesentlich verbessere, weil auch dort schon Löschpflichten normiert sind, ist dem entgegenzuhalten, dass der qualitative Unterschied darin besteht, dass über die Löschung oder Nicht-Löschung nicht der Seitenbetreiber in eigener Verantwortung und unter Wahrnehmung seines digitalen Hausrechtes entscheidet, sondern dass ein ordentliches Gericht in einem rechtsstaatlichen Verfahren hierüber zu entscheiden hat. Die Gerichte sind aufgrund ihrer Fachkenntnis auch durchaus in der Lage, hier binnen kürzester Zeit zu entscheiden. § 5 NetzDG stellt sicher, dass die Seitenbetreiber schon jetzt über eine ladungsfähige Anschrift im Inland verfügen, an die auch Zustellungen bewirkt werden können. Um den von der Sperre betroffenen Account-Inhabern rechtliches Gehör zu gewährleisten, bedürfte es einer Verpflichtung der Seitenbetreiber, diese von der Einleitung des Verfahrens durch elektronische Übersendung der Antragsschrift zu informieren. Diese Verpflichtung könnte im digitalen Gewaltschutzgesetz ebenso aufgenommen werden wie die datenschutzrechtliche Verpflichtung, für solche Benachrichtigungen eine E-Mail-Adresse in den Bestandsdaten zu pflegen. Prozessual müsste aller Voraussicht nach der Seitenbetreiber sowohl aus eigenem Recht als auch in gesetzlicher Prozessstandschaft für den Account-Inhaber in Anspruch genommen werden können. Dies hätte den weiteren Vorteil, dass der betroffene Inhaber des Accounts selbst in das Verfahren eintreten könnte oder gegebenenfalls eigenständig ein Rechtsmittel gegen einen Sperrbeschluss einlegen könnte.

Ein weiterer Einwand betrifft die Frage der Zweckmäßigkeit eines solchen Vorgehens. So könne es durchaus sein, dass der betroffene Account zwar gesperrt wird, der (anonyme) Nutzer dahinter aber, wenn auf seine konkrete Identität im Verfahren kein Wert gelegt werden muss, zeitgleich unter einem neuen Pseudonym auftreten könnte. Wenn dem so wäre, dann würde es sich um eine Don-Quichotterie handeln: Ein nicht zu gewinnender Kampf gegen Windmühlen, der darüber hinaus Ressourcen verschwendet. Diese These berücksichtigt aber nicht, dass das Internet und die Kommunikation darin einer eigenen Dynamik folgen. Adressaten eines (Hass-)Posts im Internet sind nicht nur die betroffenen Personen, sondern mindestens im gleichen Maße die vernetzten Freundinnen und Freunde im selben Netzwerk. Ein Account ohne Follower ist nichts. Es gibt

niemanden, der die hierüber verbreiteten Nachrichten liest. Der Aufbau eines neuen Netzwerkes hingegen ist schwierig und mühsam.

Soweit der berechtigte Einwand kommt, die Verteilung von solchen (Hass-) Posts könne unter gezielter Verwendung entsprechender Hashtags auch von Social Bots mit geringerem Aufwand erreicht werden, so ist in diesem Zusammenhang auch der damit verbundene Aufwand zu betrachten. Während auf der einen Seite eine konkrete Person zu einem konkreten Anlass sich kriminell verhält und deswegen persönlich von einer Maßnahme nach einem (zu schaffenden) digitalen Gewaltschutzgesetz betroffen wäre, geht es bei der Unterbindung von Postings, die durch Social Bots massenhafte Verbreitung finden, um ein Phänomen, das dem Kampf gegen Spam vergleichbar ist. Aber selbst hier könnte mit der Stilllegung eines Social Bots ein erheblicher Fortschritt erreicht werden, da dieser Bot durch die zu ergreifenden Maßnahmen wertlos wird. Wie im realen Leben und dem dortigen Gewaltschutzgesetz vermag die Schaffung einer digitalen Sperrvorrichtung dazu beitragen, dass weitere Gewalt verhindert wird und dass vor allen Dingen auch die konkrete Person des Opfers nachhaltig zu schützen ist.

Bleibt die Frage der polizeilichen Relevanz einer solchen Maßnahme. Hier handelt es sich bekanntermaßen um eine zivilrechtliche Auseinandersetzung zwischen Opfer und Täter beziehungsweise der Plattform. Es ist aber bei Schaffung von einheitlichen Standards für ein solches Gewaltschutzgesetz durchaus davon auszugehen, dass dann die Akten auch zügig an die Strafverfolgungsbehörden weitergeleitet werden können und entsprechende Ermittlungsverfahren eingeleitet werden können. Dadurch wird zwar gegebenenfalls die Chance der physischen Ermittlung des Täters aufgrund seiner Anonymität nicht erhöht, die dennoch spürbare Einschränkung aufgrund der ausgesprochenen Sperre dürfe aber eine nicht zu geringachtende präventive Wirkung haben.

11 Stärkung der Präventionsarbeit

Die Verfolgung von Straftaten im Internet, die kommunikationsbezogen sind, ist nicht einfach. Selbst wenn es gelingen sollte, einen Täter zu identifizieren, ist der Tatnachweis in vielen Fällen kaum oder gar nicht zu führen. Immerhin gibt es zwischenzeitlich in Nordrheinwestfalen bei der Zentral- und Ansprechstelle Cybercrime (ZAC NRW) ein Sonderdezernat „Hate Speech“. Dieses ermittelt neben Fällen, die dort von der BNetzA angezeigt werden auch Anzeigen aus dem „Verfolgen statt nur Löschen“-Projekt, in dem von mit dem Dezernat

kooperierenden Medien entsprechende Postings zur Anzeige gebracht werden.[4] Die dortigen Fallzahlen sind im Vergleich zu den mitgeteilten Löschungen der Internetkonzerne zwar gering, aber in einem Großteil der angezeigten Fälle wird auch ein Ermittlungsverfahren eingeleitet. Soweit sich das Phänomen Hate Speech nicht nur auf Plattformen der großen Internetkonzerne beschränkt, sondern auch die Kommentarspalten auf den Seiten von Medienhäusern betroffen sind, sehen diese sich einer besonderen Herausforderung gegenüber. Während einerseits ein Haftungsrisiko für die Inhalte auf den eigenen Seiten besteht, dem nur durch rigoroses Löschen begegnet werden kann, sind solche Maßnahmen im Kontext einer medienkritischen Nutzerschaft aber ihrerseits kontraproduktiv: Im Kontext einer Haltung, die sich einer vermeintlichen „System- und Lügenpresse" entgegenstellt, muss das Löschen geradezu als Bestätigung für die Richtigkeit der – nunmehr gelöschten – Behauptung aufscheinen (s. a. Kap. „Hate Speech in der Computerspielkultur"). Und genau dieses wiederum kann dann in den Filterblasen der Sozialen Medien viral verbreitet werden.

Gleiches würde gelten, wenn angesichts dessen die Redaktionen die Kommentarfunktion gänzlich abschalten würden. Allein der Umstand, dass die zum Teil strafrechtlich relevanten Inhalte nicht mehr öffentlich einsehbar sind, reicht also allein nicht aus. Weil die Redaktionen nun fragwürdige Inhalte anzeigen und diese somit sorgfältig juristisch geprüft werden, erhöht sich insgesamt die Rechtssicherheit in den Unternehmen: Zulässige Meinungsäußerungen können so von strafbaren Aussagen abgegrenzt werden. Letztlich gewinnt so auch die Meinungsvielfalt im Netz, weil durch diese Verfahren ein kontraproduktives over-blocking verhindert werden kann. Angestrebt wird daher eine konsequente Sanktionierung von Verstößen sowie eine darauf basierende generalpräventive Wirkung dieses Vorgehen (Hoppenstedt 2019).

Zu beachten ist hierbei aber, dass diese Sanktionierung in der Öffentlichkeit – sowohl in der analogen wie in der digitalen Welt – weitestgehend unbemerkt bleiben dürfte. Deswegen ist diesem Umstand in zweierlei Hinsicht entgegenzuwirken: Einerseits müssten solche Verfahren auch mit einer entsprechenden Medienarbeit begleitet werden. Hierbei bieten sich gerade die Social Media-Kanäle als interaktives Kommunikationsmittel an. Die Verbreitungsmöglichkeiten sorgen einerseits für eine Streuung der Nachricht, andererseits kann dann auch auf Antworten in den Kommentarspalten hierzu eingegangen werden. Dies hat den Vorteil, dass qualifiziert in einen digitalen „Bürgerdialog"

[4] https://www.justiz.nrw.de/JM/schwerpunkte/zac/index.php

eingetreten werden kann. Andererseits können die Strafverfolgungsbehörden in solchen Fällen auch ein sichtbares Zeichen ihrer Web-Präsenz setzen, indem aktiv auf solche Kommentare reagiert wird. Hinweise auf das Vorliegen eines Anfangsverdachts einer strafbaren Handlung dürften abschreckende Wirkungen erzielen. Soweit ein solches Vorgehen zudem „Zensur"-Vorwürfe nährt, kann diesen an Ort und Stelle wirksam begegnet werden.

Die Debattenkultur ist eine der Stärken des Internet. Aktive Präventionsarbeit erfordert daher Präsenz und Einmischung zur Wahrung und Stärkung rechtsstaatlicher Grundsätze. Dabei sind die verfassungsrechtlichen Grenzen einer zulässigen Öffentlichkeitsarbeit zu beachten: Das Bundesverfassungsgericht hat ausgeführt, dass die sachgerechte, objektiv gehaltene Information über das Recht, das den Bürger unmittelbar angeht, ein berechtigtes Anliegen im sozialen Rechtsstaat sein kann. Dadurch werde die Möglichkeit für alle, ihre Rechte zu wahren, verstärkt. In diesem Kontext findet die Öffentlichkeitsarbeit der Staatsorgane, ihre Rechtfertigung (Bundesverfassungsgericht, Urteil vom 2. März 1977 – 2 BvE 1/76).

Damit ein konstruktives Zusammenwirken von Redaktionen und Strafverfolgungsbehörden aber auch gelingen kann, ist ein organisatorischer Aufwand vonnöten, der es überhaupt erst ermöglicht, dass effiziente Verfahrensabläufe zur Verfügung stehen. Sowohl aufseiten der Seitenbetreiber wie auch auf der Seite der Strafverfolgungsbehörden sollen standardisierte Verfahren hier eine schnelle Reaktion ermöglichen. Neben dem hiermit verbundenen Selbstlernprozess in den Redaktionen ist es unerlässlich, dass diese auch entsprechend geschult werden, um die Erfolgsquoten insgesamt hochzuhalten. Wenn hierdurch schnell eine Sanktionierung von Rechtsverstößen erreicht werden kann, darf man sich davon grundsätzlich auch eine generalpräventive Wirkung erhoffen. Dabei darf nicht außer Acht gelassen werden, dass entsprechende Fälle nicht nur medial aufbereitet werden, sondern ihrerseits auch den Weg in die sozialen Medien finden müssen, um sich auch dort der Debatte zu stellen.

Hier lohnt auch ein Blick ins Ausland: Frankreich hat mit Facebook eine Vereinbarung geschlossen, wonach der Konzern sich bereit erklärt habe, auf Nachfrage der französischen Strafverfolgungsbehörden die IP-Adressen von Absendern strafrechtlich relevanter Inhalte bereitzustellen, ohne dass hierfür der Weg über ein Rechtshilfegesuch gegangen werden müsse. Bislang war das nur der Fall gewesen, wenn es um den Verdacht von Terrorismus und Kinderpornografie gegangen war. Derzeit existiert in Frankreich noch keine dem NetzDG vergleichbare Regelung, die die Löschung von inkriminierten Inhalten verlangen könnte. Ein Gesetzentwurf gegen „Cyber-Hass", der die Betreiber ähnlich der deutschen Regelung verpflichten soll, binnen 24 h Löschungen von Postings

mit strafrechtlich relevanten Inhalten in Bezug auf Rasse, Religion, Geschlecht, sexuelle Orientierung oder Behinderung vorzunehmen, wird in der französischen Nationalversammlung noch diskutiert. Durch die Ausweitung der freiwilligen Datenherausgabe auch auf Hate Speech-Delikte geht der Konzern einen Weg der Kooperation mit den staatlichen Behörden. Das Ziel ist hierbei nicht nur die effektive Verfolgung von Straftaten im Netz; Facebook hat auch ein Interesse daran, sein Image zu verbessern. Beachtenswert ist hierbei durchaus, dass dieses im Lichte des ersten Zusatzartikels zur Verfassung der Vereinigten Staaten von Amerika gesehen werden muss. Die darin garantierte Redefreiheit hat einen weit umfassenderen Schutzbereich als in fast allen anderen Ländern weltweit (Schubert 2019).

12 Fazit

Die Abwesenheit sichtbarer staatlicher Ordnung zeigt, dass Selbstregulierungskräfte im Netz in den seltensten Fällen funktionieren können, sondern hier archaischen und präzivilen Ordnungsmustern folgen. Die Internetkonzerne können heute aufgrund ihrer monopolartigen Stellung eine gesellschaftliche Macht darstellen. Eine Machtfülle dieses Umfangs lässt sich aber nur durch das Recht selbst begrenzen und beschränken. Dies ist genau genommen die „spezifische Konstellation“, von der das Bundesverfassungsgericht in seiner Stadionsverbot-Entscheidung gesprochen hatte (Ruffert 2018).

Die aus den Grundrechten resultierende Schutzpflicht gebietet es dem Staat und seinen Organen, sich nach außen wie im Innern schützend vor seine Bürger zu stellen. Er muss sie vor rechtswidrigen An- und Eingriffen vonseiten Dritter ebenso bewahren wie von anderen Gefährdungslagen. Er hat letztlich den Status positivus, also die Sicherheit und Freiheit eines jeden Einzelnen zu garantieren. Damit darf sich der Staat aber nicht zurückhalten; vielmehr hat er seine ihm zustehende legitime Macht zum Schutz der Bürgerinnen und Bürger und der Gewährleistung ihrer Grundrechte einzusetzen (Hopfauf in: Schmidt-Bleibtreu, Hofmann und Henneke, Einleitung RdNr. 307). Rechtsstaatlichkeit setzt innere Sicherheit voraus und gebietet zugleich ihren Schutz (Möstl 2002).

Die liberale Staatsidee war und ist geprägt von der Vorstellung, der einzelne Bürger müsse vor dem übermächtigen Staat geschützt werden. Deswegen übernahmen die liberalen Verfassungen wegen der verengten Sicht auf die Freiheitsgefährdungen im Wesentlichen nur die abwehrrechtlichen Elemente. Gleichwohl war auch der Gedanke an den Schutz des Einzelnen durch den Staat, der im Übrigen schon in den älteren amerikanischen Verfassungsurkunden und in der

französischen Erklärung der Menschenrechte verankert war, nie gänzlich verschwunden. Das Prinzip, wonach Sicherheit durch den Staat zu gewährleisten sei, ist nie gänzlich durch jenes, wonach dem Einzelnen die Sicherheit vor dem Staat zu gewährleisten sei, ersetzt worden (Dietlein 2005). Das Bundesverfassungsgericht führte in seiner Entscheidung zur Rasterfahndung 2006 aus:

> „In dem Spannungsverhältnis zwischen der Pflicht des Staates zum Rechtsgüterschutz und dem Interesse des Einzelnen an der Wahrung seiner von der Verfassung verbürgten Rechte ist es dabei zunächst Aufgabe des Gesetzgebers, in abstrakter Weise einen Ausgleich der widerstreitenden Interessen zu erreichen (vgl. BVerfGE 109, 279 <350>). Dies kann dazu führen, dass bestimmte intensive Grundrechtseingriffe erst von bestimmten Verdachts- oder Gefahrenstufen an vorgesehen werden dürfen. Entsprechende Eingriffsschwellen sind durch eine gesetzliche Regelung zu gewährleisten (vgl. BVerfGE 100, 313 <383 f.>; 109, 279 <350 ff. [BVerfG 26. Februar 2004 – 2 BvH 1/04]>; BayVerfGH, Entscheidung vom 7. Februar.2006 – Vf. 69-VI-04).“ (Bundesverfassungsgericht, Urteil vom 4.April 2006 – 1 BvR 518/02)

Auf die hier behandelte Themenstellung bezogen ist daraus zu schließen, dass der Gesetzgeber gehalten ist, die hier widerstreitenden Interessen der Sicherheit des Einzelnen gegen die Eingriffe in die jeweiligen Grundrechte abzuwägen. Hierbei spielen Eingriffstiefe und Rechtfertigungshöhe eine entscheidende Rolle: Je schwerwiegender das zu schützende Rechtsgut ist, umso stärker kann in die Grundrechte eingegriffen werden und dadurch entweder Gefahrenvorsorge oder Gefahrenabwehr erreicht oder effektiv Strafverfolgung betrieben werden. Diese Aufgaben kann man bei den hier behandelten Problemfeldern, die den Schutz der Menschenwürde, die freie Entfaltung der Persönlichkeit, das allgemeine Persönlichkeitsrecht und die Meinungsfreiheit betreffen, nicht den Internetkonzernen allein überlassen. Es genügt hier auch nicht, die staatliche Regulierung im Wesentlichen auf die Überwachung der den Unternehmen übertragenen Überwachungs- und Löschpflichten zu reduzieren. Die Eingriffstiefe auf Täterseite ist hier nicht entscheidend, es kommt vielmehr auf die zu schützenden Rechtsgüter der Betroffenen an. Auch unter Berücksichtigung realer Schwierigkeiten bei der Strafverfolgung kommt es deswegen umso mehr auf die Straftatenverhütung an.

Die Hoffnung auf die Selbstregulierungskräfte darf dabei nicht überschätzt werden. Gerade weil wirtschaftliche Interessen, und – wie nicht zuletzt auch die versuchten Wahlmanipulationen im Rahmen der US-Präsidentenwahl gezeigt haben – politische Interessen ein besonderes Gewicht in der kommunikativen Auseinandersetzung im Internet haben, braucht es die ordnende staatliche Hand. Statt Selbstregulierung bedarf es einer sichtbaren Präsenz der Polizei in den entsprechenden Online-Plattformen. Diese müssen flankiert werden mit einfach zu

bedienenden Interaktions- und Kommunikationsmöglichkeiten, damit schnell und frühzeitig entsprechende Maßnahmen auch eingeleitet werden können. Neben den hier zu nennenden Social Media-Auftritten der Polizeibehörden wären hier auch die sogenannten Internetwachen sowie eigens hierfür entwickelte Apps für mobile Endgeräte zu nennen. Hier besteht noch ein enormes Potenzial, das ausgebaut werden kann (Rüdiger 2018).

Einen weiteren Weg hat das Forschungsprojekt „Präventive digitale Sicherheitskommunikation“ (PräDiSiKo) beschrieben: Hier steht am Anfang die Erkenntnis, dass sich die klassische Kriminalprävention auch an das geänderte und digitalisierte Kommunikationsverhalten anpassen muss. Die Folge hieraus ist, dass die Präventionsarbeit für die Bürger umfassender als bisher auch und gerade in sozialen Netzwerken erreichbar sein muss. Weil die digitalen Kommunikationsprozesse und das Konsumverhalten sich von der analogen Welt unterscheiden, müssen entsprechende Inhalte so umgearbeitet werden, dass sie schnell erfasst, wahrgenommen und konsumiert werden können. Dieses Forschungsprojekt hatte sich zunächst drei Schwerpunktthemen gesetzt, die allesamt mit dem hier behandelten Thema zu tun haben: Gewalt, Hass im Netz und Radikalisierung. Als Ziel dieser Arbeit wurde die Förderung der Zivilcourage der Nutzer benannt, um die Sicherheit jedes Einzelnen und der Gesellschaft durch und in den sozialen Netzwerken erhöhen zu können (Bubenitschek und von Bissingen 2018). Als technologisches Ziel dieses Forschungsprojekts wurde formuliert nicht nur Empfehlungen für die kriminalpräventive Kommunikation zu entwickeln, sondern darüber hinaus sich Informations- und Kommunikationsmöglichkeiten für die kriminalpräventive Arbeit in den sozialen Onlinenetzwerken zu widmen. Dabei kommt den ethischen und datenschutzrechtlichen Aspekten eine herausragende Bedeutung zu.

In diesem Sinne hatte sich auch der Präsident des Bundeskriminalamts, Holger Münch anlässlich der Herbsttagung des BKA 2018 geäußert: *„Insofern ist es wichtig, dass wir beides tun: vor Ort für Bürgerinnen und Bürger präsent sein, bewährte analoge Polizeiarbeit machen, aber gleichzeitig auch unsere digitalen Fähigkeiten ausbauen“* (Münch 2018). Damit ist auch gemeint, dass die digitalen Fähigkeiten sich nicht nur in den Befugnissen oder Zuständigkeiten erschöpfen, sondern dass sich die Polizeien in Bund und Ländern auch der kulturellen Aufgabe stellen, den virtuellen Raum als digitale Agora zu begreifen, auf der Menschen, wenn sie miteinander in Interaktion treten, Straftaten vorbereiten und begehen. Sowohl Prävention als auch Repression bedarf einer sichtbaren Polizeipräsenz im Netz und einer leichten Erreichbarkeit. Was für Cybercrime im engeren Sinne schon Realität ist, sollte auch für die Deliktsfelder ins Auge gefasst

werden, die auf der Agenda des NetzDG stehen. Hierzu gehören beispielsweise zentralisierte Zuständigkeiten bei Polizei und Justiz.

Die Bündelung von Kompetenzen hat hier einen klaren Vorteil für sich: Aufgrund der nicht verortbaren virtuellen Welt als Tatort können auch die Strafverfolgungsbehörden völlig ortsunabhängig agieren. Letztlich ist aber dabei der Interaktion zwischen Nutzer und Polizei eine wichtige Rolle einzuräumen. Aufgrund der Tatsache, dass die Netzkultur von Kommunikation zwischen den einzelnen Nutzern geprägt ist, erwartet in der Regel jemand, der auf diesem Wege mit der Polizei in Kontakt tritt, eine entsprechend zugeschnittene und passgenaue Antwort. Standard-Autoresponder dürften an dieser Stelle eher abschreckend wirken. Automatisierte und verlässliche Chat-Bots könnten, wenn sie verfügbar sind, hier eine wertvolle Ergänzung bilden. Am Ende ist aber der persönliche Kontakt zwischen Polizei und Bürger auch in der digitalen Umgebung unverzichtbar.

Literatur

Ablon, L., Libicki, M. C., & Abler, A. M. (2014). *Markets for cybercrime tools and stolen data: Hackers' bazaar*. Santa Monica: RAND Corporation, RR-610-JNI. https://www.rand.org/pubs/research_reports/RR610.html.

Amann, M., Deleja-Hotko, V., & Rosenbach, M. (2019). Digitales Vermummungsverbot Schäuble drängt auf Klarnamen im Netz. https://www.spiegel.de/netzwelt/netzpolitik/wolfgang-schaeuble-will-klarnamen-pflicht-im-internet-a-1267993.html.

Berthel, R. (2019). Sicherheit in einer offenen und digitalen Gesellschaft. *Die Polizei,* 144.

Bubenitschek, G., & von Bissingen, S. (2018). Gewalt, Hass im Netz,Radikalisierung – Forschungsprojekt PräDiSiKo testet mit „Zivile Helden" Kriminalprävention in sozialen Netzwerken. *Kriminalistik,* 648.

Buermeyer, U. (2019). Statt Klarnamen: Digitales Gewaltschutzgesetz. https://background.tagesspiegel.de/statt-klarnamen-digitales-gewaltschutzgesetz.

Bundeskriminalamt. (2016). Bundeslagebild Cybercrime, S. 2.

Bundesregierung der Republik Östereich. (2019). 134/ME XXVI. GP – Ministerialentwurf – Erläuterungen, S. 1.

Bundesregierung der Republik Östereich. Entwurf für ein Bundesgesetz, mit dem ein Bundesgesetz über Sorgfalt und Verantwortung im Netz erlassen und das KommAustria-Gesetz geändert wird. https://www.ris.bka.gv.at/Dokumente/Begut/BEGUT_COO_2026_100_2_1631073/BEGUT_COO_2026_100_2_1631073.html. Zit.: Gesetzentwurf Österreich.

Christie, N. (1977). Conflicts as property. *The British Journal of Criminology, 1,* 1 ff.

de Tocqueville, A. (1799). Democracy in America. Zit. nach: http://xroads.virginia.edu/~HYPER/DETOC/toc_indx.html.

Dietlein, J. (2005). *Die Lehre von den grundrechtlichen Schutzpflichten* (2. Aufl., S. 23). Berlin: Duncker & Humblot.

DIVSI Entscheider-Studie zu Vertrauen und Sicherheit im Internet, Heidelberg, 2013.
Elsaß, L., Labusga, J.-H., & Tichy, R. (2017). Löschungen und Sperrungen von Beiträgen und Nutzerprofilen durch die Betreiber sozialer Netzwerke. *CR,* 234–241.
Engeler, M. (2018). Meinungsfreiheit: Warum Facebook (zu Recht) nicht an Grundrechte gebunden ist. https://netzpolitik.org/2018/meinungsfreiheit-warum-facebook-zu-recht-nicht-an-grundrechte-gebunden-ist/.
Enquete-Kommission. (2003). Globalisierung der Weltwirtschaft – Herausforderungen und Antworten. BT-Drucksache 24/9200, S. 461 ff.
Ewald, I. (2005). *Privatisierung staatlicher Aufgaben* (S. 15). Brühl: Fachhochsch. des Bundes für Öffentliche Verwaltung.
Grimm, D. (2002). Das staatliche Gewaltmonopol. In W. Heitmeyer & J. Hagan (Hrsg.), *Internationales Handbuch der Gewaltforschung* (S. 1297 ff.). Wiesbaden: Westdeutscher Verlag.
Guggenberger. (2017). Das Netzdurchsetzungsgesetz – Schön gedacht, schlecht gemacht. *ZRP,* 98.
Hansen, E. T. (2012). Warum die Amerikaner ihre Waffen so lieben. *Die Zeit*. https://www.zeit.de/politik/ausland/2012-07/USA-waffen.
Herzog, R. (2013). Vorwort zur Entscheiderstudie. In *DIVSI Entscheider-Studie zu Vertrauen und Sicherheit im Internet* (S. 6). Heidelberg: Deutsches Institut für Vertrauen und Sicherheit im Internet.
Hoppenstedt, M. (2019). Strafbare Postings in sozialen Netzwerken: "Woher der Hass kommt, ist wirklich nur schwer zu begreifen" – Interview mit Christoph Hebbecker. https://www.spiegel.de/netzwelt/netzpolitik/netzdg-staatsanwalt-christoph-hebbecker-ueber-hass-in-sozialen-netzwerken-a-1273176.html.
Ipsen, H. P. (1954). Gleichheit. In F. L. Neumann, H. C. Nipperdey, & U. Scheuner (Hrsg.), *Die Grundrechte* (Vol. II, S. 111 ff.). Berlin: Duncker & Humblot.
Isensee, J. (2006). Siebenter Teil, Ziele, Aufgaben und Grenzen des Staates, I. Ziele und Grenzen staatlichen Handelns, § 71 Gemeinwohl im Verfassungsstaat. In J. Isensee & P. Kirchhof (Hrsg.), *Handbuch des Staatsrechts der Bundesrepublik Deutschland: Bd. IV. Aufgaben des Staates* (3. Aufl., § 71 Rn. 76). München: C.F. Müller.
Kaßing, G., & Weinreich, G. (2018). J. Das Gewaltschutzgesetz RdNr. 373. In P. Gerhardt, B. von Heintschel-Heinegg, & M. Klein (Hrsg.), *Handbuch des Fachanwalts Familienrecht* (11. Aufl.). Neuwied: Luchterhand.
Kirsch, G. (1988). Die Deregulierungsdebatte – Anmerkungen zu einem bornierten Staat. In T. Schmid (Hrsg.), *Entstaatlichung* (S. 38 ff.). Berlin: Wagenbach.
Kluth, W. (2008). Rechtliche und funktionelle Unterschiede des Kammerrechts zum Vereinsrecht, S. 3.
Krings, G. (2019). Pro und Contra: Mit Klarnamen oder anonym im Netz? *DRiZ, 6,* 214.
Kultusministerkonferenz. (2016). *Bildung in der digitalen Welt* (S. 3). Berlin: Kultusministerkonferenz.
Ladeur, K. H. (2018). Netzwerkrecht als neues Ordnungsmodell des Rechts. In M. Eifert & T. Gostomzyk (Hrsg.), *Netzwerkrecht. Die Zukunft des NetzDG und seine Folgen für die Netzwerkkommunikation* (S. 169, 185). Baden-Baden: Nomos.
Liesching, M. (2018). Die Durchsetzung von Verfassungs- und Europarecht gegen das NetzDG – Überblick und wesentliche Kritikpunkte. MMR, S. 26–30.
Lobo, S. (2019). Auf dem digitalen Fußballplatz Drei Elfer, eine Ecke. https://www.spiegel.de/netzwelt/web/wenn-ueber-fussball-so-gesprochen-wuerde-wie-ueber-das-internet-a-1266384.html.

Marx, K. (2019). Verrohung und Online-Interaktion – Eine enge Koalition? Beleidigungskultur – Von verrohtem Diskursverhalten bis Cybermobbing, BPJMAktuell 2, S. 5.

May, A. (2017). *Cyberfähigkeit der deutschen Strafverfolgungsbehörden – Können wir mit der Entwicklung Schritt halten?* Redebeitrag zur BKA Herbsttagung 2017, Polizei im Umbruch – Herausforderungen und Zukunftsstrategien.

Mitteis, L. (1992). *Deutsche Rechtsgeschichte* (19. Aufl., S. 32). München: C.H. Beck.

Möstl, M. (2002). *Die staatliche Garantie für die öffentliche Sicherheit und Ordnung: Sicherheitsgewährleistung im Verfassungsstaat, im Bundesstaat und in der Europäischen Union.* Habilitationsschrift LMU München 2001 (S. 14 ff.). Tübingen: Mohr Siebeck.

Münch, H. (2018). *Kriminalitätsbekämpfung weiterdenken: Phänomene – Herausforderungen – Handlungsoptionen im Zeitalter von Big Data, Algorithmen und autonomen Systemen*. Redebeitrag BKA Herbsttagung 21.–22. November 2018: Sicherheit in einer offenen und digitalen Gesellschaft, S. 2.

Notz, Kv. (2019). Pro und Contra: Mit Klarnamen oder anonym im Netz? *DRiZ, 6,* 215.

Papier, H. J. (2017). Rechtsstaatlichkeit und Grundrechtsschutz in der digitalen Gesellschaft, *NJW,* 3025.

Rawls, J. J., & Orsi, R. J. (1999). *A golden state: Mining and California*. Berkley: University of California.

Reip, H. (2002). *Die Selbstregulierung im Internet*. Jena, S. 23.

Robertz, F. J., & Rüdiger, T.-G. (2012). Die Hacktivisten von Anonymous – Der schmale Grat zwischen guter Absicht und Selbstjustiz. *Kriminalistik, 2,* 79.

Rogan, F. (2018). Nebelkerzen um Staatstrojaner und Online-Durchsuchung. https://netzpolitik.org/2018/nebelkerzen-um-staatstrojaner-und-online-durchsuchung/.

Rosenkranz, C., & Feddersen, C. (2010). Managing viable virtual communities: An exploratory case study and explanatory model. *International Journal of Web Based Communities, 6*(1), 5–24.

Rüdiger, T.-G. (2018). Das Broken Web: Herausforderung für die Polizeipräsenz im digitalen Raum. In T. G. Rüdiger & P. S. Bayerl (Hrsg.), *Digitale Polizeiarbeit – Herausforderungen und Chancen* (S. 259 ff.). Wiesbaden: Springer VS.

Rüdiger, T.-G. (2019). Haben wir eine Unrechtskultur im digitalen Raum? *Kriminalistik, 1,* 37.

Ruffert, M. (2018). Common sense statt strikte Dogmatik? Zutreffendes aus Karlsruhe zu Stadionverboten. https://verfassungsblog.de/common-sense-statt-strikte-dogmatik-zutreffendes-aus-karlsruhe-zu-stadionverboten/.

Schiff, A. (2018). Meinungsfreiheit in mediatisierten digitalen Räumen. *MMR,* 366.

Schmidt-Bleibtreu, Hofmann, Henneke. (2017). Grundgesetz (14. Aufl.). Köln: Carl Heymanns Verlag.

Schöddert, L. (2018). Die mittelbare Drittwirkung von Grundrechten bei Facebook Account-Sperren und Stadionverboten. http://www.rechtstheorie.uni-koeln.de/die-mittelbare-drittwirkung-von-grundrechten-bei-facebook-account-sperren-und-stadionverboten/.

Scholz. (2009). In Maunz & Dürig. (Hrsg.), *Grundgesetz, 56. Ergänzungslieferung*, Art. 9 RdNr. 11. München: C.H. Beck.

Schubert, C. (2019). Facebook will Absender von Hassbotschaften enthüllen. *F.A.Z.* Einspruch vom 26. Juni 2019.

Schulze, M. (2019). *Governance von 0-Day-Schwachstellen in der deutschen Cyber-Sicherheitspolitik* (S. 7). Berlin: Stiftung Wissenschaft und Politik.

Schumacher, S. (2002). Mehr Schutz bei Gewalt in der Familie. *FamRZ,* 645.

Stang, F. L. (2017). Zur Haftung von YouTube nach § 816 Abs. 1 Satz 2 BGB, ZUM 2017, Heft 5, 380.

Stern, K., & Becker, F. (2019). *Grundrechte-Kommentar* (3. Aufl.), Artikel 9 GG RdNr. 11.

Stockhaus, H. (2015). *Regulierte Selbstregulierung im europäischen Chemikalienrecht*. Diss., Berlin, S. 83.

Taniguchi, N. J. (2016). *Dirty deeds, land, violence and the 1856 San Francisco Vigilance Committee*. Oklahoma: University of Oklahoma.

Vowe, G., Emmer, M. (2001). Elektronische Agora? Digitale Spaltung? – Der Einfluss des Internet-Zugangs auf politische Aktivitäten der Bürger. Ergebnisse einer empirischen Untersuchung. In: Internationales Wissenschaftliches Kolloquium, Technische Universität Ilmenau; 46 (Ilmenau): 2001.09.24–27, Reihe II/Workshop 5.

Walter, B. (2012). Das Gewaltmonopol des Staates – Ein praktisches Beispiel. *Polizei, 8,* 211.

Weber, M. (1922). *Wirtschaft und Gesellschaft – Grundriss der verstehenden Soziologie*. Mohr, Tübingen: Musaicum Books.

Weinzierl, Q. (2018). Warum das Bundesverfassungsgericht Fußballstadion sagt und Soziale Plattformen trifft. JuWissBlog Nr. 48/2018 v. 24.05.2018. https://www.juwiss.de/48-2018/.

Wiedemann, C. (2012). Open collectivity. In U. Herb (Hrsg.), *Open Initiatives – Offenheit in der digitalen Welt und Wissenschaft* (S. 205 ff.). Saarbrücken: universaar.

Zippelius, R. (1980). Gesellschaft und Recht. München: C.H. Beck.

Problematik der Hell- und Dunkelfeldanalyse im Bereich Cybercrime

Edith Huber und Bettina Pospisil

1 Einleitung

> „Kriminalität ist ein Spiegel der Gesellschaft. In der jeweiligen inhaltlichen Bestimmung des Kriminellen drückt sich pars pro toto die jeweilige Gesellschaft in ihrem Normalitätsverständnis und ihrer Toleranzbereitschaft aus.“ (Kunz und Singelnstein 2016, S. 10)

Bei einem näheren Blick auf die Kriminalitätsstatistiken der letzten Jahre ist unschwer zu erkennen, dass Delikte im Umfeld der Computerkriminalität[1] zumeist im Steigen begriffen sind. Waren es in Deutschland im Jahr 2006 noch 29.155 Anzeigen zu Cybercrime im engeren Sinne, so wurden im Jahr 2017 bereits 85.960 angezeigte Fälle erfasst. Im Jahr 2018 war die Zahl erstmalig rückläufig: es wurden 63.496 Fälle zur Anzeige gebracht (Bundeskriminalamt 2019a). Ähnlich verhält es sich mit den Zahlen in Österreich. Hier wurden im Jahr 2006 3257 Anzeigen von Cybercrime im engeren wie auch im weiteren Sinne gezählt,

[1]Computerkriminalität wird in der Polizeilichen Kriminalstatistik (PKS) von Deutschland und Österreich in Cybercrime im engeren Sinne und Cybercrime im weiteren Sinne unterschieden, jedoch nicht in gleicher Detailgetreue dargestellt. Aus diesem Grund wird immer konkret beschrieben, um welche Art von Cybercrime es sich bei den Zahlen handelt.

E. Huber (✉) · B. Pospisil
Donau-Universtität Krems, Krems, Österreich
E-Mail: edith.huber@donau-uni.ac.at

B. Pospisil
E-Mail: bettina.pospisil@donau-uni.ac.at

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

T.-G. Rüdiger und P. S. Bayerl (Hrsg.), *Cyberkriminologie,*
https://doi.org/10.1007/978-3-658-28507-4_4

im Vergleich dazu im Jahr 2017 bereits 16.804 Fälle (Bundesministerium für Inneres n. d.). 2018 stieg die Zahl erneut an; insgesamt wurden 19.627 Fälle von Internetkriminalität im engeren und weiteren Sinne zur Anzeige gebracht.

Dabei ist jedoch augenscheinlich, dass sich zwar insgesamt die Zahl der Anzeigen erhöhte, wie auch in Deutschland verringerten sich jedoch die Anzeigen von Computerkriminalität im engeren Sinne gegenüber dem Jahr 2017 um rund 13 % (Bundeskriminalamt 2019b). So kann in Bezug auf beide Länder zuletzt von einem leichten Rückgang der angezeigten Fälle im Bereich der Computerkriminalität gesprochen werden. Offen bleibt, worin sich dieser begründet. Die hier genannten Zahlen geben die Daten der amtlichen Polizeistatistik wider, beziehen sich also auf jene Fälle, in denen es zu einer Anzeige kam. Diese in den Aufzeichnungen erfassten Zahlen bilden jedoch weder alle real verübten noch alle erfolgreichen Cybercrime-Delikte ab. Diese Differenz zwischen Realität und Statistik ergibt sich aus unterschiedlichen Gründen und zeigt wie wichtig die Reflexion der eigenen Forschungsarbeit in Bezug auf Methode, Grundgesamtheit und Aussagekraft ist. Der folgende Beitrag beschäftigt sich mit dem Thema der Hell- und Dunkelfeldanalyse im speziellem Kontext des Phänomens Cybercrime.

1.1 Cybercrime – der Versuch einer Definition bzw. Phänomenologie

Bevor es zu einer Beschäftigung mit den Delikten der Cyber-Kriminalität kommt und die Entstehungszusammenhänge des Hell- und Dunkelfelds näher beleuchtet werden, gilt es das Phänomen Cybercrime näher zu definieren. Die Wissenschaftssprache an sich ist eine stark formalisierte Sprache, beherrscht von Definitionen und Theorien. Nähert man sich dem Phänomen Cybercrime ergeben sich unterschiedliche Betrachtungsmomente. Bei genauerer Analyse wird ersichtlich, dass jede Begriffsbeschreibung von Cybercrime andere und unterschiedliche Aspekte umfasst, bzw. Sachverhalte anspricht. Einige Definitionen beziehen sich ausschließlich auf den Begriff „Computer“. Dieser steht aber in keinem Zusammenhang mit „Computernetzwerken“, die unser aller Leben beeinflussen. Andererseits wird „Cybercrime“ oder „Virtual-Crime“ als ein Phänomen verstanden, das nur zutrifft, wenn dieser Computer mit dem Internet, also dem World Wide Web, in Verbindung steht (Morris 2004).

Eine weitere Herausforderung im Kontext der Definitionen ist, dass innerhalb der verschiedenen Wissenschaftsdisziplinen unterschiedliche Betrachtungsmomente eines Begriffes im Vordergrund stehen. Im Falle des von großer

Interdisziplinarität geprägten Begriffes „Cybercrime“ spannt sich der Bogen der Definitionen von Technik-, Rechts- und Wirtschaftswissenschaft bis hin zur Kriminologie, Psychologie und Soziologie. Diese Disziplinen haben sich nicht auf eine einheitliche Definition verständigt, sodass in Bezug auf den Begriff „Cybercrime“ passenderer Weise eher von einer Phänomenologie als von einer Definition gesprochen werden kann.

Die derzeit in den verschiedensten Disziplinen am häufigsten angewendete Art der relativ grundlegenden Unterscheidung ist die folgende:

- *Variante 1 – Cybercrime im engeren Sinn* (*core cybercrime* bzw. *cyber-dependent crime*): Unter diese Definition fallen alle Delikte, die es in keiner Variante offline gibt. Diese Kategorie meint die Verletzung der Vertraulichkeit, Integrität und Verfügbarkeit von Netzwerken sowie von Geräten, Daten und Services in diesen Netzwerken. Dazu zählen das Hacking (s. Kap. „Phänomenologie von digitalen Delikten“ und „Identitätsbildung im digitalen Zeitalter“), der Cyber-Vandalismus, die Verbreitung von Viren und vieles mehr.
- *Variante 2 – Cybercrime im weiteren Sinn* (*non-cyberspecific cybercrime* bzw. *cyberenabled crime*): Delikte, die unter diese Kategorie fallen, treten in ihrer ursprünglichen Form auch offline auf. Dazu zählen Delikte wie beispielsweise der Kreditkartenmissbrauch, Informationsdiebstahl, Cyberstalking sowie die Nutzung, Verbreitung und Zurverfügungstellung kinderpornografischer Inhalte (McGuire und Dowling 2013). In diesen Fällen ist der Computer das Tatmittel zur Umsetzung des Delikts.
- *Variante 3 – Verschleierung der Identität:* Diese Kategorie von Delikten betrifft Täter[2], die sich einen Online-Avatar zulegen, und die daraus resultierende Anonymität dazu verwenden, kriminell zu handeln, bzw. Täter, die sich gestohlener Identitäten oder Fake-Identities bedienen (Kirwan und Power 2013). Dazu zählt beispielsweise die Verbreitung von nationalsozialistischem Gedankengut in den sozialen Medien unter Nutzung eines falschen Namens.

[2]Aus Gründen der Lesbarkeit wurde im Text die männliche Form gewählt, nichtsdestoweniger beziehen sich die Angaben auf Angehörige beider Geschlechter. Im Falle von geschlechterspezifischen Differenzierungen wird sowohl die männliche, als auch die weibliche Form gesondert dargestellt.

Diese weit verbreitete Klassifizierung lässt jedoch trotzdem viele Aspekte unberücksichtigt. Ein weiterer Definitionsversuch stammt von Kshetri (2010), welcher beschreibt:

> „a cybercrime is defined as a criminal activity in which computers or computernetworks are the principal means of committing an offense or violation of laws, rules, or regulation“ (Kshetri 2010, S. 143).

Dieser Definition zur Folge stellt Cybercrime eine kriminelle Aktivität dar, die mit Computer oder Computernetzwerken durchgeführt wird, um eine Straftat zu begehen. Diese Definition ist sehr generell und meint, dass sobald ein Computer im Laufe eines Kriminaldelikts verwendet wird, auch ein Cybercrime-Delikt anfällt.

Darüber hinaus kann Cyber-Kriminalität dem nationalen Kontext entsprechend nach dem rechtlichen Rahmen definiert werden, unter dem Cybercrime-Delikte klassifiziert werden. Diese Klassifizierung spiegelt sich in der PKS (Polizeiliche Kriminalstatistik) wieder. Dabei unterscheidet die Kriminalstatistik jedoch nicht nach der Rolle der Technik in Bezug auf das Delikt (siehe Varianten 1–3) und somit unterscheidet sich die juristische Definition von cyber-kriminellem Verhalten je nach nationaler Gesetzeslage. Diese fehlende Harmonisierung internationaler Gesetze stellt angesichts der Notwendigkeit einer internationalen Verbrechensbekämpfung ein großes Problem dar (s. a. Kap. „Der digitale Raum ist kein (grund-)rechtsfreier Raum“). Die Vereinheitlichung des Rechtsrahmens, so die Europol, sei gerade im Kontext des grenzenlosen Cyberspace jedoch unabdingbar. Dazu definierte das United Nations Office on Drugs and Crime (UNODC 2013) grundlegende Eigenschaften von Cybercrime und damit einhergehenden Notwendigkeiten:

1. Die Intensität von Cybercrime hängt von kulturellen, juristischen, wirtschaftlichen und regionalen Einflussfaktoren ab.
2. Traditionelle Methoden der Verbrechensbekämpfung greifen in Bezug auf dieses Phänomen nicht mehr. Elektronische ‚Beweise‘ verteilen sich oft über mehrere Orte der Welt, was ein Auffinden der Täter erschwert.
3. In der Zeit von Cloud Computing usw. muss sich die Legislative künftig überlegen, welche Beweise zur Verurteilung von Tätern infrage kommen, damit eine effiziente Strafverfolgung möglich wird.
4. Es bedarf einer Harmonisierung der nationalen Rechte, um eine Strafverfolgung im internationalen Umfeld zu erleichtern.
5. Die Cybercrime-Prävention muss international eine hohe Priorität einnehmen.

2 Das Hellfeld und das Dunkelfeld

„Die Strafe kann ihre soziale Wirksamkeit nur bewahren, solange die Mehrheit nicht bekommt, was sie verdient.“ (Popitz 1968, S. 20)

2.1 Definition von Hellfeld und Dunkelfeld

Um Delikte des Cybercrime, aber auch alle anderen Verstöße gegen das Gesetz, untersuchen zu können, müssen Forscher sich zunächst damit auseinandersetzen, zu welchen Daten sie Zugang haben. Kriminalität an sich ist ein schwer zählbares Phänomen, das erst durch die gesellschaftliche Wahrnehmung und Ahndung in Erscheinung tritt. Damit ist garantiert, dass viele Fälle von Kriminalität nicht festgehalten werden und somit auch nicht analysierbar sind. Darüber hinaus wird Kriminalität über die einzelne Handlung des kriminellen Verhaltens gemessen, wodurch jede Statistik, die sich auf aggregierte Datenmengen beruft, bereits eine Interpretation der Wirklichkeit darstellt. Wird eine kriminelle Tat nun offiziell gemeldet, so schlägt sie sich in der Statistik nieder und zählt laut Kunz und Singelnstein (2016) zum *Hellfeld.* Dem gegenüber steht das *Dunkelfeld* das, den Autoren zufolge, all jene kriminellen Handlungen umfasst, welche keine offiziellen Reaktionen nach sich zogen. Die Auffassungen und konkreten Definitionen gehen hier etwas auseinander. Für Schneider (1993) zählen beispielsweise auch jene Delikte zum Dunkelfeld, die zwar der Polizei gemeldet wurden, jedoch nicht aufgeklärt werden konnten, da die Täter unbekannt blieben.

Das Verhältnis von Dunkel- und Hellfeld wird als *Dunkelziffer* bezeichnet. Diese soll abbilden, in welchem Verhältnis die real vorkommenden Kriminalitätsfälle offiziell erfasst werden. Dabei ist jedoch zu berücksichtigen, dass eben diese real vorkommenden Kriminalitätsfälle sich wiederum nur auf jene Fälle beziehen können, welche gesellschaftlich wahrgenommen und durch eine Reaktion der Bevölkerung sichtbar wurden. Wahrnehmung und Reaktion der Bevölkerung sind jedoch stets von konkreten Perspektiven und Vorurteilen der einzelnen Personen geprägt, weswegen sie sehr subjektiv sind. Das tatsächliche Kriminalitätsgeschehen bleibt einmal mehr im Dunkeln und wird aus diesem Grund als doppeltes oder *absolutes Dunkelfeld* bezeichnet (Kunz und Singelnstein 2016; s. Abb. 1). Als Erweiterung dieser Überlegungen differenzierte Schneider (1993) darüber hinaus auch jene Fälle, bei denen die Ermittlung aus unterschiedlichen Gründen eingestellt werden mussten, als *‚Graufeld der Kriminalität‘* (Schneider 1993, S. 47 f.), da unklar bleibt, ob es sich um Verbrechen handelt.

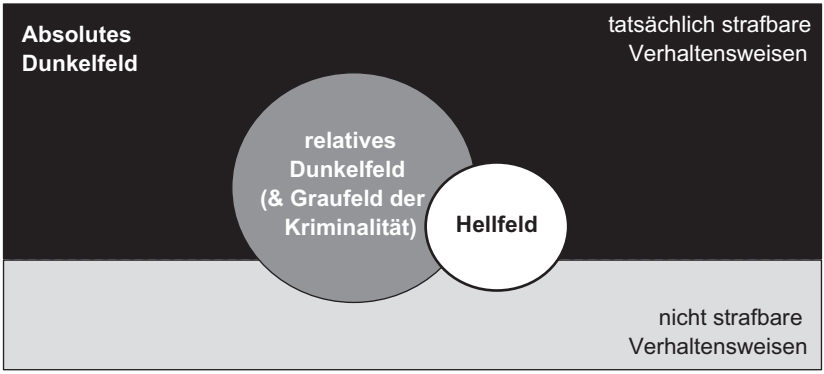


Abb. 1 Hellfeld und Dunkelfeld nach dem Vorbild von Kunz und Singelnstein (2016)

Mit Bezug auf die Cyber-Kriminalität kann somit bei allen angezeigten Delikten vom Hellfeld gesprochen werden; je nach Auslegung auch bei jenen Fällen die nicht aufgeklärt wurden. Jene Delikte, welche zwar als solche wahrgenommen, jedoch nicht angezeigt werden, können als *relatives Dunkelfeld* bezeichnet werden. Dies sind beispielsweise Angriffe auf sensible Daten großer Firmen, welche diese nicht anzeigen möchten, da sie einen Reputationsverlust fürchten. Unter dem absoluten Dunkelfeld können letztendlich jene Delikte subsumiert werden, die dem Opfer selbst nicht bewusst sind. Dazu zählen beispielsweise Delikte in denen Computer in Botnetze eingebunden werden, welche in weiterer Folge für Angriffe verwendet werden, ohne dass der Besitzer des Computers etwas davon ahnt.

2.2 Beschreibung am Verlauf der Registrierung

Kriminelles Verhalten wird nur dann offiziell gemeldet und registriert, wenn es nach geltendem Recht auch strafbar ist. Somit sind Hell- und Dunkelfeld auch stark von nationalen Unterschieden in der Gesetzgebung abhängig und können je nach Region bzw. Nation variieren. Darüber hinaus bestimmt die Selektion von Fällen während des Prozesses der Strafverfolgung das Verhältnis von Dunkel- und Hellfeld. So sind bereits mehrere Bedingungen dafür notwendig, dass ein kriminelles Verhalten den Weg in die PKS schafft:

1. Das Verhalten muss auftreten, beispielsweise wird eine Handlung gesetzt oder aber auch Unterlassen.
2. Dieses Verhalten muss von der Polizei oder einem anderen Vertreter der Gesellschaft als kriminell wahrgenommen werden.
3. Diese Wahrnehmung muss im Sinne einer Strafanzeige kommuniziert werden.
4. Im Falle der Wahrnehmung des abweichenden Verhaltens durch eine andere Person als einen Polizisten, muss dieses Delikt außerdem noch in die Bearbeitung der Polizei übergehen. Erst wenn diese die Fälle an die Staatsanwaltschaft weitergibt, kommt es zu einer Aufzeichnung in der PKS (Kunz und Singelnstein 2016).

Erst wenn diese vier Prozessschritte erfüllt sind, wird das kriminelle Verhalten in der PKS, der ersten statistischen Sammlung gelistet (s. Abb. 2).

Wird die PKS für wissenschaftliche Analysen herangezogen, muss somit stets reflektiert werden, dass die Ergebnisse und somit die Aussagekraft dieser jenes kriminelle Verhalten ausschließen, welches nicht von der Gesellschaft als solches wahrgenommen, nicht angezeigt oder nicht weiter durch die Polizei verfolgt wird. Im Verlauf dieses Prozesses der Strafverfolgung wird die Anzahl der Delikte in allen folgenden Statistiken immer geringer, da laufend Delikte ausscheiden, die bestimmte Faktoren nicht erfüllen. Je nachdem, ob es zu einem personenbezogenen Tatverdacht kommt, eine Anklage ausgesprochen wird bzw. eine

B & W IN PRINT

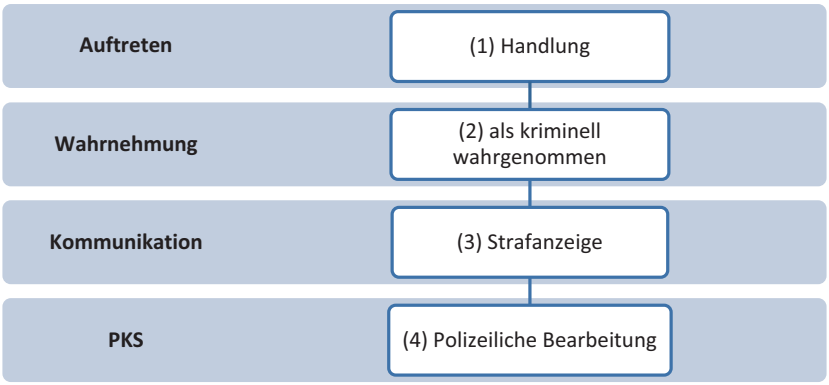


Abb. 2 Verlaufsschema von der Klassifizierung zur Registrierung

Verurteilung erfolgt oder freiheitsentziehende Sanktionen vollzogen werden, kann kriminelles Verhalten schlussendlich bis in die Strafvollzugsstatistik gelangen.

Grundsätzlich ist es wichtig zu verstehen, dass sowohl die Hellfeld- als auch die Dunkelfeldforschung die Wahrnehmung und Bewertung von Handlungen durch bestimmte Personengruppen bzw. Institutionen misst:

> „Wie in der Kriminalstatistik wird somit in der Dunkelfeldforschung nicht reales Kriminalitätsgeschehen erfasst. Beide Forschungszweige reproduzieren die ihren unterschiedlichen Forschungsdesigns zugängliche Kriminalitätswahrnehmung von Instanzen und Bevölkerung.“ (Kunz und Singelnstein 2016, S. 230)

Die Dunkelfeldforschung setzt lediglich früher an – bei der 2) Wahrnehmung des Verhaltens als kriminell – und bezieht auch jene Fälle mit ein, welche nicht 3) zur Strafanzeige gebracht oder 4) polizeilich bearbeitet wurden (vgl. Abb. 2). Die Handlung an sich kann jedoch nicht naturalistisch analysiert werden, denn erst durch diese Zuschreibung, also die Wahrnehmung durch den Menschen als kriminelles Verhalten, entsteht Kriminalität. Die Kriminalität ist folglich nichts Natürliches vom Menschen Unabhängiges, sondern etwas von ihm Geschaffenes (Durkheim 1979).

2.3 Methoden zur Erforschung von Hellfeld und Dunkelfeld

> „Beide Erhebungsformen kriminalstatistischer Daten liefern sich nicht ausschließende, sondern sich vielmehr ergänzende, konvergierende, übereinstimmende Zahlen über Delinquenz und Kriminalität, die für die kriminologische Forschung von großem Wert sind.“ (Schneider 1993, S. 57)

Nachdem nun ein grundlegendes Verständnis von Hell- und Dunkelfeld aufgebaut wurde, beschäftigen wir uns mit der Frage, welche Auswirkungen diese Differenzierung auf die anzuwendende Forschungsmethode hat. Dazu wird jedoch zunächst das Verhältnis von Hellfeld und Dunkelfeld thematisiert und anschließend Methoden zur Erforschung der unterschiedlichen Bereiche von Kriminalität illustriert.

2.3.1 Verhältnis von Hellfeld und Dunkelfeld

Lange Zeit herrschte in der Kriminologie die Überzeugung vom „Gesetz der konstanten Verhältnisse“ von Adolphe Jacques Quételet (1869, S. 253) vor. Dieses Gesetz besagt, dass zwischen dem Hellfeld und dem Dunkelfeld einer Deliktart

ein konstantes und feststehendes Verhältnis besteht. Erst nach dem die repräsentative Bedeutung des Hellfeldes für das Dunkelfeld kritisiert wurde, stieg die praktische Auseinandersetzung mit der Dunkelfeldforschung (Schneider 1993). Nach Schwind (2013) kann das Verhältnis von Hell- und Dunkelfeld drei Formen annehmen: 1) das konstante Verhältnis, 2) das additive Verhältnis oder 3) kein Verhältnis. Das *konstante Verhältnis* meint, dass bei einem Anstieg der Delikte im Hellfeld auch die Delikte im Dunkelfeld im gleichen Ausmaß ansteigen. Dieses Verhältnis wurde lange Zeit angenommen, ist heute aber sehr umstritten. Das *additive Verhältnis* hingegen geht davon aus, dass die Summe der Delikte im Hell- und im Dunkelfeld gemeinsam immer gleich groß ist. Dieses Verhältnis meint also, dass beispielsweise ein Anstieg der Delikte im Hellfeld mit einem Rückgang der Delikte im Dunkelfeld einhergeht. Schließlich gibt es auch die Möglichkeit, dass Hellfeld und Dunkelfeld in keinem Abhängigkeitsverhältnis zueinanderstehen.

In Bezug auf die Cyber-Kriminalität wird von einem verhältnismäßig großen Dunkelfeld ausgegangen (siehe dazu unter anderen Bundeskriminalamt 2019b).

2.3.2 Methoden zur Erforschung des Hellfeldes

Um Aussagen über das Hellfeld zu tätigen, wird häufig eine Sekundärdatenanalyse durchgeführt. Dazu werden beispielsweise amtliche Kriminal- und Strafrechtspflegestatistiken, das Bundeszentralregister sowie Ermittlungsakten der Staatsanwaltschaft herangezogen. Diese Statistiken enthalten Daten zur Art und Häufigkeit von Straftaten genauso wie zu den Tatverdächtigen und Opfern der Delikte. Je nach Statistik finden sich auch Details zum Ermittlungs- und Prozessverfahren. Die zur Analyse am häufigsten verwendeten Statistiken sind die polizeiliche Kriminalstatistik, die Strafvollzugsstatistik sowie die Rückfallstatistik (Kersting und Erdmann 2015). Darüber hinaus können auch Mediennutzungsstudien unterschiedlicher Institutionen herangezogen werden. Beispiele dafür stellen in Deutschland die Kindheit, Internet, Medien (KIM)-Studie bzw. die Jugend, Information, Media (JIM)-Studie, in Österreich Studien der Initiative saferinternet.at, der Austrian Internet Monitor oder des SOS-Kinderdorfes und in der Schweiz die JAMES-Studie sowie die Medien, Interaktion, Kinder, Eltern (MIKE)-Studie dar.

Als Erfassungsmethode für Sekundärdaten wird häufig eine quantitative Aktenanalyse angewendet (unter anderen nach Dölling 1984). Dazu wird zunächst anhand von bestehendem Wissen aus der Theorie ein Analysebogen erstellt, der die für die Forschungsfrage notwendigen Variablen abfragt. Dieser Bogen wird mithilfe des Datenmaterials befüllt. Nach der Erhebung werden diese Daten in ein Statistikprogramm eingelesen und analysiert. Die Aktenanalyse

von Sekundärdaten ist ein quantitatives Werkzeug und hat somit zum Ziel, Fälle und ihre Zusammenhänge zu beschreiben und zu erklären. Aufgrund der Herangehensweise mit vorgefassten Kategorien und dem geschlossenen Analysebogen kann diese Methode nicht die Relevanzstruktur der Täter bzw. Opfer beleuchten.

Dieses Ziel haben qualitative Forschungsmethoden, die das Phänomen und ihren Ursprung verstehen wollen. Dabei können Fragen zu sozialen und psychologischen Hintergründen der Tat näher behandelt werden. Dies ist vor allem hinsichtlich einer genaueren Beschreibung von Viktimisierung und Täterwerdung sowie der Ermittlung des Modus Operandi notwendig. In diesen Fällen können beispielsweise qualitative Interviews, die mit bekannten Tätern und Opfern geführt werden, neue Erkenntnisse bringen. Dazu können sehr offene Interviewformen wie das narrative Interview genauso angewendet werden wie problemzentrierte und leitfadengestützte Interviews (Diekmann 2010). Die Interviews werden anschließend transkribiert und mit einer qualitativen Auswertungsmethode wie beispielsweise der Inhaltsanalyse nach Mayring (2000) oder der hermeneutischen Methode analysiert.

2.3.3 Methoden zur Erforschung des Dunkelfelds

Wenn von Forschungsmethoden in Bezug auf das Dunkelfeld gesprochen wird, ist stets zu berücksichtigen, dass die Dunkelfeldforschung sowohl die nicht registrierten wie auch die registrierten Fälle zu analysieren versucht, also das Ziel verfolgt, die Gesamtheit kriminellen Verhaltens zu erfassen. Da im Gegensatz zur Hellfeldanalyse die interessierenden Daten bei der Dunkelfeldanalyse erst erhoben werden müssen, zählen Befragungen – wie die Täter-, Opfer- oder Informanten-Befragung – die teilnehmende wissenschaftliche Beobachtung sowie das Experiment zu möglichen Methoden der Datenerhebung (Prätor 2015; Roll 2017; Schneider 1993). Da Experimente in ihrer Durchführung sehr aufwendig und die aus ihnen gewonnenen Ergebnisse nur schwer verallgemeinerbar sind, werden sie nur selten im Rahmen der Dunkelfeldforschung eingesetzt. Die Teilnehmende Beobachtung bietet dem Forscher einen von Täter und Opfer unabhängigen Einblick in die Struktur des kriminellen Verhaltens. Herausforderungen sind jedoch ethische Probleme genauso wie Gedächtnislücken und Fehlinterpretationen. In Hinblick auf die Datenerhebung in der Dunkelfeldforschung kommt, so Prätor (2015), der Befragung die bedeutendste Rolle zu. Gründe dafür sind unter anderen der verhältnismäßig geringe Aufwand und der große Personenkreis, der damit erreicht werden kann. Grundsätzlich wird eine Bevölkerungsgruppe nach ihren Erfahrungen als Täter, Opfer oder Zeuge von Straftaten befragt. Je nach Forschungsfrage kann eine Querschnitts- oder eine Längsschnittbefragung durchgeführt werden.

Bei der Täterbefragung wird eine spezielle Bevölkerungsgruppe danach gefragt, ob sie in einem bestimmten Zeitraum oder generell irgendwann in ihrem Leben unterschiedliche Straftaten begangen hat. So kann das abweichende Verhalten in seiner Quantität abgefragt und mit verschiedenen Bedingungs- und Risikofaktoren in Beziehung gesetzt werden. Demgegenüber können mittels Opferbefragungen spezielle Bevölkerungsgruppen dahin gehend befragt werden, ob sie bereits Opfer bestimmter Straftaten wurden. Dabei können Informationen über die Entwicklung der Kriminalität genauso gewonnen werden wie über die speziellen Umstände der Opferwerdung und die daraus resultierenden Folgen. Häufig werden Fragen zur Viktimisierung in Täterbefragungen inkludiert. Ist die für das Forschungsinteresse relevante Population nur schwer erreichbar, gibt es außerdem die Möglichkeit Informantenbefragungen durchzuführen. Die Befragten werden hier gebeten Angaben zu Delikten zu machen, von welchen sie lediglich Zeuge wurden.

Methodische Herausforderungen der Dunkelfeldforschung sind im Speziellen die soziale Erwünschtheit, die Inkongruenz von Alltagsvorstellungen und juristischen Definitionen, die Coverage-Problematik[3], der Mode- und der Telescoping-Effekt[4], welche Einflüsse durch Erhebungsmethoden und das Erinnerungsvermögen der Befragten meinen (Prätor 2015). Um speziell den Effekt der sozialen Erwünschtheit geringer zu halten, kann die Randomized-Response-Technik[5] als spezielle Form der Befragung angewendet werden.

Das bedeutendste Beispiel für die Dunkelfeldforschung ist der seit 1973 jährlich in den USA durchgeführte *National Crime Victimization Survey* (Bureau of Justice Statistics n. d.). Bei näherer Betrachtung zeigt sich, dass die größtenteils eingesetzten Methoden der Dunkelfeldforschung quantitativer Natur sind. Qualitative Fragestellungen können damit nicht erhoben werden. Darüber hinaus sind die Erhebungsmethoden auch dahin gehend kritisch zu hinterfragen, da sie einen Teil des Dunkelfelds ausklammern bzw. nicht erreichen. Beispielsweise schließt eine Opferbefragung je nach Art der Durchführung (online, telefonisch) immer bestimmte Personengruppen aus.

[3]Ein statistischer Erhebungsfehler hinsichtlich der Grundgesamtheit.

[4]Die Neigung der Befragten, Ereignisse aus der Vergangenheit in die Zukunft zu projizieren.

[5]Diese Technik garantiert den Befragten vollständige Anonymität und bietet über die Kombination aus Befragung und Zufallsmechanismus die Möglichkeit, eine Population in zwei Gruppen einzuteilen: in die Träger und die Nichtträger eines interessierenden kritischen Merkmals (Diekmann 2010).

Zusammenfassend sei daher anzumerken, dass jede Erhebungsmethode, ob nun im Hell- oder Dunkelfeld ihre Stärken und Schwächen hat. Je nach Delikt und Rahmenbedingungen muss entschieden werden, welcher methodische Ansatz am besten geeignet ist, um dem bestehenden Forschungsinteresse zu begegnen. Grundsätzlich sollte deshalb bei Erhebungen im Dunkelfeld immer die Forschungsmethode mitreflektiert werden, da diese Auswirkungen auf die Aussagekraft der Ergebnisse haben.

> „Nicht alles, was zählt, kann gezählt werden, und nicht alles, was gezählt werden kann, zählt!“ (Albert Einstein, 14.03.1879–18.04.1955)

3 Das Hellfeld und das Dunkelfeld im Cybercrime

3.1 Wer sind die Täter und Opfer im Cybercrime-Umfeld?

Statistiken, wie diese von ITU (2018) in Abb. 3 zeigen, dass weltweit rund jeder Zweite Teil des World Wide Web ist. Durch die immer stärker anwachsende Vernetzung der globalen Welt steigt der Personenkreis jener, welche zum Opfer aber auch Täter von Cyber-Kriminalität werden können. Damit liegt auf der Hand, dass sowohl die Erfassung des Hell- als auch des Dunkelfelds vor neuen Herausforderungen steht. Nun stellt sich die Frage: Eignen sich bestehende

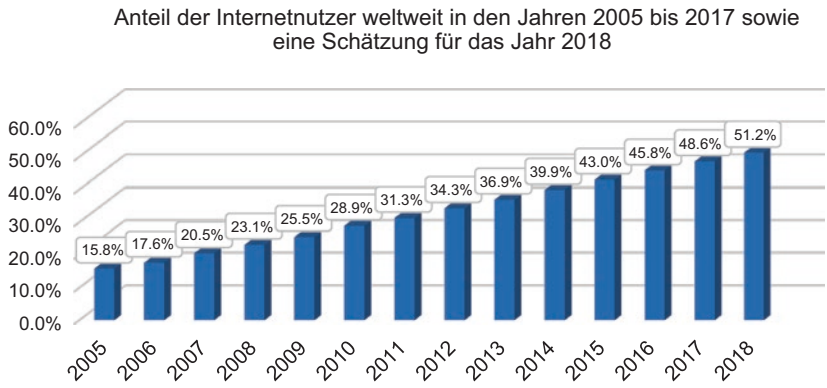


Abb. 3 Anteil der Internetznutzer weltweit (ITU 2018)

B & W IN PRINT

Erhebungsmethoden noch, oder müssen neue methodische Ansätze entwickelt werden, um das Phänomen Cyber-Kriminalität zu erfassen?

Laut dem Anti-Virenhersteller Symantec (2017) lag der Schaden, der durch Cyber-Kriminalität verursacht wird, im Jahr 2017 weltweit bei $172 Mrd. In Deutschland waren es US$2,6 Mrd. Zu kaum einem anderen Thema wie der Cyber-Kriminalität gibt es so viele Statistiken, Hochrechnungen usw. Dabei sollten bei der Betrachtung dieses Materials stets einige kritische Fragen im Hinterkopf behalten werden:

1. Wie generiert der Autor seine Zahlen?
2. Wie sind die Täter bzw. die Opfer von Cybercrime definiert?
3. Wie wird der Schaden gemessen?
4. Spiegeln diese Zahlen die Realität wieder?
5. Handelt es sich um Hellfeldzahlen oder sind auch Dunkelfeldzahlen inkludiert?

Besonders wichtig ist es, bei solchen Erhebungsmethoden immer auch die Zielgruppe sowie die Erfassungsmethode zu definieren. Ist der Erfasser ein IT-Security Unternehmen, das beispielsweise Anti-Viren-Software verkauft, so erfasst es zumeist die Cyber-Angriffe, die es durch die eigenen Systeme verhindern konnte. Bei dieser Zahl wird nicht zwischen erfolgreichen (die Angreifer konnten sich Zugriff verschaffen) und nicht erfolgreichen Angriffen (die Angreifer konnte sich keinen Zugriff verschaffen) unterschieden. Darüber hinaus gilt es auch festzuhalten, dass nicht jede Cyber-Attacke automatisch unter den Bereich Cybercrime fällt.

3.2 Methoden zur Erforschung von Cybercrime

3.2.1 Erfassung von Hellfelddaten im Bereich Cybercrime

Wie bei anderen Kriminalitätsdelikten werden auch im Bereich Cybercrime die Fälle des Hellfelds in erster Linie über strafrechtlich relevante Anzeigen gemessen. Um das komplexe Phänomen Cybercrime besser fassen zu können, ist es auch üblich verschiedene Methoden der Hellfeldanalyse (beispielsweise Meta-Analyse, Sekundärdatenanalyse und Experteninterviews bzw. Gruppendiskussionen) zu kombinieren (siehe unter anderem Bundeskriminalamt 2015a).

In Bezug auf Cyber-Kriminalität gibt es jedoch die zusätzliche – bereits beim Thema der Definition angesprochene – Problematik der unterschiedlichen Rechtsrahmen (Brenner 2006; Csonka 2004). So muss bei jeder Hellfeldanalyse

zum Thema Cybercrime genau reflektiert werden, welche Paragraphen in der jeweiligen Nation unter diese Klassifizierung fallen und welche Auswirkungen dies auf die Aussagekraft der Ergebnisse hat. Beim Thema Cybercrime kommt es dabei zu Verschiebungen in beide Richtungen: So werden Delikte, welche eigentlich offline erfolgen, jedoch einen elektronischen Vorgang beinhalten – wie bspw. der Klau einer Bankomatkarte und das anschließende Bezahlen mit dieser – als Cybercrime eingestuft, während andere Delikte, die Großteils über technische Komponenten erfolgen – beispielsweise das Cyberstalking, welches heutzutage vielfach über soziale Medien passiert – nicht zu Cybercrime gezählt werden. Im Speziellen beim Cyberstalking ist es nicht immer einfach die kriminelle Handlung zu klassifizieren. Es gibt Fälle, bei denen man von einem klassischen Stalking im Sinne einer beharrlichen Verfolgung sprechen kann. Darüber hinaus gibt es Cyberstalking-Täter, die sich illegal Zugriff auf die IT-Systeme der Opfer verschaffen. Dann stellt sich die Frage, handelt es sich um ein typisches Stalking-Delikt oder sind die Tatbestände der Cyber-Kriminalität gegeben?

Darüber hinaus muss bei Hellfelderhebungen im Cybercrimebereich berücksichtigt werden, dass sich im Gegensatz zu anderen Kriminalitätsdelikten, wie beispielsweise Mord oder Einbruch, der Modus-Operandi nicht über den angeklagten Paragraphen bestimmt werden kann. So wird beispielsweise in Österreich der Identitätsdiebstahl über Bankomatkarten-Daten, egal ob er online (Täter verschafft sich Zugriff auf die Daten mittels Phishing-Attacke) oder offline (Täter stielt die Bankomatkarte aus der Geldtasche des Opfers) erfolgt, nicht unterschieden. Beide Täter nutzen die illegal erworbenen Bankomatkarten-Daten zum Erwerb von Produkten bzw. Dienstleistungen. Somit werden beide Delikte unter dem § 148 a[6] zur Anzeige gebracht, obwohl eindeutig ein anderer Tathergang hinter dem Delikt liegt. Damit ergibt sich eine verzerrte Zählung der Cybercrime-Fälle.

Ein weiterer wichtiger Aspekt in der Auseinandersetzung mit Sekundärdaten in Bezug auf Cybercrime, ist die Unterscheidung zwischen jenen Fällen, welche bei Gericht verhandelt wurden und jene, welche nicht geklärt werden konnten. Wie das Fallbeispiel[7] in diesem Artikel zeigt, gibt es im Bereich Cyber-Kriminalität eine große Anzahl an Fällen, die nicht geklärt werden kann. Diese können trotzdem zum Hellfeld gezählt werden, liefern jedoch nur wenige Informationen, da die Ermittlungen in vielen Fällen sehr schnell an ihre Gren-

[6]Betrügerischer Datenverarbeitungsmissbrauch.

[7]Siehe Abschn. 4. Fallbeispiel: Hellfeldanalyse von Cybercrime-Delikten.

zen stoßen. Somit muss auch bei den Ergebnissen innerhalb der Hellfelddaten der weitere Verlauf der Akten reflektiert werden.

Neben der Sekundärdatenanalyse gibt es auch in Bezug auf das Thema Cyber-Kriminalität die Möglichkeit qualitative Interviews durchzuführen. Eine große Herausforderung stellt hier jedoch das Verständnis der sehr technischen Fachsprache und des Fachwissens dar. Dieses kann sowohl beim Interview mit Opfern (bspw. Unverständnis der Fragestellung beim Opfer) wie auch mit Tätern (bspw. Unverständnis des Erzählten beim Interviewer) schwerwiegende Folgen für den Erkenntnisgewinn haben.

3.2.2 Erfassung von Dunkelfelddaten im Cybercrime

Da sich die Erfassung der Hellfelddaten bereits schwierig gestaltet, ist es selbstredend, dass Dunkelfelddaten noch schwieriger zu ermitteln sind. Grundsätzlich unterscheiden sich die Methoden zur Erfassung von Dunkelfelddaten im Bereich Cybercrime nicht von jenen in anderen Deliktsarten. Wie bereits im Abschn. 2.3.3. (Methoden zur Erforschung des Dunkelfelds) beschrieben, werden quantitative Befragungstechniken verwendet, um einerseits die Dunkelziffer zu ermitteln und andererseits Informationen zum kriminellen Verhalten zu generieren (siehe dazu unter anderen Bundeskriminalamt 2015b). Neben der schon geschilderten methodischen Problematik, ergeben sich darüber hinaus noch weitere Herausforderungen im speziellen Themenfeld Cybercrime.

So können Opfer bei einer Befragung nur über jene Fälle von Kriminalität berichten, welche sie selbst wahrgenommen haben. Speziell im Fall von Cyber-Kriminalität sind sich die Opfer ihrer Opferwerdung jedoch häufig gar nicht bewusst. Weitere problematische Aspekte sind, ähnlich wie beim qualitativen Interview, die Fachsprache und das Fachwissen. Nach Diekmann (2010) gibt es drei grundlegende Bedingungen die für die erfolgreiche Durchführung eines Interviews notwendig sind: die Kooperation der Befragten, die Norm der Aufrichtigkeit und die gemeinsame Sprache bzw. das gemeinsame Verständnis bestimmter Begrifflichkeiten. Dieser dritte Aspekt wird beim Thema Cyber-Kriminalität zur Herausforderung. Denn die Fachsprache rund um Cybercrime ist eine technische, in welcher Begriffe häufig nur in englischer Form existieren und keine bedeutungsgleiche Übersetzung ins Deutschsprachige erfahren. So ist es auch mit den Angriffsformen im Bereich Cybercrime, welche fast ausschließlich englische Bezeichnungen haben (Phishing, Ransomware, Spyware, usw.). Während manche diese Begriffe noch nie gehört haben, gibt es andere, die diese zwar kennen, sie jedoch unterschiedlich verstehen und deuten. Diese Sprachbarriere erschwert die Erfassung des Dunkelfelds, da es für die Vergleichbarkeit des Antwortverhaltens im Rahmen einer großflächigen

Befragung der allgemeinen Verständlichkeit bestimmter Begrifflichkeiten bedürfte.

3.2.3 Klassifizierung von Internet-Usern

Ein neuer methodischer Ansatz das Dunkelfeld näher zu beleuchten, wäre die Anwendung eines wissenschaftlich fundierten Gesellschaftsmodells mit bisher breiter kommerzieller Anwendung, dem Sinus-Milieus-Modell. Das ursprünglich aus dem Marketing stammende Modell diente zuerst der Produktentwicklung im Dienstleistungssektor. Das Modell geht davon aus, dass die Welt der sozialen Milieus in einer Gesellschaft ständig in Bewegung ist und sich laufend verändert. Zwar bleiben die milieukonstituierenden Merkmale, die Wertorientierungen der Menschen, auch in turbulenten Zeiten relativ konstant. Dennoch: Wenn sich die Gesellschaft fortentwickelt, wenn es Wertewandel gibt, bleibt das längerfristig nicht ohne Einfluss auf die Milieustruktur (Flaig und Barth 2014).

Mit Blick auf die oben angeführten bisherigen Methoden der Dunkelfeldforschung, kann davon ausgegangen werden, dass klassische soziodemografische Merkmale alleine nicht greifen, um zielgruppengerecht Cybercrime-Opfer zu identifizieren. Auf Basis des Sinus-Milieus Modells könnten eigene Kategorien sowie ein Ansatz für Mediennutzung mit Fokus auf Kriminalprävention und die Erfassung der Dunkelfeldziffer in Bezug auf Cybercrime-Delikte entwickelt werden.

4 Fallbeispiel: Hellfeldanalyse von Cybercrime-Delikten

Im Rahmen eines drittmittelfinanzierten Forschungsprojekts[8] erhoben die Autorinnen dieses Beitrages Hellfelddaten im Bereich der Cyber-Kriminalität. Die Forschungsergebnisse sind sehr umfassend und wurden in unterschiedlichen Kontexten publiziert (beispielsweise Huber et al. 2018, 2019). Dieses Kapitel fasst die zentralsten Ergebnisse der Hellfeldanalyse zusammen.

[8]Das Forschungsvorhaben „CERT-Komm II“ wurde im Rahmen des Österreichischen Sicherheitsforschungs-Förderprogramms KIRAS – einer Initiative des Bundesministeriums für Verkehr, Innovation und Technologie (BMVIT) – gefördert.

4.1 Einleitung und methodischer Ansatz

2017 stellte sich ein österreichisches Forschungsteam die Frage, welche Fälle von Cybercrime bis dato bereits einem Strafvollzug unterzogen wurden und welche nicht. Wie sieht der typische Cyber-Kriminelle aus? Wer sind die Opfer? Wie gestaltet sich der Tathergang (Modus Operandi)? Zur Beantwortung dieser Forschungsfragen wurde beim Wiener Straflandesgericht Antrag auf Akteneinsicht gestellt. Ziel war es, in zwei Schritten jene Akten zu analysieren, bei denen die Täter verurteilt wurden und jene, bei denen es keine Verurteilung gab. In einem ersten Schritt wurden alle Akten, die im Zeitraum von 2006–2016 unter den Sammelbegriff „Cybercrime“[9] fielen, erhoben. Dabei konnten 5404 Fälle gezählt werden. Berücksichtigt wurden alle Varianten von Cybercrime, also Delikte im engeren wie auch Delikte im weiteren Sinn.[10] Von der erfassten Grundgesamtheit von 5404 Fällen wurden nur 399 Fälle (N) letztendlich vom Gericht verhandelt. Auf Basis dieser 399 Fälle wurde eine repräsentative Stichprobe von 22 % (n) gezogen und ausgewertet.

Anschließend wurden in einem zweiten Schritt jene Fälle betrachtet, bei denen der Täter unbekannt war und jene, bei denen die Akten ausschließlich bei der Staatsanwaltschaft behandelt wurden. Dabei wurde eine inhaltliche Eingrenzung durchgeführt, sodass alle Fälle des Identitätsdiebstahls sowie Akten, die aus unterschiedlichen Gründen nicht zugänglich waren, aus der Analyse ausgeschlossen wurden. Dies ergab eine Grundgesamtheit von (N) 2720 von jenen Fällen, bei denen es zu keiner Verurteilung kam. Aus den Akten wurde eine repräsentative Zufallsstichprobe (n = 20 %) mittels Listenauswahl gezogen.

Zur Analyse der Akten wurde eine quantitative Aktenanalyse nach Dölling (1984) herangezogen. Zur Ermittlung des Modus Operandi wurde der Tathergang qualitativ nach Mayring (2000) ausgewertet. Der Zeitraum, in dem die Datenerhebung durchgeführt wurde, erstreckte sich von Jänner bis Juni 2017.

---

[9]Paragraphen unter dem Bereich ‚Cybercrime‘ im österreichischen StGB (Strafgesetzbuch) gelistet: §§ 118a Widerrechtlicher Zugriff auf ein Computersystem, 119 Verletzung des Telekommunikationsgeheimnisses, 119a Missbräuchliches Abfangen von Daten, 126a Datenbeschädigung, 126b Störung der Funktionsfähigkeit eines Computersystems, 126c Missbrauch von Computerprogrammen, 148a Betrügerischer Datenverarbeitungsmissbrauch sowie 225a Datenfälschung.

[10]Delikte der pornographischen Darstellung Minderjähriger sowie der Anbahnung von Sexualkontakten zu Unmündigen fanden keine Berücksichtigung.

4.2 Die Fälle mit anschließender Gerichtsverhandlung

4.2.1 Der typische Cyber-Kriminelle

Bei der statistisch-idealtypischen Betrachtung der demografischen Merkmale der Täter[11] zeigt sich, dass diese meist männlich (75 %) und zwischen 21 und 30 Jahre alt sind (36 %). Die meisten Täter sind in Österreich (47 %) oder in einem anderen EU-Land (25 %) geboren.[12] Das Bildungsniveau der Täter ist abhängig von der Komplexität des verübten Delikts. Allgemein kann jedoch festgestellt werden, dass in Bezug auf die verurteilten Fälle der Bildungsstand zumeist gering ist. 54 % der Täter haben einen Pflichtschulabschluss oder eine Lehre, rund 12 % besitzen einen Abschluss mit Matura (Abitur) und nur 8 % weisen einen höheren Bildungsabschluss auf.

Anhand einer Clusteranalyse wurde eine Typisierung[13] von Cyber-Kriminellen nach demografischen Merkmalen vorgenommen:

- *Typ 1: Der Business-Man:* Dieser Typ umfasst rund ein Drittel (31 %) der Fälle und ist gänzlich männlich. Der Business-Man besitzt unter allen Profilen den höchsten Bildungsabschluss (30 % Fachhochschul- oder Universitätsabschluss) und geht typischerweise einer regulären Beschäftigung nach (52 %). Das durchschnittliche Alter dieses Täter-Typs liegt bei rund 35 Jahren. Typisch für dieses Profil sind gute bis sehr gute Kenntnisse im Bereich der IT-Anwendungen, der IT-Security und/oder Informatik. Zwischen Täter und Opfer besteht zumeist ein berufliches Verhältnis oder ein Bekanntschaftsverhältnis.

[11]Der Täterbegriff wird in diesem Fall nur angewendet, wenn es zu einer Verurteilung durch das Gericht kam. Sonst wird von Tatverdächtigen und/oder Angeklagten gesprochen.

[12]Es sollte bei Betrachtung dieses Ergebnisses jedoch berücksichtigt werden, dass die Datenbasis aus jenen Fällen besteht, bei denen es eine rechtswirksame Verurteilung in Wien gab. Das Ergebnis lässt daher nicht den Umkehrschluss zu, dass es keine Täter aus Drittstaaten gibt. Außerdem ist von einem Zusammenhang zwischen dem Aufenthaltsland des Täters und der Aufklärungsquote des Deliktes auszugehen.

[13]Die Clusterqualität liegt mit 0,4 im Durchschnitt. Das Modell weist damit eine mittelmäßige Qualität auf. Wird der Prädikatoren-Einfluss betrachtet, ist erkennbar, dass die Variable Geschlecht mit 100 % am stärksten in die Typenbildung miteinbezogen wurde. Danach folgen mit 52 % die Variable Bildung, mit 35 % die Variable Beschäftigungsverhältnis und mit 10 % die Variable Alter.

- *Typ 2: Die Hausfrau:* Die zweite Gruppe umfasst rund ein Fünftel aller Fälle (18 %) und besteht zu 100 % aus Frauen. Der Bildungsstatus ist eher gering (50 % unter Matura-Niveau) und einer Beschäftigung wird typischerweise nicht nachgegangen (63 %). Ein großer Anteil dieser Personen ist in sonstigen Anstellungsverhältnissen (beispielsweise Karenz, Pension usw.). Dieser Täterinnen-Typ ist rund 32 Jahre alt und nutzt aus einem finanziellen Motiv heraus eine bestehende Schwachstelle aus. Darüberhinausgehende Fähigkeiten in der IT-Security bzw. der Informatik sind nicht vorhanden.
- *Typ 3: Der Perspektivlose:* Der Perspektivlose stellt den dritten Typ und auch die größte Gruppe an Tätern (51 %) dar. Personen dieses Typs sind ausschließlich männlich und haben in jedem Fall einen geringen Bildungsabschluss (Pflichtschule oder Lehre) sowie keine reguläre Beschäftigung. Die Täter sind im Durchschnitt 30 Jahre alt und haben Großteils eine Vorstrafe (57 %). Der Perspektivlose ist typischerweise ein durchschnittlicher IT-Anwender, der keine speziellen Kenntnisse im Informatiksektor hat und aus dem Motiv der finanziellen Bereicherung agiert.

Neben der statistischen Typenbildung anhand der Cluster-Analyse lassen sich weitere Themen in Bezug auf die Charakterisierung von Cyber-Kriminalität formulieren:

- *Bildung und Motivation:* In den aufgeklärten Fällen von Cybercrime gibt es einen klaren Zusammenhang zwischen der Komplexität des Verbrechens und den Kenntnissen des Täters in Bezug auf IT-Security bzw. Informatik.
- *Beschaffungskriminalität:* Die Ergebnisse der Studie lassen den Schluss zu, dass einige der Täter ihre Straftaten verübten, um eine Sucht zu finanzieren. Dabei wurden Fälle von Spielsucht als häufigste Suchterkrankung genannt, gefolgt von der Alkoholsucht und Drogensucht.
- *Formation:* Die Ergebnisse der Studie zeigen, dass mehr als die Hälfte der Täter aus einer Gruppe heraus agiert. Die Gruppe basiert auf familiären und solidarisierenden Strukturen (beispielsweise gemeinsames Herkunftsland). Es ist davon auszugehen, dass es sich auch um mafiöse Verbindungen handelt.

4.2.2 Wie gestaltet sich der Tathergang (Modus Operandi)?

Die Differenzierung des Tathergangs stellt eine besondere Herausforderung dar, da es je nach Technologieentwicklung und Kreativität der Täter unterschiedlichste Muster gibt. Nicht der Paragraph, nach dem Anklage erhoben wird, bestimmt den Modus Operandi, sondern unterschiedliche Facetten des Verbrechens. Im Rahmen einer qualitativen Analyse des Tathergangs wurden

verschiedene Dimensionen[14] zur Beschreibung des Modus Operandi herangezogen: Auf dieser Basis konnten sechs unterschiedliche Typen ermittelt werden:

- *Typ 1: Technische Hilfsmittel:* Die Täter verfügen über einen hohen Wissensstand zur Funktionsweise von IT-Security und nutzen technisch komplexere Angriffsarten sowie Verschleierungsmaßnahmen. Bei dieser Vorgehensweise wählen die Täter ihr Opfer meist zielgerichtet oder skalpellartig und agieren aus den Motiven heraus, jemandem bewusst Schaden zu wollen sowie finanziellen Gewinn zu erbeuten.
- *Typ 2–5: Identitätsdiebstahl:* Der Identitätsdiebstahl ist in Österreich die mit Abstand häufigste Form von Cybercrime. Unter dieser Vorgehensweise subsumieren sich unterschiedliche Ausprägungen, wie die ‚illegale Überweisungen', ‚illegale Verwendung von Bank- und Kreditkarten', ‚Verwendung einer illegalen Identität zum Zwecke des Glückspiels' sowie ‚illegales Online-Shopping'. Die Täter finden sich in allen sozialen Schichten, Altersklassen und Geschlechtern. Die Planung von Identitätsdiebstählen ist meist banal und erfolgt aus finanziellen Motiven heraus.
- *Typ 6: Datenmissbrauch bei Firmen:* Im Rahmen der Tathandlung missbrauchen Personen bewusst ihr Wissen oder ihre Berechtigungen in einem Unternehmen, um sich dadurch einen Vorteil zu verschaffen bzw. um das Unternehmen bewusst zu schädigen. Diese Fälle sind komplexer in der Planung und erfordern eine Strategie. Typischerweise werden Daten einer Firma gestohlen, gelöscht, verändert oder weitergegeben.
- *Typ 7: Schwachstellenausnutzung:* Allgemeines Muster bei Fällen dieses Modus Operandi ist, dass der Täter bei einer Firma eine systematische oder eine IT-Schwachstelle erkennt und zum eigenen Vorteil ausnutzt. Um solche Taten zu begehen, muss der Täter die Schwachstelle erst ausmachen, was häufig durch Zufall oder die Trial-Error-Methode passiert.
- *Typ 8: Fälschung:* Die Fälschung an sich ist ein offline Delikt, mit den neuen Methoden der digitalen Bildverarbeitung hat es jedoch auch Einzug in die Computerkriminalität gefunden. Fälschungsdelikte erfordern Planung und

[14]Häufigkeit: n = (Anzahl der Akten), Cybercrime-Art: Cybercrime im engeren Sinn, Cybercrime im weiteren Sinn, Täter: Merkmalsträger, Opfer: Merkmalsträger, Komplexität: leicht – mittel – schwierig, Motiv: extrinsisch vs. intrinsisch, Beziehungsstatus: zwischen Täter und Opfer, Opferwahl: nicht zielgerichtet, zielgerichtet, skalpellartig, Methode: Merkmalsträger, Technik: Merkmalsträger.

strategisches Denken sowie gute Kenntnisse in der Bildverarbeitung. Oft werden ganze Lebensläufe und die dazu gehörigen Dokumente gefälscht, um sich den gewünschten Vorteil zu verschaffen.

- *Typ 9: Rache:* Unter den Fällen, die eine gerichtliche Verurteilung zur Folge hatten, weist dieser Modus Operandi eine Sonderstellung auf. Im Vordergrund steht hier die konkrete Motivation der Rache, die in der Umsetzung mit anderen Modi Operandi verknüpft sein kann. Großes Unterscheidungsmerkmal für die Typisierung ist die bewusste Planung der Tat als Racheakt. In einigen Fällen kann die Tat auch als eine Ausweitung des Cyberstalkings betrachtet werden.

4.3 Die ungelösten Fälle

Im folgenden Abschnitt werden die typischen Tathergangsmuster bzw. -motive der ungelösten Cybercrime-Fälle des Wiener Straflandesgerichts erläutert. Wie in der Methode bereits illustriert, ist auch hier von einem großen Ausmaß an Identitätsdiebstahl auszugehen. Der Fokus dieser Analyse lag jedoch auf den darüberhinausgehenden Modi Operandi. Es konnten folgende Muster festgestellt werden.

4.3.1 Revenge-Crime

Rund 43 % aller Fälle können unter diesen Typ subsumiert werden. Augenfällig ist, dass es zahlreiche Anzeigen in diesem Bereich gibt, diese aber nur zu wenigen Verurteilungen führen. Cybercrime wird in diesem Fall bewusst eingesetzt, um sich an einer Person oder Firma zu rächen. Dafür werden Informationen, die aus einem Vertrauensverhältnis gewonnen wurden, gegen das Opfer eingesetzt. Die Komplexität der Delikte ist somit eher gering. Aufgrund der zunehmenden Digitalisierung der unterschiedlichen Lebensbereiche ist die Überschneidung des Typs Revenge-Crime mit Delikten des Stalkings groß.

4.3.2 Financial Crime

Rund ein Drittel aller Fälle (29 %) ist der Kategorie „Financial-Crime“ zuzuordnen. Die meist in kleinen kriminellen Organisationen agierenden Tatverdächtigen haben als primäres Ziel, sich finanziell zu bereichern. Typischerweise besteht keine Beziehung zwischen dem Tatverdächtigen und dem Opfer, welche sowohl Privatpersonen als auch Firmen sein können. Tatverdächtige dieses Typs wollen mit möglichst wenig Aufwand einen möglichst hohen finanziellen Ertrag erzielen. Die Schwachstelle ist meist die Leichtgläubigkeit bzw. Unwissenheit des Opfers.

4.3.3 Show-Off-Crime

Der Typ „Show-Off Crime“ umfasst 12 % der analysierten Fälle. Die Tatverdächtigen möchten ihre Fähigkeiten und die damit einhergehenden Möglichkeiten demonstrieren. Sie greifen in erster Linie Behörden oder Firmen mit hoher Sichtbarkeit an, da sie möglichst große Aufmerksamkeit erregen möchten. Die Tatverdächtigen verfügen im Normalfall über fundiertes Wissen zu IT-Technologien, welches sie durch eine Ausbildung erhielten oder sich selbst aneigneten. Von Tool-basierten Angriffsformen bis hin zu Distributed-Denial-of-Service (DDoS-) Attacken werden unterschiedliche Verfahren angewendet.

4.3.4 Conviction Crime

5 % aller Fälle können unter den Typ des „Conviction Crime“ subsumiert werden. Tatverdächtige dieses Typs handeln in Gruppierungen der gleichen Gesinnung und haben das Motiv, ihren Glauben bzw. ihre Ideologie mit Hilfe von cyber-kriminellem Verhalten zu verbreiten. Sie sind vor allem auf der Suche nach geeigneten Plattformen wie Homepages und attackieren diese mit dem Ziel, damit ihre eigene Botschaft verbreiten zu können.

4.3.5 Follower Crime

Der Typ des „Follower-Crime“ ist eher selten (rund 4 %) und tritt häufig in Verbindung mit dem Typ des Show-Off Crime auf, denn Tatverdächtige des Typs Show-Off Crime teilen die widerrechtlich erlangten Zugangsdaten und Informationen zur Straftat häufig in sozialen Netzwerken. Der Tatverdächtige des Follower Crime ist ein Nachfolgetäter; er begeht aus Neugierde oder aus einem fehlenden Bewusstsein heraus mit ebendiesen Informationen eine Straftat. Diese ist demnach weder zielgerichtet noch komplex und erfordert keine speziellen IT-Security-Kenntnisse.

5 Fazit

Der Blick auf die Cybercrime-Fälle von 2006–2016 in Wien ist ernüchternd. Trotz der stetig steigenden Anzahl an Anzeigen, ist die Aufklärungsquote äußerst gering. Darüber hinaus kann im Vergleich zu anderen Kriminalitätsdelikten kein eindeutiger Zusammenhang zwischen dem Modus Operandi und den angeklagten Paragraphen festgestellt werden. Zu Verurteilungen kommt es am häufigsten bei Delikten des Identitätsdiebstahls, wobei es sich bei diesen zum großen Teil um Delikte handelt, die viele Offline-Komponenten enthalten und weniger komplex sind. Der eindeutige Trend geht in Richtung einer Verlagerung dieser

Kleinkriminalität in den Cyberspace. Täter und Tatverdächtige benötigen für diese Art von Cyber-Kriminalität zumeist keine speziellen IT-Kenntnisse und nutzen ihr Insiderwissen um Schwachstellen, Vertrauensbeziehungen sowie grundlegende IT-Anwender Kenntnisse um die Delikte zu begehen.

Delikte des High-Tech-Crime, also jene die spezielle Informatikkenntnisse und eine Auseinandersetzung mit der Materie voraussetzen, wie beispielsweise das Versenden von Malware oder großflächige Cyber-Attacken (DDoS-Attacken, Crime as a Service, usw.) werden nur in sehr geringer Zahl aufgeklärt. Ein Grund dafür ist, dass eine Vielzahl der Angriffe nicht rückverfolgt werden kann.

Dieser Umstand führt zu einem fehlenden Wissen über das Vorgehen von Cyber-Kriminellen, welches durch das hohe Dunkelfeld in diesem Bereich noch verstärkt wird. Cybercrime ist die Kriminalitätsform mit der – so die Vermutungen – mit Abstand höchsten Dunkelziffer. Um dies zu ändern, müsste an den Stadien von der Klassifizierung bis zur Registrierung[15] angesetzt werden. Dazu müsste 1) der Anreiz zur Durchführung der kriminellen Handlung gemildert, 2) die Wahrnehmung der Bevölkerung geschult, 3) die Hemmnisse einer Strafanzeige gesenkt und 4) die Ermittlungen der Staatsanwaltschaft ausgebaut werden. Mögliche Schritte, um diese Entwicklungen zu erreichen, wären grundlegende Veränderungen im Sozialsystem, der Ausbau von Bewusstsein und Wissensstand der Bevölkerung sowie eine spezielle Weiterbildung der Fachkräfte, die mit dem Thema Cybercrime befasst sind, und eine Harmonisierung des internationalen Rechtsrahmens. Besonders was die Wahrnehmung und die Anzeigebereitschaft betrifft, ist jedoch ein grundlegendes Umdenken in Hinblick auf die Verantwortung eines jeden Einzelnen notwendig.

Literatur

Brenner, S. W. (2006). Cybercrime jurisdiction. *Crime, Law and Social Change, 46*(4–5), 189–206.

Bundeskriminalamt. (2015a). Hacktivisten. Abschlussbericht zum Projektteil der Hellfeldbeforschung. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/Forschungsergebnisse/2015HacktivistenProjektteilHellfeldbeforschung.pdf?__blob=publicationFile&v=3. Zugegriffen: 24. Apr. 2019.

Bundeskriminalamt. (2015b). Hacktivisten. Ergebnisbericht Online-Befragung. Projektteil Dunkelfeld. https://cdn.netzpolitik.org/wp-upload/2016HacktivistenProjektteilDunkelfeldOnlineBefragung.pdf. Zugegriffen: 24. Apr. 2019.

[15]Siehe dazu Abschn. 2.2. Beschreibung am Verlauf der Registrierung.

Bundeskriminalamt. (2019a). PKS 2018 – Standard Übersicht Falltabellen. https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2018/Standardtabellen/standardtabellenFaelle.html?nn=108686. Zugegriffen: 6. Juni 2019.

Bundeskriminalamt. (2019b). Die Polizeiliche Kriminalstatistik 2018. Österreich ist so sicher wie noch nie. https://bundeskriminalamt.at/501/files/PKS_18_Broschuere.pdf. Zugegriffen: 6. Juni 2019.

Bundesministerium für Inneres Österreich (Bundeskriminalamt). (n.d.). Angezeigte Fälle von Cybercrime in Österreich von 2004 bis 2017. Statista – Das Statistik-Portal. https://de-1statista-1com-167jz42nt037e.han3.donau-uni.ac.at/statistik/daten/studie/294141/umfrage/cybercrime-in-oesterreich/. Zugegriffen: 24. Apr. 2019.

Bureau of Justice Statistics. (n. d.). Data Collection: National Crime Victimization Survey (NCVS). https://www.bjs.gov/index.cfm?ty=dcdetail&iid=245. Zugegriffen: 6. Juni 2019.

Csonka, P. (2004). The Council of Europe Convention on cyber-crime: A response to the challenge of the new age? In G. Ilarda & G. Marullo (Hrsg.), *Cybercrime: Conferenza internazionale. La Convenzione del Consiglio d'Europa sulla Criminalità Informatico* (S. 3–29). Milano: Giuffrè.

Diekmann, A. (2010). *Empirische Sozialforschung. Grundlagen, Methoden, Anwendungen*. Reinbek bei Hamburg: Rowohlt Taschenbuch.

Dölling, D. (1984). Probleme der Aktenanalyse in der Kriminologie. In H. Kury (Hrsg.), *Methodologische Probleme in der kriminologischen Forschungspraxis* (S. 265–286). Köln: C. Heymanns.

Durkheim, E. (1979). Kriminalität als normales Phänomen. In F. Sack & R. König (Hrsg.), *Kriminalsoziologie* (3. Aufl.). Wiesbaden: Akademische Verlagsgesellschaft.

Flaig, B. B., & Barth, B. (2014). Die Sinus-Milieus® 3.0 – Hintergründe und Fakten zum aktuellen Sinus-Milieu-Modell. In M. Halfmann (Hrsg.), *Zielgruppen im Konsumentenmarketing* (S. 105–120). Wiesbaden: Springer Gabler.

Huber, E., Pospisil, B., Hötzendorfer, W., Quirchmayr, G., Löschl, L., & Tschohl, C. (2018). *Die Cyber-Kriminellen in Wien: Eine Analyse von 2006–2016*. Krems an der Donau: Edition Donau-Universität Krems.

Huber, E., Pospisil, B., Hötzendorfer, W., Löschl, L., Quirchmayr, G., & Tschohl, C. (2019). Without a Trace – Die ungeklärten Cybercrime-Fälle des Straflandesgerichts Wien. In E. Schweighofer, F. Kummer, & A. Saarenpää (Hrsg.), *Internet of Things. Tagungsband des 22. Internationalen Rechtsinformatik Symposions IRIS 2019* (S. 573–580). Bern: Editions Weblaw.

ITU. (n. d.). Anteil der Internetnutzer weltweit in den Jahren 2005 bis 2017 sowie eine Schätzung für das Jahr 2018. Statista – Das Statistik-Portal. https://de.statista.com/statistik/daten/studie/805943/umfrage/anteil-der-internetnutzer-weltweit/. Zugegriffen: 25. Apr. 2019.

Kersting, S., & Erdmann, J. (2015). Analyse von Hellfelddaten – Darstellung von Problemen, Besonderheiten und Fallstricken anhand ausgewählter Praxisbeispiele. In S. Eifler & D. Pollich (Hrsg.), *Empirische Forschung über Kriminalität* (S. 9–29). Wiesbaden: Springer.

Kirwan, G., & Power, A. (2013). *Cybercrime: The psychology of online offenders*. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511843846.

Kshetri, N. (2010). *The global cybercrime industry: Economic, institutional and strategic perspectives*. Heidelberg: Springer. https://doi.org/10.1007/978-3-642-11522-6.

Kunz, K. L., & Singelnstein, T. (2016). *Kriminologie. Eine Grundlegung* (7. Aufl.). Bern: Haupt.

Mayring, P. (2000). Qualitative content analysis. *Forum Qualitative Sozialforschung/Forum Qualitative Social Research, 1*(2), Art. 20. http://www.qualitative-research.net/index.php/fqs/article/view/1089/2385.

McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. Research Report 75. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf. Zugegriffen: 24. Apr. 2019.

Morris, S. (2004). The future of netcrime now: Part 1 – Threats and challenges. Home Office Online Report, 62/04. Crown. https://globalinitiative.net/wp-content/uploads/2017/12/Home-Office-The-future-of-netcrime-now-Part-1-%E2%80%93-threats-and-challenges-1.pdf. Zugegriffen: 24. Apr. 2019.

Popitz, H. (1968). *Über die Präventivwirkung des Nichtwissens: Dunkelziffer, Norm und Strafe*. Tübingen: Mohr.

Prätor, S. (2015). Ziele und Methoden der Dunkelfeldforschung. Ein Überblick mit Schwerpunkt auf Dunkelfeldbefragungen im Bereich der Jugenddelinquenz. In S. Eifler & D. Pollich (Hrsg.), *Empirische Forschung über Kriminalität* (S. 9–29). Wiesbaden: Springer.

Quételet, A. (1869). *Soziale Physik oder Abhandlung über die Entwicklung der Fähigkeiten des Menschen*. Jena: Gustav Fischer.

Roll, H. (2017). Erste Untersuchung zum Dunkelfeld der Kriminalität in Mecklenburg-Vorpommern. Abschlussbericht. www.fh-guestrow.de/doks/forschung/dunkelfeld/Abschlussbericht_2017_11_05.pdf. Zugegriffen: 24. Apr. 2019.

Schneider, H. J. (1993). *Einführung in die Kriminologie* (3. Aufl.). Berlin: De Gruyter.

Schwind, H. D. (2013). *Kriminologie – Eine praxisorientierte Einführung mit Beispielen* (22. Aufl.). Heidelberg: Kriminalistik & HJR-Verlag.

Symantec. (2017). Finanzieller Schaden durch Internetkriminalität in ausgewählten Ländern weltweit im Jahr 2017 (in Milliarden US-Dollar). Statista – Das Statistik-Portal. https://de.statista.com/statistik/daten/studie/802737/umfrage/finanzieller-schaden-durch-cybercrime-nach-laendern-weltweit/. Zugegriffen: 25. Apr. 2019.

United Nations Office on Drugs and Crime (UNODC) Vienna. (2013). Comprehensive Study on Cybercrime. Draft. http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. Zugegriffen: 24. Apr. 2019.

Strafverfolgung digital

Ohnmacht im Netz oder wirkungsvolles Instrument?

Dirk Kunze

1 Die Entstehungsgeschichte der Internetfahndung in NRW

Bereits im Jahr 2007 richtete das Land Nordrhein-Westfalen in der damaligen Analyse- und Auswerteabteilung des Landeskriminalamtes Nordrhein-Westfalen (LKA NRW) nach Bayern die Zentrale Internetrecherche (ZIR) zur anlassunabhängigen Recherche ein – die Streife im Internet war in NRW geboren (Verlag Deutsche Polizeiliteratur 2016). Was zunächst intern scherzhaft und auch abwertend als „*Streife in Second Life*“[1] und „*Bewachen von Linden Dollars*[2]“ bezeichnet wurde, zeigte frühzeitig seine Bezüge zur Realität. Bereits 2007 führte die Staatsanwaltschaft Halle ein Ermittlungsverfahren wegen des Verdachts des Verbreitens kinderpornografischer Schriften in Second Life (Der Spiegel 2007). Hier entwickelte sich schnell eine hohe Kompetenz. Ziel war und ist nicht nur das Entdecken und Verfolgen von Straftaten, sondern vielmehr auch das Erkennen und Abwehren von Gefahren im Internet. Insbesondere das frühzeitige Erkennen von Gefahrenlagen wie Amokandrohungen und Suizidankündigungen und das Treffen von Maßnahmen zum Schutz von Leib und Leben waren Ziele der ZIR.

[1]Second Life – Online Rollenspiel https://secondlife.com/?lang=de-DE.

[2]Virtuelle Währung in Second Life mit realen Gegenwerten und Wechselkursen.

D. Kunze (✉)
Landeskriminalamt NRW, Düsseldorf, Deutschland
E-Mail: dirk.kunze@polizei.nrw.de

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

T.-G. Rüdiger und P. S. Bayerl (Hrsg.), *Cyberkriminologie,*
https://doi.org/10.1007/978-3-658-28507-4_5

Bereits im Jahr 2003, ein Jahr nach dem Amoklauf am 26. April 2002 am Erfurter Gutenberg-Gymnasium, konnten durch den damals im Kriminaldauerdienst des Polizeipräsidiums Köln eingesetzten Autor die beiden Urheber einer Amokdrohung gegen eine Abiturfeier in Köln ermittelt und in Gewahrsam genommen werden. Das Identifizieren der hinter einem Pseudonym verborgenen Täter, das Ermitteln der IP-Adressen, der genutzten E-Mail-Accounts und das Personifizieren der handelnden Personen konnte nur durch beharrliches Nachhaken bei Forenbetreibern gelingen. Die besondere Herausforderung dabei war eine fehlende spezialgesetzliche Ermächtigungsgrundlage im Bereich der Gefahrenabwehr.

Was damals basierend auf Einzelwissen umgesetzt werden konnte, wurde mit Einrichtung der ZIR zum Standard. Mehrere Länder folgten dem Beispiel. Bereits früh erkannte man, dass im Online-Zeitalter nur ein koordiniertes Vorgehen erfolgversprechend sein könne (Schulzki-Haddouti 1998), um eine doppelte Bearbeitung von Sachverhalten zu vermeiden. Nachdem das Bundeskriminalamt zunächst die „Zentralstelle für anlaßunabhängige Recherche in Datennetzen“ (ZaRD) eingerichtet hatte (Nolde 2003), ging aus dieser die „Koordinierungsstelle für anlassunabhängige Recherchen im Internet“ (KaRIn) hervor.

2 Schwerpunktbereiche der Internetfahndung

Basierend auf den Erfahrungen der ZIR wurde im LKA NRW beginnend im Oktober 2016 die Konzeption zur Aufstellung des „Cyber-Recherche- und Fahndungszentrums“ (CRuFz) vorangetrieben. Ausgehend von der Fragestellung, ob Diebesgut aus Wohnungseinbruchsdiebstählen im Internet erfolgversprechend verfolgt, die Hehler und letztendlich darüber die Einbrecher ermittelt werden könnten, wurde in einem partizipativen Prozess der Mitarbeiterbeteiligung in einer Fokusgruppendiskussion nach DACUM (Institut für berufliche Bildung, Arbeitsmarkt- und Sozialpolitik 2018) ein umfassendes Tätigkeitsbild erhoben und die Aufgaben beschrieben. Dabei konnten deutlich vier Schwerpunkte herausgearbeitet werden:

1. Der personenzentrische Ansatz
2. Der sachbezogene Ansatz
3. Die Unterstützungsleistungen
4. Ermittlungskommissionen (die bisher neben der ZIR im gleichen Dezernat geführt wurden)

Dabei wurden die Ausrichtungen der Bereiche so gewählt, dass spätere neue Phänomene oder neue politische Schwerpunkte eine Anpassung der Aufgabenbeschreibung ermöglichten, ohne Organisationsänderungen nach sich zu ziehen.

2.1 Der personenzentrische Ansatz

Ausgehend von den Überlegung der besten organisatorischen Gestaltung wurden mögliche Unterschiede in den einzelnen Phänomenbereichen beleuchtet. Insbesondere im Deliktsfeld der politisch motovierten Internetkriminalität und der Verbreitung kinderpornografischen Materials sowie der Annäherungsdelikte ist, basierend auf den erhobenen Erfahrungen, zunächst eine meist unbekannte Person und deren Handeln die feststellbare Komponente. Von diesen Ausgangspunkten sollen hier die Tat, Opfer, Täter und Tatmittel und Modus Operandi aufgeklärt und dokumentiert werden. Auch Staatsschutz- und Meinungsdelikte werden hier verfolgt. Spezielle Konzepte gegen besondere Phänomene werden hier erarbeitet, auf Praxistauglichkeit hin überprüft und umgesetzt. Ein Beispiel hierfür ist ein Konzept zur Bekämpfung von Cybergrooming, dass sowohl auf den Opferschutz als auch auf die Ermittlung und das Ergreifen der Täter abzielt. Hier sind den Ermittlern häufig durch die fehlende Strafbarkeit von Annäherungsdelikten oder deren Versuche Grenzen gesetzt. Hier wird in enger Zusammenarbeit mit der Justiz bestehender Rechtsetzungsbedarf beschrieben.

2.2 Der sachbezogene Ansatz

Im Unterschied zum personenzentrischen Ansatz ist der Ausgangspunkt der Ermittlungen hier eine auf Sachen ausgerichtete Handlung, ein Gegenstand oder etwas Vergleichbares. Insbesondere der Handel mit Betäubungsmitteln, Waffen und anderen inkriminierten Gütern sowie Verstöße gegen das Arzneimittelgesetz sind hier Gegenstand der Ermittlungen. Auch die zunächst für die Einrichtung des CRuFz ausschlaggebende Fragestellung nach dem Auffinden entwendeten Diebesgutes im Internert wird hier bearbeitet. Hier wird zum Beispiel in Zusammenarbeit mit den Herstellern von Spielekonsolen die Frage untersucht, wie diese für Diebe unattraktiv gemacht werden können.

2.3 Unterstützungsleistungen

Wissenschaftliche Unterstützung mit Methodik und speziellem Analyse- und Auswertewissen, gepaart mit der Entwicklung von Werkzeugen für die Aufgaben des CRuFz, die Marktsichtung und Erprobung existierender Werkzeuge prägen den Alltag dieser Dienststelle. So wird hier z. B. gemeinsam mit der Wirtschaft derzeit ein Werkzeug zur Video- und Bildanalyse digitaler Asservate zum Erkennen von Waffen, Fahrzeugen und Symbolen verfassungsfeindlicher Organisationen entwickelt. Für die Polizei Nordrhein-Westfalen wurde zudem eine einheitliche Oberfläche für das Durchführen Open Source Intelligence-Maßnahmen (OSINT Horizon) geschaffen, die den Datenschutz- und IT-Sicherheitsrichtlinien entspricht und einheitliche Standards ermöglicht.

2.4 Ermittlungskommissionen

Die Ermittlungskommissionen bearbeiten grundsätzlich herausragende Delikte von Cybercrime im engeren Sinne, insbesondere Wirtschaftsspionage, Angriffe auf Firmen und Behörden und mit besonders herausragendem technischen Sachverstand ausgeführte Angriffe. Daneben stellen die Ermittlungskommissionen die Critical Incident Response Group (CIRG) des LKA NRW. Diese übernimmt die ersten Ermittlungen bei Cyberangriffen vor Ort, inbesondere bei Angriffen auf kritische Infrastrukturen und ähnlich schwerwiegende Angriffe. Sofern große Firmen wie Energieversorger und DAX-Konzerne betroffen sind, trifft die CIRG häufig die ersten Maßnahmen. Der Aufbau von Vertrauen und die Geheimhaltung dieser Ermittlungen insbesondere zum Schutz der Geschädigten genießen höchste Priorität.

2.5 Zusammenwirken

Häufig verschwimmen die Grenzen der Phänomene und Zuständigkeiten sind nicht eindeutig oder verlagern sich. So konnten die Spezialisten im personenzentrierten Ansatz Hinweise auf ein Forum zur Verbreitung von kinder- und jugendpornografischer Schriften erlangen. Im Rahmen der Ermittlungen identifizierten die Ermittler ein potenzielles Opfer und die Person, die den Übergriff plante. Durch die Lokalisierung der Personen durch OSINT-Recherchen konnten örtliche Polizeikräfte gefahrenabwehrende Maßnahmen einleiten und den Übergriff verhindern. In diesem Zusammenhang konnten auch deutsche Kinder als Geschädigte eines sexuellen Missbrauchs durch deutsche Täter auf Mallorca

identifiziert und lokalisiert und die Informationen den spanischen Behörden zugeleitet werden. Daneben wurden Hinweise auf einen Waffenhandel entdeckt, die durch die Mitarbeitenden der Sachfahndung weiter verfolgt wurden. In Zusammenarbeit mit den Ermittlungskommissionen als operativer Einheit konnte der Verkäufer ermittelt und festgenommen werden.

In beiden Fällen ist natürlich das Ziel, die dahinter liegenden Strukturen zu zerschlagen. So führen die Ermittlungskommissionen gemeinsam mit den phänomenbezogenen Ermittlern im Anschluss häufig Ermittlungen gegen die Betreiber solcher Plattformen, die oft auch in einer bundesweiten oder weltweiten Kooperation münden, wie zum Beispiel bei den Ermittlungen gegen die Betreiber des Undergroundeconomy-Forums „Crimnetwork.biz“.

3 Kriminalitätsformen im Darknet und Surfaceweb

3.1 Clearweb

Das Internet, wie wir es beim Öffnen des Browsers sehen, stellt nur einen äußerst geringen Teil dar, das sogenannte Surface-Web oder auch Clearweb. Das Clearweb sind die Bereiche, die öffentlich zugänglich und durch Suchmaschinen indizierbar sind, also für jederman zugänglich. Dem Clearweb werden lediglich ca. 6 % des gesamten Internet zugerechnet.

3.2 Deepweb

Das Deepweb ist dem gegenüber der Bereich des Internets, der nicht indizierbar und somit nicht ohne Weiteres auffindbar ist, weil zum Beispiel eine Anmeldung erforderlich ist, z. B. in Foren. Das Deepweb macht ca. 90 % des Internet aus. Auch große Teile der sozialen Medien – die Teile, die erst nach dem Registrieren, Anmelden oder Beitreten zu einer Gruppe sichtbar sind – zählen zum Deepweb (s. a. Kap. „Darknet – die dunkle Seite des Internets?“).

3.3 Darknet

Das Darknet stellt mit seinen ca. 4 % den kleinsten Teil dar. Das Darknet ist der Teil des Internets, der nur mithilfe bestimmter Verschlüsselungsmechanismen, Browser und Kenntnis der Zieladresse nutzbar ist. Das TOR-Netzwerk ist der bekannteste Teil des Darknet.

Ein besonderer Fokus auf das Darknet wurde nach dem Amok-Lauf eines 18-Jährigen in München am 22. Juli 2016 gelegt. Nach Ermittlungen des Zollfahndungsamtes Frankfurt am Main hatte dieser sowohl die Tatwaffe als auch die Munition bei einem 31-jährigen Deutschen im Darknet gekauft (Zollfahndungsamt Frankfurt am Main 2016). Dabei wurden auch die Ermittlungsschritte dargelegt, die zur Ergreifung des 31-jährigen Waffenhändlers geführt hatten. Der spätere Amok-Täter hatte im Rahmen seiner Versuche, eine Waffe zu erwerben, auch mit Internetfahndern des Zollfahndungsamts Frankfurt am Main gechattet. Ebenso wurde der Verkäufer der Waffe auf diese Weise identifiziert (Förster 2017). Auch der Betreiber des Forums, über das die Waffe gehandelt wurde – Deutschland im Deepweb (DiDW) – wurde nach umfangreichen Ermittlungen zu einer sechsjährigen Haftstrafe verurteilt (Tagesschau 2019).

Der Waffenhandel über das Darknet und die Verwenung der Waffe richtete einen besonderen Fokus auf den relativ kleinen Bereich des Internet. Bestrebungen, diesen öffentlichkeitswirksamen Teil der Ermittlungen weiter zu treiben und im Darknet besondere Aktivitäten zu entfalten, begründet die Gefahr, dass die anderen Bereiche unterproportional beleuchtet werden. Dabei sind nich nur das Darknet, sondern auch das Deep- und das Surfaceweb Orte gesetzeswidriger Handlungen und illegalen Handels. Häufig werden Foren als Handelsplätze umfunktioniert oder Geschäfte über Foren angebahnt (Safferling und Rückert 2018).

3.4 Kriminalitätsentwicklung im Netz

Die Entwicklungen der Kriminalität verlagern sich immer mehr ins Netz. Insbesondere die Betrugskriminalität wird immer mehr durch die digitale Variante abgelöst (Landeskriminalamt Nordrhein-Westfalen 2018). Auch neue Phänomene wie Datenhehlerei zeichnen sich vermehrt ab. Dabei stellen die festgestellten Entwicklungen nur das Hellfeld, basierend auf der Polizeilichen Kriminalstatistik (PKS) dar. Bei einem geschätzten Dunkelfeld zwischen 90 % und 99,9 % (Scheuplein 2019) dürften die tatsächlichen Schäden viel höher liegen. Viele Angriffe und Versuche werden bereits durch technische Maßnahmen wie SPAM-Filter, Virenschutz etc. abgefangen und durch die potenziellen Opfer gar nicht entdeckt.

Dem gegenüber stehen aber Betrugsstraftaten auf renommierten Online-Plattformen wie Amazon. Hier locken sogenannte „Fake-Shops“ Kunden mit vermeintlichen Angeboten (Gewerkschaft der Polizei). Tatsächlich erfolgt jedoch nur die Lieferung gefälschter oder minderwertiger Ware. Teilweise erfolgt auch keine Lieferung. Auch Plattformen wie Ebay bieten ein Einfallstor für

Betrüger. Die Möglichkeiten polizeilichen Einschreitens sind hier nur sehr eingeschränkt, da dies ein ständiges Beobachten aller Angebote bedeuten würde. Hier erscheint ein präventives Vorgehen der Anbieter angezeigt.

3.5 Soziale Netzwerke als kriminelle Plattformen?

Gleichzeitig entwickeln sich Verkaufsgruppen in sozialen Netzwerken immer weiter. Das Landeskriminalamt Niedersachsen zählte im Jahr 2017 über 300 Schwarzmarktgruppen auf Facebook und leitete 51 Ermittlungsverfahren ein (Bundeskriminalamt 2017). Hier werden neben Betäubungsmitteln auch verbotene Gegenstände wie Elektroschocker in Form von Taschenlampen angeboten. Selbst ein Auftreten als Polizei schreckt die Täter dabei nicht ab, entsprechende Angebote zu unterbreiten. Ausgehend von einem szenetypischen Angebot von „Grünschnitt“, was als Synonym für Marihuana verwendet wird, erfolgte im Laufe der Kommunikation das Angebot, „etwas für den Selbstschutz“ zu erwerben. Ausgehend von diesen Feststellungen konnten im vorliegenden Sachverhalt funktionsfähige Schusswaffen und Munition sichergestellt werden. Gleiches konnte in öffentlichen Foren beobachtet werden. Hier führten die Ermittlungen zur Identifizierung eines Tatverdächtigen und Sicherstellung einer funktionsfähig gemachten Schusswaffe und Munition. Hierbei ist die Grenze zwischen der Wahrnehmung als nicht offen ermittelnder Polizeibeamter (NoeP) und Scheinkäufer bzw. dem Einsatz verdeckter Ermittler schmal und stellt eine besondere Herausforderung dar. Auch der Einsatz von Angestellten ist hier nicht unkritisch zu betrachten. Der Autor vertritt die Auffassung, dass auch Personen, die nicht Ermittlungspersonen im Sinne des § 152 Gerichtsverfassungsgesetzes sind, dem Strafverfolgungszwang unterliegen.

3.6 Underground Economy

Dies stellt allein für die Beobachtung von illegalen Online-Marktplätzen eine besondere Herausforderung dar. Der 2017 beschlagnahmte Marktplatz „Alphabay“ (Heise online 2017) bot ein umfangreiches Angebot an illegalen Dienstleistungen und Gütern. Allein ca. 165.000 Angebote (s. Abb. 1) an Drogen sprechen – unabhängig davon, ob es sich um wirkliche Angebote oder Betrugsversuche handelt – eine deutliche Sprache.

Gefälschte Führerscheine und Waffen (s. Abb. 2) sind nur einige der weiteren Angebote, die auf diesen Plattformen gefunden werden können.

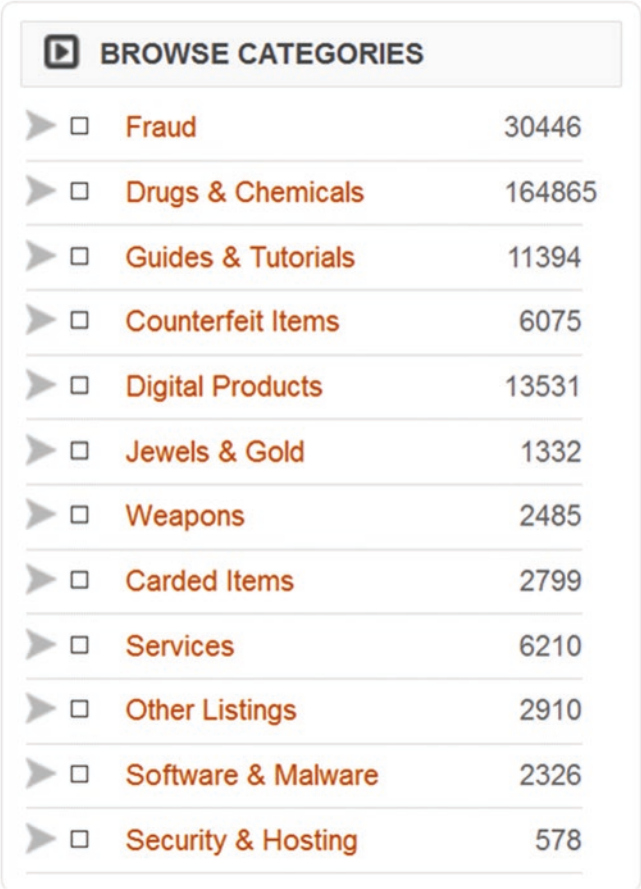


Abb. 1 Übersicht von Angeboten auf dem ehemaligen Darkweb Marktplats „Alphabay“ (Screenshot)

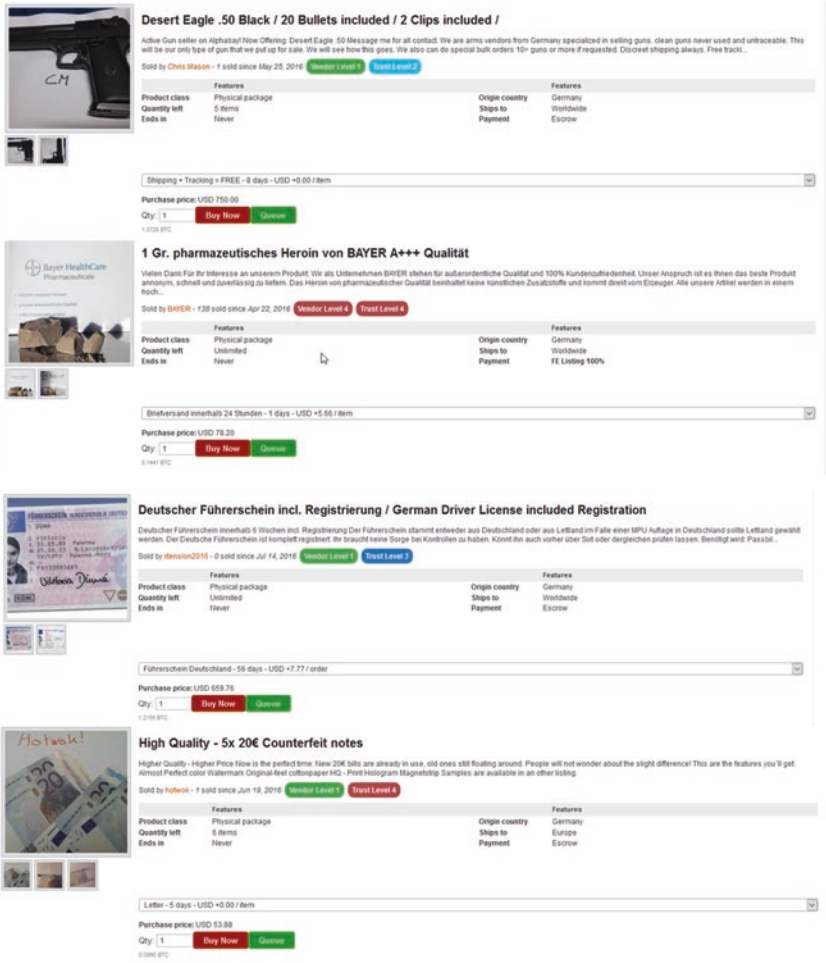


Abb. 2 Angeboten auf dem ehemaligen Darkweb Marktplats „Alphabay“ für Waffen, gefälschte Dokumente und Banknoten

4 Ohnmacht im Netz?

Schon dieser Umfang der Angebote wirft für die Strafverfolgungsbehörden die Frage nach dem Umgang mit diesen auf. Jedes dieser Angebote stellt grundsätzlich einen Straftatbestand dar und ist, dem Legalitätsprinzip Rechnung

tragend, zu verfolgen. Bei diesen Zahlen stellt dies sowohl die Polizei als auch die Staatsanwaltschaften und Gerichte vor besondere Herausforderungen an die Ressourcenbereitstellung. Hier ist bereits vor der Sichtung dieser Angebote mit der sachleitenden Staatsanwaltschaft eine Abstimmung über das gemeinsame Vorgehen erforderlich. Hier kommen auch Aspekte der ökonomischen Verfahrensführung zum Tragen. Daneben stellen die örtlichen Zuständigkeiten und das Vermeiden von doppelter Verfolgung des gleichen Sachverhalts besondere Herausforderungen an die Strafverfolgungsbehörden. Nicht nur, dass das Identifizieren der Angebote und das Verorten im Geltungsbereich der StPO nicht immer im Einzelfall möglich ist. Auch das Identifizieren der Serverstandorte außerhalb des Bundesgebietes erfordert umfassende internationale Zusammenarbeit. Darüber hinaus werden die genutzten Infrastrukturen häufig durch technische Maßnahmen gegen Ermittlungen geschützt. Aus diesem Grund erfolgt bundesweit in regelmäßigen Abständen eine Abstimmung und Koordinierung der Ermittlungsschwerpunkte der einzelnen Länder. Darüber hinaus ist die Bekämpfung von Handelsplattformen nur in gemeinsamer nationaler und internationaler Anstrengung möglich.

Gleichwohl bedeuten diese Verfahren für die Betreiber dieser Plattform zunächst scheinbar keine Gefahr. Der Betrieb einer solchen Plattform, die allein bei Sichtung der Angebote augenscheinlich keinem legalen Zwecke dienen kann und deren Administratoren und Treuhänder durch Gebühren am Verkaufserlös beteiligt werden, ist nicht strafbewährt. Maßnahmen gegen die Plattform wie deren Identifizierung, zur Identifizierung der Administratoren und Treuhänder sowie der Schließung der Plattform können aktuell nur dann begründet werden, wenn den Betreibern der Plattform eine Beteiligung an den einzelnen rechtswidrigen Handlungen, zumindest aber das Wissen und das Bereitstellen der Handelsplattform als Beihilfe, in jedem Einzelsachverhalt nachgewiesen werden können. Unabhängig von der Verfolgung der Handelsplattformen erschwert dies das Vorgehen gegen diese erheblich.

Aus diesem Grund hat das Land Nordrhein-Westfalen gemeinsam mit Hessen und Bayern einen Gesetzentwurf zur Bekämpfung von illegalen Marktplätzen in den Bundesrat eingebracht (Heise online 2019). Dabei wird jedoch die Ausgestaltung des Gesetzes im Rahmen der parlamentarischen Befassung besonderes Augenmerk verdienen. Eine alleinige Einschränkung auf Marktplätze, die über das Darknet erreichbar sind, wird aus der Erfahrung der Ermittlungskomplexe wenig bis keine Wirkung entfalten. Die Formulierung des besonderen Schutzes und Zugriffsbeschränkungen (Darknet) greifen zu kurz und sind nicht sachgerecht. Das Darknet selbst stellt weder eine Zugriffsbeschränkung noch einen Zugriffsschutz dar, lediglich einen verschlüsselten Zugangsweg.

Eine Beschränkung darauf würde den Sinn des Entwurfes bereits vor dessen Umsetzung wirkungslos machen. Bereits heute sind Darknet-Marktplätze auch aus dem Clearweb erreichbar. Bereits das Ermöglichen des Zugangs über das Clearweb könnte zur Straflosigkeit führen und damit diese Vorschrift von vorn herein überflüssig machen.

Die Kritik an einzelnen Formulierungen erscheint in Teilen angemessen (Bäcker und Golla 2019). Insbesondere die Abgrenzung sozial adäquaten Verhaltens dürfte eine besondere Herausforderung darstellen. Gleichwohl können illegale Handelsplattformen in der Regel eindeutig aufgrund ihrer Angebote identifiziert werden. Hier erscheint ein klares Herausarbeiten der tatsächlichen Anforderungen an einen Straftatbestand die besondere Problemstellung. Das alleinige Anbieten einer verschlüsselten Zugangstechnologie stellt an sich kein ahndungswürdiges Verhalten dar. Das Bundesamt für Sicherheit in der Informationstechnik wirbt offensiv um die Nutzung verschlüsselter Kommunikation. Gleichwohl muss der dargelegten Verlagerung der Kriminalität ins Internet durch Anpassung der Strafvorschriften und der Eingriffsbefugnisse Rechnung getragen werden. Dies bedarf einer sachgerechten Diskussion unter Einbeziehung technischer Expertise zum Vermeiden wirkungsloser Strafvorschriften und der Kriminalisierung sozial adäquaten Verhaltens.

Die öffentliche Fokussierung der Strafverfolgungsbehörden auf das Darknet lässt einen schutzfreien Raum im Internet vermuten. Dies stellt auch der Behördenspiegel deutlich heraus:

> „Bürger in Deutschland erwarten in Zukunft mehr Polizeipräsenz im Internet. Acht von zehn Nutzern sind der Meinung, es sollen mehr Ressourcen in spezielle Einheiten investiert werden, die gezielt gegen Cyber-Kriminalität vorgehen. Rund 90 Prozent sehen in dem Bereich eine wachsende Bedrohung, 84 Prozent befürchten darüber hinaus Aktivitäten ausländischer Geheimdienste im digitalen Raum in der Bundesrepublik Deutschland. Das sind Ergebnisse einer Umfrage des Bitkom unter 1.000 Internetnutzern. ‚Wie im analogen Leben muss der Staat die Sicherheit seiner Bürger auch im Internet gewährleisten', fordert Susanne Dehmel, Mitglied der Bitkom-Geschäftsleitung. ‚Wenn die Gefährdung zunimmt, müssen auch die Ressourcen der Polizei für Online-Einsätze aufgestockt werden.' Die Nutzer hätten inzwischen ein größeres Bewusstsein für Gefahren im Internet. Gleichzeitig fühlen sich laut Umfrage aber viele schlecht gegen Cyber-Kriminalität gewappnet: Zwei Drittel geben an, dass sie es nicht merken würden, wenn ihre Computer oder Endgeräte ausgespäht würden." (Behördenspiegel 2019, S. 2)

Auch die zunehmende Hasskriminalität im Netz geht an den Strafverfolgungsbehörden nicht spurlos vorbei. Nachdem im Jahr 2015 bei LKA NRW das Projekt „Bekämpfung rechter Internethetze" erste Erfolge erzielen konnte, kam es

nach der Übernahme der Aufgabe in das Alltagsgeschäft zu neuen Phänomenen. Während zunächst im Wesentlichen persönliche Angriffe überwogen, die die Straftatbestände von Beleidigung bis hin zur Volksverhetzung erfüllten, waren anschließend zunehmend fremdenfeindliche und volksverhetzende Kommentare auf Webseiten von Medienunternehmen und Sendungen zu verzeichnen. In der gemeinsamen Kampagne „Verfolgen statt nur Löschen“ setzen sich die Landesanstalt für Medien Nordrhein-Westfalen und die Staatsanwaltschaft Köln gemeinsam für das Verfolgen dieser Hasskriminalität im Netz ein. 280 Strafanzeigen waren die Bilanz des Jahres 2018 (Landesanstalt für Medien NRW 2019). Darüber hinaus kommen Aufgaben nach dem Netzdurchsetzungsgesetz auf die Strafverfolgungsbehörden zu. Meldungen über potenziell strafrechtlich relevante Inhalte, die durch Nutzer den Sozialen Netzwerken gemeldet, aber durch diese nicht innerhalb von 24 h gelöscht werden. Erfolgt dies nicht, können diese einer strafrechtlichen Prüfung zugeleitet werden. Diese erfolgt aufgrund der für das Bundesamt der Justiz zuständigen örtlichen Zuständigkeit ebenfalls durch die Staatsanwaltschaft Köln. Sollte die Identifizierung der Urheber nicht mit einfachen Mitteln möglich sein, werden die Ermittlungen dem Landeskriminalamt Nordrhein-Westfalen übertragen, die diese bis zur Begründung einer anderen Zuständigkeit oder zum Abschluss der Ermittlungen führt. Hier ist der Grat zwischen Strafverfolgung und öffentlich wahrgenommener Zensur sehr schmal. Gleichwohl stellen in der Regel die gemeldeten Verstöße eindeutige Straftatbestände dar. Auf das Lösch-/Sperrverhalten der Anbieter wird dabei kein Einfluss genommen.

Eine besondere Problematik sowohl für Repression als auch für Prävention stellen Annäherungsdelikte (z. B. das sogenannte Cybergrooming) im Netz und die Verlagerung des Vertriebs und Tauschs von Kinderpornografie in das Internet dar. Foren und Chatplattformen wie „Knuddels“ sind frei aus dem Internet zugänglich, ohne besondere Anonymisierungsdienste nutzen zu müssen. Hier ist eine beliebte Quelle für solche Annäherungs- und Sexualdelikte. Mädchen und Jungen werden hier regelmäßig zu Opfern von Straftaten, bei denen sich Männer ihnen annähern und zu sexuellen Handlungen auffordern. Diese werden dann vor Webcams vorgenommen oder fotografiert und dann den Tätern geschickt. Auch nehmen die Täter selbst Manipulationen an ihren Geschlechtsteilen vor, fotografieren diese und senden diese den Geschädigten. Hier stehen die Strafverfolgungsbehörden häufig vor der Frage der Strafbarkeit von Handlungen. Stellt das zeigen eines erigierten Gliedes gegenüber einem Ermittler, von dem der Täter glaubt, es sei ein Kind, nun eine Straftat dar oder nicht? Die juristischen Bewertungen gehen hier auseinander, sodass häufig nur die gefahrenabwehrende Komponente greift und nach erfolgter Identifizierung lediglich

Gefährderansprachen durchgeführt werden können. Das Bundesministerium der Justiz und für Verbraucherschutz hat es sich zum Ziel gesetzt, diesen vermeintlich untauglichen Versuch beim sog. Cybergrooming als eigene Tatbestandsvariante des Kindesmissbrauchs unter Strafe zu stellen. Der dazu vorliegende Referentenentwurf (RefE) vom 2. April 2019 befindet sich derzeit in der Abstimmung. Die Prävention in diesen Bereichen ist besonders schwierig, da die Täter sich das Vertrauen der Kinder erschleichen und nur durch eine frühzeitige Stärkung der Medienkompetenz der Eltern und Kinder positiv auf diese Entwicklung Einfluss genommen werden kann.

Schwieriger wird es für die Ermittler, sich z. B. in Kinderporno-Foren oder Tauschbörsen zu bewegen. Häufig wird hier durch die Täter von den Ermittlern das Begehen szenetypischer Straftaten, eine sogenannte ‚Keuschheitsprobe', gefordert (Friedrich-Alexander-Universität Erlangen-Nürnberg 2019). Das bedeutet, dass der Täter die Ermittler in nahezu allen Fällen auffordern, selbst zunächst kinderpornografisches Material zu übersenden, um anschließend in die geschützten Bereiche der Foren aufgenommen zu werden und Tauschmaterial angeboten zu bekommen, was wiederum Voraussetzung für das Identifizieren der Täter und eine wirkungsvolle Strafverfolgung ist. Mit dieser Keuschheitsprobe sollen Ermittler identifiziert werden, die genau solche Daten nicht übermitteln dürfen, ohne sich selbst strafbar zu machen. Hier werden unter der Federführung Bayerns derzeit Bestrebungen der Justizministerkonferenz vorangetrieben, rechtliche Möglichkeiten für Ermittler zu schaffen, unter Wahrung der Rechte von Geschädigten entsprechendes künstliches Material zu übersenden (Truscheit 2018).

Die polizeiliche Präsenz im Netz wird dabei augenscheinlich nicht wahrgenommen. Dies mag der geringen Wahrnehmbarkeit polizeilichen Handelns und der in der Öffentlichkeitsarbeit latenten Kritik von Zensur und der damit verbundenen Zurückhaltung in der Öffentlichkeitsarbeit geschuldet sein. Digitale polizeiliche Präsenz ist nicht mit der Wahrnehmbarkeit eines Streifenwagens in einer belebten Innenstadt vergleichbar.

Die Erfolge der Polizei auch in Nordrhein-Westfalen bei der Identifizierung und Verfolgung von Straftaten im Netz und der Nutzung digitaler Spuren zur Aufklärung analoger Straftaten sind ansprechender Beweis, dass das Internet kein rechtsfreier Raum ist und die Strafverfolgungsbehörden sowohl im Clear- als auch im Deep- oder Darkweb präsent sind, Sachverhalte aufdecken und der Strafverfolgung zuführen. Allerdings sind die Strafverfolgungs- und Gefahrenabwehrbehörden noch nicht auf dem Stand, den sie in der analogen Welt haben. Hier bedarf es fortwährender Anstrengungen, Methodiken und (rechtliche und technische) Grundlagen zu schaffen, Prävention und Repression im Internet voran zu treiben, um auch die formelle Sozialkontrolle in diesem scheinbar rechtsfreien

Raum wirkungsvoll und spürbar zu gestalten. So ist die aktuelle Diskussion um die Strafbarkeit des Betreibens von Infrastrukturen, die der Begehung von Straftaten dienen zu begrüßen. Hier ist aber auch auf ein Vorgehen mit Augenmaß zu achten, um nicht eine Kriminalisierung klassischer Angebote, die zweckentfremdet genutzt werden, zu erreichen. Die klare Trennung wird hier schwierige Aufgabe der Gesetzgebung sein. Die Anpassung gefahrenabwehrender Vorschriften hält hier ebenso wenig mit den technischen Entwicklungen Schritt, wie die Strafvorschriften oder die strafprozessualen Ermächtigungsgrundlagen. Die alleinige Annäherung beim Cyber-Grooming und das Zeigen und Vornehmen sexueller Handlungen im Glauben, dabei ein Kind oder einen Jugendlichen vor sich zu haben statt eines Ermittlers, ist derzeit nicht strafbar. Hier sind den Ermittlern häufig die Hände gebunden. Zur strafrechtlichen Verfolgung solcher Täter müssen sie Kinder oder Jugendliche als Geschädigte identifizieren und in das Strafverfahren einbringen, was ggf. zu weiteren Belastungen führt. Das vom Täter ausgehende Agieren gegenüber einem verdeckten Ermittler reicht hier nicht aus. Hier ist der Gesetzgeber gefordert. Wenn die Ermittler hier nicht einschreiten können oder dürfen, ist die Wahrscheinlichkeit, dass der Täter beim nächsten Mal auf ein echtes Opfer trifft, sehr hoch.

Literatur

Bäcker, P. D., & Golla, D. S. (21. März 2019). Strafrecht der Finsternis: Zu dem Vorhaben eines “Darknet-Tatbestandes”. *Mainz*. https://verfassungsblog.de/strafrecht-in-der-finsternis-zu-dem-vorhaben-eines-darknet-tatbestands/. Zugegriffen: 21. Mai 2017.

Behördenspiegel. (9. Mai 2019). Newsletter Netzwerk Sicherheit – Mehr Internetpolizei (U. Proll, Hrsg., & U. Proll, Redakteur). Bonn.

Bundeskriminalamt. (13. Dezember 2017). Protokoll zur 26. Tagung der Koordinierungsstelle für Dienststellen für anlassunabhängige Recherchen im Internet (KaRIn). Düsseldorf.

Bundesregierung. (3. Februar 2018). *Die Bundesregierung*. https://www.bundesregierung.de/breg-de/mediathek/die-kanzlerin-direkt/merkel-das-internet-ist-kein-rechtsfreier-raum–1007676.

Der Spiegel. (11. Mai 2007). *Spiegel Online*. https://www.spiegel.de/netzwelt/web/kinderpornos-in-second-life-staatsanwaltschaft-hat-heisse-spur-a-482431.html.

Förster, A. (28. August 2017). *Berliner Zeitung*. https://www.berliner-zeitung.de/politik/prozess-um-amoklauf-von-muenchen-die-waffe-aus-dem-darknet-28221438.

Friedrich-Alexander-Universität Erlangen-Nürnberg. (22. Mai 2019). Keuschheitsproben für Verdeckte Ermittler? (P. D. Safferling, Redakteur) Erlangen. https://www.str1.rw.fau.de/2018/03/29/keuschheitsproben-fuer-verdeckte-ermittler/. Zugegriffen: 22. Mai 2019.

Gewerkschaft der Polizei. (kein Datum). Fake-Shops bei Amazon. https://www.polizei-dein-partner.de/themen/internet-mobil/detailansicht-internet-mobil/artikel/fake-shops-bei-amazon.html. Zugegriffen: 20. Mai 2019.

Heise. (20. Juli 2017). Darknet-MArktplätze: Ermittler schließen neben AlphaBay auch Hansa Market. https://www.heise.de/newsticker/meldung/Darknet-Marktplaetze-Ermittler-schliessen-neben-AlphaBay-auch-Hansa-Market-3779559.html. Zugegriffen: 21. Mai 2019.

Heise online. (15. März 2019). Bundesrat einigt sich auf Vorgehen gegen illegale Darkent-MArktplätze. https://www.heise.de/newsticker/meldung/Bundesrat-einigt-sich-auf-Vorgehen-gegen-illegale-Darknet-Marktplaetze-4337843.html. Zugegriffen: 21. Mai 2019.

Institut für berufliche Bildung, Arbeitsmarkt- und Sozialpolitik. (2018). Entwicklung von Berufsprofilen mit Hilfe der DACUM Methode. https://www.inbas.com/leistungen/produkte/dacum.html.

Landesanstalt für Medien NRW. (15. Januar 2019). Neue Medienpartner stärken Initiative gegen Hassrede. Düsseldorf. https://www.medienanstalt-nrw.de/service/pressemitteilungen/pressemitteilungen-2019/2019/januar/neue-medienpartner-staerken-verfolgen-statt-nur-loeschen.html. Zugegriffen: 21. Mai 2019.

Landeskriminalamt Nordrhein-Westfalen. (2018). *Lagebild Cybercrime*. Düsseldorf.

Nolde, M.-D. (2003). Ermittlungsmaßnahmen im Internet. *Polizeiliche Tätigkeit im Vorfeld von Anfangsverdacht*. Hannover.

Safferling, C., & Rückert, C. (Februar 2018). *Konrad Adenauer Stiftung*. https://www.kas.de/analysen-und-argumente/detail/-/content/das-strafrecht-und-die-underground-economy1.

Scheuplein, I. (2019). Waffenhandel, digitale Erpressung, massenweise gestohlene Kreditkartendaten und Passwörter: Schaden geht in die Milliarde – Quelle: https://www.svz.de/14398351 © 2019. Zugegriffen: 29. Aug. 2019; https://www.svz.de/14398351.

Schulzki-Haddouti, C. (3. September 1998). *heise.de*. https://www.heise.de/tp/features/Strafverfolgung-im-Internet-Metasuchmaschinen-und-Internetstreifen-3411764.html.

Tagesschau. (14. März 2019). *Tagesschau.de*. https://www.tagesschau.de/inland/muenchen-amoklauf-waffe-darknet-101.html.

Truscheit, K. (2. August 2018). So will Bayern der Kinderpornographie ein Ende setzen. *FAZ*. https://www.faz.net/aktuell/gesellschaft/kriminalitaet/wie-bayern-der-kinderpornographie-ein-ende-setzen-will-15718453.html. Zugegriffen: 22. Mai 2019.

Verlag Deutsche Polizeiliteratur. (2016). *Die Kriminalpolizei*. https://www.kriminalpolizei.de/service/praevention-kompakt.html?tx_contagged[source]=default&tx_contagged[uid]=33&cHash=593bb3b101b36e3c12dfeb9a40359657.

Zollfahndungsamt Frankfurt am Main. (16. August 2016). ZOLL-F: Festnahme des mutmaßlichen Lieferanten der beim Amoklauf in München am 22.07.2016 verwendeten Schusswaffe und Munition. https://www.presseportal.de/blaulicht/pm/116258/3405387.

Defensible Digital Space

Die Übertragbarkeit der Defensible Space Theory auf den digitalen Raum

Cindy Ehlert und Thomas-Gabriel Rüdiger

1 Einleitung

Eine Grundannahme der Kriminologie ist stets, dass viele Formen der Kriminalität vor allem aus zwischenmenschlichen Prozessen entstehen; seien es Gewalt-, Sexualdelikte, Raub- oder Diebstahlshandlungen. Hierfür müssen Menschen in irgendeiner Form aufeinandertreffen, sei es aktiv, z. B. wenn sich Menschen begegnen und interagieren, oder passiv, wenn der Täter z. B. eine Person beobachtet und diese basierend auf den Rückschlüssen und Rahmenbedingungen zu seinem Opfer erklärt. Diese Form des Aufeinandertreffens erforderte bisher einen physischen Raum, in dem eine derartige Interaktion stattfinden kann – unabhängig davon wie groß dieser ist. Seit ungefähr 30 Jahren wird eine solche Form der Interaktion nun ergänzt um einen virtuellen Raum, in dem Menschen in einer annähernd vergleichbaren Art und Weise – jedoch ohne physische Grenzen – in Interaktion treten können.

Newman thematisierte bereits 1996 die Frage, inwiefern die architektonische Gestaltung eines Raumes Einfluss auf die Kriminalitätsbegehung hat (Newman 1996). Er bezog sich dabei auf den strukturellen und sozialen Verfall von

C. Ehlert (✉)
Hochschule der Polizei des Landes Brandenburg, Oranienburg, Deutschland
E-Mail: cindy.ehlert@hpolbb.de

T.-G. Rüdiger
Institut für Polizeiwissenschaft, Hochschule der Polizei des Landes Brandenburg, Oranienburg, Deutschland
E-Mail: thomas.ruediger@hpolbb.de

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

T.-G. Rüdiger und P. S. Bayerl (Hrsg.), *Cyberkriminologie,*
https://doi.org/10.1007/978-3-658-28507-4_6

Pruitt-Igoe, einem Stadtteil von St. Louis, Missouri, in den Vereinigten Staaten. In den Jahren 1950 bis 1954 wurde Pruitt-Igoe im Rahmen eines Projekts des öffentlich geförderten Wohnungsbaus als ein Großstadtkomplex geschaffen. Diese Projekte wurden als „public housing“ bezeichnet und sollten Menschen im Siedlungsraum St. Louis ein kostengünstiges Heim schaffen. Die Häuser, welche am Rande der Stadt in sogenannten Slumquartieren nach den Vorstellungen des modernen Wohnungsbaus errichtet wurden, bestanden aus Gebäudezellen mit rund 2800 Wohnungen (Newman 1996, S. 9). Man wollte viele Menschen, auch mit geringem Einkommen, möglichst kostengünstig unterbringen und dafür war die Hochhausform offenbar naheliegend (Frondorf 2007). Auf etwaige soziale oder auch individuelle Bedürfnisse der zukünftigen Bewohner sind die Architekten bei der Planung ihrer Wohnsilos jedoch nicht weiter eingegangen. Vielmehr stand die Grundüberlegung im Mittelpunkt, dass die zukünftigen Bewohnen Menschen aus der nordamerikanischen Mittelschicht mit einfachen Wohnansprüchen seien (Rolinski 1980).

Die Projektverantwortlichen setzten dabei auf Architekten, die für die anwachsende Wohnbevölkerung Wohneinheiten schaffen sollten, in denen viele Menschen privat leben können, die aber auch am selben Ort Raum für neue Begegnungen ermöglichen. Die 11-stöckigen Geschosse sollten dafür jeweils im Erdgeschoss und im 1. Obergeschoss über Räumlichkeiten für Gemeinschaftsaktivitäten verfügen sowie über einen Gemeinschaftskorridor und auf jeder 3. Etage einen Wäscheraum, einen Gemeinschaftsraum und einen Müllraum mit einem Müllschlucker bekommen (Newman 1996). Die allein rechnerisch große Anzahl von Wohneinheiten ermöglichte allerdings kaum die Etablierung und Ausübung informeller soziale Kontrolle – beispielsweise durch die Aktivierung einer gemeinsamen Identität und Verantwortung. Dadurch wurde ein Teil des Lebensraums zu einer Art anomischem Raum, für den sich keiner verantwortlich zeichnete und in der es zu keiner wirksamen Form der Kontrolle kommen konnte.

Newman betrachtete diese Situation und stellte sich die Frage, inwiefern auch architektonische – also letztlich bauliche – Maßnahmen einen Einfluss auf Normenkontrolle und -brüche haben können. Im Rahmen dieser Überlegungen beschrieb er das Konzept eines „Creating Defensible Space“. Hiermit verfolgte er das Ziel, durch das Design eines (Lebens-)Raumes einen Schutz bietenden Ort zu schaffen, der zum einen von seiner architektonischen Gegebenheit wehrhaft und verteidigungsfähig und zum anderen auch für die Bewohner attraktiv, überschaubar und damit sicher gestaltet ist (Schnittger und Schubert 2002).

Dabei muss angemerkt werden, dass Umwelt und menschliches Verhalten sowie Erleben in einem engen Zusammenhang zueinanderstehen. Das heißt, dass die physische als auch die soziale Umwelt den Menschen in seinen

Verhaltensweisen lenkt. Sie kann sowohl ursächlich für sein Verhalten sein sowie es beeinflussen und Verhaltensmuster verstärken (Kube 1982). Für die nachfolgende Betrachtungsweise ist dies von Bedeutung, Das wirft die Fragen auf, inwiefern dieses Konzept auf onlinebasierte Strukturen – also digitale Räume – adaptiert werden könnte, welchen Aussagewert dies vor allem für die Prävention von digitalen Straftaten hat und welche kriminalpolitischen Schlussfolgerungen hieraus gezogen werden können.

2 Newmans „Defensible Space“ Ansatz

Wie dargestellt war der Ausgangspunkt für Newmans theoretischen Ansatz das rasante Anwachsen der amerikanischen Wohnbevölkerung im 20 Jahrhundert. Demnach habe sich diese im Zeitraum von 1920 bis 1970 von 106 auf 203 Mio. annähernd verdoppelt (Rolinski 1980). Die große wirtschaftliche Entwicklung nach 1900 und das Streben nach dem „American Way of Life“ begünstigten die Zuwanderungen in die USA (Sautter 2011). Der Anteil derer, die im großstädtischen Bereich leben, wuchs dabei von 50 % auf 69 % an. Die Zuwanderer im städtischen Bereich sind überwiegend weniger einkommensstark, als die, die in den Vorstädten leben. Für diese Masse an Menschen musste finanziell leistbarer Wohnraum geschaffen werden. Da Wohnraum knapp und damit teuer war, lag es auf der Hand, architektonische Bauten zu platzieren, die auf geringer Fläche eine große Anzahl von Menschen beherbergen können. Die Idee der sogenannten Wohnsilos entstand (Rolinski 1980).

2.1 Elemente der Unsicherheit

Newman fand in seinen Recherchen heraus, dass die Menschen in Pruitt-Igoe ihren Wohnraum von innen heraus tatsächlich physisch zerstörten und damit dieser Raum auch immer stärker verwahrloste. Im Äußeren waren diese Zerstörungen aber erst wahrnehmbar, als sie sich von innen nach außen ausbreiteten. Die Menschen – Bewohner oder Besucher – beschädigten z. B. Briefkästen, Leuchtmittel oder auch Gebäudeteile. Ganze Gebäudekomplexe wurden nach Newman von den Bewohnern und den mit ihnen verkehrenden Gesellschaftsmitgliedern nicht mehr angenommen; sie fühlten sich in ihrem Zuhause offenbar nicht heimisch, konnten sich quasi mit ihrem Wohnraum nicht mehr identifizieren (Rolinski 1980).

Diese Situation lässt sich auch durch den nicht unumstrittenen *Broken Windows* Ansatz von Kelling und Wilson (1982) erklären. Demnach führt eine sichtbar begangene Normenüberschreitung, die nicht sichtbar geheilt bzw. gegen die nicht vorgegangen wird, zu einer generellen Senkung der Hemmschwelle zur Begehung weiterer Normenbrüche. Kelling und Wilson verdeutlichen dies anhand der namensgebenden zerbrochenen Fensterscheibe, die, wenn sie nicht repariert wird, das Fehlen einer informellen Normenkontrolle verdeutlicht (Kelling und Wilson 1982, S. 1 ff.). Jede weitere Überschreitung intensiviert diesen Effekt und führt zu einer Art Kreislauf. Dieser Mechanismus ist offenbar auch in den von Newman untersuchten Wohnblöcken zu verzeichnen gewesen.

Der Verstärkungseffekt der Normenüberschreitungen könnte darin liegen, dass eine gewisse Abhängigkeit der Nutzer von diesem Wohnraum bestand, denn sie konnten schlicht nirgendwo anders hin. Hieraus könnte sich eine innere Aggression ergeben, aufgrund des hilflosen Gefühls keinen Einfluss auf die Verbesserung der eigenen Wohnsituation nehmen zu können, die dann eine ablehnende, zerstörerische Haltung hervorgerufen. Dieser Umstand stellte sowohl die Polizei als auch Architekten vor eine große Herausforderung (Rolinski 1980). Auch wenn davon ausgegangen werden kann, dass Architektur allein nicht der Auslöser für Kriminalität im Lebensraum ist, kann sie zumindest eine mitursächliche Variable darstellen. Nach Schwind und Kube (2003, zitiert in Born 2009, S. 54; Schwind 2016, S. 359 ff.) könnten sich folgende weitere raumbezogene Variablen, im Sinne eines multikausalen Erklärungsansatzes, kriminalitätsbegünstigend zeigen:

- Niedriger sozio-ökonomischer Status eines Raumes mit weiterer sozialer Abstiegstendenz zum sozialen Brennpunkt, nicht zuletzt aufgrund hoher Fluktuation und hohem Leerstand von Wohnungen
- Starkes Vorhandensein benachteiligter Minderheiten und/oder Randgruppen sowie kinderreicher Familien bei alleinerziehendem Elternteil
- Hoher Anteil männlicher Jugendlicher
- Wohnbereich mit hohem Straftäteranteil
- Defizitäres, monofunktionales Wohnumfeld
- Hohe Dichte von Zielobjekten kriminellen Verhaltens
- Günstige Tatgelegenheiten, u. a. gute Flucht- oder Versteckmöglichkeiten durch Randbepflanzungen für Straftäter sowie Dunkelzonen

Hierbei wird ersichtlich, dass neben der tatsächlichen objektbezogenen Baustruktur, die Sozialstruktur bei der Entstehungsbetrachtung der Kriminalität ein entscheidender Punkt darstellt (Schwind 2016, S. 359 ff.).

Soll ein „defensible space“ nach Newman geschaffen werden, muss folglich dafür gesorgt werden, dass die Bewohner den halbprivaten Raum adaptieren und sich für diesen verantwortlich fühlen. Ein so entwickeltes soziokommunikatives System der anwohnenden Individuen lässt das Wohnobjekt für Unrechtspersonen durch die aktive Normenkontrolle durch die die Anwohner – und die damit einhergehende erhöhte Entdeckungswahrscheinlichkeit – unattraktiv werden (Rolinski 1980). Dies ist auch nach der *Routine Activity Theorie* von Cohen und Felson (1979) nachvollziehbar. Demnach sind Menschen in einer konkreten Situation zu einem Normenbruch bereit, beziehungsweise überschreiten die Hemmschwelle zur Tatbegehung, wenn sie eine grundsätzliche Motivation aufweisen, ein lohnendes Ziel vor Augen haben und die Risiken – auch in Form von Sicherheitsmechanismen – in einem entsprechenden Verhältnis zueinanderstehen (Cohen und Felson 1979). Eine intakte Nachbarschaft erhöht die Schutzmechanismen und lässt damit die Risiken für den Täter höher erscheinen, was wiederum auch Hemmschwelle zur Tatbegehung erhöht.

2.2 Elemente, die Sicherheit schaffen

Um im eigenen Wohnrevier soziale Kontrolle im Sinne von Newman ausüben zu können, setzt dieser auf Barrieren – reale wie symbolische – sowie auf Bereiche der planerisch definierten Einflussnahme und Gelegenheiten natürlicher Überwachung. Er geht davon aus, dass die Bewohner durch die maßgebliche Einflussnahme auf die Verteidigungsfähigkeit die Erhöhung der Sicherheit für sich und ihr Wohnumfeld (z. B. Nachbarn) selbst in der Hand haben, wodurch ihre Wohn- und damit Lebensqualität merklich gesteigert wird (Schnittger und Schubert 2002).

Schutz bietende Räume ergeben sich also nicht automatisch mit dem Bau eines Wohnraums. Vielmehr müssen sie gestaltet, also erst speziell geschaffen werden. Möglichkeiten zur Schaffung sieht Newman in vier Planungsansätzen verwirklicht, die er Territorialität, natürliche Überwachung, Image und Milieu betitelt (Schnittger und Schubert 2002).

2.2.1 Territorialität

Unter *Territorialität* versteht Newman die Identifizierung der Bewohner mit dem Raum, sodass eine Art soziale Beziehung entsteht, die ein Verteidigungsverhalten seitens der Bewohner entstehen lässt. Bewohner wollen ihren Raum in Folge vor unangebrachten Handlungen und Übergriffen schützen. Dieses sogenannte Territorialitätsverhalten muss bei Bewohnern erst erzeugt bzw. aktiviert werden

(Kube 1982, S. 22). Das geschieht, indem Barrieren geschaffen werden, sogenannte Zonen im Wohnumfeld, die es den Bewohnern ermöglichen, sich gegenüber Fremden abzugrenzen und so leichter soziale Kontrolle auszuüben. Diese Zonen lassen sich in den privaten, halbprivaten/halböffentlichen und öffentlichen Raum einteilen. Durch das Einpflegen von Symbolen und Zeichen, insbesondere im halbprivaten/halböffentlichen Bereich, werden die Übergänge der Räume zueinander markiert und die Verantwortlichkeit der Bewohner für diesen Raum gefördert. Diese Symbole können tatsächlich rein objektive Hindernisse darstellen wie Zäune, Hecken, Mauern oder auch Türen (Born 2009). Durch die territorialen Markierungen zeigen die Bewohner, dass es normenkontrollierende Instanzen gibt, die Anspruch auf diesen Raum erheben und diesen ggf. auch verteidigen werden, was im Umkehrschluss höhere Risiken für mutmaßliche Täter darstellt. Wenn klare Zeichen fehlen, wird der Raum Unrechtspersonen gegenüber weder symbolische noch reale Barrieren setzen. Durch das Prinzip der Territorialität können sich Bewohner besser mit ihrem Raum identifizieren und sind eher gewillt, Verantwortung dafür zu übernehmen; in Folge ist es wahrscheinlicher, dass das Verhalten von Fremden in die gewünschte, sozialadäquate, Richtung gelenkt wird (Schnittger und Schubert 2002).

2.2.2 Natürliche Überwachung

Das Element der *natürlichen Überwachung* setzt darauf, bauliche Mittel einzusetzen, die innerhalb der Nachbarschaft ein gewisses Maß an Aufmerksamkeit erzeugen (Schnittger und Schubert 2002). Das geschieht dadurch, dass die Architektur die aktive Ausübung informeller sozialer Kontrolle ermöglicht (Kube 1982, S. 22). Dies kann ermöglicht werden, durch Sichtbarkeit (Visibilität) im Wohnumfeld, etwa einer sogenannten „kontaktfördernden“ Eingangsgestaltung; z. B. durch Einsichtsmöglichkeiten auf Eingangsbereiche von der Wohnung aus, durch gemeinsam nutzbare Gärten oder auch Spielplätze. So kann gewährleistet werden, dass Bewohner Fremde rechtzeitig erkennen – diese sich also beim Betreten des Raumes beobachtet fühlen – und sie nach dem Grund ihres Aufenthaltes befragen könnten. Gleichzeitig kann so aber auch eine Kontrolle der Bewohner untereinander gewährleistet werden (Kube 1982).

2.2.3 Image

Das Merkmal *Image* zielt darauf ab, einem negativen Stigma durch ansprechende und optisch abgestimmte Gebäudeformen und Umfeldgestaltung zu entgehen. Newman geht davon aus, dass durch ein gutes Image nicht nur privat mehr in den Raum investiert wird, sondern auch die Bereitschaft der Bewohner soziales Engagement zu zeigen steigt (Schnittger und Schubert 2002, S. 7). Auch bei diesem

Aspekt geht es im Kern darum, dass das Risiko, entdeckt zu werden, für Menschen, die die informellen und formellen gesellschaftlichen Regeln in diesem Raum überschreiten, erhöht wird.

2.2.4 Millieu

Die Schaffung eines *Milieus* wird realisiert, indem die städtebauliche Anordnung der Gebäude auf einen möglichst hohen Einfluss sozialer Kontrolle gerichtet ist. Dies geschieht z. B. durch eine Planung von großen Fensterbereichen und möglichst wenigen Wohneinheiten pro Hauseingang (Schnittger und Schubert 2002, S. 7).

Newmans Planungsansätze sollten sich am ehesten in sogenannten Mini-Nachbarschaften (mini-neighborhoods) umsetzen lassen. Der Vorteil dieser kleinteilig angelegten Nachbarschaft besteht darin, dass die Bewohner ihr Wohnumfeld überblicken können (Schnittger und Schubert 2002, S. 7). Für die Entwicklung eines Verantwortlichkeitsgefühls und der damit einhergehenden Verpflichtung zur Ausübung sozialer Kontrolle, muss eine persönliche Identifizierung mit dem Lebensumfeld stattfinden – nicht zwingend im rechtlich verständlichen Sinne, sondern sozial im Sinne eines Eigentums- oder Besitzanspruches. Diese gelingt jedoch nur, wenn eine Art physische Begrenztheit für den Einzelnen erkennbar ist. Erst durch eine überschaubare Raum(-auf)teilung ist es möglich, diesen Anspruch zu gewinnen.

Newman hat diese sogenannten Mini-Nachbarschaften daher in der Form eines griechischen Kreuzes konzipiert. Die Häuser in den dabei entstandenen – maximal drei – Straßenzügen (zwei horizontal, einer vertikal) sollten sich durch bauliche Maßnahmen in die Zonen privat, halbprivat/halböffentlich und öffentlich abgrenzen lassen, was für jede einzelne Wohneinheit (z. B. bei einem Einfamilienhaus oder einer Doppelhaushälfte) durch bauliche Maßnahmen gut umsetzbar schien. Weiterhin sollten sich die benachbarten Mini-Nachbarschaften schon rein optisch voneinander unterscheiden, was innerhalb der Nachbarschaft eine Art Zugehörigkeitsgefühls zur eigenen Mini-Nachbarschaft suggerieren sollte. Außerdem sollten die Bewohner einer Nachbarschaftsgemeinde an der Entscheidung der Zugänglichkeit für z. B. den öffentlichen Verkehr (etwa durch die Festlegung einer Sackgasse oder gar Spielstraße) direkt beteiligt werden (Schnittger und Schubert 2002, S. 7). Beteiligung in diesem Sinne sorgt für mehr soziale Identifikation mit dem Wohnumfeld, Motivation zur Eigenkontrolle und insgesamt zu einem erhöhten Grad an Zufriedenheit im eigenen Wohnumfeld.

2.3 Kritik an der Theorie

Nachdem Newman seine Ideen zur Schaffung eines wehrfähigen Raumes, z. B. in Five Oakes, wo es zuvor zu einem Wohnraumverfall kam – umsetzen konnte und sich hier tatsächlich die Kriminalitätsrate verringerte sowie das subjektive Sicherheitsgefühl und auch das grundsätzliche Lebensgefühl der Bürger in diesem Wohnbereich verbesserte, wurde angenommen, dass der Ansatz bei einer kleinteiligen Umsetzung in der Lage ist, Kriminalität zumindest punktuell zu vermindern (Kanol 2008, S. 6 f.). Andere Studienlagen kamen jedoch zu gegenteiligen Ergebnissen. So wurden in mehreren amerikanischen Städten nach Newmans Vorstellungen Elemente des Defensible Space Ansatzes umgesetzt, mit dem Ergebnis, einer kurzzeitigen Verringerung der Kriminalitätsraten (Kanol 2008). Der Erfolg wurde jedoch zeitnah durch einen erneuten Anstieg der Kriminalität getrübt. Zwar hat sich durch spezielle Maßnahmen wie z. B. vermehrte Beleuchtung, das subjektive Sicherheitsgefühl der Bewohner verbessert, was einherging mit einer geringeren Kriminalitätsfurcht, jedoch gab es keine Erfolge im Sinne einer dauerhaft gesunkenen Kriminalitätsrate zu verzeichnen.

Die konkreten Gründe für diese Situation sind nicht eindeutig identifizierbar. Einerseits ist denkbar, dass die Menschen in diesen so geschützten Räumen eine stärkere Identifikation mit dem Rechtssystem entwickelten haben und sich daher schneller für eine Strafanzeige als Instrument der Normendurchsetzung entschieden, was sich in der Folge in den polizeilichen Kriminalstatistiken widerspiegelte. Andererseits könnte tatsächlich die Situation eingetreten sein, dass die Bewohner zwar ein höheres Sicherheitsgefühl entwickelten, damit aber langfristig unvorsichtiger wurden, was sie wiederum für Kriminelle – auch nach dem Routine Acitvity Ansatz – zu leichteren Zielen, faktisch Opfern, machen würde (Cohen und Felson 1979). Kube kommt sogar zu folgendem Fazit: *„Hier wird deutlich, daß bauliche Gestaltungsmerkmale – soweit sie Kontakte und Kommunikation und damit auch informelle soziale Kontrolle intensivieren sollen – in ihrer Bedeutung leicht überschätzt werden“* (Kube 1982).

3 Opfer im realen Raum auch Opfer im digitalen Raum?

Es stellt sich nun die Frage inwiefern die Grundüberlegungen von Newman auch prinzipiell auf den digitalen Raum übertragbar sind. Dabei wird von der Annahme ausgegangen, dass auch das Internet bzw. verschiedene Online-Programme, eine Raumeigenschaft aufweisen können. Diese Eigenschaft zeigt sich u. a. darin, dass

der Begriff des Raumes (z. B. des Chatrooms) häufig für Internetthemen genutzt wird. Die zweite Hypothese ist, dass dieser digitale Raum zwar andere Formen der Kriminalität hervorbringt – z. B. Handlungen wie virtual rape (virtuelle Vergewaltigung) durch Avatare oder der gesamte Komplex um Malware – aber sich die Regeln und Mechanismen von Kriminalitätsentstehung und Normenkontrolle vom physischen Raum auch in den digitalen übertragen lassen (Rüdiger 2018).

Kriminologische Aspekte, die sich jedoch offensichtlich noch nicht angenähert haben, sind bezogen auf das deutsche Kriminalitäts- und Rechtsverständnis, u. a. eine viel höhere Dunkelzifferrelation bei annähernd allen digital begangenen Kriminalitätsformen (Rüdiger 2019b) sowie eine bisher nur geringe kriminologische Reflexion und Übertragung der bisherigen Theorien zur Erklärung und dem besseren Verständnis von Normen und Normenkontrolle.

Allein aktuelle Nutzerzahlen zeigen jedoch wie relevant dies wäre. Nach einer Studie von Frees und Koch (2019) nutzten im Jahr 2018 alleine 90,3 % aller Deutschen ab 14 Jahren das Internet. Bei den 14–19-Jährigen erreicht dieser Wert sogar 100 % (Frees und Koch 2019). Die Nutzungsdauer hat sich dabei von 177 min im Jahr 2016 auf 240 min im Jahr 2018 erhöht (Frees und Koch 2019). Die Nutzung des Internets ist dabei vorwiegend geprägt von sogenannten Sozialen Medien, also onlinebasierten Programmen, die vornehmlich der Kommunikation und Interaktion – in Form einer Vernetzung zwischen Menschen – dienen (Rüdiger 2018). Soziale Medien erfassen damit fast alle Formen von Programmen im Netz von Messenger wie WhatsApp und KIK über klassische Soziale Netzwerke wie Facebook, Twitter oder auch Instagram bis zu Onlinegames wie Fortnite, Clash of Clans oder World of Warcraft. Allein 31 % der deutschen Bevölkerung soll zumindest einmal wöchentlich Facebook nutzen, 15 % Instagram und 9 % Snapchat. Weitere 45 % nutzen täglich Whatsapp mit einer Nutzungsdauer von 87 min und 9 % spielen täglich mindestens 16 min online (Frees und Koch 2019).

Auch wenn es faktisch keine wahrnehmbaren physischen Grenzen in diesem digitalen Raum gibt, so achten doch alle Programme darauf, einen gewissen designtechnischen Wiedererkennungswert zu haben. Unabhängig davon, ob die Nutzer bewusst die Programme aufrufen, erkennen sie doch bereits optisch, ob sie sich bei Twitter, Instagram oder gerade auf WhatsApp befinden. Gleichzeitig beinhalten fast alle Programme in irgendeiner Form Individualisierungsmöglichkeiten; sei es, dass man sich Profilbilder geben kann, in einem Onlinespiel eine Gilde gründet oder einfach durch geschriebene Postings oder geteilte Links. Dabei ist die Interaktion mit anderen Menschen ein wesentlicher Eckpfeiler. Teilweise kommt es gerade darauf an, dass Menschen sich in Gruppen zusammenfinden und kollektiv miteinander interagieren. Wie dieses Miteinander geregelt wird, ist jedoch auch von Programm zu Programm unterschiedlich und wird von den Nutzern selbst gestaltet.

Gleichzeitig entsteht eine Vielzahl an Kriminalitätsformen im digitalen Raum gerade aus der Interaktion der Menschen miteinander. Dies können beleidigende Kommentare sein, sexuelle Belästigungen, das unerwünschte zusenden pornografischer Medien oder schlicht Betrugshandlungen, wenn es sich um Vermögenswerte wie Gamingaccounts oder Waren auf eBay oder Amazon handelt (Rüdiger und Pfeiffer 2015). All diese Delikte basieren einerseits auf der Interaktion zwischen Opfer und Täter und sind andererseits von den jeweiligen Mechanismen geprägt, die das digitale Umfeld – also das konkrete soziale Medium – vorgibt. So erfordert beispielhaft das unerwünschte Zusenden pornografischer Medien auch die Möglichkeit, dass Bilder oder Videos einem anderen Nutzer zugesandt werden können wie beispielsweise bei Messengern wie KIK, WhatsApp oder auch Instagram.

Mit Sozialen Medien liegen also Konstruktionen vor, die eine Art von „Einwohnern“ haben, die ihre Zeit in diesen digitalen Räumen verbringen und dort mit anderen Menschen kommunizieren und interagieren. Gleichzeitig sind diese optisch voneinander abgrenzbar und es herrschen in ihnen teilweise unterschiedliche Normenverständnisse. Diese Mechanismen lassen Soziale Medien Konstruktionen wie Wohn- oder Stadtvierteln ähneln. An diesen Aspekten sollen die weiteren Überlegungen anknüpfen.

4 Unterschiedliche Normenüberschreitungen in Sozialen Medien?

Die U25 Studie des Deutschen Instituts für Vertrauen und Sicherheit im Internet kam im Jahr 2018 zu dem Ergebnis, dass 64 % der befragten jungen Deutschen von 14 bis 24 Jahren der Meinung sind, dass *„wer sich dort [Anm: das Internet] äußert, müsse damit rechnen, beleidigt oder beschimpft zu werden“* (Borgstedt et al. 2018). Ein Ergebnis dieser Situation sei, dass es für 38 % der Befragten nicht infrage kommt, sich im Internet öffentlich zu äußern, da diese keine Lust hätten, beleidigt zu werden. Von den Autoren wird dieser Umstand als eine vorhandene „Beleidigungskultur“ beschrieben.[1]

[1]Dabei ist es nicht ganz korrekt in diesem Zusammenhang von dem Internet als solchem zu sprechen; vielmehr kann eine Beleidigung nur in der Kommunikation bzw. durch Kommentare verübt werden, seien sie schriftlich oder verbal, was wiederum die Nutzung Sozialer Medien oder artähnlicher Programme wie Kommentarspalten in Nachrichtenportalen indiziert.

Sei es der Begriff der Beleidigungskultur – oder auch Unrechtskultur – im digitalen Raum oder die stetig bemühte Prämisse, dass das *„Internet kein rechtsfreier Raum“* sei, diese Zahlen deuten daraufhin, dass einige Menschen das Internet bzw. die Sozialen Medien als eine Art Angstraum wahrnehmen (Rüdiger 2019a, b; s. a. Kap. „Der digitale Raum ist kein (grund-)rechtsfreier Raum“). So gaben im Rahmen des Sicherheitsindex 2018 29,3 % der befragten Nutzer an, sich im Verhältnis zum Vorjahr bei der Nutzung des Internets unsicherer zu fühlen (Berneis et al. 2018; s. a. Kap. „Kriminalität und Unsicherheit im virtuellen Raum“ und „Strafbedürfnis und Kriminalitätsfurcht im Cyberspace“). Dabei stimmten 65,4 % der Nutzer der Aussage zu, dass die Nutzung sozialer Netzwerke das individuelle Risiko für Kriminalität erhöhen würde und 55,9 % waren der Meinung, dass sie der Umgang mit persönlichen Daten im Rahmen Sozialer Netzwerke verunsichern würde (Berneis et al. 2018). Aber nicht nur in „klassischen“ Sozialen Netzwerken scheint ein gewisses toxisches Verhalten vorhanden zu sein. Im Zusammenhang mit dem Onlinegame ‚Mordhau‘ wurde bekannt, dass das Spiel Nutzer verliert, da es im Spiel eine toxische Community gäbe, die u. a. rassistische Kommentare posten würde (Horti 2019). Interessanterweise soll das toxische Spieleverhalten vornehmlich auf Servern der Betreiber stattfinden; auf Servern, die von der Community betrieben werden, soll das Problem weniger ausgeprägt sein. Die Begründung liegt darin, dass der Betreiber zu wenige Moderatoren hätte, um gegen Hass in seinem Programm vorzugehen, die Community dies jedoch besser schaffen würde. Eine ähnliche Situation gab es auch in dem Onlinespiel *League of Legends,* dass mit einer toxischen Spielerschaft zu kämpfen hat. Der Betreiber Riot Games schaffte das Konstrukt eines Tribunals, was bedeutete, dass die Spielerschaft selbst über Fehlschritte anderer Nutzer urteilten durfte (Konert et al. 2016). Obwohl das Tribunal wieder abgeschafft wurde (Riot Games 2018), wirft diese Betrachtungsweise doch einen interessanten Aspekt auf: Sind Normenüberschreitungen auch im digitalen Raum dort stärker, wo sich die Community nicht für das jeweilige Medium einsetzt? Oder anders gefragt, dort wo die Community eine positive Verbindung mit dem Programm aufbaut, reguliert diese auch eher Normenbrüche?

5 Normenkontrolle in Sozialen Medien

Nach der Routine Activity Theorie gibt es im Kern drei Möglichkeiten für ein soziales Medium, auf den Normenbruch in seinem Bereich Einfluss zu nehmen (Cohen und Felson 1979). Einerseits kann versucht werden, die potenziellen Opfer von unterschiedlich denkbaren Delikten – von Betrugs- über Hass- bis

Sexualdelikte – widerstandsfähiger zu machen. Es kann versucht werden, die Täter durch die Vermittlung von Normen auf der jeweiligen Plattform von ihrem Normenbruch abzuhalten, im Sinne der Stärkung einer moralischen Widerstandsfähigkeit. Oder es kann versucht werden das Risiko für die Täter in unterschiedlichster Art und Weise zu erhöhen, sodass bei der Abwägung der Tathandlung die Schwelle nicht überschritten wird.

Wie und in welchen Umfang diese Mechanismen umgesetzt werden, ist wiederum eine individuelle Entscheidung der Betreiber. Dabei muss auch berücksichtigt werden, dass es keinen gemeinsamen Wertekanon alle Sozialer Medien Betreiber im Internet gibt. Zwar teilen sich diese eine digitale Infrastruktur, jedoch sind die Entscheidungsträger – sofern sie nicht aus einem Land stammen wie z. B. bei Facebook, Instagram und WhatsApp – von jeweils anderen rechtlichen, sozialen aber auch technischen Rahmenbedingungen geprägt. Gleichzeitig ist die Erwartungshaltung der Nutzer, die ebenfalls von völlig unterschiedlichen Rechtskonstrukten geprägt sind, entsprechend unterschiedlich (Hindelang 2019, S. 300). Beispielsweise wurde in Deutschland lange der Umgang von Facebook mit gewalthaltigen Videos und Medien im Verhältnis zu Bildern von stillenden Müttern thematisiert, da Facebook aus deutscher Sicht bei gewalthaltigen Medien zu wenig getan hat und bei „nackten Tatsachen“ wiederum rigoros handeln würde (Stern 2014). Diese Thematik zeigt sich zudem bei der Debatte um die Bekämpfung von sogenannter Hatespeech, wo gerade auch aus deutscher Sicht Facebook vorgeworfen wird, nicht aktiv genug vorzugehen. So wurde auf Basis des Netzwerkdurchsetzungsgesetzes (NetzDG) erstmalig gegen Facebook, aber nicht gegen andere Soziale Medien, ein Bußgeld in Höhe von 2 Mio. EUR verhängt (Berger 2019).

Gerade im Bereich des Kinder- und Jugendmedienschutzes zeigt sich, dass die Betreiber als solches nicht in der Lage sind, Normenbrüche angemessen zu verhindern. So sind aus nahezu allen Sozialen Medien Fälle von Cybergrooming – also der onlinebasierten Einleitung oder Intensivierung eines sexuellen Kindesmissbrauchs – oder anderen Übergriffen, wie dem unerwünschten Übersenden von pornografischen Medien, bekannt (Rüdiger 2019a; s. a. Kap. „Grooming-Umgebungen von pädophilen und hebephilen Männern in Deutschland“).

Ähnlich wie Stadtviertel oder ganze Städte unterschiedliche kriminogene Belastungen aufweisen können, scheint es auch bei Soziale Medien unterschiedliche Belastungsintensitäten zu geben. Wenn beispielsweise Twitternachrichten oder die Kommentare bei YouTube oder Facebookdiskussionen eher als toxisch betrachtet werden (Julentek 2019), so werden beispielhaft Programme wie LinkedIn, Xing, Jodel oder auch Instagram eher als positiv in der Normenkontrolle und der Kommunikationskultur wahrgenommen (Jodel 2019). Dies zeigt sich

weiterhin auch im Bereich der Gamingkultur, in der ähnliche Spiele – etwa *Battlefield* und *Call of Duty* – unterschiedlich wahrgenommen werden. So wird die Community in Call of Duty als wesentlich toxischer betrachtet als die in *Battlefield* (Stammler 2017). Gründe hierfür seien unter anderem, wie sich die Community zusammensetzt und mit dem Programm bzw. mit dem Game identifiziert (ebd.).

Offenbar ist die Frage wie Normen in Sozialen Medien angenommen und eingehalten werden, und ob damit das Programm selbst als toxisch wahrgenommen wird, auch davon abhängig, welche Rahmenbedingungen der Betreiber durch Sicherheitsmaßnahmen setzt und wie die Community sich mit dem jeweiligen Programm identifiziert und ggf. selbst die Normenkontrolle durchführt. Würde hier der Begriff der Sozialen Medien ausgetauscht werden mit dem des Wohnblocks oder des Stadtviertels, würde die Betrachtung stark dem Blickwinkel von Newman ähneln. Dies eröffnet die Frage, welche Erkenntnisse Betreiber Sozialer Medien ggf. aus der Defensible Space Theory ableiten können.

6 Handlungsmöglichkeiten von Betreibern Sozialer Medien nach der Defensible Space Theory

Nach Newman wird die Frage, ob ein Raum toxisch wird, vor allem durch die Aspekte der Territorialität, der natürlichen Überwachung, des Images und des Milieus bestimmt. Bezogen auf Soziale Medien könnte die Entstehung eines Territorialitätsbestrebens seitens der Einwohner – bzw. der Nutzer – bedeuten, dass diese sich gegen toxisches Verhalten von Nutzern wehren und das sie sich mit dem Sozialen Medium identifizieren und Normenbrüche als schädigendes Verhalten in dem jeweiligen Medium erfassen. Solche Ansätze und Tendenzen lassen sich in vielen Sozialen Medien finden. So bildete sich in dem Metaversum *Second Life* bereits relativ früh eine Art von Bürgerpolizei, die gegen Kriminalität in der Welt vorgehen wollte (Lundquist 2008). Andererseits gibt es auch immer wieder Aufrufe von Communitys, sich z. B. aktiv gegen Hassnachrichten zu stellen (s. a. Kap. „Hate Speech in der Computerspielkultur“). Ein bekanntes Beispiel hierfür ist das Konzept der Counterspeech, bei dem auf Hassnachrichten mit aktiver Gegenrede reagiert werden soll (Sponholz 2018, S. 197). Dies soll erfolgen, um eine Normalität des Normenbruchs, oder gar die Entstehung eines anomischen Raumes, zu verhindern. Dabei wird davon ausgegangen, dass Counterspeech vor allem dann wirksam ist, wenn es aus unterschiedlichen Quellen kommt (Sponholz 2018, S. 199). Dies ergibt Sinn, da dies den Hatespeechern zeigt, dass ein größerer Umfang der Community offenbar entsprechende

Normenüberschreitungen nicht hinnimmt. Dies erhöht – auch im Sinne einer moralischen Konfrontation – die Risiken für einen Täter, was nach der Routine Activity Theory wiederrum die Hemmschwelle zur Normenüberschreitung ansteigen lässt.

Counterspeech erfordert jedoch einige Rahmenbedingungen. Auf der einen Seite muss sich überhaupt eine gewisse Anzahl an Nutzern zusammenfinden, um aktiv gegen Normenüberschreitungen zu agieren. Hierzu müssen die Nutzer es auch für relevant erachten, sich für ein bestimmtes Medium einzusetzen. Es muss also letztlich ein Milieu in dem Programm entstehen, dass überhaupt ein Interesse an einer Normeneinhaltung hat. Dieser Umstand kann beispielhaft dann relevant werden, wenn die Nutzer denken, dass ein Betreiber wenig Interesse an einer Normenregulierung in seinem Programm hat, sich also ein Einsatz kaum lohnt. Es hängt demnach auch vom Image der Betreiber ab.

Aus Sicht des Betreibers könnte eine Art Kosten-Nutzen-Analyse vorgenommen werden: wie viel kostet eine entsprechende Unterstützung und Gestaltung einer positiven Community und wie viele – je nach Geschäftsmodell zahlende – Nutzer verliert er, wenn die positive Umsetzung nicht erfolgt, die Community also als toxisch oder ‚gekippt' gelten kann. Dies unterscheidet – nicht per se gänzlich, aber doch in einem gewissen Umfang – wiederum die Interessenlagen von Betreibern Sozialer Medien von denen eines Bürgermeisters. Obwohl prinzipiell beide ein Interesse haben sollten, eine „Community of Interest" zu schaffen – also eine Community, die das Bewusstsein gewonnen hat, selbst für Sicherheitsbelange verantwortlich zu sein (Kube 1982, S. 44) – da dies auch wirtschaftlich gesehen ein kostengünstigerer Sicherheitsfaktor ist, so stehen für einen Betreiber ökonomische Faktoren vermutlich höher im Blickfeld als für diesen Bürgermeister oder Politiker. Hier bieten gerade Onlinespiele Beispiele für die Möglichkeiten der Schaffung eines positiven Milieus und einem entsprechenden Image. So könnten Nutzer, die sich aktiv für ein positives Klima einsetzen, für positive Handlungen belohnt werden – beispielhaft durch besondere optische Markierungen, Items oder auch sog. Skins.

Als eine kriminalpolitische Maßnahme, um gegen Angsträume vorzugehen, kann das Prinzip des „Crime Prevention Through Environmental Design" (CPTED), also eine Art natürliche Überwachung, angesehen werden. Das Credo dabei lautet, Menschen in ihrem Verhalten innerhalb ihres Lebensraumes positiv und damit zu sozial adäquatem Verhalten zu lenken und im besten Fall auch Kriminalität vorzubeugen (Schnittger und Schubert 2002). Während im physischen Raum im Rahmen der kriminalpräventiven Siedlungsgestaltung risikoreiche Aspekte erkannt werden können, die es zu verändern gilt wie z. B. die unzureichende Beleuchtung, unübersichtliche Nischen, Orte mit illegaler

Abfallentsorgung und Ähnlichem (Schnittger und Schubert 2002, S. 9 ff.), gibt es für Soziale Medien vor allem im Bereich des Jugendmedienschutzes mit dem Konzept „Safety by Design“ ein vergleichbares Instrument (Croll und Gräter 2015). Dieses Konzept bedeutet, dass der Betreiber Sozialer Medien ein digitales Umfeld schafft, dass bereits durch seine Konstruktion Normenüberschreitungen – faktisch Kriminalität – verhindern bzw. erschweren soll. Die Mechanismen hierzu sind unterschiedlichster Natur und reichen von Klarnamenpflicht, die beispielhaft über Post-Identverfahren sichergestellt werden könnten, über die Implementierung von Algorithmen zur automatischen Detektion von Normenüberschreitungen wie Beleidigungen, Hasskriminalität (Geschke et al. 2019) oder sexuellen Belästigung bis zu Belohnungselementen für positives Normenverhalten, wie das Herausheben von Kommentaren oder das Kennzeichnen von Avataren.

Der Defensible Space Ansatz sagt zudem, dass gerade wenig einsehbare Bereiche – die also z. B. baulich wenig Licht haben oder verwinkelt sind und nicht zur Identitätsbildung beitragen – Normenüberschreitungen begünstigen könnten (Rolinski 1980). Auf Soziale Medien übertragen bedeutet dies, dass vor allem private Bereich – die also von der Allgemeinheit der Nutzer eher wenig reflektiert und damit aufgesucht werden – eher für Normenabweichungen genutzt werden. Ein gutes Beispiel hierfür sind im Bereich virtueller Welten private Gruppenräume oder Instanzen, bei denen die Ersteller die Möglichkeit haben, die Nutzer, die diese Räume betreten, einzugrenzen. So wurde bei dem bekannten Metaversum *Second Life* aufgezeigt, wie in durch Nutzer selbst gestalteten Räumen, Normenbrüche bis hin zur Darstellung des Missbrauchs von Kindern oder der Vergewaltigung von Frauen und Tieren stattfinden (Dirry und Rüdiger 2015, S. 128 ff.). Auf einer Metaebene könnte entsprechend auch das Darknet hierunter erfasst werden. Im Bereich des Cybergroomings wollen zudem Täter – soweit es das jeweilige Programm zulässt – meist Kommunikationen in einen privaten Bereich umlagern. Das können auch private Räume sein wie es sie z. B. in *Habbo Hotel* – einem Metaversum – gibt (Dölling und Baier 2013). Obwohl es natürlich im Interesse der Nutzer als auch der Betreiber ist, dass es entsprechende private Rückzugsmöglichkeiten gibt und diese beispielsweise ggf. auch vulnerablen Gruppen und Individuen Sicherheit bieten können, muss ein Betreiber ähnlich wie ein Stadtplaner solche Aspekte berücksichtigen und gerade virtuelle Räume möglichst transparent gestalten.

Neben solchen „raumgestalterischen“ Maßnahmen kann ein Betreiber – genauso wie ein Bürgermeister oder Stadteilverantwortlicher – natürlich auch auf flankierende Maßnahmen wie Moderation und der Kooperation mit der Justiz setzen. Nach dem Broken Web Ansatz kommt es hierbei jedoch nicht darauf an, dass z. B. der Betreiber einfach normenbrechende Kommentare oder auch

verursachende Accounts löscht. Vielmehr kommt es darauf an, dass der Betreiber für seine Community sichtbar gegen Normenverstöße vorgeht. Das kann z. B. passieren, in dem ein Kommentar nicht stillschweigend gelöscht wird, sondern an der entsprechenden Stelle der Hinweis erfolgt, dass hier ein Kommentar gegen die Regeln oder das jeweils gültige Strafrecht verstoßen hat und daher gelöscht wurde. Diese Sichtbarkeit zeigt den Nutzern, dass der Betreiber ein Interesse an der Normendurchsetzung hat. Potenziellen Tätern wird wiederum aufgezeigt, dass eine Tathandlung ein Risiko beinhalten kann, was wiederum die Hemmschwelle zur Tatbegehung erhöhen könnte. Und letztlich wird potenziellen Opfern signalisiert, dass gegen Normenverstöße auch tatsächlich vorgegangen wird, was wiederum deren Bereitschaft sich zu wehren, z. B. durch Counterspeech, erhöhen kann.

Obwohl der Ansatz von Newman wie dargestellt in vielen Aspekten auf den digitalen Raum übertragbar ist, ist doch auch erkennbar, dass der Ansatz nicht gänzlich auf das Internet adaptiert werden kann. Dies liegt einerseits daran, dass nicht alle physischen Möglichkeiten auch eine digitale Entsprechung haben. So ist eine Hecke als sichtbare Abgrenzung kaum in einem klassischen Sozialen Medium – mit Ausnahme von virtuellen Welten – denkbar. Auch sind die rechtlichen, kulturellen und sozialen Rahmenbedingungen – je nach Sozialem Medium – geprägt von dem jeweiligen Ursprungsstaat aus dem der Betreiber stammt. Ein alleiniger defensible Space im Sinne eines gesamten durch technische Maßnahmen geschützten digitalen Raumes, erscheint zum aktuellen Zeitpunkt nicht denkbar. Zu unterschiedlich erscheinen beispielsweise Überwachungsmaßnahmen wie Social Scoring aus China und beispielhaft der Diskussion um die Vorratsdatenspeicherung in Deutschland.

Dennoch ist es bezogen auf einzelne Soziale Medien durchaus denkbar, das Betreiber Maßnahmen des Defensible Space Ansatzes auch umzusetzen. Dies kann von Möglichkeiten der Territorialität – durch Individualisierungsmöglichkeiten z. B. der Accounts, der natürlichen Überwachungsmaßnahmen – indem Zugangsdaten z. B. durch EPost-Identverfahren vergeben werden, Klarnamen eingesetzt werden, aber auch der Schaffung eines positiven Images und der Gestaltung eines entsprechenden Milieus (vgl. Abb. 1).

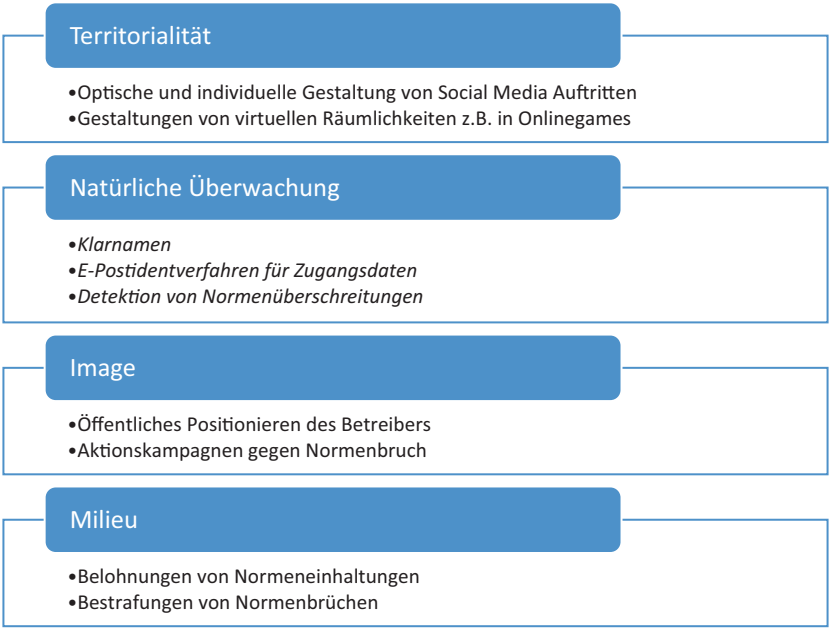


Abb. 1 Gestaltungsmöglichkeiten nach Newman

7 Schlussfolgerungen

Diese vorgenannten Gedankengänge haben Auswirkungen auf kriminalpolitische Lösungsansätze für Normenüberschreitungen im digitalen Raum. Denn ein System kann zwar für sich selbst Normen durchsetzen, Menschen bewegen sich aber nicht nur in einem Stadtviertel bzw. einem Sozialen Medium. Wenn Menschen immer wieder in Bereichen unterwegs sind, in denen Normen nicht durchgesetzt werden, kann sich ein Gefühl entwickeln, dass Normen im gesamten Metasystem – hier dem Internet – nicht durchgesetzt werden. Vergleichbar wäre dies zu einer Situation, in der Menschen immer nur in Stadtgebieten unterwegs sind, in denen eine Art Angstkultur herrscht und sie diese auf das gesamte Stadtgebiet übertragen. Entsprechend könnte dies einen Grund für die häufig genutzt Analogie der „Rechtsfreiheit des Internets“ darstellen (Stadler 2009).

Sailer beschreibt Angsträume als subjektiv empfundene Unsicherheitsbereiche. In Abgrenzung zum klassischen Tatort muss also keine statistische

oder aber tatsächliche Unsicherheit herrschen (Sailer 2003, S. 53). Die entscheidende Komponente in dem Angstraum ist das Element „Sicherheit“ (Sailer 2003). Schon Maslow hat in seiner bekannten Maslowschen Bedürfnispyramide der Sicherheit einen hohen Stellenwert beigemessen. Sie folgt gleich nach dem Grundbedürfnis nach Essen, Trinken und Schlafen (Kappeler 2001, S. 1 ff.). Wenn Menschen etwas als Gefahr wahrnehmen bzw. Angst haben, reagieren sie mit Schutz- oder Vermeidungsverhalten (Köhn und Bornewasser 2012, S. 2 ff.). Die U25 Studie ergab beispielsweise, dass 1/3 der befragten Jugendlichen aufgrund der Konfrontation mit Hasskriminalität im Netz auf eigene Meinungsäußerungen verzichten, also Vermeidungsverhalten zeigen (Borgstedt et al. 2018). Silencing – also das Vermeiden einer politischen Meinungsäußerung als Reaktion auf Hasskommentare – wird nach einer weiteren repräsentativen Studie von fast 54 % der Internetnutzer als adäquate Lösung angesehen und weitere 47 % vermeiden die Teilnahme an Diskussionen im Internet (Geschke et al. 2019, S. 28). Anscheinend wird von vielen Internetnutzern das Internet als ein Angstraum wahrgenommen. Insofern kann von einer Art „Herrschaft der Unrechtskultur“ im Internet gesprochen werden (Rüdiger 2019a).

Die Erkenntnisse der Defensible Space Theory können hierbei wichtige Ansätze liefern, auch die Strukturen von Sozialen Medien anzupassen und diese Entwicklung sowohl auf einer Makro- als auch auf einer Metaebene zu begegnen. Die Frage inwiefern Betreiber – die vornehmlich ein wirtschaftliches Interesse verfolgen – Safety by Design umsetzen und welche Maßnahmen dies genau erfasst, ist dabei nicht singulär zu beantworten. Einerseits werden Betreiber Aspekte wie das Image ihrer Plattform und den Normenbruch vermutlich vor allem dann berücksichtigen, wenn sich dies in schwindenden Nutzerzahlen äußern sollte. Andererseits gibt es kein gemeinsames Normen- oder Moralverständnis, das alle Betreiber Sozialer Medien teilen. Hier ist wiederum die Schnittstelle zur Politik, die letztlich entsprechende Vorgaben an die Betreiber Sozialer Medien geben könnte. Dies erfolgte z. B. im Rahmen der Umsetzung des Netzwerkdurchsetzungsgesetzes (NetzDG), nach welchem die Politik den Betreibern Sozialer Medien Vorgaben zur Bekämpfung von Normenbrüchen gemacht hat, insbesondere durch die Implementierung eines Melde- und Beschwerdeverfahrens. Undenkbar ist so etwas nicht: so ist im Rahmen des § 1 Abs. 6 Nr. 1 des Baugesetzbuches (BauGB) geregelt, dass bei der Aufstellung von Bauleitplänen die Sicherheit der Wohn- und Arbeitsbevölkerung zu beachten ist, im Sinne einer Zielbestimmung. Ähnliches wäre auch für Betreiber Sozialer Medien denkbar.

Eines muss aber einer Gesellschaft klar sein: wenn die Normenkontrolle weitestgehend auf die Betreiber einzelner Plattformen ausgelagert wird, schwächt

dies – auch im Sinne von Newman – die klassischen rechtstaatlichen Prinzipien. Entsprechend wichtig scheint es, diese Mechanismen nur als einen Teil einer kriminalpolitischen Gesamtstrategie anzusehen; ähnlich wie auch bauliche Maßnahmen als ortsbezogene Kriminalprävention betrachtet werden können, die aber dennoch in ein übergeordnetes Rechts- und Normenkonstrukt eingebunden sind. Im digitalen Raum ist dies noch nicht der Fall wie u. a. die Debatten um digitale Polizeiarbeit und deren Verortung zeigen, aber auch der stetigen Betonung „das Internet sei kein rechtsfreier Raum“ zu entnehmen ist. Klassische kriminologische Ansätze können aber dennoch bei einer an diesen digitalen Raum orientierten Adaption wertvolle Erkenntnisse liefern, die nicht unbeachtet gelassen werden sollten. Denn eine Art digitale Architektur, die auf den Grundlagen von Newman basiert, hat das Potenzial Normenbruch im Netz zu minimieren.

Literatur

Berger, D. (2019). NetzDG: Facebook muss Millionen-Bußgeld zahlen. https://www.heise.de/newsticker/meldung/NetzDG-Facebook-muss-Millionen-Bussgeld-zahlen-4460759.html.

Berneis, N., Lückmann, H., Möllering, A., & Weber, T. (2018). Sicherheitsindex 2018. Digitale Sicherheitslage der Verbraucher in Deutschland. DSIN.

Borgstedt, S., Borchard, I., Jurczok, F., Javakhishvili, E., & Repohl, I. (2018). DIVSI U25-Studie – Euophorie war gestern. Die “Generation Internet” zwischen Glück und Abhängigkeit. DIVSI. https://www.divsi.de/wp-content/uploads/2018/11/DIVSI-U25-Studie-euphorie.pdf.

Born, S. (2009). *Kommunale Kriminalprävention in einer Großstadt. Mehr Prävention oder mehr Repression? Eine Risiko- und Potenzialanalyse kommunaler Präventionsstrukturen in Berlin* (Zugl.: Berlin, Humboldt-Univ., Diss., 2008). Berlin: Logos.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588. https://doi.org/10.2307/2094589.

Croll, J., & Gräter, T. (2015). Konkretisierung des Prinzips Safety by Design anhand von drei Produkttypen. Zentrum für Kinderschutz im Internet – Jahresbericht 2015. https://kinderrechte.digital/assets/includes/sendtext.cfm?aus=11&key=1496. Zugegriffen: 17. Juni 2019.

Dirry, V., & Rüdiger, T.-G. (2015). Second Life in aller Munde. In T.-G. Rüdiger & A. Pfeiffer (Hrsg.), *Game! Crime?* (S. 126–138). Frankfurt: Verl. für Polizeiwiss.

Dölling, D., & Baier, D. (2013). Täter, Taten, Opfer. Grundlagenfragen und aktuelle Probleme der Kriminalität und ihrer Kontrolle. Mönchengladbach: Forum-Verl. Godesberg (Neue Kriminologische Schriftenreihe, 114). http://www.krimg.de/drupal/files/9783942865111.pdf.

Frees, B., & Koch, W. (2019). ARD/ZDF-Onlinestudie 2018. Zuwachs bei medialer Internetnutzung und Kommunikation. *Media Perspektiven, 9/2018,* 398–413.

Frondorf, E. (2007). Pruitt-Igoe: Utopic Expectations Meet Tenement-Infused Realities. Yale. https://ctl.yale.edu/sites/default/files/files/Frondorf-American%20Studies5.pdf.

Geschke, D., Klaßen, A., Quent, M., & Richter, C. (2019). #Hass Im Netz. Forschungsbericht.

Hindelang, S. (2019). *Freiheit und Kommunikation. Zur verfassungsrechtlichen Sicherung kommunikativer Selbstbestimmung in einer vernetzten Gesellschaft*. Berlin: Springer. https://doi.org/10.1007/978-3-662-57687-8.

Horti, S. (2019). Rampant racism and toxicity are driving players away from Mordhau. https://www.facebook.com/pcgamermagazine. https://www.pcgamer.com/rampant-racism-and-toxicity-are-driving-players-away-from-mordhau/. Zugegriffen: 6. Juli 2019.

Jodel – Jodel bleibt bunt. (2019). https://jodel.com/blog/jodel-bleibt-bunt/. Zuletzt aktualisiert am 17.04.2019, Zugegriffen: 16. Juli 2019.

Julentek. (2019). Online-Diskussionen führen zwangsläufig zu Hass und Hetze. https://www.facebook.com/thebuzzard.org/. https://thebuzzard.org/2019/01/03/soziale-medien-hass-hetze/. Zugegriffen: 16. Juli 2019.

Kanol, E. (2008). Eine Analyse ausgewählter raumstrukturbezogenen Kriminalitätstheorien: „Defensible Space“ und „Broken Windows“.

Kappeler, A.-M. (2001). *Öffentliche Sicherheit durch Ordnung. Konfliktlagen im öffentlichen Raum und ihre Bekämpfung durch aufenthaltsbeschränkende Maßnahmen (Platzverweis und Aufenthaltsverbot): Bd. 1. Schriften zum Recht der inneren Sicherheit* (Zugl.: Passau, Univ., Diss., 1999–2000). Stuttgart: Boorberg.

Kelling, G.L., & Wilson, J. Q. (1982). Broken windows: The police and neighborhood safety. *Atlantic Monthly, 249*(3), 29–38.

Köhn, A., & Bornewasser, M. (2012). Subjektives Sicherheitsempfinden. https://www.pal-verlag.de/lebenshilfe-abc/vermeidungsverhalten.html.

Konert, J., Söbke, H., & Wendel, V. (2016). Social network games. In R. Dörner, S. Göbel, M. Kickmeier-Rust, M. Masuch, & K. A. Zweig (Hrsg.), *Entertainment computing and serious games* (S. 442–475). International GI-Dagstuhl Seminar 15283, Dagstuhl Castle, Germany, July 5–10, 2015. Revised selected papers (Lecture notes in computer science, 9970). Cham: Springer.

Kube, E. (1982). *Städtebau, Wohnhausarchitektur und Kriminalität. Prävention statt Reaktion: Bd. 15. Kriminalistik, Wissenschaft & Praxis*. Heidelberg: Kriminalistik.

Lundquist, R. (2008). Einsatz für die Polizei in Secondlife. http://rikeswochenschau.blogspot.com/2008/05/einsatz-fr-die-polizei-in-secondlife.html.

Newman, O. (1996). *Creating defensible space*. U.S. Department of Housing and Urban Development.

Riot Games. (2018). Kommt das Tribunal zurück? https://nexus.leagueoflegends.com/de-de/2018/08/will-tribunal-return/.

Rolinski, K. (1980). Wohnhausarchitektur und Kriminalität – BKA Forschungsreihe Band 13, Wiesbaden. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/BkaForschungsreihe/2_13_WohnhausarchitekturUndKriminalitaet.html. Zugegriffen: 13. Nov. 2018.

Rüdiger, T.-G. (2018). Das Broken Web: Herausforderung für die Polizeipräsenz im digitalen Raum. In T.-G. Rüdiger & P. S. Bayerl (Hrsg.), *Digitale Polizeiarbeit. Herausforderungen und Chancen (Research)* (S. 259–299). Wiesbaden: Springer VS.

Rüdiger, T.-G. (2019a). Haben wir eine Unrechtskultur im digitalen Raum? *Kriminalistik, 1,* 37–43.

Rüdiger, T.-G. (2019b). Polizei im digitalen Raum (21–23/2019), S. 18–23. http://www.bpb.de/apuz/291183/polizei-im-digitalen-raum?p=all.

Rüdiger, T.-G., & Pfeiffer, A. (Hrsg.). (2015). *Game! Crime?* Frankfurt: Verl. für Polizeiwiss.

Sailer, K. (2003). Sicherheit im öffentlichen Raum aus feministischer Perspektive. https://kerstinsailer.files.wordpress.com/2013/05/sicher.pdf.

Sautter, U. (2011). bpb.de – Dossier USA – Geschichte – Nach der Eroberung des Westens – Eine Nation betritt die Weltbühne. Bundeszentrale für politische Bildung. http://www.bpb.de/internationales/amerika/usa/10601/die-usa-betreten-die-weltbuehne. Zuletzt aktualisiert am 24.11.2011, Zugegriffen: 25. Febr. 2019.

Schnittger, A., & Schubert, H. (2002). *Sicheres Wohnquartier Gute Nachbarschaft. Handreichung zur Förderung der Kriminalprävention im Städtebau und in der Wohnungsbewirtschaftung*. http://www.sicherheit-staedtebau.de/html/download.cms?id=18&datei=Sicheres-Wohnquartier-gute-Nachbarschaft-18.pdf. Zugegriffen: 20. Nov. 2018.

Schwind, H.-D. (2016). *Kriminologie und Kriminalpolitik. Eine praxisorientierte Einführung mit Beispielen: Bd. 28. Grundlagen – Die Schriftenreihe der "Kriminalistik"* (23., neu bearbeitete underweiterte Aufl., Unter Mitarbeit von Jan-Volker Schwind). Heidelberg: Kriminalistik.

Sponholz, L. (2018). *Hate Speech in den Massenmedien. Theoretische Grundlagen und empirische Umsetzung*. Wiesbaden: Springer Fachmedien.

Stadler, T. (2009). Internet-Law » Das Internet ein rechtsfreier Raum? http://www.internet-law.de/2009/06/das-internet-ein-rechtsfreier-raum.html. Zugegriffen: 17. Juli 2019.

Stammler, C. (2017). Darum werden Online-Communites toxisch. https://gamingnewstime.de/darum-werden-online-communites-toxisch/.

Stern, C. (2014). Facebook löschte Foto von stillender Mutter – WELT. https://www.facebook.com/welt. https://www.welt.de/vermischtes/article133816821/Facebook-loescht-Brust-Foto-und-sagt-danach-sorry.html. Zuletzt aktualisiert am 01.01.2014, Zugegriffen: 9. Juli 2019.

Phänomenologie von Kriminalität im digitalen Raum

Darknet – die dunkle Seite des Internets?

Tim Henkel

Wenn Waffen, Betäubungsmittel, gefälschte Ausweise, Falschgeld, Dienste eines Hackers oder gestohlene Daten den Besitzer wechseln und diese Geschäfte im digitalen Raum zustande kommen, befinden wir uns mit an Sicherheit grenzender Wahrscheinlichkeit im sogenannten Darknet.

Was ist das Darknet? Wie gelangt man dorthin? Wer benutzt es?

Warum bei einer einfachen Suche im Internet nach dem Begriff Darknet ein Eisberg eine große Rolle spielt, worum es sich bei diesem Darknet überhaupt handelt und wie dunkel dieser Teilbereich des Internet tatsächlich ist, soll im Rahmen dieses Kapitels geklärt werden, um somit Licht ins „dunkle Netz" zu bringen.

Das durch jeden täglich genutzte Internet wird in Abgrenzung zu den Begriffen „Deepweb" und „Darknet" auch als „Clearnet", „Surface Web" oder auch „visible Web" bezeichnet. Letzteres zeichnet sich dadurch aus, dass es durch gängige Internet-Suchmaschinen indexiert, also auffindbar und mit den üblichen Internetbrowsern erreichbar ist. Als „Deepweb" bezeichnet man den Teilbereich des Internet, der mit üblichen Internet-Suchmaschinen nicht indexiert wird, somit nicht durch Suchbegriffe auffindbar, jedoch mit üblichen Internetbrowsern erreichbar ist (Eckermann 2017). Hier sind als Beispiele unternehmensinterne Computernetzwerke (Intranets) oder ähnliche interne Netzwerke (z. B. Datenbanken) für geschlossene Benutzergruppen zu nennen.

Ein Teilbereich des Deepweb ist das sogenannte „Darknet". Hierbei handelt es sich um ein Netzwerk, welches zusätzlich zu der fehlenden Indexierung durch gängige Internet-Suchmaschinen, auch nicht mit herkömmlichen Browsern erreichbar ist

T. Henkel (✉)
Mainz, Deutschland
E-Mail: timhenkel@gmx.de

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

T.-G. Rüdiger und P. S. Bayerl (Hrsg.), *Cyberkriminologie,*
https://doi.org/10.1007/978-3-658-28507-4_7

und bei dem sämtliche Daten anonymisiert übermittelt werden. Man spricht in diesem Zusammenhang daher auch von „hidden services“, also versteckten Diensten.

Der Begriff des „Darkweb“ (Kompositum aus Darknet und Deepweb) wird unregelmäßig und eher außerhalb Deutschlands als Synonym des beschriebenen Darknet genutzt. Im Folgenden wird auf eine Nutzung dieses Kompositums verzichtet.

1 Wie kommt nun der Eisberg ins Spiel?

Man geht derzeit davon aus, dass die Datenmenge des eben beschriebenen Clearnet die Spitze eines Eisbergs aus Daten darstellt. Der verborgene Teil dieses Dateneisberges, welcher unter Wasser liegt und nicht sichtbar ist, beinhaltet das zuvor genannte Deepweb, in welchem auch das Darknet zu finden ist. Die exakte Größe des Deepweb kann nicht eindeutig bestimmt werden, da der Zugriff auf dort befindliche Datenbanksysteme und Webseiten von außerhalb nicht möglich ist.

Es existieren Studien aus dem Jahr 2001, wonach die Datenmenge des Deepweb die des Clearnet zum damaligen Zeitpunkt um das 500fache übersteigen sollte (Bergman 2001). Zum Zeitpunkt dieser Studien wurden mehr als 200.000 Deepweb-Seiten festgestellt, darunter auch Darknet-Webseiten. Die dezidierte Messung der Anzahl der „hidden services“ war jedoch nicht Gegenstand der genannten Studien.

2 Darknet: Mythos vs. Realität

Ist ein hoher technischer Sachverstand oder sind sogar die richtigen Kontakte zu Kriminellen notwendig, um ins Darknet zu gelangen? Kann ich mich versehentlich ins Darknet klicken und mich so einer etwaigen Strafverfolgung aussetzen?

Bevor das Thema Darknet durch mediale Berichterstattung in den Vordergrund drang, bestand der weit verbreitete Mythos, dass man dieses nur durch spezielle technische Affinität und Kontakte aus der analogen Welt erreichen könne. In Teilen existiert dieser Irrglaube weiterhin.

Tatsächlich besteht die Möglichkeit mittels des Internetbrowsers Tor (Akronym von „The Onion Router“) ohne größere Hindernisse in den sogenannten „dunklen“ Teil des Internets zu gelangen. Der Download der zugehörigen, kostenlosen Software ist vergleichsweise einfach. Es existieren einschlägige, legale Webseiten im Internet, welche die benötigte Software zum Download anbieten. Die Installation und Einrichtung des Browsers ist ebenfalls problemlos, da dieser auf dem

bekannten Internetbrowser Mozilla Firefox basiert. Dieser ist für seine einfache Handhabung bekannt, da er in den Standardeinstellungen keinen Einrichtungsaufwand benötigt.

2.1 Wie funktioniert Tor?

Dem Namen nach handelt es sich bei „The Onion Router“ um die Leitung oder Führung nach dem Zwiebelprinzip (The Tor Project o. D.a). Herkömmliche Internetbrowser bauen die Verbindung zu Webseiten oder Diensten bei entsprechendem Aufruf über den jeweiligen Internetprovider auf. So ist es für Internetprovider anhand der jeweiligen IP-Adresse seiner Kunden möglich zu erkennen, welche Webseiten dieser besucht. Tor hingegen verschachtelt die Internetverbindung des Nutzers und baut diese nicht, wie beschrieben, mittelbar über den jeweiligen Internetprovider, sondern über drei zufällig ausgewählte Knotenpunkte (sog. „Nodes“ oder „Guards“) auf. Beim Verbindungaufbau erfährt so jeweils nur der direkt benachbarte „Node“, von wem die Anfrage kam. Diese Knotenpunkte stehen stellvertretend für die Schale einer Zwiebel und waren Basis für die Namensgebung von Tor.

Diese Art des Verbindungsaufbaus führt zu einer völligen Anonymität des Nutzers im Internet, da sich die IP-Adresse durch dieses Prinzip nicht einer Person zuordnen lässt. Durch das Prinzip dieser Kaskadierung ist jedoch die Performance von Tor, also die Schnelligkeit des Verbindungsaufbaus, deutlich vermindert. Dies ist für viele Nutzer ein Ausschlusskriterium für den täglichen Gebrauch von Tor als Standard-Internetbrowser. Aufgrund der weitreichenden Popularität von Tor wird hier auf die Erläuterung von weiterer Software, die ähnlichen Zwecken dient, wie beispielsweise i2P (The invisible Internet project) oder Hornet (Highspeed Onion Routing Network) aus Gründen der vereinfachten Darstellung verzichtet.

Tor kann wie ein herkömmlicher Internetbrowser genutzt werden. Es ist also möglich mittels Tor jede Webseite im Clearnet anonym aufzurufen. Zusätzlich kann Tor neben dieser Nutzung als Standard-Browser auch der Schlüssel zu Webseiten innerhalb des Darknet sein, die auch als „hidden services“ oder „Onion-Seiten“ bezeichnet werden. Diese Bezeichnung rührt daher, dass diese die Domainendung .onion tragen und nicht andere generische (.net, .org) oder länderspezifische Top-Level-Domains (.de, .at, .ch). Diese .onion-Seiten sind nur mittels Tor zu erreichen.

Die „hidden services“ zeichnen sich neben der Domainendung auch durch eine Domain aus, welche aus einer zumeist nicht logisch zusammenhängenden

Kombination aus Buchstaben und/oder Zahlen besteht. So könnte beispielsweise eine Darknet-Domain aussehen: *3g2upl5pq3knfc4m.onion.*

Aber warum werden diese hidden services und nicht normale Webseiten genutzt?

Die hidden services zeichnen sich dadurch aus, dass aufgrund der Anonymität innerhalb des Tor-Netzwerks deren Standort und deren Betreiber nicht ohne weiteres zu ermitteln sind. Tor-Nutzer, die den hidden service aufrufen, tun dies über einen zugewiesenen Meeting-Point innerhalb des Tor-Netzwerkes. Dieser kennt ebenfalls nur seinen nächsten Nachbarn und kann den Datenverkehr somit selbst nicht mitlesen (Schmidt 2016). Es gibt diverse Programme, die bei der Erstellung solcher Domains behilflich sind, beispielsweise *The Enterprise Onion Toolkit* (EOTK) des Entwicklers Alec Muffet.

Auch ist es möglich, aufgrund bestehender Clearnet-Domains eine zugehörige Onion-Domain zu erstellen. Facebook beispielsweise besitzt seit 2014 auch eine Domain, welche sich im Darknet befindet, und über die Onion-Domain *facebookcorewwwi.onion* erreichbar ist.

Dass die Nutzung von Tor nicht unmittelbar mit dem Darknet gleichzusetzen ist, ist essenziell für das Verständnis des Verhältnisses zwischen Tor und dem Darknet. Versucht man nun zur Verbesserung des Verständnisses eine Analogie zwischen Tor und einem anderen Gegenstand aus der analogen Lebenswirklichkeit herzustellen, könnte man hier als Beispiel eine Sturmhaube anführen. Diese ist wie Tor frei und ohne Restriktionen erwerbbar. Sie dient dem eigentlichen Zweck nach beispielsweise Motorradfahrern oder Feuerwehrkräften zum Schutz, kann jedoch auch missbräuchlich bei der Begehung von Straftaten genutzt werden, beispielsweise zur Verschleierung der Identität bei Raubstraftaten oder ähnlich gelagerten Delikten. Der Besitz oder das Tragen einer Sturmhaube ist in Deutschland, mit wenigen Ausnahmen (bspw. Vermummungsverbot), jedoch grundsätzlich nicht unter Strafe gestellt.

Tor ist somit eine digitale Sturmhaube, die sowohl dem Schutz unbescholtener Nutzer in Bezug auf deren Identität dient, aber auch etwaige Straftäter schützen kann (s. a. Kap. „Strafverfolgung digital“).

2.2 Die Geschichte von Tor

Tor wurde offiziell im Jahre 2002 durch das gemeinnützige Tor-Project, welches seinen Sitz in den USA hat, veröffentlicht, zunächst mit der Maßgabe und dem Zweck die Privatsphäre und Sicherheit seiner Nutzer zu schützen (The Tor Project o. D.a, b) so liest es sich zumindest auf der projekteigenen Webseite. Die Anfänge von

Tor liegen jedoch weiter zurück und werden auch heute noch deutlich umstrittener diskutiert.

Mitte der 90er Jahre startete ein gemeinsames Forschungslabor der United States Navy und dem United States Marine Corps (US Naval Research Laboratory) ein Projekt, mittels welchem verschiedene Computer innerhalb eines Netzwerks verschlüsselt kommunizieren können und mittels welchem sowohl Quelle als auch Ziel der Kommunikation verschleiert werden sollten. Nach 1997 wurde dieses Projekt durch die Forschungsbehörde des Verteidigungsministeriums der USA (Defense Advanced Research Projects Agency, DARPA) weiter entwickelt. Erst 2002 wurde das Projekt an eine gemeinnützige Stiftung und von dort aus dem Tor Project übergeben. Die Mehrheit der finanziellen Unterstützung rührt jedoch immer noch aus Regierungskreisen, vor allem aus der USA und Schweden (ExpressVPN 2018).

Diese Einbindung von Regierungsbehörden in den Anfängen der Entwicklung von Tor sind natürlich ein Nährboden für Verschwörungstheorien und Kritiker von Tor. Dennoch haben neben Journalisten in autoritären Staaten mit deutlichen Einschränkungen der Pressefreiheit und politisch Verfolgte oder Minderheiten auch Kriminelle die Vorteile der Anonymität von Tor erkannt. Es sei jedoch gesagt, dass es sich hierbei nicht ausschließlich um Cyberkriminelle handeln muss. Auch andere Deliktfelder, wie der Handel mit Waffen, Betäubungsmitteln und gefälschten Urkunden, welche eher analoger Natur sind, finden sich im Darknet wieder.

3 Die helle Seite

Es wäre fatal und falsch Tor oder gar alle Nutzer von Tor zu kriminalisieren. In einem demokratischen Staat, der Menschen – und Grundrechte – achtet, wird man allerdings eher auf seine Nutzung verzichten, als in Staaten, die autoritär regiert werden und in welchen die Grundrechte auf freie Meinungsäußerung und Pressefreiheit nicht den unabdingbar hohen Schutz genießen, wie beispielsweise in Deutschland. Hier wären als Nutzer zum Beispiel Journalisten in autoritären Staaten, Dissidenten, politisch Verfolgte sowie Minderheiten zu nennen. Die „helle Seite“ von Tor bzw. des Darknet zeigte sich zum Beispiel im Rahmen des arabischen Frühlings.

Als im Dezember 2010 der sog. „Arabische Frühling“ in Tunesien seinen Anfang nahm und die Menschen in den Ländern Nordafrikas und im Nahen Osten auf die Straßen gingen, um gegen die Autokratie in deren Staaten zu protestieren, formierte sich auch im digitalen Bereich der Widerstand (Baurmann 2016). Zum

Schutz vor staatlicher Strafverfolgung nutzten viele Aktivisten, Pressevertreter und Oppositionelle die Anonymität von Tor und gründeten darüber hinaus Foren und anderen Informationsplattformen innerhalb des Darknet (de Roquefeuil 2011; Schlag und Wenz 2018). Vordergründig ist hierbei die Verschleierung der eigenen digitalen Identität zum Schutz der eigenen Person priorisiert, also die Nutzung von Tor als Internetbrowser und nicht unbedingt das Erstellen und Nutzen der „hidden services“ im Darknet.

Im Nachgang führte der arabische Frühling zu einer staatlichen Zensur im digitalen Raum in Ägypten und Tunesien, wobei hier der Kurznachrichtendienst Twitter im Vordergrund dieser Zensur stand (Biermann 2011). In Russland ist die Nutzung von gewissen Anonymisierungsdiensten, darunter auch Tor, seit 2017 verboten (Gutmann 2017). Darüber hinaus ist bekannt, dass die Nutzung von Tor in China nicht ohne weiteres gelingt, da dort Mechanismen zur Zensur des Internets wirken (Projekt Goldener Schild), welche die Nutzung von Anonymisierungsdiensten einschränken oder gar gänzlich verhindern (Kleinz 2015). Auch in der Türkei kam es Ende 2016 zu einer staatlichen Blockade des Tor-Netzwerkes (Albert 2016). In den Ländern Saudi-Arabien, Iran und Bahrain gelingt das Surfen mit Anonymisierungsdiensten, wie Tor, aufgrund dortiger Restriktionen ebenfalls nicht zuverlässig (Osborne 2016).

Diese staatlichen Bestrebungen, welche zum Teil schon in digitalen Restriktionen mündeten, zeigen einmal mehr, welch wichtige Rolle die Nutzung von Tor als Möglichkeit der digitalen Anonymisierung spielt, bezogen auf Menschenrechte wie Presse- und Meinungsfreiheit.

4 Die dunkle Seite

Neben den bereits beleuchteten positiven Aspekten der Nutzung von Tor haben natürlich auch Kriminelle die Anonymität dieser Software für sich entdeckt. Im Vordergrund steht hier eindeutig der Vertrieb illegaler Güter wie Waffen, Betäubungsmittel, Daten, gefälschte Urkunden, Falschgeld und inkriminierter Dienste und Services, aber auch die Nutzung des Darknet als verschlüsselte Kommunikationsplattform.

4.1 Drei, Zwei, Eins, meins?

Grundsätzlich lassen sich die Angebotsformen innerhalb des Darknet derzeit in drei Kategorien einordnen: Marktplatz, Forum und Vendorshop.

4.1.1 Marktplatz

Innerhalb des Marktplatzes bieten viele verschiedene Verkäufer ihre Waren in unterschiedlichen Kategorien an. Hier werden die Angebote samt Produktbeschreibung mit sog. „Proofpics“, also Beweisfotos versehen. Nach der aufgegebenen Bestellung erfolgt die möglichst anonyme Bezahlung der inkriminierten Güter durch sog. Kryptowährungen, also digitales Geld. Die Bezahlung erfolgt dabei automatisiert über ein Warenkorbsystem. Dieser Vorgang wird im nächsten Absatz anhand der derzeit populärsten Zahlungsmethode Bitcoin (BTC) näher erläutert. Die Nutzung weiterer Kryptowährungen wie Monero (XMR) oder Ether (ETH) ist derzeit eher marginal. Mittels der in der Regel implementierten Feedbackfunktion können sowohl Käufer als auch Verkäufer die jeweilig abgewickelten Geschäfte bewerten. Somit unterscheiden sich diese Marktplätze nur aufgrund der dort angebotenen Waren und der Zahlungsmodalitäten von herkömmlichen digitalen Marktplätzen, wie Amazon oder eBay.

4.1.2 Forum

Innerhalb der Darknet-Foren, welche sich wohl nur wegen der Inhalte von anderen, gewöhnlichen Internetforen unterscheiden, werden neben einem (mehr oder weniger) unbedenklichem Informationsaustausch häufig auch inkriminierte Güter zum Verkauf angeboten. Das Angebotsportfolio unterscheidet sich unmerklich von dem der Marktplätze. Die Güter werden zumeist innerhalb einer bestimmten Rubrik in einem durch den jeweiligen Verkäufer eröffneten Beitrag (sog. Thread) mittels Proofpics und der jeweiligen Preise mehr oder weniger professionell angeboten. Die Käufer melden sich in der Regel mit einer privaten Forennachricht oder auf anderen verschlüsselten Kommunikationskanälen bei dem Käufer und das Geschäft wird im persönlichen Gespräch abgewickelt. In der Regel erfolgt nach Erhalt der Ware ein Feedback durch den Käufer.

4.1.3 Vendorshop

Ein Vendorshop ist ein Onlineshop des Verkäufers, in welchem dieser seine Ware anbietet. Zumeist erfolgt dies mittels der bereits genannten Proofpics und der Auflistung der Preise. Im Unterschied zu den Angeboten im Forum implementieren die Verkäufer in ihren Vendorshops zumeist ein Warenkorbsystem, welches die Abwicklung der Geschäfte automatisiert übernimmt, ähnlich der legalen Onlineshops im Clearnet. In der Regel ist auch hier eine Feedbackfunktion für Käufer implementiert.

4.2 Bitcoin – ein kurzer Exkurs

Eng verzahnt mit dem Darknet ist auch die Kryptowährung Bitcoin. Eine ausführliche Ausarbeitung hierzu kann und hat schon mehrere Bücher gefüllt. Diese kurze Einführung soll nur ein Überblick darstellen.

Bitcoin wurde im Jahre 2009 durch einen bislang Unbekannten mit dem Pseudonym „Satoshi Nakamoto“ veröffentlicht und stellt eine Kryptowährung, also digitales Geld dar, welches auf der sog. Blockchain-Technologie basiert. Bei der Blockchain handelt es sich um eine dezentrale Datenbank, in welcher alle Bitcoin-Transaktionen registriert werden. Diese werden somit transparent und für Jedermann nachvollziehbar gespeichert. Dezentral bedeutet, dass es keine zentrale Prüf- oder Verwaltungsinstanz (Bank) gibt, sondern dies durch die Nutzer gewährleistet wird (Weingärtner o. D.).

Die weitläufige Meinung, dass es sich bei Bitcoin um ein anonymes Zahlungsmittel handelt, führte dazu, dass dieser besonders im Bereich des Darknet beliebt wurde. Es herrscht keine Klarnamenpflicht bei Transaktionen, man benötigt lediglich eine sog. Bitcoin-Adresse, von welcher man die gewünschte Anzahl an Bitcoin an die gewünschte Zieladresse sendet.

Bei Bitcoin handelt es sich tatsächlich jedoch um ein pseudonymes Zahlungsmittel (Schneider 2019). Wie bereits angeführt, wird jede Bitcoin-Transaktion in der Blockchain gespeichert und somit für Jedermann nachvollziehbar. Auch müssen die Bitcoins zunächst einmal erworben und schlussendlich auch wieder in Form von Bargeld in den Geldbeutel des Inhabers gelangen. Dies ist ohne eine Bankverbindung nur deutlich erschwert möglich.

Der Kursverlauf des Bitcoin-Wertes, welcher sich ähnlich zu Aktien an Angebot und Nachfrage orientiert, reichte von $0,08 im Herbst 2010 bis hin zu sage und schreibe $20.000 (in Worten Zwanzigtausend) pro Bitcoin im Dezember 2017 (French 2017; Sixt 2016). Somit sind Bitcoin nicht nur im Bereich des Darknet ein beliebtes Zahlungsmittel, sondern auch im Bereich der Finanzspekulation ein bevorzugtes Produkt. Neben Bitcoin existieren derzeit laut der wohl prominentesten Webseite für Kryptowährungen (coinmarketcap.com) etwa 2000 verschiedene Arten des digitalen Geldes.

4.3 Bestellt, gekauft, bezahlt

Wie kommen nun die inkriminierten Güter zu den Käufern?

Sofern es sich bei den Gütern nicht um digitale, sondern physische handelt, machen sich die Täter die herkömmlichen Versanddienstleister zunutze.

Die bisherigen Erfahrungen der Strafverfolgungsbehörden zeigen, dass sich die Mehrzahl der Käufer die physischen Waren zu ihrer tatsächlichen Wohnanschrift liefern lassen und nicht zu sog. „Drops“. Bei Letzteren handelt es sich beispielsweise um verwaiste Briefkästen an Mehrfamilienhäusern oder um Packstationen, welche mit gestohlenen Kundendaten betrieben werden. Dieses Verhalten zeigt einmal mehr, wie sicher sich die Täter im Bereich der vermeintlichen digitalen Anonymität fühlen. Um die dunkle Seite des Darknet plastischer darzustellen, folgen nun einige Fallbeispiel aus der jüngsten Vergangenheit.

5 Von der Seidenstraße bis zum Kinderzimmer: Beispiele aus dem Darknet

5.1 Silk Road

Der erste große, bekannte Darknet-Marktplatz nannte sich „Silk Road“ (Seidenstraße) und war von Januar 2011 bis Oktober 2013 in Betrieb. In diesem Zeitraum wurden dort mit dem Verkauf von u. a. Drogen, Waffen, gefälschten Urkunden und Daten umgerechnet etwa 1 Mrd. EUR umgesetzt. Hierbei sollen umgerechnet etwa 70 Mio. EUR an Provision an die Betreiber des Marktplatzes geflossen sein (Greenberg 2013).

Im Rahmen von Ermittlungen amerikanischer Behörden wurde der vermeintliche alleinige Betreiber, der damals 29-jährige Amerikaner Ross Ulbricht, im Oktober 2013 in den USA festgenommen, die Webseite beschlagnahmt und Ulbricht im Mai 2015 zu einer lebenslangen Freiheitsstrafe verurteilt (Wendt 2015). Zum Zeitpunkt der Beschlagnahme waren bei Silk Road knapp 1 Mio. Nutzer registriert.

5.2 Silk Road 2.0

Im November 2013, also einen Monat nach der Festnahme Ulbrichts ging der Nachfolger von Silk Road unter dem Namen Silk Road 2.0 online und wurde ein Jahr später ebenfalls durch amerikanische Strafverfolgungsbehörden beschlagnahmt (Briegleb 2014). Ein Betreiber konnte nicht identifiziert werden.

5.3 AlphaBay

Der „Marktführer“ im Jahr 2017 nannte sich, in Anlehnung an einen berühmten legalen Internetmarktplatz, AlphaBay. Das Angebotsportfolio war ähnlich zu dem von Silk Road. Der Tagesumsatz von AlphaBay, welcher zu Spitzenzeiten etwa 200.000 Nutzer aufwies, soll sich auf etwa 700.000€ belaufen haben (Wilkens 2017b). Der vermeintliche Betreiber, der 25-jährige Kanadier Alexandre Cazes, wurde im Juli 2017 in Thailand festgenommen und wenige Tage nach seiner Festnahme in seiner Gewahrsamszelle in Thailand tot aufgefunden. Nach Darstellung der thailändischen Behörden habe er sich mutmaßlich durch Erhängen das Leben genommen, um einer Anklage und Hauptverhandlung in den USA zuvorzukommen, in welche er ausgeliefert werden sollte (Murdoch 2017).

5.4 Hansa Market

Der Marketplace Hansa Market, welcher von zwei 30- und 31-jährigen Deutschen von 2014 bis Juli 2017 betrieben wurde, wies zum Zeitpunkt seiner Beschlagnahme 400.000 Nutzer auf. Im Rahmen einer multinationalen Operation (OP Bayonet) amerikanischer, niederländischer und deutscher Strafverfolgungsbehörden konnte im Juli 2017 zunächst der damalige und bereits erwähnte Branchenprimus AlphaBay geschlossen werden.

Die im Nachgang zu verzeichnende Wanderung der Verkäufer und Käufer zu dem Marktplatz Hansa Market konnte insofern durch die Ermittlungsbehörden begrüßt werden, da diese zu diesem Zeitpunkt bereits den Betrieb dieses Marktplatzes von staatlicher Seite (Niederlande) übernommen hatten, somit einen großen Informationszugewinn verzeichneten und zwei Wochen später Hansa Market ebenfalls schließen konnten (Greenberg 2017). Diese konzertierte Aktion führte zu einer bis dato noch nie da gewesenen Verunsicherung und einem Misstrauen innerhalb der Darknet-Community, sodass diese zunächst keinen größeren Nachkömmling mehr hervorbrachte.

5.5 Deutschland im Deep Web

Das größte deutschsprachige Darknet-Forum „Deutschland im Deep Web“ bestand seit März 2013 und wurde durch den Administrator „Luckyspax“ betrieben. In verschiedenen Beiträgen wurden die für solche Foren klassischen inkriminierten Güter (Betäubungsmittel, Waffen, Daten, Services) angeboten und verkauft.

Unter diesen Gütern war auch die Schusswaffe (Pistole Glock 17), mittels welcher der 18-jährige David S. den Amoklauf vor dem Münchener Olympiazentrum am 22. Juli 2016 verübte und neun Menschen starben. Kurz nach diesem Amoklauf änderte der Administrator „Luckyspax“ die Struktur seines Forums, sodass die prominent im Bereich „Biete“ platzierte „Waffen“-Sektion in einen anderen Forenbereich verschoben und wenige Monate später gänzlich geschlossen wurde.

Im Rahmen strafrechtlicher Ermittlungen durch das BKA konnte Luckyspax als der 30-jährige Informatikstudent Alexander U. aus Karlsruhe identifiziert werden. Im Juni 2017 konnte dieser festgenommen und das Forum, welches bis dato 23.000 registrierte Nutzer aufwies, abgeschaltet werden (Wilkens 2017a, b). Im Rahmen der Hauptverhandlung im Dezember 2018 wurde Alexander U. zu einer Haftstrafe von sechs Jahren verurteilt (Cooper 2019).

5.6 Das Hydra-Phänomen im Darknet

Egal ob Marktplatz, Forum oder Vendorshop – nach einer staatlichen Intervention, sei es durch Festnahme des Verantwortlichen oder durch Beschlagnahme der digitalen Infrastruktur und Abschaltung des entsprechenden „hidden services“, verstreicht meist nicht allzu viel Zeit bis ein Nachkömmling die Rolle des vorigen Primus einnimmt. Man könnte hier von einer Hydra sprechen.

Erfolgreiche konzertierte, globale Aktionen, wie bereits ausgeführt, führen zwar zu einer länger anhaltenden Verunsicherung und zu Misstrauen, jedoch nicht zu einem abschließenden Umdenken der Täter. Hinzu kommt die Lernkurve der Täter, die es staatlichen Strafverfolgern zukünftig sicher nicht einfacher macht, Erfolge zu verzeichnen und Täter zu identifizieren. Trotzdem bleibt auch hier der Mensch der entscheidende Faktor und Menschen machen bekanntlich Fehler.

6 Straftaten im Darknet

Die bisher bekannt gewordenen Straftaten innerhalb des Darknet sind der Handel mit Betäubungsmitteln, Waffen, widerrechtlich erlangten Daten (Kreditkartendaten, personenbezogene Daten), gefälschten Dokumenten und Urkunden, Falschgeld und illegale Services (z. B. Hacker). Darüber hinaus existieren innerhalb des Darknet auch Bereiche, in denen kinderpornographische Inhalte angeboten oder getauscht werden. Zusätzlich sind Darknet-Seiten bekannt, die sog. Hitman-Services, also Mord auf Bestellung anbieten. Es ist jedoch bekannt, dass es sich bei einer Vielzahl dieser Seiten um sog. „Scams“ (Betrug) handelt,

denn bislang wurde noch kein Fall bekannt, dass es sich bei diesen Angeboten um „echte“ handeln könnte.

Trotzdem muss die reine Existenz solcher Angebote für Strafverfolgungsbehörden ein alarmierendes Signal bedeuten sowohl bezüglich vermeintlicher Verkäufer als auch vermeintlicher Käufer. Die Frage, ob sich nun die Delikte und die jeweiligen Täter im digitalen Raum zu denen des analogen Lebens unterscheiden, wird in folgendem Abschnitt näher beleuchtet.

7 Kinderzimmer oder Bahnhofsvorplatz?

Als Beispiel wird hier das der Rauschgiftkriminalität beleuchtet unter Einbeziehung des Falls des sog. „Kinderzimmerdealers“.

Im Februar 2015 wurde der Leipziger Maximilian S., seinerzeit 20 Jahre alt und Betreiber des Vendorshops „Shiny Flakes“, welcher sowohl über das Darknet, als auch über das Clearnet erreichbar war, festgenommen. Maximilian S. vertrieb aus dem Kinderzimmer im Elternhaus heraus von Dezember 2013 bis Februar 2015 geschätzte 600 kg Betäubungsmittel.

Im Rahmen der Durchsuchung wurden 320 kg verschiedene Betäubungsmittel mit einem Straßenverkaufswert von über 4 Mio. EUR aufgefunden und sichergestellt. Im Rahmen der weiteren Ermittlungen konnten ihm mehrere tausend Verstöße gegen das Betäubungsmittelgesetz nachgewiesen werden (Locker und Schöler 2016). Der Umsatz zwischen Oktober 2014 und Februar 2015 allein soll 1 Mio. EUR betragen haben. Darüber hinaus wurden 325.000€ in Bitcoin sichergestellt.

Realschulabsolvent Maximilian S. gilt als hochintelligent, aber auch als überheblich, ignorant und sich selbst überschätzend. Im Umgang mit seinen Kunden wurde er als arrogant dargestellt. Im Rahmen der Hauptverhandlung wurde er zu sieben Jahren Haft verurteilt.

Die Geschichte um den Kinderzimmer-Dealer Maximilian S. diente als Vorlage für eine deutsche TV-Serie, welche im Jahr 2019 veröffentlicht werden soll.

7.1 Wie unterscheiden sich die Delikte im analogen und digitalen Raum?

In Zeiten des legalen Onlinehandels ist es für viele schon alltäglich von zuhause aus Dinge des täglichen Konsums zu kaufen und sich diese dann bis zu seiner Haustür liefern zu lassen. Diese bequeme und unkomplizierte Art der Bestellung lässt sich

auch auf die Konsumenten von Betäubungsmitteln im Darknet übertragen. Es ist nicht mehr notwendig sich mit windigen Dealern auf Bahnhofsvorplätzen oder in Parks zu treffen, um seine Betäubungsmittel zu erwerben. Hinzu kommt ein vermeintlich deutlich gemindertes Entdeckungsrisiko durch Strafverfolgungsbehörden sowohl für Verkäufer als auch für Käufer im digitalen Raum. Auch dürfte das Ausweichen auf andere Verkäufer oder andere Ware bei entsprechenden (positiven oder negativen) Feedbacks im digitalen Raum einfacher sein.

Im digitalen Raum kommt es dann eher zu virtuellen Auseinandersetzungen durch Preiskämpfe, Denunzierungen und durch das Säen von Misstrauen bei Konkurrenten. Die Rohheitsdelikte (Raub- und Körperverletzungsdelikte) im Bereich des Straßenhandels finden im digitalen Raum nicht statt. Laut der Studie einer Rechtsprofessorin und eines Professors für Kriminalwissenschaften aus dem Jahre 2014 habe der Handel mit Betäubungsmitteln auf dem Marktplatz Silk Road durch die Verringerung des physischen Kontakts zwischen Drogenhändlern und den jeweiligen Abnehmern zu einem Rückgang von Rohheitsdelikten in der analogen Welt geführt (Aldrige und Décary-Hétu 2014). Laut dieser Studie waren die wichtigsten Kunden innerhalb des Marktplatzes Drogendealer, die dort ihre Betäubungsmittel für ihren lokalen Straßenhandel bezogen. Somit geht die Studie davon aus, dass dieser virtuelle Standort Gewalt, Einschüchterung und Territorialismus reduzierte.

Für den jeweiligen Verkäufer dürfte es sich zwar einerseits bequemer und sicherer darstellen aus dem digitalen Raum zu agieren, jedoch spiegelt sich der logistische Mehraufwand durch Abarbeiten der Bestellungen und den Versand der Ware in deutlich höheren Preisen wider. Auch die im digitalen Raum vorherrschende Anonymität ist natürlich nachteilig, wenn man seine Kunden nicht persönlich kennt. Die diesem Umstand innewohnende Betrugsgefahr, die in der Szene als „Scams“ bekannt sind, ist dort sehr hoch, da es nicht zu einer persönlichen Übergabe der Ware und der Zahlung kommt.

Darüber hinaus veranschaulichen die bereits aufgezeigten Umsätze der populärsten Marktplätze sehr deutlich, mit welchen Summen dort gehandelt wird. Diese verleiten Administratoren solcher Marktplätze regelmäßig zu sogenannten „Exit-Scams“, welche in der Regel mit dem Vereinnahmen der auf der Plattform oder in dortigen Treuhandkonten befindlichen Vermögenswerten der Mitglieder der jeweiligen Plattform und dem Abschalten selbiger einhergehen.

Inwiefern sich die Delikte unterscheiden, kann besonders am Beispiel eines Betäubungsmittelkonsumenten, welcher seine Drogen aus dem Darknet bezieht, plakativ und stellvertretend veranschaulicht werden. Innerhalb des Darknet existieren plattformübergreifend deutliche Unterschiede in der Ware, vor allem im Bereich der Wirkstoffkonzentration von Betäubungsmitteln, was bei einem Wechsel der

Bezugsquelle zu einer einfacheren Überdosierung führen kann. Weiterhin ist durch den einfachen möglichen Wechsel der Bezugsquelle auch nicht gesichert, welche Streckmittel oder sonstige Stoffe zur Gewichtsmaximierung beigemischt werden.

7.2 Wie unterscheiden sich die Täter im analogen und digitalen Raum?

Kaum vorstellbar, dass der 20-jährige Maximilian S. mit seiner Arroganz und Ignoranz gegenüber seinen Kunden auf einem Bahnhofsvorplatz zu einem Dealer aufgestiegen wäre, der innerhalb eines Jahres dort 1 Mio. EUR umgesetzt hätte.

Die Tätertypologien bezogen auf die innerhalb des Darknet agierenden Verkäufer dürften sich von denen in der analogen Welt deutlich unterscheiden, da im digitalen Raum ein anderer logistischer Aufwand (Bestellungen und Versand) notwendig erscheint. Auch eine gewisse Affinität bezogen auf informationstechnische Systeme und solcher Abläufe scheint Grundvoraussetzung für den Erfolg des eigenen Darknet-Geschäftsmodells zu sein, betrachtet man die technischen Abläufe zum Schutz der eigenen Identität mittels verschlüsselter Kommunikation (Tor, verschlüsselte Nachrichtendienste) in Verbindung mit pseudonymer Bezahlung (Bitcoin). Die Täter im digitalen Raum bezogen auf die Konsumenten und Käufer dürften sich von denen im analogen Raum nicht derart stark, jedoch ebenfalls merklich unterscheiden, da hier der Weg des Erwerbs deutlich verändert ist und ebenfalls ein Grundverständnis der oben genannten informationstechnischen Abläufe erforderlich ist.

8 Licht im Dunkeln?

Die jüngsten Erfolge der Strafverfolgungsbehörden im Darknet zeigen, dass die Ermittler aufholen und gezielt vorgehen. Was diesen Erfolgen jedoch auch innewohnt ist die exponentielle Lernkurve der Täter im Darknet. Mit jedem Erfolg zerschlägt sich prinzipiell die Art der Ermittlungsführung, weil Ermittlungsmethoden der Behörden oder unter Umständen auch die täterseitigen Fehler öffentlich bekannt werden. Viele Methoden, die heute noch erfolgversprechend waren, sind es im nächsten Moment nicht mehr und Ermittlungsverfahren gipfeln in Katz- und Maus-Spielen. Eine weitere Herausforderung neben der Nutzung verschlüsselter Internetbrowser wie Tor, sind zusätzlich genutzte Nachrichtendienste (Messenger, mobile Apps), welche die Kommunikation der Teilnehmer verschlüsseln.

In unregelmäßigen Abständen werden Bestrebungen laut, welche die Abschaltung des Darknet mit der Gleichsetzung des Verbots der Nutzung von Tor in Deutschland fordern. Diese werden damit begründet, dass man in einem demokratischen Staat wie Deutschland seine Identität im digitalen Raum nicht verschleiern müsse. Jedoch nur, weil Bürger in Deutschland keine Strafverfolgung zu befürchten haben, wenn sie im digitalen Raum ihre Meinung äußern oder Pressevertreter dort Artikel veröffentlichen, bedeutet dies im Umkehrschluss nicht, dass der Staat hier (ab)schalten und walten kann, wie es ihm beliebt. Dies unterliegt nämlich ebenfalls der persönlichen Freiheit des Einzelnen und diese ist Grundvoraussetzung für eine freiheitlich demokratische Grundordnung.

9 Ein Blick in die Glaskugel

Bereits jetzt ist eine verstärkte Nutzung neuer Technologien zu verzeichnen. Neben der im Darknet etablierten pseudonymen Krypotwährung Bitcoin gewinnt Monero deutlich an Akzeptanz und legt einen deutlichen Fokus auf die tatsächliche Anonymität der Transaktionen und somit auch der Nutzer. Auch der bereits eingeschlagene Weg zu anderen Plattformen und Arten der Kommunikation, wie die Abwicklung von illegalen Geschäften über mobile Messengerdienste (Wickr) oder dezentrale Marktplätze (Open Bazaar) werden Strafverfolgungsbehörden weltweit beschäftigen. Trotz der unbestrittenen hellen Seiten des Darknet, stellt dieses neben anderen Phänomenbereichen eine große Herausforderung für Strafverfolgungsbehörden weltweit, vor allem im Bereich der verschlüsselten Kommunikation und der Nutzung neuer Technologien, dar. Hier bedarf es vor allem im polizeilichen Bereich eines Wandels der gewachsenen Strukturen, um zu dem im höchsten Maße flexiblen, technisch und technologisch weit fortgeschrittenen „Gegenüber“ aufschließen zu können.

In Teilen ist dieser Wandel bereits erkennbar. Polizeibehörden verstärken sich personell mit IT-Spezialisten und Analysten, da es undenkbar ist, dass ausgebildete Polizeibeamte, selbst mit gewisser Affinität oder Zusatzbildung, diesen Tätern auf Augenhöhe begegnen können. Überdies bedarf es vor allem im Bereich der Technologie, sei es im Rahmen von Ermittlungen zu Kryptowährungen oder bei der Auswertung von Massendaten, adäquater Mittel. Die vor allem in Polizeibehörden beliebten „Bordmittel“, also das Nutzen polizeilich erstellter Programme erscheint hier nicht mehr zeitgemäß. Sowohl die personelle Verstärkung durch Spezialisten, als auch die Akquise zeitgemäßer Ermittlungstools geht jedoch einher mit deutlichen finanziellen Aufwendungen.

Es wird sich zeigen, wie schnell Strafverfolgungsbehörden Schritt halten und diesen Herausforderungen begegnen können.

Literatur

Albert, A. (2016). Türkei will anonymes Surfen unmöglich machen. http://www.spiegel.de/netzwelt/netzpolitik/tor-und-vpn-tuerkei-will-anonymes-surfen-unmoeglich-machen-a-1126540.html. Zugegriffen: 11. März 2019.

Aldrige, J., & Décary-Hétu, D. (2014). Not an ‚ebay for drugs': The cryptomarket ‚silk road' as a paradigm shifting criminal innovation. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2436643. Zugegriffen: 11. März 2019.

Baurmann, J.-G. (2016). Eine ziemlich gute Sache. *DIE ZEIT* Nr. 33/2016.

Bergman, M.-K. (2001). The deep web: Surfacing hidden value. *The Journal of Electronic Publishing, 7*(1), 16.

Biermann, K. (2011). Ägypten blockiert twitter, facebook und mobiltelefone. https://www.zeit.de/digital/internet/2011-01/aegypten-internet-twitter. Zugegriffen: 11. März 2019.

Briegleb, V. (2014). Onymous: Razzia gegen Silk Road 2.0 und das Darknet. https://www.heise.de/newsticker/meldung/Onymous-Razzia-gegen-Silk-Road-2-0-und-das-Darknet-2443945.html. Zugegriffen: 11. März 2019.

Cooper, D. (2019). Deutschland im deep web: Wie das größte deutsche Darknet-Forum aufflog. https://www.heise.de/hintergrund/Deutschland-im-Deep-Web-Wie-das-groesste-deutsche-Darknet-Forum-aufflog-4247033.html. Zugegriffen: 11. März 2019.

de Roquefeuil, C. (2011). Wie Facebook und Twitter die Proteste vorantreiben. https://www.stern.de/politik/ausland/revolution-2-0-in-aegypten-und-tunesien-wie-facebook-und-twitter-die-proteste-vorantreiben-3927248.html. Zugegriffen: 11. März 2019.

Eckermann, I.-M. (2017). Was ist eigentlich das Darknet? https://www.gdata.de/ratgeber/was-ist-eigentlich-das-darknet. Zugegriffen: 11. März 2019.

ExpressVPN. (2018). The unlikely history of Tor. https://www.expressvpn.com/internet-privacy/tor/history. Zugegriffen: 1. Apr. 2019.

French, S. (2017). Here's proof that this bitcoin crash is far from the worst the cryptocurrency has seen. https://www.marketwatch.com/story/heres-proof-that-this-bitcoin-crash-is-far-from-the-worst-the-cryptocurrency-has-seen-2018-02-09. Zugegriffen: 18. März 2019.

Greenberg, A. (2013). End of the silk road: FBI says it's busted the web's biggest anonymous drug black market. https://www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market/#65024ce85b4f. Zugegriffen: 6. Juni 2019.

Greenberg, A. (2017). Global police springs a trap on thousands of dark web users. https://www.wired.com/story/alphabay-hansa-takedown-dark-web-trap/. Zugegriffen: 11. März 2019.

Gutmann, T. (2017). Russland beschließt Verbot von VPN, Proxy & Tor. https://ostexperte.de/tor-vpn-proxy/. Zugegriffen: 11. März 2019.

Kleinz, T. (2015). 32C3: Wie Chinas Große Firewall Tor-Verbindungen sabotiert. https://www.heise.de/newsticker/meldung/32C3-Wie-Chinas-Grosse-Firewall-Tor-Verbindungen-sabotiert-3057095.html. Zugegriffen: 11. März 2019.

Locker, T., & Schöler, M. (2016). Urteil rechtskräftig: Shiny Flakes-Admin schuldet Deutschland mehrere Millionen. https://motherboard.vice.com/de/article/bmv9wv/nachdem-bgh-urteil-ist-shiny-flakes-auch-finanziell-arm-dran. Zugegriffen: 11. März 2019.

Murdoch, L. (2017). AlphaBay suspected co-founder Alexandre Cazes found dead in Thai jail. https://www.brisbanetimes.com.au/world/alphabay-suspected-cofounder-alexandre-cazes-found-dead-in-thai-jail-20170715-gxburv.html. Zugegriffen: 11. März 2019.

Osborne, C. (2016). How to access Tor, even when your country says you can't. https://www.zdnet.com/article/how-to-dance-around-censorship-and-access-tor-even-when-blocked/. Zugegriffen: 11. März 2019.

Schlag, G., & Wenz, B. (2018). Die helle Seite des Darknet. https://www.deutschlandfunk.de/investigativer-journalismus-die-helle-seite-des-darknet.2907.de.html?dram:article_id=410574. Zugegriffen: 6. Juni 2019.

Schmidt, J. (2016). Tor und die versteckten Dienst. https://www.heise.de/security/artikel/Tor-und-die-versteckten-Dienste-3280904.html. Zugegriffen: 19. März 2019.

Schneider, P. (2019). Anonyme Bitcoin-Nutzung. https://www.kryptopedia.org/darum-sind-Bitcoin-transfers-nicht-wirklich-anonym/. Zugegriffen: 5. März 2019.

Sixt, E. (2016). *Bitcoins und andere dezentrale Transaktionssysteme: Blockchains als Basis einer Kryptoökonomie* (S. 20–21–105–107). Wiesbaden: Springer Gabler.

The Tor Project. (o. D.a). Tor FAQ. https://www.torproject.org/docs/faq#WhyCalledTor. Zugegriffen: 11. März 2019.

The Tor Project. (o. D.b). Tor overview. https://www.torproject.org/about/overview.html.en. Zugegriffen: 11. März 2019.

Weingärtner, T. (o. D.). Blockchain einfach erklärt. https://blog.hslu.ch/informatik/blockchain-einfach-erklaert/. Zugegriffen: 11. März 2019.

Wendt, J. (2015). Ross Ulbricht: Silk-Road-Gründer muss lebenslang hinter Gitter. https://www.zeit.de/digital/internet/2015-05/ross-ulbricht-silk-road-strafmass-urteil. Zugegriffen: 11. März 2019.

Wilkens, A. (2017a). Betreiber eines Darknet-Forums in Karlsruhe festgenommen. https://www.heise.de/newsticker/meldung/Betreiber-eines-Darknet-Forums-in-Karlsruhe-festgenommen-3740829.html. Zugegriffen: 11. März 2019.

Wilkens, A. (2017b). Darknet-Marktplatz AlphaBay nach Razzia geschlossen. https://www.heise.de/newsticker/meldung/Darknet-Marktplatz-AlphaBay-nach-Razzia-geschlossen-3771649.html. Zugegriffen: 18. März 2019.

Terrorismus und die Nutzung des Internet

Holger Nitsch

1 Einleitung

Die technologische Innovation der Kommunikation ging in den letzten Jahren mit einer unglaublichen Geschwindigkeit vonstatten. Die Zahl der Nutzer des Internet hat global in den letzten Jahren zugenommen. Im März 2019 haben fast 90 % der Menschen in Nordamerika und Europa das Internet genutzt, aber auch über 50 % der Menschen in Asien und fast 40 % der Bevölkerung Afrikas (Internet Worlds Stats 2019). Dies beinhaltet ein großes Potenzial an möglichen Einflussmöglichkeiten von verschiedenen Seiten. Neben den vielfältigen Möglichkeiten für Personen sich Informationen zu beschaffen und zu interagieren und auch über große Entfernungen mit Bekannten und Freunden in Kontakt zu bleiben, bietet die Vielzahl der Nutzer und die Diversität des Mediums auch vielfältige Möglichkeiten des Missbrauchs. Zukünftige Entwicklungen, wie das Internet der Dinge (Internet of Things, IoT), online Banking, das Dark- oder Deepweb, aber auch das normale Surface-Web bieten viele Möglichkeiten für den Missbrauch für kriminelle Aktivitäten oder für die Weiterverbreitung extremistischer Propaganda (s. Kap. „Darknet – die dunkle Seite des Internets?“). Gerade dieser Aspekt hat in den letzten Jahren eine steigende Rolle gespielt.

Einige kriminelle Aktivitäten sind sehr einfach gehalten; aber allgemein ist das Niveau mit den technischen Möglichkeiten steigend und damit auch die Bedrohung für den Bürger Opfer solcher Aktivitäten zu werden. Wie in anderen Beiträgen erwähnt (z. B. Kap. „Strafverfolgung digital“ und „Darknet – die dunkle Seite des Internets?“), macht das sogenannte Surface-Web nur einen klei-

H. Nitsch (✉)
Fürstenfeldbruck, Deutschland
E-Mail: holger.nitsch@pol.hfoed.bayern.de

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

T.-G. Rüdiger und P. S. Bayerl (Hrsg.), *Cyberkriminologie,*
https://doi.org/10.1007/978-3-658-28507-4_8

nen Teil des eigentliche Internet aus. Der weitaus größere Teil ist das Deepweb und das darunter liegende Dark-Web. Dies ermöglicht es den Nutzern (Usern) anonym im Netz Informationen zu teilen oder sich zu bewegen. Die ursprünglich militärische Nutzung des Dark-Web machte es schwierig und unattraktiv für User es zu nutzen, da die Kenntnis der genauen Zieladresse notwendig war und es keine Suchmaschinen gab. Die änderte sich 2004, als „Hidden Wiki" einen Katalog der Dark-Web Sites veröffentlichte (Chertoff 2016).

Weitere Kommunikationsplattformen wie *4chan.org* oder *8chan.org* bieten Menschen auf der einen Seite Möglichkeiten unzensiert ihre Meinung kundzutun, aber haben eben auch das Potenzial für kriminelle Aktivitäten, die Verbreitung von Fehlinformationen oder des Diffamierens von anderen. Ursprünglich war *4chan.org* eine Plattform zur Verbreitung von Animationen, aber sehr schnell entwickelte sie sich zu einer Seite auf der alle möglichen Inhalte zu finden waren. Das beliebteste Board zu Beginn war /b/ in 4chan. Dies hatte im Monat bis zu 20 Mio. Besucher. Es gab hier auch ein paar Regeln, die in /b/tards dargestellt wurden. Regel 1 und Regel 2 waren identisch: über „/b/ wird nicht geredet", oder auch Regel 32: „Hier gibt es keine Grenzen" (Bartlett 2016, S. 28). Die von vielen Usern verwendeten Mechanismen hatten zum primären Ziel die Diskreditierung von Personen und Desinformation. Dies verlagerte sich später unter anderem auch in diverse Social Media Kanäle oder ins Dark-Web. Die Sprache ist in der Regel sehr einfach und umgangssprachlich, was die Kommunikation stark vereinfacht.

Gerade im Hinblick auf junge User, die das Internet entdecken und die Freiheiten erfahren, sind solche Angebote attraktiv, da sie unkonventionell sind und einfache Lösungen bieten. Die vermeintliche Anonymität des Netzes verringert die Aufmerksamkeit gegenüber möglicher Gefahren und verleitet insbesondere junge Menschen auch leicht zu kriminellen Aktivitäten. Das illegale Herunterladen von Inhalten, wie Filmen und Musik ist sicherlich nur ein Aspekt; auch Anleitungen für schwerwiegendere kriminelle Aktivitäten sind leicht zu finden. Als Problemstellungen der diversen Formen des Internet werden in der Regel das Verbreiten von Betrugssoftware oder Erpressungssoftware, das Verbreiten von Falschinformationen und Hasskriminalität, sowie die Verbreitung extremistischer Inhalte gesehen.

Nachfolgender Artikel befasst sich im Schwerpunkt mit der Verbindung zwischen Cyberkriminalität und Extremismus, beziehungsweise Terrorismus; aber aufgrund der Natur des Kommunikationsmittels spielen die anderen Bereiche auch eine Rolle.

2 Möglichkeiten der Nutzung für extremistische Gruppierungen

Unabhängig von der Definition von Extremismus oder extremistischer Gruppierungen haben diese Gruppen gemeinsam, dass sie den demokratischen Rechtsstaat in seiner jetzigen Form ablehnen, die Repräsentanten nicht anerkennen und diesen umformen wollen. Gemein ist ihnen auch, dass ihre Staatsvorstellung totalitär ist und Pluralismus abgelehnt wird, da diese Ideologien von der Überzeugung geprägt sind, den einzig richtigen Weg zum Zusammenleben zu kennen. In diesem Kontext kann auch von der Vorstellung von Erziehungsdiktaturen gesprochen werden. Dies trifft auch auf ökoterroristische Gruppierungen wie die Animal Liberation Front (ALF) zu, da andere Sichtweisen auf Tierhaltung oder Experimente für die Forschung mit Tieren nicht akzeptiert und mit Gewalt bekämpft werden. Dies zeigt sich insbesondere dadurch, dass die Propaganda der Gruppierungen, egal welcher Couleur, Andersdenkende ausschließt und als „schlecht“ brandmarkt. Die Verbreitung der Propaganda ist das offensichtlichste Merkmal extremistischer Gruppierungen im Internet. Das Ziel ist zum einen Sympathien für die Ideologien zu gewinnen und zum anderen neue Mitglieder zu rekrutieren (s. Kap. „Posterboys und Terrorpropaganda“).

Ein weiterer Aspekt ist die Nutzung der verschiedenen Möglichkeiten des Internets zur Finanzierung von Aktionen. Insbesondere Terrorismus ist häufig kostenintensiv und daher wird Geld benötigt um Aktionen, aber auch die Organisation und das tägliche Leben zu finanzieren. Der sogenannte Islamische Staat benötigte Geld für die Kämpfer in Syrien, aber auch für die Propaganda und die Finanzierung von Anschlägen. Das Internet bietet eine Vielzahl von Finanzierungsmöglichkeiten von Aufrufen zu Spenden oder der Verbreitung von Ideen der Finanzierung bis hin zur Nutzung von finanzieller Schadsoftware und Erpressungssoftware.

Gewaltaffine Gruppierungen können durch die Möglichkeiten des Internet auch Ideen für Anschläge kommunizieren, sodass auch Personen, die nicht direkt Mitglieder sind, aber mit der Ideologie sympathisieren, sich Anregungen, Ideen und Training über die diversen Kanäle verschaffen können. Musste der potenzielle Gewalttäter in der Zeit vor dem Internet sich noch indizierte Literatur, wie „The terrorist cookbook“ besorgen, steht ihm die Information jetzt online zur Verfügung. Gerade hinsichtlich einer stärkeren Vernetzung der Welt und der weiteren technologischen Entwicklung steigt auch die Gefahr eines möglichen Anschlags im Bereich des Cyberterrorismus auf das Internet of Things. Auch die Informationsbeschaffung über mögliche Anschlagsziele ist dadurch erheblich erleichtert worden.

Im Folgenden wird auf die einzelnen Aspekte intensiver eingegangen und auch mögliche Gegenmaßnahmen dargestellt.

2.1 Finanzierung

Die Möglichkeiten im Internet Geld zu akquirieren sind vielfältig. Der Bericht von Kaspersky über 2017 beinhaltet eine hohe Zahl von Schadsoftware und damit verwandten Zwischenfällen. Fast 1 Mio. Nutzer wurden Opfer einer solchen Attacke und 65 % attakierter Firmen verloren Teile oder sogar alle ihrer Daten (Kaspersky 2017). Im Jahr 2018 waren es 30,01 % aller Computer von Nutzern (Kaspersky 2019). Das Internet bietet für kriminelle Aktivitäten den Vorteil, nicht in direkten Kontakt mit dem Opfer stehen zu müssen und daher die eigene Identität besser verbergen zu können. Durch die Verbesserung der Sicherungsmechanismen ist es für kriminelle Aktivitäten auch wichtig geworden, ein Geschäftsmodell zu entwickeln, um die Einnahmen zu garantieren. So besteht zum einen die Möglichkeit sich seine eigene Schadsoftware zu designen und zum anderen eine gewisse Serviceleistung dem kenntnisärmeren Nutzer anzubieten (wie er zum Beispiel an Bitcoins als potenzielles Zahlungsmittel kommt oder vergleichbares). Dies wird „Crime as a service“ (CaaS) genannt. Der Umsatz durch diese Aktivitäten betrug 2014 laut des Internet Crime Threat Assessment von Europol 300 Mrd. US$ (IOCTA 2014).

Die Benutzung der Software, insbesondere von Erpressungssoftware ist häufig mit Kosten verbunden, da der Täter diese in vielen Fällen nicht selber programmiert, sondern im Internet kauft. Ein ökonomisches Modell mithilfe der Spieltheorie hilft bei der Einschätzung, welche Software wahrscheinlich erfolgreicher ist als andere. An der Universität von Kent wurde hierzu eine entsprechende Untersuchung durchgeführt. Kriminelle sind sich oft der ökonomischen Aspekte ihres Handelns nicht bewusst. Sie wissen nicht, mit welcher Schadsoftware sie den größtmöglichen Erfolg haben. Nach diesen Gesichtspunkten würden sie versuchen, den optimalen Preis einer Erpressungssoftware zu antizipieren, um diese erfolgreich einzusetzen. Dieser ist auch spieltheoretisch zu ermitteln, was für die Einschätzung der Relevanz der Schadsoftware von Bedeutung ist: Je besser der Service, desto häufiger wird die Nutzung durch Kriminelle sein. In der Realität wird dies oft durch verschiedene Versuche ermittelt. In der Untersuchung von 149 betroffenen Opfern in Canterbury wurde für 2017 festgestellt, dass 9 % der Täter einen Ertrag von £990 akzeptieren würden und die Bereitschaft bei potenziellen Opfern zu zahlen bei £200 liegt. Dies lässt Rückschlüsse auf den eigentlichen Wert der angenommenen Zahlung zu, der in der Regel geringer ist, als von kriminellen Organisationen oder Einzeltätern angenommen (Hernandez-Castro et al. 2017). Rechnerisch führt dies dazu, dass eine geringere Erpressungssumme in der Summe der Opfer zu mehr Zahlungsbereitschaft führt, als in der Realität gefordert wird, da der Preis der eigenen Erpressungssumme oft falsch eingeschätzt wird.

Tab. 1 beschreibt das spieltheoretische Modell.

Hier besteht ein Verhandlungsspielraum zwischen Täter und Opfer. Falls der Täter sich entscheidet, den Computer des Opfers zu infizieren, ist C verhandelbar. Bei der Betrachtung der Auszahlungen ist es nicht unerheblich, ob ein gewisser „Service“ angeboten wird, der zum Beispiel hilft, sich Bitcoins zu verschaffen, um die Daten wieder freizuschalten. Dies erhöht die Wahrscheinlichkeit der Zahlung. Das Risiko des Täters ist ebenso dargestellt.

Für Strafverfolgungsbehörden ist die Kenntnis der Wahrscheinlichkeit einer erfolgreichen Erpressungssoftware relevant, da sie dann beim ersten Erscheinen einer neuen Software die Wahrscheinlichkeit des Erfolgs einschätzen kann. Ein weiterer Erfolgsfaktor ist das Anbieten von Dienstleistungen zur Bezahlung. Weiß das Opfer nicht, wie es an Bitcoins kommt, kann ihm durch Serviceleistungen geholfen werden, um den erpressten Betrag zu bezahlen.

Der Begriff „Crime as a service“ (CaaS) bedeutet in diesem Kontext, dass Hilfestellungen bei der Durchführung krimineller Aktivitäten und zusätzliche Dienstleistungen angeboten werden. So kann der Täter zwischen verschiedenen Modellen beim Kreieren der Schadsoftware wählen und auch diverse Dienstleistungen, wie die oben genannte integrieren, oder aber er erhält gegen Gebühr Hilfestellung bei der Konfiguration und dem Design der Schadsoftware. Für die Anbieter von CaaS ist die illegale Aktivität relativ risikofrei, da nicht zu erwarten ist, dass ein Täter die Quelle seiner Information ohne weiteres preisgibt und der Anbieter dies auch nicht offen macht, sondern meist mit ausreichender Anonymisierung sich überall auf der Welt befinden kann – eher selten im Land der eigentlichen Tat. Dies trifft auch auf Ermittlungsbehörden zu. Erfahren sie von einer neuen Schadsoftware, können sie sich aufgrund des angebotenen Services darauf einstellen, ob dies nur Wenige betreffen wird oder ob aufgrund der Serviceleistungen ein größerer Schaden zu erwarten ist.

Tab. 1 Spieltheoretisches Modell für die Finanzierung von Malware. (Quellen: Ramses project: https://ramses2020.eu./ und Hurley-Smith et al. 2017, S. 23)

Ergebnis	Nutzen	
	Verbrecher	Opfer
Verbrecher infiziert Computer nicht	0	0
Freigabe der Daten für V	C	-C
Daten zerstört	-Y	-W
Verbrecher gefangen nach der Freigabe der Daten	-X	0
Verbrecher gefangen nach der Zerstörung der Daten	-Z	-W

Diese beispielhaft aufgeführte Methode der Finanzierung trifft nicht nur für kriminelle Einzeltäter zu, sondern ist auch Teil der Organisierten Kriminalität und kann von extremistischen Gruppierungen genutzt werden, um ihre Aktivitäten zu finanzieren. Gerade die derzeitige Entwicklung auf Bargeld zu verzichten und den Zahlungsverkehr per App zu verrichten, bietet vielseitige Möglichkeiten für kriminelle Aktivitäten.

2.2 Propaganda

Das Internet ist mittlerweile mit das wichtigste Medium für die Propaganda extremistischer Gruppen. Die Verbreitung der extremistischen Ideologie verfolgt zum einen das Ziel, neue Mitglieder zu gewinnen, zum anderen Sympathien für die Ideologie oder Aspekte dieser Ideologie zu gewinnen. Es gibt im Netz nicht nur viele Beispiele islamistischer Propaganda, auch linksextremistische, rechtsextremistische oder andere Gruppierungen nutzen diese Möglichkeit der Kommunikation intensiv (s. a. Kap. „Wired Drug War“). Gerade während und nach dem Flüchtlingsstrom 2015 nach Europa wurden von rechtsextremistischen und rechtspopulistischen Organisationen und Betreibern von Websites viele Unwahrheiten und verschwörungstheoretische Inhalte verbreitet. Häufig findet die Verbreitung mittels sozialer Medien und im sogenannten Surface-Web statt, also im offenen Internet. Dreiviertel aller Hasskommentare 2018 sind rechtsextremistisch oder rechtspopulistisch motiviert (Deutscher Bundestag 2019). Besonders jüngere Menschen habe bereits Kontakt mit Hasskommentaren gemacht. Laut einer Umfrage waren das 2018 61 % der 14-24-Jährigen und 48 % der 25-44-Jährigen, insgesamt waren es 30 % aller Internetnutzer, die mit Hasskommentaren in Berührung gekommen sind (Statista 2019).

Das Deepweb und das Darknet spielen erst im weiteren Radikalisierungsprozess eine größere Rolle. Laut einer Studie des Bundeskriminalamts (BKA) zu Ausreisenden nach Syrien, ist der Einfluss solcher Informationen bei über 50 %, aber mit rückläufiger Tendenz (44 %) (Bundeskriminalamt et al. 2016, S. 20 f.), wobei auch Unsicherheitsfaktoren der Untersuchung aufgezeigt werden (ebda., S. 10). Das Angebot ist bedauerlicherweise hier sehr vielfältig. Zu jeder Ideologie lassen sich entsprechende Seiten finden, die diese stützen und weiteren ideologischen Input liefern. Die Überzeugungstechniken von Cialdini (2006) finden sich in allen diesen Ideologien. Sie werden oft und auch in verschiedenen Foren und Posts wiederholt, was die Richtigkeit der Botschaft verdeutlichen soll. Der Sender tritt mit einer bestimmenden Autorität auf, die nicht an seiner Ansicht zweifeln lassen soll. Die Algorithmen der meisten Suchmaschinen sind

diesbezüglich auch nicht hilfreich, da sie den Empfänger bei Suchanfragen immer auf Seiten auf der Basis seiner vorigen Suchen und Seiten leiten, sodass der Eindruck entsteht, dass es sich hier um eine große Fülle an verschiedenen Seiten handelt, wobei es oft die gleichen Betreiber und die gleiche Information ist. Alternative Informationen werden nicht angeboten.

Inhaltlich lassen sich die Argumentationen von extremistischen Gruppierungen in der Regel den jeweiligen Ideologien gut zuordnen. Die Feindbilder werden klar definiert und sind leicht zu erkennen. Diese sind von großer Bedeutung, da im klassisch manichäischen Denken extremistischer Ideologien eindeutig definiert sein muss, wer der Feind ist, der an den gesehenen Missständen schuld ist. Diese Schuldzuweisung findet sich gerade im Internet auf eine bemerkenswert klare Weise. Allen ist die Ablehnung des Staates in seiner existierenden Form gemein.

Für Linksextremisten ist der Gegner neben dem Staat auch die Wirtschaft und insbesondere die Großkonzerne. Hier springen sie auch auf den Zug der Globalisierungsgegner auf. Rechtsextreme habe andere Ethnien zum Feindbild erklärt, die für alle Probleme verantwortlich gemacht werden. Auch sie sind erklärte Gegner der Globalisierung, die angeblich der Migration Tür und Tor öffnet und die eigene Wirtschaft schädigen soll. Salafistische Islamisten nutzen ebenfalls Globalisierungskritik in ihrer Argumentation, haben aber auch die Vereinigten Staaten, den Westen allgemein, Israel, Schiiten und andere muslimische Glaubensrichtungen als Feindbild.

Es lassen sich in der Darstellung der Feindbilder daher durchaus Gemeinsamkeiten bei verschiedenen Ideologien finden. Nur ist der Lösungsweg jeweils ein anderer, auch wenn teilweise die gleiche Literatur angeboten wird, wie die „Protokolle der Weisen von Zion“. Bei der Betrachtung der Inhalte dieser drei Ideologien, bedienen sie sich durchaus ähnlicher Argumentationen, was in Abb. 1 verdeutlichen wird. Auch gibt es Wechselwirkungen zwischen den einzelnen Feindbildern.

Neben dem übergeordneten Ziel des Umsturzes des existierenden Systems haben die anderen Elemente den Charakter, dass diese von den Gruppen in ihren Beiträgen in der Form verwendet werden, um weitere Begründungen für das primäre Ziel des Umsturzes zu haben. Daneben bedienen sich die Gruppierungen auch weiterer medialer Hilfsmittel. Neben reinen Texten werden vor allem Bilder verwendet, die häufig bearbeitet wurden, und gerade rechtsextremistische Seiten bieten häufig auch Musik an. Dies soll insbesondere Jugendliche ködern, da Musik als Teil der Jugendkultur ein Medium ist, mit dem sich gut Botschaften verbreiten lässt. Indizierte Bands, deren Musik nicht mehr auf Formaten wie YouTube oder ähnlichen zu finden sind, werden weiterhin auf alternativen Seiten

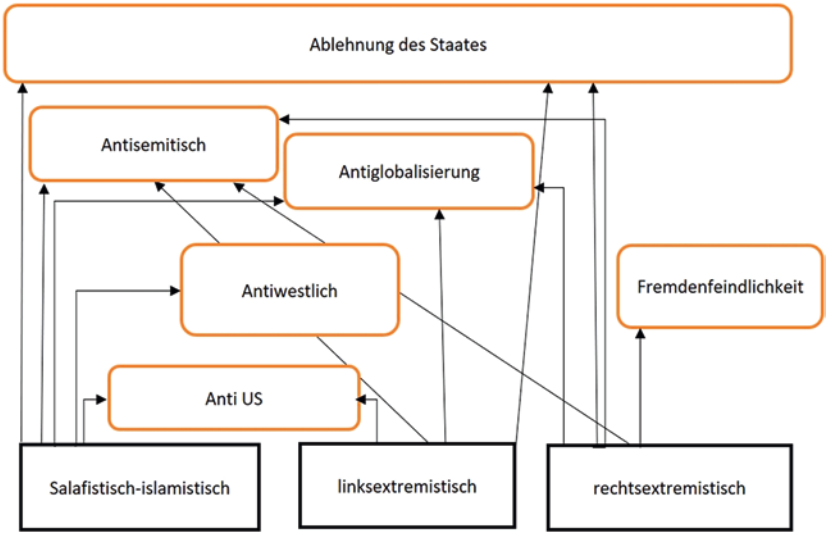


Abb. 1 Wechselwirkung extremistischer Ideologien

gebracht oder sind über das Darknet abrufbar. Videos des Islamischen Staates sind oft mit sogenannten Nasheeds unterlegt; Gesänge von Männern oft mit viel Hall ohne Instrumente, welche häufig die inhumanen Bilder und Videos mit vermeintlich religiösen, aber menschenverachtenden Texten noch verstärken.

Ein weiteres Element, dass die Wirkung der Propaganda noch nachhaltiger macht, ist der Einsatz von Verschwörungstheorien. Alle extremistischen Ideologien bedienen sich dieser und gerade im Internet ist die Verbreitung effektiv und nachhaltig. Einige dieser Verschwörungstheorien sind vollkommen unsinnig, aber sie werden verwendet, solange sie der Verbreitung der Ideologie dienen, ungeachtet von Fakten, die diesen widersprechen. Die Nähe zu den in den letzten Jahren in die Mode gekommenen Bezeichnung „Fake News“ liegt auf der Hand.

Es handelt sich hierbei nicht um ein neues Phänomen. Im Jahr 2000 schrieb Wilson (2000) das „Lexikon der Verschwörungstheorien“ und fasste einige der am weitesten verbreiteten zusammen. Mit dem Aufschwung des Internet und insbesondere der sozialen Medien nahm die Verbreitung dynamisch an Fahrt auf. Durch die Möglichkeiten Posts zu „retweeten“ und zu „liken“ haben diese in der Bearbeitung stark zugenommen. Für die Produzenten neuer Verschwörungstheorien ist die Verbreitung ein Geschäftsmodell. Sowohl David Icke, der Erfinder

der Reptinolautentheorie, nach der alle wichtigen Staatsmänner von außerirdischen Reptilien gesteuert werden, als auch Alex Jones mit seinem Portal *Infowars,* in dem diverse Theorien ein Portal finden, haben einen nicht geringen Profit dabei, da sie auch für Produkte werben, mit denen die Protagonsiten Geld verdienen. Per se wird immer mit Sorgen und Ängsten der Bevölkerung gespielt und dies ist auch auf politische Inhalte von Verschwörungstheorien übertragbar. Da diese einfache Lösungen bieten, fallen sie nicht selten auf fruchtbaren Boden (Cassam 2019, S. 33 ff.). Dabei werden in der Regel drei kognitive Vorurteile angesprochen:

- *Beabsichtigtes Vorurteil:* meint die Vermutung, dass ein Zustand absichtlich herbeigeführt wurde und nicht zufällig entstanden ist
- *Bestätigungsvorurteil:* bezeichnet das Suchen nach weiteren Aussagen zum bestehenden Vorurteil und dem Ignorieren von gegenteiligen Argumenten
- *Proportionales Vorurteil:* ist die Annahme, dass große Ereignisse auch große Ursachen haben, was unsere Anfälligkeit für Verschwörungstheorien erhöht (Cassam 2019, S. 40 f.)

Alle drei Aspekte kommen auch bei der Verbreitung von extremistischen Ideologien zum Tragen, da diese meist Elemente von Verschwörungstheorien beinhalten. Auch in der Vergangenheit war dies bereits zu beobachten. Anhänger oder Sympathisanten der linksterroristischen „Rote Armee Fraktion“ (RAF) waren der Überzeugung, dass die Mitglieder der ersten Generation der RAF, die in Stuttgart Stammheim inhaftiert waren, sich nicht suizidiert hatten, sondern, dass der Staat sie ermordet hatte. Und wenn sie es doch selber getan hatten, dann war der Staat dafür verantwortlich, da er sie zu diesem Schritt getrieben hatte (Aust 1997, S. 649). Die Sympathisanten/Empfänger dieser Theorie waren nicht bereit gegenteilige Argumente gelten zu lassen oder zu prüfen.

Häufig kommt es auch zu einer Vermischung verschiedener Ideologien mit dem Ziel eine möglichst große Bandbreite an potenziellen Rezipienten zu erreichen. Der vorab genannte David Icke, der Erfinder der „Reptilonauten“ hat neben rechtsextremen und antisemitischen Einstellungen auch ökologische Aspekte in seinen Publikationen. Ebenso finden sich auf verschiedenen Portalen neben klassischen rechtsextremen Einstellungen auch ökologische oder religiöse, meist esoterische Aspekte oder der germanische Götterkult. Dies ist auch bei dementsprechenden Verlagen und Vertriebsportalen ersichtlich.

Verschwörungstheorien sind anpassungsfähig und können auf diverse Aspekte der Ideologie angewandt werden (Abb. 2). Insbesondere im Falle eines besonderen Ereignisses kann die Verschwörungstheorie verwendet werden, um

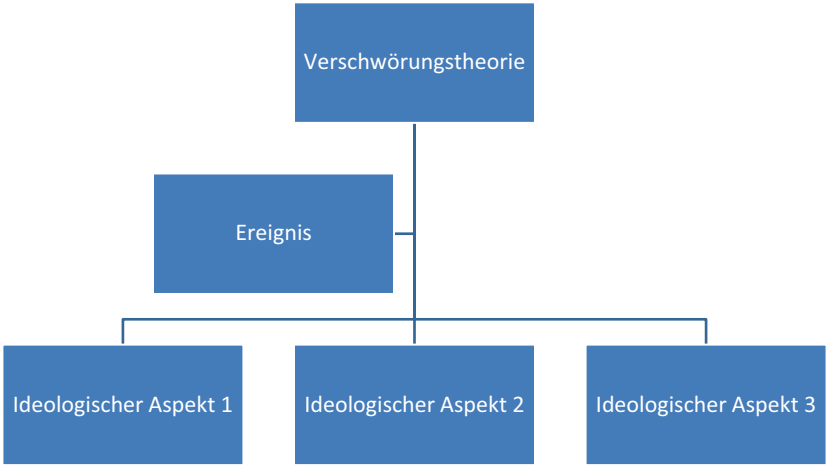


Abb. 2 Flexibilität von Verschwörungstheorien im Rahmen extremer Ideologien

den entsprechenden Aspekt zu erklären. Ein drastisches Beispiel ist der Anschlag vom 9. September 2001 gegen das World Trade Center in New York. Die Verschwörungstheorien drehten sich insbesondere um den Einsturz der Gebäude und dass diese so nicht hätten einstürzen dürfen. Für Islamisten war es ein Anschlag des Mossad und der CIA, da alle Juden vorher das Gebäude verlassen hätten, und für amerikanische Rechtsextremisten ist es ebenfalls das Werk der Regierung, um eine weitere Einschränkung der Freiheit und stärkere Überwachung zu rechtfertigen.

Häufig sind solche Theorien auch auf Portalen wie *4chan* zu finden und waren insbesondere auf *8chan* vorhanden. Nach den Anschlägen in Christchurch, Neuseeland und El Paso, Texas wurde das letztere Portal geschlossen. Gerade in den Unterforen fanden sich häufig rassistische Kommentare und Posts und der Attentäter von El Paso hatte seine Tat hier angekündigt. Obwohl die Seite von Google nicht mehr unterstützt wurde, gehörte sie zu den 5000 am meisten besuchten Webseiten der Welt (Kühl 2019). Eine Schließung des Portals, die mittlerweile vorgenommen wurde, dürfte das Problem allerdings nicht beseitigen, da die Nutzer ausweichen und sich auf anderen Portalen austauschen oder gar ins Darknet und zu den dort vorhandenen Foren abwandern.

Ziel der Propaganda ist das Erreichen von weiteren Personen, um sie für „die Sache“ zu gewinnen. Im salafistischen Spektrum ist das online Angebot ebenfalls sehr vielfältig. Diverse Foren laden zu Diskussionen ein, und das Ziel ist es am

Ende, zu einem persönlichen Kontakt zu kommen. Dieser Kontakt stellt die erste Unterhaltung dar; meist ist auch ein physischer Kontakt nötig, um Personen zu radikalisieren, aber nicht in jedem Fall. Die Zahl der Personen, die sich nur durch Kontakte über das Internet radikalisierten hat gerade im Bereich des Salafismus zugenommen. Die Autorin Lamya Kadoor beschreibt in ihrem Buch über die Radikalisierung Deutscher zum Salafismus diese Wirkweise. Im Anhang stellt sie noch eindrucksvoll ein solches Anbahnungsgespräch unter Frauen dar (Kaddor 2015). In der Dokumentation der Unterhaltung fällt auf, dass häufig auf religiöse Begriffe zurückgegriffen wird (s. a. Kap. „Posterboys und Terrorpropaganda“). Die Senderin (Radikalisiererin) verwendet die Begriffe allerdings anders als die Empfängerin. Auch ist die Senderin bemüht, einen gewissen Duktus einzuhalten, der typisch ist für ihre ideologische Ausrichtung. So verwendet sie Begriffe wie Khalif, Sheikh, Dawla und Kuffar. Auch ist sie in keinster Weise empfänglich für andere Sichtweisen. Besonders augenscheinlich wird dies bei der Sequenz über die Tötung von Frauen und Kindern. Die Senderin hat kein Verständnis für das religiöse Gegenargument und beschuldigt die Empfängerin, keine Gottesfurcht zu haben (ebd, S. 237 ff.). Diese Unterhaltung ist typisch und zeigt deutlich die Sichtweise von Extremisten und das Ignorieren anderer Meinungen sowie das Negieren von möglichen Alternativen.

Die Verwendung einer bestimmten Sprache ist ein Phänomen, dass auch in anderen extremistischen Ideologien zu finden ist. Rechtsextreme sprechen von „Tonträgern“, nicht von CDs, oder sprechen von „Volksgesundheit“ und verwenden andere aus dem Nationalsozialismus stammende Begriffe. Linksextreme betonen die Begriffe Masse (pauschalisiert: Bevölkerung), Kampf (gegen das System) und Revolution, ein Begriff, der auch im Rechtsextremismus immer wieder vorkommt, als Mittel das herrschende System zu beseitigen.

Soziale Medien und diverse Foren, auch im Darknet, bieten den Beteiligten die Möglichkeit zur Kommunikation. Der Attentäter von Ansbach etwa hatte während seines Anschlags Kontakt mit seinem vermutlichen Führungsmann in der Organisation. Gleiches gilt auch für die Attentäter von Mumbai, die währen der Tat dazu aufgefordert wurden, das größtmögliche Chaos zu verursachen und möglichst viele Menschen zu töten.

2.3 Kommunikation

Betrachtet man Terrorismus gemäß Waldmann (2011) als Kommunikationsstrategie, wird durch die Tat unter anderem auch die Ideologie transportiert. Seit der Einführung der sozialen Medien ist dieser Effekt noch gesteigert worden. So gibt es

für jede Stufe des Radikalisierungsprozesses das passende Material, welches online angeboten wird. Für den Gemeinschaftssinn und die Kameradschaft – ein Bedürfnis gerade für junge Menschen – sorgen unter anderem Videos von Pfingstreffen der mittlerweile verbotenen „Heimatreuen Deutschen Jugend“ oder Videos, in denen die selbsternannten „Gotteskrieger“ gemeinsam Kochen oder Wäsche waschen. Die Bilder, die das Fernsehen nicht zeigt, da sie zu brutal sind und entmenschlichend sind, werden insbesondere vom „Islamischen Staat“ selbst ins Netz gestellt. Sowohl im Deepweb, als auch im Darknet lassen sich viele solche Beispiele finden. Diese werden aber auch über Facebook und andere soziale Medien weiterverbreitet. Gerade im Deepweb findet sich eine große Anzahl solcher Videos und Posts, allerdings handelt es sich oft um dieselben Inhalte. Zudem werden Accounts oft geschlossen, sodass diese nur kurze Zeit auf den Adressen zu finden sind.

Zum einen geht es den Tätern hierbei um eine Selbstdarstellung und das Zeigen von Macht und der Lust an der Ausübung von Macht. Das soll beim Empfänger, welcher der Ideologie Sympathie entgegenbringt, das Bedürfnis wecken, auch Teil dieser „großen Sache“ zu sein. Im Idealfall ihn auch dazu animieren, selbst zu gewalttätigen Aktionen bereit zu sein und sich dem militanten Arm anzuschließen.

Zum anderen soll das Zeigen von erfolgreichen Anschlägen bei der Bevölkerung Angst auslösen und verstärken. Obwohl die Wahrscheinlichkeit in Westeuropa bei einem Autounfall ums Leben zu kommen, um ein Vielfaches höher ist, ist in der breiten Bevölkerung die Angst, Opfer eines Terroranschlags zu werden, deutlich höher. In der Studie der R+V Versicherung (2019) zu den Ängsten der Deutschen 2019 steht die Angst vor politischem Extremismus mit 47 % auf dem fünften Rang und vor Terrorismus mit 44 % auf dem neunten. Verglichen mit dem Spitzenreiter, der Angst der Überforderung durch Flüchtlinge mit 55 %, sind diese Ängste nahe dran. Allerdings hat die Angst vor Terrorismus im Vergleich zum Vorjahr um 15 % abgenommen. Angesichts der Höhe der Scheidungsrate in Deutschland ist die Angst vor dem Zerbrechen der Partnerschaft auf Rang 20 mit 15 % ebenfalls nicht sehr realistisch. Dies zeigt, dass Ängste etwas sehr subjektives und emotionales sind, wogegen rationale Erklärungen nur bedingt Abhilfe schaffen. Genau an dieser Stelle setzt die Kommunikation der Extremisten an. Sie spielen mit den Ängsten der Bevölkerung. Rechtspopulismus und Fremdenhass sind leichter zu steigern, wenn ein nicht geringer Teil der Bevölkerung durch Zuwanderung eine Gefahr für den Staat sieht. Das Internet bietet ein hervorragendes Medium zur Kontaktanbahnung und zur Verbreitung ihrer Ideen. Gerade bei der Radikalisierung kann es von großem Nutzen sein (Neumann 2013). Wenn es dann konkreter wird, können sich die Beteiligten in der Regel in geschlossene Foren oder auch das Darknet zurückziehen.

Die Wirkung von extremistischer Propaganda, die über das Internet kommuniziert wird, wirkt sich bei einer bereits vorhandenen Nähe zur Ideologie oder auch bei einem niedrigeren Bildungsstand stärker aus (Rieger et al. 2013). In einem weiteren Vergleich lässt sich feststellen, dass diese Form der Darbietung bei rechtsextremistischen und islamistisch-jihadistischen Inhalten sich sehr ähneln und durch Verschwörungstheorien und die Darstellung erlebnisorientiert ist (Schmitt et al. 2017). Es wäre allerdings ein Trugschluss davon auszugehen, dass ein höherer Bildungsstand die Gesellschaft vor Radikalisierung schützt. Er macht die Überzeugungsarbeit nur schwerer.

In den Online-Publikationen extremistischer Organisationen wird nicht nur die Ideologie verbreitet und allgemeine Informationen wiedergegeben, sondern es wird auch ganz spezifisch das Feindbild gestärkt, auf die angeblichen Verbrechen der „Anderen" verwiesen und warum der Staat oder andere Feinde der Ideologie schlecht sind. Häufig werden diese dann abgewertet. Das „Inspire" Magazin der al-Qaeda ist professionell aufgemacht und bedient viele verschieden Bedürfnisse der Empfänger. So wird auch hier das Feindbild des Westens oder Saudi Arabiens und auch anderer Staaten und Organisationen regelmäßig gepflegt und verstärkt. Die Texte sind oft mit Bildern unterlegt, welche die Botschaft weiter verstärken. Hier finden sich auch konkrete Aufrufe zu Straftaten, insbesondere zu Anschlägen oder gezielt zur Ermordung spezieller Personen.

Der „Islamische Staat" geht in seinen Online-Publikationen „Dabiq" und „Rumiyah" noch einen Schritt weiter und ruft öfter zu Straftaten auf (Landes 2017). In den von Landes untersuchten 45 Ausgaben der Publikationen waren 11 solcher Aufrufe von al-Qaeda und 41 vom „Islamischen Staat". Es handelt sich dabei nicht nur um westliche Politiker und Aktivisten, sondern sogar um salafistische Gelehrte, die den Weg der Gewalt des „Islamischen Staates" nicht in der gewünschten Form unterstützen, wie unter anderem der bekannte salafistische Prediger Pierre Vogel. Sprachlich werden den Appellen oft Beispiele von anderen Taten beigefügt, um die Dringlichkeit zu betonen und den Empfänger zu motivieren, einen ähnlichen „Heldenstatus" zu erreichen (z. B. „folgt dem Beispiel der Löwen aus Frankreich und Belgien, dem Beispiel des gesegneten Paares aus Kalifornien und den Beispielen der Ritter aus Orlando und Nizza!").

Auch die begleiteten Bilder sind dementsprechend so animiert und bearbeitet, dass sie Ähnlichkeit mit Kinoplakaten aufweisen (s. a. Kap. „Posterboys und Terrorpropaganda"). Das gleiche gilt für die Videoaufnahmen. In einem knapp 15 min langen Clip über die Struktur des „Islamischen Staates" werden alle Teile der Organisation erläutert. Dies geschieht mit einer guten grafischen Darstellung und gut geschnittenen Aufnahmen aus dem Gebiet des „Islamischen Staates". Es wird mit Zeitraffer, Slowmotion und Bildbearbeitung gearbeitet. In den letzten

drei Minuten werden allerdings auch in äußerst inhumaner Weise Aufnahmen von Hinrichtungen in Nahaufnahmen und Slowmotion gezeigt. Auch in der rechtsextremistischen oder der linksextremistischen Onlineszene lassen sich vergleichbare Beispiele finden. Eine Interaktion zwischen Sender und Empfänger ist hier natürlich nicht möglich, aber die Publikationen bieten ein solides Fundament für weitere Diskussionen, die sich dann in Foren abspielen.

2.4 Training

Eine weitere Funktion, die sich im Internet findet, ist das Bereitstellen von Informationen um Aktionen durchzuführen. Darunter finden sich auch Aufrufe zu Gewalttaten und wie man diese am besten ausführt. Die online Zeitschriften des Islamischen Staates „Dabiq“ und jetzt „al Rumiyah“ geben hier ebenso Tipps für Anschläge, wie das von al-Qaeda veröffentlichte „Inspire“ Magazin. Eine deutschsprachige Zeitschrift namens „Kybernetik“, die dem „Islamischen Staat“ nahe steht oder von ihm herausgegeben wird – dies ist nicht ganz klar – ruft zu Hackerangriffen auf. In der ersten Ausgabe heißt der Leitartikel „Wir töten auf der Basis von Metadaten“ und auf der letzten Seite ist die Anleitung für eine nähere Kontaktaufnahme über den Tor-Browser, vulgo das Darknet.

Neben den oben bereits erwähnten Aufrufen zu gezielten Morden findet sich in den Online-Medien auch ein große Anzahl an Material zur Durchführung von Attacken. In einer der letzten Ausgaben des „Inspire“ Magazins wird nicht nur zu Angriffen auf Bahnsystem aufgerufen, sondern es wird eine detaillierte Anleitung gegeben, wie ein Zug entgleisen kann. Die Attentäter auf die U-Bahn von London haben ihre Bomben in Anlehnung an den entsprechenden Artikel im „Inspire“ Magazin der al-Qaeda mit dem Titel „make a bomb in the kitchen of your mom. The AQ Chef“ gebaut. Darüber hinaus finden sich beim „Islamischen Staat“ sowohl in den Online-Publikationen als auch in Videos Anregungen und Anleitungen für Attacken. Vor dem Anschlag mit einem Lastwagen in Nizza waren Tipps für einen solchen Anschlag in Ihren Publikationen zu finden. Auch gibt es eine Videoanleitung für Angriffe mit dem Messer.

In „Rumiyah“ des „Islamischen Staates“ nimmt ein großer Teil der Berichte die Darstellung der erreichten Ziele und die Begründung der Überlegenheit des „Islamischen Staates“ ein (17,59 %). Das Konzept des Feindes kommt auf 11,98 % und legitimiert damit Angriffe auf die Feindbilder. Die Trainingsaspekte sind in der Regel Anleitungen zur Durchführung von Attacken. Insgesamt nehmen diese 11,98 % ein (Mattes 2018, S. 398 ff.). In der zweiten Ausgabe werden Messerangriffe von Einzeltätern en detail erläutert; in der dritten Ausgabe werden

Anschläge mit Fahrzeugen beschrieben. Die vierte Ausgabe bezieht sich wieder auf Messerangriffe, diesmal aber mit vielen Grafiken und Bildern. Ausgabe 5 behandelt Anschläge mit Gift und den Einsatz von Molotov-Cocktails und in der neunten Ausgabe geht es um Geiselnahmen und Anschläge mit Lastkraftwagen (Mattes 2018, S. 40 f.).

Die beiden oben genannten Gruppierungen bieten im Moment das meist Material an. Jedoch auch auf den Seiten von links- oder rechtsextremistischen Organisationen finden sich Handlungsanleitungen, wie z. B. mit unliebsamen Journalisten oder dem Gegner zu verfahren ist – oft auch mit Adressenliste.

3 Cyberterrorismus

Der Begriff Cyberterrorismus ist ähnlich wie Terrorismus unbestimmt und nicht klar definiert. Das Präfix „Cyber-“ wird mittlerweile vielen verschiedenen Begriffen zugeordnet und wirkt teils verwirrend und nicht immer eindeutig. Eindeutig ist allerdings die steigende Aktivität extremistischer Gruppen im Internet. Im weitesten Sinne kann der Begriff „Cyberterrorismus“ so verstanden werden, dass die bereits behandelte Propaganda und die Kommunikation als Unterpunkt unter diesem Begriff subsumiert werden können. Es beschreibt zunächst lediglich, dass die Aktivitäten in irgendeiner Form mit dem Internet zu tun haben. Die zu Beginn des Artikels genannte Finanzierung gehört im weitesten Sinne ebenfalls dazu, wie auch andere Formen des Cybercrime. Hier ist auch ein Nexus zwischen Terrorismus und organisierter Kriminalität; zum einen in der Finanzierung, zum anderen im gegenseitigen Unterstützen zu beidseitigem Nutzen, je nachdem welche Seite auf welchem Gebiet die besseren Kenntnisse hat. Ähnlich wie beim Narcoterrorismus, wo Organisierte Kriminalität und terroristische Gruppen kooperieren, wie in Kolumbien zwischen der FARC und den Kartellen von Medellin und Kali, ist es auch denkbar, dass hier Synergieeffekte genutzt werden. Viren werden im Darknet als Bausätze angeboten, sodass der Täter sich eigene aus verschiedenen Komponenten zusammenbauen kann, teilweise auch verbunden mit einer Serviceleistung. Für den Anbieter ist das Entdeckungsrisiko eher als gering einzustufen und der Täter hat die Möglichkeiten diese vielseitig einzusetzen. Ob der Täter rein finanzielle Interessen verfolgt, und folglich der klassischen Organisierten Kriminalität zuzuordnen ist, oder ob dabei auch ideologische Elemente eine Rolle spielen oder dies der Finanzierung solcher Ideologien gilt, ist dabei für die Begrifflichkeit Cybercrime nicht relevant, nur für die Zuordnung zum Oberbegriff Cyberterrorismus.

Hinsichtlich des Internet of Things (IoT) – und der damit stärker werdenden Vernetzung von Systemen des täglichen Lebens – sind auch weitere potenzielle Gefahren für die Zukunft denkbar. Gerade durch Hackerangriffe auf diese neuen Systeme könnte zum Beispiel die Wasserversorgung von Kommunen abgeschaltet, Ampeln willkürlich geschaltet oder in der Zukunft auch das automatisierte Fahren angegriffen werden. Das sogenannte „doxing“ (d. h. das Offenlegen von anonymen Accounts) oder das Hacken von gesicherten Personendaten kann sowohl für Cybercime als auch für Cyberterrorismus verwendet werden. Durchaus in diesen Kontext passt der Aufruf im Internet zur Ermordung von Personen, deren Adressen dann auch veröffentlicht werden, oder das Konstruieren von sogenannten „Fake News“, um die Bevölkerung zu verunsichern und Staaten instabiler zu machen. Die momentanen Hackerangriffe im Rahmen von Cyberterrorismus haben noch nicht den gleichen Medienerfolg und die gleichen Opferzahlen wie die Anschläge mit konventionellen Mitteln, aber es ist eine Steigerung zu beobachten und teils macht es auch die Kombination aus beiden aus.

Die vier genannten Aspekte Propaganda, Cybercrime, Kommunikation und Anschläge stellen daher die Grundlage der Verwendung des Begriffs „Cyberterrorismus“ dar (s. Abb. 3), da alle in dem gleichen Kontext stehen. Propaganda, Kommunikation und Cybercrime sind für Organisationen notwendig, um einen cyberterroristischen Anschlag durchzuführen.

Mehrere Gruppierungen sind mittlerweile mit einer ideologischen Motivation aktiv. Zum einen sind es Aktivisten, deren Ansinnen sich auf das Offenlegen von Missständen bezieht, wofür sie aber illegale Mittel einsetzen. Das ist allerdings

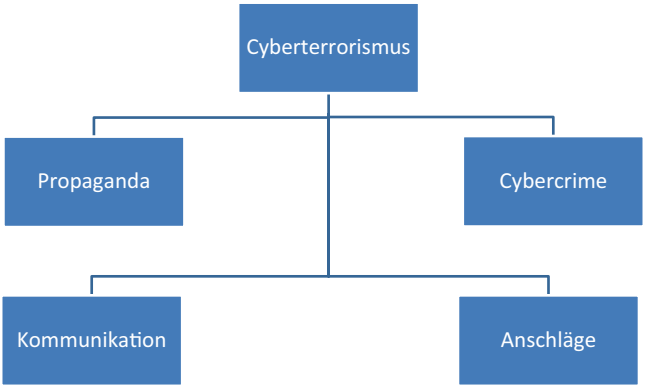


Abb. 3 Elemente des Cyberterrorismus

eine andere Qualität als Gruppierungen, die es sich zum Ziel gesetzt haben, Systeme zu zerstören und dafür auch auf den Cyberterrorismus zurückgreifen. Gerade der „Islamische Staat“ ist in diesem Bereich sehr aktiv.

Eine Untergruppe des „Islamischen Staates“ ist die 2015 gegründete „Islamic State Hacking Division“ oder das „Cyber-Caliphate“. Beide Namen wurden verwendet, aber es handelte sich um die gleichen Personen. Insbesondere der britische Hacker Junaid Hussain spielte hier eine führende Rolle. Junaid war früh als Hacker mit dem Namen TriCK bekannt. Geboren in einem Viertel in Birmingham mit hoher Kriminalität war er ein zurückhaltender Junge, der seine Freizeit gerne mit Spielen im Internet verbrachte. Nachdem sein Spieleaccount gehackt wurde, wollte er als Wiedergutmachung auch hacken und informierte sich dementsprechend. Er begann seine Karriere als TriCK und hackte oft die „English Defense League“, eine rechtsgerichtete britische Organisation. Darüber hinaus recherchierte er auch Verschwörungstheorien wie die Illuminati, die Freimauerer oder das Komitee der 300. Er tat sich in der Folge mit anderen Hackern mit Namen wie TeaMPoisoN (einer Gruppe von acht Hackern), MLT, forsaken und anderen zusammen. Sie hackten den Account von Sarkozy, dem Staatspräsidenten Frankreichs oder den Facebook-Account von Mark Zuckerberg. Wegen dieser und anderer Taten wurde er 2012 verhaftet (Nafees 2018). Auch TeaMPoisoN war vorher erfolgreich. Sie hackten unteranderem Kroatiens NATO-Website und in 2012 die Hotline des Counter Terrorism Commands von Großbritannien (Liebowitz 2012). Die Seite erhielt dauerhaft Anrufe, und wenn ein Mitarbeiter abhob, sagte eine Roboterstimme: „Team Poison“ (Liebowitz 2012).

Im Gefängnis radikalisierte sich Hussain zusehends. Vor seiner Inhaftierung sah er sich als ein Extremist, der Ungerechtigkeiten aufdecken und bekämpfen wollte, der aber keine Verbindungen zum radikalen Islam hatte. Nach seiner Inhaftiereung hatte er eine islamische Sichtweise auf viele Dinge. Angeblich wurde er in der Haft erleuchtet (Nafees 2018). Nicht lange danach wanderte er nach Syrien aus und war weiterhin auf Twitter und Facebook aktiv. Sein Profilfoto auf Twitter zeigt ihn halbmaskiert mit einer Maschinenpistole. Hier heiratete Sally Jones, die auch als weiße Witwe bekannt wurde, und die er bereit in England kennengelernt haben soll. Jones, die ihren Sohn mitgenommen hatte, wurde eine Ikone der Bewegung und versuchte nach Hussains Tod dessen Rolle einzunehmen (Asharq-Al Aswat 2018). Zu Beginn war das Hauptziel die Rekrutierung neuer Mitglieder und *foreign fighter* durch Online-Gruppen wie „Raqqa12“ und „The Legion“. Aber sehr schnell kamen Handlungsanleitungen zur Durchführung von Anschlägen insbesondere in Großbritannien hinzu. Auch gab er seine Kenntnisse über das Hacken im Zuge der „Islamic State Hacking Division“ weiter (Nafees 2018). Ardit Ferizi, ein 20-Jähriger aus dem Kosovo, der in Malaysia

Computerwissenschaften studierte, veröffentlichte daraufhin eine Liste mit den Adressen von 1351 Regierungs- und Militärmitarbeitern der USA (Nafees 2018). Seine Gruppe, die „Kosova Hacker's security" hackte über 20.000 europäische und amerikanische Webseiten, managte *penvid.com,* eine file-sharing Seite für Inhalte des „Islamischen Staates", bevor er seine Liste der zu tötenden Mitarbeitern der US-Regierung veröffentlichte (Alexander und Bennett 2019).

Eine weitere Gruppierung ist die „Muslim Cyber Army", deren Hauptoperationsgebiet in Indonesien und Malaysia liegt und die sich dem „Islamischen Staat" verpflichtet hat. So werden Personen, die angeblich den Islam verunglimpft haben, ausfindig gemacht, und deren persönliche Daten veröffentlicht. Dabei werden die Aktivitäten dieser Personen und deren wahren Identitäten veröffentlicht. Dieser Prozess wird „doxing" genannt. Kritische Beiträge auf Facebook wurden nach zwei bis fünf Tagen angegriffen und Gruppierungen, wie die „Islamic Defenders Front" fordern die Personen auf, sich öffentlich zu entschuldigen und beginnen eine Einschüchterungskampagne (Indonesia at Melbourne 2018). Diese Angriffe richten sich auch gegen Kommunisten, LGBT-Vertreter oder Ausländer. Neben der Verbreitung der gängigen Propaganda gehört auch das Verbreiten von Falschnachrichten elementar zur Arbeit der „Muslim Cyber Army". So wurde immer wieder behauptet, dass Indonesien in den Fängen der Volksrepublik China sei und deren Machthaber nur deren Erfüllungsgehilfen. Die Anzahl der Follower solcher Nachrichten geht in die Tausende (Chand 2019). Auch der Präsident von Indonesien wurde diffamiert und als Kommunist und Chinese bezeichnet (Jakarta Post 2018).

Eine Dachorganisation ist das „United Cyber Caliphate". Das Banner der Gruppe ist in der typischen Aufmachung des „Islamischen Staates" gestaltet und soll auch auf die Vereinigung verschiedener islamistischer cyberterroristischer Gruppen verweisen (s. Abb. 4). Die Darstellung ist ähnlich einem Kinoplakat; die Bilder sind aggressiv und bedrohend und der Schriftzug ist auch typisch für Action oder Horrofilme.

Das „United Cyber Caliphate" ist seit 2016 der Zusammenschluss verschiedener Organisationen, um das weitere Vorgehen besser zu koordinieren (Liang 2017, S. 6 f.). Nichts desto trotz operieren einige angegliederte Organisationen auch unabhängig. So wurden 2016 die Namen von 3600 namhaften und einflussreichen Bürgern von New York in einer Todesliste veröffentlicht (ICT 2016). Viele dieser Informationen werden über den russischen Anbieter Telegram übermittelt, aber auch das Darknet und das Deepweb spielen hier eine große Rolle.

Die Operationsweise hat sich seither nicht wesentlich geändert. Weiterhin werden Listen veröffentlicht und Hinweise zur Durchführung von Anschlägen gegeben. Auch sind Rekrutierungsmaßnahmen ein wesentlicher Bestandteil der

Abb. 4 Banner des United Cyber Caliphate

Aktivitäten. Ein weiterer Aspekt ist die Beschaffung von Waffen oder der Schutz der eigenen Identität im Netz (Liang 2017, S. 7). Die Bedrohung für die Datensicherheit bleibt auch nach vielen Rückschlägen für den „Islamischen Staat“ bestehen, da erst 2018 weitere Maßnahmen angekündigt wurden. Insbesondere gegen Hacktivisten, die gegen den „Islamischen Staat“ operieren, einschließlich Personen, die bei „Anonymus“ aktiv sind (Johnson 2019). In einer Untersuchung des amerikanischen Ministry of Homeland Security wurde dazu festgestellt, dass die persönlichen Informationen von Mitarbeitern von sieben von acht Regierungsinstitutionen nicht ausreichend gegen Datenmissbrauch geschützt sind (Homeland Security 2019). Das Ziel der Organisation ist unter anderem, den Willen der US-Bevölkerung zu brechen. Das Vertrauen in die Datensicherheit soll schwinden und das versuchen sie konsequent mit Veröffentlichung von personenbezogenen Daten zu erreichen. Auch die von Wikileaks unter „Vault 7“ veröffentlichten Informationen der CIA Cyber Intelligence könnten es in Zukunft extremistischen Organisationen und der organisierten Kriminalität erleichtern, auf Daten zurückzugreifen oder diese in der Kommunikation abzugreifen (Liang 2017, S. 8).

Der „Islamische Staat“ hat in den letzten Jahren Fortschritte in der Benutzung des Internet für seine Zwecke gemacht. Neben den physischen Attacken auf Charlie Hebdo 2015 wurden 19.000 französische Websites angegriffen. Der Effekt war gering, aber einige „denial of service“ Attacken waren erfolgreich. Auch wurden

parallel zur Attacke Unterstützungsposts gesendet und versucht, die Tat zu heroisieren (Giantas und Stergiou 2018).

Neben den beschriebenen Organisationen und Aktivitäten der dem „Islamischen Staat“ zugehörigen Organisationen gibt es eine Vielzahl weiterer Organisationen für die unterschiedlichen extremistischen Ideologien. Das Prinzip bleibt aber meist dasselbe. Die Organisationen im Kontext des „Islamischen Staat“ sind aber in ihrer Professionalität gut geeignete Beispiele. Gerade auch im rechten Spektrum lassen sich ähnliche Muster erkennen, die in ihrer Wirkweise ebenso erfolgreich sind. Die Arbeit mit Medien ist dort ebenso effizient; sei es mit Videos, wie dem „Unsterblich“-Video zur Anwerbung, in dem kaum Inhalte vermittelt werden, aber im Rahmen einer Demonstration Gemeinschaftsgefühl geweckt wird und das Gefühl, zu einer größeren Sache zu gehören, oder der Verbreitung von Propaganda durch Musik und Publikationen unterschiedlicher Ausprägung. Auch im linksextremistischen Spektrum ist dies beobachtbar. In Deutschland sind allerdings die meisten Hasskommentare und Posts auf das rechte Spektrum zurückzuführen, noch vor dem islamistischen.

4 Schlussbemerkung

Die Bandbreite der Aktivitäten von extremistischen Organisationen im Internet, sei es im Surface-Web, im Deepweb oder im Darknet ist groß. Im Moment lässt sich feststellen, dass die Hauptaktivitäten in der Verbreitung von Propaganda, der Rekrutierung neuer Personen und in der Hilfestellung für Anschläge steht. Auch das Offenlegen von persönlichen Daten muss in diesem Kontext gesehen werden.

Hinsichtlich der Finanzierung ergibt sich die die Möglichkeit der Kooperation zwischen extremistischen Organisationen und der organisierten Kriminalität. Hierbei ist es für die Zukunft wichtig, die Verteilungswege zu eruieren und mögliche Finanzierungswege auszuschließen. Der Täter des Attentats von Halle hatte von einem Unbekannten 720 EUR oder 0,1 Bitcoins als Unterstützung erhalten (Roebel 2019). Dies lässt darauf schließen, dass der Täter vorher über die Tat in irgendeiner Art kommuniziert hat. Solche Aktivitäten können über das Darknet gemacht worden sein. Finanzierung kann auf vielfältige Weise erfolgen und das Darknet spielt hier eine nicht unerhebliche Rolle, gerade wenn es um Malware geht. Ein weiterer Aspekt ist, dass die Meldung auch international abrufbar war (z. B. Sheva 2019). Für Deutschland weist das Bundeskriminalamt knapp 86.000 Fälle aus, was einer Steigerung von 4 % im Bereich Cybercrime entspricht (Bundeskriminalamt 2019). Insgesamt macht das 4,4 % aller Fälle aus und der Schaden ist durchschnittlich 4000 EUR pro Fall. Dies klingt nach nicht viel, aber

es ist zu befürchten, dass die Dunkelziffer deutlich höher liegt (vgl. Kap. „Problematik der Hell- und Dunkelfeldanalyse im Bereich Cybercrime“).

Die Kommunikation hat oft die Radikalisierung zu Ziel. Häufig werden die Betroffenen dann in das Darknet geholt, um eine entsprechende offene Kommunikation weiter zu gewährleisten. Aber ein Großteil findet zu Beginn im Surface-Web statt. Hier werden oft gewisse Narrative verwendet. Es gibt eine Diskussion, ob Gegennarrative sinnvoll sind; aber nach Ansicht des Autors sollten diese – auch rückblickend auf Fälle aus der Vergangenheit – durchaus eingesetzt werden, da diese eine klare Stellungnahme zeigen und damit durchaus einen Effekt haben können. Insbesondere hinsichtlich der Ängste und Unsicherheiten der betreffenden Personen besteht eine Chance diese zu erreichen. Besonders für Unentschlossene stellt dies ein Instrument zur Anti-Radikalisierung dar.

Gerade den Verschwörungstheorien, denen offensichtlich auch der Täter von Halle anhing, sollte und muss entgegenwirkt werden. Extremistische Organisationen nutzen diese gerne zur Erklärung der „Ungerechtigkeit der Welt“ aus ihrer Sicht. Die bekanntesten Feindbilder sind Freimaurer, Juden und Illuminati. Dies erfordert ein konsequentes Entgegnen der Zivilgesellschaft. Auch Fake News entstehen aus dem gleichen Konzept: Jemand ist schuld an der aktuellen Situation. Extremistische Organisationen arbeiten sehr gerne damit, weil es ihre Argumentationskette deutlich vereinfacht. Es gilt diesen konsequent entgegen zu argumentieren. Die Einrichtung der Faktenchecker vieler Medieneinrichtungen ist hier hilfreich, wobei demjenigen, der bereits überzeugt ist, diese nicht mehr glaubwürdig erscheinen. Für Personen aber, die überlegen, welche Informationen stimmen, sind diese Informationen hilfreich. Eine gesamtgesellschaftliche Herausforderung muss es sein, Falschmeldungen zu begegnen, da diese Informationen viele Aspekte der Gesellschaft negativ betrifft.[1] Auf der anderen Seite, die Sperrung eines Portals wie *8chan* kann durchaus kritisch gesehen werden, da dadurch Informationen verloren gehen. Die Kommunikation wird weiterhin stattfinden, aber sich jetzt auf verschiedene andere Medien verteilen. Dadurch wird eine Überwachung der Aktivitäten schwieriger.

Um den Bedrohungen von Extremisten aus dem Netz begegnen zu können, ist es notwendig, die Strafverfolgungsbehörden mit den notwendigen Mitteln rechtlich

[1]Das EU finanzierte Projekt PROPHETS etwa untersucht das Verhalten von Personen, die online radikalisiert werden. Diese Untersuchung bietet die Möglichkeit einer frühzeitigen Intervention durch die Analyse des online-Verhaltens. PROPHETS (preventing radicalisation online through the proliferation of harmonized toolkits); EU Projekt finanziert unter dem Horizon 2020 Program (Nr. 786894); für mehr Informationen siehe: https://www.prophets-h2020.eu/.

und technisch auszustatten. Aber dabei ist es unabdingbar, die Balance zwischen Freiheit und Sicherheit zu wahren. Neue technische Möglichkeiten können hier unterstützen. Die Publikation von Trainingsmaterial lässt für Strafverfolgungsbehörden die Möglichkeit zu, auch neue und nicht erwartete Anschlagsszenarien zu antizipieren. Zudem findet hier auch eine Kommunikation statt, die nicht unberücksichtigt bleiben sollte.

Die Gesellschaft wird immer stärker vernetzt und die Ausbreitung des Internet of Things (IoT) nimmt immer mehr zu. Viele Geräte haben aber keinen ausreichenden Schutz, sodass das angesprochene „doxing" sehr viel einfacher wird, wenn sich der Täter in ungeschützte Medien hacken kann. Das bedeutet, dass neben den „großen Szenarien", die vorstellbar sind, das IoT auch die Möglichkeit bietet, bisherige Aktivitäten einfacher auszuführen, da viele neue Geräte nicht den notwendigen Schutz vor fremden Zugriffen und Missbrauch haben. Eine Kooperation zwischen Industrie und Staat ist hier gefordert. Offensichtlich ist, dass die Gruppen voneinander lernen, unabhängig ihrer Ideologie. Die Bandbreite der bisherigen Aktivitäten und der zukünftig vorstellbaren ist sehr breit. Zivilgesellschaftlich bedarf es hier einer weiteren Aufklärung über die Gefahren, um diesen in der Zukunft adäquat begegnen zu können.

Literatur

Alexander, A., & Bennett, C. (2019). Doxing and defacements: Examining the Islamic state's hacking capabilities. https://ctc.usma.edu/doxing-defacements-examining-islamic-states-hacking-capabilities/. Zugegriffen: 23. Juni 2019.

Arutz Sheva. (2019). German synagogue shooter received $800 prior to attack, International News http://www.israelnationalnews.com/News/News.aspx/270061. Zugegriffen: 14. Okt. 2019.

Asharq-al Aswat. (2018). Sally Jones, the most dangerous ISIS operative alive. https://aawsat.com/english/home/article/1441726/sally-jones-most-dangerous-isis-operative-alive. Zugegriffen: 12. Juli 2019.

Aust, S. (1997). *Der Baader Meinhof Komplex*. Hamburg: Hoffmann und Campe.

Bartlett, J. (2016). *The dark net*. Kulmbach: Plassen.

Bundeskriminalamt, Bundesamt für Verfassungsschutz, Hessisches Informations- und Kompetenzzentrum gegen Extremismus (Hrsg.). (2016). Analyse der Radikalisierungshintergründe und -verläufe der Personen, die aus islamistischer Motivation aus Deutschland in Richtung Syrien oder Irak ausgereist sind.

Bundeskriminalamt. (2019). Cybercrrime in zahlen 2017, Lagebild 2017. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2017.html?nn=28110. Zugegriffen: 22. Sept. 2019.

Cassam, Q. (2019). *Conspircy theories*. Cambridge: Polity.

Chand, N. (2019). Indonesia arrests muslim cyber army member for spreading fake news and hate speech, International Business Times. https://www.ibtimes.com/indonesia-arrests-muslim-cyber-army-member-spreading-fake-news-hate-speech-2803728. Zugegriffen: 23. Juli 2019.

Chertoff, M. (2016). A public policy perspective of the dark web. https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1298643. Zugegriffen: 4. Juni 2019.

Cialdini, R. (2006). *Die Psychologie des Überzeugens*. Bern: Huber.

Deutscher Bundestag. (2019). Hasspostings im internet 2018, Kleine Anfrage der Abgeordneten Petra Pau, Dr. André Hahn, Doris Achelwilm, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 19/11394. https://dip21.bundestag.de/dip21/btd/19/119/1911908.pdf. Zugegriffen: 3. Okt. 2019.

Europol. (2014). The internet organised crime threat assessment. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2014. Zugegriffen: 13. Juni 2019.

Giantas, D., & Stergiou, D. (2018). From terrorism to cyber-terrorism: The case of ISIS, Hellenic Institute for Startegic Studies, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3135927. Zugegriffen: 23. Aug. 2019.

Hernandez-Castro, J., Cartwright, E., & Stepanova, A. (2017). Economic analysis of ransomware. https://arxiv.org/pdf/1703.06660.pdf.

Homeland Security. (2019). Bipartisan report shows 8 federal agencies' cybersecurity failures put Americans' personal information at risk. https://www.hstoday.us/subject-matter-areas/cybersecurity/bipartisan-report-shows-8-federal-agencies-cybersecurity-failures-put-americans-personal-information-at-risk/. Zugegriffen: 12. Aug. 2019.

Hurley-Smith, D., Hernandez-Castro, J., Cartwright, E., & Stepanova, A. (2017). D4.1 Findings on economic modelling of malware as business model. https://ramses2020.eu/wp-content/uploads/sites/3/2016/09/D4.1-Findings-on-economic-modelling-of-malwares-a-business-modell.pdf. Zugegriffen: 03. Okt. 2019.

ICT. (2016). "Killing lists" – The evolution of cyber terrorism? https://www.ict.org.il/Article/1793/killing-lists-the-evolution-of-cyber-terrorism#gsc.tab=0. Zugegriffen: 12. März 2018.

Indonesia at Melbourne. (2018). The muslim cyber army: What is it and what does it want? https://indonesiaatmelbourne.unimelb.edu.au/the-muslim-cyber-army-what-is-it-and-what-does-it-want/. Zugegriffen: 12. Aug. 2018.

Internet Worlds Stats. (2019). Usage and population statistics. https://www.internetworldstats.com/stats.htm. Zugegriffen: 4. Mai 2019.

Jakarta Post. (2018). Editorial: Comabatting caber lies. https://www.thejakartapost.com/academia/2018/03/01/editorial-combating-cyber-lies.html. Zugegriffen: 12. Aug. 2019.

Johnson, B. (2019). New ISIS cyber campaign announced as supporters share U.S. agency vulnerabilities, homeland security today. https://www.hstoday.us/subject-matter-areas/counterterrorism/new-isis-cyber-campaign-announced-as-supporters-share-u-s-agency-vulnerabilities/. Zugegriffen: 13. Aug. 2019.

Kaddor, L. (2015). *Zum Töten bereit*. München: Piper.

Kaspersky Lab and Global Research and Analysis Team. (2017). Kaspersky security bulletin 2017 https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07164824/KSB_Story_of_the_Year_Ransomware_FINAL_eng.pdf. Zugegriffen: 12. Febr. 2019.

Kaspersky Lab and Global Research and Analysis Team. (2019). Kaspersky security bulletin 2018. https://securelist.com/kaspersky-security-bulletin-2018-statistics/89145/. Zugegriffen: 22. Juni 2019.

Kühl, E. (2019). Wo weiße Terroristen posten. Zeit online. https://www.zeit.de/digital/internet/2019-08/8chan-plattform-forum-attentat-el-paso-cloudflare. Zugegriffen: 4. Juni 2019.

Landes, S. (2017). Analyse zu Aufrufen zur Begehung von extremistischen Gewalthandlungen und Straftaten über Online-Medien im Bereich Jihadismus/Salafismus, Masterarbeit. Deutsche Hochschule der Polizei, Münster.

Liang, C. (2017). Unveiling the „United cyber caliphate“ and the birth of the e-terrorist, Georgetown Journal of International Affairs, International Engagement on Cyber VII, Volume XVIII, Nr. III. https://dam.gcsp.ch/files/2y10J90JJDcWfuIrVEExJU5SuOkDgq8V08daYodqmvT26flfqCIibJmC. Zugegriffen: 12. Febr. 2019.

Liebowitz, M. (2012). TeaMPoison hacks MI-6 – Then calls to boost. NBC News. http://www.nbcnews.com/id/47032601/ns/technology_and_science-security/t/team-poison-hacks-mi-then-calls-boast/#.XaN3ZWB7nIU. Zugegriffen: 3. Okt. 2019.

Mattes, T. (2018). *Rumiyah, Masterarbeit*. Münster: Deutsche Hochschule der Polizei.

Nafees, H. (2018). The British hacker who Became the Islamic state chief terror cybercoach: A profile of Junaid Hussain. https://ctc.usma.edu/british-hacker-became-islamic-states-chief-terror-cybercoach-profile-junaid-hussain/. Zugegriffen: 10. Okt. 2018.

Neumann, P. (2013). Options and strategies for countering online radicalisation in the United States. *Studies in Conflict and Terrorism, 36* (6), 431–459.

R + V Versicherung. (Hrsg.). (2019). Die Ängste der Deutschen. https://www.ruv.de/presse/aengste-der-deutschen/grafiken-die-aengste-der-deutschen. Zugegriffen: 26. Sept. 2019.

Rieger, D., Frischlich, L., & Bente, G. (2013). *Propaganda 2.0. Psychligical Effects of Right Wing and Islamic Extremist Internet Videos, Polizei und Forschung* (Bd. 44). Köln: Wolters Kluwer.

Roebel, S. (2019). Halle-Attentäter wurde von Unbekanntem finanziell unterstützt. Spiegel online. https://www.spiegel.de/panorama/justiz/halle-saale-attentaeter-wurde-von-unbekanntem-finanziell-unterstuetzt-a-1291171.html. Zugegriffen: 14. Okt. 2019.

Schmitt, J., Ernst, J., Frischlich, L., & Rieger, D. (2017). rechtsextreme und islamistische Propaganda im Internet: Methoden, Wirkungen und Präventionsmöglichkeiten. In R. Altenhoff, S. Bunk, & M. Piepenschneider (Hrsg.), *Politischer Extremismus im Vergleich. Beiträge zur Politischen Bildung* (Bd. 3). Berlin: LIT.

Statista. (2019). Wie häufig haben Sie persönlich schon Hassrede bzw. Hasskommentare im Internet gesehen? https://de.statista.com/statistik/daten/studie/808263/umfrage/umfrage-zur-wahrnehmungshaeufigkeit-von-hasskommentaren-im-internet-nach-alter/. Zugegriffen: 3. Okt. 2019.

Waldmann, P. (2011). *Terrorismus. Provokation der Macht*. Hamburg: Murmann.

Wilson, A. (2000). *Lexikon der Verschwörungstheorien*. Köln: Eichborn.

Wie Cyberterrorismus stattfindet – und warum wir ihn nicht sehen

Wirklichkeitsmanipulation als virtuelle Gewalt

Sebastian Enghofer, Daniel Müller und Alessandro Parrino

1 #Pizzagate – Ein Präzedenzfall

Verschwörungstheorien von im Untergrund herrschenden „Echsenmenschen“ oder einer „flachen Erde“ mögen in den Augen eines aufgeklärten Menschen abwegig und bizarr erscheinen, doch tatsächlich erfahren diese Narrative dank dem Internet erhöhte Beachtung. Schon lange sind Ufos, die „false-flag-Anschläge“ von 9/11 und die gefälschte Mondlandung Teil eines virtuellen Erklärungsangebots an Menschen, die grundsätzliches Misstrauen gegenüber traditionellen Medien oder dem „Mainstream-Glauben“ hegen. Während diese Devianz in der bisherigen Form keine oder kaum Auswirkungen auf gesellschaftliche Prozesse hatte, ist ab 2016 eine Zeitenwende erkennbar. Verschiedene Indizien geben Anlass zur Sorge, denn obwohl sog. „alternative Fakten“ – Falschmeldungen, Fake-News und Desinformationen – keine gänzlich neuen politischen Phänomene darstellen, erhöht sich deren virulente Wirkung durch das Internet. Dabei sticht insbesondere ein Vorfall hervor, der als Präzedenzfall einer Wirklichkeitsmanipulation mit weitreichender Implikation gelten kann: #Pizzagate.

S. Enghofer (✉) · D. Müller
Regensburg, Deutschland
E-Mail: sebastian.enghofer@ur.de

D. Müller
E-Mail: daniel1.mueller@ur.de

A. Parrino
München, Deutschland
E-Mail: A.Parrino@protonmail.com

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

T.-G. Rüdiger und P. S. Bayerl (Hrsg.), *Cyberkriminologie,*
https://doi.org/10.1007/978-3-658-28507-4_9

Am 4. Dezember 2016 stürmte der 28-Jährige Edgar Maddison Welch, bewaffnet mit einem AR-15 Sturmgewehr, das Pizzarestaurant *Comet Ping Pong* und feuerte drei Schüsse ab. Nach eigenen Aussagen wollte Welch Nachforschungen anstellen und die Opfer eines mutmaßlichen Kinderpornografie-Rings befreien. Seine Informationen und Motive basierten auf einer viralen Verschwörungstheorie, die auf der Internet-Plattform *4chan* ihren Anfang genommen hatte. Als der Wahlkampfmanager von Hillary Clinton, John Podesta, Opfer einer E-Mail-Phishingattacke wurde, gelang es den Angreifern, interne Emails zu stehlen. Nach der Veröffentlichung auf Wikileaks wurden vor allem die E-Mails zwischen Podesta und James Alefantis, dem Besitzer von Comet Ping Pong, Teil einer wirren Spekulation von 4chan-Nutzern. Demnach sollen Geheimcodes in den E-Mails einen Kinderpornografie-Ring der Demokratischen Partei belegen und das Restaurant *Comet Ping Pong* als Umschlagplatz sowie Zentrale dienen. Während davon auszugehen ist, dass auf 4chan Trolls hinter dieser bizarren Herleitung steckten, übertrug sich die Kinderpornoring-Narrative schnell auf das Subreddit *r/The_Donald.* Trump-Anhänger teilten auf Facebook und Twitter die Verschwörungsanalysen der Trolle unter #Pizzagate und, als der sog. „Info-Krieger" Alex Jones die Thematik aufnahm, überschlugen sich die Falschmeldungen. In einem später gelöschten Video mit insgesamt 420.000 Aufrufen, das Anfang November 2016 veröffentlicht wurde, erklärte Jones, dass Hillary Clinton höchstpersönlich Kinder getötet habe (Lopez 2016).[1]

Angetrieben durch ein Klima des politischen Wahlkampfs und kanalisiert durch virtuell geteilte Gerüchte, Verschwörungen und Desinformationen beschloss Welch den Kinderpornografie-Ring selbst zu sprengen. Seine Wahrnehmung der Wirklichkeit wurde dahin gehend beeinflusst, dass er mit einer geladenen Waffe das Gesetz selbst in die Hand nahm, um dem angeblich ungeheuerlichen Treiben der demokratischen Eliten um Hillary Clinton ein Ende zu setzen. Aus einer virtuellen Verschwörungstheorie wurde ein Fall realer Gewalt, der nur aufgrund glücklicher Umstände keine Menschenleben forderte. Diese Wechselwirkung stellt eine Zäsur dar, die es wissenschaftlich zu untersuchen gilt.

Dieses Kapitel wird den Vorfall „Pizzagate" zum Anlass nehmen, ein neues Phänomen im Cyber- und Informationsraum zu skizzieren, welches die Grundfesten der Demokratie auf ähnliche Weise wie klassischer Terrorismus attackiert.

[1]Für einen detaillierten chronologischen Verlauf der Geschehnisse siehe Lopez (2016) und Tuters und Jakubauskaité (2018).

Anders als gängige Interpretationen innerhalb des Forschungsdiskurses gehen die Autoren davon aus, dass Cyberterrorismus existiert und bereits stattfindet, aber dieses Phänomen aufgrund veralteter Definitionen nicht als solches wahrgenommen wird.

Kern der Hypothese ist die Existenz rein „virtueller" Gewalt, welche in ihren Konsequenzen den klassischen Wirkmitteln terroristischer Bestrebungen in nichts nachsteht. Als prägnantes Beispiel dafür gilt die Manipulation von empfundener Wirklichkeit, mithilfe derer die breite Verunsicherung der Bevölkerung und die Destabilisierung des öffentlichen Raumes genauso erreicht werden kann wie mit konventionellen Anschlägen. Insofern folgern die Autoren aus einer rein konsequentialistischen und nicht ätiologischen oder deduktiven Herangehensweise, dass Cyberterrorismus bereits stattfindet und wir neue Paradigmen zu seiner Einordnung finden müssen. Um diese Argumentation einzulösen, stellen wir den „Cyberkrieg" als maximale Eskalation im Cyber- und Informationsraum vorweg, um Cyberterrorismus und dessen Kommunikationsgrundlagen abzustecken. Anschließend wird im demokratietheoretischen Kontext die Ambiguitätstoleranz verhandelt, welche vor allem die Schaffung einer wahrhaften Wirklichkeitsperzeption kritisch diskutiert. Zu guter Letzt werden beide Ansätze synthetisiert, um das Phänomen der „virtuellen" Gewalt als Wirkmittel cyberterroristischer Strategie in eine „reale" Wirklichkeitsmanipulation aufzuschlüsseln. Abgeleitet aus der Logik der Vertrauenssabotage (Rid 2018, S. 58) transformiert in eine terroristische Kommunikationsstrategie (Waldmann 2011) wird das Selbstverständnis der Gesellschaft mittels „virtueller" Gewalt gestört. Diese Störung stellt faktisch eine Manipulation der Wahrnehmung einzelner Individuen dar, welche sich dann partizipatorisch kollektiv entladen kann.

2 Von Krieg, Terrorismus und Gewalt im Cyber- und Informationsraum

Der Krieg im Cyber- und Informationsraum ist nicht neu. Bereits im Jahr 1993 erklärten John Arquilla und David Ronfeldt in ihrem viel zitierten Beitrag (Arquilla und Ronfeldt 1993) für die RAND Corporation: *„Der Cyberkrieg kommt!"* Auch wenn Informationen immer Teil der Kriegsführung waren, nehmen die Autoren deren exzeptionelle Bedeutung mit der von ihnen proklamierten „Informationsrevolution" (Arquilla und Ronfeldt 1998, S. 24–56) vorweg. Diese Revolution betrifft die zunehmende Computerisierung aller Teilbereiche des Lebens und ist damit kriegsführungsrelevant. 1993 war diese Revolution noch ganz am Anfang. Heute ist die Computerisierung und Technisierung aller Lebensbereiche vollendet.

Aus der inzwischen Realität gewordenen Feststellung leiteten Arquilla und Ronfeldt bereits damals die Kernmaxime ab, dass Informationen selbst zu einer Ressource werden und damit eine strategische Größe darstellen (Arquilla und Ronfeldt 1998, S. 26). Frei nach Clausewitz[2] ist der Krieg im Cyber- und Informationsraum ein Mittel heutiger Politik und, um diesen zu gewinnen, gilt es die fünfte Dimension militärisch zu kontrollieren. Für den Cybermilitärtheoretiker Sandro Gaycken ist dieser Trend eines „Cyberwar" vollständig gegeben, denn heute ist der Computer ein dezidiertes und gar natürliches Angriffsziel.

Die digitale Abhängigkeit und Computerisierung westlicher Armeen und Gesellschaften offenbart virtuelle Schwachstellen, welche bereits systemisch angelegt sind (Gaycken 2011, S. 45). Während Gaycken vor allem die Hardware in den Fokus nimmt, erklärten Arquilla und Ronfeld, dass der Cyberkrieg das *„Selbstverständnis des Gegners"* attackieren müsse. So soll die *„Beantwortung der Fragen, wer er ist, wo er ist, was er wann tun kann, warum er kämpft, welchen Bedrohungen er sich zuerst stellen soll, usw."* (Arquilla und Ronfeldt, 1998, S. 31) verhindert werden. Clausewitz spricht vom *„Niederwerfen des Gegners"*, um ihm die Möglichkeit des Widerstandes zu nehmen. Komplementär bildet sich das eigentliche Ziel einer kriegerischen Unternehmung, denn es gilt, den Gegner wehrlos zu machen. Für Herfried Münkler zeichnet sich der Cyberkrieg nicht durch eine möglichst hohe eigene Truppenstärke aus, die mit schierer Übermacht eine Willensdurchsetzung erwirkt, sondern er soll das Nervensystem und die Infrastruktur des Feindes stören, welche erst eine Willensentwicklung ermöglichen (Münkler 2015, S. 276). Der instrumentelle und politische Charakter deckt sich sowohl mit Gayckens Notwendigkeit, die Schwachstellen der Computerisierung zu nutzen, als auch mit der Feststellung von Münkler, dass die sog. „Neuen Kriege"[3] und mehr noch der Cyberkrieg von der politischen Zielsetzung geprägt sind, dem Gegner die Grundlage seiner Willensbildung zu nehmen.

---

[2]Nach Clausewitz muss jeder kriegerische Akt einen gewaltvollen, instrumentellen und politischen Charakter haben. Das erste Element seiner Trias des Krieges ist *„ein Akt der Gewalt, um den Gegner zur Erfüllung unseres Willens zu zwingen"* (Clausewitz 2010, S. 3). Das Mittel des Krieges ist demnach Gewalt, um den Zweck der Willensprojektion zu erfüllen. Vorrangiges Ziel des Krieges ist es, den Gegner wehrlos zu machen. Das „Wehrlosmachen" eines Feindes führt demnach unmittelbar zu dessen Willenlosigkeit bzw. zu der Möglichkeit für den Sieger, Macht über den Besiegten auszuüben. (Clausewitz 2010).

[3]Herfried Münkler rückt die Umweltbedingungen kriegerischer Auseinandersetzungen nach clausewitzschen Vorbild in den Mittelpunkt. Demnach werden die „Neuen Kriege" als Konflikte zwischen nichtstaatlichen, innerstaatlichen und multistaatlichen Akteuren definiert (Münkler 2015, S. 217 f.).

Thomas Rid erklärt vor dem Hintergrund der clausewitzschen Definition von Krieg[4], dass es keinen Cyberkrieg gibt, der einen Akt der Gewalt darstellt. Stattdessen wird der Begriff Cyberkrieg für gänzlich andere staatliche Mittel falsch verwendet, denn in Wirklichkeit finden lediglich niederschwellige Konflikte im Cyber- und Informationsraum wie Spionage, Sabotage oder Subversion statt. Rid bewertet den Einsatz von Gewalt als entscheidenden Faktor, um eine kriegerische Handlung zu definieren. Der Politikwissenschaftler sieht jedoch den Cyberaspekt der Gewaltausübung nur in mittelbarer Form gegeben. Demnach kann ein Programmcode nur indirekte Gewalt verursachen, da er selbst nicht die Waffe ist, sondern das Ziel zur Waffe werden lässt (Rid 2018, S. 37). Rids Argumentation ist grundsätzlicher und philosophischer Natur. So ist das „wahre" Zielobjekt von kriegerischer Gewalt genuin der menschliche Körper, jedoch können Cyberwaffen nur Maschinen direkt attackieren. Folglich ist der physische Charakter von Gewalt im Zusammenhang mit modernen Kriegsführungskonzepten ein definitorisches Problem, da Cybermittel erstmalig nur virtuell und im nicht physischen Raum wirken. Clausewitz *„Akt der Gewalt"* muss dementsprechend neu beurteilt werden (Rid 2018, S. 13–48). Rid vertritt die Meinung, dass die Wirkung von Cyberangriffen unter Einbeziehung verschiedenster Gewaltformen – körperlich, symbolisch und emotional – im Vergleich zu den analogen Methoden vernachlässigbar ist.

Jedoch können Cyberangriffe, so Rid (2018, S. 49–55), auf das die Gesellschaft konstituierende Vertrauen ähnlich destruktiv wirken. Er attestiert Cyberattacken eine „Logik der Vertrauenssabotage", welche letztlich, in psychologische Effekte übersetzt, erschütternde Wirkungen erzeugen können. Rid negiert zwar grundsätzlich den Begriff „Cyberkrieg", erkennt aber Kausalitäten, die eine staatliche Tätigkeit – Sabotage, Spionage, Subversion – im Cyberraum zumindest theoretisch nützlich macht. Rid verweist ebenfalls auf den terroristischen Akteur, dessen Hauptziel es ist:

> „die Meinungsführer in der Bevölkerung eines Landes davon zu überzeugen, dass ihre derzeitige Regierung weder nach außen noch im Inneren in der Lage sein wird, das Gewaltmonopol zu behaupten oder wieder an sich zu reißen. Cyberattacken können die Vertrauenswürdigkeit einer Institution auf [physisch] gewaltfreie Weise erschüttern." (Rid 2018, S.57)

Die moderne Gesellschaft und Staatlichkeit fußen auf global vernetzter Informationstechnik, welche Industrieanlagen, kritische Infrastruktur sowie öffentliche und wirtschaftliche Dienste erst möglich macht. Die massive Störung solcher

[4] *„Der Krieg ist also ein Akt der Gewalt, um den Gegner zur Erfüllung unseres Willens zu zwingen"* (Clausewitz 2010, S. 3).

kommt heute einem Wehrlosmachen oder Niederwerfen gleich. Damit kann der Krieg im Cyber- und Informationsraum als maximale Eskalation nicht nur das Selbstverständnis des Gegners attackieren, also die psychologische Komponente eines Staates, sondern auch dessen Körper, das Machtfundament, das Nervensystem moderner Staatlichkeit. Im Verbund mit einer Logik der Vertrauenssabotage öffnet sich ein weites Feld der operationellen terroristischen Möglichkeiten.

In der neueren Terrorismusforschung wird Terrorismus definiert als die Anwendung physischer und psychischer Gewalt mit dem Ziel, Verunsicherung sowie Angst und Schrecken in der Bevölkerung zu verbreiten. Dadurch sollen politische Institutionen destabilisiert und zugleich eigene politische Ziele vermittelt werden. Terrorismus stellt dementsprechend primär eine Kommunikationsstrategie dar (Waldmann 2011).

Vor dem Hintergrund des Cyberterrorismus ist diese Definition essenziell, denn der Cyber- und Informationsraum ist die ultimative Kommunikationsplattform (BKA 2016, S. 20). Zum einen lässt sich daraus ableiten, dass Terroristen im Internet operieren, um die Aufmerksamkeit für ihre Agenda zu erhöhen. Diese Form des Cyberterrorismus nutzt das Internet nur als Werkzeug, um analoge und klassische Formen der Kampfstrategie zu unterstützen. Zum anderen lassen sich Angriffe im Cyberspace selbst als terroristischer Akt werten. Im akademischen Diskurs finden sich zwei unterschiedliche Definitionen (Jarvis et al. 2014, S. 28). Die eng gefasste Sichtweise, welche auf Dorothy Denning zurückgeht, stellt die Attacken gegen Computer in den Mittelpunkt:

> „Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.“ (Denning 2000, S. 1)

Dennings Definition von Cyberterrorismus aus dem Jahr 2000 ist eine der ersten ihrer Art. Besonders an dieser Definition ist, dass der Angriffsvektor von Cyberterroristen der Computer an sich ist bzw. dessen Struktur und Daten.[5] Grenzen zieht ihre Definition in der Konsequenz dieser Angriffe. Um als ein „Cyberterroristischer Angriff“ zu gelten, muss dieser mindestens entweder in Gewalt gegen Individuen, Sachen oder in allgemeiner Angst oder Verunsicherung

[5]Insbesondere ist hier die Äquivalenz zu Gayckens Trend zum Cyberkrieg hervorzuheben, denn da IT-Infrastruktur ideale Schwachstellen besitzt, kann und muss das Ausnutzen dieser ebenfalls als cyber-terroristische Methodik erkannt werden.

resultieren. Bemerkenswert ist die klare Linie, die Denning zu einer Störung/Unterbrechung von Diensten zieht, die nicht kritisch oder essenziell sind. Angriffe, welche zwar zu einem kostspieligen Ärgernis führen oder die Nerven strapazieren, aber sonst keinen kritischen Schaden anrichten, sind explizit kein Cyberterrorismus. Dennings Definition ist eine enge und konsequentialistische Version, denn laut Gordon und Ford beschreibt sie „nur" das idealtypische Phänomen des „pure Cyberterrorism".[6]

Nach der breit angelegten Definition von Gordon und Ford lässt sich bereits der Onlinekauf von Flugtickets für die Ausführung der 9/11-Anschläge als Cyberterrorismus begreifen (Jarvis et al. 2014, S. 28).

Eine Differenzierung erweist sich in Anbetracht der möglichen Spielarten des Cyberterrorismus als obligatorisch. Maura Conway unterscheidet deswegen grundlegend zwischen *„terrorist use of computers as a facilitator of their activities [und] terrorism involving computer technology as a weapon or target"* (Jarvis et al. 2014, S. 28). Zum einen umfasst der Begriff Cyberterrorismus die Nutzung moderner Kommunikations- und Informationstechnik als terroristisches Hilfsmittel, um Anschläge in der realen Welt durchzuführen. Zum anderen kann der terroristische Akteur den Computer als Waffe und Angriffsvektor zugleich definieren.

In Anlehnung an die scharfe Abgrenzungsstrategie von Conway werden in diesem Beitrag ebenfalls computerisierte Systeme als Mittel und Ziel eines cyberterroristischen Aktes gewertet. Darüber hinaus gilt die klassische Definition von Waldmann, welche die politische Dimension voranstellt und Gewalt als extreme Übermittlungs- und Aufmerksamkeitsfunktion beschreibt. Zusätzlich liefert Denning einen weiteren Aspekt, denn Cyberterrorismus muss in der direkten oder indirekten Konsequenz gewaltvoll, schädlich für Leib und Leben sein und/oder enormen sachlichen Schaden verursachen. Dieser virtuelle Akt von Gewalt erzeugt allgemeine Angst und Verunsicherung. Das zwingende und einschüchternde Element dieser Handlungskette nötigt Regierung und Öffentlichkeit letztendlich zu handeln (Denning 2007, S. 2).

[6]Gorden und Ford erweitern die enge Denfinition Dennings wie folgt: *„Indeed, we believe that the true impact of her opening statement ('the convergence of terrorism and cyberspace') is realized not only when the attack is launched against computers, but when many of the other factors and abilities of the virtual world are leveraged by the terrorist in order to complete his mission, whatever that may be"* (Gordon und Ford 2003, S. 4).

Jonathan Brickely definiert Cyberterrorismus dementsprechend als *„destructive militant operations in cyberspace to create and exploit fear through violence or the threat of violence in the pursuit of political change“* (Brickley 2012, S. 6). Brickley kombiniert die Gewalt mit Angst, welche politische Veränderung bewirken soll und schafft somit einen Distinktionsrahmen, in dem sich alle Cyberaktivitäten nach cyberterroristischen Motivlagen untersuchen lassen. Komplementär stellt Conway fest, dass die Androhung von Gewalt oder die Gewalt selbst im Cyberspace nicht hinreichend erforscht bzw. gar definiert ist.

Die „virtuelle“ Gewalt und ihre Folgen sind ein verhältnismäßig neues Phänomen, das viele Fragen offen lässt. Insbesondere müssen Schwellenwerte virtueller Gewalt festgelegt werden, um Terroristen von anderen, nichtstaatliche Akteuren abzugrenzen (Conway 2014, S. 105). Conway verweist hier auf Denning, welche bereits frühzeitig die Folgen cyberterroristischer Aktionen in den Fokus der Definition genommen hat.[7]

Beispielhaft nennt Denning, das Stören oder Zerstören kritischer Infrastruktur oder sonstiger wichtiger öffentlicher Dienste, infolgedessen Menschen zu Schaden kommen. Erst dann kann von Cyberterrorismus gesprochen werden. Ein weiteres Problem offenbart sich, wenn man das Kosten-Nutzen-Kalkül klassischer Terroristen im Vergleich zu Cyberterroristen untersucht (Conway 2014, S. 103–122). Demnach wird der Terrorist immer die dramatische Kommunikationsform verwenden, die mehr Aufmerksamkeit verursacht. Low-Tech-Attacken sind besser medial wahrnehmbar und mittelbarer als ein hochkomplexer Cyberangriff auf das Stromnetz. Zwar kann ein Angriff auf die IT-Systeme der kritischen Infrastruktur gewaltige hypothetische Schadensdimensionen entwickeln, doch im Vergleich zu einem konventionellen Bombenanschlag sind die theoretisierten Vorteile nicht gegeben.

Im Zusammenhang mit dem bereits definierten Phänomen des Cyberkrieges, welcher idealtypisch und a priori staatlichen Akteuren zugeordnet wird, geht der Cyberterrorismus idealtypisch von nicht-staatlichen Akteuren aus (Denning 2007, S. 2 f.). Die Eskalationsstufe und die entsprechenden Angriffsziele sind aber äquivalent zueinander. Zusammenfassend formuliert sind Cyber-Terroristen demnach nichtstaatliche Akteure, die mittels computerisierter und digitaler Systeme u. U. kritischen Schaden verursachen, welcher, in Gewalt und Angst übersetzt, einer

[7] *„To fall in the domain of cyber-terror, a cyberattack should be sufficiently destructive or disruptive to generate fear comparable to that from physical acts of terrorism, and it must be conducted for political and social reasons.“* (Denning 2007, S. 3).

spezifischen politischen Agenda dient. Die Motivlage von Cyber-Terroristen entspricht ihrem analogen Pendant, denn sie nutzen bewusst virtuelle Gewalt als Kommunikationsmittel.

3 Vom Spannungsfeld zwischen Wahrheit und Demokratie

Gemäß der bisherigen Definition sind terroristische Anschläge kein Selbstzweck, sondern dienen als virtuelle Gewalt der Kommunikation. Sie sollen schockieren und damit das Vertrauen in die staatliche Ordnung untergraben. Wie jedoch können Terroristen Angst und Schrecken im und mittels des Cyberspace verbreiten?

Zur Erhellung dieser Frage soll zuerst auf den Aspekt der Kommunikation eingegangen werden. Terroristen sähen Unsicherheit und Angst nicht nur, indem die Angegriffenen konkret um ihre Gesundheit und ihr Leben fürchten. Der Schockeffekt der terroristischen Gewalttat entsteht vielmehr dadurch, dass in westlichen Gesellschaften in den letzten Jahrzehnten eine „Entwöhnung" von Gewalt stattgefunden hat (Pinker 2011), aufgrund derer die unerwartete „Rückkehr" der Gewalt ins alltägliche Leben so schockierend und beängstigend erscheint (Waldmann 2011, S. 46). Das eigentliche Angriffsziel der terroristischen Tat ist damit letztlich selbst auch wieder ein Akt der Kommunikation: das Konstrukt des Gesellschaftsvertrages, demzufolge der moderne Staat vor allem zum Schutze von *„life, liberty and property"* (Locke) geschaffen wurde und dessen Legitimität an seiner Fähigkeit hängt, dies auch garantieren zu können. Max Weber spricht in diesem Kontext von einem Staat, der sich durch sein *„Monopol legitimer physischer Gewaltsamkeit"* (Weber 2011, S. 7) auszeichnet. Damit kann freilich nicht gemeint sein, dass bereits einzelne Verletzungen dieser staatlichen Schutzpflicht das Vertrauen der Bürger untergraben – Terrorismus verfängt aber gerade aufgrund des medial vermittelten Schockeffekts sowie der bewussten politischen Botschaft, was ihn von anderen Gewalttaten wesentlich unterscheidet.

Das Narrativ des staatlichen Gesellschaftsvertrages kann jedoch auch an anderer Stelle untergraben werden, um den gleichen Effekt zu erzielen wie durch physische Gewaltanwendung. Die Weiterentwicklung der Demokratie innerhalb der politischen Philosophie erweitert bekanntlich die Rolle des Staates weit über das bloße Schützen von *„life, liberty and property"* (Locke) hinaus, indem sie – ausgehend von Spinozas *Tractatus Theologico-Politicus* (Enghofer 2017) – der Kommunikation der Bürger untereinander eine zentrale Rolle bei der Wahrung staatlicher Stabilität und Legitimität zuspricht.

Dabei gewinnt der Begriff der Wahrheit eine zentrale Rolle: Kommunikation dient dazu, so die philosophische Konsenstheorie (Gloy 2004, S. 203), im interpersonellen Austausch Wahrheit zu finden, was sie fundamental von der Korrespondenztheorie, aber auch Kohärenztheorien, unterscheidet. Politisch schlägt sich diese kommunikative Epistemologie in demokratietheoretischen Konzepten wie der deliberativen Demokratie nieder. Diese auf Jürgen Habermas zurückgehende Vorstellung stellt nicht nur den sog. „herrschaftsfreien Diskurs" ins Zentrum der Demokratie, sondern erweitert ihn in ihrer starken Form (Kelly 2012, S. 44–58) auch um eine epistemische Komponente. Ein herrschaftsfreier Diskurs, so das Argument, führt nicht nur zu allgemein zustimmungsfähigen politischen Entscheidungen, sondern überträgt diesen auch in eine epistemische Korrektheit: das bessere Argument setzt sich im idealen Diskurs nicht nur durch, sondern führt letztlich auch zum „besten", also „objektiv richtigen" Argument, gegen das keine weiteren Einwände mehr möglich sind (Habermas 1984, S. 104, 1986, S. 352).

Ausgehend von dieser Prämisse kann der Gesellschaftsvertrag deliberativer Demokratien somit essenziell verletzt werden, indem der diskursive Prozess zwischen den Bürgern gestört oder gar verunmöglicht wird. Die Voraussetzungen des Ideals eines herrschaftsfreien Diskurses liegen bekanntlich in einer möglichst starken Gleichberechtigung hinsichtlich Artikulation, Zugang zum Diskurs, symmetrischer Machtsituation und der Akzeptanz des *„zwanglosen Zwang[s] des besseren Argumentes"* (Habermas 2009, S. 144). Diese Voraussetzungen der idealen Sprechsituation, die Habermas aus den teleologischen Geltungsansprüchen idealer Sprechakte – Wahrheit, Richtigkeit, Wahrhaftigkeit und Verständlichkeit – ableitet, stellen jedoch einen Zirkelschluss dar, den Habermas nicht vermeiden kann: die genannten Zielsetzungen des herrschaftsfreien Diskurses, welche *„in einem einzigen [konvergieren]: dem der Vernünftigkeit"* (Habermas 1984, S. 104), bilden zugleich auch seine Voraussetzung. Somit stellt das Ideal der deliberativen Demokratie ein autopoietisches System[8] dar, welches den rationalen und vernünftigen Diskurs samt epistemischen Wahrheitsanspruch ins Zentrum stellt.

Das Vertrauen der Bürger innerhalb dieser Demokratievorstellung hängt also essenziell an der Fähigkeit des Staates, nicht nur seine „klassischen" Aufgaben wahrzunehmen, sondern darüber hinaus auch ein kommunikatives Milieu der

[8]Der Begriff *autopoiesis* (Selbstreproduktion) entstammt der systemischen Forschung der Neurobiologen Maturana und Varela (Mingers 1991) und wird von Niklas Luhmann auf soziale Systeme übertragen.

Rationalität und Vernünftigkeit aufrecht zu erhalten. Schockeffekte lassen sich erzeugen, wenn Akteure innerhalb des Diskurses offen gegen die Regeln der Wahrheit, Richtigkeit, Wahrhaftigkeit und Verständlichkeit verstoßen und damit einen ähnlichen „provokativen Normbruch“ (Paris 1989) erzielen, wie ihn klassische Terroristen durch physische Gewalt innerhalb des lockeschen Narrativs erzeugen können.

Die Unterminierung der „vernünftigen“ Diskurskultur erfolgt, indem Debatten emotionalisiert statt versachlicht werden, wenn bewusst Falschmeldungen verbreitet, die Absichten des Senders bewusst verschleiert oder verfälscht oder letztlich epistemisch leere Aussagen, die der bloßen Provokation dienen, in Umlauf gebracht werden (s. a. Kap. „Warum automatische Verfahren bei der Detektion von Hate Speech nur die halbe Miete sind“). Innerhalb des Cyber- und Informationsraumes lassen sich nicht nur für alle diese Mechanismen Beispiele finden, sondern es zeigt sich auch die *bewusste Nutzung* dieser Mechanismen für politische Zwecke. Eine derartige Störung rationaler Diskurskultur, welche geeignet ist, „Unsicherheit und Schrecken“ zu verbreiten, ist demnach als Cyberterrorismus zu bezeichnen.

Die diskursiven Manipulationsmechanismen sind freilich nicht neu, lassen sich jedoch erst im Cyber- und Informationsraum in hinreichender Wirksamkeit bei gleichzeitig geringen Kosten realisieren. Die einfache Verbreitung von Bildern und Videos, welche bewusst einen primär emotionalen Inhalt transportieren, sog. „Memes“, fällt ebenso darunter wie das einfache Verbreiten von echt wirkenden Falschmeldungen, „Fake News“. Diese absichtsvollen Elemente der Diskursmanipulation werden ergänzt und verschärft durch technisch-psychologische Aspekte aufseiten der Plattformen und der Nutzer. So beeinflussen Filteralgorithmen beispielsweise die Informationsbasis der Nutzer auf Grundlage ihrer bisherigen Präferenzen, was zu einer zentrifugalen Fragmentierung der Informationsbasis gemeinsamer politischer Deliberation führen kann (Filterblasen-Phänomen) (Helbig 2018). Dieser technische Effekt wird ermöglicht aufgrund des psychologischen „confirmation bias“, also der menschlichen Tendenz, eher Informationen anzunehmen, welche die eigene Weltsicht bestätigen statt herausfordern (Singer und Brooking 2018, S. 125). Zusammengenommen wird hier also eklatant das Egalitätsgebot der deliberativen Demokratie untergraben.

Wie reagieren deliberative Demokratien auf solche Fundamentalangriffe auf ihre Prinzipien? Grundsätzlich lassen sich zwei – einander nicht ausschließende – Lösungen identifizieren: eine regulative sowie eine edukative Herangehensweise. Die regulative Reaktion auf Störungen des deliberativen politischen Prinzips besteht darin, Falschmeldungen, „Hassrede“ und Ähnliches soweit möglich aus dem Cyber- und Informationsraum zu löschen, zu blockieren oder anderweitig ihre Verbreitung zu verhindern oder zumindest zu minimieren. Dies passiert

beispielsweise in Deutschland im Zuge des Netzwerkdurchsetzungsgesetzes (NetzDG) und in Kooperation oder auch auf Eigeninitiative der sozialen Netzwerke wie Facebook oder Twitter. Die edukative Variante hingegen setzt auf die Rationalität der Nutzer und vertraut weiterhin auf den *„zwanglosen Zwang des besseren Arguments"* (Habermas 2009, S. 144), indem versucht wird, durch „Faktenchecker" Falschmeldungen und emotionalisierende Diskurselemente zu widerlegen. Dies erfolgt sowohl direkt von staatlicher Seite, wie bspw. in Deutschland mit dem geplanten Abwehrzentrum gegen Desinformation im Netz, als auch von privater Seite durch investigative Initiativen wie bellingcat (Singer und Brooking 2018, S. 73–77).

Beiden Ansätzen ist dabei gemein, dass sie sich als Antwort auf die zunehmende, politisch bewusst instrumentalisierte Unterminierung deliberativer Prämissen verstehen; aus unterschiedlichen, sowohl theoretischen als auch pragmatischen Erwägungen sind jedoch die bisherigen Versuche, diesem Phänomen des Cyberterrorismus zu begegnen, gescheitert.

Die edukative Lösung des Problems krankt zum einen an verfehlten psychologischen Annahmen. So zeigen verschiedene Studien (Levy 2017; Nyhan und Reifler 2010), dass der confirmation bias nicht nur eine höhere Aufnahmebereitschaft bestätigender Informationen zur Folge hat, sondern dass auch die erzwungene Konfrontation mit abweichenden Sichtweisen zu einer weiteren Selbstbestätigung führt. Der erwünschte Effekt, das Gegenüber durch den zwanglosen Zwang des besseren Arguments zu überzeugen, ist also häufig psychologisch nicht haltbar, ja kann sich sogar in sein Gegenteil verkehren (backfire-Effekt) (Levy 2017, S. 497).[9] Zum anderen operieren manipulative Elemente gegen die deliberative Demokratie und ihre Verteidiger nicht auf derselben Ebene. Wie erwähnt, besteht der Angriff auf diskursive Prämissen gerade im Verlassen der Prinzipien von Rationalität und Vernunft, um stattdessen Emotionen anzusprechen und zu politisieren (Nussbaum 2018). Ein Insistieren auf Vernunft und Ratio erscheint dann als Verteidigung geradezu anachronistisch – der Faktenchecker wird zum Don Quijote der deliberativen Demokratie, der im Kampf gegen die Windmühlen der politischen Emotionalisierung deren Natur völlig verkennt und damit zwangsläufig scheitert.[10]

[9]Zur kritischen Beurteilung des „backfire-Effekts" siehe exemplarisch Guess und Coppock (2016).

[10]Zur Unterscheidung zwischen den unterschiedlichen Entscheidungsprinzipien vergleiche (Haidt 2013; Kahneman 2012). Neuere Studien zeigen auch eine Korrelation dieser Muster mit politischen Einstellungen, dazu zusammenfassend Prell und Prell (2015, S. 195–201).

In der regulativen Vorgehensweise findet sich zudem das Problem der „wehrhaften“ oder „streitbaren“ Demokratie wieder: ein Staat, der den möglichst freien Zugang zu Informationen und zu Diskursen zu seinem Fundament erklärt, kann nur schwerlich zugleich eine Einschränkung genau dieser Freiheit vornehmen, möchte er sich nicht dem Verdacht aussetzen, seine eigenen Prinzipien nicht ernst zu nehmen – eine demokratietheoretische Auseinandersetzung, die in Bezug auf die Einschränkung von Freiheitsrechten im „analogen“ Raum hinlänglich bekannt ist und sich in der Bundesrepublik im Konzept der wehrhaften Demokratie samt ihrer Instrumentarien – von Parteien- über Propagandaverbote bis hin zum Verfassungsschutz – niederschlägt.

Dabei darf zu guter Letzt nicht vergessen werden, dass der fundamentale Streitpunkt insofern noch eine Ebene tiefer liegt, als dass die deliberative Demokratie nur eine von mehreren Demokratiemodellen darstellt. Ihre grundsätzliche Prämisse, wonach „Wahrheit“ eine konstitutive Rolle in der Demokratie erfüllt, wird von vielen, epistemisch weniger anspruchsvollen Theorien abgeschwächt oder negiert (Kelly 2012). So schreibt bspw. Hans Kelsen in seiner berühmten „Verteidigung der Demokratie“ (1932):

> „Gewiß, wenn die Frage nach dem, was sozial richtig, was das Gute, das Beste ist, in einer absoluten, objektiv gültigen, für alle unmittelbar einleuchtenden Weise beantwortet werden könnte: dann wäre die Demokratie schlechthin unmöglich. Denn was könnte es für einen Sinn haben, über eine Maßnahme, deren Richtigkeit über allem Zweifel erhaben feststeht, abstimmen und die Mehrheit entscheiden zu lassen?“ (Kelsen 2006)

Auch andere liberale Demokratietheoretiker wie Karl Popper, August von Hayek, Joseph Schumpeter oder Hannah Arendt verweisen darauf, dass Wahrheitsansprüche mit demokratischer Politik zumindest in einem problematischen Spannungsverhältnis stehen (Hidalgo 2014). Eine staatliche Lenkung der Diskurslandschaft im Interesse der deliberativen Selbsterhaltung erscheint damit als genau jenes Paradoxon, dessen Ausnutzung sich politische Extreme seit jeher bedient haben: die Parole Saint-Justes „Keine Freiheit den Feinden der Freiheit“ erklärt ihn eben selbst zu einem Feind der unbedingten Freiheit. Das Kalkül extremistischer Gruppierungen besteht darin, durch einen *„absichtlich herbeigeführte[n] Normbruch, den Anderen in einen offenen Konflikt hinein[zu]ziehen und zu einer Reaktion [zu] veranlassen, die ihn, zumal in den Augen Dritter, moralisch diskreditiert und entlarvt“* (Paris 1989). In diese Falle drohen sowohl edukative als auch regulative Reaktionen auf Diskursmanipulationen zu tappen, womit – im Sinne der Aktions-Repressions-Spirale – eine weitere Radikalisierung und Stärkung dieser Form des Terrorismus entstehen kann.

Trotz dieser Probleme bleibt klar, dass die Lösung nicht einfach im anderen Extrem einer postmodernen Beliebigkeit liegen kann, wonach letztlich alles relativ ist und Wahrheit als Maßstab völlig verabschiedet wird. Auch die resignative Losung Kelsens – *„Man muß seiner Fahne treu bleiben, auch wenn das Schiff sinkt; und kann in die Tiefe nur die Hoffnung mitnehmen, daß das Ideal der Freiheit unzerstörbar ist und daß es, je tiefer es gesunken, umso leidenschaftlicher wieder aufleben wird"* (Kelsen 2006, S. 237) – kann wohl kaum als adäquate Antwort gelten. Ein epistemischer, so Habermas, oder mindestens prozeduraler Minimalkonsens (Mouffe 2015), muss Basis der Demokratie bleiben, ohne dabei in die Falle Saint-Justes zu tappen.

Zusammenfassend ist festzustellen, dass Wahrheit und Demokratie somit in einem antinomischen, das heißt nicht letztgültig auflösbaren Spannungsverhältnis stehen: einerseits lebt die Demokratie vom politischen Streit um politische Lösungen und kennt gerade keine unumstößlichen Wahrheiten, welche nicht dem politischen Diskurs und dem Ringen um einen mehrheitsfähigen Konsens beständig ausgesetzt sind. Gleichzeitig kann dieser Verzicht auf inhaltliche Wahrheiten im Politischen nicht bedeuten, dass deswegen die Rahmenbedingungen der Demokratie, innerhalb derer um die „richtige" Lösung gerungen wird, selbst ebenfalls zur relativistischen Disposition stehen: gerade erst die Existenz eines institutionellen Rahmens, welche die Auseinandersetzung zwischen verschiedenen politischen Meinungen sicherstellt, ermöglicht politische Stabilität bei gleichzeitig beständigem diskursiven Streit um das Gemeinwohl.[11] Der Erfolg einer solchen „demokratischen Sozialtechnik" (Kelsen 2006) hängt jedoch essenziell davon ab, inwiefern sein zugrundeliegendes Menschenbild der Ambiguitätstoleranz erhalten bleibt. Wird die Bereitschaft, abweichende Meinungen auszuhalten, dabei jedoch gleichzeitig nicht einer völligen Beliebigkeit des Diskurses zu verfallen im Cyber- und Informationsraum durch die Schaffung von selbstverstärkenden Echokammern einerseits, einer informationellen Beliebigkeit andererseits zersetzt (Bauer 2018), kann sich dies auf die Funktionsweise demokratischer Institutionen ähnlich verheerend auswirken wie physische Gewaltakte.

[11] Auf die Kritik, welche bspw. an Ernst Fraenkels Konzeption des „nicht-kontroversen Sektors" als Begriff für diese Rahmenbedingungen von verschiedenster Seite vorgebracht wird, soll hier nicht näher eingegangen werden.

4 Von virtueller zur realer Gewalt

Die schier grenzenlosen Kommunikationsmöglichkeiten des Internets, manifestiert in der Sphäre des Cyber- und Informationsraumes, kommen der terroristischen Grundambition – der Verbreitung von Angst und Schrecken mit dem Ziel, das vorherrschende demokratische politische System zu destabilisieren – ideal zugute. Nicht nur die Abläufe des täglichen Lebens profitieren auf allen Ebenen von der Kommunikationsbeschleunigung des Internets, von der Informationsvielfalt und deren ständigen Verfügbarkeit, sondern auch terroristische Akteure. Diese können im Cyber- und Informationsraum zielgerichtet ihre Bestrebungen und Ideologien kommunizieren, akteursgerichtet geplant wirken und ungefiltert nahezu jedes Mitglied der Gesellschaft erreichen, wenn dieses in der neuen Sphäre partizipiert. Dieser im Grunde grenzenlose Wirkungsraum ist bisher einzigartig in der Geschichte der Menschheit. Neben seinen vielen und unbestreitbaren positiven Effekten für den Fortschritt, für die Wirtschaft und für die Kultur (Enders 2011, S. 11) lassen sich dennoch gleichermaßen negative Einflüsse von teilweise essenzieller Bedeutung ausmachen.

Die im Punkt 1. aufgestellte Hypothese, dass Cyberterrorismus existiert, jedoch – anders als sein analoges Pendant – als solcher von der breiten Öffentlichkeit nicht wahrgenommen wird, ist im Kontext dieses Paradigmas als essenzielle Bedrohung zu verstehen. Der Schlüssel hierbei ist die Transformation von virtueller zu realer Gewalt im digitalen Medium. Die bewusste Instrumentalisierung der Wirklichkeitsperzeption durch terroristische Akteure als Teil der cyberterroristischen (Kommunikations-)Strategie, schafft eine Wirkung, die sich zwar virtuell verortet entfaltet, sich jedoch in realen Konsequenzen und fühlbaren Effekten niederschlagen kann.

Die Frage nach der Wirkung von virtueller Gewalt auf ihre Konsumenten ist für die Wissenschaft keine Unbekannte und fand in der Vergangenheit v. a. große Aufmerksamkeit im Zusammenhang mit der Frage nach Gewalt in den Medien und ihr Einfluss auf z. B. jugendliche Amoktäter an Schulen (Rötzer 2003). Dieses Forschungsfeld erfreut sich bis heute einer ungebremsten Publikations- und Studienflut. Dabei haben 2006 schon die Autoren Michael Kunczik und Astrid Zipfel festgestellt, dass Schätzungen – auch wenn deren Basis oft unklar ist – von über 5000 zur Thematik durchgeführten Studien ausgehen. Dabei unterscheiden die Autoren bewusst zwischen Fachliteratur und sog. „Betroffenheitsliteratur“ (Kunczik und Zipfel 2006, S. 12), welche sich zumeist ohne ausreichenden Kenntnisstand des akademischen Diskurses und der Forschungslage aufgrund persönlicher Besorgnis und Common Sense populärwissenschaftlich sowie meist spekulativ mit der Thematik auseinandersetzen (Kunczik und Zipfel 2006).

Im Laufe der Zeit hat sich eine Vielzahl von Wirkungstheorien entwickelt, welche die Folgen von Gewaltdarstellungen auf ihre Konsumenten erklären sollen. Bemerkenswert ist hierbei, dass diese Theorien sich nicht nur in mehrere Hauptrichtungen unterteilen lassen, sondern sich teilweise fundamental widersprechen. Eine Strömung empfindet mediale Gewaltdarstellungen als schädlich für ihren Rezipienten, andere empfinden sie entweder als bedeutungslos oder sogar als gesellschaftlich hilfreich (Kunczik und Zipfel 2006). Für die Arbeit mit diesen ist es somit wichtig, nicht nur den jeweiligen ideologischen Standpunkt ihrer Autoren und Anhänger im Blick zu haben, sondern sich auch dem Fakt bewusst zu sein, dass bisher keine der aufgestellten Hypothesen als empirisch gesichert betrachtet werden kann (Frerichs o. J., S. 5).

Dennoch – und in diesem Kriterium sind sich alle Wirkungstheorien einig – hat die Darstellung von Gewalt in den Medien tatsächlich einen Effekt auf ihre Konsumenten. Unabhängig davon, ob dieser nun positiv oder negativ ist, für die Betrachtungsweise der Wirkmöglichkeiten cyberterroristischer Akteure ist allein dieser Fakt von Belang.

Überprüfen lässt sich diese These gut an dem eingangs bereits beleuchteten Vorfall, der unter dem Namen *Pizzagate* im Jahr 2016 Einzug ins kollektive Gedächtnis gefunden hat. Die mittels Hacking erbeuteten – und im Grunde ursprünglich belanglosen – Informationen aus dem E-Mail-Austausch zwischen dem Pizzeria-Besitzer James Alefantis und dem damaligen Wahlkampfmanager Hillary Clintons, John Podesta, waren im Cyber- und Informationsraum, speziell von Nutzern des Imageboards 4chan, ob bewusst oder unbewusst, fehlinterpretiert und zu einer handfesten Verschwörungstheorie konstruiert worden. Im Mittelpunkt der falschen Anschuldigungen stand die damalige Präsidentschaftskandidatin Hillary Clinton und ihr Wahlkampfmanager Podesta als die Verantwortlichen eines Kinderpornografie-Ringes, der aus dem Keller der *Comet Ping Pong Pizzeria* heraus international agiert haben soll (Spiegel 2016). Die Verschwörungstheorie wurde via Twitter, Reddit und 4chan stark verbreitet und erreichte nach Einschätzungen des Nachrichtensenders CNN blitzartig Millionen von Menschen (CNN 2016). Unabhängig von der ursprünglichen Intention der anonymen User des Bilderbrettes 4chan – bei der rückblickend betrachtet fatalen Fehlinterpretation der E-Mails und Instagram-Bilder ist vor allem die nahezu ungebremste Dynamik, mit der die Verschwörungstheorie sich im Cyber- und Informationsraum ausbreitete, bemerkenswert, sowie die Wandlungsfähigkeit der Informationen, welche in kürzester Zeit nach dem Prinzip einer Flüsterpost immer groteskere Züge annahmen (Rationalwiki 2019).

Real wurde die Gefahr für die Betroffenen der Verschwörungstheorie faktisch, als am 4. Dezember 2016 der mit einem Gewehr bewaffnete 28-jährige Edgar

Maddison Welch die Pizzeria stürmte, um in Selbstjustiz den mutmaßlichen Kinderpornografie-Ring zu zerschlagen, die angeblich festgehaltenen und missbrauchten Kinder zu retten und die Täter zur Rechenschaft zu ziehen. Nachdem er seinen Irrtum erkannt hatte, ließ sich der Angreifer widerstandslos von der Polizei festnehmen und wurde rechtskräftig verurteilt. Verletzt wurde bei Welchs Aktion niemand (CNN 2017).

Die hier stattgefundene Wirklichkeitsmanipulation der anonymen 4chan-User hat in ihrer Verbreitung und Konzipierung eine derartige Reaktion und Emotionalisierung bei manchen Rezipienten verursacht, dass in letzter Konsequenz ein im Grunde fehlgeleiteter Mann aus einem vermeintlich ehrenvollen Ziel heraus zum Täter wurde. Aus der virtuell erlebten – und zudem vollkommen fiktiven – Gewalterfahrung der missbrauchten und entführten Kinder, die von dem *„satanic pedophilia ring run by prominent members of the Democratic Party“* (Tuters und Jakubauskaitéc 2018) festgehalten wurden, hat Welch mit seiner Entscheidung, dem mit der Waffe in der Hand ein Ende zu setzen, reale Gewalt werden lassen.

Ob die Wirklichkeitsmanipulation durch die 4chan-User tatsächlich als eine cyberterroristische Aktion gewertet werden kann, lässt sich dennoch nicht kohärent argumentieren. Wäre ihre Intention bei der Fehlinterpretation der E-Mails die bewusste Diskreditierung von Clinton und Co. gewesen, die Öffentlichkeit in Anbetracht einer solch verwerflichen Tat aufzustacheln und zu manipulieren, sodass es in letzter Konsequenz zu einem realen Gewaltakt kommen sollte – wie er dann mit der Figur Welchs real eingetreten ist – so könnten die Grundannahmen terroristischer Ambitionen als erfüllt betrachtet werden. Das 4chan-Forum/pol/zeichnet sich jedoch durch eine bewusst politisch unkorrekte Haltung, gewollt schwarzen Humor und als Spielplatz zynischer Internettrolle aus. Es als ein Sammelbecken von (Cyber-)Terroristen zu verstehen, die dort gezielt demokratiegefährdende Aktionen initiieren, würde die Bedeutung des Imageboards maßlos fehlinterpretieren und dort vermutlich zu großer Erheiterung führen (Tuters und Jakubauskaitéc 2018).

Anders verhält es sich mit Kommentatoren und Multiplikatoren, die solche Wirklichkeitsmanipulationen bewusst für ihre Zwecke instrumentalisieren. Bei Pizzagate spielte beispielsweise der rechte Verschwörungstheoretiker Alex Jones mit seiner Website *InfoWars* eine wichtige Rolle bei der Verbreitung der Falschmeldung. Zwar entschuldigte er sich im März 2017 für deren Unterstützung und Verbreitung, der reale Schaden war jedoch schon angerichtet (NYTimes 2017). Seine genauen Motive für die Unterstützung nennt Jones nicht. Es liegt jedoch auf der Hand, dass diese in ihrer Konzipierung ideal in sein Weltbild und seine politische Orientierung passte. Mit diesen Formen der Wirklichkeitsmanipulationen bzw. mit der bewussten Instrumentalisierung von Falschmeldungen verfolgen Demagogen wie Jones genau das Ziel der

Schädigung des vorhandenen politischen Systems und der öffentlichen Ordnung. Es ist anzunehmen, dass Jones sich der Wirkung und des Effektes einer Meldung wie Pizzagate vollkommen bewusst ist.

Politische Extremisten streben mit ihrer Arbeit gesellschaftliche Veränderungen an. Eine Eskalation, bei der auf Worte tatsächlich physische Gewaltakte folgen, sind dabei eine Grenze, die im Grunde auch Alex Jones nicht überschreiten will.

Der klassische Terrorismus verwendete physische Gewalt, um Unsicherheit und Angst zu verbreiten. Er zielt also auf die Psyche der Bevölkerung ab. Demgegenüber zeigt der Fall Pizzagate, dass Cyberterrorismus umgekehrt wirken kann: das Verbreiten von Schrecken erfolgt primär durch psychische Manipulation im Cyber- und Informationsraum mittels Wirklichkeitsmanipulation. Physische Gewaltakte können dadurch initiiert werden, womit sich die Wirkungskette des klassischen Terrorismus umdreht.

5 Conclusio

Der Cyber- und Informationsraum wird als kriminologisch relevante Sphäre zunehmend bedeutender. Die bisher gängigen Auffassungen, dass Cyberterrorismus aufgrund des Fehlens von physischer Gewalt nicht existieren könne, werden durch die Analyse des Überganges von virtueller Gewalt hin zu realer Gewalt widerlegt. Cyberterrorismus existiert und findet statt. Der Schlüssel für die Nachvollziehbarkeit ist der Umgang mit dem Wirkmittel der Wirklichkeitsmanipulation. Wird dieses im Cyber- und Informationsraum gezielt eingesetzt, um mittels Emotionalisierung der Rezipienten zum einen Angst und Schrecken zu verursachen, zum anderen, durch das Schaffen faktischer Realitäten, zu realen Handlungen anzuspornen, die u. U. in ihrer letzten Konsequenz tatsächlich physische Gewaltakte zur Folge haben können, so können die Ambitionen terroristischer Zielsetzungen als erfüllt betrachtet werden.

Basis für die Nachvollziehbarkeit dieser Argumentation ist das Verständnis von Demokratien als im Grunde antinomische Staatsformen, die sich durch ihre Ambivalenzfähigkeit auszeichnen. Idealtypisch existieren in einer funktionierenden Demokratie keine unumstößlichen politischen Wahrheiten. Vielmehr leben Demokratien von der Fähigkeit zur Ambiguitätstoleranz und vom Erhalt eines Rahmens zum Austausch widersprüchlicher Vorstellungen des Politischen. Die gezielte Manipulation der öffentlichen Meinung durch Schaffung z. B. sog. alternativer Fakten, insbesondere im Cyber- und Informationsraum, führt zu einer Krise dieser Ambiguitätstoleranz.

Die schier grenzenlosen Kommunikationsmöglichkeiten der Cyber- und Informationssphäre kommen terroristischen Grundambitionen ideal zugute. Anders als bisher in der Forschung angenommen, bedarf es für die Manipulation der Wirklichkeitswahrnehmung kaum nennenswerter Ressourcen. Durch die Möglichkeit des direkten Wirkens auf Rezipienten und durch die Eigendynamiken von Kommunikationswegen im Cyberspace, die, ganz im Sinne des Prinzips einer Flüsterpost, zur Dramaturgie von geschaffenen Fakten das Ihrige beitragen, kann ein kleiner Funken in der Diskussion auf einem Imageboard und ein geschickt verbreitetes Gerücht, gestreut auf verschiedenen Plattformen, ausreichen, um Millionen von Rezipienten zu emotionalisieren und nachhaltig zu beeinflussen. Wird in der Folge der Entwicklung die Schwelle von virtueller Gewalt zu realer Gewalt überschritten, ist die Sphäre des Cyber- und Informationsraumes überwunden und die terroristische Ambition in der Realität angekommen.

6 Einordnung und Ausblick

Der #Pizzagate verbreitete sich auf dem Kurznachrichtendienst Twitter bis in die höchsten Ränge des Wahlkampfteams von Präsidentschaftskandidat Donald Trump. So twitterte Michael G. Flynn Jr. – Sohn des designierten Sicherheitsberaters Michael T. Flynn – am 5. Dezember 2016 unter dem Hashtag Pizzagate und befeuerte damit selbst einen Tag nach Welchs Angriff auf die Pizzeria die Verschwörungstheorie.

Die Ereignisse zeigen dabei exemplarisch, dass viele Kommunikationskanäle im Cyber- und Informationsraum gerade nicht dazu angetan sind, das anthropologische Ideal des *homo democraticus* zu fördern: statt eines *„Typus des relativ herabgesetzten Ich-Gefühls, […] des sympathisierenden, friedliebenden, nicht-aggressiven Menschen“* (Kelsen 2006, S. 239) wird eher der *„Typus des gesteigerten Ich-Bewusstseins“* (Kelsen 2006, S. 240) gefördert, dessen nach außen gerichtetes Aggressions- und Sendungsbewusstsein dem demokratischen Ideal abträglich erscheint.

Die Phänomene im Cyber- und Informationsraum, welche sich dergestalt negativ auf die psychologischen Voraussetzungen der Demokratie auswirken, führen jedoch, wie an #Pizzagate ersichtlich wird, nur mittelbar zu physischer Gewalt. Dementsprechend erscheint eine Bekämpfung der Probleme auf physischer Ebene als bloße Symptombekämpfung, welche die Wurzeln nicht anzugehen vermag. Wie gezeigt wurde, ist jedoch auch eine Bekämpfung der Perzeptionsmanipulation problematisch. Aus diesem Grund kann der demokratische

Staat lediglich versuchen, die Immunität der Bürger gegen manipulative Phänomene, welche die Fähigkeit zur Ambiguitätstoleranz untergraben, zu erhöhen.

Immunisierung heißt dabei, Bürger im Geiste des kritischen Rationalismus zu fördern, also eine Fähigkeit zum kritischen Denken zu fördern, welche Individuen sensibel macht für vermeintlich eindeutige Weltsichten und ihnen zu einer kritischen Haltung im Sinne Karl Poppers verhilft, wonach immer die Möglichkeit besteht, der andere könne Recht haben (Popper 2011). Diese Einsicht darf jedoch zugleich nicht dazu führen, Kritik zum Selbstzweck verkommen zu lassen, und unter dem Deckmantel einer „kritischen Haltung" letztlich jegliche Faktizität anzuzweifeln und damit erst anfällig zu werden für vermeintlich eindeutige Ideologien.

Die Möglichkeit von Cyberterrorismus besteht nun genau im Ausnutzen dieser beiden Extreme von Eindeutigkeit und Beliebigkeit; so definiert beispielsweise das Cybercrime Convention Komitee der EU Cybergewalt als

> „the use of computer systems to cause, facilitate, or threaten violence against individuals that results in, or is likely to result in, physical, sexual, psychological or economic harm or suffering and may include the exploitation of the individual's circumstances, characteristics or vulnerabilities" (Cybercrime Convention Committee 2017, S. 5).

Gerade diese psychologische Komponente, inwiefern die psychischen Voraussetzungen der Demokratie durch virtuell vermittelte Perzeptionsmanipulationen und dadurch ausgelöste Gewalt zerstört werden, ist jedoch in den bisherigen Lösungsansätzen nicht hinreichend berücksichtigt. Dementsprechend verbleibt bei der Frage der Prävention gegen solche Formen des Cyberterrorismus zuerst die Einsicht, dass die Wirkung mit der Responsivität der Bevölkerung zusammenhängt: je schwächer die Kultur der Ambiguitätstoleranz ausgeprägt ist, desto eher können Phänomene wie #Pizzagate sich entfalten und zur Eskalation, ganz im Sinne klassischer Terrorismustheorien, beitragen.

Literatur

Arquilla, J., & Ronfeldt, D. (1993). „Cyberwar is coming!". *Comparative Strategy, 12*(2), 141–165. https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf.

Arquilla, J., & Ronfeldt, D. (1998). Der Cyberkrieg kommt! In C. Schöpf & G. Stocker (Hrsg.), *Information.Macht.Krieg* (S. 24–56). Wien: Springer.

Bauer, T. (2018). *Die Vereindeutigung der Welt: über den Verlust an Mehrdeutigkeit und Vielfalt* (3., erneut durchgesehene Aufl.). Ditzingen: Reclam.

BKA. (2016). Hacktivisten. Abschlussbericht. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/Forschungsergebnisse/2016HacktivistenqAbschlussbericht.html.

Brickey, J. (2012). Defining cyberterrorism. Capturing a broad range of activities in cyberspace. *CTC Sentinel, 5*(8). https://ctc.usma.edu/app/uploads/2012/08/CTCSentinel-Vol5Iss81.pdf.

Clausewitz, C. (2010). Vom Kriege. https://static.clausewitz-gesellschaft.de/wp-content/uploads/2014/12/VomKriege-a4.pdf.

CNN (2016). Fake news, real violence: „Pizzagate“ and the consequences of an Internet echo chamber. CNNMoney. https://money.cnn.com/2016/12/05/media/fake-news-real-violence-pizzagate/index.html.

CNN (2017). „Pizzagate“ shooter sentenced to 4 years in prison. CNN. https://www.cnn.com/2017/06/22/politics/pizzagate-sentencing/index.html.

Conway, M. (2014). Reality check: Assessing the (un)likelihood of cyberterrorism. In T. M. Chen, L. Jarvis, & S. Macdonald (Hrsg.), *Cyberterrorism* (S. 103–122). New York: Springer.

Denning, D. E. (2000). Cyberterrorism. Testimony before the special oversight panel on terrorism. https://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf.

Denning, D. E. (2007). A view of cyberterrorism five years later. https://pdfs.semanticscholar.org/86c6/5470e204b8b93685e3accc77976cc3e3f0f5.pdf.

Enders, T. (2011). Vorwort. In A. Schönbohm (Hrsg.), *Deutschlands Sicherheit. Cybercrime und Cyberwar* (S. 11–12). Münster: MV-Verlag.

Enghofer, S. (2017). Baruch de Spinoza, der theologischpolitische Komplex im Judentum und das Problem des freiheitlichen Staates. In O. Hidalgo & C. Polke (Hrsg.), *Staat und religion* (S. 159–174). Wiesbaden: Springer VS.

Frerichs, S. (o. J.). Grundlagen der Gewaltwirkungsforschung – wie wirkt Brutalität in Fernsehnachrichten und -filmen? Wirkungen von Gewaltdarstellungen im Fernsehen (unveröffentlichte Aufsatzsammlung). https://www.stefre.de/html/gewaltwirkungsforschung.html.

Gaycken, S. (Hrsg.). (2011). *Cyberwar. Das Internet als Kriegsschauplatz*. München: Open Source Press.

Gloy, K. (2004). *Wahrheitstheorien: eine Einführung*. Tübingen: A. Francke.

Gordon, S., & Ford, R. (2003). Cyberterrorism? Symantec security response. https://www.symantec.com/avcenter/reference/cyberterrorism.pdf.

Guess, A., & Coppock, A. (2016). The exception, not the rule? The rarely polarizing effect of challenging information. https://pdfs.semanticscholar.org/d53a/59ce58efed9bb67b3cbd23b5ae8a3b2b70ba.pdf.

Habermas, J. (1984). *Vorstudien und Ergänzungen zur Theorie des kommunikativen Handelns*. Frankfurt a. M.: Suhrkamp.

Habermas, J. (1986). Entgegnung. In A. Honneth & H. Joas (Hrsg.), *Kommunikatives Handeln. Beiträge zu Jürgen Habermas‘ „Theorie des kommunikativen Handelns“* (S. 327–405). Frankfurt a. M.: Suhrkamp.

Habermas, J. (2009). *Philosophische Texte. Bd. 1: Sprachtheoretische Grundlegung der Soziologie*. Frankfurt a. M.: Suhrkamp.

Haidt, J. (2013). *The righteous mind: Why good people are divided by politics and religion*. London: Penguin Books.

Helbig, K. (2018). Der Einfluss von Algorithmen auf demokratische Deliberation. In R. Mohabbat-Kar, B. E. P. Thapa, & P. Parycek (Hrsg.), *(Un)berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft* (S. 339–363). Berlin: Kompetenzzentrum Öffentliche IT.

Hidalgo, O. (2014). *Die Antinomien der Demokratie*. Frankfurt a. M.: Campus.

Jarvis, L., Nouri, L., & Whiting, A. (2014). Understanding, locating and constructing cyberterrorism. In T. M. Chen, L. Jarvis, & S. Macdonald (Hrsg.), *Cyberterrorism* (S. 25–42). New York: Springer.

Kahneman, D. (2012). *Thinking, fast and slow*. London: Penguin Books.

Kelly, J. T. (2012). *Framing democracy: A behavioral approach to democratic theory*. Princeton: Princeton University Press.

Kelsen, H. (2006). *Verteidigung der Demokratie: Abhandlungen zur Demokratietheorie* (M. Jestaedt & O. Lepsius, Hrsg.). Tübingen: Mohr Siebeck.

Kunczik, M., & Zipfel, A. (2006). Vorwort. In M. Kunczik & A. Zipfel (Hrsg.), *Gewalt und Medien. Ein Studienhandbuch* (S. 11–12). Köln: Böhlau.

Levy, N. (2017). Nudges in a post-truth world. *Journal of Medical Ethics, 43*(8), 495–500.

Lopez, G. (2016). Pizzagate, the fake news conspiracy theory that led a gunman to DC's Comet Ping Pong, explained. https://www.vox.com/policy-and-politics/2016/12/5/13842258/pizzagate-comet-ping-pong-fake-news.

Mingers, J. (1991). The cognitive theories of Maturana and Varela. *Systems Practice, 4*(4), 319–338.

Mouffe, C. (2015). *Über das Politische: wider die kosmopolitische Illusion*. Frankfurt a. M.: Suhrkamp.

Münkler, H. (2015). *Kriegssplitter. Die Evolution der Gewalt im 20. und 21. Jahrhundert*. Berlin: Rowohlt.

Nussbaum, M. C. (2018). *The monarchy of fear: A philosopher looks at our political crisis* (Fir. Simon & Schuster hardcover Aufl.). New York: Simon & Schuster.

Nyhan, B., & Reifler, J. (2010). When corrections fail: The persistence of political misperceptions. *Political Behavior, 32*(2), 303–330.

NYTimes (2017). Alex Jones Apologizes for Promoting ‚Pizzagate' Hoax. The New York Times. https://www.nytimes.com/2017/03/25/business/alex-jones-pizzagate-apology-comet-ping-pong.html. Zugegriffen: 21. Jan. 2020.

Paris, R. (1989). Der kurze Atem der Provokation. *Kölner Zeitschrift für Soziologie und Sozialpsychologie, 41,* 33–52.

Pinker, S. (2011). *Gewalt: eine neue Geschichte der Menschheit* (S. Vogel, Übers.). Frankfurt a. M.: Fischer.

Popper, K. (2011). *The Open Society and Its Enemies*. Oxon: Routledge.

Prell, D., & Prell, T. (2015). Neuropolitics: Möglichkeiten und Grenzen bildgebender Verfahren für die Analyse der politischen Einstellungen und des Wahlverhaltens. In T. Faas, C. Frank, & H. Schoen (Hrsg.), *Politische Psychologie* (S. 196–221). Baden-Baden: Nomos.

Rationalwiki. (2019). Pizzagate. https://rationalwiki.org/wiki/Pizzagate.

Rid, T. (2018). *Mythos Cyberwar. Über digitale Spionage, Sabotage und andere Gefahren*. Hamburg.

Rötzer, F. (Hrsg.). (2003). *Virtuelle Welten – reale Gewalt*. Hannover: Heinz Heise.

Singer, P. W., & Brooking, E. T. (2018). *Likewar: the weaponization of social media*. Boston: Houghton Mifflin Harcourt, an Eamon Dolan Book.

SPIEGEL (2016). Washington: Bewaffneter Mann stürmt Pizzeria um Hillary-Clinton-Gerücht nachzugehen – DER SPIEGEL – Panorama. https://www.spiegel.de/panorama/justiz/washington-mann-stuermt-mit-waffe-wegen-pizzagate-eine-pizzeria-a-1124399.html. Zugegriffen: 21. Jan. 2020.

The Cybercrime Convention Committee (T-CY), T-CY. (2017). Mapping study on cyberviolence, counsil of Europe. https://rm.coe.int/t-cy-2017-10-cbg-study-provisional/16808c4914.

Tuters, M., & Jakubauskaité, B. D. (2018) Post-Truth Protest: How 4chan Cooked Up the Pizzagate Bullshit. *M/C Journal.* http://journal.media-culture.org.au/index.php/mcjournal/article/view/1422.

Waldmann, P. (2011). *Terrorismus. Provokation der Macht*. Hamburg: Murmann.

Weber, M. (2011). *Politik als Beruf*. Köln: Anaconda.

Liebesschwindel im Cyberspace

Aktuelle Forschungsergebnisse zum Phänomen des Romance Scam im Überblick

Christian Thiel

1 Einführung

„Wenn sich der Traummann als Betrüger entpuppt“[1], *„Im Netz des falschen Traumprinzen“*[2] oder *„Wenn Sehnsucht blind macht“*[3] – mit diesen Schlagzeilen berichteten Zeitungen über den Fall einer verwitweten Rentnerin, die im Internet einen angeblichen US-Soldaten kennengelernt und ihm – ohne ihn jemals gesehen zu haben – ihr gesamtes Erspartes überwiesen hat. Sie hatte bereits einen Kredit von mehr als 40.000 EUR beantragt, als ein Mitarbeiter der Bank misstrauisch wurde und die Polizei einschaltete. Diese eröffnete der Frau, dass sie Opfer eines „Romantikbetrugs“ geworden ist.

Dieser in der medialen Darstellung unglaublich erscheinende Betrug ist kein Einzelfall. Allein das Landeskriminalamt Baden-Württemberg hat innerhalb des Jahres 2017 ganze 131 solcher Fälle erfasst.[4] Die Dunkelziffer ist vermutlich um ein Vielfaches höher, denn schließlich lohnt sich diese Betrugsmasche: Die Summen, um die Romantikbetrüger ihre Opfer schädigen, sind häufig exorbitant hoch – der Schaden kann in die Hunderttausende gehen.

[1] Berliner Kurier, 27. November 2017, S. 38.

[2] Frankfurter Rundschau, 27. November 2017, S. 34.

[3] Frankfurter Presse, 27. November 2017, Echo Vermischtes, S. 1.

[4] Frankfurter Rundschau, 27. November 2017, S. 34.

C. Thiel (✉)
Universtität Augsburg, Augsburg, Deutschland
E-Mail: christian.thiel@phil.uni-augsburg.de

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

T.-G. Rüdiger und P. S. Bayerl (Hrsg.), *Cyberkriminologie,*
https://doi.org/10.1007/978-3-658-28507-4_10

Der Romantikbetrug ist grundsätzlich ein recht neues Phänomen der Internetkriminalität, weswegen nur wenige Erkenntnisse hierzu vorliegen. Ziel dieses Beitrags ist es, einen systematischen Überblick der bisherigen Forschungsergebnisse zum Romantikbetrug zusammenzustellen. Auf Grundlage der internationalen Literatur aus Kriminologie, Psychologie und Soziologie wird das Phänomen zunächst dargestellt und verortet (Abschn. 2) und dann der typische Verlauf nachgezeichnet (Abschn. 3). Es folgen Erkenntnisse über die Täter (Abschn. 4) und die Geschädigten (Abschn. 5). Abschließend werden diverse Erklärungsansätze hinsichtlich der Wirkungsweise dieser Betrugsart vorgestellt (Abschn. 6).

2 Das Phänomen Romantikbetrug

2.1 Hintergrund: Dating und Täuschung in der virtuellen Welt

Der Romantikbetrug – obgleich keineswegs eine „Erfindung“ des Internetzeitalters (vgl. Abschn. 4) – muss vor dem Hintergrund der durch das Internet angestoßenen gesellschaftlichen Veränderungen betrachtet werden. Einer der Bereiche des alltäglichen Lebens, den das Internet fundamental verändert, ist der der Liebe und Sexualität (Kaufmann 2011). So ist beispielsweise das seit einigen Jahren boomende „Online-Dating“ mittlerweile zu einer gesellschaftlich breit akzeptierten Form der Kontaktanbahnung intimer Beziehungen geworden (Aretz et al. 2017). Dabei ist ein äußerst lukrativer Markt mit hohen Teilnehmer- und Umsatzzahlen entstanden, der jedoch auch Gefahren birgt. Zu diesen gehören neben unseriösen Geschäftspraktiken (Abofallen, etc.) und Datenschutzproblemen auch Manipulationen und *Täuschungen* diverser Akteure – von bezahlten Animateuren (sog. IKM-Schreibern[5]) über Trolle und Stalker bis hin zu „malware writers and scammers“ (Arora und Scheiber 2017, S. 414).

[5]Der Begriff „Internet-Kontaktmarkt“-Schreiber bezeichnet Personen, die gegen Bezahlung virtuelle Identitäten im Internet (v. a. auf Singlebörsen und Social Media) einnehmen. Dies dient dazu, andere Teilnehmer zu einer fortgesetzten Teilnahme am Portal oder zu Inanspruchnahme kostenpflichtiger Dienste zu motivieren und ihnen teilweise auch unlautere oder betrügerische Angebote zu unterbreiten.

Grundsätzlich ist Täuschung ein allgegenwärtiges Element in der Online-Welt. Vor allem bei der Selbstdarstellung im Bereich der virtuellen Partnersuche wird getrickst und geschummelt. So werden etwa Angaben (etwa zu Gewicht, Größe, Verdienst etc.) geschönt oder Bilder durch allerlei Kniffe „optimiert". Allerdings gibt es hierbei – im Normalfall – ein mäßigendes Korrektiv, und zwar die Antizipation eines Face-to-Face-Treffens (Toma 2017, S. 425). Das Online-Dating spaltet nämlich die Begegnung in zwei Phasen – das initiale Kennenlernen online und das anschließende Treffen im „richtigen" Leben. Zwischen diesen beiden Phasen gibt es einen „Brucheffekt" (Kaufmann 2011, S. 17), denn das erste reale Treffen ist keine bloße Fortsetzung des Onlinekontakts. Die sich treffenden Individuen sind in verschiedener Hinsicht „anders", als sie im Netz waren – schon weil sie jetzt physisch in Erscheinung treten. Wenn dabei die reale Erscheinung zu sehr von der Online-Inszenierung abweicht, sprich hemmungslos getäuscht wurde, gilt dies als „relational deal-breaker" (Toma 2017, S. 425). Die Täuschungen in der virtuellen Selbstpräsentation müssen also in einem „konventionell akzeptablen Maß" (Zillmann et al. 2011, S. 312) bleiben, da eine zu große „Ent-Täuschung" beim ersten realen Treffen die Chance auf eine Beziehung deutlich verringern würde. Die meisten Menschen gehen also beim Online-Dating davon aus, dass die Selbstdarstellungen ihres Gegenübers wahrscheinlich geschönt, jedoch nicht komplett erfunden sind. Gleichzeitig versuchen sie beständig, die Vertrauenswürdigkeit des anderen über dessen Kommunikationsverhalten einzuschätzen. Dies gibt ihnen eine gewisse Sicherheit, die allerdings – wie Studien zeigen – eine trügerische ist. Denn *„people tend to rely on the wrong cues"* (Toma 2017, S. 426). Sie achten primär auf Signale, die entweder gar nichts über die tatsächliche Vertrauenswürdigkeit aussagen oder leicht in betrügerischer Absicht kopiert werden können. Kurz zusammengefasst: Viele Menschen gehen in der virtuellen Welt davon aus, dass Täuschungen *erstens* meist auf ein geringes Maß beschränkt bleiben und *zweitens* relativ sicher von ihnen erkannt werden können. Diese Überzeugungen erweisen sich beim Romantikbetrug, aber auch bei vielen anderen Delikten aus dem Bereich der Internetkriminalität, als gefährlicher Trugschluss.

2.2 Definition und Prävalenz des Romantikbetrugs

Der Romantikbetrug (im Folgenden als „IRS“ abgekürzt[6]) kann definiert werden als eine Betrugsform, bei der Kriminelle mittels falscher Identitäten (Profile) und über onlinebasierte Kommunikation (Dating-Seiten, Messenger, Soziale Medien, etc.) strategisch ein Vertrauensverhältnis zu einem Opfer anbahnen, dabei eine romantische Beziehung vortäuschen und das Opfer derart in emotionale Abhängigkeit verstricken, dass es dem Täter für vorgebliche Gründe teils hohe Geldsummen zukommen lässt.

Der IRS beinhaltet Elemente mehrerer teils alter Betrugspraktiken (Heiratsschwindel, Identitätsdiebstahl, Massenmarketing-Betrug), die neu kombiniert wurden und sich zudem die Eigenheiten des Internetzeitalters zunutze machen (Buchanan und Whitty 2014, S. 262; Marx und Rüdiger 2017, S. 211; Whitty 2013, S. 667). Es handelt sich dabei allerdings keineswegs um eine simple Masche, die nur bei naiven und gefühlsduseligen Personen Wirkung zeigt, sondern um einen *„advanced, sophisticated and therefore very dangerous type of scam“* (Kopp et al. 2016, S. 148).

Nicht selten wird der IRS in der medialen Berichterstattung aufgrund angenommener Wesensverwandtschaft (das „Ausnutzen von Liebe“) oder ähnlicher Modi Operandi gemeinsam mit weiteren Delikten abgehandelt. Dabei drohen jedoch charakteristische Merkmale – das typische Vorgehen, die charakteristischen Opfer- und Tätergruppen, usw. – aus dem Blick zu geraten. Vom IRS abzugrenzende Delikte sind *im Internet* etwa „Sextortion“ (eine Erpressungsmethode mit kompromittierendem Bildmaterial), „Cybergrooming“ (eine Art des onlinebasierten sexuellen Missbrauchs von Kindern; vgl. Rüdiger 2012; s. a. Kap. „Grooming-Umgebungen von pädophilen und hebephilen Männern in Deutschland“) oder „Realfakes“/„Catfishing“ (eine komplexe Identitätstäuschung mit dem Ziel der emotional-psychischen Manipulation der Betroffenen; vgl. Schwartz 2015); *in der Realwelt* gibt es (immer noch) den „klassischen Heiratsschwindel“, auch in einer modernisierten, globalisierten Form als „Bezness“ bekannt (junge Liebesbetrüger vorwiegend aus den Maghreb-Ländern gehen zum Zwecke der finanziellen Ausbeutung Beziehungen/Ehen mit westlichen Touristinnen ein).

[6]Der Romantikbetrug firmiert unter einer ganzen Reihe an Begrifflichkeiten: Romance Scam (bzw. Scamming), Love Scam, Sweetheart Scam, Online Dating Scam, Liebesbetrug oder Online-Heiratsschwindel. Inzwischen ist auch in der deutschen Kriminalistik die englische Bezeichnung „Romance Scam“ üblich. Das Akronym „IRS“ (für: Internet Romance Scam) soll die Wiederholung unschöner Anglizismen vermeiden und grenzt die Deliktform deutlicher von realweltlichen Heiratsschwindeleien und Romantikbetrügereien ab.

Leider existieren zum Delikt „IRS“ bisher kaum belastbare Zahlen. In Deutschland wird diese Betrugsform nicht separat in der Polizeilichen Kriminalstatistik (PKS) aufgeführt, sondern wie viele andere Betrugsdelikte unter der Sammelkategorie „sonstige weitere Betrugsarten“ (518900) subsumiert. In anderen Ländern gibt es zumindest einige Statistiken. In den *USA* rangiert der IRS laut „Internet Crime Complaint Center“ (IC3)[7] seit 2016 unter den Top 3 (nach Schadenshöhe) der zur Anzeige gebrachten Internetverbrechen. 2017 haben sich in den USA über 15.000 Betroffene gemeldet, von denen 57 % einen Vermögensschaden erlitten haben. Dieser summierte sich auf über 211 Mio. US$. In *Australien* erreichten die Regierungsorganisation „Scamwatch“[8] im Jahr 2017 über 3000 Meldungen, davon 23,5 % vollendete Taten mit einem Gesamtschaden von über 20 Mio. AU$. Auch in *England*[9] zählt der IRS zu den häufigsten Betrugsarten (Action Fraud listet ihn unter den „Top 8 Scams“ für 2018[10]). Hier wurden im Jahr 2016 3889 Opfer um insgesamt £39 Mio. betrogen.[11] Der Royal Canadian Mounted Police in *Kanada* wurden im Jahr 2016 1142 Fälle von IRS angezeigt, davon 770 vollendete Taten mit einem Gesamtschaden von mehr als 18 Mio. CAD.[12] Alles in allem lassen sich aufgrund der mangelhaften Datenlage, die durch die dem IRS immanente enorme Dunkelziffer (vgl. Füllgrabe 2015) zusätzlich verzerrt wird, keine belastbaren Aussagen zu regionaler Häufigkeit/Verbreitung, Viktimisierungsquoten, Prävalenzraten, usw. treffen. Mit einiger Vorsicht lässt sich jedoch Folgendes ableiten: Es scheint, dass der IRS ein relativ neues

[7]Das IC3 ist eine 2001 gegründete Arbeitsgruppe des Federal Bureau of Investigation (FBI), des National White Collar Crime Center (NW3C) und des Bureau of Justice Assistance (BJA). Es bietet Opfern von Cyberkriminalität die Möglichkeit, unkompliziert Delikte zu melden. Die „Annual Reports“ finden sich unter https://www.ic3.gov/media/annualreports.aspx [28.03.2018].

[8]Scamwatch wird betrieben von der Regierungsbehörde „Australian Competition and Consumer Commission (ACCC)“. Statistiken finden sich unter https://www.scamwatch.gov.au/about-scamwatch/scam-statistics [28.03.2018].

[9]Das „National Fraud Intelligence Bureau (NFIB)“ ist eine an die Metropolitan Police London angegliederte Polizeidienststelle, die Informationen zu Betrug und finanziell motivierter Cyberkriminalität sammelt und auswertet. Die von ihr betriebene Einrichtung „Action Fraud“ (https://www.actionfraud.police.uk) dient als Meldestelle für Betrugsopfer und als Informationsschnittstelle für die Öffentlichkeit.

[10]https://www.actionfraud.police.uk/news/the-top-8-frauds-to-watch-out-for-in-2018 [28.03.2018].

[11]http://www.bbc.com/news/uk-38678089 [28.03.2018].

[12]http://www.rcmp.gc.ca/en/gazette/romance-scams?fe [28.03.2018].

Phänomen ist, das erstmals um 2007 herum in den Blick der Strafverfolgungsbehörden rückte (Whitty und Buchanan 2012). Die Fallzahlen und damit auch die Schadenssummen sind seither kontinuierlich, teilweise sogar drastisch gestiegen. Insgesamt ist von relativ hohen Geschädigtenzahlen und großen Schadenssummen auszugehen.

3 Typischer Verlauf des Romantikbetrugs

Der IRS folgt in der Praxis häufig einem sehr schematischen Ablauf. Verschiedene Studien haben diese Ablaufmuster herausgearbeitet und in unterschiedliche Phasen unterteilt (etwa Marx und Rüdiger 2017, S. 213; Whitty 2013, S. 677–679). Der vorliegende Beitrag schlägt ein etwas abgewandeltes Modell vor, bei dem folgende Phasen unterschieden werden: Ködern – Vertrauen aufbauen – Vermögen abschöpfen – Reviktimisieren.

3.1 Die Phase des Köderns

Der erste Schritt für die Täter ist es, ein fiktives Profil, also eine initiale Selbstpräsentation, zu erstellen, die zumeist aus Angaben wie Name, Nationalität, Alter, Beruf, Hobbies, Lebenseinstellungen sowie einigen Fotos besteht. Dieser Profilerstellung kommt im Cyberspace allgemein eine tragende strategische Bedeutung zu. Schließlich bestimmt die Art und Weise der hier durchgeführten Selbstdarstellung im Wesentlichen das Ausmaß der Aufmerksamkeits- und Kontaktchancen und somit die Wahrscheinlichkeit, dass ein Nutzer in der Masse der Profile überhaupt wahrgenommen und positiv beurteilt wird. Wichtig ist dabei v. a. eines: Da die – gerade dem Online-Dating inhärente – Selbstdarstellung mittels Texten und Fotos eine Art einseitiges Kommunikationsangebot an potenzielle Profilbetrachter darstellt, darf sie – will das Profil erfolgreich sein – nicht einfach individuelle Besonderheiten abbilden, sondern muss die Darstellung in erster Linie an die Erwartungen der anderen anschlussfähig machen. Anders formuliert: Es geht nicht um individuelle Einmaligkeit, sondern um eine Einordnung in verschiedene soziale Bewertungskategorien. Eine Ausrichtung am „common sense“ hinsichtlich Attraktivität, Geschlechterrollen, Interessen und sozioökonomischem Status ist hier ausgesprochen wichtig. Dies wiederum ermöglicht Betrügern, die ja nicht der o. g. „Bremse“ eines möglichen Face-to-Face-Treffens unterliegen, ein geradezu „über-ideales“ Profil zu gestalten. Typische Profile sind etwa:

- *Der männliche Scammer:* Der Betrüger präsentiert sich als gut aussehender Mann zwischen 40 und 60 Jahren, der beruflich als Geschäftsmann, Manager oder hochrangiger Militärangehöriger[13] tätig ist, kurzum einen hohen sozioökonomischen Status innehat. Er beschreibt sich als wohlhabend, loyal, respektvoll, humorvoll, religiös sowie maskulin. Sofern Hobbys genannt werden, besteht kein Interesse an typischen „Männer-Aktivitäten" (wie etwa Fußball), sondern an Tätigkeiten wie Fitness, Kochen oder Tanzen. Zumeist hat er eine tragische Lebenssituation hinter sich (Tod der Ehefrau, des Kindes, der Eltern; schwierige Scheidung usw.) und sucht nun eine liebende Frau (Füllgrabe 2015; Kopp et al. 2015; Whitty 2013, 2015). Als Nationalität geben die in Deutschland agierenden Betrüger meist englischsprachige Länder an (USA, England, Australien), womit sie auch ihre schlechten Deutschkenntnisse erklären.[14] In den englischsprachigen Ländern wird hingegen häufig die Nationalität der Opfer vorgetäuscht.
- *Der weibliche Scammer:* Fake-Frauen sind deutlich jünger als ihre männlichen Pendants (meist nicht älter als 30) und äußerlich ausgesprochen attraktiv. Sie sind finanziell unabhängig, aber nicht wohlhabend; meist haben sie schlecht bezahlte Jobs als Krankenschwestern, Lehrerin, Studentin oder Verkäuferin. Ihre Hobbys entsprechen gängigen Gender-Stereotypen (Musik, Fitness, Sport; selten auch ungewöhnlichere Aktivitäten wie Motorsport oder Fußball). Sie sind nicht an Geld interessiert, selbstbewusst und suchen die „wahre Liebe", was sexuelle Anzüglichkeiten nicht ausschließt. Mit dem nicht selten erheblichen Altersunterschied zu den (männlichen) Opfern haben sie selbstredend kein Problem (Füllgrabe 2015; Kopp et al. 2015; Whitty 2013, 2015). Die vorgegebenen Nationalitäten variieren hier mehr als bei den Fake-Männern, nicht selten werden sogar die wahren Herkunftsländer angegeben[15].

---

[13]Diese Legende ist derart typisch, dass sie auch als „Military Scam" bekannt geworden ist.

[14]Laut kriminalpolizeilicher Einschätzung sind rund 95 % der Englisch sprechenden Kontakte auf deutschen Dating-Seiten Romance-Scammer. Es gibt allerdings auch etliche, die perfekt Deutsch sprechen. https://www.polizei-beratung.de/themen-und-tipps/betrug/scamming/rat-und-hilfe/ [letzter Zugriff: 18. April 2019].

[15]Der Russian Dating Scam ist eine (kriminalistischen Einschätzungen zufolge nicht mehr so verbreitete) Variante des IRS, die sich vom hier behandelten IRS v. a. hinsichtlich der dahinterstehenden Tätergruppierungen unterscheidet. Die zumeist russischstämmigen Betrüger posieren dabei als gutaussehende Frauen auf Partnersuche. Als Wohnort wird zumeist Russland (insbesondere Cheboksary, Kasan, Moskau, Luhansk) angegeben – wohl, weil dort der Mittelpunkt des betrügerischen Netzwerkes angesiedelt ist (Heubrock und Böttcher 2011, S. 79).

Weiterhin wird auch von homosexuellen Profilen berichtet, wobei diese noch keine so große Verbreitung gefunden zu haben scheinen oder aber eine noch höhere Dunkelziffer aufweisen.

Das Profil ist quasi der „Köder“ und die Betrüger versuchen diesen so zu gestalten, dass er für ihre Opfer möglichst attraktiv ist. Sie greifen dazu verbreitete, stereotype Annahmen über Partnerwünsche von Frauen und Männern (z. B. Frauen suchen Partner mit hohem sozioökonomischen Status, Männer achten eher auf physische Attraktivität[16]) auf und bedienen diese durch entsprechende Fotos[17] und Angaben, die meist eher vage gehalten sind, wodurch sie es dem Opfer ermöglichen, die „Leerstellen“ mit den eigenen Wünschen und Hoffnungen aufzufüllen (Füllgrabe 2015, S. 488; Whitty 2013, S. 677). Natürlich ist auch ein attraktiv und überzeugend gestaltetes Profil kein Selbstläufer; in einem bestimmten situativen Kontext jedoch – also eben beispielsweise auf einer Dating-Seite, deren Mitglieder stark motiviert sind, ihren idealen Partner zu finden (Whitty 2013, S. 677) – kann es einen starken Effekt haben.

Grundsätzlich stecken die Betrüger in den Aufbau der Profile viel Arbeit; wahrscheinlich testen sie auch, welche Arten von Profilen am erfolgreichsten sind. Die Angaben in den Profilen (Beruf, Fotos, Hobbys und Interessen) dienen dabei nicht nur der Präsentation eines idealen Partners, sondern geben gleichzeitig subtile Hinweise für die weitere Entwicklung der Betrugsnarration.

Mit dem erstellten Profil kontaktieren die Täter ausgewählte Opfer. Nach welchen Kriterien sie ihre Auswahl treffen, ist nicht bekannt und lässt sich allenfalls aus einer Typologisierung der Opfer ableiten (die natürlich durch die Dunkelziffer verzerrt ist). In den vergangenen Jahren erfolgte die Kontaktaufnahme zu den Opfern v. a. über Dating-Portale oder Soziale Medien (v. a. Facebook), inzwischen oft auch direkt über Fotos-Apps (v. a. Instagram) (Marx und Rüdiger 2017, S. 212). Auch direkte Ansprachen via Messenger und E-Mail kommen vor; die Adressen recherchieren die Täter aus dem Netz oder beziehen sie über teils dubiose Adresshändler.

[16]Darin spiegeln sich auch typische asymmetrische Mechanismen der Partnerwahl: Frauen präferieren eher Männer mit hoher Bildung und Einkommen; Männer sind auch gewillt, sich mit vergleichsweise niedriger gebildeten und einkommensschwachen Frauen zu treffen (Aretz et al. 2017, S. 19 f.).

[17]Die von den Scammern verwendeten Fotos (sehr attraktiver Menschen) sind in den meisten Fällen gestohlen oder einfach von den Social Media-Auftritten der jeweiligen Personen kopiert. Einige dieser zu Täuschungszwecken missbrauchten Bilder zieren inzwischen Hunderte von gefälschten Profilen. Gerade Bilderserien von einer Person sind für Scammer interessant, denn sie können damit dem Opfer immer wieder fotographische „Beweise“ ihrer Existenz schicken.

Unabhängig vom Kontaktkanal gestaltet sich die Kontaktaufnahme immer gleich: Ein kurzes „Hallo“, gefolgt von einer Einladung zum Chatten, der dann – sofern diese angenommen wird – die Selbstpräsentation des Betrügers (das Profil sowie einige ansprechende Fotos) folgt. Die anschließende Kommunikation erfolgt teils in Englisch, teils auch in Deutsch, wobei dann ein Computerübersetzungsprogramm (google translator) genutzt wird. An den dadurch entstehenden oft radebrechenden Formulierungen *(„Honig ich werde Sie zahlen zurück mit Interesse“)* stören sich nur die wenigsten Opfer. Falls der Kontakt über ein Dating-Portal zustande gekommen ist, leiten die Betrüger ihre Opfer kurz nach dem ersten Kontakt auf direkte Kommunikationskanäle (wie Messenger oder Email) um. Dadurch machen sie sich von der Partnerbörse unabhängig und laufen nicht Gefahr, durch Entlarvung und Sperrung seitens des Administrators den Kontakt zu den Opfern zu verlieren (Heubrock und Böttcher 2011, S. 77). Denn nicht selten werden die Fake-Profile nach dem „Abfischen“ der Mail-Adressen bereits nach wenigen Tagen gelöscht: entweder durch den Administrator, sofern dieser den Account als Scammer identifiziert hat, oder durch den Scammer selbst, der damit vermeidet, dass sein Opfer die Korrespondenz mit den Profilangaben abgleicht und dabei möglicherweise Widersprüche aufdeckt (Heubrock und Böttcher 2011, S. 78).

3.2 Die Phase des Vertrauensaufbaus

In dieser auch „Grooming“ (Whitty 2013) genannten Phase wickeln die Täter das Opfer ein. Sie erschleichen sein/ihr Vertrauen, indem sie eine scheinbar sichere Umgebung schaffen, in der das Opfer seine intimsten Gedanken, Geheimnisse und Unsicherheiten erzählen kann. Dies funktioniert gerade über computervermittelte Kommunikation sehr gut. Das Fehlen nonverbaler Signale bei der computervermittelten Kommunikation führt nämlich – wie der Kommunikationswissenschaftler Joseph Walther in seinem „hyperpersonal model“ (Walther 1996) beschreibt – dazu, dass mehr persönliche Informationen ausgetauscht werden als in der Face-to-Face-Kommunikation. Solche hyperpersonellen Kommunikationen erscheinen manchen attraktiver als Face-to-Face-Kommunikationen, da sie die Möglichkeit bieten, einem idealisierten (und sich selbst idealisierenden) Gegenüber in einem scheinbar geschützten und unsichtbaren Raum das tiefste Innere zu offenbaren. Die rein auf die Nachricht beschränkte selektive Selbstdarstellung, die aufgrund der Asynchronität der Kommunikation obendrein optimierbar ist, kann leicht zu einer Idealisierung des Kommunikationspartners führen. Dieser Effekt verstärkt sich noch, indem die Betrüger ihre Kommunikation auf ihr

jeweiliges Opfer zuschneiden. Durch geschicktes Fragen und genaues Zuhören finden die Betrüger heraus, welche Vorstellung einer idealen Beziehung bzw. eines idealen Partners das Opfer hat, die sie dann entsprechend bedienen.

Auffällig ist ferner, dass die meisten Betrüger das Opfer sehr schnell mit Kosenamen ansprechen, ihm die Liebe erklären und das Bild einer gemeinsamen Zukunft aufbauen (Füllgrabe 2015). Hierbei kommt eine Fülle an schwülstig-poetischen Liebeserklärungen und Komplimenten zum Einsatz, bei denen die Scammer zumeist auf vorgefertigte Skripte zurückgreifen. Diese bausteinartigen Liebesschwüre sowie das regelmäßig geheuchelte Interesse *(„wie war dein Tag?“)* sind sozusagen das Minimalprogramm, das in vielen Fällen schon ausreicht. Versiertere Betrüger geben darüber hinaus auch noch vermeintlich private Details aus ihrem fiktiven Leben preis – sie erzählen von ihren Kindern, ihrem Beruf, ihren Problemen, Hoffnungen und Wünschen. Damit entlocken sie ihrem Opfer reziprok intime Details über sein/ihr Leben, die sie wiederum geschickt in ihre Betrugsnarrationen einflechten. Das Opfer erlebt dies als vermeintlichen Seelengleichklang und übersieht, dass die wahrgenommenen Gemeinsamkeiten – sei es der Musikgeschmack, die politischen Ansichten oder die Hobbys – nur aufgrund der eigenen Erzählungen oder der im Internet preisgegebenen Informationen konstruiert wurden.[18]

Zusätzlich beschwichtigen die Scammer geschickt (und teilweise prospektiv) das vielleicht noch latent vorhandene Misstrauen. Unaufgefordert bestätigt der Betrüger seine Erzählungen, sei es durch die Übersendung von Fotos oder Dokumenten oder durch die Aussagen anderer Personen (vermeintliche Freunde, Familienangehörige, Rechtsanwälte, Diplomaten oder Ärzte). Manche Opfer bestehen in dieser Phase auf Telefonate oder gar Videochats. Die Betrüger wissen sich auch hier zu helfen: Telefonate werden mittels Follow-me-Mobiltelefonen oder über IP-Telefonie geführt, wodurch die Herkunft des Anrufenden verschleiert werden kann (so kann etwa ein Scammer aus Ghana mit einer britischen Vorwahl telefonieren). Bei Videochats (Skype) werden technische Probleme vorgeschoben, wegen derer die Kamera nicht verwendet werden können oder gestohlene Videos vorgespielt, während man aufgrund des „defekten“ Mikrophons schriftlich kommuniziert.

[18]Der „digitale Narzissmus“, der einige Menschen eine Vielzahl an Informationen über ihr berufliches und privates Leben im Netz preisgeben lässt, macht es den Täter einfach, sich auf die spezifischen Bedürfnisse und Interesse ihrer Opfer einzustellen (Marx und Rüdiger 2017, S. 212).

Insgesamt hat dieses mal Tage, mal Monate dauernde „Grooming“ für das Opfer folgende Konsequenzen: Es befindet sich nun in einer sehr intimen „Beziehung“, die schon aufgrund der hohen Kommunikationsfrequenz (mehrere SMS, Mails, Chats pro Tag) einen großen Teil seines/ihres Alltag einnimmt. Mitunter resultiert daraus auch ein Stück weit Isolation vom gewohnten sozialen Umfeld, zumindest wenn dieses skeptisch oder kritisch darauf reagiert, dass das Opfer eine derart tiefe Bindung zu einer Person hat, die keiner je gesehen hat, die aber gleichzeitig „zu toll um wahr zu sein“ scheint.[19] An diesem Punkt fühlt sich das Opfer in einer sich entwickelnden Liebesgeschichte, die – den Versprechen des Betrügers zufolge – sehr bald in ein glückliches und finanziell abgesichertes, mitunter sogar luxuriöses Leben zu zweit münden soll.

3.3 Die Phase der Vermögensabschöpfung

Nachdem die Betrüger einige Zeit lang Vertrauen aufgebaut haben, kommt unweigerlich der für sie entscheidende Punkt: Sie bitten das Opfer um Geld. Um zu verhindern, dass die von ihnen sorgsam aufgebaute „Liebesgeschichte“ durch die Geldforderung einen vorzeitigen Bruch erfährt, bereiten die Täter dies sorgsam vor (Kopp et al. 2015, S. 212). Von Beginn an entwickeln sie parallel zu der Liebesgeschichte eine zweite Narration – gewissermaßen das „Geld-Drama“, indem sie subtil entsprechende Hinweise streuen und beide Erzählstränge anschließend so miteinander verflechten, dass das Geld zur Vorbedingung der Liebe, also der glücklichen gemeinsamen Zukunft, wird (Kopp et al. 2016). Die entsprechenden „Geld-Dramen“ variieren stark, lassen sich aber in der Regel zwei großen Kategorien zuordnen: Krisen und Investments. *Krisengeschichten* thematisieren eine Notlage, in die der/die vermeintlich Zukünftige unverschuldet geraten ist und wegen der er/sie sich verzweifelt an das Opfer mit Bitte um finanzielle Hilfe wendet (geschäftliche Schwierigkeiten, Krankheit, Verhaftung, etc.). *Investitionsgeschichten* wiederum stellen dem Opfer einen finanziellen Gewinn (bzw. ein gemeinsames Leben in Wohlstand) in Aussicht, zu dessen Erlangung allerdings vorab finanzielle Investitionen zu leisten sind (Schatzfund, Hausverkauf, Erlangung von Pensionsansprüchen etc.). Die Betrüger nutzen verschiedene

[19]Diese Isolationstendenzen verstärken sich immens, sobald die erste Geldzahlung stattgefunden hat. Viele Opfer verheimlichen dann bewusst die Beziehung (zumindest den Teil mit dem Geld), schon um keine warnenden Hinweise signifikanter Anderer (v. a. Familie, Freunde) zu erhalten, die sie in kognitive Dissonanz versetzen würden.

Taktiken, die sie ggf. auch abwechseln oder kombinieren, um Geldforderungen in ihre Geschichten einzubetten – mal werden zur Überprüfung der Zahlungsbereitschaft des Opfers nur kleine Geschenke erbeten (Buchanan und Whitty 2014, S. 262), mal wird eine anfänglich kleine Unterstützung im Laufe einer eskalierenden „Krise“ sukzessive erhöht, mal werden unmittelbar hohe Geldforderungen gestellt und bei Weigerung des Opfers schrittweise reduziert (Whitty 2013) und mal verlangen die Betrüger nur kleine Geldbeträge (Begleichen von Lebenshaltungskosten, Universitätsgebühren etc.), dies dafür aber regelmäßig und über mehrere Jahre (Füllgrabe 2015, S. 489).

Schlägt eine Taktik fehl und das Opfer weigert sich zu zahlen, wird zur Phase des Vertrauensaufbaus zurückgekehrt, um zu einem späteren Zeitpunkt erneut einen Versuch mit derselben oder einer anderen Taktik zu unternehmen (Whitty 2013, S. 679). Auf diese Weise werden die Geldüberweisungen auch aufrechterhalten. Auf einen erfolgten Geldtransfer folgen immer ein erneuter Vertrauensaufbau und dann wieder eine Geldforderung. Meist ist die Frequenz, in der Geld gefordert wird, sehr hoch und es liegen nur wenige Tage zwischen der angeblich „einmaligen“ oder „garantiert letzten“ Finanzspritze und dem erneuten Einfordern eines Betrags. Weigert sich das Opfer, bauen die Täter massiv Druck[20] auf – es wird gefleht, die baldige Rückzahlung mit Zinsen in Aussicht gestellt oder mit Beziehungsende, Gesamtverlust des bisher „geliehenen“ Geldes oder gar Selbstmord gedroht. Häufig dramatisiert sich die Situation zunehmend – die „Krise“ wird immer schlimmer und gleichzeitig rückt die Aussicht, den „Geliebten“ bei sich zu haben, immer näher. Dieses ständige Schwanken zwischen emotionalen Extremen – Liebe und Wunscherfüllung einerseits, Druck und Angst andererseits – ist für die Opfer sehr belastend.

3.4 Die Phase der Reviktimisierung

Die Täter würden die Täuschung nie von sich aus auflösen, es sei denn, sie gründen einen erneuten Betrug darauf. Wie und wann können sich Opfer also aus der Täuschung befreien? Gemeinhin würde man vermuten, dass im Laufe des Betrugs der psychologische Druck bei den Opfern – allein schon durch das zunehmende Ausschöpfen der eigenen Geldquellen – derart zu- und die

[20]So forderte etwa ein Betrüger seine „Verlobte“ dazu auf, ihren 93-jährigen Erb-Onkel zu töten, mit der Begründung, dann könne man endlich eine schöne Hochzeit feiern (Nürnberger Nachrichten, Samstag 20. August 2016, Rubrik Stadt Nürnberg).

Plausibilität der ständigen Geldforderungen derart abnimmt, dass sie quasi automatisch zur Erkenntnis kommen, betrogen worden zu sein. Das scheint allerdings kaum der Fall zu sein. Es kommt zwar vor, dass Opfer durch eigene Zweifel und Recherchen der Täuschung auf die Schliche kommen und den Kontakt zu dem Betrüger abbrechen. Dies geschieht jedoch eher selten und wenn, in frühen Phasen des Betrugs. Je mehr und je öfter ein Opfer Geld übereignet hat, desto tiefer ist es in die Täuschung verstrickt. In den meisten Fällen bedarf es deswegen eines Anstoßes durch Dritte, in erster Linie der Polizei (die etwa durch Bankmitarbeiter, besorgte Verwandte und Freunde oder im Rahmen einer Geldwäsche-Ermittlung auf den Fall aufmerksam wird). Doch selbst nachdrückliche Warnungen und das Vorlegen von Beweisen für die falsche Identität der Täter durch die Polizei stoßen bei vielen Opfern auf taube Ohren.[21] Denn die „Ent-Täuschung" vom Betrug ist emotional äußerst schmerzvoll. Viele Opfer haben gefühlt nicht nur Geld, sondern auch einen geliebten Menschen verloren. Sie leiden nach der Aufdeckung des Betrugs unter negativen Gefühlen wie Depression, Scham, Ärger, Furcht, Suizidgedanken usw. (Füllgrabe 2015, S. 490). Schon deswegen wollen viele mal mehr, mal weniger bewusst den Kontakt mit dem Betrüger nicht ganz abbrechen.

Häufig erfolgt dann eine *Reviktimisierung* bzw. eine *„second wave of the scam"* (Whitty und Buchanan 2016, S. 182), denn die Betrüger melden sich erneut, reaktivieren alte Gefühle und setzen dann entweder die alte Masche fort oder bringen neue Betrugsgeschichten in Anschlag. Opfern, die das Geld am meisten schmerzt, suggerieren die Täter beispielsweise, sie seien Polizisten, die – gegen Gebühr – das erbeutete Geld zurückbringen könnten. Bei jenen, die der verlorenen Liebe nachtrauern, meldet sich etwa ein Bestatter, der berichtet, der Partner wäre auf dem Weg zum Flughafen tödlich verunglückt und könne nur mit finanzieller Hilfe des Opfers eine würdige Bestattung erhalten. Oder aber der Scammer gibt schließlich „reumütig" zu, er sei ein Betrüger, doch habe er sich inzwischen in das Opfer verliebt (und brauche aber natürlich weiterhin Geld) (Whitty und Buchanan 2016, S. 185). Sollten die Geschädigten irgendwann definitiv kein Geld mehr haben bzw. auftreiben können, werden sie von den Betrügern nicht selten als Finanzagenten eingesetzt.[22]

---

[21]Mitunter geht die Verfangenheit in der Täuschung so weit, dass Opfer, die nicht wahrhaben wollen, dass hinter ihrem Traumpartner eigentlich kriminelle Organisationen stecken, nach Afrika fliegen, um sich auf die Suche nach diesem zu begeben. Dabei werden Fälle von Kidnapping und hohen Lösegeldforderungen berichtet.

[22]Finanzagenten sind Personen, die für die Betrüger bewusst oder unbewusst die Weiterleitung und damit Verschleierung von Geldtransfers übernehmen.

4 Täter und Täterwissen

Bisher liegen nur wenige Erkenntnisse über Täter und Täterwissen vor. Nach der Einschätzung vieler Ermittler sind die meisten IRS auf Täter aus Nigeria, Ghana und Kamerun zurückzuführen. Gleichzeitig handelt es sich beim IRS um ein globales Phänomen. Auch wenn der Schwerpunkt in Bezug auf die Opfer auf Australien, Europa und den USA zu liegen scheint, häufen sich in den letzten Jahren Berichte aus aller Welt, v. a. aus dem südostasiatischen Raum, aus Malaysia (Koon und Yoong 2013) und Indien (Arora und Scheiber 2017).

Der IRS kann dabei einer primär in Westafrika verorteten „Subkultur des Betrugs" zugerechnet werden, auf deren Konto auch andere typische Cybercrime-Delikte gehen (Boateng et al. 2011; Ellis 2016; Oduro-Frimpong 2014). Kriminalhistorisch erlebte diese ihre Initialzündung, als in den 1980er Jahren nigerianische Banden begannen – zunächst per Fax, später via E-Mail – hunderttausende Betrugs-Anschreiben in alle Welt zu versenden. Ihre bekannteste Masche, der „419 scam"[23], wurde zu einem globalen Massenphänomen und die dahinterstehenden Tätergruppierungen als „Nigeria Connection" berühmt-berüchtigt. Auch wenn diese Bezeichnung es nahelegt, handelt es sich hier nicht um eine strukturierte Organisation, sondern (zumindest derzeit noch) um viele kleine – teils unabhängige, teils lose verbundene – Gruppen. Diese verändern sich ständig und entwickeln auch ihre Modi Operandi weiter. Anstelle der klassischen langen und erzählerisch ausgeschmückten Nigeria-Mails treten heute zunehmend Variationen und teils auch Kombinationen mit anderen Betrugsmaschen auf.[24] Eine derartige Weiterentwicklung ist auch der IRS, der das erste

[23]Die Masche lässt sich zwar unter dem Namen „spanish prisoner" bis ins 16. Jahrhundert zurückverfolgen Gillespie (2017), ist aber seit mehreren Jahrzehnten derart mit Nigeria verknüpft, dass sie nach dem § 419 („Betrug") des nigerianischen Strafgesetzbuchs benannt wurde. Das Grundprinzip ist, einer Person in einem Anschreiben ein großes Vermögen (Erbe, Lottogewinn, geheimes Konto etc.) in Aussicht zu stellen, davor jedoch verschiedene „Gebühren" (als Vorschuss) zu kassieren. Das Geld existiert natürlich nicht, die Vorschuss-Zahlungen können allerdings schnell exorbitante Höhen erreichen.

[24]So finden sich anstelle oder gemeinsam mit dem klassischen 419 scam Betrugsmaschen wie der CEO-Fraud, der Facebook Swindle, Heimarbeit-Betrug, der Hitman-Scam oder der Wash-wash-Scam.

Mal 2007 in England aktenkundig wurde (Buchanan und Whitty 2014, S. 262).[25] Seine Entwicklung hing v. a. damit zusammen, dass nigerianische Betrüger um die Jahrtausendwende ihre Betrugsaktivitäten nach Ghana verlagerten, wohl wegen des seit damals erhöhten Ermittlungsdrucks durch die nigerianische Finanzpolizei. Sie brachten ihr „Betrugswissen" mit, also jene *„cyber-fraud paradigms or storylines that have proven economically fruitful when employed in the past"* (Warner 2011, S. 743). Die lernwilligen ghanaischen Betrüger adaptierten diese und modifizierten Köder und Zielgruppe: die „Geschäftsbeziehung" beim 419 scam, mit der ein großes Vermögen erlangt werden soll, wurde beim IRS zu einer „Liebesbeziehung", die ein Happy End in Zweisamkeit (und Wohlstand) in Aussicht stellt.

Diese so entstandene „Masche" des Liebesbetrugs wurde (und wird) sukzessive verbessert und professionalisiert. So ist einer der Hauptschwachpunkte beim IRS der „Version 1.0", nämlich der direkte Bezug zu Afrika, inzwischen weitgehend eliminiert. Früher konnten Dating-Portale auffällige IP-Adressen aus Verdachtsländern einfach herausfiltern, Banken und Geldtransfer-Organisationen Warnhinweise bei entsprechenden Überweisungen aussprechen oder die Opfer selbst Verdacht schöpfen, wenn sie vom vermeintlichen Geliebten mit einer afrikanischen Vorwahl angerufen wurden. Heute nutzen die Betrüger diverse Tricks wie das Umleiten von IP-Adressen oder call-ID-spoofing (zur Verschleierung von Telefonnummern). Und für Geldtransfers wurden inzwischen von den Betrügern (teils mit unwissentlicher Hilfe durch Finanzagenten) in den Zielländern Konten angelegt und Mittelsmänner engagiert. Hinzu kommt, dass durch die Massenemigration, die ab den 1980er Jahren in Nigeria stattfand, eine weltweite Diaspora entstanden ist, die eine Art „human internet" (Ellis 2016, S. 165) bildet. Das bedeutet, dass die Online-Betrüger, die ja (derzeit) als Einzeltäter oder in kleinen Gruppen (also ohne übergreifende Organisationsstrukturen) operieren, Zugriff auf ein weltumspannendes soziales Netzwerk haben, von dem sie Informationen beziehen und auf das sie für die Abwicklung ihrer Betrügereien (etwa Geldwäsche, Finanztransfers etc.) zurückgreifen können. Dieses Netzwerk ist aufgrund der dort stattfindenden Kommunikation in regionalen Dialekten fast

[25]Es gibt auf den ersten Blick ähnliche Maschen im Zusammenhang mit internationalen Partnervermittlungen (sog. „Katalogehen"). Gerade die „Russian Bride Scammer" erlangten um die Jahrtausendwende einige Popularität Heubrock und Böttcher 2011. Bei einer genaueren Betrachtung zeigen sich allerdings deutliche Unterschiede zum IRS (hinsichtlich Täter, Opfer und Modi Operandi).

nicht überwachbar und aufgrund verwandtschaftlicher und ethnischer Bande kaum infiltrierbar. Wie die Entwicklung hier – und damit beim IRS – weiter verläuft, lässt sich schwer sagen. Es wird befürchtet, dass es zu einer zunehmenden Organisierung, Zusammenarbeit und damit Professionalisierung der verschiedenen Gruppierungen kommt, mit der Folge, dass „enormous fraud rings“ (Rege 2009, S. 501) und ein arbeitsteilig differenzierter „underground market“ (Interpol und Trend Micro 2017, S. 4) entstehen. Dies würde eine zunehmende Verbesserung der zum Zweck der Täuschung eingesetzten Technologien und Vorgehensweisen nach sich ziehen – und damit ein noch stärkeres Gefährdungspotenzial.

Werfen wir einen kurzen Blick auf die anfangs angesprochene „Subkultur der Online-Betrüger“. Internet-Betrug – das ist das Ergebnis etlicher ethnologischer Studien – hat in einigen (west-)afrikanischen Ländern mit der Zeit eine distinkte (Sub-)Kultur hervorgebracht (Cassiman 2018; Ellis 2016; Oduro-Frimpong 2011). Betrugspraktiken wurden in alte Glaubenssysteme von Magie und Aberglaube eingebettet und mit einer aggressiven Zurschaustellung des (illegal erworbenen) Vermögens sowie Referenzen auf Rap-Musik und -Modestil verschmolzen. Das „Scamming“ ist in Westafrika also keineswegs eine nur Eingeweihten bekannte Tätigkeit, sondern ein bedeutsames popkulturelles Phänomen. Da sich die Selbstdarstellung der Scammer weitestgehend um „hot money“ dreht, also das (viele) betrügerisch erworbene Geld, das genauso schnell ausgegeben wie erlangt wird (Ellis 2016, S. 128), entwickeln sie eine gewisse Anziehungskraft auf Jugendliche. Gerade für (die häufig arbeitslosen) Universitätsabsolventen stellt dieser kriminelle Bereich inzwischen eine Karriereoption dar (Ojedokun und Eraye 2012).

Beispiel Ghana: Bei den dortigen Romantikbetrügern („Sakawa Boys“) handelt es sich um junge ghanaische Männer (zu 90 % unter 30 Jahren und meist undergraduate students), die in oder in der Nähe von urbanen Zentren wie Accra oder Kumasi (bzw. in den dortigen Slums wie Nima, Maamobi, Accra New Town oder Mallam Atta) leben. Sie sind oftmals arbeitslos und verbringen ihre Tage in Internetcafés (Warner 2011, S. 741). Diese sind nicht nur Orte jugendlicher Vergemeinschaftung, sondern teils auch Orte gemeinschaftlichen Betruges. Die sich selbst auch als „browsers“ (Cassiman 2018, S. 79) bezeichnenden Betrüger versuchen mit falschen Identitäten über Soziale Medien bzw. Online-Dating westliche Opfer – im dortigen Jargon als „paypal“ bezeichnet – zur Überweisung möglichst hoher Geldsummen zu bewegen. Sind dafür Telefonate erforderlich, greifen die „browsers“ auf entsprechende Komplizen („phone girls/boys“) zurück (Cassiman 2018, S. 81). Die erfolgreichsten Betrüger, ehrerbietig

„hitter“ oder „barons“ genannt, nutzen ihr betrügerisch erworbenes Vermögen, um in bessere Viertel zu ziehen und sich dort mit einer Entourage an jungen, lernwilligen „browser“-Aspiranten zu umgeben. Die Anfänger in diesen Gruppierungen – „boy“ oder „maid“ genannt – müssen zunächst Hilfsarbeiten für ihren Master leisten, etwa Profilbilder beschaffen, IP-Adressen verschleiern, kleinere Chats übernehmen usw. (Cassiman 2018, S. 82). Die Tatsache, dass erfolgreiche „Barons“ betrügerisch große Vermögen erwerben und dies auch habituell nach außen hin demonstrieren, hat immensen Einfluss auf die Erwerbsaspirationen junger Afrikaner. Denn Online-Betrug ermöglicht (zumindest theoretisch) jedem, der bereit ist das „browsen“ zu lernen und ein paar ghanaische Cedis für das Internetcafé hat, die Chance auf einen schnellen sozialen Aufstieg. Die unmoralische Seite dieser Tätigkeit wird rationalisiert, indem das Scamming als „Revanche“ für Jahrhunderte der Kolonisierung und Ausbeutung wahrgenommen wird (Warner 2011, S. 746).

Diese Sichtweise wird von vielen Landsleuten allerdings *nicht* geteilt. Bis hin in höchste Regierungskreise wird die Betätigung im Betrug als höchst unmoralisch gesehen, die Betrüger werden als faul, gierig und verdorben öffentlich gebrandmarkt. Und in der Tat hat die zunehmende Ausbreitung der Interkriminalität weitreichende gesellschaftliche Auswirkungen: Die vormals wirksamen Verteilungsmechanismen innerhalb der Gesellschaft erodieren – während einst Reiche ihre Verwandten, Freunden und Untergebenen an ihrem Vermögen teilhaben ließen, bleibt das betrügerisch erworbene Geld nun innerhalb kleiner krimineller Banden. Um Begehrlichkeiten zu entgehen, verlassen diese ihre angestammten Viertel und damit auch ihre ursprünglichen sozialen Beziehungen (Cassiman 2018, S. 84). In der Folge erodieren frühere Mechanismen von Loyalität und Freundschaft. Viele Betrüger haben qua ihres finanziellen Reichtums eine Vorbildfunktion, die sich auch auf die von ihnen vorgelebte Gier, Ichbezogenheit und Attitüde der ständigen Täuschung erstreckt. Dies wird auch von vielen Jugendlichen als ein moralischer Verfall empfunden. Auf der anderen Seite hat der Boom des Cybercrime Raub und Diebstahl in den Straßen von Nima deutlich verringert (Cassiman 2018, S. 84). Beachtlich ist außerdem, dass durch betrügerische Tätigkeiten gewonnenes Geld nicht mehr wie vormals benutzt wird, um ins Ausland zu reisen bzw. dorthin zu emigrieren. Stattdessen bleiben die Jugendlichen in Ghana, genießen dort den durch das Geld ermöglichten luxuriösen Lebensstil und demonstrieren diesen auch nach außen. All dies trägt dazu bei, dass der Romantikbetrug aller Voraussicht nach in Zukunft wohl eher zunehmen wird.

5 Die Geschädigten

5.1 Charakteristika

Oft stößt man beim IRS auf das Vorurteil, dass nur ein bestimmter „Typ Mensch" hier überhaupt zum Opfer werden kann. Die Studienlage zeichnet allerdings ein differenziertes Bild: Aufgrund seiner Variabilität kann der IRS unterschiedlichste Opfer ins Visier nehmen. Die Scammer können sich auf Alter, Geschlecht, Lebensumstände, sexuelle Orientierung usw. einstellen. Beispielsweise scheint es eine zunehmende Viktimisierung bei LGBT (engl. für Lesben, Schwule, Bisexuelle und Transgender) zu geben (Gillespie 2017, S. 219). Das derzeit typische Opfer des IRS ist allerdings eine Frau mittleren Alters – zumindest deuten (Hellfeld-)Statistiken und kriminalistische Lageeinschätzungen darauf hin. So hat das FBI festgestellt, dass die erfassten Opfer von IRS zu 82 % weiblich und nur zu 18 % männlich waren.[26] Zu ähnlichen Ergebnissen kommt Whitty (2018) in ihrem aktuellen Überblick zu Charakteristika von IRS-Opfern. Neben dem Geschlecht spielt der Bildungsgrad eine Rolle, allerdings nur insofern, als dass Kenntnisse über Gefahren und Sicherheitsmaßnahmen im Internet die Wahrscheinlichkeit senken, Opfer eines derartigen Betrugs zu werden (Whitty 2018, S. 107).[27]

Nur wenige Studien befassen sich mit den psychologischen Charakteristika bzw. Persönlichkeitsmerkmalen der IRS-Opfer. Buchanan und Whitty (2014) testeten etwa verschiedene psychologische Items hinsichtlich ihrer Viktimisierungsrelevanz. Das Ergebnis: Nur wer in besonderem Maße an „Romantik" glaubt (erhöhter Grad des Items „Romantic Beliefs"), hat eine signifikant höhere Wahrscheinlichkeit zum Opfer zu werden. Ein Teilaspekt ist hier besonders relevant – der Glaube an die „Perfektheit" einer Beziehung („belief of idealization") (Buchanan und Whitty 2014, S. 273). Man kann sich vorstellen, dass eine Person mit derartigen Vorstellungen leicht Gefahr läuft, einen Scammer als etwas zu betrachten, was er nicht ist, dabei mögliche Warnsignale zu übersehen und so in eine „Beziehung" gezogen

[26]Bei derartigen Statistiken ist natürlich immer auch das Anzeigeverhalten unterschiedlicher Opfer zu berücksichtigen. Möglicherweise haben gerade Männer eine höhere Hemmschwelle, solche „liebesbedingten" Betrugstaten zur Anzeige zu bringen.

[27]Es ist also keineswegs so, dass niedrige Bildung die Viktimisierungswahrscheinlichkeit erhöht. Im Gegenteil, Studien deuten darauf hin, dass bei vielen Betrugsmaschen gilt: Je gebildeter eine Person ist, desto wahrscheinlicher ist es, dass sie zum Opfer wird. Möglicherweise führt Bildung zu einer gewissen Selbstüberschätzung (Fischer et al. 2013).

zu werden (Buchanan und Whitty 2014, S. 278). Allerdings ist die Aussagekraft beschränkt, da es sich hier nur um einen einzelnen psychologischen Faktor mit einer sehr niedrigen Effektstärke (Vorhersagekraft) handelt (Buchanan und Whitty 2014, S. 279).

In einer weiteren Studie prüft Whitty (2018) deswegen weitere Variablen, die IRS-Opfer kennzeichnen: Typische Opfer scheinen (mittelalte und höher gebildete) Frauen mit einem vergleichsweise hohen Grad an Impulsivität (hohe Werte bei Dringlichkeit und „Sensation Seeking“) zu sein, was möglicherweise erklärt, warum sie so gut auf die dramatisierten Narrationen der Betrüger reagieren. Zudem verfügen sie über eine gewisse Sucht-Disposition – vielleicht fällt es ihnen deswegen so schwer, sich aus der Täuschung zu befreien (Whitty 2018, S. 108). Weiterhin zeichnen sich IRS-Opfer durch eine geringere Freundlichkeit („Kindness“) aus. Vielleicht verfügen sie über kleinere Netzwerke oder dieser Wert ist ein Effekt des Betrugs selbst – in dem Sinne, dass der Betrüger das Opfer im Laufe der Täuschung in eine gewisse soziale Isolation gebracht und von seinen Netzwerken separiert hat (Whitty 2018, S. 108). Zu guter Letzt scheinen IRS-Opfer auch vergleichsweise vertrauensseliger als Nicht-Opfer zu sein. Keine dieser Variablen konnte jedoch die Viktimisierung durch den IRS hinreichend erklären. Insgesamt gilt also: IRS-Opfer lassen sich weder durch sozialstatistische noch durch psychologische Variablen zweifelsfrei charakterisieren – es gibt allenfalls Tendenzen.

5.2 Folgen

Ein IRS kann gravierende emotionale und psychische Folgen für Opfer haben – von Scham, Verlegenheit und Angst über Wut, Stress und Schock bis hin zu Depressionen, posttraumatischen Störungen und mitunter sogar Selbstmord. Viele Opfer geben sich selbst die Schuld (Whitty und Buchanan 2016, S. 186).

Besonders perfide am IRS ist, dass die Opfer mit der Aufdeckung des Betrugs einen zweifachen Schlag erleiden – sie verlieren ihr Geld und ihre (vermeintliche) Beziehung (Whitty 2018, S. 105). In einer Interview-Studie mit Opfern berichten diese von vielfältigen Auswirkungen (Whitty und Buchanan 2016): Ihr emotionaler Zustand nach dem Betrug ist äußerst negativ beeinflusst durch Gefühle von Scham, Ekel und Wut. Einige fühlen sich gewissermaßen sexuell missbraucht und vergewaltigt (Whitty und Buchanan 2016, S. 180). Die meisten (Männer wie Frauen) sind depressiv, manche suizidal. Hinzu kommt nicht selten eine negative Reaktion des Umfelds. Zentrale Personen im Leben des Opfers reagieren mit Unverständnis, sind teils wütend über den finanziellen Verlust (v. a. potenzielle Erben), verweigern

die so nötige Unterstützung und stigmatisieren die Opfer als dumm (Whitty und Buchanan 2016, S. 181). Aufgrund des massiven Geldverlustes leiden nicht wenige Opfer unter einer Verschlechterung ihrer sozialen Situation – der durch den Betrug bedingte finanzielle Ruin beschränkt ihre sozialen und lebensweltlichen Möglichkeiten enorm (Whitty und Buchanan 2016, S. 182). Am schwersten wiegt der Verlust der Beziehung. Der fiktive Partner wurde als „idealer Partner" erlebt. Für manche war die Beziehung regelrecht therapeutisch, in dem Sinne, dass sie sich ihrem Gegenüber vollends anvertrauen konnten, ohne Vorwürfe oder Kritik zu erfahren: *„This relationship was so intense because they were able to self-disclose their inner most selves"* (Whitty und Buchanan 2016, S. 183).

Dementsprechend finden es viele Opfer äußerst schwierig, den Kriminellen von seiner vorgetäuschten Identität zu separieren. Manchen ist die Beziehung so wichtig, dass sie auch weiterhin zahlen würden, nur um sie fortzusetzen. Andere begeben sich auf die Suche nach den wahren Personen hinter den gestohlenen Bildern oder versuchen sogar die Betrüger ausfindig zu machen (Whitty und Buchanan 2016, S. 182).

Im Hinblick auf mögliche Ent-Täuschungs- und Bewältigungsstrategien scheint eine Enthüllung signifikanten Anderen (Familie, Freunde, Bekannte) gegenüber zumeist nicht hilfreich, sondern eher schädlich zu sein. Denn seitens des sozialen Nahfeldes erfahren Opfer dieser unglaublich erscheinenden Masche statt Unterstützung häufig offen oder verdeckt geäußerte Vorwürfe und Unverständnis. Der Umgang mit der Polizei hingegen ist für viele Opfer regelrecht therapeutisch. Die Beamten zeigen in der Regel eine hilfreiche *„unconditional positive regard"* (Whitty und Buchanan 2016, S. 186). Ein Nebeneffekt dieser neutral-empathischen Haltung kann allerdings sein, dass Opfer die Intentionen der Beamten missinterpretieren und sich in diese verlieben („transference effect"; vgl. Whitty und Buchanan 2016, S. 187).

6 Psychologische und soziologische Erklärungsversuche

Retrospektiv erscheint der IRS sowohl den Opfern als auch äußeren Beobachtern unerklärlich. Wie ist es möglich, dass sich – obwohl zwischen Opfer und Täter niemals physischer Kontakt bestand – eine derart starke emotionale Bindung und suggestive Kraft besteht, dass große Vermögenswerte scheinbar ohne jegliche Zweifel und Vorbehalte übergeben werden?

Die psychologische und sozialpsychologische Forschung setzt sich intensiv mit Persuasion und Suggestion auseinander. Einige Arbeiten thematisieren dabei

explizit den IRS und formulieren eine Reihe möglicher Erklärungen für dessen Wirksamkeit. Neben den oben erwähnten psychologischen Merkmalen der Opfer werden hier v. a. die von den Betrügern verwendeten „persuasive techniques“, die kognitive und motivationale Schwachstellen bei Entscheidungsprozessen ausnutzen, angeführt. Die entsprechenden Studien analysieren hierfür die initialen Scam-Mails (Carter 2015; Kich 2005), die Mail-Korrespondenzen zwischen Tätern und Opfern (Koon und Yoong 2013) oder deren Selbstbeschreibungen (Archer 2017). Das Ergebnis: Die Betrüger referieren den Autoren zufolge auf grundlegende Überzeugungsprinzipien (wie Reziprozität, Autorität, Sympathie, Knappheit etc.; etwa Archer 2017). Des Weiteren beruhe ihre Überzeugungskraft auf Kommunikationsstrategien zur Erzeugung von Glaubwürdigkeit – hierunter fällt beispielweise unmittelbare Befürchtungen ansprechen, auf dem Opfer Vertrautes/von ihm Geglaubtes referieren, dem Opfer eine Identität als Glückspilz o.ä. zuweisen (Carter 2015, S. 97), Sorge und Hingebung demonstrieren (Freiermuth 2011), Naivität/Hilfsbedürftigkeit vorspiegeln oder sich (scheinbar) selbst offenbaren (Koon und Yoong 2013, S. 32). In diesen Zusammenhang gehört auch das Betonen moralischer und/oder religiöser Werte, etwa durch demonstratives Sprechen über den eigenen Glauben oder das Engagement in humanitären Organisationen (Kopp et al. 2017, S. 91).

Einen etwas anderen Ansatz verfolgt die Linguistin Konstanze Marx. Sie geht davon aus, dass die zentrale persuasive Strategie der Täter die der „kalkulierten Emotionskreation“ (Marx 2012, S. 149) ist. Im Rahmen ihrer „linguistischen Persuasionsforschung“ über Täter-E-Mails kommt sie zu folgendem Ergebnis (Marx 2012; Marx und Rüdiger 2017): Die wesentlichen Konstituenten einer Liebesbeziehung (Leidenschaft, Intimität, Verbindlichkeit) lassen sich auch über digitale Text-, Ton- und Bildbotschaften verwirklichen. Teilweise erscheinen solche reinen „Netz“-Beziehungen sogar noch intensiver, da auf den normalerweise durch körperliche Präsenz oder Alltagsprobleme besetzten Ebenen Projektionsflächen entstehen, die mit Wunschvorstellungen und Träumen aufgefüllt werden (Marx 2012, S. 150). Liebesbetrüger nutzen dies mittels einer „kalkulierten Emotionskreation“ aus, die auf drei Faktoren (Qualität, Intensität, Dauer) basiert.

Hinsichtlich der „Qualität“ stellen sie sich als vertrauenswürdige Personen dar und bedienen dabei moralische wie geschlechtsspezifische Stereotype. „Intensität“ erzeugen sie nicht nur durch häufiges Kommunizieren, sondern auch durch die exzessive Verwendung von emotionsbezeichnenden und emotionsausdrückenden Wörtern (Kosenamen, Anredeformeln, Komplimente, Liebeserklärungen etc.) sowie einen höchst privaten Inhalt der Kommunikation (Erzählen des Alltags, Austauschen von Intimitäten, usw.). Diese Korrespondenzen werden schließlich auf (eine gewisse) „Dauer“ gestellt, d. h. die Phase der

Vertrauensetablierung umfasst mitunter bis zu ein Jahr, in dem hunderte, wenn nicht tausende Nachrichten ausgetauscht werden. Die Kontinuität und die schiere Menge der Informationen wirken sich vertrauensstabilisierend aus (Marx und Rüdiger 2017, S. 216). All dies zielt darauf, das Opfer in eine emotionale Falle zu locken. Diese Falle wird geplant und kalkuliert aufgebaut. Sie ist darauf ausgerichtet, das Opfer zu überzeugen, es gäbe jemanden, der tiefe Gefühle für es empfindet; gleichzeitig wird dem Opfer vermittelt, dass es auch „wert" sei, Adressat dieser Gefühle zu sein. Entsprechend wichtig und geschätzt ist der Täter für das Opfer und der Wunsch wächst, sich von Angesicht zu Angesicht zu sehen (Marx und Rüdiger 2017, S. 216). Wenn der Täter nun in eine scheinbar ausweglose Situation gerät, bleibt dem Opfer fast keine andere Möglichkeit, als ihm zu helfen.

Kopp (2016) greift auf einen anderen, mehr opferbezogenen Erklärungsansatz zurück. Für ihn beruht der Erfolg des IRS darauf, dass dieser auf tief verwurzelte erzählerische Deutungsrahmen zielt. Kopp bezieht sich dabei auf den Psychologen Robert J. Sternberg, nach dem jede Liebesbeziehung einer impliziten „story" (Sternberg 1995) folgt. Jeder Mensch hat dezidierte, teils unbewusste Vorstellungen, wie Liebe sein sollte (Sucht, Kunst, Geschäft, Fantasie, Spiel, Herrschaft, Krieg, usw.). Der Betrüger stellt sich also auf die Liebesgeschichte des Opfers ein und erschafft – je mehr Details das Opfer über sich preisgibt – eine immer passendere Geschichte. Das Kennenlernen ist so kein mitunter ernüchterndes Ersetzen von Fiktionen durch Fakten, wie das normalerweise geschieht, sondern ein geradezu rauschhaftes Bestätigen oder Übertreffen von Fiktionen, die in eine „ideale" Liebesgeschichte münden (Kopp et al. 2015, S. 212). Das Opfer hat so (vom Täter beabsichtigt) das Gefühl, die Beziehung folge einem göttlichen/schicksalshaften Ablauf bzw. das Gegenüber sei der lange ersehnte „soul mate" (Koon und Yoong 2013, S. 32). Der Betrüger *„begin[s] to build an individual imagination of an ideal partnership"* (Kopp et al. 2016, S. 147). Nicht selten werden in die sich so entwickelnde Liebesgeschichte subtil Hinweise für spätere krisenhafte Wendungen eingeflochten, die dann als Basis für die nächsten Schritte des Betrugs fungieren (Kopp et al. 2015, S. 210). Dadurch bereitet er das Opfer unbemerkt auf die zu leistenden Geldzahlungen vor. Und nachdem diese erfolgt sind, baut er sie derart in die Beziehung ein, bis die Tätigkeit des „Geldschickens" zu einer normalen Aktivität wie Schreiben, Chatten oder Bilder Schicken geworden ist. Füllgrabe (2015) bezeichnet das als „psychologische Falle", die ihre Wirksamkeit daraus gewinnt, dass die Betrüger den jeweiligen Bindungsstil und das Selbstkonzept ihres Opfers ausnutzen.

Die Kriminalpsychologin Monica Whitty, die sich seit Jahren mit dem IRS befasst, beurteilt die meisten dieser Ansätze als mögliche, jedoch nicht hinreichende

Erklärungen für die Überzeugungskraft des IRS (Whitty 2013). Ihrer Ansicht nach ergibt sich diese eher aus dem prozesshaften Aufbau des Betrugs. Dieses „Scammers Persuasive Technique Model“ führe dazu, dass die Opfer den Kommunikationsprozess mit dem Täter wie eine „Flow-Erfahrung“ erleben, die sie immer mehr in den Bann dieser Beziehung hineinzieht und andere Interaktionen in ihrem Leben ausblenden lässt: *„Victims described being caught up in the situation and in some ways immersing themselves into a world with the scammer“* (Whitty 2013, S. 679). Verstrickt in diese vom Täter induzierte Wirklichkeitskonstruktion akzeptieren die Opfer Whitty zufolge die ständigen Geldzahlungen unhinterfragt als Teil der Beziehung und sehen es nicht selten als Herausforderung, das viele Geld für den vermeintlichen Geliebten in Not zu besorgen (über Kredite, Freunde, Familie) und einen Weg zu finden, es diesem zukommen zu lassen. Manche Opfer seien erstaunlich findig darin, mögliche Schutzvorrichtungen (z. B. Überweisungssperren bei Banken oder Bargeldtransfersystemen wie Western Union) zu umgehen.[28]

7 Präventionsmaßnahmen

Der IRS, wie er hier mit Blick auf bisherige internationale Forschungsergebnisse dargestellt wurde, erweist sich als komplexe, aber dennoch typische „Betrugsmasche“, die zudem einem ständigen Formwandel unterliegt. Polizeiliche Ermittlungs- und Präventionsarbeit stehen dabei vor großen Schwierigkeiten (s. a. Kap. „Alter Wein in Neuen Medien?“). Derzeit laufen die meisten Ermittlungen beim IRS ins Leere – meist lassen sich aufgrund der Verschleierungsmöglichkeiten im Internet gar keine Täter identifizieren. Ist dies durch Zurückverfolgung der Kommunikation oder der Geldflüsse doch einmal möglich, so scheitern Festnahmen an der mangelnden internationalen Rechtshilfe mit den afrikanischen Ländern. In letzter Zeit ist es zwar – teils durch Zusammenarbeit mit Geschädigten – einige Male gelungen, Geldabholer bei der Übergabe zu verhaften. Diese spielen jedoch meist nur eine untergeordnete Rolle innerhalb der Betrügergruppierungen. In einigen anderen vom IRS betroffenen Ländern wurden deswegen verschiedenste Anstrengungen zur Bekämpfung des IRS bzw. der Cyberkriminalität insgesamt unternommen.

[28]Wieso die Täter-Opfer-Kommunikation derart suggestiv ist, kann Whitty allerdings nicht vollends plausibel erklären. Was hier noch aussteht, sind empirische Analysen des konkreten Interaktionsgeschehens beim IRS. Der Autor dieses Beitrages bereitet derzeit entsprechende Analysen aus soziologischer Perspektive vor.

In *Großbritannien* beispielsweise gibt es seit einiger Zeit eine eigene Abteilung für Cyberkriminalität, die auch für den IRS zuständig ist. Diese Abteilung ist innerhalb der SOCA (Serious Organised Crime Agency) angesiedelt und setzt in der Bekämpfung des Romantikbetruges auf eine offensive Präventionstaktik. Diese beinhaltet sowohl das Informieren der Bevölkerung als auch die Erarbeitung von Gesetzen, die es erleichtern, potenzielle Romantikbetrüger bei den Behörden zu melden, ohne als Organisation gegen Datenschutzbestimmungen zu verstoßen. In *Australien* wiederum werden opferorientierte Präventionsansätze getestet, bei denen „financial intelligence" von den australischen Behörden zur aktiven Bekämpfung von verschiedenen „online frauds", u. a. auch dem IRS, eingesetzt wurde (Cross 2016). Hierbei werden all jene identifiziert, die Geldüberweisungen in für den IRS typische Länder getätigt haben. Diese bekamen dann von den Polizeibehörden einen Brief übersandt, in dem vor einem möglichen Betrug gewarnt und Ansprechmöglichkeiten bei der Polizei genannt wurden. Die Evaluierung dieser Maßnahmen zeigte durchaus Erfolg und ein Großteil der Briefempfänger führte keine weiteren Geldtransfers durch. Der scheinbare Erfolg dieser Präventionsstrategie muss jedoch relativiert werden: Erstens muss nicht jeder Geldtransfer in eines der typischen IRS-Länder auch ein Betrug sein. Zweitens ist ungewiss, ob ein direkter Zusammenhang zwischen dem Brief und dem Einstellen der Zahlung besteht. Drittens ist die verfolgte Strategie mitnichten rein proaktiv, da schließlich mindestens eine finanzielle Transaktion bereits erfolgt sein muss. Und viertens sind Geldtransfers an Betrüger nicht auf einige typische westafrikanische Länder beschränkt. Es ist zu vermuten, dass auch die Täter zunehmend globaler agieren und/oder auf Finanzagenten im Inland zurückgreifen. Außerdem ist eine Überprüfung sämtlicher finanzieller Transaktionen ins Ausland logistisch für Ermittlungsbehörden nicht möglich und datenschutzrechtlich kritisch zu sehen.

8 Fazit

Das hier dargestellte Delikt des Romantikbetrugs mag im Kontext der Gesamtkriminalität gesehen eine eher marginale Rolle einnehmen. Gleichwohl verdeutlicht es exemplarisch einen wichtigen Punkt: Bei „Cybercrime" handelt es sich keineswegs immer um genuin neue Formen der Kriminalität, sondern es haben sich auch altbekannte Delikte (wie Diebstahl, Geldwäsche oder Pornographie) durch die Digitalisierung eine neue Plattform gesucht (Yar 2009). Dies gilt insbesondere für *„alle erdenklichen Modi Operandi des Betrugs"* (Priebe und Hartwig 2011). Grund dafür ist, dass das Internet es ermöglicht, die den „klassischen"

Betrugsmaschen zugrunde liegenden, erprobten Täuschungsmanöver auf ein globales Level zu skalieren. Gleichzeitig haben sich verschiedene Teilaspekte des Betrugs, etwa die Suche nach oder das Ausspähen von passenden Opfern, durch Massenkommunikation und virtuelle Selbstdarstellung immens erleichtert, während die Strafverfolgung durch die Anonymität im Netz sowie der globalen, grenzüberschreitenden Online-Kommunikation kaum Möglichkeiten hat (Button et al. 2014). Betrug und Täuschung werden so zu zentralen Herausforderungen in der Bekämpfung der Internetkriminalität, schließlich setzen sie an einem Punkt an, der sich nur sehr bedingt durch rechtliche Regelungen und technische Verfahren absichern lässt – den menschlichen Schwächen.

Literatur

Archer, A. K. (2017). "I made a choice": Exploring the persuasion tactics used by online romance scammers in light of cialdini's compliance principles. All Regis University Theses (823). https://epublications.regis.edu/theses/823. Zugegriffen: 12. Febr. 2018.

Aretz, W., Gansen-Ammann, D.-N., Mierke, K., & Musiol, A. (2017). Date me if you can. Ein systematischer Überblick über den aktuellen Forschungsstand von Online-Dating. *Z Sex-Forsch, 30*(01), 7–34. https://doi.org/10.1055/s-0043-101465.

Arora, P., & Scheiber, L. (2017). Slumdog romance. Facebook love and digital privacy at the margins. *Media Culture & Society, 39*(3), 408–422. https://doi.org/10.1177/0163443717691225.

Boateng, R., Longe, O., Stephen Isabalija, R., Budu, J., & Foundation Ghana, P. (2011). Sakawa -Cybercrime and criminality in Ghana. *Journal of Information Technology Impact, 11*(2), 85–100. https://www.researchgate.net/publication/265446452_Sakawa_-Cybercrime_and_Criminality_in_Ghana. Zugegriffen: 30. Apr. 2018.

Buchanan, T., & Whitty, M. T. (2014). The online dating romance scam: Causes and consequences of victimhood. *Psychology, Crime and Law, 20*(3), 261–283. http://www.scopus.com/inward/record.url?eid=2-s2.0-84893921823&partnerID=40&md5=883a89518bca17c153d83232b5864f98.

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds. Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology, 47*(3), 391–408. https://doi.org/10.1177/0004865814521224.

Carter, E. (2015). The anatomy of written scam communications. An empirical analysis. *Crime, Media, Culture, 11*(2), 89–103. https://doi.org/10.1177/1741659015572310.

Cassiman, A. (2018). Browsers and phone girls. The intricate socialities of friendship, trust and cyberlove in Nima (Accra). *Africa, 88*(S1), 72–89. https://doi.org/10.1017/s0001972017001152.

Cross, C. (2016). Using financial intelligence to target online fraud victimisation. Applying a tertiary prevention perspective. *Criminal Justice Studies, 29*(2), 125–142. https://doi.org/10.1080/1478601x.2016.1170278.

Ellis, S. (2016). *This present darkness. A history of Nigerian organised crime*. London: Hurst & Company.

Fischer, P., Lea, Stephen E. G., & Evans, K. M. (2013). Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance. *Journal of Applied Social Psychology, 43*(10), 2060–2072. https://doi.org/10.1111/jasp.12158.

Freiermuth, M. R. (2011). Text, lies and electronic bait: An analysis of email fraud and the decisions of the unsuspecting. *Discourse & Communication, 5*(2), 123–145. https://doi.org/10.1177/1750481310395448.

Füllgrabe, U. (2015). (Online-) Heiratsschwindel und andere Beziehungsfallen. *Kriminalistik, 69*(8–9), 487–493. Zugegriffen: 14. Dez. 2017.

Gillespie, A. A. (2017). The electronic Spanish prisoner. *The Journal of Criminal Law, 81*(3), 217–231. https://doi.org/10.1177/0022018317702803.

Heubrock, D., & Böttcher, M.-H. (2011). Scamming – Betrug durch vorgetäuschte Heiratsabsichten in Internet-Partnerschaftsportalen. *Kriminalistik, 65*(2), 75–81.

Interpol, & Trend Micro. (2017). Cybercrime in West Africa. Poised for an Underground Market. https://documents.trendmicro.com/assets/wp/wp-cybercrime-in-west-africa.pdf?_ga=2.124475466.1999533346.1525266343-1117850583.1525266343. Zugegriffen: 2. Mai 2018.

Kaufmann, J.-C. (2011). *Sex@mour. Wie das Internet unser Liebesleben verändert* (1. Aufl.). Konstanz: UVK.

Kich, M. (2005). A rhetorical analysis of fund-transfer-scam solicitations. *Cercles, 14*, 129–142. Zugegriffen: 22. Febr. 2018.

Koon, T. H., & Yoong, D. (2013). Preying on lonely hearts. A systematic deconstruction of an internet romance scammer's online lover persona. *Journal of Modern Languages, 23*(1), 28–40. Zugegriffen: 21. Febr. 2018.

Kopp, C. (2016). Structural analysis of online romance scams by applying the transtheoretical model in conjunction with the theory of personal love stories. Federation university Australia. https://library.federation.edu.au/record=b2687776. Zugegriffen: 12. Febr. 2018.

Kopp, C., Layton, R., Sillitoe, J., & Gondal, I. (2015). The role of love stories in romance scams: A qualitative analysis of fraudulent profiles. *International Journal of Cyber Criminology; ISSN: 0974–2891, 9* (9), 205–217. Zugegriffen: 12. Febr. 2018.

Kopp, C., Sillitoe, J., Gondal, I., & Layton, R. (2016). The online romance scam: A complex two-layer scam. *Journal of Psychological and Educational Research, 24*(2), 144–161.

Kopp, C., Sillitoe, J., & Gondal, I. (2017). "I am your perfect online partner". analysis of dating profiles used in cybercrime. *APJABSS, 3*(2). doi: https://doi.org/10.25275/apjabssv3i2ss5.

Marx, K. (2012). Liebesbetrug 2.0 – Wie emotionale Illusionen sprachlich kreiert werden. In M. Iakushevich & A. Arning (Hrsg.), *Strategien persuasiver Kommunikation* (S. 147–165). Hamburg: Kovač. (Schriftenreihe Philologia, 168).

Marx, K., & Rüdiger, T.-G. (2017). Romancescamming. Eine kriminologisch-linguistische Betrachtung. *Kriminalistik, 71*(4), 211–218.

Oduro-Frimpong, J. (2011). Sakawa: On occultic rituals and cyberfraud in ghanaian popular cinema. Working paper presented to the Media anthropology network e-seminar european association of social anthropologists, 18 Jan- 1 Feb 2011. http://www.media-anthropology.net/file/frimpong_rituals_cyberfraud.pdf. Zugegriffen: 12. Apr. 2018.

Oduro-Frimpong, J. (2014). Sakawa Rituals and Cyberfraud in Ghanaian Popular Video Movies. *African Studies Review, 57*(02), 131–147. https://doi.org/10.1017/asr.2014.51.

Ojedokun, U. A., & Eraye, M. C. (2012). Socioeconomic lifestyles of the yahoo-boys: A study of perceptions of university students in Nigeria. *International Journal of Cyber Criminology; ISSN: 0974–2891, 6*(2), 1001–1013.

Priebe, R., & Hartwig, M. A. (2011). Internet-Kriminalität – Cyberkriminalität und die neue Strategie der inneren Sicherheit für die Europäische Union. *Kriminalistik 65*(2), 67–69.

Rege, A. (2009). What's love got to do with it? Exploring online dating scams and identity fraud. *International Journal of Cyber Criminology; ISSN: 0974–2891, 3*(2), 494–512. http://www.cybercrimejournal.com/AunshulIJCCJuly2009.pdf. Zugegriffen: 16. Mai 2013.

Rüdiger, T.-G. (2012). Cybergrooming in virtuellen Welten – Chancen für Sexualtäter? *Deutsche Polizei. Zeitschrift der Gewerkschaft der Polizei, 61*(2), 29–35.

Schwartz, V. (2015). *Wie meine Internet-Liebe zum Albtraum wurde. Das Phänomen Realfakes* (2. Aufl.). München: Blanvalet.

Sternberg, R. J. (1995). Love as a story. *Journal of Social and Personal Relationships, 12*(4), 541–546. https://doi.org/10.1177/0265407595124007.

Toma, C. L. (2017). Developing online deception literacy while looking for love. *Media, Culture and Society, 39*(3), 423–428. https://doi.org/10.1177/0163443716681660.

Walther, J. B. (1996). Computer-mediated communication. *Communication Research, 23*(3), 3–43. https://doi.org/10.1177/009365096023001001.

Warner, J. (2011). Understanding cyber-crime in ghana: A view from below. *International Journal of Cyber Criminology; ISSN: 0974–2891, 5*(1), 736–749. http://cybercrimejournal.com/warner2011ijcc.pdf. Zugegriffen: 30. Apr. 2018.

Whitty, M. T. (2013). The scammers persuasive techniques model. Development of a stage model to explain the online dating romance scam. *British Journal of Criminology, 53*(4), 665–684. https://doi.org/10.1093/bjc/atz009.

Whitty, M. T. (2015). Anatomy of the online dating romance scam. *Security Journal, 28*(4), 443–455. https://doi.org/10.1057/sj.2012.57.

Whitty, M. T. (2018). Do you love me? Psychological characteristics of romance scam victims. *Cyberpsychology, Behavior and Social Networking, 21*(2), 105–109. https://doi.org/10.1089/cyber.2016.0729.

Whitty, M. T., & Buchanan, T. (2012). The online romance scam. A serious cybercrime. *Cyberpsychology, Behavior and Social Networking, 15*(3), 181–183. https://doi.org/10.1089/cyber.2011.0352.

Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam. The psychological impact on victims – both financial and non-financial. *Criminology & Criminal Justice, 16*(2), 176–194. https://doi.org/10.1177/1748895815603773.

Yar, M. (2009). The Novelty of „Cybercrime". An Assesment in Light of the Routine Activity Theory. In G. Furst (Hrsg.), *Contemporary readings in criminology* (S. 47–55). Los Angeles: SAGE (Contemporary readings series).

Zillmann, D., Schmitz, A., & Blossfeld, H.-P. (2011). Lügner haben kurze Beine. Zum Zusammenhang unwahrer Selbstdarstellung und partnerschaftlicher Chancen im Online-Dating. *Zeitschrift für Familienforschung, 23*(3), 291–318.

Hate Speech in der Computerspielkultur

Affinitätsräume als Ort der Diskriminierung und Ausgrenzung?

Sonja Gabriel

1 Hate Speech – ein Definitionsversuch

Hate Speech (auf Deutsch auch Hassrede) ist ein Begriff, der durch die starke Verbreitung unterschiedlicher sozialer Medien in den letzten Jahren stark an Präsenz gewonnen hat. Sucht man nach einer Definition von Hate Speech, so wird schnell deutlich, dass es auch hier noch keine endgültige Einheitlichkeit gibt. Bereits 1997 hat sich das Ministerkomitee des Europarats mit Hassrede beschäftigt und eine Empfehlung dazu verabschiedet. In dem Papier wird Hatespeech folgendermaßen definiert:

> „Jegliche Ausdrucksformen, welche Rassenhass, Fremdenfeindlichkeit, Antisemitismus oder andere Formen von Hass, die auf Intoleranz gründen, propagieren, dazu anstiften, sie fördern oder rechtfertigen, einschließlich der Intoleranz, die sich in Form eines aggressiven Nationalismus und Ethnozentrismus, einer Diskriminierung und Feindseligkeit gegenüber Minderheiten, Einwanderern und der Einwanderung entstammenden Personen ausdrückt.“ (Council of Europe 1997)

In dieser Definition stehen vor allem fremdenfeindliche Motive für Hassreden im Vordergrund, doch die Formulierung, dass auch *„andere Formen von Hass, die auf Intoleranz gründen“* darin inkludiert werden, macht diese Definition ebenfalls für Diskriminierung aufgrund von sexueller Orientierung, psychischer oder physischer Behinderung oder Zugehörigkeit zu einer bestimmten sozialen Klasse passend, wie dies auch später in einer Publikation der OSCE ausdrücklich aufgenommen

S. Gabriel (✉)
KPH Wien/Krems, Wien, Österreich
E-Mail: sonja.gabriel@kphvie.ac.at

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

T.-G. Rüdiger und P. S. Bayerl (Hrsg.), *Cyberkriminologie,*
https://doi.org/10.1007/978-3-658-28507-4_11

wird (Mihajlova et al. 2013). Die No Hate Speech Kampagne schlägt folgende Definition vor:

> „Als Hassrede bezeichnen wir sprachliche Handlungen gegen Einzelpersonen und/oder Gruppen mit dem Ziel der Abwertung oder Bedrohung aufgrund ihrer Zugehörigkeit zu einer benachteiligten Gruppe in der Gesellschaft. Die Person oder Gruppe muss dafür rein zahlenmäßig nicht in der Minderheit sein, andersherum sind Minderheitengruppen nicht automatisch benachteiligt.“ (No-Hate-Speech.de o. A.)

Es gibt allerdings einige Merkmale, die in allen Definitionen gleich sind bzw. zumindest ansatzweise vorkommen. Dazu gehören:

- Hate-Speech umfasst sprachliche Angriffe (mündlich oder schriftlich) bzw. die Verwendung von Bildern (Memes[1])
- menschenverachtende Aussagen, die bewusst getätigt werden
- Ziel ist die Abwertung von Gruppen aufgrund ihrer Hautfarbe, Herkunft, Sexualität, Geschlecht, Alter, Religion, Behinderung, Zugehörigkeit zu einer bestimmten Gesellschaftsschicht oder Berufsgruppe
- Betroffene definieren, ob eine Aussage zu Hassrede zählt oder nicht

Die Muster von Hate Speech sind sehr vielfältig und können von der bewussten Verbreitung falscher Aussagen, die auch als Humor oder Ironie getarnt sein können, über herabwürdigende Begriffe und Beleidigungen bis hin zur Verbreitung von Stereotypen und Vorurteilen und Verschwörungstheorien reichen. Häufig werden zudem auch Verallgemeinerungen oder die sprachliche Unterteilung in „wir“ und „die“. Plakative Bildsprache oder auch Memes, die ebenfalls Stereotype reproduzieren und/oder Vorurteile verstärken, wird verwendet. Ebenso sind Gleichsetzungen, z. B. von Homosexualität mit pädosexueller Kriminalität, zu finden. Teilweise wird sogar zu Gewalt außerhalb der Online-Welt aufgerufen oder sexualisierte Gewalt befürwortet oder angedroht (Landesanstalt für Medien NRW et al. 2016).

[1]Memes sind eine Kombination aus Bildern mit Texten, die dadurch zu neuen Varianten von sich selbst werden. Diese Varianten werden – aufgrund von Selektionsprozessen – unterschiedlich stark in sozialen Netzwerken verbreitet und wieder verändert (Bülow 2004).

Gemäß Schmitt (2017) lassen sich die Gründe für Hate Speech auf zahlreiche Faktoren zurückzuführen, können aber grundsätzlich in vier Motivlagen grob eingeteilt werden. Dazu gehören:

- *Ausgrenzung:* Personen(gruppen) werden aus sozialen Netzwerken oder anderen Online-Gruppierungen ausgeschlossen. Innerhalb dieser Gruppen kommt es durch Hassrede zu verbalen Herabwürdigungen und somit zur gezielten Ab- und Ausgrenzung dieser Gruppen sowie zur Dehumanisierung, was die Hemmschwelle für physische Gewalt sinken lässt.
- *Einschüchterung:* Häufig fühlen sich Menschen durch andere Gruppen bedroht und versuchen durch die Verbalisierung ihres Hasses diese fremde Personengruppe einzuschüchtern. Die Interessen der eigenen Gruppe werden in den Fokus gestellt, während Angst, Zweifel und Konflikte gegen „die anderen" geschürt werden.
- *Dominanz und Deutungshoheit:* Die eigene Gruppe wird als gesellschaftlich und sozial überlegene Gruppe gesehen. Durch Hassrede werden andere Personengruppen abgewertet und zudem sollen auch weitere Personen dazu gebracht werden, die Einstellung der Hassredner*innen zu übernehmen.
- *Spaß und Nervenkitzel:* Durch die (vermeintliche) Anonymität des Internets kann es durchaus auch Personen geben, die weniger aufgrund ihrer Überzeugungen und Werten, sondern einfach aus Freude daran, andere Gruppen beleidigen und erniedrigen.

Besonders durch die Verbreitung von sozialen Netzwerken und verstärkter Kommunikationsmöglichkeiten über das Internet – so hat sich die Produzenten-/Konsumentenbeziehung verschoben, da Jede/r Inhalte konsumieren, aber auch produzieren kann – hat sich die Nachrichtenverbreitung stark verändert (Latour 2017).

2 Hate Speech und Online Games

Wie unterschiedliche Umfragen und Statistiken zeigen, erfreuen sich digitale Spiele bei Jugendlichen (Medienpädagogischer Forschungsverbund Südwest 2018) und Erwachsenen (Börner 2018) durchaus großer Beliebtheit und sind ein fixer Bestandteil in der Freizeit. Am meisten wird mittlerweile über das Smartphone gezockt (SPLENDID RESEARCH GmbH 2018). Besonders für Kinder und Jugendliche gilt das digitale Spiel mit all seinen Ausprägungen (Computer, Konsole, Mobilgeräte, etc.) als ein wesentliches (Leit-)Medium (Baldauf et al. 2015).

Durch verbesserte Internetverbindungen bzw. der Möglichkeit mobil online zu gehen nimmt auch die Zahl von Online-Games zu. Natürlich betrifft Hate Speech in und um Videospiele vor allem Multiplayergames, also jene Spiele, in denen das Miteinander- oder Gegeneinanderspielen über das Internet ein wesentlicher Bestandteil des Gameplays ist.[2] Besonders in Massively Multiplayer Online Role-Playing Games (MMORPG), also internetbasierten Computerspielen, in denen sich bis zu mehreren tausend Spielenden gleichzeitig aufhalten können, rückt aufgrund der stark komplexen Abläufe im Spiel die Kommunikation stark in den Vordergrund (Stertkamp 2017).

Mittels Avataren (also einer virtuellen Repräsentation der Spielerin/des Spielers) wird mit anderen Spielenden bzw. Non-Playable Charakteren (NPC – vom System gesteuerten Figuren) in der persistenten[3] virtuellen Spielwelt interagiert. Der erhöhte Kommunikationsbedarf ergibt sich in solchen Spielen (wie z. B. World of Warcraft) dadurch, dass gewisse Quests (Aufgaben) nur als Team bewältigbar sind. Dies bedeutet allerdings nicht, dass es nur die Online-Rollenspiele sind, die von Hassrede betroffen sind, da es mittlerweile zahlreiche onlinebasierte Spiele mit integrierten Kommunikationsmöglichkeiten gibt. Vor allem für Kinder und Jugendliche interessant sind Free-to-Play-Games, die vorwiegend über mobile Geräte spielbar sind. Laut JIM-Studie 2018 ist Fortnite das beliebteste Spiel bei 12- bis 17-Jährigen (Medienpädagogischer Forschungsverbund Südwest 2018). Auch jüngere Kinder nutzen das Smartphone als Spielekonsole (Medienpädagogischer Forschungsverbund Südwest 2019).

Gerade diese Kommunikationsmöglichkeiten, die in viele Online-Games integriert sind, bieten sich auch als idealen Nährboden für Hassrede. Diese Problematik ist mittlerweile so weit verbreitet, dass auch international immer mehr in den Medien darüber berichtet wird. So findet sich bereits 2010 auf der Webseite von NBC-News ein Artikel über Hate Speech in der Online-Version von *Call of Duty: „One gamer told an opponent he presumed to be Jewish that he wished Hitler had succeeded in his mission. Many exchanges involve talk of rape or exult over the atomic bombing of Japan. There are frequent slurs on homosexuals, Asians, Hispanics and women“* (Geraniols 2010). Aber auch Handlungen innerhalb von

[2]Lokale Multiplayerspiele (beispielsweise über Split-Screen) sind weniger von Hate Speech betroffen, da sich die Spieler*innen hier zumeist kennen bzw. sehen können.

[3]Unter einer persistenten Welt versteht man Online-Spiele, die jederzeit für Spielende zugänglich sind und die sich auch weiterentwickeln, wenn Spielende nicht eingeloggt sind bzw. sich nicht aktiv am Spielgeschehen beteiligen.

Online-Games werden verwendet, um andere Spielende zu erniedrigen oder ihnen eine Meinung aufzuzwingen:

> „Take the survival shooter game 'H1Z1: King of the Kill', currently the third-most-popular on the world's biggest online game platform. Matches in Asia are sometimes interrupted by the Red Army, a band of Chinese players who have won praise from local media for championing in-game nationalism. One tactic involves cornering rivals and forcing them to pay tribute to the motherland by saying 'China No. 1.' Those who fail to comply are swiftly dispatched." (Bloomberg 2017).

Besonders bekannt wurde die Thematik Hate Speech in und rund um Games durch die sogenannte Gamergate-Affäre. Die feministische Videobloggerin Anita Sarkeesian startete im Frühjahr 2012 eine äußerst erfolgreiche Kickstarter-Kampagne, um Geld zu sammeln, um eine Reihe von Videos über die Thematik weibliche Stereotype mit dem Titel *Tropes vs Women in Video Games*[4] zu erstellen. Bereits in der Finanzierungsphase wurde die Bloggerin sexistisch beschimpft, herabgewürdigt und ihr Gewalt angedroht. Sie sammelte alle diese Angriffe auf einer eigenen Webseite (Sarkeesian 2012). Es wurde aufgrund dieser sehr bipolaren Diskussion sogar ein Spiel entwickelt, in dem Spielende eine Figur nach dem Vorbild Sarkeesians zusammenschlagen konnten (Fernandez-Blance 2012). Unter #gamergate entflammte eine Diskussion, die weit über Spieleforen hinausging und auch in den Medien heftig diskutiert wurde (Freidel 2014).

Im englischsprachigen Raum wird häufig von „toxic environment" und „toxic game communities" (Liukkonen 2018) gesprochen. Gerade beim Spielen werden viele (negative) Emotionen freigesetzt, die sich dann in Kommentaren und Äußerungen anderen Mitspielenden gegenüber entladen können. In manchen Spielumgebungen sind beleidigende und herabsetzende Kommentare die Norm, obwohl diese Spieler*innen weder extreme politische Ansichten haben und sich selbst auch nicht als diskriminierend beschreiben würden. Häufig geben solche Gamer an, dass sie die Äußerungen ohnehin nicht so gemeint haben (Craker und March 2016; Hardaker 2010). Dazu kommt noch, dass – häufig anders als in sozialen Netzwerken – mit den anderen einfach Mitspielende gemeint sind, ohne dass diese einer bestimmten Gruppe angehören: *„Most importantly, the ‚other' is not* me *or* us, *the 'other' is the opposite of me. And in the mind of every gamer*

[4]Die Videos sind auf YouTube unter https://www.youtube.com/user/feministfrequency zu sehen.

who has ever engaged in toxic behavior, I am better than the 'other'" (Liukkonen 2018). Wie Breuer (2017) zudem feststellt, können auch Niederlagen in Online-Spielen negative Emotionen hervorrufen, wodurch eine höhere Wahrscheinlichkeit von aggressivem Verhalten gegeben ist:

> „Spieler*innen, die sich stark mit dem Hobby Online Games bzw. bestimmten Genres oder Spielen identifizieren, können die Anwesenheit von Personen, die anders sind als sie selbst (etwa im Hinblick auf Geschlecht, Ethnizität oder sexuelle Orientierung), auch als Bedrohung ihrer sozialen Identität wahrnehmen, wenn sie der Meinung sind, dass bestimmte Personengruppen keine ‚wahren/echten/richtigen' Gamer*innen sind." (ebd. S. 110)

Gruppen, die ihren Hass auf bestimmte andere Gruppen verbreiten wollen, nutzen Computerspiele unter anderem auch, indem sie diesen Hass in das Game-Design integrieren. So entstanden schon Anfang des 20. Jahrhunderts Computerspiele wie *Ethnic Cleansing* oder *Shoot the Blacks,* in denen bestimmte ethnische Gruppen das Ziel waren (Council of Europe 2012). Ein weiterer Faktor in der Verbreitung von Hate Speech ist das stärker werdende Interesse an E-Sport[5] und die große weltweite Verbreitung. Hierbei spielen vor allem Zuschauer*innen eine große Rolle. Erst im Februar 2019 sorgte ein Tweet eines dänischen *Counter-Strike*-Teams für Aufregung. In öffentlichen Chats bzw. in Direktnachrichten erhielten die Profispieler Nachrichten wie *„Ich hoffe, ihr sterbt alle"* (Krishan 2019), die vom Teamkapitän öffentlich gemacht wurden. 2018 begann die US-amerikanische E-Sportlerin Spawntaneous Videos zu veröffentlichen[6], die einen Einblick darin geben, mit welchen Aussagen weibliche Gamer ständig konfrontiert werden. Dies reicht von Ausrufen wie *„Oh mein Gott, ein Mädchen!"* bis hin zu aufdringlichen Flirt-Versuchen, der Aufforderung Nacktfotos zu schicken bis hin zu sexistischen Klischees oder Vergewaltigungsandrohungen. Dies hatte zur Folge, dass besonders auch im Bereich E-Sport die Thematik Hassrede medial Beachtung fand und diskutiert wurde.

[5]Unter E-Sport versteht man im Allgemeinen, dass sich E-Sportler wettbewerbsmäßig mit Hilfe von Computerspielen messen. Zumeist wird der Wettkampf im Mehrspielermodus (als Individual- oder Mannschaftssport) ausgetragen. Die Regeln werden einerseits durch das Spiel selbst, aber auch durch extern festgelegte Wettkampfbestimmungen festgelegt.

[6]Die Videos sind auf YouTube unter OMG A GIRL Series zu finden. https://www.youtube.com/playlist?list=PLEDsO12Ccv9ES1Qlnwu_Gi72udJyhVXyZ.

3 Affinititätsräume

Affinititätsräume, so wie sie von Gee und Hayes (2012) definiert werden, sind Orte, wo sich Personen aufgrund eines gemeinsamen Interesses oder einer gemeinsamen Aktivität freiwillig zu Gruppen zusammenfinden. Diese Räume können sich durchaus auch online befinden, z. B. innerhalb von Game-Communities. Das Zusammengehörigkeitsgefühl wird dabei nicht aufgrund von Herkunft, sozialem Hintergrund, Ethnie oder Geschlecht bestimmt, sondern vorwiegend aufgrund der gemeinsamen Interessen, Ziele und Aktivitäten. Es findet dort auch der Austausch und Aufbau von Wissen bzw. Fertigkeiten statt (Gee 2013, 2017). Für manche Personen fungieren besonders Online-Rollenspiele als sogenannter dritter Ort, der neben Heim und Arbeitsplatz einen Raum bietet, den man freiwillig wählt und mit dem man sich identifiziert. Diese Orte vermitteln ein Gefühl des Zuhauses und dienen dem Stressabbau bzw. der Flucht aus dem Alltag. Kommunikation spielt eine große Rolle (Ducheneaut et al. 2007).

Inhalte in Affinitätsräumen entstehen vor allem durch soziale Interaktionen und Tätigkeiten in diesem sozialen Raum (Hudson et al. 2016):

> „This whole set of physical and virtual spaces (and the physical and digital routes among them) that characterize the comings and goings of gamers with a shared affinity is an affinity space. These sorts of affinity spaces today are often really squishy. They are fluid and ever changing and hard to strictly demarcate.“ (Gee 2017, S. 29)

Partizipation kann auf unterschiedliche Formen und Arten stattfinden; es gibt keine fix definierten Leader dieser Gruppen und den Status erreichen Mitglieder durch verschiedene Aktivitäten (Gee 2004).

Das bedeutet also, dass sowohl Online-Spiele als auch die Foren und Community-Angebote rund um Computerspiele (wie z. B. Let’s Play-Kanäle) unter die Definition von Affinitätsräume fallen. Darunter fallen auch Dienste wie beispielsweise *Discord*[7] oder die Community rund um den Spiele-Online-Vertrieb *Steam.* Hier tauschen sich Gleichgesinnte zu Spielstrategien, Spielerlebnissen und Ähnlichem aus bzw., wenn es um Kommunikation im Spiel geht, vor allem über die aktuelle Spielsituation und die Rollen im Team, aber auch über Alltagsthemen. Diese Affinitätsräume, die grundsätzlich Lernen und Austausch

[7]Discord ist eine Chat-App für alle Plattformen, die sowohl Privat-Chats, aber auch Gruppen-Chats und Voice-over-IP Gespräche umfasst. Zudem kann die App auch in Online-Spiele integriert werden.

begünstigen, können aber durchaus auch Orte sein, an denen Hate Speech in unterschiedlicher Form entsteht und weitergetragen wird (Moor et al. 2010).

Ziele der Ausgrenzung sind in Online-Spielen neben den allgemein betroffenen Gruppen wie Frauen, Angehörige anderer Kulturen und Religionen vor allem auch unerfahrene Spieler*innen. Eine Studie, die das bekannte Massively Multiplayer Online Rollenspiel *World of Warcraft* betrifft, fand heraus, dass die Community hier vor allem feindlich gegenüber Homosexuellen, Bisexuellen und Transgendern eingestellt ist (Pulos 2013). Eine weitere Untersuchung, die Xbox Live Community betreffend, fand heraus, dass vor allem farbige Frauen, die über Voice-Chat im Spiel mit ihren Teammitgliedern kommunizieren, von Hate Speech betroffen sind (Gray 2016). Dieses Verhalten bewirkt, dass sich Frauen oft nicht als Gamer verstehen, da die Identität und Gruppenzugehörigkeit stark männlich definiert ist (Groen 2017). Verstärkt wird dieses Gefühl vor allem auch durch die Inhalte und Darstellung von Frauen in digitalen Spielen – zumeist werden diese stark sexualisiert und hilflos dargestellt (Chenelle 2019). Das Design von Spielen kann durchaus dazu führen, dass Hate Speech in Computerspielumgebungen eher akzeptiert wird als in anderen Bereichen (Rogers 2016).

Zudem sind im jeweiligen Game unerfahrene Spielende häufig Opfer von Hassrede. Da Spielen immer mit Emotionen verbunden ist, kann es hier leicht zu verbalen Übergriffen kommen, wenn Spielende aufgrund ihrer Unerfahrenheit oder Ungeschicklichkeit durch eine Aktion setzen, die dazu führt, dass eine Team-Aufgabe nicht bewältigt wird. Trotzdem ist hier eine deutliche Grenze zu ziehen zwischen einem emotionalen Ausbruch und Hate Speech. In manchen Fällen führt dies sogar zu Drohungen, Stalking oder verschiedenen Formen von Griefing.[8] Extreme Ausprägungen von Online-Hostility können sogar die Grenzen des Online-Spiels verlassen. Das bedeutet, dass Opfer in sozialen Netzwerken (z. B. Facebook oder Twitter) belästigt werden.

Neben Hate Speech in Form von verbalen Äußerungen über Chat- oder Voice-over-IP-Kommunikation findet sich eine indirekte Form von Diskriminierung. Indem Spieler*innen einen Spieler- oder Gildennamen wählen, der absichtlich abwertend ist, bringen sie ihre Abneigung gegen gewisse Gruppen zum Ausdruck. So gab es beispielsweise im auch bei Kindern und Jugendlichen beliebten Spiel *Clash Royale* (Supercell) eine Reihe antisemitischer oder rassistischer Gildennamen (Diver

[8]Unter Griefer versteht man Spieler*innen in einem Multiplayer-Spiel, der durch seine gesetzten Maßnahmen versucht, anderen den Spaß am Spiel zu verderben. Dies kann durch Spielbehinderung (z. B. Blockieren von Ausgängen), Belästigung oder einer Art Stalking passieren. Griefer bewegen sich dabei immer im Rahmen der Spielregeln.

2016). Namen wie „jews HHiittler didnt do anything wrong“ oder „burn blacks“ sind zu finden. Vor allem das Hinzufügen oder Weglassen von Buchstaben führt dazu, dass automatische Filter, die zahlreiche Spieleanbietern einsetzen, umgangen werden können. In manchen Fällen können solche Namen gemeldet werden und die betroffenen Spieler*innen werden sanktioniert, doch das ist noch nicht durchgängig der Fall und bedingt vor allem ein Aktivwerden durch die Spieler*innen selbst. Besonders auch die Kommunikations-Plattform Discord sieht sich Vorwürfen konfrontiert, dass sie zu wenig gegen Chat-Kanäle und Gruppen unternehmen, die rechtes, rassistisches oder anti-semitisches Gedankengut verbreiten oder auch gegen User, deren Benutzernamen eindeutig in die Kategorie Hate-Speech fallen (Sinclair 2018).

Einen besonderen Fall von Hate Speech sind Spieler*innen von *Red Dead Redemption 2* ausgesetzt, die als Charakter einen Afro-Amerikaner auswählen. Nicht nur, dass diese Avatare öfters innerhalb der Open-World-Spielwelt angegriffen werden, es werden in Kommunikationen Begriffe wie „Nigger“ durchgängig von anderen Spieler*innen verwendet: *„Another player, who is white but says he often makes black in-game characters to add ‚diversity‘ to his friend group, told The Verge that every single time he kills someone in Red Dead Online, he gets called the n-word.“* (Hernandez 2019). Auch in der Gaming-Community, wo gerne ausprobiert wird, was in Open-World-Spielen alles möglich ist, zeigt dieses Spiel seltsame Beispiele – so gibt es einen YouTuber, der ausprobiert, ob man eine Feministin einem Alligator zum Fraß vorwerfen kann oder was passiert, wenn man einen Afro-Amerikaner zu Mitgliedern des KuKlux Klan bringt (Hernandez 2019). Solche Videos verzeichnen millionenfache Zugriffe. Gerade Let’s Play-Video-Ersteller*innen lassen sich des Öfteren zu rassistischen Spielhandlungen oder Äußerungen hinlassen – teilweise wohl auch, um in Diskussion zu bleiben und eventuell noch mehr Views für die eigenen Videos zu erhalten. 2017 machten die antisemitischen Hassparolen des bis dahin erfolgreichsten YouTubers der Welt, PewDiePie, international Schlagzeilen (Nowak 2017). Ein Twitch-Streamer, MontanaBlack, wurde von der Plattform 2018 für zwei Monate gesperrt, nachdem er rassistische Kommentare live äußerte (Sidorov 2018).

Die Gründe für Hate Speech sind dabei vielfältig – vor allem verhilft die vermeintliche Anonymität im Internet, dass Personen, die im realen Leben vielleicht anders agieren würden, sich trotzdem zu rassistischen oder diskriminierenden Äußerungen hinreißen lassen. Da die virtuelle Persönlichkeit von der realen oft getrennt wird, erwarten die Verursacher von Hasskommentaren keine realweltlichen Konsequenzen für die menschenverachtenden Äußerungen. Begünstigend wirkt sich zudem auch noch aus, dass in Online-Spielen ein größeres Publikum zugegen ist – besonders dann, wenn diese Zuseher*innen nicht eingreifen oder Partei für das Opfer ergreifen (Breuer 2017).

4 Gegenbewegungen und Gegenmaßnahmen

Sich gegen Hate Speech zu wehren bzw. Gegenmaßnahmen zu ergreifen, ist kein einfaches Unterfangen, da die Situationen häufig voneinander abweichen und es keine allgemeingültige Lösung gibt. Unterschieden kann jedoch werden zwischen Maßnahmen, die ein Individuum treffen kann, und jene, die von einem Plattform-Anbieter eingeführt werden können.

4.1 Strategien auf individueller Ebene

Die Webseite *Take Back the Tech* listet beispielsweise folgende mögliche Strategien auf, die man anwenden könnte, wenn man Hate Speech ausgesetzt ist (Take Back the Tech o. A.):

- *Ignorieren:* Wenn immer es möglich ist, sollten Hater ignoriert oder blockiert werden. In vielen Online-Spielen, die auf Kommunikation unter den Spieler*innen basieren, gibt es die Möglichkeit, einzelne davon stumm zu schalten (mute). Das bedeutet, dass die Verursacher*innen von Hate Speech keine Aufmerksamkeit mehr erhalten. Allerdings besteht auch die Gefahr, dass diese Debatten von anderen aufgegriffen werden und daher immer mehr Spieler*innen ignoriert werden müssen.
- *Melden:* Zahlreiche soziale Netzwerke, aber auch andere Webseiten sowie teilweise auch Online-Games bieten mittlerweile eigene Buttons oder Kontaktmöglichkeiten, mittels derer Verhalten, das nicht den Umgangsregeln entspricht, zu melden.
- *Bloßstellen:* Vor allem, wenn es eine Community rund um ein Spiel oder eine Webseite gibt, sollte jegliche Form von Hate Speech aufgezeigt werden. Damit werden nicht nur andere User gewarnt, sondern die Verursacher*innen der Hate Speech eventuell auch zum Nachdenken über ihr Verhalten angeregt. So gibt es beispielsweise in der Community rund um das Spiel *Grand Theft Auto* immer wieder Hinweise von einzelnen Spieler*innen über das Fehlverhalten anderer, die dann auch zu Diskussionen und Kommentare anderer führen[9].
- *Miteinbeziehen:* Indem man das Verhalten von Hate Speech Verursacher*innen thematisiert und ihnen auch Gelegenheit gibt, ihre Handlungsweise bzw.

[9]Siehe beispielsweise https://support.rockstargames.com/community/200063373/360002990988.

Motivation darzulegen, kann ebenfalls eine Diskussion entfacht werden, die aufzeigt, dass viele User mit Hate Speech nicht einverstanden sind.

- *Unterstützung suchen:* Wenn man von Hate Speech betroffen ist, kann es hilfreich sein, wenn man merkt, dass man nicht alleine ist. Es gibt andere, die genauso betroffen sind und viele, die Hate Speech nicht gutheißen. Daher wird geraten, etwas gegen Hate Speech zu unternehmen.
- *Anonym bleiben:* Gerade wenn man in Online-Welten unterwegs ist, kann es auch durchaus helfen, einen möglichst neutralen Namen für seinen Avatar auszuwählen, der keine Rückschlüsse auf die eigene Herkunft, Geschlecht, Religion, etc. zulässt. Damit wird eine bestimmte Distanz zwischen der Online-Identität und dem realen Ich geschaffen.
- *Sich nicht unterkriegen lassen:* Hater haben dann gewonnen, wenn sie es schaffen, eine Person aus einer bestimmten Umgebung (z. B. einem Online-Spiel) zu vertreiben. Sie merken dann, dass sie mit ihren Methoden Erfolg haben. Daher ist es von Bedeutung, Durchhaltevermögen zu zeigen.

In den letzten Jahren haben vor allem weibliche Gamer begonnen, das Verhalten einiger männlicher Mitspieler aufzuzeigen und haben damit eine Diskussion angestoßen, die auch außerhalb der Spiele fortgeführt wird und dazu führt, dass aufgrund von Gamegate digitale Spiele in völlig neuem Licht gesehen werden (Mortensen 2018). Allerdings greift individuelles Handeln immer noch zu kurz, es sind auch die Betreiber von Plattformen und Online-Spielen gefordert, hier Aktivitäten zu setzen, um ein Ausufern von Hate Speech und damit eine Vergiftung der Spieleratmosphäre zu verhindern.

4.2 Der Umgang von Plattformen und Online-Spiele-Anbietern mit Hate Speech

In vielen Communities und Online-Netzwerken gibt es den Community Code of Conduct – also eine Sammlung von Regeln und Verhaltensweisen, wie man sich im Netzwerk bzw. im Spiel verhalten soll, die mittlerweile auch explizit Hate Speech erwähnen. So heißt es beispielsweise im Community Code of Conduct des Playstation-Netzwerks:

> „You may not abuse or harass others, including stalking behavior. You may not take any action, or upload, post, stream, or transmit any content, language, images or sounds in any forum, communication, public profile, or other publicly viewable areas or in the creation of any Online ID that SIE LLC or its affiliates find, in their

> sole discretion, offensive, hateful, or vulgar. This includes any content or communication that SIE LLC or its affiliates deem racially, ethnically, religiously or sexually offensive, libelous, defaming, threatening, bullying or akin to stalking. You may not organize hate groups.“ (Sony 2019b)

In diesem Verhaltenskodex werden also dezidiert Verhaltensweisen, die der Definition von Hate Speech unterliegen, als Verstoß bezeichnet. Es gibt allerdings keine eindeutige Aussage, was passiert, wenn gegen den Community Code of Conduct verstoßen wird – hier wird nur sehr allgemein darauf verwiesen, dass sich Sony das Recht vorbehält, Aussagen und Nachrichten ohne vorherige Ankündigung zu löschen bzw. Konten vorübergehend oder für immer zu sperren. In den FAQs wird allerdings Hate Speech ausdrücklich als einen Grund für eine Sperre des Nutzerkontos aufgeführt (Sony 2019a).

Auch andere Online-Spiele bzw. Communities rund um digitale Spiele verfügen über einen Code of Conduct, der sich im Regelfall ebenfalls auf Hate Speech bezieht. Beispielsweise heißt es im Verhaltenskodex des beliebten Online-Rollenspiels *Dungeons and Dragons:*

> „You may not use or distribute sexually explicit, harmful, threatening, abusive, defamatory, obscene, hateful, racially or ethnically offensive language (including, by way of example, but not limited to, ethnic slurs and religious epithets), content, character names, titles, descriptions, or in-game labels (including, by way of example, but not limited to, offensive or inappropriate guild names, pet names and inscriptions). You may not distribute or spotlight sexually explicit, harmful, threatening, abusive, defamatory, obscene, hateful, racially or ethnically offensive content.“ (Standing Stone Games LLC 2017)

Konsequenzen gegen den Verstoß dieser Richtlinien werden ebenfalls – je nach Ermessen des Plattformbetreibers – ermahnt oder (vor allem bei ernsthaften oder wiederholten Verstößen) temporär oder permanent vom Spiel ausgeschlossen. Spielcharaktere oder Spielkonten können sogar ohne vorherige Warnung gelöscht werden. Zudem werden alle Kommunikationen innerhalb des Spiels (auch private Chats) mitprotokolliert, um im Zweifelsfall darauf zurückzugreifen.

In anderen Online-Spielen, wie beispielsweise dem beliebten *Fortnite Battle Royale* (Epic Games), gibt es innerhalb des Games eine Möglichkeit, Hate Speech und Spieler*innen, die diese verwenden, mithilfe eines Systems innerhalb des Spiels zu melden (Ditch the Label 2019). Noch einen Schritt weiter gehen die Betreiber von *Rainbow Six Siege*[10]: Seit Juli 2018 werden Spielende automatisch

[10]*Rainbow Six Siege* ist ein taktischer Ego-Shooter aus der Computerspielserie von Ubisoft. Hier ist der Fokus vor allem auf den Mehrspieler-Modus ausgelegt.

für einen kurzen Zeitraum gesperrt, wenn sie rassistische oder homophobische Äußerungen im Text-Chat verwenden (Park 2018). Angekündigt wurden diese und ähnliche Maßnahmen schon im Blog des Entwicklers etwas früher, da sich Ubisoft gezwungen sieht, etwas gegen die steigende Toxicity zu unternehmen: *„Our end goal ist to track negative player behavior, manage those that behave poorly, and eventually implement features that will encourage players to improve their behavior“* (Ubisoft 2018).

Trotz all dieser Maßnahmen, die mittlerweile von allen renommierten Anbietern von Online-Spielen in ihren Nutzungsbedingungen aufgenommen wurden, finden sich in vielen Foren zahlreiche Beiträge von Spieler*innen, die zeigen, dass Hate Speech dennoch ein großes Problem ist, das nicht einfach dadurch bekämpft werden kann, weil es als unerwünschtes Verhalten bezeichnet wird. Zudem kann auch durchaus finanzielles Interesse von Spiele-Providern vorrangig gegenüber den Schutz der Community eingestuft werden, wie ein Games-Moderator berichte: Da ein Gamer, der zwar ständig anderer Spieler*innen im Game terrorisierte, allerdings den Betreibern Geld einbrachte, wurde nur im Chat stummgeschalten, aber nicht aus dem Spiel verbannt (Williams 2018).

Das Auftreten von Hasskommentare führt unter Umständen sogar dazu, dass Spielende Abstand davon nehmen, eine Online-Community noch weiter zu nutzen, wie das Beispiel aus der *League of Legends* Community zeigt. Ein User postet hier beispielsweise das Folgende:

> „I'm tired of playing games and getting harassed by people. If the internet was properly policed most of your community would be rotting in jail for hate crimes. I'm tired of it. I shouldn't have to mute players every game I play. I shouldn't have to deal with the homophobic and racial slurs. Reporting players does nothing because they'll simply make a new account and keep harassing other players. I can't just play a game, and have fun? I have to be harassed and hazed for simple mistakes. I just want to play a game – but if I make even the simplest mistake I get bombarded with BULLSHIT. Delete this post Riog, idgaf. I'm done with your toxic community, and I'm done with your piss-poor policies that commend this sort of behavior.“[11]

Wie aus diesem Posting erkennbar wird, sind Spielende nicht wirklich zufrieden damit, wie die Betreiber von Online-Spielen bzw. den dazugehörigen Foren

[11]Forumposting aus dem Forum des Online-Games League of Legends (Riot Games), ein Free to Play Multiplayer Spiel, in dem Spielende in Teams gegeneinander kämpfen. (Quelle des Postings: https://boards.na.leagueoflegends.com/en/c/player-behavior-moderation/xnEKAVJo-homophobic-slurs-every-game-im-done).

mit Hate Speech umgehen. In zahlreichen Postings wird ein härteres Durchgreifen bzw. auch Überwachen der Kommunikation im Spiel verlangt, damit verletzende und diskriminierende Nachrichten nicht unentdeckt und vor allem nicht ungestraft bleiben. Zudem wird, wie auch aus obenstehendem Zitat erkennbar, die Macht- und Hilflosigkeit gegenüber den Verursachern von Hasspostings verdeutlicht, da selbst das Sperren oder Löschen eines Accounts vonseiten der Betreiberwebseiten nicht bedeutet, dass Hassredner mit ihren Aktionen aufhören. Daher wird der Funktion „Hate Speech melden", die es mittlerweile in zahlreichen Spielen bzw. Communities gibt, nicht viel Bedeutung beigemessen: *„And then he ended the conversation by telling me that he has 22 accounts and if I try to report him for threatening to kill me then he will create 6 more accounts to harass me. He said something like 'cut one head off and 6 more will grow back'"*.[12] Das Problem besteht häufig auch darin, dass schriftliche Äußerungen (z. B. in Chats oder Foren) gemeldet werden können, bei Voice-Chats fällt die Beweislage schon wesentlich schwieriger aus. Auch Spieler*innen- oder Gilden-Namen können nicht immer einfach über eine In-Game-Funktion gemeldet werden. So ist diese Funktion beispielsweise bei *Fortnite* im Feedback-Menü gut versteckt (Knoop 2018).

Die Diskussionen, die sich aus solchen oder ähnlichen Postings (wo beispielsweise Spieler*innen aufzeigen, mit welchen Formen von Hate Speech sie im Spiel konfrontiert waren) entwickeln, zeigen ein vielfältiges Spektrum von jenen, die Hate Speech verurteilen und striktes Vorgehen gegen die Verursacher fordern bis hin zu jenen, die meinen, dass die Betroffenen nicht so sensibel darauf reagieren sollten – das sei eben ein Teil des Spiels. Anhand der vielen Forumpostings und den Emotionen, die hier vor allem in den Argumentationen freigesetzt werden, ist zu erkennen, dass die Thematik der Hassrede viele betrifft und die Meinungen dazu hier oft unterschiedliche Positionen aufzeigen. Objektive Argumentation ist eher selten – es werden teilweise zwar auch Gesetze zitiert, um zu zeigen, in welchem Ausmaß hier auch illegal gehandelt wurde, zumeist werden aber eigene Erfahrungen oder Erfahrungen von Bekannten (auch außerhalb von Online-Spielen) geschildert. Teilweise wird auch die technische Ebene diskutiert, wie beispielsweise, ob jemand anhand seiner IP-Adresse lokalisiert werden kann, auch wenn er/sie über ein öffentlich zugängliches W-LAN in das Spiel eingeloggt war. In Einzelfällen kann allerdings auch die Community jemanden davon

[12]Forumposting aus dem Forum des Online-Games League of Legends. (Quelle des Postings: https://boards.na.leagueoflegends.com/en/c/player-behavior-moderation/FIqJTvdp-i-received-a-death-threat-from-a-post-i-made-here-in-player-behavior).

überzeugen, dass seine/ihre Kommentare nicht den Regeln entsprechen und es kommt zu Entschuldigungen im Forum.[13]

Den Betreibern der Online-Plattformen sind diese negativen Auswüchse wie Hate Speech durchaus bekannt. So versprach Phil Spencer, Verantwortlicher für die Xbox bei Microsoft, Maßnahmen gegen die steigenden Online-Gewalt auf der Spielplattform zu unternehmen. Dazu wurden bereits die Xbox Community Standards aktualisiert und Maßnahmen, die auf verstärkte Sicherheitsmaßnahmen abzielen, angekündigt (Shanley 2019). Hier bleibt abzuwarten, welche Maßnahmen genau gesetzt werden und ob dadurch das Phänomen Hate Speech eingedämmt werden kann.

Gefordert ist natürlich auch die politische Ebene – die Thematik Hate Speech wird in Europa derzeit noch vollkommen unterschiedlich gehandhabt. So gibt es beispielsweise in Österreich noch keine Rechtsdefinition von Hasskriminalität und es gilt auch nicht als eigener Straftatbestand. Vor allem digitale Spiele nehmen hier nochmal eine Sonderstellung ein. Als 2018 das Netzdurchwirkungsgesetz in Deutschland, das Hassinhalte im Internet eindämmen soll, in Kraft trat, waren Online-Spiele nicht darin inkludiert, obwohl sie in einem ersten Entwurf des Gesetzes enthalten waren (Brause 2018). Auch der Jugendmedienschutz geht bei der Alterseinstufung von Spielen nicht nach dem Potenzial von Hate Speech, sondern nach den Inhalten der Spiele, der Grafik, der im Spiel von Spielcharakteren verwendeten Sprache, etc. vor. Dies wirft natürlich die Frage auf, wie man gerade Kinder und Jugendliche davor bewahren kann, derartigen Hasskommentaren ausgesetzt zu werden.

5 Fazit

Hate Speech ist in Online-Spielen und in Communities rund um digitale Spiele ein wachsendes Problem. Gruppen, die auch im realen Leben von Ausgrenzung, Diskriminierung und Rassismus betroffen sind, aufgrund von Geschlecht, Herkunft, religiöser oder sexueller Orientierung werden auch in Spielumgebungen mit Stereotypen und negativen Kommentaren konfrontiert. Das Aufzeigen dieser toxischen Verhaltensweisen führt zwar dazu, dass dieses in einer breiteren Öffentlichkeit bekannt und diskutiert wird, aber noch nicht dazu, dass Hate

[13]Ein Beispiel für eine derartige „öffentliche“ Entschuldigung ist im Forum von League of Legends unter https://boards.na.leagueoflegends.com/en/c/player-behavior-moderation/qzMdNQrw-sorry zu finden.

Speech eingedämmt wird. Hier sind verstärkt die Betreiber der Online-Spiele bzw. Communities gefragt, Maßnahmen zu setzen, die stärker ins Bewusstsein rücken, dass es sich bei Hasskommentaren nicht um ein Kavaliersdelikt handelt und derartiges Verhalten keinen Platz hat in einer Online-Spielwelt, die eigentlich für alle zugänglich ist und barriere- und vorurteilsfrei den Spaß am gemeinsamen Spielen in den Vordergrund setzen sollte. Gefragt sind zudem die Game-Designer von Computerspielen, damit sich hier eine stark stereotype Darstellung von Frauen, aber auch von anderen Gruppen – vor allem in den Blockbuster-Games – verändert.

Literatur

Baldauf, J., Falk, F., Fischer, M., Groen, M., Neundorf, G., Rathje, J., & Switkes vel Wittels, M. (2015). Gaming und Hate Speech. Computerspiele in zivilgesellschaftlicher Perspektive. Hg. v. Amadeu Antonio Stiftung. Berlin. https://www.amadeu-antonio-stiftung.de/wp-content/uploads/2018/08/gaming-internet-1-1.pdf. Zugegriffen: 10. Apr. 2019.

Bloomberg. (Hrsg.). (2017). Racial and ethnic hate speech thrives in online games. https://www.japantimes.co.jp/news/2017/05/14/business/tech/racial-ethnic-hate-speech-thrives-online-games/#.XLlzQaTgqUk. Zugegriffen: 19. Apr. 2019.

Börner, M. (2018). Die Gaming-Trends 2018. (Hg.). v. Bitkom. https://www.bitkom.org/sites/default/files/file/import/Bitkom-Praesentation-Gaming-Trends-2018.pdf. Zugegriffen: 9. Apr. 2019.

Brause, C. (2018). Die gefährliche Lücke im Maas-Gesetz. https://www.welt.de/politik/deutschland/article173229873/NetzDG-Justizminister-Heiko-Maas-verschont-Online-spiele-Branche.html. Zugegriffen: 17. Juni 2019.

Breuer, J. (2017). Hate speech in online games. In K. Kaspar, L. Gräßer, & A. Riffi (Hrsg.), *Online hate speech. Perspektiven auf eine neue Form des Hasses* (Bd. 4, S. 107–112). Düsseldorf, München: www.kopaed.de (Schriftenreihe zur digitalen Gesellschaft NRW).

Chenelle. (2019). Wie die Gamingindustrie den Sexismus prägt und fördert. https://blog.hslu.ch/majorobm/2019/03/17/teil-2-studien-und-fakten-wie-die-gamingindustrie-den-sexismus-pr%C3%A4gt-und-f%C3%B6rdert/. Zugegriffen: 9. Juni 2019.

Council of Europe. (1997). Recommendation No. R (97) 20. Hg. v. Council of Europe. https://rm.coe.int/1680505d5b. Zugegriffen: 9. Apr. 2019.

Council of Europe. (Hrsg.). (2012). Mapping study on projects against hate speech online. https://www.google.at/url?sa=t&rct=j&q=&esrc=s&source=web&cd=17&cad=rja&uact=8&ved=2ahUKEwjy7ba9gN7hAhULkMMKHRW2Db44ChAWMAZ6BAgCEAI&url=https%3A%2F%2Frm.coe.int%2F16807023b4&usg=AOvVaw2JTpRqFRanoq8HBL5BI4zT. Zugegriffen: 20. Apr. 2019.

Craker, N., & March, E. (2016). The dark side of Facebook®: The Dark Tetrad, negative social potency, and trolling behaviours. *Personality and Individual Differences, 102,* 79–84. https://doi.org/10.1016/j.paid.2016.06.043.

de Latour, A. (2017). *We can! Taking action against hate speech through counter and alternative narratives*. Strasbourg: Council of Europe. (Revised edition. Hrsg. v. Celina Del Felice und Menno Ettema).

Ditch the Label. (Hrsg.). (2019). Battle royale bullying: How to report in-game abuse in fortnite. https://www.ditchthelabel.org/battle-royale-bullying-how-to-report-in-game-abuse-in-fortnite/. Zugegriffen: 16. Juni 2019.

Diver, M. (2016). Hey supercell, what's with this anti-semitic garbage in 'clash royale'? https://www.vice.com/en_uk/article/yvjek5/hey-supercell-whats-with-this-anti-semitic-garbage-in-clash-royale-943. Zugegriffen: 17. Juni 2019.

Ducheneaut, N., Moore, R. J., & Nickell, E. (2007). Virtual "third places": A case study of sociability in massively multiplayer games. *Comput Supported Coop Work, 16*(1–2), 129–166. https://doi.org/10.1007/s10606-007-9041-8.

Fernandez-Blance, K. (2012). Gamer campaign against Anita Sarkeesian catches Toronto feminist in crossfire. Hg. v. The Star. https://www.thestar.com/news/gta/2012/07/10/gamer_campaign_against_anita_sarkeesian_catches_toronto_feminist_in_crossfire.html. Zugegriffen: 20. Apr. 2019.

Freidel, M. (2014). Wenn Kritik kommt, hört das Spiel auf. Hg. v. FAZ. https://www.faz.net/aktuell/feuilleton/medien/gamergate-wenn-kritik-kommt-hoert-das-spiel-auf-13232818.html. Zugegriffen: 20. Apr. 2019.

Gee, J. P. (2004). *Situated language and learning. A critique of traditional schooling*. New York, London: Routledge (Literacies). http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10162948.

Gee, J. P. (2013). *Good video games and good learning. Collected essays on video games, learning and literacy* (2. Aufl.). New York: Lang. (New literacies and digital epistemologies, 67).

Gee, J. P. (2017). Affinity spaces and 21st Century learning. *Educational Technology, 57*(2), 27–31. www.jstor.org/stable/44430520. Zugegriffen: 19. Apr. 2019.

Gee, J. P., & Hayes, E. (2012). Nurturing affinity spaces and game-based learning. In C. Steinkuehler, K. Squire, & S. A. Barab (Hrsg.), *Games, learning, and society. Learning and meaning in the digital age* (S. 129–153). Cambridge: Cambridge University Press. (Learning in Doing: Social, Cognitive and Computational Perspectives).

Geraniols, N. K. (2010). Hate speech corrodes online games. Players report frequent slurs on homosexuals, Asians, Hispanics and women. http://www.nbcnews.com/id/36572021/ns/technology_and_science-games/t/hate-speech-corrodes-online-games/#.XLlxT6TgqUk. Zugegriffen: 19. Apr. 2019.

Gray, K. L. (2016). *Race, gender, and deviance in Xbox Live. Theoretical perspectives from the virtual margins*. London: Routledge.

Groen, M. (2017). "gogo let's rape them" – Sexistischer Sprachgebrauch in Online Gaming Communities. In K. Kaspar, L. Gräßer, & A. Riffi (Hrsg.), *Online hate speech. Perspektiven auf eine neue Form des Hasses* (Bd. 4, S. 113–119). Düsseldorf, München: www.kopaed.de (Schriftenreihe zur digitalen Gesellschaft NRW).

Hardaker, C. (2010). Trolling in asynchronous computer-mediated communication: From user discussions to academic definitions. *Journal of Politeness Research. Language, Behaviour, Culture, 6*(2), 277. https://doi.org/10.1515/jplr.2010.011.

Hernandez, P. (2019). Playing red dead online as a black charcter means enduring racist garbage. https://www.theverge.com/2019/1/15/18183843/red-dead-online-black-character-racism. Zugegriffen: 16. Juni 2019.

Hudson, R. C., Duncan, S., & Reeve, C. (2016). Affinity spaces for informal science learning: Developing a research agenda. report of workshop held July 6 & 7 at Games+Learning+Society 2015. Hg. v. TPT Twin Cities Public Television. https://www.google.at/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=2ahUKEwjn3LLT3dvhAhXmwosKHWMeDacQFjADegQIABAC&url=http%3A%2F%2Fwww.informalscience.org%2Fsites%2Fdefault%2Ffiles%2FAffinitySpacesFinalReport.pdf&usg=AOvVaw274cwb82QZdzrMd_19xRDU. Zugegriffen: 19. Apr. 2019.

Knoop, J. (2018). What happens if you say something racist in the most popular multiplayer games. https://www.pcgamer.com/what-happens-if-you-say-something-racist-in-the-most-popular-multiplayer-games/. Zugegriffen: 17. Juni 2019.

Krishan, M. R. (2019). "Ich hoffe, ihr sterbt alle" E-Sport und Hate Speech. Hg. v. Spiegel Online. https://www.spiegel.de/netzwelt/games/e-sport-und-stoptoxicity-ich-hoffe-ihr-sterbt-alle-a-1253227.html.

Landesanstalt für Medien NRW, klicksafe.de, & Arbeitsgemeinschaft Kinder und Jugendschutz Landesstelle NRW (Hrsg.). (2016). Hate Speech – Hass im Netz. http://www.ajs.nrw.de/wp-content/uploads/2016/06/160617_HateSpeech_WEB2.pdf. Zugegriffen: 20. Apr. 2019.

Liukkonen, I. (2018). Managing hate speech in gaming media. Hg. v. BrandBastion. https://info.brandbastion.com/hate-speech-in-the-gaming-community-and-social-media. Zugegriffen: 20. Apr. 2019.

Medienpädagogischer Forschungsverbund Südwest. (2018). JIM-Studie 2018. Jugend, Information, Medien. Basisuntersuchung zum Medienumgang 12- bis 19-Jähriger. Hg. v. MPFS. https://www.google.at/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwjs-7SGtcPhAhVoAxAIHfzED_oQFjABegQIBhAC&url=https%3A%2F%2Fwww.mpfs.de%2Ffileadmin%2Ffiles%2FStudien%2FJIM%2F2018%2FStudie%2FJIM_2018_Gesamt.pdf&usg=AOvVaw3sNO1bzwPQraFFOyY4w1cv. Zugegriffen: 9. Apr. 2019.

Medienpädagogischer Forschungsverbund Südwest. (Hrsg.). (2019). KIM-Studie 2018. Kinderheit, Internet, Medien. https://www.mpfs.de/fileadmin/files/Studien/KIM/2018/KIM-Studie2018_Web.pdf. Zugegriffen: 17. Juni 2019.

Mihajlova, E., Bacovska, J., & Shekerdjiev, T. (2013). *Freedom of expression and hate speech*. Skopje: OSCE, Mission to Skopje.

Moor, P. J., Heuvelman, A., & Verleur, R. (2010). Flaming on YouTube. *Computers in Human Behavior, 26*(6), 1536–1546. https://doi.org/10.1016/j.chb.2010.05.023.

Mortensen, T. E. (2018). Anger, fear, and games: The long event of #gamergate. *Games and Culture, 13*(8), 787–806. https://doi.org/10.1177/1555412016640408.

No-Hate-Speech.de. (o. A.): Was ist eigentlich Hate Speech? o. A. https://no-hate-speech.de/de/wissen/. Zugegriffen: 9. Apr. 2019.

Nowak, V. (2017). Ist PewDiePie ein Antisemit? https://www.br.de/puls/themen/popkultur/pewdiepie-antisemitismus-vorwuerfe-100.html. Zugegriffen: 16. Juni 2019.

Park, M. (2018). Rainbow six siege players who use slurs are now getting instantly banned. https://www.pcgamer.com/rainbow-six-toxicity-ban/. Zugegriffen: 16. Juni 2019.

Pulos, A. (2013). Confronting heteronormativity in online games. A critical discourse analysis of LGBTQ sexuality in world of warcraft. *Games and Culture, 8*(2), 77–97.

Rogers, R. (2016). *How video games impact players. The pitfalls and benefits of a gaming society*. Lanham: Lexington Books.

Sarkeesian, A. (2012). Image based harassment and visual misogyny. https://feministfrequency.com/2012/07/01/image-based-harassment-and-visual-misogyny/. Zugegriffen: 16. Juni 2019.

Schmitt, J. B. (2017). Online hate speech: Definition und Verbreitungsmotivationen aus psychologischer Perspektive. In K. Kaspar, L. Gräßer, & A. Riffi (Hrsg.), *Online Hate Speech. Perspektiven auf eine neue Form des Hasses* (Bd. 4, S. 51–56). Düsseldorf, München: www.kopaed.de (Schriftenreihe zur digitalen Gesellschaft NRW).

Shanley, P. (2019). Xbox head addresses "toxic stew of hate speech, bigotry" in gaming. https://www.hollywoodreporter.com/news/xbox-head-phil-spencer-addresses-toxic-stew-hate-speech-bigotry-gaming-1211729. Zugegriffen: 9. Juni 2019.

Sidorov, W. (2018). Twitch – Montana Black für einen Monat gebannt. https://www.playcentral.de/spiele-news/twitch/montanablack-einen-monat-gebannt-id76494.html. Zugegriffen: 16. Juni 2019.

Sinclair, B. (2018). Discord's problem: Which Nazi group were you reporting again? https://www.gamesindustry.biz/articles/2018-10-12-discords-problem-which-nazi-group-were-you-reporting-again. Zugegriffen: 17. Juni 2019.

Sony. (2019a). Information on banned accounts, consoles and ip addresses. https://support.playstation.com/s/article/Information-on-Banned-Accounts-and-Consoles?language=en_US. Zugegriffen: 2. Juni 2019.

Sony. (2019b). Terms of service and user agreement. https://www.playstation.com/en-us/network/legal/terms-of-service/, zuletzt aktualisiert am 01.04.2019, zuletzt geprüft am 02.06.2019.

SPLENDID RESEARCH GmbH. (2018). Gaming in Deutschland. Eine repräsentative Umfrage unter 2.024 Deutschen zu Videospielen und Microtransactions. Hamburg. https://www.splendid-research.com/de/studie-gaming.html?idU=1. Zugegriffen: 9. Apr. 2019.

Standing Stone Games LLC. (2017). Dungeons & dragons online – Code of conduct. https://www.ddo.com/en/dungeons-dragons-online-code-conduct-en.

Stertkamp, Wolf. (2017). *Sprache und Kommunikation in Online-Computerspielen. Untersuchungen zu multimodaler Kommunikation am Beispiel von World of Warcraft*. Gießen: Gießener Elektronische Bibliothek. (Linguistische Untersuchungen, 11).

Take Back the Tech. (Hrsg.). (o. A.): Hate speech: strategies. https://www.takebackthetech.net/be-safe/hate-speech-strategies. Zugegriffen: 29. Apr. 2019.

Ubisoft. (Hrsg.). (2018). Dev blog: Toxicity. https://rainbow6.ubisoft.com/siege/en-us/news/152-321200-16/dev-blog-toxicity. Zugegriffen: 16. Juni 2019.

von Bülow, C. (2004). Mem. In J. Mittelstraß, S. Blasche, G. Wolters, & M. Carrier (Hrsg.), *Enzyklopädie Philosophie und Wissenschaftstheorie* (Bd. 5, S. 318–324). Unveränd. Sonderausg. Stuttgart: Metzler. Zugegriffen: 9. Apr. 2019.

Williams, C. (2018). Games-Moderator erzählt, warum Arschloch-Gamer so selten bestraft werden. https://www.vice.com/de/article/43pndd/warum-arschloch-gamer-nicht-bestraft-werden-moderator-community-management. Zugegriffen: 17. Juni 2019.

Von der Straße ins Netz

Eine Analyse belgischer Beteiligung am illegalen Drogenhandel auf Kryptomärkten

Geert Slabbekoorn, Charlotte Colman, Noel Klima und Maud De Meyer

1 Einleitung

Entwicklungen in der Technologie können nicht nur Aspekte unseres täglichen Lebens verändern, sondern auch die Art und Weise beeinflussen, wie illegale Transaktionen organisiert werden, beispielsweise das Angebot und die Nachfrage nach illegalen Drogen. Anstatt sich mit Drogenhändlern von Angesicht zu Angesicht auszutauschen, treffen sich die Akteure auch online im Internet. Obwohl der Handel mit illegalen Drogen im Internet erst vor relativ kurzer Zeit die Aufmerksamkeit von Wissenschaftlern und der breiten Öffentlichkeit auf sich gezogen hat (Martin 2014a), ist die Online-Transaktion von Drogen nicht neu. Es wird davon ausgegangen, dass die erste Transaktion mit Cannabis bereits in den 1970er Jahren stattgefunden hat, durchgeführt von Universitätsstudenten, die dazu das ARPAnet des US-Verteidigungsministerium benutzten (EMCDDA 2017; Markoff 2005).

G. Slabbekoorn (✉) · C. Colman · N. Klima · M. De Meyer
Universiteit Gent, Gent, Belgien
E-Mail: geert.slabbekoorn@ugent.be

C. Colman
E-Mail: charlotte.colman@ugent.be

N. Klima
E-Mail: noel.klima@ugent.be

M. De Meyer
E-Mail: maud.demeyer@ugent.be

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

T.-G. Rüdiger und P. S. Bayerl (Hrsg.), *Cyberkriminologie,*
https://doi.org/10.1007/978-3-658-28507-4_12

Seit einiger Zeit kommt es jedoch vermehrt zu Drogentransaktionen im Darknet, einem offen zugänglichen, aber stark verschlüsselten kleinen Teil des Deepwebs. Ein Darknet-Marktplatz, der in diesem Beitrag als Kryptomarkt bezeichnet wird, könnte zum Beispiel als Online-Forum definiert werden, in dem Waren und Dienstleistungen zwischen Parteien ausgetauscht werden, die ihre Identität mithilfe digitaler Verschlüsselung verbergen (Martin 2014b, S. 356; s. a. Kap. „Darknet – die dunkle Seite des Internets?“). In der Tat bieten Kryptomärkte aufgrund des erforderlichen speziellen Netzwerk-Routing-Protokolls im Onion Router (Tor)-Netzwerk, eine relative Anonymität. Diese sorgt dafür, dass unter anderem der Standort des Website-Servers und Benutzer-IDs wie IP-Adressen sowie die automatische Verschlüsselung der gesamten Kommunikation durch Pretty Good Privacy (PGP)-Kryptografie verborgen werden. Hinzu kommen Zahlungen mit digitalen Währungen wie Bitcoin oder Monero ausgeführt (Roxburgh et al. 2017; Paquet-Clouston et al. 2018).

Diese Kryptomärkte sind seit 2011 – als der wohl bekanntesten Drogenkryptomarkt „Silk Road 1.0“ auf dem Markt erschien – rasant gewachsen. Silk Road 1.0 war mehr als zwei Jahre in Betrieb, wobei die meisten Angebote illegale Drogen, pornografisches Material oder gefälschte Dokumente, wie beispielsweise nachgemachte Personalausweise betrafen (EMCDDA 2017; s. a. Kap. „Strafverfolgung digital“). Es gibt keine verfügbare vollständige Liste (geschweige denn eine Methode zum Erstellen derselben) der Gesamtanzahl der derzeit bestehenden Kryptomärkte. Zum Zeitpunkt der Erstellung dieses Beitrags (Juli 2019) war jedoch eine Liste der wichtigsten Kryptomärkte auf Darknetlive.com verfügbar bestehend aus 21 aktiven Märkten (Darknetlive 2019). Vor der Stilllegung durch die Strafverfolgungsbehörden Anfang Mai 2019 bezog sich das weit verbreitete DeepDotWeb auf 19 aktive Kryptomärkte (DeepDotWeb 2019). Genau wie Silk Road 1.0 bieten die meisten dieser Märkte eine breite Palette von (hauptsächlich illegalen) Produkten und Dienstleistungen an, dennoch besteht die große Mehrheit der verfügbaren Produkte aus illegalen Drogen (EMCDDA 2017).

Kryptomärkte sind dynamische und anpassungsfähige Märkte. Während die Mehrheit dieser Märkte zumeist nicht länger als ein Jahr besteht (EMCDDA 2017), dominier(t)en einige wenige dieser Märkte das Darknet für zwei Jahre oder länger. Dies gilt insbesondere für Silk Road 1.0 (2011 gegründet und 2013 eingestellt) oder Dream Market (gegründet im Jahr 2013, Betrieb eingestellt im Jahr 2019) (Darknet Stats, Juni 2018; ZDNet 2019). Sobald ein führender Kryptomarkt geschlossen wird (z. B. aufgrund von Eingriffen der Strafverfolgungsbehörden oder aufgrund von Exit-Scam-Praktiken), migrieren viele

seiner Benutzer zu verbleibenden Kryptomärkten oder es entstehen kurze Zeit später neue Kryptomärkte. So wurde beispielsweise im Oktober 20013 Silk Road 1.0 heruntergefahren und nur einen Monat später (November 2013) Silk Road 2.0 online geschaltet, und zwar von den ehemaligen Administratoren von Silk Road 1.0.

Kryptomärkte bieten beispiellose Möglichkeiten, einen Drogenmarkt in seiner Gesamtheit zu untersuchen und neue Trends bei der Verfügbarkeit und dem Gebrauch von Drogen zu beobachten (Barratt und Aldridge 2016; Broséus et al. 2016). Seit ein paar Jahren haben Drogenkryptomärkte bei Forschern großes Interesse geweckt, da sie Daten zum Verbraucherprofil (Van Hout und Bingham 2013), zu den gehandelten Substanzen (Broséus et al. 2016) und zur Struktur von Kryptomärkten (Duxbury und Haynie 2017) enthalten. Viele dieser Studien konzentrieren sich auf Silk Road 1.0 (Barratt et al. 2013) und ihre bekanntesten Nachfolger wie Silk Road 2.0 und Alphabay (Tzanetakis 2018). Die verfügbaren Forschungsergebnisse zeigen, dass zwar die Teilnehmer am Drogenkryptomarkt aus der ganzen Welt kommen, die Anbieter aber insbesondere in westlichen Ländern, wie den Vereinigten Staaten, Großbritannien, den Niederlanden, Deutschland und Kanada leben (Christin 2013). Einige Länder bzw. deren nationale Behörden haben sich zu Recht der Erforschung dieses Trends verschrieben, indem sie Trendberichte verfasst haben, wie zum Beispiel das *National Drug and Alcohol Research Center* (NDARC), welches das Phänomen aus australischer Sicht beleuchtet. Einige nationale Ministerien, wie das niederländische Ministerium für Sicherheit und Justiz (Kruithof et al. 2016), geben wissenschaftliche Studien in Auftrag, um Erkenntnisse über das Phänomen in einem bestimmten Land zu erhalten.

Trotz des zunehmenden akademischen und politischen Interesses gibt es auf diesem Gebiet noch viele Unklarheiten. Bis vor kurzem gab es beispielsweise keine Studien, die auf belgische Käufer und Verkäufer auf neueren Kryptomärkten gerichtet waren, was – zumindest partiell – einen blinden Fleck in der Kryptomarktforschung darstellte. Der Global Drug Survey 2017 ergab, dass 10,8 % der belgischen Befragten ihre Drogen in den letzten 12 Monaten über Kryptomärkte bezogen haben. Jüngste Untersuchungen (Colman et al. 2018) haben zudem ergeben, dass sich der belgische Einzelhandelsmarkt diversifiziert hat. Die belgischen Strafverfolgungsbehörden stellten eine Verschiebung auf den Drogenverkaufsmärkten fest – einschließlich des Auftretens neuer Phänomene wie Call-Center, sog. „Gras-Kuriere“ („wietkoerier“) und Online-Transaktionen (Kryptomarkt). Um die vorstehend genannte Forschungslücke zu schließen, startete

2019 ferner das belgische multidisziplinäre Forschungsprojekt CRYPTODRUG, finanziert durch den belgischen Föderalen Öffentlichen Programmierungsdienst für Wissenschaftspolitik (Belspo), um ihrerseits das Verhalten belgischer Konsumenten und Anbieter auf Kryptomärkten zu untersuchen.[1]

In diesem Kapitel werden die ersten Ergebnisse der CRYPTODRUG-Studie vorgestellt. Die Ergebnisse beschreiben die Drogenangebotsseite in Bezug auf zwei der größten Kryptomärkte, die zu Beginn der Studie in Betrieb waren (dem „Dream Market“ und dem „Wall Street Market“) und widmet sich der Bedeutung und dem Profil der belgischen Anbieter im illegalen Drogenhandel.

2 Methode: Data Scraping aus Kryptomärkten

Nach der von Kruithof et al. (2016) und von anderen Forschern entwickelten Methode zur Durchführung kriminologischer Untersuchungen zu Kryptomärkten (wie Aldridge und Décary-Hétu 2016; Tzanetakis 2018), wird die Forschungsfrage durch die Sammlung und Analyse von abgeschöpften Daten aus Kryptomärkten beantwortet. Dazu mussten Kryptomärkte ausgewählt werden. Stabilität und Gesamtgröße waren hierbei die Hauptauswahlkriterien. Zu Beginn des Datenerfassungsprozesses im Oktober 2018 waren Dream Market (DM) und Wall Street Market (WSM) die beiden größten und auch relativ stabile Kryptomärkte, die dem Verkauf von (unter anderem) illegalen Drogen eine Plattform boten.

DM wurde regelmäßig untersucht (z. B. Kruithof et al. 2016), wohingegen WSM weniger umfassend kartiert wurde, was höchstwahrscheinlich darauf zurückzuführen ist, dass WSM erst in jüngerer Zeit in Erscheinung getreten ist und deshalb eine (noch) relativ beschränkte Nutzung erfährt. Beide Plattformen ermöglichten den Handel mit (meist illegalen) Waren, darunter Kreditkartendaten, Handbücher für Betrug, gestohlene Wertsachen wie Schmuck und Software für andere Formen der Internetkriminalität. Die größte Einzelkategorie auf beiden Märkten waren jedoch illegale Drogen, unserem zentralen Forschungsgegenstand.

DM wurde Ende 2013 gegründet (Kruithof et al. 2016). Mit Blick auf öffentlich verfügbare Daten für DM (Gwern et al. 2015) hatte die Plattform Mitte 2014 nur einige Dutzend Produktangebote, während es Mitte 2015 bereits ca. 1800 waren. Zum Zeitpunkt unserer Analyse war DM sogar der weltweit größte Markt-

[1]Belspo DR/82: http://www.belspo.be/belspo/fedra/proj.asp?l=en&COD=DR%2F82.

platz. Der Betrieb wurde Ende März 2019 eingestellt. WSM war eine deutlich neuere Plattform, die erst 2016 eingeführt wurde und weltweit den zweiten Platz in Bezug auf die Gesamtmenge der Ende 2018 angebotenen Produkte einnahm (DeepWebSitesLinks 2019). Am 3. Mai 2019 wurde deutlich, dass die WSM-Administratoren sich mit Benutzergeldern abgesetzt hatten. Sie konnten sich jedoch nicht an den Früchten ihres „Exit-Scams" erfreuen: Sie wurden monatelang von den niederländischen und US-amerikanischen Strafverfolgungsbehörden sowie von Europol observiert und konnten kurz nach ihrem Verschwinden von der deutschen Zentralstelle zur Bekämpfung der Internetkriminalität und dem Bundeskriminalamt festgenommen werden (BKA 2019).

Um die Entwicklung dieser Märkte über einen Zeitraum von 5 Monaten zu dokumentieren, haben wir monatlich Daten erhoben. Diese Längsschnittanalyse war deshalb von Interesse, weil diese Märkte in einem dynamischen Umfeld operieren, das zum einen zwar ständigen Wachstum zeitigt, zum anderen aber auch unterschiedlichen Zwischenereignissen wie vorübergehende oder dauerhafte Nichtverfügbarkeit oder Eingriffe Dritter in das Ökosystem des Darkwebs unterworfen ist (Soska und Christin 2015; Van Buskirk et al. 2014).

2.1 Datensammlung und Analyse

Um die relevanten Informationen von den ausgewählten Plattformen zu extrahieren, wurde eine speziell entwickelte Web-Scraping-Software verwendet (z. B. Paoli et al. 2017; Kruithof et al. 2016). Diese Software startet bei einer bestimmten Webdomain, lädt die Seite im HTML-Format herunter, findet die Links auf der Seite und folgt diesen. Danach beginnt der Prozess für jede Unterseite von vorne. Für die Analyse haben wir die Unterkategorie „Drogen" als Ausgangspunkt gewählt, von wo aus alle Produktlistenseiten zusammen mit den dazugehörigen Anbieterprofilseiten heruntergeladen wurden. Eine Auflistung ist eine einzelne Seite für ein einzelnes Produktangebot, in der Regel mit einer bestimmten Menge, Form, Versandart, einer kurzen Produktbeschreibung, mit Angabe des Anbieters, usw. (Broséus et al. 2016). Nachdem der Scrap-Vorgang abgeschlossen ist, beginnt die Analyse der HTML-Dokumente. Hierbei werden die verschiedenen Variablen aus dem HTML-Code extrahiert und Datentabellen geschrieben, die wiederum eine ordnungsgemäße Analyse ermöglichen.

Nach einer Testrunde im Oktober 2018 wurde der eigentliche Datenextraktionsprozess im November 2018 ausreichend entwickelt. Dabei ging es insbesondere darum, die Vollständigkeit und die Nicht-Duplizität von abgeschöpften Seiten zu bestätigen (Dolliver 2015). Die Abschöpfungen erfolgten trotz häu-

figer Unregelmäßigkeiten bei der Verfügbarkeit der Märkte aufgrund einer dem Tor-System innewohnenden Anfälligkeit etwa monatlich (Torproject 2019). Die Daten aus dem DM wurden bis zur Ankündigung seiner Auflösung Ende März 2019 durch seinen eigenen Administrator abgeschöpft. Anschließend haben wir das Scraping von WSM auf wöchentliche Intervalle intensiviert, um die Bewegung von Markt zu Markt zu dokumentieren. Dies geschah, bis WSM um den 20. April seinen Betrieb einstellte. Für den DM gibt es insgesamt vier komplette Scrapings; für WSM sind es insgesamt acht (für die exakten Daten siehe Tab. 1 und 2).

Das Abschöpfen und Analysieren (Scraping und Parsing) führte zu zwei Hauptdatensätzen pro Markt: Inserate und Anbieterprofile. Obwohl sich die Märkte in Bezug auf Layout und technische Ausstattung teilweise unterschieden, stimmen die Datensätze hauptsächlich in Bezug auf Variablennamen und Definitionen überein. Die beiden Märkte wiesen in etwa ähnliche Mechanismen auf und zeigten übereinstimmende Informationen an. Einige Variablen erscheinen jedoch auf den Plattformen auf unterschiedliche Weise oder werden, wie im Einzelnen noch erläutert wird, leicht unterschiedlich verwendet. Für die PGP-Schlüssel der Anbieter wurde keine zusätzliche Analyse durchgeführt. Broséus et al. (2016) zeigen, dass nur ein kleiner Teil der Anbieternamen mit mehreren PGP-Schlüsseln und nur ein kleiner Teil der PGP-Schlüssel mit mehreren Anbieterkonten verknüpft sind.

Die relevantesten Variablen, die aus den Auflistungen extrahiert wurden, waren der Versandursprung und der Versandort für jedes Produkt, der Name des Anbieters, der Preis, die übergeordnete Kategorie (unter welcher Drogenkategorie das Produkt auf dem Markt angeboten wurde) und eine kurze Produktbeschreibung des Verkäufers. WSM lieferte zusätzlich eine Kundenbewertung pro Einzelprodukt.

In Bezug auf die Anbieterprofile waren der Name des Anbieters und die Anzahl der abgeschlossenen Transaktionen die wichtigsten relevanten Variablen. Zusätzliche Variablen bezogen sich auf die Reputationsmarker, die beide Kryptomärkte zur Verfügung stellten. In Bezug auf DM ergaben sich folgende Haupt-

Tab. 1 DM Wachstum weltweit

	23.11.2018	19.12.2018	24.01.2019	06.03.2019	TOTAL	%
# Angebote	61.372	63.950	72.361	75.848	14.476	23
# Anbieter	2315	2453	2742	2834	519	22

Tab. 2 WSM Wachstum weltweit

	26.11.2018	20.12.2018	24.01.2019	22.02.2019	25.03.2019	04.04.2019	10.04.2019	17.04.2019	TOTAL	%
# Angebote	5905	6162	6908	7850	9386	12.108	13.612	15.857	9952	169
# Anbieter	790	890	980	1171	1385	1815	2011	2227	1437	182

variablen für Anbieter: „Anzahl der Bewertungen“ und die von Kunden abgegebene Durchschnittsbewertung, „Vertrauensstimmen“, „Misstrauensstimmen“ und Beitrittsdatum. In WSM wurden keine (nicht) vertrauenswürdigen Stimmen protokolliert. „Anbieter Niveau“ war jedoch ein weiterer Indikator für die Reputation.

Einige der aufgezeichneten Variablen verdienen eine kurze Erläuterung: Dies betrifft zunächst das Herkunftsland (country of origin, COO), aus dem hervorgeht, aus welchem Land ein Produkt versandt wurde. Wenn das COO Belgien ist, wird dies in der vorliegenden Studie als Proxy für „belgisch sein“ verwendet. Selbst wenn der Verkäufer kein Belgier ist, ist es bei enger Auslegung wahrscheinlich, dass das Produkt belgisches Hoheitsgebiet bzw. belgische Postdienste durchlaufen hat. Van Buskirk et al. (2016) weisen darauf hin, dass es eher wahrscheinlich ist, dass das vom Anbieter für das jeweilige Produkt angegebene COO tatsächlich der Ort ist, von dem aus das Paket gesendet wird. Bei Versand ins Ausland ist das COO anhand der Briefmarken gut erkennbar. Da das COO eine Variable ist, die sich auf die Angebote und nicht auf den Anbieter bezieht, ist es jedoch möglich, dass ein einzelner Anbieter seine Produkte von verschiedenen Standorten aus versendet. Ebenso ist es möglich, dass ein Anbieter bestimmte Produkte innerhalb eines Monats von einem Standort aus versendet und anschließend sein Geschäft über die Grenze in ein anderes Land verlagert.

Eine zweite mehrdeutige Variable ist die Kategorisierung der verschiedenen angebotenen Substanzen. Erstens haben beide Märkte unterschiedliche Kategorien, denen Angebote angehören können. Daher sind Vergleiche möglicherweise nicht aussagekräftig, wenn sie auf der Grundlage der Kategorien der Kryptomärkte vorgenommen werden. Auch bei der Einstufung von Arzneimitteln spielten Ambiguitätsprobleme eine Rolle, da möglicherweise die Anbieter selbst die Substanz einstufen (Soska und Christin 2015). In unserem Datensatz wurden beispielsweise Amphetamine unter „Stimulanzien“ gefunden, aber auch unter „Amphetamine“. Kokain kann sowohl in „Kokain“ als auch in „Stimulanzien“ vorkommen. 2C-B war unter „Pillen“ zu finden. unter „RCs“ (Forschungschemikalien) und unter „Sonstige“. Außerdem kam es gelegentlich zu einer völligen Fehlkategorisierung, beispielsweise wurde unter „Benzos“ ein neuartiges synthetisches Cannabinoid namens 4F-ADB gefunden. Da die in jeder Auflistung enthaltenen Produktbeschreibungen detailliertere Informationen enthielten, wurde die Kategorisierung von Substanzen für den belgischen Markt manuell vorgenommen. Alle in einem Angebot enthaltenen Informationen (z. B. Produktbeschreibung) wurden kombiniert, was zu einer höheren Stichhaltigkeit hinsichtlich der Drogenkategorien führte. Dabei wurden ähnliche Substanzgruppen verwendet wie von Van Buskirk et al. (2016), lediglich mit geringfügigen Anpassungen zur Minimierung der Gruppe „Sonstige/Unbekannte“.

3 Ergebnisse

Dieser Teil beschreibt die ersten Ergebnisse der CRYPTODRUG-Studie und betrifft belgische Drogenanbieter, die auf den beiden Kryptomärkten DM und WSM aktiv sind. Die Ergebnisse beschreiben Trends zu Marktgröße, Zielländern, Schätzungen der getätigten Transaktionen und verfügbaren Drogenkategorien. Zunächst wird kurz die globale Präsenz von Angeboten und Anbietern auf diesen Märkten vorgestellt. Anschließend folgt eine Beschreibung der belgischen Anbieter. Am Ende eines jeden Paragraphen werden einzelne erwähnenswerte Fälle aus Belgien oder mit belgischem Bezug reflektiert.

3.1 Kryptomärkte auf globaler Ebene: Anhaltendes Wachstum

Um die belgischen Daten im internationalen Rahmen zu interpretieren, geben die Tab. 1 und 2 einen Überblick über die weltweite Größenordnung der beiden Kryptomärkte. DM war mit Abstand der größte Markt, da er zum ersten Messzeitpunkt ungefähr zehnmal so groß war wie WSM ($N = 61.372$ gegenüber $N = 5905$; Abb. 1) und hinsichtlich der Anbieter etwa dreimal so groß ($N = 2315$ gegenüber $N = 790$, Abb. 2). Obwohl kein vergleichender Überblick aller anderen Märkte vorgenommen werden konnte, zeigt ein Vergleich mit Kruithof et al. (2016), dass DM auf seinem Höhepunkt im Jahr 2019 etwa doppelt so groß war wie der größte aktive Markt „AlphaBay“ mit fast 39.000 Angeboten im Januar 2016.

Auf beiden untersuchten Plattformen war ein allgemeiner Wachstumstrend zu erkennen, was sowohl für die Anzahl der Angebote als auch für die Anzahl der Anbieter gilt, die zum Zeitpunkt der Messung eine oder mehrere Angebote eingestellt hatten. Insbesondere ist für WSM – ab dem Zeitpunkt der Bekanntgabe durch DM, den Betrieb Anfang 2019 einstellen zu wollen – ein exponentielles Wachstum, um den Faktor 4 zu beobachten. Zwischen dem 22. Februar und 25. März 2019 wurden 1536 Angebote bei WSM hinzugefügt. In weniger als einer weiteren Woche (bis 4. April 2019) kamen 2245 weitere Angebote hinzu, und bis zum 17. April noch einmal 2245. Auch die Anzahl der Anbieter stieg in kürzester Zeit stetig. Zunächst um 214 und nach der Ankündigung von DM um weitere 430 neue Anbieter. In den darauffolgenden beiden Wochen kamen dann noch einmal 196 bzw. 216 neue Anbieter hinzu (Abb. 2).

Die Daten zeigen ein viel höheres durchschnittliches „Angebote-pro-Anbieter-Verhältnis“ für DM als für WSM, das auf beiden Märkten zeitlich stabil

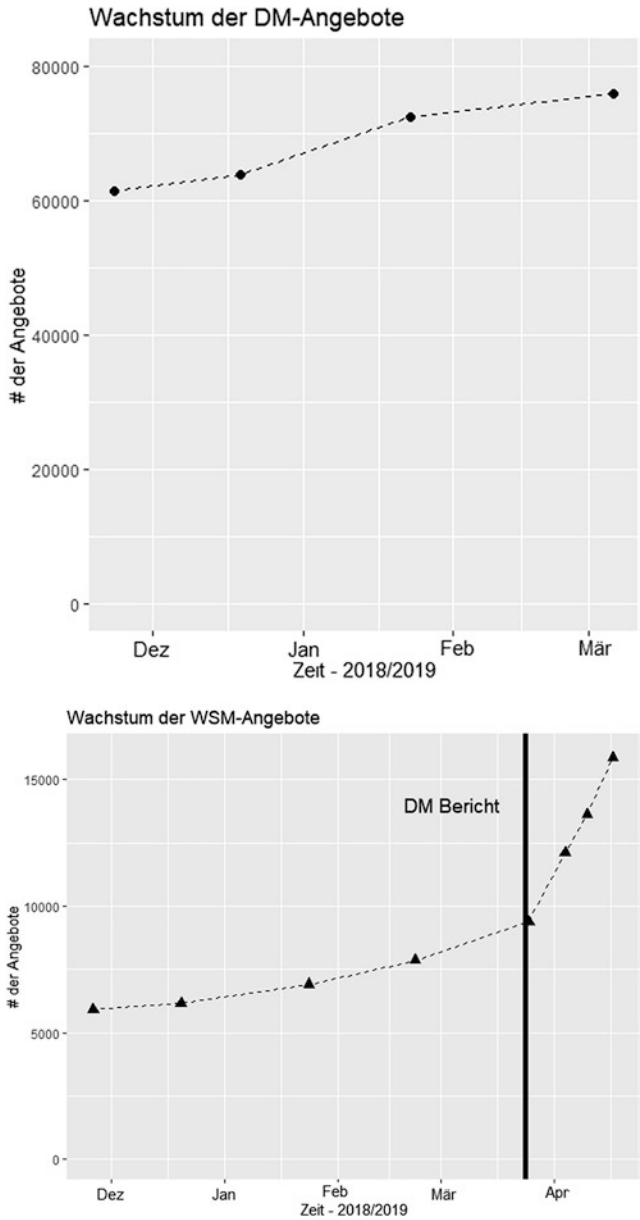


Abb. 1 Wachstum an Angeboten für DM und WSM

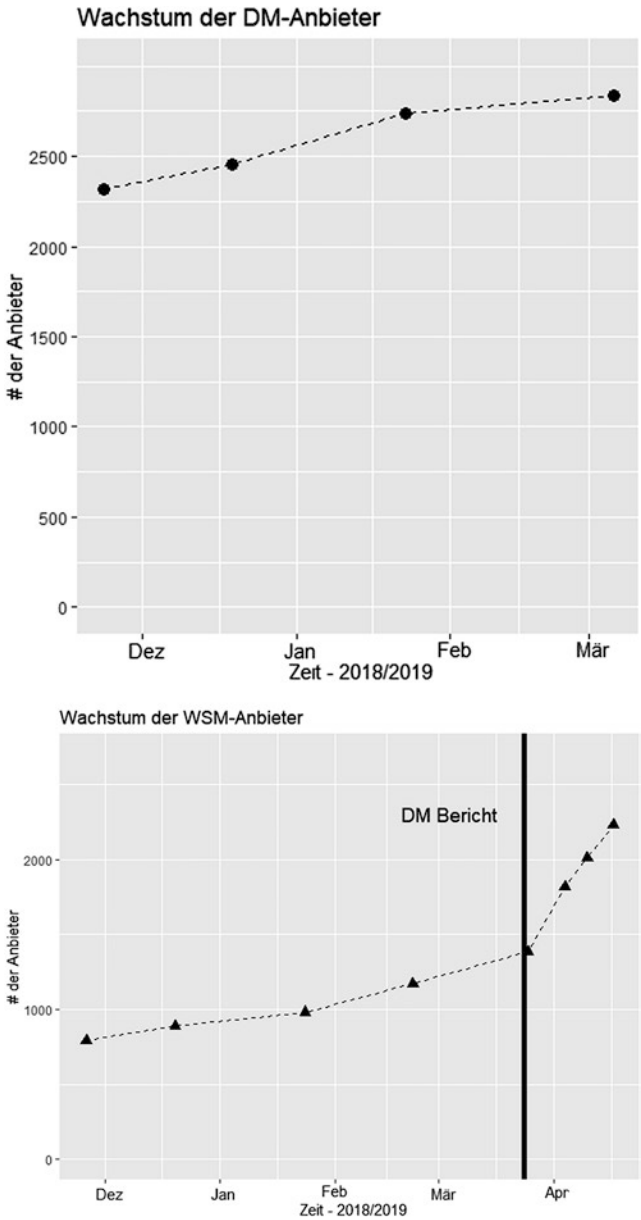


Abb. 2 Wachstum an Anbietern für DM und WSM

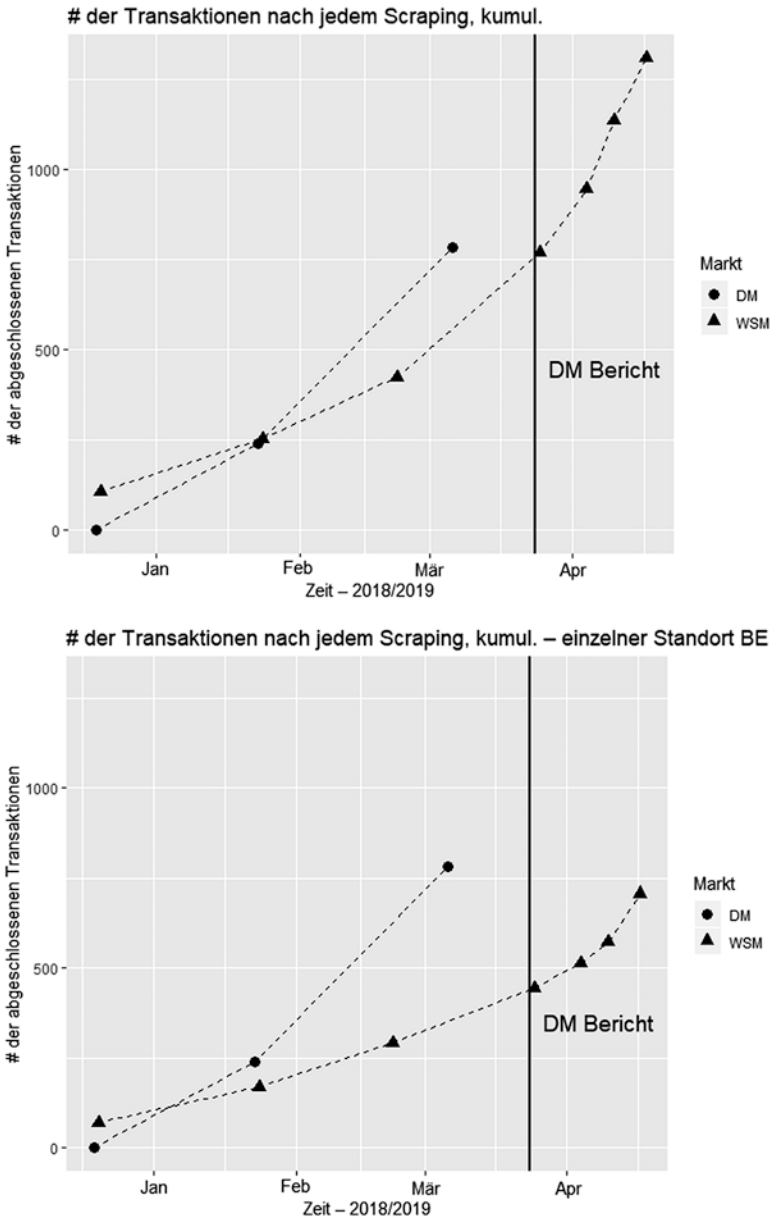


Abb. 3 Anzahl an Transaktionen

ist: ungefähr 26 Angebote pro Anbieter für DM und 6,5–7,5 für WSM-Anbieter. Im Vergleich zu den von Kruithof et al. (2016) erhobenen Daten aller aktiven Märkte vom Januar 2016, liegt DM über dem Durchschnitt der Angebote pro Anbieter, während WSM weit darunter liegt. Dieses Verhältnis bei WSM ändert sich nach dem Verfall des DM nicht, was darauf hindeutet, dass vor allem neue Anbieter eine neue Plattform für das Angebot ihrer Waren benötigten, während bestehende Anbieter ihr bestehendes Angebot nicht erweiterten.

In Bezug auf die Anzahl der Angebote pro Land ist das Ranking für beide Märkte eindeutig. Auf der DM-Liste liegt Großbritannien durchweg an der Spitze, gefolgt von den USA. Die Plätze 3, 4 und 5 halten die EU als Ganzes, die Niederlande und Deutschland. Beim WSM liegen die USA mit großem Abstand vorne, gefolgt von Großbritannien. Es folgen Deutschland, die Niederlande und die EU als Ganzes in zeitlich wechselnder Reihenfolge. Ausgehend von März 2019 als Referenzmonat, konnten bei DM etwa 24 % aller Angebote Großbritannien zugeordnet werden. In dieser Zeit stammen bei WSM 34 % aller Angebote aus den USA.

3.2 Die belgische Präsenz auf Kryptomärkten: Ein Spiegelbild des weltweiten Trends

Die belgische Marktgröße macht nur einen kleinen Bruchteil des globalen Gesamtmarktes aus. Die Tab. 3 und 4 zeigen die belgischen Angebote und Anbieter pro Markt. In Bezug auf DM steht Belgien für einen Gesamtanteil von 0,23 % des weltweiten Angebots und 0,32 % der weltweiten Anbieter. Bei WSM ist der Anteil etwas größer: 0,57 % bzw. 0,94 %. Damit fällt Belgien in Bezug auf DM nicht unter die Top 20 der Länder mit der höchsten Anzahl Einträge pro Land, wohingegen Belgien bei WSM auf Rang 15 lag.

Bei Anbietern und Angeboten aus Belgien ist der Wachstumstrend auf DM auf globaler Ebene weniger stark ausgeprägt. Das liegt daran, dass bei dem ersten Messmoment die überwiegende Mehrheit der belgischen Angebote (319

Tab. 3 DM Wachstum Belgien

	23.11.2018	19.12.2018	24.01.2019	06.03.2019	TOTAL	%
# Angebote	366	54	113	173	−193	−111
# Anbieter	5	4	8	9	4	80

Tab. 4 WSM Wachstum Belgien

	26.11.2018	20.12.2018	24.01.2019	22.02.2019	25.03.2019	04.04.2019	10.04.2019	17.04.2019	TOTAL	%
# Angebote	35	46	44	45	48	57	61	68	33	94
# Anbieter	8	10	11	11	14	19	18	19	11	138

von 366) einem einzelnen Anbieter zugeordnet werden konnte.[2] Für WSM entspricht der Wachstumstrend sowohl bei den Anbietern als auch bei den Angeboten weitgehend der weltweiten Entwicklung: Ein stetiges Wachstum, das sich nach Bekanntgabe durch DM erheblich beschleunigt (ungefähr um den Faktor 4).

Wie bereits erwähnt, besteht eine gewisse Unsicherheit hinsichtlich der Eignung der Variable „Versand aus Belgien", da sich ein einzelner Anbieter entscheiden kann, unterschiedliche Produkte von unterschiedlichen Standorten aus zu versenden und die Versandherkunft auch im Laufe der Zeit geändert werden kann. Genau diese Ambiguität erlaubt es jedoch, einige interessante Anbietereigenschaften abzuleiten. Auf der belgischen Seite des DM ist zum einen das Phänomen der Verkäufer mit multipler Herkunft (multiple origin vendors – MOVs) begrenzt. Von allen 15 Anbietern, die im Verlauf der Analyse identifiziert wurden, verschifften nur drei aus Belgien und mindestens einem anderen Standort, was bedeutet, dass die Mehrheit der belgischen DM-Anbieter ausschließlich aus Belgien versandt haben. Die Änderungen in den MOVs-Profilen auf DM lassen auf eine geografische Bewegung schließen. Aus der Analyse kann geschlussfolgert werden, dass ein Anbieter, der in früheren Monaten noch aus Belgien versandt hatte, bis Anfang März den Versandstandort aller angebotenen Waren nach Deutschland verschoben hatte. Ein zweiter Verkäufer hat alle seine Waren Ende 2018 noch aus den Niederlanden verschickt und dann im Januar 2019 Belgien als zweiten Versandstandort hinzugefügt. Bis Februar 2019 hat dieser Anbieter dann alle seine Versandaktivitäten nach Belgien verlagert. Ein dritter MOV auf DM hat seine gesamte Angebotspalette zwischen Ende Januar und Anfang März von den Niederlanden nach Belgien verschoben.

Mit insgesamt 26 verschiedenen belgischen Verkäufer-IDs, davon 12 MOVs, ist WSM in dieser Hinsicht etwas komplexer. Insgesamt vier Anbieter, die von Belgien aus liefern, versendeten zum Zeitpunkt der Messung auch aus den Niederlanden. Die übrigen angegebenen Herkunftsländer sind recht unterschiedlich, wobei die Mehrzahl der Herkunftsländer (11) innerhalb der EU liegt. Die anderen drei Länder sind die USA, Australien und die EU als solche. Die Analyse der Anbieter von WSM zeigt zudem keine eindeutigen Standortverlagerungen.

Dennoch sollen an dieser Stelle einige belgische WSM-Anbieterprofile erwähnt werden. Es gibt zum Beispiel einen MOV, deren Versandstandorte auf drei Kontinente mit sieben Ländern verteilt sind. Dies könnte darauf hinweisen,

[2]Teile der Daten aus der Scraping-Analyse im Oktober 2018 lassen darauf schließen, dass es sich bei dem genannten einzelnen Anbieter um eine Anomalie handelt, die jedoch noch nicht bestätigt werden kann.

dass möglicherweise mehrere Personen in den Prozess involviert sind. Ein zweiter MOV, dessen Name möglicherweise eine Verbindung mit Frankreich impliziert, liefert nur aus Belgien und Spanien und verweist anscheinend auf eine sehr hohe Mobilität eines Anbieters oder erneut auf mehrere Personen. Ein dritter Anbieter gibt an, aus Polen, Tschechien, Ungarn und Bosnien zu versenden, was eine zusätzliche geografische Ausbreitung darstellt.

3.3 Anzahl der Transaktionen: Ein kontinuierliches Wachstum des belgischen Marktes

Auf beiden Märkten wird die Anzahl der abgeschlossenen Transaktionen jedes Anbieters protokolliert und auf der Profilseite als Metrik angezeigt. Subtrahiert man die Anzahl der Transaktionen, die zum vorherigen Bewertungszeitpunkt angegeben wurden, von den Transaktionen in der aktuellen Bewertung, kann man schlussfolgern, wie viele Transaktionen ein Verkäufer zwischen zwei aufeinanderfolgenden Bewertungszeitpunkten ausgeführt hat. Die Anzahl der Transaktionen gibt keinen Hinweis auf die genaue Menge der beschafften Substanzen oder den Geldbetrag, der mit jeder Transaktion verbunden ist. Es deutet jedoch auf einen Richtwert der Anzahl der Pakete hin, die möglicherweise verschiedene Rechtsräume bzw. Hoheitsgebiete durchlaufen haben.

Die genannten Zahlen unterschätzen höchstwahrscheinlich die tatsächliche Gesamtzahl der Transaktionen, was damit zusammenhängt, dass unsere Bewertungsmethode nur dann die Anzeige des Anbieterprofils ermöglicht, wenn während unseres Messzeitpunktes ein Angebot aktiv ist. Es ist denkbar, dass Einträge vor dem Scraping entfernt wurden, wodurch sie für die Analyse unsichtbar bleiben. Dies hat zur Folge, dass potenzielle Steigungen der Transaktionen dieser Anbieter nicht berücksichtigt werden können. Des Weiteren müssen die verschiedenen Arten von Anbietern berücksichtigt werden: solche die nur aus Belgien versenden und solche die auch aus anderen Ländern versenden.

Abb. 3 (oben) zeigt die Anzahl der Transaktionen für alle mit Belgien verbundenen Anbieter während der verschiedenen Messperioden. Im Verlauf der DM-Bewertung haben diese 15 Anbieter in einem Zeitraum von 3,5 Monaten rund 800 Transaktionen abgeschlossen. In der gesamten Messperiode von WSM (4,5 Monate) sind dies ungefähr 1300 Transaktionen von 26 verschiedenen Anbietern. Die Anzahl der Transaktionen, die, soweit sich aus diesen Daten ableiten lässt, von ausschließlich belgischen Anbietern gesendet wurden (ohne MOVs), liegt für DM auf dem gleichen Niveau (vgl. Abb. 3). Dies hängt mit der geringeren Anzahl von MOVs und der geringen Anzahl von Versandstandorten

pro MOV – wie oben für DM angegeben – zusammen. Für WSM liegt die Anzahl der ausschließlichen Nicht-MOVs viel niedriger. Dies führt zu fast 750 Transaktionen von 19 Nicht-MOVs bis Mitte April 2019. Insgesamt gab es in dem für beide Märkte gemessenen Zeitraum mindestens 1550 erfolgreiche Transaktionen, die wahrscheinlich belgischen Versandursprungs sind.

3.4 Versandziele

Kryptomarktanbieter geben auch an, wohin sie ihre Produkte liefern. Das System für Versandziele funktioniert für beide Märkte leicht unterschiedlich, da DM nur eine sehr begrenzte Spezifikation zuließ, während WSM-Anbieter eine detaillierte Beschreibung in Form einer Liste angeben konnten, wohin die Waren gesendet werden sollen und wohin nicht. Es gibt zwei Metriken von potenziellem Interesse (Broséus et al. 2017): Versandziele belgischer Anbieter und Anbieter (ob belgisch oder nicht belgisch) mit Versandziel „Belgien“.

Der erste allgemeine Trend bei den belgischen DM-Anbietern zeigt den weltweiten und den EU-Versand als die am häufigsten angegebenen Ziele (Tab. 5). Der erwähnte Anbieter mit einer großen Anzahl von Angeboten im November 2018 gibt an, weltweit und in die USA zu versenden, was diese beiden Ziele zu den am häufigsten vorkommenden Zielen im November machte. In den anderen untersuchten Monaten stellen die Versandziele EU, Großbritannien und weltweit die Top-3-Liste. Im letzten Messmonat wurden bemerkenswerterweise mehrere Produkte nur nach Belgien gesendet. Diese wenigen innerbelgischen Angebote stammen alle von einem einzigen Anbieter und beziehen sich alle auf den Verkauf von Cannabis.

Tab. 5 DM Anbieter Belgien – Versand nach

	23.11.2018	19.12.2018	24.01.2019	06.03.2019
WW	361	49	57	78
EU	36	8	65	82
GB	2	0	33	82
US	322	0	0	24
CH	0	0	21	0
BE	0	0	0	5
IE	1	0	0	0
TOTAL	722	57	176	271

Das Versandziel der WSM-Verkäufer entspricht in gewissem Maße dem Versandzielen auf DM. Alle belgischen Anbieter geben an, entweder innerhalb der EU oder weltweit zu versenden. WSM erlaubt jedoch das Hinzufügen oder Ausschließen bestimmter Länder. Insbesondere Ozeanien und Nordamerika werden relativ häufig ausgeschlossen, möglicherweise aufgrund der erhöhten Grenzsicherung und des hohen Strafmaßes für Drogenhandel (Broséus et al. 2017).

Letztendlich sind Anbieter, die ihre Produkte ausschließlich nach Belgien liefern, während unseres Messzeitraums so gut wie nicht vorhanden (mit Ausnahme des oben erwähnten Falles). Die Gründe dafür liegen auf der Hand: Zum einen deckt die EU als Versandziel Belgien bereits mit ab, zum anderen besteht in Belgien keine ungewöhnlich strenge Überwachung der Zollpost. Bestellungen aus einem Land innerhalb der EU (oder eher innerhalb des Schengen-Raums) könnten daher immer noch unter das fallen, was Norbutas (2018) als lokale Nischen (local niches) bezeichnet.

3.5 Kategorien angebotener Substanzen: Allround-Märkte

Der belgische Markt ist in Bezug auf die verschiedenen angebotenen Substanzen sehr vielfältig. Betrachtet man DM (Tab. 6) kommen Amphetamin, MDMA, XTC/Pillen und Kokain relativ kontinuierlich vor, sodass man diese unter der Superkategorie „Stimulanzien“ verzeichnen kann. Ketamin, (verschreibungspflichtige) Opioide[3], Cannabis und Benzodiazepine wurden dagegen nicht immer angeboten. Andere Arzneimittel[4] (in diesem Fall Dextroamphetamin) und Substanzen der Kategorie 2C-x traten wiederum während der Scrapingperiode nur einmal auf.

Bei DM gibt es den Unterschied zwischen Allround-Anbietern (die mehrere Kategorien von Substanzen verkaufen) und Anbietern, die nur eine einzige Kategorie anbieten. Während der neuesten und größten Messung für DM von Anfang März 2019, verkauften fünf von neun Anbietern nur eine einzige Substanz, während die anderen vier zwei oder mehr Substanzen anboten. Im Januar 2019 vertrieben vier von acht Anbietern Einzelsubstanzen, während es in den Monaten

[3](Verschreibungspflichtige) Opioide sowie alle natürlichen und synthetischen Opioide, einschließlich z. B. Oxycodon, Heroin und Morphin, jedoch nicht Fentanyl wegen des aktuellen öffentlichen Interesses an der Substanz (z. B. Ball et al. 2019).

[4]Diese Kategorie umfasst Substanzen, die generell verschreibungspflichtig sind (Van Buskirk et al. 2016). Im belgischen Abschnitt des CRYPTODRUG-Datensatzes sind dies Viagra, Modafinil, Dextroamphetamin und Ritalin.

Tab. 6 WSM Wachstum Belgien – Versand nach

	26.11. 2018	20.12. 2018	24.01. 2019	22.02. 2019	25.03. 2019	04.04. 2019	10.04. 2019	17.04. 2019
WW	20	20	22	19	10	20	34	46
WW, IUS	9	10	8	10	10	10	10	10
EU	5	10	10	9	8	9	8	7
WW, !BE*, INL	0	0	0	3	4	5	6	0
WW, !US, !AU	0	0	2	2	2	2	0	0
WW, !US, !NZ	0	0	0	0	1	1	1	1
WW, !US, !RU, !JP, !AU	0	0	0	1	2	1	1	0
WW, !INZ, !CA	0	0	0	0	1	1	1	1
WW, !NZ	0	0	0	0	0	0	0	0
WW, !US, !NZ, !AU	1	1	2	1	0	0	0	0
TOTAL	35	41	44	45	48	57	61	65

* ! bezeichnet „*kein* Versand nach“

zuvor drei von vier bzw. drei von fünf waren. Die Anbieter von Einzelsubstanzen verkauften in dem gemessenen Zeitraum LSD, Amphetamin, MDMA, XTC/Pillen, Benzos oder Cannabis.

Auf WSM ist das Angebot vielfältiger: Von den 18 verwendeten Kategorien waren unter den belgischen Angeboten bei jeder Messung mindestens 14 vertreten (Tab. 7). Obwohl die Anzahl der Angebote pro Kategorie eher gering ist, und der beobachtete Trend daher für geringfügige Veränderungen anfällig ist, bleibt festzuhalten, dass die Kategorie XTC/Pillen die am häufigsten angebotene Substanz ist.

Tab. 7 WSM Anbieter Belgien – Kategorien

	23.11. 2018	19.12. 2018	24.01. 2019	06.03. 2019	04.04. 2019	10.04. 2019	17.04. 2019
2X-x	1	1	1	1	1	1	1
Benzos/ Relaxantien	2	1	0	0	0	0	1
Cannabis	4	4	4	7	9	7	6
Kokain	1	3	4	3	6	6	6
Ketamin	1	1	2	2	2	2	2
Halluzino-gene	1	1	1	1	1	1	1
MDMA	1	3	2	3	4	9	13
Metham-phetamine	2	2	0	1	2	2	1
(Vorgeschr.) Opioide	4	5	6	6	7	7	7
Andere Arznei-mittel	3	6	6	1	2	0	1
Drogenaus-gangsstroffe	1	1	1	1	1	1	1
RCs/NPs	4	4	4	4	4	4	4
Amphet-amine	3	4	3	5	5	5	5
Synthe-tisches Cannabis	0	0	0	0	0	0	0
Tabak	0	0	1	1	1	2	2
Unbekannt/ andere	3	3	3	3	5	5	5
XTC/Pillen	2	6	5	7	7	9	12
Fentanyl	0	0	0	0	0	0	0

Der Anteil der Anbieter von Einzelsubstanzen lag bei WSM bei vier von acht im November 2018, bei vier von zehn Ende Dezember 2018, bei sechs von elf im Januar 2019, bei sieben von elf im Februar und bei acht von 14 bis Ende März. In den darauffolgenden Wochen belief sich der Anteil auf 10 von 19, auf 10 von 18 und auf neun von 19. Auch hier erkennt man, ähnlich wie bei DM, keine Spezialisierung hinsichtlich einiger weniger Substanzen. Einzelanbieter verkauften Substanzen aus mehr als zehn Kategorien.

Zusätzlich zu den bei DM gefundenen Kategorien gibt es auch ein konsequentes Angebot an Forschungschemikalien (RCs)/NPS[5], das hier aus Methoxetamin (MXE), Mephedron (4MMC) und 4-Fluoramphetamin (4-FA) besteht. Ähnlich verhält sich das Anbieten von Drogenausgangsstoffen wie Pseudoephinedrin, das zur Herstellung von anderen Substanzen verwendet werden kann. Unter der Überschrift „Unbekannt/andere“ wurden Kladden mit einer nicht identifizierten Substanz, ein Leitfaden für den Marihuana-Anbau und benutzerdefinierte Angebote für einzelne Kunden mit nicht identifizierten Substanzen aufgeführt.

Neben den auf DM und WSM tatsächlich vorhandenen Substanzen sind auch einige nicht angebotene Substanzen von Interesse. Obwohl zu erwarten ist, dass Substanzen, die häufig in einem Land verwendet werden, in diesem Land im Internet verfügbar sind, ist dies nicht unbedingt der Fall. So hat zum Beispiel keiner der Märkte synthetische Cannabinoide im Angebot, obwohl ihre Präsenz vor Ort in Belgien nicht zu vernachlässigen ist (Richeval et al. 2018). Zwar ist Ball et al. (2019) zufolge in Zukunft mit einer gewissen Präsenz von Fentanyl auf den Märkten zu rechnen. Zumindest für Belgien ist dies jedoch (noch) nicht der Fall.

4 Diskussion

4.1 Der illegale Drogenhandel auf Kryptomärkten nimmt zu: Springen belgische Anbieter auf diesen Zug?

Der illegale Drogenhandel im Internet könnte als eine Ausweitung der kriminellen Aktivitäten im Allgemeinen und des Drogenhandels im Besonderen angesehen werden (Broséus et al. 2016). Dennoch macht der illegale Drogenhandel auf

[5]Neue psychoaktive Substanzen: Substanzen, die nicht in den wichtigsten internationalen Drogenabkommen enthalten sind, jedoch klassische Drogen durch minimale chemische Veränderungen nachahmen (z. B. Van Buskirk et al. 2017).

Kryptomärkten weniger als 1 % des weltweiten Drogenhandelsumsatzes aus (Décary-Hétu und Giommoni 2016). Der Marktanteil ist im Vergleich zum allgemeinen Drogenhandel damit gering. Angaben aus dem Jahr 2016 zufolge beläuft sich der Umsatz auf Kryptomärkten auf schätzungsweise US$170 bis US$300 Millionen pro Jahr (UNODC 2018), während sich der weltweite Umsatz mit dem Drogenhandel auf geschätzt US$426 bis US$652 Mrd. beläuft (May 2017; Kowalski et al. 2019).

Die Anzahl von Angeboten und Anbietern in Bezug auf Belgien folgt bis zu einem gewissen Grad dem globalen Wachstumsmuster: So zeigt die Anzahl der getätigten Transaktionen eindeutig einen starken und beständigen Wachstumstrend. Der belgische Marktanteil macht dabei jedoch nur einen kleinen Bruchteil des globalen Gesamtmarktes aus. Im Vergleich zu anderen Nationalitäten sind belgische Anbieter und Angebote mit weniger als 1 % relativ beschränkt. Dieselben Erkenntnisse wurden auch auf anderen Kryptomärkten gefunden. Zum Vergleich: Eine Längsschnittanalyse eines Marktes namens „Evolution“ von Broséus et al. (2017) gibt an, dass Belgien im Jahr 2015 einen Anteil von rund 1,3 % an der weltweiten Anzahl drogenbezogener Angebote auf diesem Kryptomarkt hatte. Tzanetakis (2018) kam bei ihrer Analyse von Alphabay in den Jahren 2015–2016 zu dem Ergebnis, dass der belgische Anteil – obwohl Belgien Top 15-Herkunftsland der Anbieter war – nur rund 0,4 % des Gesamthandels deckte (in den meisten Fällen – 25,3 % – wurden die Pakete aus den USA verschickt). Es muss allerdings auch festgestellt werden, dass das Herkunftsland des Anbieters häufig (in etwa 25 % der Fälle) unbekannt oder nicht eindeutig war (Tzanetakis 2018).

Studien zu verschiedenen Kryptomärkten zeigen, dass Cannabis, synthetische Drogen (MDMA und Amphetamine) und Kokain die beliebtesten online verkauften Drogen sind und etwa 70 % aller Verkäufe ausmachen (Paquet-Clouston et al. 2018; Soska und Christin 2015). Zum Vergleich: Das belgische Drogenangebot auf den untersuchten Kryptomärkten weist keine ausgeprägte Spezialisierung auf, da eine Vielzahl von Drogenkategorien von Cannabis bis Ketamin angeboten wird. Synthetische Drogen wie MDMA und Amphetamine sind jedoch kontinuierlich und überdurchschnittlich häufig vertreten. Dies mag daran liegen, dass diese Produkte von belgischen Anbietern problemlos bezogen werden können. Belgien ist zusammen mit den Niederlanden das Hauptproduktionsland von MDMA und Amphetaminen und diese Produkte werden aufgrund ihrer Position in der Lieferkette weltweit mit hohen Gewinnen vertrieben (Colman et al. 2018; Tops et al. 2018).

4.2 Die Darkweb-Umgebung und Risikominderung

Aufgrund des Potenzials, illegale Drogen über die physische Umgebung der Anbieter hinaus zu verbreiten, könnten Kryptomärkte, im Vergleich zum Offline-Handel, eine (relativ) anonyme und (als sicher empfundene) Plattform für den Handel mit illegalen Drogen darstellen (Aldridge et al. 2017). Obwohl verschiedene Arten von Risiken wie Geldverlust, Exit-Scams, Beschlagnahme durch den Zoll oder Arten von Gewalt wie Doxing auftreten, weisen Kryptomarktteilnehmer darauf hin, dass ein geringeres Risiko im Zusammenhang mit dem illegalen Drogenhandel auf Kryptomärkten wahrgenommen wird (Barratt et al. 2016). Dieses geringere Risiko könnte als die geringere Wahrscheinlichkeit angesehen werden, von den Strafverfolgungsbehörden entdeckt oder mit Begleit- und Beschaffungsdelikten konfrontiert zu werden wie z. B. „Abzocke“, Gewalttaten zur Aufrechterhaltung des Ansehens oder der Wiederherstellung von Verlusten (Barratt et al. 2016). Schließlich erfordern Kryptomärkte keinen direkten Kontakt zwischen den beteiligten Parteien. Und wie bereits erwähnt, erfordert der Zugang zu Kryptomärkten die Verwendung des anonymisierenden Netzwerk-Routing-Protokolls im Tor-Netzwerk, was die Verwendung manueller oder sogar automatisierter Verschlüsselung aller Kommunikation über PGP-Kryptografie erfordert. Außerdem müssen Zahlungen in digitalen Währungen abgewickelt werden, um die Identität des Anbieters zu schützen (Roxburgh et al. 2017).

Kryptomärkte erleichtern den grenzüberschreitenden Drogenhandel. Infolgedessen stellt der Versand über den regulären Postweg für die Täter ein hohes Risiko dar, insbesondere wenn die illegalen Drogen über die internationalen Grenzen hinaus versendet werden (Décary-Hétu et al. 2016). Es ist dann schließlich das erste Mal, dass die virtuellen Kryptomarkttransaktionen die Offline-Umgebung erreichen.

In Übereinstimmung mit Studien zu anderen Regionen (Broséus et al. 2016) ergab diese Studie, dass belgische Anbieter im Allgemeinen international versenden, und zwar sowohl EU-weit als auch weltweit. Obwohl es nicht in allen Fällen möglich war, die spezifischen Versandziele zu identifizieren, weist dies darauf hin, dass belgische Anbieter in der Lage und bereit sind, grenzüberschreitend zu versenden. Nur ein belgischer Anbieter (fünf Einträge, sichtbar auf DM) gibt an, dass er ausschließlich bereit war, alle Einträge im Inland zu versenden, möglicherweise um die Wahrscheinlichkeit zu verringern, dass die Ware von den Strafverfolgungsbehörden beschlagnahmt wird. Wie von Norbutas (2018) erwähnt, könnte der inländische Drogenhandel mit Hilfe von Kryptomärkten

unterschätzt werden, da keine Informationen über das Herkunftsland des Verkäufers vorliegen, was die Berechnungen des Anteils internationaler Sendungen aus Kryptomärkten erschwert. Norbutas (2018) weist ferner darauf hin, dass Kryptomärkte zwar die Möglichkeit des Zugangs zu weltweiten Märkten implizieren, aber durch rationale Kosten – und Nutzenberechnungen (in Bezug auf die Ermittlung durch die Strafverfolgungsbehörden oder die Lieferzeit) – eine geografische Zentrierung (insbesondere im Inland) von Anbietern und Käufern die Folge sein könnte.

Jüngste Untersuchungen haben in der Tat gezeigt, dass die Anbieter zunehmend über das Risiko der Enttarnung besorgt sind und dies möglicherweise die Entwicklung des Online-Marktes beeinflusst. Ebenso interessant sind die Zielländer, in die belgische Verkäufer nicht liefern sowie die sich ändernden Versandstandorte. Einige belgische Anbieter geben beispielsweise an, dass sie nicht nach Nordamerika oder in die Niederlande liefern. Dies könnte auf die strengeren Sanktionen gegen den illegalen Drogenhandel in Amerika und die verstärkte Aufmerksamkeit der niederländischen Behörden für die Bekämpfung des illegalen Drogenhandels zurückzuführen sein, im Ergebnis also ein wahrgenommenes erhöhtes Entdeckungsrisiko. Angesicht der Tatsache, dass die Niederlande als einer der weltweit wichtigsten Anbieter von synthetischen Drogen gelten (Tops et al. 2018), könnte darüber hinaus die niederländische Frankierung internationaler Pakete bei ausländischen Zollbehörden Verdacht erregen.

Obwohl die Mehrheit der belgischen Verkäufer ausschließlich aus Belgien versendet, nutzen einige Anbieter ebenfalls andere Versandorte, wie z. B. die Niederlande oder Deutschland. Dies könnte auch das Ergebnis der wahrgenommenen Effektivität der Strafverfolgung bei der Erkennung von Postpaketen im eigenen Land sein, wie aus der Studie von Décary-Hétu et al. (2016) hervorgeht.

4.3 Belgien und die Niederlande: Ein Spielfeld?

Jüngste Forschungsergebnisse haben den Zusammenhang zwischen dem niederländischen und dem belgischen Drogenmarkt festgestellt, insbesondere dem Cannabismarkt und dem Markt für synthetische Drogen (Colman et al. 2018). Der professionelle Cannabisanbau und der Produktionsmarkt für synthetische Drogen in Belgien haben sich hauptsächlich durch den Zusammenschluss von belgischen und niederländischen Gruppen, die der organisierten Kriminalität zugeordnet werden können. Dieser Zusammenschluss erfolgte auf dem synthetischen Produktionsmarkt viel früher als beim Cannabisanbau. In den neunzi-

ger Jahren begannen niederländische kriminelle Organisationen im Süden der Niederlande, sich auf die Herstellung synthetischer Drogen im belgisch-niederländischen Grenzgebiet zu konzentrieren. Im Laufe der Zeit erstreckte sich diese belgisch-niederländische Zusammenarbeit auf die gesamte Kette der Herstellung und des Handels mit synthetischen Drogen und Cannabis.

Angesichts der gemeinsamen Rolle Belgiens und der Niederlande bei der Herstellung und dem Handel mit Cannabis und insbesondere auch mit synthetischen Drogen wäre es interessant zu überprüfen, ob dieser Zusammenhang auch auf den Online-Drogenmärkten zu finden ist. Es gibt Hinweise auf diesen Zusammenhang in der aktuellen CRYPTODRUG-Studie. Wie bereits erwähnt, versenden einige Anbieter sowohl aus Belgien als auch aus den Niederlanden. Ungefähr 45 % der MOV-Angebote auf WSM werden sowohl aus Belgien als auch aus den Niederlanden verschickt. Die wenigen MOV-Angebote, die auf DM angezeigt werden, stammen mit einer Ausnahme (Deutschland) aus den Niederlanden und Belgien. Ein Einzelfall, der diesbezüglich Erwähnung verdient, ist ein Versender aus Luxemburg, der angibt weltweit zu versenden mit Ausnahme von Luxemburg, den Niederlanden und Belgien.

Diese Daten implizieren die Nutzung der niederländisch-belgischen Grenze für den illegalen Drogenhandel. Um diesen Zusammenhang zu ergründen, sind jedoch weitere Untersuchungen, insbesondere mit anderen Methoden, erforderlich. So ist es beispielsweise ungewiss, ob die Taktik der organisierten Kriminalität (Ausnutzung der Unterschiede beider Rechtsgebiete) in irgendeiner Weise mit den Praktiken zusammenhängt, die während des CRYPTODRUG-Projekts beobachtet wurden (Anbieter wechseln beispielsweise den Standort, um einen verdächtigen Stempel auf dem Paket zu vermeiden).[6]

4.4 Werden Kryptomärkte weiter wachsen?

Seit das derzeitige System des illegalen Drogenhandels in Darknet Anfang 2010 Einzug fand, sind die Schätzungen hinsichtlich des Umsatzes und der Anzahl der Konsumenten gestiegen. Die Benutzerfreundlichkeit und die Wahrnehmung von Kryptomärkten als Mittel zur Beschaffung von Drogen mit begrenztem Risiko

[6]Für den deutschsprachigen Raum haben Tzanetakis und Stöver (2019) einige Anknüpfungspunkte zwischen organisierter Kriminalität und dem Drogenhandel im Darknet näher beleuchtet.

könnten unter anderem dazu führen, dass immer mehr Verbraucher auf diese Märkte gelangen (EMCDDA 2017).

Obwohl umfangreiche disruptive Maßnahmen von Strafverfolgungsbehörden wie die „Operation Bayonet“ kurzfristige Auswirkungen haben, werden Marktlücken schnell durch neue oder bestehende Märkte und Anbieter geschlossen. Dabei werden häufig technische Sicherheitsupdates installiert, mit der Folge, dass der Prozess von vorne beginnt (Ladegaard 2019). Man kann den Zustand in der Zeit nach einem Eingriff der Strafverfolgungsbehörden in der Online-Welt (Drogenhandel auf Kryptomärkten) in etwa vergleichen mit der geographischen Verlagerung von Teilnehmern in der Offline-Welt (Décary-Hétu und Giommoni 2016). So kann der verstärkte Fokus einer Strafverfolgungsbehörde auf eine bestimmte Offline-Straftat in einer bestimmten Gegend (z. B. Straßendrogenhandel oder illegale Prostitution in einer bestimmten Straße) dazu führen, dass die Aktivitäten an einem anderen Ort wieder aufgenommen werden, nachdem die Polizei eingegriffen hat. Die von Décary-Hétu und Giommoni (2016) beschriebene Verlagerung auf andere Märkte im Cyberspace könnte das Online-Äquivalent einer solchen Dynamik sein: Nach der Schließung eines Marktes scheinen viele Benutzer ihre Angebote zu verlagern und ihre Aktivitäten auf anderen Märkten fortzusetzen. Die CRYPTODRUG-Forschungsergebnisse legen das gleiche nahe.

4.5 Vieles bleibt unerwähnt

Im Gegensatz zu Offline-Drogenmärkten ermöglichen Kryptomärkte die Erfassung und Analyse von „öffentlich zugänglichen“ Marktdaten wie generierte Einnahmen, die Art und die Menge der angebotenen Drogen, sowie von Anbietern selbst angegebene Herkunfts- und Zielländer und des Durchschnittspreises. Forscher nutzen diese Gelegenheit zu Recht, um Daten über illegale Drogentransaktionen in beispiellosem Umfang und mit beispielloser Genauigkeit zu sammeln. Es gibt jedoch verschiedene Einschränkungen, die bei dieser Art von Daten zu beachten sind.

Erstens gibt es, wie oben erläutert, verschiedene Verschleierungstechniken, die von Anbietern auf diesen Märkten verwendet werden, um die Möglichkeit der Erkennung einzuschränken. Einige davon können gemessen werden (z. B. die Verschiebung des Versandursprungsortes im Laufe der Zeit), aber Anbieter melden möglicherweise ihren Standort absichtlich falsch oder gar nicht (viele Angebote versenden z. B. von „weltweit“).

Erkenntnisse über die Verbraucherseite bei Kryptomärkten sind weiterhin begrenzt, insbesondere im Hinblick auf das Verhältnis zwischen denjenigen Akteuren, die ihre Substanzen offline beschaffen, und denen, die auf Kryptomärkten einkaufen. Daten aus dem *Global Drug Survey* (2016) zeigen beispielsweise, dass die Mehrheit der Käufer von Kryptomarkt-Substanzen Drogenkonsumenten sind, die schon zuvor Drogen konsumiert haben. Lediglich 5 % der Einkäufer auf Kryptomärkten konsumierten überhaupt keine Drogen, bevor sie Zugang zum Kryptomarkt hatten. Von den Käfern gaben 32,1 % an, auf ein breiteres Spektrum von Drogen zugegriffen haben als zuvor. Daher vermuten wir, dass Kryptomärkte die einzelnen Drogenkarrieren beeinflussen können, und zwar einschließlich Beginn, Häufigkeit, Intensität, Eskalation, Umstellung, Expansion, Substitution und Genesung. Untersuchungen haben außerdem gezeigt, dass Konsumenten Drogen online kaufen, weil sie eine höhere Anonymität und Sicherheit, eine bessere Qualität, eine größere Auswahl an Drogen und mehr Komfort als auf Offline-Märkten wahrnehmen. Dies deutet darauf hin, dass sich der Drogenhandel im Internet in Bezug auf Nutzerbasis und Motive entscheidend von Offline-Käufern und -Verkäufern von Drogen unterscheidet (Barratt et al. 2016; Kruithof et al. 2016).

Eine teilweise Aufhebung dieser Einschränkungen könnte in der Verwendung zusätzlicher Methoden liegen, um so eine ganzheitliche Sicht auf das Phänomen zu schaffen. Qualitative Ansätze wie Interviews mit (verurteilten) Anbietern oder die Erstellung von Übersichten verfügbarer juristischer Dokumentation, die in Kryptomarktfällen verwendet wurden, könnten nützliche Informationen liefern. In ähnlicher Weise fordern EMCDDA und Europol (EMCDDA 2017) die Forschungsgemeinschaft auf, sich bei Untersuchungen mehr auf Motive und Gründe für den Kauf von Substanzen auf Kryptomärkten zu konzentrieren. Die nächsten Schritte im CRYPTODRUG-Projekt sind Benutzerumfragen und -interviews, die möglicherweise einige der Wissenslücken über die belgischen Kryptomarkt-Benutzer schließen können.

Literatur

Aldridge, J., & Décary-Hétu, D. (2016). Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. *International Journal of Drug Policy, 35,* 7–15.

Aldridge, J., Stevens, A., & Barratt, M. (2017). Will growth in cryptomarket drug buying increase the harms of illicit drugs? *Addiction, 113,* 789–796.

Ball, M., Broadhurst, R., & Trivedi, H. (2019). *How Much Fentanyl is Available on the Darknet?* Statistical Bulletin No. 18 (Australian Institute of Criminology).

Barratt, M., & Aldridge, J. (2016). Everything you always wanted to know about cryptomarkets* (*but were too afraid to ask). *International Journal of Drug Policy, 35,* 1–6.

Barratt, M., Ferris, J., & Winstock, A. (2013). Use of silk road, the online drug marketplace, in the United Kingdom, Australia, and the United States. *Addiction, 109,* 774–783.

Barratt, M., Ferris, J., & Winstock, A. (2016). Safer scoring? Cryptomarkets, social supply and drug market violence. *International Journal of Drug Policy, 35,* 24–31.

BKA. (2019). Festnahme der Mutmaßlichen Verantwortlichen des Weltweit Zweitgrößten Illegalen Online-Marktplatzes im Darknet „Wall Street Market" und Sicherstellung der Server des Marktplatzes. https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2019/Presse2019/190503_WallStreetMarket.html;jsessionid=B9263CD8A38588520F76B599D79B35DC.live0612. Zugegriffen: 23. Juli 2019.

Broséus, J., Rhumorbarbe, D., Mireault, C., Ouellette, V., Crispino, F., & Décary-Hétu, D. (2016). Studying illicit drug trafficking on darknet markets: structure and organisation from a canadian perspective. *Forensic Science International, 264,* 7–14.

Broséus, J., Rhumorbarbe, D., Morelato, M., Staehli, L., & Rossy, Q. (2017). A geographical analysis of trafficking on a popular darknet market. *Forensic Science International, 277,* 88–102.

Christin, N. (2013). Traveling the silk road: A measurement analysis of a large anonymous online marketplace. In Proceedings of the 22nd international world wide web conference, Rio de Janeiro, Brazil.

Colman, C. (Hrsg.), De Middeleer, F., Spapens, A., Van Nimwegen, S., Ceulen, R., Gerbrands, S., Paoli, L., & Roevens, E. (2018). *De grens voorbij – Belgische en Nederlandse drugsmarkten in beweging.* Den Haag: Boom Criminologie.

Darknetlive. (2019). Darknet markets. https://darknetlive.com/darknet-market-list/. Zugegriffen: 10. Aug. 2019.

Décary-Hétu, D., & Giommoni, L. (2016). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of operation onymous. *Crime, Law, and Social Change, 61,* 55–75.

Décary-Hétu, D., Paquet-Clouston, M., & Aldridge, J. (2016). Going international? Risk taking by cryptomarket drug vendors. *International Journal of Drug Policy, 35,* 69–76.

DeepDotWeb. (2019). Updated: List of dark net markets (Tor & I2P). https://www.gwern.net/docs/sr/2019-04-22frenchdarknetdeepdotweb-dnmlist.html. Zugegriffen: 10. Aug. 2019.

DeepWebSitesLinks. (2019). Wallstreet market review – Alternative darknet marketplace. https://www.deepwebsiteslinks.com/wallstreet-market-review/. Zugegriffen: 23. Juli 2019.

Dolliver, D. S. (2015). A rejoinder to authors: Data collection on Tor. *International Journal of Drug Policy, 26,* 1128–1129.

Duxbury, S., & Haynie, D. (2017). The network structure of opioid distribution on a darknet cryptomarket. *Journal of Quantitative Criminology, 34,* 921–941.

EMCDDA. (2017). *Drugs and the darknet: Perspectives for enforcement, research and policy*. Luxembourg: EMCDDA-Europol Joint Publications, Publications Office of the European Union.

Kowalski, M., Hooker, C., & Barratt, M. J. (2019). Should we smoke it for you as well? An ethnographic analysis of a drug cryptomarket environment. *International Journal of Drug Policy, 73,* 245–254.

Kruithof, K., Aldridge, J., Décary-Hétu, D., Sim, M., Dujso, E., & Hoorens, S. (2016). *Internet-facilitated drugs trade an analysis of the size, scope and the role of the Netherlands*. Santa Monica: RAND Corporation.

Ladegaard, I. (2019). Crime displacement in digital drug markets. *International Journal of Drug Policy, 63,* 113–121.

Markoff, J. (2005). *What the dormouse said: How the sixties counterculture shaped the personal computer industry*. London: Penguin.

Martin, J. (2014a). *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs*. London: Palgrave Macmillan.

Martin, J. (2014b). Lost on the Silk Road: Online drug distribution and the ‚cryptomarket'. *Criminology & Criminal Justice, 14*(3), 351–367.

May, C. (2017). *Transnational crime and the developing world*. Washington, District of Columbia: Global Financial Integrity.

Nielandt, J., Bronselaer, A., & De Tré, G. (2016). Predicate enrichment of aligned XPaths for wrapper induction. *Expert Systems with Applications, 51,* 259–275.

Norbutas, L. (2018). Offline constraints in online drug marketplaces: An exploratory analysis of a cryptomarket trade network. *International Journal of Drug Policy, 56,* 92–100.

Paoli, G. P., Aldridge, J., Ryan, N., & Warnes, R. (2017). *Behind the curtain: The illicit trade of firearms, explosives and ammunition on the dark web*. Santa Monica: RAND Corporation.

Paquet-Clouston, M., Décary-Hétu, D., & Morselli, C. (2018). Assessing market competition and vendors' size and scope on alphabay. *International Journal of Drug Policy, 54,* 87–98.

Richeval, C., Wille, S. M. R., Nachon-Phanithavong, M., Samyn, N., Allorge, D., & Gaulier, J. (2018). New psychoactive substances in oral fluid of French and Belgian drivers in 2016. *International Journal of Drug Policy, 57,* 1–3.

Roxburgh, A., Van Buskirk, J., Burns, L., & Bruno, R. (2017). *Drugs and the internet, issue 9, December 2017*. Sydney: National Drug and Alcohol Research Centre.

Soska, K., & Christin, N. (2015). Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. In Paper presented at the 24th USENIX security symposium.

Tops, P., van Valkenhoef, J., van der Torre, E., & van Spijk, L. (2018). *Waar een klein land groot in kan zijn: Nederland en synthetische drugs in de afgelopen 50 jaar*. Den Haag: Boom Criminologie.

Torproject. (2019). Objective 1, activity 2: Denial of service defences. https://trac.torproject.org/projects/tor/ticket/29999. Zugegriffen: 15. Juli 2019.

Tzanetakis, M. (2018). Comparing cryptomarkets for drugs. A characterisation of sellers and buyers over time. *International Journal of Drug Policy, 56,* 176–186.

Tzanetakis, M., & Stöver, H. (Hrsg.). (2019). *Drogen, Darknet und Organisierte Kriminalität – Herausforderungen für Politik, Justiz und Drogenhilfe*. Baden-Baden: Nomos.

UNODC. (2018). *World drug report 2018*. Vienna: United Nations.

Van Buskirk, J., Roxburgh, A., Bruno, R., & Burns, L. (2014). *Drugs and the internet, issue 3*. Sydney: National Drug and Alcohol Research Centre.

Van Buskirk, J., Naicker, S., Roxburgh, A., Bruno, R., & Burns, L. (2016). Who sells what? Country specific differences in substance availability on the Agora cryptomarket. *International Journal of Drug Policy, 35,* 16–23.

Van Buskirk, J., Griffiths, P., Farrell, M., & Degenhardt, L. (2017). Trends in new psychoactive substances from surface and "dark" net monitoring. *The Lancet Psychiatry, 4*(1), 16–18.

Van Hout, M., & Bingham, T. (2013). 'Surfing the Silk Road': A study of users' experiences. *International Journal of Drug Policy, 24,* 524–529.

ZDNet. (2019). Top dark web marketplace will shut down next month. Abgerufen von https://www.zdnet.com/article/top-dark-web-marketplace-will-shut-down-next-month/.

Cyberangriffe gegen private Internetnutzer*innen

Gleiches Risiko für alle?

Arne Dreißigacker, Bennet von Skarczinski, Marie Christine Bergmann und Gina Rosa Wollinger

1 Einleitung

In wenigen Jahren nahm die Digitalisierung und weltweite Vernetzung sehr stark zu und hat immer größere Auswirkungen auf unsere Kommunikation und viele Bereiche unseres Lebens (Initiative D21 e. V. 2016, 2018; Papsdorf 2013; Stengel 2017). Neben den unzähligen Chancen und Potenzialen zur Steigerung der Lebensqualität hat diese Entwicklung auch ihre Schattenseiten wie die zunehmende Cyberkriminalität (Huber 2015, S. 396; Münch 2017, S. 10 f.).[1]

[1]Nach Ziercke (2016, S. 240) hat Cybercrime das „Potenzial zum Massendelikt"; Rüdiger (2018) spricht in Anlehnung an die Broken Windows Theorie vom „Broken Web".

Der Beitrag basiert auf dem englischsprachigen Artikel von Bergmann et al. (2018).

A. Dreißigacker (✉) · B. von Skarczinski
Kriminologisches Forschungsinstitut Niedersachsen e. V., Hannover, Deutschland
E-Mail: arne.dreissigacker@kfn.de

B. von Skarczinski
E-Mail: bennet.skarczinski@kfn.de

M. C. Bergmann
Sozialwissenschaftlichen Dienst der Zentralen Polizeidirektion Niedersachsen, Hannover, Deutschland
E-Mail: marie-christine.bergmann@polizei.niedersachsen.de

G. R. Wollinger
Hochschule für Polizei und öffentliche Verwaltung NRW, Köln, Deutschland
E-Mail: ginarosa.wollinger@hspv.nrw.de

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

T.-G. Rüdiger und P. S. Bayerl (Hrsg.), *Cyberkriminologie,*
https://doi.org/10.1007/978-3-658-28507-4_13

In Anbetracht der rasanten Verbreitung von vernetzten und zunehmend mobilen Endgeräten betrifft dies nicht nur Unternehmen (Rantala 2008), Staaten und deren Institutionen (Bollhöfer und Jäger 2018; Steinbicker 2012; Ziercke 2016), sondern jede einzelne Privatperson, die digitale Inhalte und entsprechende Endgeräte nutzt (BITKOM/Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. 2014; Nurse und Bada 2019). Eine Umfrage der Deutsche Telekom AG (2016) weist darauf hin, dass bereits 48 % der Deutschen Opfer von Internetkriminalität wurden. Weltweit wurden 65 % aller Internetnutzer Opfer von Cyberkriminalität, gibt eine Studie des Softwareunternehmens Symantec (2010) an.

Strafrechtlich gesehen umfasst Cyberkriminalität einen weitreichenden Deliktsbereich. Hierzu zählen Straftaten wie Betrug, sexuelle Belästigung oder Bullying, die mittels des Internets begangen werden. Diese werden häufig unter „Cyberkriminalität im weiteren Sinn“[2] gefasst, da das Internet und darüber verbundene IT-Systeme lediglich als „Tatmittel“ dienen und nicht das eigentliche Ziel des Angriffs darstellen. Sie werden in der Regel unter schon lange bestehende Straftatbestände innerhalb des Strafgesetzbuches (StGB) subsumiert. Demgegenüber werden mit „Cyberkriminalität im engeren Sinn“ Straftaten umfasst, die erst mit der digitalen Vernetzung möglich wurden und sich primär gegen IT-Systeme bzw. digitale Daten richten. Für diese Delikte wurden neue Straftatbestände im StGB geschaffen. Dazu gehören z. B. das Ausspähen oder Abfangen von Daten (§§202a, 202b und 202c StGB), die Datenhehlerei (§202d StGB), die Datenveränderung oder die Computersabotage (§§303a und 303b StGB).

Die kriminologische Forschung, die sich mit Cyberkriminalität befasst, fokussiert vergleichsweise häufig Delikte aus dem Bereich „Cyberkriminalität im weiteren Sinne“ (Chen et al. 2016; Fansher und Randa 2018; Näsi et al. 2017; Tsitsika et al. 2015; Wegge et al. 2016), wobei allgemein immer noch relativ wenig kriminologische Forschungen vorliegen, insbesondere im deutschsprachigen Raum (Huber 2015; Meier 2012; s. a. Kap. „Ist der Begriff „Cyberkriminalität“ in Forschung und Praxis hinreichend konturiert und somit adäquater (Sozial-) Kontrolle zugänglich?“).[3] Vor allem fehlen weiterhin Studien, die über eine

[2]Zur Unterscheidung zwischen Cyberkriminalität im weiteren und im engeren Sinn siehe z. B. Council of Europe (2001), Eisele (2016, S. 255), Robertz et al. (2016, S. 2), Seidl und Starnecker (2017, S. 338) und Wall (2004, S. 20).

[3]Einen Überblick über die Dunkelfeldforschung zum Thema Cybercrime in Europa geben Reep-van den Bergh und Junger (2018).

beschreibende Darstellung der Verbreitung von Cyberkriminalität hinausgehen und Einflussfaktoren auf das Viktimisierungsrisiko untersuchen (Meško 2018).

Aus diesem Grund geht der folgende Beitrag anhand einer repräsentativen Bevölkerungsbefragung in Niedersachsen und Schleswig-Holstein ($n = 33.538$) der Frage nach, welche Faktoren das Viktimisierungsrisiko für drei differenzierte Angriffsarten aus dem Bereich „Cybercriminalität im engeren Sinne“ beeinflussen.

2 Untersuchungsgegenstand

Im Gegensatz zu anderen kriminologischen Untersuchungsgegenständen – wie z. B. klassische Eigentumskriminalität – ist die Dunkelfeldforschung insbesondere zum Thema „Cyberkriminalität im engeren Sinne“ mit verschiedenen Schwierigkeiten verbunden (s. a. Kap. „Problematik der Hell- und Dunkelfeldanalyse im Bereich Cybercrime“). Die Variations- und Kombinationsmöglichkeiten von Angriffsvektoren[4], Schadsoftware und Vorgehensweisen der Täter*innen sind im Zuge einer schnellen technologischen Entwicklung kaum mehr zu überblicken.[5] Hinzu kommt, dass das sogenannte absolute Dunkelfeld[6] sehr groß sein dürfte, insofern bestimmte Angriffe oder einzelne Schritte zusammenhängender Angriffe, wie das unbefugte Kopieren und Weitergeben von persönlichen Daten, durch die Opfer häufig gar nicht erkannt werden. Möglicherweise werden deren Folgen zu einem späteren Zeitpunkt offensichtlich, wenn ein konkreter Schaden (z. B. ein Datenverlust oder ein finanzieller Schaden) eingetreten ist. In einer

[4]Als Angriffsvektoren werden Kombinationen von Angriffswegen und -techniken bezeichnet, mit denen sich Angreifer*innen unerlaubt Zugang zu IT-Systemen verschaffen (Bundesamt für Sicherheit in der Informationstechnik 2017, S. 78).

[5]Zum Thema Cyberkriminalität existieren in der kriminologischen Forschung ganz unterschiedliche Herangehensweisen und Perspektiven bei der Differenzierung und Klassifikation von Cyberangriffen. Je nach Fokus (Vorgehensweise oder Ziele der Täter*innen, Konsequenzen für die Opfer u. a.) werden Cyberangriffe in mehr oder weniger trennscharfe Kategorien geordnet und untersucht (Meško 2018).

[6]Zum Dunkelfeld der Kriminalität gehören alle Straftaten, von denen die Polizei keine Kenntnis erlangt und die daher nicht in die offizielle Kriminalitätsstatistik eingehen. Dabei kann zwischen dem *relativen Dunkelfeld,* das sich mit Dunkelfeldforschung zumindest teilweise „erhellen“ lässt, und dem *absoluten Dunkelfeld* unterschieden werden. Zum *absoluten Dunkelfeld* gehören strafrechtlich relevante Handlungen, die von den Beteiligten z. B. nicht erinnert oder nicht erkannt werden (Prätor 2014).

Studie zum Thema Identitätsdiebstahl gibt das Beratungsunternehmen (Pascual und Marchini 2015) beispielsweise an, dass Privatpersonen deren Kreditkartendaten durch Vorfälle bei Banken oder Handelsunternehmen im Vorjahr entwendet wurden, ein fast dreimal höheres Risiko aufweisen Opfer von Identitätsdiebstahl zu werden. Die Intentionen der Täter*innen – z. B. zu welchem Zweck Daten unbefugt kopiert, manipuliert oder zerstört werden – ist für die Opfer in vielen Fällen ebenfalls nicht unmittelbar zu erkennen und selbst die Frage, ob es sich um einen gezielten Angriff handelt oder einen, von dem eine Vielzahl von Internetnutzern*innen betroffen sind, dürfte nur vage beantwortet werden können. Vor diesem Hintergrund scheint es im Rahmen von Viktimisierungsbefragungen in diesem Kontext sinnvoll zu sein, auf die Art der erlebten Schädigung abzustellen.

In dieser Studie stehen daher drei gängige Angriffsarten im Mittelpunkt, die einen erkennbaren Schaden nach sich ziehen. Dazu gehören der Datenverlust/-beschädigung infolge einer Malware-Infektion, die Datenverschlüsselung und Erpressung infolge einer Ransomware-Infektion und der Missbrauch persönlicher Daten, die unbefugt erlangt wurden.

Malware ist ein allgemeiner Sammelbegriff für schädigende bzw. „bösartige“ (engl. malicious) Computerprogramme, wie Viren, Würmer, Trojaner, Rootkits, Ransomware, Spyware, Scareware, etc. Da die Bandbreite und Kombinationsmöglichkeit von Schadprogrammen permanent zunimmt und eine sinnvolle Abgrenzung kaum möglich erscheint, wurde aus der allgemeinen Malware-Infektion lediglich die Ransomware-Infektion ausgeklammert und gesondert erhoben.

Ransomware bezeichnet Schadprogramme, die die Daten infizierter Computer oder ganzer Netzwerke verschlüsseln und somit für die Nutzer*innen unbrauchbar machen. In einem zweiten Schritt werden die Opfer erpresst, indem die Entschlüsselung der Daten erst nach der Zahlung eines Lösegelds (engl. ransom) meist in einer digitalen Währung (z. B. Bitcoin[7] oder Monero) in Aussicht gestellt wird.

Missbrauch persönlicher Daten liegt vor, wenn bestimmte unbefugt erlangte Daten zur Ausweisung einer Identität wie beispielsweise Passwörter, Kreditkarten- oder andere Zugangsdaten von den Tätern*innen unerlaubt weitergeben oder selbst beispielsweise zum Bestellen von Waren oder zur Geldabbuchung genutzt werden.

[7]Zu Bitcoin-Transaktionen im Zusammenhang mit Ransomware siehe Paquet-Clouston et al. (2018).

3 Forschungsstand

Mit der Annahme, dass Cyberkriminalität und Cyberkriminelle keine Landesgrenzen kennen (Kigerl 2012; Rieckmann und Kraus 2015), könnte davon ausgegangen werden, dass das Risiko einer Opferwerdung unabhängig vom Wohnsitz ist. Der Forschungsstand scheint diese These jedoch zu widerlegen: Gemäß Symantec (2010) sind Internetnutzer*innen in China, Brasilien, Indien und der USA allgemein gesehen am stärksten betroffen. Eine mögliche Erklärung für diesen Befund liefert Kigerl (2012), indem er auf den Anteil der Internetnutzer*innen sowie die Arbeitslosenquote als Prädiktor für die Spam-Rate bzw. die Phishing-top-level-domain-Rate[8] auf staatlicher Ebene aufmerksam macht.

Erhebliche Unterschiede nach Art der Angriffe zeigen sich sowohl innerhalb der Europäischen Union (European Commission 2015; Reep-van den Bergh und Junger 2018) als auch innerhalb Deutschlands (Rieckmann und Kraus 2015). Beispielsweise variiert die Häufigkeitszahl[9] für Identitätsdiebstahl innerhalb der Bundesländer zwischen 1265 und 4135 Fällen pro 100.000 Einwohnern (Rieckmann und Kraus 2015, S. 299).[10] Ähnliche Unterschiede finden sich auch bei anderen Deliktformen wie z. B. Malware-Infektion.[11]

Neben solchen regionalen Unterschieden zeigen internationale Studien, dass es auch individuelle Merkmale und Verhaltensweisen der Internetnutzer*innen gibt, die das Risiko einer Viktimisierung durch Cyberkriminalität beeinflussen. Bezüglich der berichteten Ergebnisse sind diese allerdings nicht immer konsistent (Reyns et al. 2016). So berichten z. B. Holt und Bossler (2013, S. 431),

[8]Mit Top-level domain (TLD) wird der letzte Abschnitt rechts vom Punkt einer Domain im Internet bezeichnet (z. B. https://www.[Domain-Name].de). Die Zahl der Server mit einer nationalen TLD (.de, .us, .ru usw.) von denen Phishing-Angriffe ausgingen wurde von Kigerl (2012) ins Verhältnis zur Populationsgröße der Staaten gesetzt und dient ihm neben der Spam-Rate als Proxy für den Standort von Cyberkriminellen.

[9]Die Häufigkeitszahl gibt den Anteil der Straftaten pro 100.000 Einwohner*innen an und ermöglicht somit, die Kriminalitätsbelastung von regionalen Gebieten mit unterschiedlicher Einwohneranzahl miteinander zu vergleichen.

[10]Rieckmann und Kraus (2015) führen als mögliche Erklärungen die unterschiedlichen infrastrukturellen Möglichkeiten der Internetnutzung (insbesondere im Vergleich der neuen und alten Bundesländer) sowie den demografischen Wandel und die Landflucht an, die sich auf die Häufigkeit der Internetnutzung und den Anteil der Internetnutzer auswirken.

[11]Bayerl und Rüdiger (2018) weisen darauf hin, dass die Polizeiliche Kriminalstatistik (PKS) in Hinblick auf Cybercrime-Delikte aufgrund des vermutlich sehr großen Dunkelfeldes kaum aussagekräftig ist.

dass Internetnutzerinnen häufiger von Cyberkriminalität betroffen sind als Internetnutzer, während van Wilsem (2011, S. 123) keinen Geschlechtereffekt feststellen konnte. Leukfeldt und Yar (2016) fanden relevante Zusammenhänge zwischen individuellen Merkmalen, Online-Verhalten bzw. verwendeter IT-Umgebung und Viktimisierung durch Hacking, Malware-Infektion, Identitätsdiebstahl, Computerbetrug und Cyberstalking. Sie zeigen außerdem, dass sich die Einflussfaktoren für die verschiedenen Deliktformen im Zusammenhang mit Cyberkriminalität unterscheiden. Jüngere Internetnutzer*innen haben z. B. ein höheres Risiko, gehackt zu werden, als ältere. Das Risiko eines Malware-Angriffs scheint vor allem mit dem Geschlecht, dem Bildungsniveau, der Beschäftigungssituation, dem persönlichen Einkommen und der Häufigkeit der Internetnutzung zusammenzuhängen (Leukfeldt und Yar 2016, S. 273).[12]

Andere Studien verweisen auf den Zusammenhang zwischen illegalem Online-Verhalten und der Viktimisierung durch Malware-Infektion (Bossler und Holt 2009; Choi 2008; Holt und Bossler 2013; Ngo und Paternoster 2011). Dass die im Internet verbrachte Zeit mit verschiedenen Arten von Cybercrime-Viktimisierung in Verbindung steht, z. B. mit einem gezielten Computerbetrug, zeigen Pratt et al. (2010). Widersprüchliche Ergebnisse werden bezüglich des Einflusses des Schutzverhaltens im Internet auf das Viktimisierungsrisiko berichtet: Bossler und Holt (2009) sehen keinen Zusammenhang, Choi (2008) berichtet einen risikomindernden und Ngo und Paternoster (2011) einen risikosteigernden Effekt.[13]

Die Relevanz solcher Effekte und der damit verbundenen Möglichkeiten, präventive Maßnahmen abzuleiten, wird in Hinblick auf die Folgen von Cyberkriminalität für die Opfer deutlich. Neben dem Verlust von Daten und zum Teil erheblichen finanziellen Schäden wird z. B. bei Dreißigacker und Riesner (2018)

[12]Auch Näsi et al. (2017), Hutchings und Hayes (2009), Marcum et al. (2010), Pratt et al. (2010) und van Wilsem (2011, 2013) untersuchten potenzielle Viktimisierungsfaktoren für Internetnutzer und ihr Verhalten mit Bezug auf den Routine-Activity-Ansatz (Cohen und Felson 1979).

[13]Dies könnte u. a. an Unterschieden bei Operationalisierung des Schutzverhaltens liegen. Während sich z. B. Choi (2008) auf vorhandene Schutzsoftware (Antiviren-, Antispyware- und Firewall-Programme) bezieht, unterscheiden Bossler und Holt (2009) innerhalb ihres Modells zwischen persönlichen Fähigkeiten, dem Einsatz von Schutzsoftware und dem riskanten Onlineverhalten im Freundeskreis. Ngo und Paternoster (2011) differenzieren zwischen Fähigkeiten der Nutzer*innen, Verwendung von Sicherheitssoftware und Information über Cyberkriminalität. Anders als bei Bossler und Holt (2009) fassen Ngo und Paternoster (2011) die Verwendung von Sicherheitssoftware in einer Maßzahl zusammen.

ersichtlich, dass ein nicht unerheblicher Teil der Betroffenen unter anhaltenden Belastungen zu leiden hat. So fühlen sich fast zwei Drittel der Opfer eines Missbrauchs persönlicher Daten (65,5 %) von der Tat anhaltend (sehr/eher) belastet (ebd., S. 39). Kirwan und Power (2012) weisen zudem darauf hin, dass die Folgen bis zu Symptomen ähnlich posttraumatischer Belastungsstörungen reichen können und damit nicht unterschätzt werden sollten.

Zusammenfassend lässt sich festhalten, dass verschiedene Forschungsergebnisse auf den Einfluss verschiedener individueller Faktoren und Online-Verhaltensweisen hindeuten, die das Viktimisierungsrisiko von Internetnutzer*innen beeinflussen können. Diese Ergebnisse sind allerdings zum Teil widersprüchlich und basieren häufig auf relativ kleinen Stichproben mit eingeschränkter Verallgemeinerbarkeit der Ergebnisse (z. B. wenn nur Studenten*innen befragt wurden). Hinzu kommt, dass die vorhandenen Studien selten Differenzierungen zwischen verschiedenen Angriffsformen zulassen, vor dem Hintergrund rasanter Entwicklungen teilweise veraltet sind und sich kaum auf den deutschsprachigen Raum beziehen.

4 Hypothesen

Mit Bezug zum Routine-Activity-Ansatz (Cohen und Felson 1979), mit dem die Ursachen von Straftaten nicht allein bei den Tätern*innen zu suchen sind, gehen wir davon aus, dass bestimmte individuelle Merkmale von Opfern und situativen Umständen auch im Bereich der Cyberkriminalität das Risiko einer Viktimisierung beeinflussen. Der Routine-Activity-Ansatz betont vor allem eine raumzeitliche Koinzidenz[14] von motivierten Tätern*innen, geeigneten Tatzielen und nicht ausreichendem Schutz als entscheidende Voraussetzung für die Begehung von Straftaten.

Wie verschiedene Kriminalitätsstatistiken zeigen, gibt es potenzielle Täter*innen, die zur Begehung von Cybercrime-Delikten motiviert sind (Kigerl 2012; Rieckmann und Kraus 2015). Als geeignete Ziele können prinzipiell alle Internetnutzer*innen angeführt werden, auch wenn anzunehmen ist, dass deren Risiko, Opfer von Cyberkriminalität zu werden, von weiteren individuellen Faktoren, Haushaltseigenschaften oder Online-Verhaltensweisen abhängt. In Hinblick auf

[14]Zur Frage der Übertragbarkeit der theoretischen Annahme einer räumlich und zeitlich geordneten Welt auf den virtuellen Raum siehe Yar (2005) und Leukfeldt und Yar (2016).

das Fehlen von ausreichendem Schutz gehen wir davon aus, dass präventive Verhaltensweisen oder IT-Sicherheitsmaßnahmen, wie z. B. die Verwendung von Antivirensoftware, eine solche Schutzfunktion haben.

4.1 Individuelle Faktoren

Da jüngere Menschen das Internet häufiger und intensiver nutzen als ältere (Dreißigacker und Riesner 2018), gehen wir davon aus, dass das Risiko, Opfer von Cyberkriminalität zu werden, bei jüngeren Menschen entsprechend größer ist, worauf verschiedene Studien bereits hinweisen (Leukfeldt und Yar 2016). Trotz widersprüchlicher Forschungsergebnisse in Bezug auf Geschlechtsunterschiede (Holt und Bossler 2013; van Wilsem 2011), gehen wir weiter davon aus, dass Männer stärker von Cyberkriminalität betroffen sind, da sie möglicherweise häufiger unsichere Webseiten (bspw. mit pornografischen Inhalten) nutzen als Frauen. In Hinblick auf unterschiedliche sprachliche Voraussetzungen beim Erkennen potenzieller Risikosituationen (z. B. in Hinblick auf E-Mails mit gefälschten offiziellen Absendern, über die Schadsoftware verbreitet werden soll)[15] und ein unterschiedlich ausgeprägtes Risikobewusstsein bei der Nutzung des Internets, vermuten wir, dass Internetnutzer*innen mit Migrationshintergrund sowie Internetnutzer*innen mit geringerer Bildung vulnerabler für Cyberkriminalität sind als solche ohne Migrationshintergrund bzw. mit höherem Bildungsabschluss. Außerdem gehen wir davon aus, dass eine bessere wirtschaftliche Situation der Internetnutzer*innen das Risiko einer Viktimisierung aufgrund besserer IT-Sicherheitsmaßnahmen (Soft- und Hardwareschutz) verringert.

4.2 Onlineverhalten

Menschen unterscheiden sich bei der Häufigkeit der Internetnutzung (Pratt et al. 2010) sowie der Anzahl und Art der dafür verwendeten Endgeräte. Unsere Hypothese ist, dass sowohl eine höhere Häufigkeit der Internetnutzung als auch die Verwendung mehrerer verschiedener Endgeräte das Risiko der Viktimisierung

[15] Broadhurst et al. (2019) zeigen in ihrer Studie u. a., dass die Gruppe der internationalen Studierenden im Vergleich zur Gruppe der inländischen Studierenden anfälliger für E-Mail-Betrug war und führen als eine mögliche Erklärung Sprachbarrieren bei der Betrugserkennung an.

durch Cyberkriminalität erhöhen, insofern damit mehr Gelegenheiten und eine größere Angriffsfläche für potenzielle Täter verbunden sind.

4.3 Präventionsverhalten

In Bezug auf das Präventionsverhalten unterscheiden sich Menschen in ihrer Bereitschaft, Schutzmaßnahmen wie die Installation von Antivirensoftware zu treffen (Pratt et al. 2010). Wir gehen davon aus, dass Menschen mit einem niedrigeren Schutzverhalten eher Opfer von Cyberkriminalität werden. Neben möglichen Schutzmaßnahmen, können Internetnutzer*innen auch riskante Handlungen vermeiden, bspw. das Öffnen eines Anhangs von einem anonymen Absender. Solche Vermeidungsstrategien dürften sich erwartungsgemäß negativ auf das Viktimisierungsrisiko von Cyberkriminalität auswirken.

4.4 Haushaltsfaktoren

Auch wenn sich das Onlinenutzungsverhalten im Zuge der zunehmenden Verbreitung von mobilen Endgeräten verändert, gehen wir davon aus, dass 1) stationäre Computer, die von mehreren Haushaltsmitgliedern zur Internetnutzung verwendet werden, immer noch recht verbreitet sind und 2) die mobilen Endgeräte der Haushaltsmitglieder innerhalb der Wohnung bzw. des Hauses in der Regel in einem haushaltsbezogenen Netzwerk eingebunden sind. Daher dürfte sich die Zusammensetzung des Haushalts auch auf das Risiko einer Viktimisierung durch Cyberkriminalität auswirken, insofern wir bei größeren Haushalten mehr Heimnetzwerkteilnehmer*innen, eine größere Internetaktivität und damit ein höheres Risiko für Cyberkriminalität vermuten. In Hinblick auf ihr vermutlich geringeres Bewusstsein für die Gefahren im Internet, dürften sich Minderjährige im Haushalt ebenfalls risikoerhöhend auswirken.

5 Methode

5.1 Datengrundlage

Die Basis der Analyse bilden die Daten der periodischen *Befragung zur Sicherheit und Kriminalität* der Landeskriminalämter Niedersachsen und Schleswig-Holstein, die auf Grundlage zweier repräsentativer Stichproben der

Wohnbevölkerung ab 16 Jahren in Niedersachsen und Schleswig-Holstein im Jahr 2015 erhoben wurden.[16] Dabei wurden insgesamt 65.000 Personen (40.000 Personen aus Niedersachsen und 25.000 Personen aus Schleswig-Holstein) zur Teilnahme an einer Paper-Pencil-Befragung gebeten. Die Rücklaufquote betrug 51,5 % ($n = 33.538$).[17] Der in beiden Bundesländern identisch eingesetzte Fragebogen enthielt neben einem Kernbestand an Fragen zu demografischen Merkmalen, zum Leben im entsprechenden Bundesland, zur Kriminalitätsfurcht, zur Erfahrung mit Kriminalität und zur Arbeit der Polizei ein Schwerpunktmodul zum Themenbereich *Computerbezogene Kriminalität (Cybercrime)* mit gesonderten Fragen zur privaten Internetnutzung, zur Furcht vor Internetkriminalität, zu Erfahrungen mit verschiedenen Deliktformen im Jahr 2014, dem Anzeigeverhalten und den Folgen einer Viktimisierung,[18] die im Mittelpunkt der folgenden Analyse stehen.[19]

5.2 Stichprobenbeschreibung

Aufgrund der Schwerpunktsetzung des vorliegenden Beitrags wurden nur Befragte eingeschlossen, die angegeben haben, das Internet privat in ihrer Freizeit zu nutzen. Infolgedessen reduzierte sich die Stichprobengröße auf 26.665, da 5624 Befragte (16,8 %) angaben, das Internet nicht privat zu nutzen. Das Durchschnittsalter der privaten Internetnutzer*innen betrug 45 Jahre und lag zwischen 16 und 97 Jahren. Ein Anteil von 48,7 % war weiblich und 51,3 % männlich. Die Stichprobe wurde nach Alter, Geschlecht und Landkreis bzw. kreisfreier Stadt gewichtet, sodass bezüglich dieser Merkmale keine Hinweise auf eine Verzerrung der Stichprobe privater Internetnutzer*innen aus der Wohnbevölkerung ab 16 Jahren in den Bundesländern Niedersachsen und Schleswig-Holstein im Jahr 2015 mehr vorliegen.

[16] Die Kernbefunde der Befragungen finden sich bei Landeskriminalamt Niedersachsen (2016) und Dreißigacker (2016).

[17] Die Rücklaufquote in Niedersachsen betrug 51,2 % und in Schleswig-Holstein 52,3 %.

[18] Deskriptive Befunde des Sondermoduls finden sich für Schleswig-Holstein bei Dreißigacker und Riesner (2018).

[19] Für die Bereitstellung der Daten und damit die Ermöglichung dieser Analyse bedanken wir uns bei den Landeskriminalämtern Niedersachsen und Schleswig-Holstein.

5.3 Variablenbeschreibung

Insgesamt wurden vier dichotome abhängige Variablen gebildet. Diese betrafen die Erfahrung mit Malware-Infektionen, Ransomware-Infektionen und den Missbrauch persönlicher Daten und stehen für das Erleben mindestens eines Angriffs der jeweiligen Angriffsarten im Jahr 2014 durch die privaten Internetnutzer*innen. Zum Vergleich wird die Erfahrung mit mindestens einer dieser drei Formen der Cyberkriminalität in einer vierten zusammenfassenden abhängigen Variable erfasst.

Eine „Malware-Infektion“ wurde mit der Frage erhoben, ob im Jahr 2014 mindestens ein Datenverlust oder eine Datenbeschädigung durch Viren, Trojaner oder Würmer erlitten wurde. Die „Ransomware-Infektion“ wurde mit der Frage erhoben, ob im Jahr 2014 mindestens eine Erpressung/Blockierung eines Gerätes zur Internetnutzung erlebt wurde. Und die Frage, ob die Befragten im Jahr 2014 mindestens einen „Missbrauch persönlicher Daten“ erlebt haben, wurde mit folgenden Schlagworten bzw. Beispielen spezifiziert: Identitätsdiebstahl, Kontodaten, Kreditkartendaten, Missbrauch eines Benutzer-, Spiele- oder Mailkontos.

Als unabhängige Variablen wurden die individuellen Merkmale der Befragten Alter in Jahren, Geschlecht, Migrationshintergrund und Bildungsniveau herangezogen. Befragte, die nicht in Deutschland geboren wurden oder mindestens einen nichtdeutschen Elternteil haben, wurden als Personen mit Migrationshintergrund gezählt. Das Bildungsniveau wurde in drei Kategorien eingeteilt: niedriges Bildungsniveau (kein Abitur, noch Schüler*in oder Hauptschulabschluss bzw. Volksschulabschluss), mittleres Bildungsniveau (Realschulabschluss oder Polytechnische Oberschule) und hohes Bildungsniveau (Abitur, Fachhochschulreife oder Erweiterte Oberschule). Die Variable „wirtschaftliche Situation“ bezieht sich auf die eigene Bewertung der Teilnehmer der aktuellen wirtschaftlichen Situation und reicht von 1 = „sehr schlecht“ bis 6 = „sehr gut“.

Weitere unabhängige Variablen betreffen Haushaltsmerkmale, Häufigkeit der Internetnutzung, Anzahl verschiedener Geräte zur Internetnutzung sowie damit verbundenes Schutz- und Vermeidungsverhalten. Die Variable „Anzahl der im Haushalt lebenden Personen“ gibt die Anzahl der Haushaltsmitglieder an. Die vorgegebenen Kategorien reichen hierbei von 1 = „1 Person“ bis 6 = „6 oder mehr Personen“. Die Variable „in einem Haushalt lebende Minderjährige“ gibt an, dass mindestens eine Person unter 18 Jahren im Haushalt lebte. Die Anzahl der verwendeten Geräte wurde mit der Frage erhoben: „Mit welchen Geräten nutzen Sie das Internet?“. Zur Auswahl standen die Kategorien: PC, Notebook/

Laptop, Tablet, Smartphone, Unterhaltungsgeräte (z. B. Spielekonsole, Fernsehgerät) und Sonstiges. Die Häufigkeit der Internetnutzung wurde anhand einer Fünf-Punkte-Skala von 1 = „weniger als einmal pro Woche“ bis 5 = „mehrmals täglich“ gemessen. Bei den Variablen „Schutzverhalten“ und „Vermeidungsverhalten“ handelt es sich um zwei Mittelwertskalen, die aus zehn bzw. vier Einzelitems gebildet wurden. Die Einzelitems beziehen sich auf die Häufigkeit bestimmter Schutzmaßnahmen[20] bzw. die Häufigkeit der Vermeidung bestimmter riskanter Verhaltensweisen,[21] die ebenfalls unter Verwendung von Fünf-Punkt-Skalen von 1 = „nie“ bis 5 = „immer“ erhoben wurden. Höhere Werte der Mittelwertskalen deuteten entsprechend auf ein stärkeres Schutz- bzw. Vermeidungsverhalten hin. Die Variable Bundesland wurde als Kontrollvariable einbezogen und unterscheidet Internetnutzer*innen nach Bundesland.

Deskriptive Ergebnisse von allen abhängigen und unabhängigen Variablen finden sich in Tab. 1.

5.4 Analysevorgehen

Im Rahmen der multivariaten Auswertung wurden mit der Statistiksoftware Stata 14 binärlogistische Regressionsanalysen durchgeführt. Zusätzlich zu den Standardkoeffizienten solcher Analysen (Logits und Odds Ratios) werden die durchschnittlichen Marginaleffekte (average marginal effects, kurz AME) berechnet, die im Gegensatz zu Logits und Odds Ratios bei Heteroskedastizität nicht verzerrt werden (Auspurg und Hinz 2011, S. 63). Ein weiterer Vorteil

[20]Dazu zählen: „Ich benutze ein Virenprogramm“, „benutze die aktuelle Software (Updates)“, „benutze komplexe Passwörter (Kombination von Buchstaben, Zahlen, Sonderzeichen)“, „benutze verschiedene Passwörter für verschiedene Anwendungen/Internetseiten“, „wechsele regelmäßig meine Passwörter“, „überprüfe, ob eine Internetseite sicher ist (z. B. durch Reputationssoftware)“, „lösche verdächtige E-Mails, ohne sie zu öffnen“, „sichere mein WLAN vor dem Zugriff Unbefugter mit einem Passwort“, „melde mich von Internetseiten ab, wenn ich fertig bin (Logout)“ und „benutze die Internetfunktion des neuen Personalausweises“.

[21]Dazu zählen: „Ich vermeide es, verdächtigen Links zu folgen“, „unbekannte Programme oder Daten herunterzuladen“, „meine persönlichen Daten ins Internet zu stellen“ sowie „öffentliches WLAN (Hotspot) zu benutzen“.

Tab. 1 Deskriptive Statistik (Daten gewichtet)

Variablen	Prozent bzw. Mittelwert (SD)	Spannweite
Abhängige Variablen:		
Malware-Infektion (1 = passiert)	11,5	0–1
Ransomware-Infektion (1 = passiert)	3,6	0–1
Missbrauch persönlicher Daten (1 = passiert)	5,3	0–1
Cyberangriffe insgesamt (1 = passiert)	16,6	0–1
Unabhängige Variablen:		
Alter	45,0 (16,6)	16–97
Geschlecht (1 = weiblich)	48,7	0–1
Migrationshintergrund (1 = ja)	12,1	0–1
Wirtschaftliche Situation	4,3 (0,96)	1–6
Bildungsniveau		
Niedrig (1 = ja)	22,2	0–1
Mittel (1 = ja)	35,4	0–1
Hoch (1 = ja)	42,4	0–1
Personen, die im Haushalt leben	2,7 (1,18)	1–6
Minderjährige leben im Haushalt (1 = ja)	34,2	0–1
Häufigkeit der privaten Internetnutzung	4,4 (1,02)	1–5
Anzahl der Geräte zur Internetnutzung	2,4 (1,19)	0–6
Schutzverhalten (Mittelwertskala)	3,7 (0,59)	1–5
Vermeidungsverhalten (Mittelwertskala)	4,2 (0,75)	1–5
Kontrollvariable:		
Bundesland (1 = Schleswig-Holstein)	39,5	0–1

liegt in deren besseren Interpretierbarkeit. Während sich Logits und Odds Ratios lediglich hinsichtlich der Effektrichtung interpretieren lassen, geben die AMEs in unserem Fall die mittlere prozentuale Änderung der Wahrscheinlichkeit einer Viktimisierung an, wenn sich die betreffende erklärende Variable (marginal) um eine Einheit ändert (Auspurg und Hinz 2011, S. 66).

6 Ergebnisse

Die deskriptiven Ergebnisse zeigen, dass ein beträchtlicher Teil der Befragten (16,6 %) im Jahr 2014 mindestens eine Form der hier im Mittelpunkt stehenden Cyberangriffsarten erlebt hat.[22] Die Prävalenzrate von Malware-Infektionen ist dabei am höchsten (11,5 %). Das Erleben mindestens einer Ransomware-Infektionen bzw. eines Missbrauchs persönlicher Daten wurden seltener berichtet (3,6 % bzw. 5,3 %). Die multivariaten Analyseergebnisse in Tab. 2 zeigen, dass es für die drei unterschiedenen Arten von Cyberkriminalität tatsächlich unterschiedliche Risikofaktoren gibt.

Der erwartete Alterseffekt, d. h., dass mit zunehmendem Alter das Viktimisierungsrisiko sinkt, ließ sich lediglich beim Missbrauch persönlicher Daten feststellen, während es sich bei der Ransomware-Infektion genau anders herum verhält: Mit zunehmendem Alter wird das Risiko eines erfolgreichen Ransomware-Angriffs größer. Dazu muss erwähnt werden, dass beide Effekte zwar statistisch signifikant aber auch sehr klein sind. Keinen statistisch relevanten Einfluss hatte das Alter auf das Risiko, Opfer mindestens eines der drei zusammengefassten Deliktformen bzw. mindestens einer Malware-Infektionen zu werden.

Hinsichtlich des Geschlechtes kann die Hypothese, Männer haben ein höheres Viktimisierungsrisiko als Frauen mit einer Ausnahme bestätigt werden. Lediglich beim Missbrauch persönlicher Daten spielte das Geschlecht keine signifikante Rolle. Tendenziell sind aber auch hier Männer stärker betroffen als Frauen. Der Geschlechtereffekt könnte mit unterschiedlichen Risikobewertungen zu erklären sein, die nicht in den Modellen enthalten sind. Insofern Frauen z. B. häufiger zu der Einschätzung kommen, dass ein Link verdächtig oder eine Internetseite unsicher ist als Männer,[23] wäre ihr Online-Verhalten unter Kontrolle der Vermeidungshäufigkeit solcher Links oder Internetseiten weniger riskant. Zukünftige Forschung dazu, inwiefern sich das Online-Verhalten zwischen den Geschlechtern qualitativ und quantitativ unterscheidet, wäre in diesem Kontext sicherlich aufschlussreich.

[22]Werden alle innerhalb des Sondermoduls erfragten Deliktformen miteinbezogen, also auch Betrug beim Warenhandel, Abofallen, Stalking, persönliche sexuelle Belästigung und Mobbing im Internet, dann liegt die Gesamtprävalenzrate unter den privaten Internetnutzer*innen bei 23,6 % (Dreißigacker und Riesner 2018, S. 35).

[23]Dafür spräche, dass Frauen eine signifikant höhere affektive und kognitive Furcht vor Cyberkriminalität haben (Dreißigacker und Riesner 2018, S. 27–29).

Tab. 2 Binärlogistische Regression (Daten gewichtet)

	Cyberangriffe insgesamt			Malware-Infektion			Ransomware-Infektion			Missbrauch persönlicher Daten		
	Logits	SE	AME	Logits	SE	AME	Logits	SE	AME	Logits	SE	AME
Alter *(Zehn-Jahres-schritte)*[a]	−,009	,013	,001	,021	,015	,002	,063*	,025	,002*	−,067**	,021	,003**
Geschlecht *(weibl. vs. männl.)*	−,238***	,036	−,032***	−,209***	,042	−,021***	−1,042***	,082	−,032***	−,027	,059	−,001
Migrations-hintergrund *(ja vs. nein)*	,031	,053	,004	−,001	,062	,000	,230*	,101	,008*	,080	,085	,004
Wirtschaftliche Situation	−,207***	,018	−,028***	−,246***	,021	−,025***	−,212***	,036	−,007***	−,120***	,030	−,006***
Bildungsniveau *(mittel vs. gering)*	,113*	,051	,015*	,043	,058	,004	,161	,100	,005	,275 **	,094	,014**
Bildungsniveau *(hoch vs. gering)*	,229***	,050	,031***	,026	,057	,003	,149	,098	,005	,577***	,090	,029***
Haushaltsgröße *(in Personen)*	−,017	,020	−,002	,024	,023	,002	−,050	,041	−,002	−,066*	,033	−,003*
Haushalt mit Minderjährigen *(ja vs. nein)*	,144**	,048	,020**	,120*	,056	,012*	,039	,101	,001	,127	,079	,006

(Fortsetzung)

Tab. 2 (Fortsetzung)

	Cyberangriffe insgesamt			Malware-Infektion			Ransomware-Infektion			Missbrauch persönlicher Daten		
	Logits	SE	AME	Logits	SE	AME	Logits	SE	AME	Logits	SE	AME
Häufigkeit der Internetnutzung	,232***	,025	,031***	,228***	,029	,023***	,163***	,047	,005***	,305***	,048	,015***
Anzahl unterschied, Geräte zur Internetnutzung	,093***	,017	,013***	,105***	,020	,010***	,018	,034	,001	,128***	,027	,006***
Schutzverhalten	−,048	,033	−,006	−,090*	,039	−,009*	−,173**	,064	−,006**	,212***	,059	,011***
Vermeidungsverhalten	−,132***	,025	−,018***	−,126***	,029	−,013***	−,118*	,047	−,004*	−,162***	,043	−,008***
Bundesland *(SH vs. NI)*	,058	,036	,008	,057	,042	,006	,048	,072	,002	,096	,058	,005
Konstante	−1,310	,199		−1,586	,230		−2,005	,378		−4,194	,364	
N	23.539			23.437			23.347			23.357		
Log-likelihood	−10.640,741			−8.395,820			−3.531,024			−4.888,625		
Nagelkerkes pseudo R^2	,040			,034			,044			,040		

[a]Aus Gründen der Darstellung wurde die Variable „Alter“ so transformiert, dass die Änderung um eine Einheit einem Sprung um zehn Jahre entspricht. Die ausgewiesenen Koeffizienten beziehen sich dementsprechend auf einen Anstieg des Alters um zehn Jahre
* $p \leq ,05$; ** $p \leq ,01$; *** $p \leq ,001$

Ob die befragten Internetnutzer*innen einen Migrationshintergrund hatten oder nicht, wirkte sich lediglich auf das Risiko einer Ransomware-Infektion in erwarteter Richtung, d. h. einem höheren Risiko für Menschen mit Migrationshintergrund, aus. Die Hypothese baut dabei auf der Vermutung auf, dass Täuschungen und Betrugsversuche umso eher erkannt werden, je höher die sprachliche Kompetenz ist. Da der Migrationshintergrund jedoch auf die anderen untersuchten Deliktformen keinen statistisch relevanten Einfluss ausübte, bleibt weiterhin näher zu untersuchen, warum sich dies ausschließlich bezüglich Ransomware-Angriffen zeigt.

Die Hypothese, dass mit höherem Bildungsniveau das Viktimisierungsrisiko sinkt, ließ sich nicht bestätigen. Kein Bildungseffekt fand sich bezüglich der Malware-Infektion und der Ransomware-Infektion. Ein signifikant gegenteiliger Effekt ist hinsichtlich des Missbrauchs persönlicher Daten zu erkennen. Personen mit einer mittleren oder hohen Bildung haben ein höheres Risiko, dass personenbezogene Daten missbraucht werden, als Personen mit geringer Bildung. Dieser Effekt findet sich etwas abgeschwächt auch bezogen auf die zusammengefasste Variable „Cyberangriffe“ insgesamt.

Eine bessere wirtschaftliche Situation wirkte sich bei allen unterschiedenen Deliktformen statistisch signifikant und erwartungsgemäß risikoreduzierend aus, während sich bezüglich der einbezogenen Haushaltsfaktoren wiederum ein unklares Bild zeigt. Die Anzahl der in einem Haushalt lebenden Personen hatte sowohl von Cyberdelikten insgesamt als auch auf das Risiko von Malware- und Ransomware-Infektionen keinen signifikanten Einfluss. Allerdings ist ein nicht erwarteter negativer Effekt im Hinblick auf den Missbrauch personenbezogener Daten zu erkennen. Je größer der Haushalt desto geringer das Viktimisierungsrisiko eines Datenmissbrauchs. Ein erwarteter risikosteigernder Effekt von Minderjährigen im Haushalt ließ sich in Hinblick auf Cyberangriffe insgesamt und Malware-Infektionen feststellen. Bei den anderen beiden Deliktformen traf dies zwar tendenziell, aber nicht statistisch signifikant zu.

Wie erwartet, hatte das Online-Verhalten einen positiven Einfluss auf das Viktimisierungsrisiko: Eine häufigere Nutzung des Internets geht mit einem signifikant höheren Risiko einher, Opfer einer der untersuchten Deliktformen zu werden. Gleiches gilt für die Anzahl der unterschiedlichen Geräte, die für die Internetnutzung verwendet werden. Mit steigender Anzahl nimmt auch das Viktimisierungsrisiko mit einer Ausnahme bei allen Deliktformen signifikant zu. In Hinblick auf die Ransomware-Infektion ist dieser Effekt aber zumindest tendenziell festzustellen.

Das Präventionsverhalten der privaten Internetnutzer*innen wirkte sich ebenfalls mit einer Ausnahme erwartungskonform aus. Internetnutzer*innen, die ein

höheres Vermeidungsverhalten zeigten, hatten bei allen Deliktformen ein geringeres Viktimisierungsrisiko. Ein gesteigertes Schutzverhalten wirkte sich hinsichtlich der Malware-Infektion sowie der Ransomware-Infektion risikoreduzierend aus. Bezogen auf den Missbrauch persönlicher Daten hatte das Schutzverhalten allerdings einen signifikant gegenläufigen Effekt. Internetnutzer*innen, die sich häufiger mit verschiedenen Maßnahmen zu schützen versuchten, tragen demnach ein höheres Risiko, Opfer eines Datenmissbrauchs zu werden. Warum sich dies so zeigt, kann allerdings nur vermutet werden. Zunächst haben Schutzmaßnahmen, die die persönlichen Endgeräte betreffen (Virenschutz, Sicherheitsupdates, Passwortschutz etc.) allenfalls einen kleinen Einfluss auf die Sicherheit der persönlichen Daten bei einem Internetdienstleister (Online-Bank, E-Mail-Dienst, Online-Versandhandel, etc.) und sind demnach kaum geeignet, vor Missbrauch solcher hinterlegter Daten zu schützen. Dies erklärt allerdings nicht den positiven Effekt auf eine derartige Viktimisierung. Möglicherweise sind Internetnutzer*innen mit höherem Schutzverhalten unabhängig von der Häufigkeit der Internetnutzung, die in den Modellen kontrolliert wird, auch aktiver in Hinblick auf die Nutzung verschiedener Internet-Dienste, die eine Registrierung und damit die Angabe von persönlichen Daten voraussetzen. Dazu bedarf es ebenfalls weiterer Forschung.

Mit Blick auf die durchschnittlichen Marginaleffekte (AME) lässt sich feststellen, dass die einzelnen Faktoren auch in der Stärke ihres Einflusses variieren. Wie in Abb. 1 dargestellt, haben das Geschlecht, die wirtschaftliche Situation

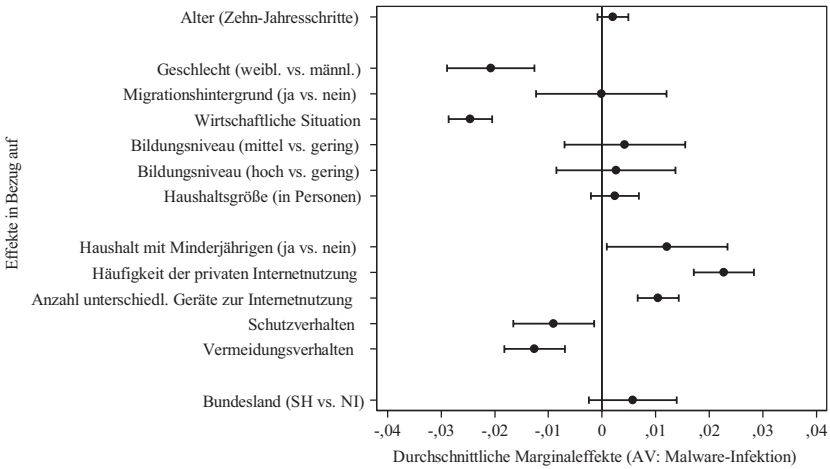


Abb. 1 Einflussfaktoren auf das Risiko einer Malware-Infektion

und die Häufigkeit der Internetnutzung den größten Einfluss auf das Risiko einer Malware-Infektion. Zum Beispiel ist die Wahrscheinlichkeit für diese Straftat im Durchschnitt bei Frauen um zwei Prozentpunkte (AME = −0,021) niedriger als bei Männern.

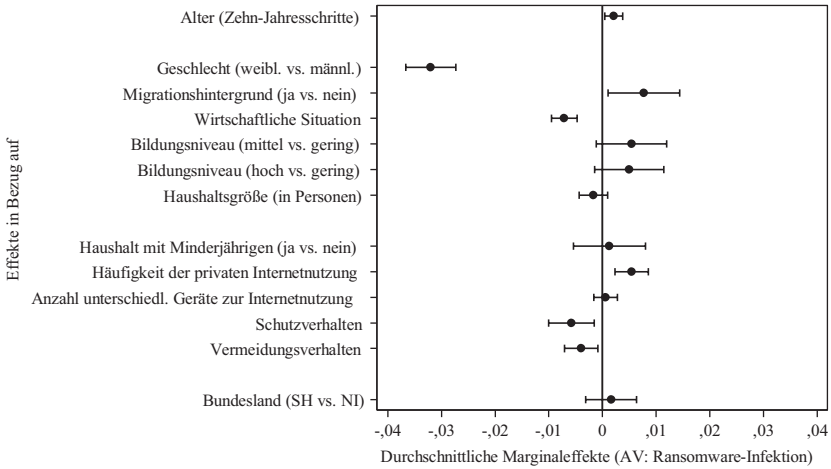


Abb. 2 Einflussfaktoren auf das Risiko einer Ransom-Infektion

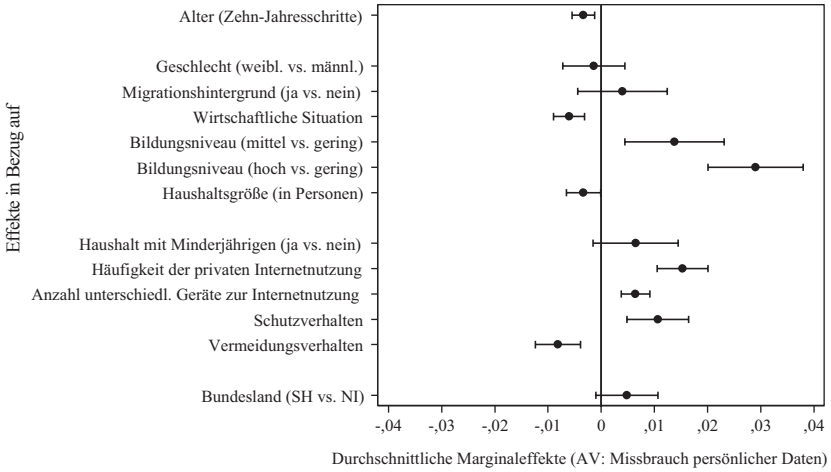


Abb. 3 Einflussfaktoren auf das Risiko des Missbrauchs persönlicher Daten

In Bezug auf das Risiko einer Ransomware-Infektion ist ebenfalls das Geschlecht von großer Bedeutung (Abb. 2) und ist im Vergleich zu den anderen Einflussfaktoren der stärkste Prädiktor (AME = −0,032). Im Gegensatz dazu hat das Geschlecht keinen wesentlichen Einfluss auf den Missbrauch personenbezogener Daten (Abb. 3). In Bezug auf diese abhängige Variable haben das Bildungsniveau und die Häufigkeit der Internetnutzung die größten Auswirkungen. Befragte mit mittlerem Bildungsniveau haben einen Prozentpunkt (AME = 0,014), und Personen mit höherem Bildungsniveau haben sogar ein um drei Prozentpunkte höheres Risiko (AME = 0,029) als Benutzer mit niedrigem Bildungsniveau.

7 Diskussion

Heutzutage ist es sehr einfach und üblich, alltägliche Aktivitäten wie Einkaufen, E-Mail-Versand und Bankgeschäfte online durchzuführen. Neben seinen vielen Vorteilen birgt das Internet jedoch auch die Gefahr der Viktimisierung durch Cyberkriminalität. Gemäß der Idee des Routine-Activity-Ansatzes (Cohen und Felson 1979) gibt es bestimmte Voraussetzungen für strafbare Handlungen, die auch auf den Bereich der Cyberkriminalität übertragen werden können.[24] Neben motivierten Tätern*innen bedarf es geeigneter Tatobjekte mit nicht ausreichendem oder fehlendem Schutz. Im vorliegenden Beitrag haben wir nach Faktoren gesucht, die sich auf das Risiko von privaten Internetnutzer*innen als potenziellen Opfern von Cyberkriminalität auswirken. Dabei haben wir die Viktimisierung durch Malware-Infektion, Ransomware-Infektion sowie Missbrauch personenbezogener Daten unterschieden. Anhand der Daten der Befragungen zu Sicherheit und Kriminalität der Landeskriminalämter Niedersachen und Schleswig-Holstein im Jahr 2015 lässt sich erkennen, dass jede/r sechste Befragte im Jahr 2014 von mindestens einer der genannten Deliktformen betroffen war. Darüber hinaus weisen die Ergebnisse auf Unterschiede in den Prävalenzraten verschiedener Formen von Cyberkriminalität hin.

Die multivariaten Ergebnisse zeigen, dass sowohl individuelle und haushaltsbedingte Faktoren als auch das Online- und Präventionsverhalten von Internet-

[24]Kritisch zur Annahme einer räumlich und zeitlich geordneten Welt im virtuellen Raum Yar (2005) und Leukfeldt und Yar (2016).

nutzern*innen deren Viktimisierungsrisiko bezüglich der drei unterschiedenen Deliktformen beeinflussen. Damit ist das Risiko einer Viktimisierung nicht für alle Internetnutzer*innen gleich groß. Tatsächlich stimmen die Ergebnisse mit dem Routine-Activity-Ansatz überein: Das Vorkommen von Cyberkriminalität hängt neben potenziellen Tätern*innen auch vom routinemäßigen (Online-)Verhalten der Nutzer*innen und vom Fehlen ausreichender Schutzmaßnahmen ab. Daraus lässt sich schließen, dass Internetnutzer*innen Möglichkeiten haben, sich vor solchen Deliktformen zu schützen.[25]

Die Auswertung brachte auch einige unerwartete Ergebnisse mit sich. Den erwarteten Alterseffekt konnten wir z. B. lediglich bezogen auf den Missbrauch persönlicher Daten feststellen. Die Annahme eines höheren Viktimisierungsrisikos für jüngere Menschen basierend auf der Annahme, dass jüngere Menschen das Internet häufiger und intensiver nutzen, ließ sich also nicht für alle Deliktformen gleichermaßen bestätigen. Bezogen auf Ransomware-Infektionen zeigt sich sogar ein gegenteiliger Effekt.

Darüber hinaus wiesen Personen mit Migrationshintergrund lediglich ein höheres Risiko auf, Opfer einer Ransomware-Infektion zu werden. Ein möglicher Grund dafür könnte sein, dass das sprachliche Verständnis vor allem bei Ransomware-Infektionen eine Rolle spielt und bei anderen Deliktformen weniger, was vermutlich an der Art der Verbreitung solcher Schadprogramme liegt. Diese gelangt häufig über die Täuschung der Internetnutzer*innen auf deren System und wird manuell ausgeführt (z. B. durch das Öffnen einer Word-Datei im Anhang einer E-Mail und die Aktivierung von Makros). Insofern wären Gruppen mit sprachlichen Schwierigkeiten im Sinne des Routine-Activity-Ansatzes besonders gegenüber Ransomware-Angriffen vulnerabler und ein in dieser Hinsicht geeignetes Ziel.

Das Bildungsniveau wirkte sich ebenfalls nicht wie erwartet aus. So zeigte sich, dass das Viktimisierungsrisiko beim Missbrauch persönlicher Daten bei Internetnutzern*innen mit mittlerem und höherem Bildungsniveau höher

[25]Meško (2018) weist im Zusammenhang mit fehlenden oder nicht ausreichenden Schutzmaßnahmen auf das Konzept der psychologischen Reaktanz hin, insofern Internetnutzer*innen Schutzmaßnahmen als Einschränkung der persönlichen Freiheit im Internet wahrnehmen könnten und dadurch von der Ergreifung geeigneter Schutzmaßnahmen abgehalten würden. Der psychologische Widerstand gegen Veränderungen spiele auch eine Rolle im Hinblick auf die schnelle technologische Entwicklung und die damit verbundene Notwendigkeit, Schutzmaßnahmen ständig anpassen zu müssen, um deren Effektivität aufrecht zu erhalten.

ist, als bei denjenigen mit niedrigem Bildungsniveau. Dies könnte damit zusammenhängen, dass höher Gebildete neben privaten sozialen Foren insbesondere auch diverse berufliche Onlinenetzwerke häufiger nutzen. Damit sind sie möglicherweise „sichtbarer“ und bieten durch die Preisgabe weiterer persönlicher Daten eine größere Angriffsfläche.

Ein weiterer kontraintuitiver Effekt zeigte sich hinsichtlich der Haushaltsgröße, wonach mit zunehmender Anzahl an Haushaltsmitgliedern das Viktimisierungsrisiko eines Missbrauchs persönlicher Daten sinkt. Eine denkbare Erklärung wäre die häufigere Einrichtung von individuellen Nutzerprofilen auf gemeinsam genutzten Endgeräten oder innerhalb des Netzwerkes in Mehrpersonenhaushalten, die für einen höheren Schutz der Daten untereinander aber auch gegenüber externen Angreifern*innen sorgt.

Allgemein zeigen die Analysen, dass die Einflüsse der einzelnen Prädiktoren zwischen den drei Deliktformen variieren. Cyberkriminalität unterscheidet sich also nicht nur in der Art des Angriffs, sondern auch hinsichtlich der Vulnerabilität verschiedener Gruppen privater Internetnutzer*innen mit entsprechend unterschiedlichen Möglichkeiten, sich vor solchen Angriffen zu schützen. Dieses Ergebnis sollte bei der weiteren Forschung berücksichtigt werden.

Abschließend ist auf einige Einschränkungen hinzuweisen, die mit den vorliegenden Daten verbunden sind. So wurde nicht gemessen, ob die Befragten vor oder nach der erlebten Viktimisierung einer der genannten Deliktformen ein bestimmtes Präventiv- oder Vermeidungsverhalten zeigten. Es kann also z. B. sein, dass ein von den Befragten angegebener Virenschutz erst nach der erlebten Malware-Infektion eingesetzt wurde und damit der gemessene risikoreduzierende Effekt des Präventionsverhaltens möglicherweise unterschätzt wird. Darüber hinaus wird das Online-Verhalten (Häufigkeit der Internetnutzung und Anzahl der verwendeten unterschiedlichen Geräte) nur sehr oberflächlich und allgemein erhoben. Zudem dienen die in dieser Studie enthaltenen Haushaltsmerkmale lediglich als Indikatoren für das Online-Verhalten der Haushaltsmitglieder. Dahinter steht die Annahme, dass es gemeinsam genutzte Geräte oder ein gemeinschaftliches Heimnetzwerk gibt und die Häufigkeit der Internetnutzung auf diesem Gerät bzw. in diesem Netzwerk mit der Anzahl der in einem Haushalt lebenden Personen ansteigt. Diese Annahme ist mit der zunehmenden Verbreitung von mobilen Endgeräten und den zunehmenden Möglichkeiten ins Internet zu gelangen in Zukunft wahrscheinlich immer weniger haltbar. Um tiefere Einsichten zu gewinnen, sollte die zukünftige Forschung derartige Unschärfen berücksichtigen und das Online- und Präventionsverhalten von privaten Internetnutzern*innen detaillierter erheben.

Literatur

Auspurg, K., & Hinz, T. (2011). Gruppenvergleiche bei Regressionen mit binären abhängigen Variablen. Probleme und Fehleinschätzungen am Beispiel von Bildungschancen im Kohortenverlauf. *Zeitschrift für Soziologie, 40*(1), 62–73.

Bayerl, P. S., & Rüdiger, T.-G. (2018). Braucht eine digitale Gesellschaft eine digitale Polizei? *Deutsche Polizei, 7,* 4–14.

Bergmann, M. C., Dreißigacker, A., von Skarczinski, B., & Wollinger, G. R. (2018). Cyber-Dependent Crime Victimization: The Same Risk for Everyone? *Cyberpsychology, Behavior and Social Networking, 21*(2), 84–90. https://doi.org/10.1089/cyber.2016.0727.

BITKOM – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Hrsg.). (2014). *Jung und vernetzt. Kinder und Jugendliche in der digitalen Gesellschaft*. Berlin. https://www.bitkom.org/sites/default/files/file/import/BITKOM-Studie-Jung-und-vernetzt-2014.pdf. Zugegriffen: 16. Jan. 2020.

Bollhöfer, E. & Jäger, A. (2018). *Wirtschaftsspionage und Konkurrenzausspähung. Vorfälle und Prävention bei KMU im Zeitalter der Digitalisierung (Max-Planck-Institut für ausländisches und internationales Strafrecht, Hrsg.) (Reihe A: Arbeitsberichte 09/2018).* Freiburg i. Br. https://pure.mpg.de/pubman/item/item_3002884_8/component/file_3016263/A_8_Wirtschaftsspionage.pdf. Zugegriffen: 16. Jan. 2020.

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology, 3*(1), 400–420.

Broadhurst, R., Skinner, K., Sifniotis, N., Matamoros-Macias, B., & Ipsen, Y. (2019). Phishing and cybercrime risks in a university student community. *International Journal of Cybersecurity Intelligence & Cybercrime, 2*(1), 4–23. https://doi.org/10.2139/ssrn.3176319.

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.). (2017). Die Lage der IT-Sicherheit in Deutschland 2017. Bonn. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf. Zugegriffen: 26. März 2019.

Chen, L., Ho, S. S., & Lwin, M. O. (2016). A meta-analysis of factors predicting cyberbullying perpetration and victimization. From the social cognitive and media effects approach. *New Media & Society,* 1–20. https://doi.org/10.1177/1461444816634037.

Choi, K. S. (2008). Computer crime victimization and integrated theory. An empirical assessment. *International Journal of Cyber Criminology, 2*(1), 308–333.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends. A routine activity approach. *American Sociological Review, 44*(4), 588–608.

Council of Europe (Hrsg.). (2001). Übereinkommen über Computerkriminalität. Budapest, 23.XI.2001. Bereinigte Übersetzung zwischen Deutschland, Österreich und der Schweiz abgestimmte Fassung. Sammlung Europäischer Verträge: 185. https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008157a. Zugegriffen: 23. Nov. 2017.

Deutsche Telekom AG. (2016). Umfrage: Fast jeder Zweite ist Opfer von Cybercrime. Pressemitteilung. http://www.emediarelease.de/PM%20Umfrage%20Computerhilfe_final.pdf. Zugegriffen: 26. März 2019.

Dreißigacker, A. (2016). Befragung zu Sicherheit und Kriminalität. Kernbefunde der Dunkelfeldstudie 2015 des Landeskriminalamtes Schleswig-Holstein (Kriminologisches Forschungsinstitut Niedersachsen e. V., Hrsg.) (KFN-Forschungsbericht Nr. 129). Hannover. www.kfn.de/wp-content/uploads/Forschungsberichte/FB_129.pdf. Zugegriffen: 17. Apr. 2019.

Dreißigacker, A., & Riesner, L. (2018). Private Internetnutzung und Erfahrung mit computerbezogener Kriminalität. Ergebnisse der Dunkelfeldstudien des Landeskriminalamtes Schleswig-Holstein 2015 und 2017 (Kriminologisches Forschungsinstitut Niedersachsen e. V., Hrsg.) (KFN-Forschungsbericht Nr. 139). Hannover. www.kfn.de/wp-content/uploads/Forschungsberichte/FB_139.pdf. Zugegriffen: 17. Apr. 2019.

Eisele, J. (2016). Cyberkriminalität. In J. Heesen (Hrsg.), *Handbuch Medien- und Informationsethik* (S. 255–261). Stuttgart: J.B. Metzler Verlag.

European Commission (Hrsg.). (2015). Cyber Security. Special Eurobarometer 423. Brüssel. http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_423_en.pdf, https://doi.org/10.2837/411118. Zugegriffen: 10. Dez. 2018.

Fansher, A. K., & Randa, R. (2018). Risky social media behaviors and the potential for victimization. a descriptive look at college students victimized by someone met online. *Violence and Gender*. https://doi.org/10.1089/vio.2017.0073.

Holt, T. J., & Bossler, A. M. (2013). Examining the relationship between routine activities and malware infection indicators. *Journal of Contemporary Criminal Justice, 29*(4), 420–436. https://doi.org/10.1177/1043986213507401.

Huber, E. (2015). Cybercrime gegen Privatpersonen. In N. Guzy, C. Birkel & R. Mischkowitz (Hrsg.), *Viktimisierungsbefragungen in Deutschland. Ziele, Nutzen und Forschungsstand* (Polizei + Forschung, Bd. 47.1, S. 393–420). Wiesbaden: Bundeskriminalamt.

Hutchings, A., & Hayes, H. (2009). Routine activity theory and phishing victimisation: Who gets caught in the ‚net'? *Criminal Justice, 20*(3), 433–451.

Initiative D21 e. V. (Hrsg.). (2016). *D21-Digital-Index 2016. Jährliches Lagebild zur Digitalen Gesellschaft.* Berlin.

Initiative D21 e. V. (Hrsg.). (2018). *D21 Digital Index 2017/2018. Jährliches Lagebild zur Digitalen Gesellschaft*. Berlin.

Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries. *Social Science Computer Review, 30*(4), 470–486. https://doi.org/10.1177/0894439311422689.

Kirwan, G., & Power, A. (2012). *The psychology of cyber crime. Concepts and principles*. Pannsylvania: IGI Global Press. https://doi.org/10.4018/978-1-61350-350-8.

Landeskriminalamt Niedersachsen (Hrsg.). (2016). Befragung zu Sicherheit und Kriminalität in Niedersachsen 2015. Bericht zu Kernbefunden der Studie. Hannover. www.lka.polizei-nds.de/download/72400/Bericht_zu_den_Kernbefunden.pdf. Zugegriffen: 23. Aug. 2016.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime. A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409.

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential factors of online victimization of youth. An examination of adolescent online behaviors

utilizing routine activity theory. *Deviant Behavior*, *31*(5), 381–410. https://doi.org/10.1080/01639620903004903.

Meier, B.-D. (2012). Sicherheit im Internet. Neue Herausforderungen für Kriminologie und Kriminalpolitik. *MschrKrim*, *95*(3), 184 (Verfügbar unter 204).

Meško, G. (2018). On some aspects of cybercrime and cybervictimization. *European Journal of Crime, Criminal Law and Criminal Justice, 26*(3), 189–199. https://doi.org/10.1163/15718174-02603006.

Münch, H. (2017). Tatort Internet – Neue Herausforderungen, neue Aufgaben. In P. E. Sensburg (Hrsg.), *Sicherheit in einer digitalen Welt* (S. 9–22). Baden-Baden: Nomos. https://doi.org/10.5771/9783845279725-9.

Näsi, M., Räsänen, P., Kaakinen, M., Keipi, T., & Oksanen, A. (2017). Do routine activities help predict young adults' online harassment: A multi-nation study. *Criminology & Criminal Justice, 17*(4), 418–432. https://doi.org/10.1177/1748895816679866.

Ngo, F., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology, 5*(1), 773–793.

Nurse, J. R. C., & Bada, M. (2019). The group element of cybercrime: Types. *Dynamics, and Criminal Operations.* https://doi.org/10.1093/oxfordhb/9780198812746.013.36.

Papsdorf, C. (2013). *Internet und Gesellschaft. Wie das Netz unsere Kommunikation verändert*. Frankfurt a. M: Campus.

Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2018). Ransomware payments in the bitcoin ecosystem. https://arxiv.org/pdf/1804.04080. Zugegeriffen: 12. März 2019.

Pascual, A., & Marchini, K. (Javelin LLC, Hrsg.). (2015). 2016 data breach fraud impact report. https://www.javelinstrategy.com/press-release/16-billion-stolen-127-million-identity-fraud-victims-2014-according-javelin-strategy. Zugegeriffen: 09. Sept. 2016.

Prätor, S. (2014). Ziele und Methoden der Dunkelfeldforschung. Ein Überblick mit Schwerpunkt auf Dunkelfeldbefragungen im Bereich der Jugenddelinquenz. In S. Eifler & D. Pollich (Hrsg.), *Empirische Forschung über Kriminalität. Methodologische und methodische Grundlagen* (Kriminalität und Gesellschaft, S. 31–65). Wiesbaden: VS Verl. für Sozialwiss.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting. Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267–296. https://doi.org/10.1177/0022427810365903.

Rantala, R. R. (2008). *Cybercrime against Businesses, 2005* (Bureau of Justice Statistics, Hrsg.) (Special Report NCJ 221943). Washington, DC.

Reep-van den Bergh, C. M. M., & Junger, M. (2018). Victims of cybercrime in Europe: A review of victim surveys. *Crime Science, 7*(1), 22. https://doi.org/10.1186/s40163-018-0079-3.

Reyns, B. W., Randa, R., & Henson, B. (2016). Preventing crime online. Identifying determinants of online preventive behaviors using structural equation modeling and canonical correlation analysis. *Crime Prevention and Community Safety*, *18*(1), 38–59. https://doi.org/10.1057/cpcs.2015.21.

Rieckmann, J., & Kraus, M. (2015). Tatort Internet: Kriminalität verursacht Bürgern Schäden in Milliardenhöhe. *DIW Wochenbericht*, (12), 295–301. https://www.diw.de/documents/publikationen/73/diw_01.c.498298.de/15-12-6.pdf. Zugegriffen: 24. Nov. 2017.

Robertz, F. J., Oksanen, A., & Räsänen, P. (2016). *Viktimisierung junger Menschen im Internet. Leitfaden für Pädagogen und Psychologen*. Wiesbaden: Springer. https://doi.org/10.1007/978-3-658-12325-3.

Rüdiger, T.-G. (2018). Das Broken Web: Herausforderung für die Polizeipräsenz im digitalen Raum. In T.-G. Rüdiger & P. S. Bayerl (Hrsg.), *Digitale Polizeiarbeit* (S. 259–299). Wiesbaden: Springer Fachmedien. https://doi.org/10.1007/978-3-658-19756-8_14.

Seidl, A., & Starnecker, T. (2017). Cybercrime: Angriff auf die Privatsphäre im virtuellen Raum. In E. Beyvers, P. Helm, M. Hennig, C. Keckeis, I. Kreknin, & F. Püschel (Hrsg.), *Räume und Kulturen des Privaten* (S. 337–368). Wiesbaden: Springer VS.

Steinbicker, J. (2012). Der Staat und das globale Internet. In M. Bach (Hrsg.), *Der entmachtete Leviathan. Löst sich der souveräne Staat auf?* (S. 197–217). Baden-Baden: Nomos. https://doi.org/10.5771/9783845244273-197.

Stengel, O. (2017). Zeitalter und Revolution. In O. Stengel, A. van Looy, & S. Wallaschkowski (Hrsg.), *Digitalzeitalter – Digitalgesellschaft* (S. 17–49). Wiesbaden: Springer VS.

Symantec (Hrsg.). (2010). Norton Cybercrime Report: Faktor Mensch.

Tsitsika, A., Janikian, M., Wójcik, S., Makaruk, K., Tzavela, E., Tzavara, C., et al. (2015). Cyberbullying victimization prevalence and associations with internalizing and externalizing problems among adolescents in six European countries. *Computers in Human Behavior, 51,* 1–7. https://doi.org/10.1016/j.chb.2015.04.048.

Van Wilsem, J. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology, 8*(2), 115–127. https://doi.org/10.1177/1477370810393156.

Van Wilsem, J. (2013). ‚Bought it, but never got it' assessing risk factors for online consumer fraud victimization. *European Sociological Review, 29*(2), 168–178. https://doi.org/10.1093/esr/jcr053.

Wall, D. (2004). What are cybercrimes? *Criminal Justice Matters, 58*(1), 20–21. https://doi.org/10.1080/09627250408553239.

Wegge, D., Vandebosch, H., Eggermont, S., van Rossem, R., & Walrave, M. (2016). Divergent perspectives. Exploring a multiple informant approach to cyberbullying victimization and perpetration. *European Journal on Criminal Policy and Research*, *22*(2), 235–251. https://doi.org/10.1007/S10610-015-9287-5.

Yar, M. (2005). The novelty of ‚cybercrime'. *European Journal of Criminology, 2*(4), 407–427. https://doi.org/10.1177/147737080556056.

Ziercke, J. (2016). Cybercrime als Herausforderung für die Internetgesellschaft. In C. Bär, A. T. Fischer, & H. Gulden (Hrsg.), *Informationstechnologien als Wegbereiter für den steuerberatenden Berufsstand* (S. 229–241). Berlin: Springer.

Cyber-Viktimisierung von Unternehmen

Selma Lamprecht und Gergana Vladova

1 Einleitung

Die Viktimologie ist die Lehre vom Opfer und als solche, wie weite Teile der als täterzentriert geltenden Kriminologie, insbesondere auf Menschen zentriert. Wenige viktimologische Betrachtungen beschäftigen sich mit Unternehmen als Opfer. Entsprechend gering ist die Übertragungs- und Anpassungsarbeit von existierenden Ansätzen, welche anhand von menschlichen Erfahrungen aufgestellt wurden, auf die Spezifika von Organisationen. Eine solche Übersetzungsarbeit erscheint gerade für den digitalen Raum wichtig, da hier die Wissensbasis verschoben ist: Es gibt viele Betrachtungen zur digitalen Opferwerdung von Unternehmen ohne den Rückgriff auf viktimologische Ansätze. Viktimologische Betrachtungen digitaler Phänomene konzentrieren sich hingegen vorrangig auf Privatpersonen und auf spezifisch Individuen betreffende Delikte (z. B. Cybermobbing).

Das vorliegende Kapitel versucht, diese Forschungslücke genauer zu fassen und einen entsprechenden Lösungsansatz bereitzustellen. Dafür werden im ersten Teil die Fragen und Themen der Opferforschung allgemein systematisiert, skizziert und vor dem Hintergrund unseres Untersuchungsschwerpunktes diskutiert. Als solcher wurden Unternehmen aus der Perspektive der Viktimologie ausgewählt, mit anderen Worten: die Betrachtung von Unternehmen als Opfer

S. Lamprecht (✉)
Berlin, Deutschland
E-Mail: selma.lamprecht@fokus.fraunhofer.de

G. Vladova
Potsdam, Deutschland
E-Mail: gergana.vladova@wi.uni-potsdam.de

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

T.-G. Rüdiger und P. S. Bayerl (Hrsg.), *Cyberkriminologie,*
https://doi.org/10.1007/978-3-658-28507-4_14

von Cybercrime. Dabei wird in diesem Beitrag der Blick auf ein sehr enges Verständnis der Cybercrime als *„crimes unique to electronic networks“* (orientiert an dem engsten Verständnis nach der Dreiteilung der Kommission der EU 2007) fokussiert, obwohl die Überlegungen auch für einen weiteren Rahmen produktiv gemacht werden können.

Im zweiten Teil zielen wir darauf hin, einen möglichen Ansatz für die von uns geforderte Übertragung und Anpassung bestehender Ansätze aus der Opferforschung anzuregen. Die vorgeschlagene Vorgehensweise legt die Betrachtung von Individuen und Unternehmen als Systeme zugrunde (vgl. z. B. Luhmann 1984) und adressiert darüber ihre wesentlichen Elemente, Prozesse und Merkmale. Der Ansatz wird am Beispiel des Karrieremodells der Viktimisierung (Lebe 2003, S. 13) veranschaulicht: Mit einem Verständnis von Organisationen als soziale Systeme konfrontiert, wird das Stufenmodell für die digitale Opferwerdung von Unternehmen neu beschrieben.

2 Themen und Fragen der Viktimologie

Die in der Kriminologie vorherrschende Unterscheidung zwischen Mainstreamkriminologie als Hauptrichtung (zumindest im englischsprachigen Raum) und einer kritischen Kriminologie als Sammlung unterschiedlicher Nebenrichtungen (Schneider 2007, S. 148) lässt sich auch in der Viktimologie finden. Der konventionellen, auch konservative oder positivistische genannten Viktimologie als Hauptrichtung werden die radikale, die kritische oder die liberale Viktimologie als Nebenströmungen gegenübergestellt (z. B. Karmen 2012; Mawby und Walklate 1994). Der Unterschied liegt wesentlich in der ursprünglichen Definition von Opfer und Opferwerdung: Während sich die Hauptströmung sehr auf Street Crime als Deliktfeld konzentrierte,[1] weiteten die Nebenströmungen die Definitionen in verschiedene Richtungen aus. Vom Einbezug der Corporate Crime (Liberale) über die Betrachtung von Stigmatisierungen (Radikale) bis hin zur

[1]Eine diesbezüglich typische Definition von Opfer bringt zum Beispiel Kirchhoff (2010; zitiert in Turvey und Ferguson 2013, S. 113): *„A victim is an individual or a group forced to cope with important (at least) potentially uprooting events that can be actuated against him or her by other humans. […] Victimization must be human-made. […] The event must come from outside; therefore, suicide is usually not included in victimological theory […]. Finally, the victimization must be socially recognized. It is not enough that someone claims victim status without societal approval.“*

Viktimisierung durch grundlegende gesellschaftliche Strukturen und der Praxis von Zu- oder Aberkennung des Opferstatus (Kritische) (vgl. Wilson 2009, S. 62–63; Mawby und Walklate 1994, S. 4 f.).[2]

Für die Strukturierung werden hier die Ansätze grob nach enger (die Hauptströmung) und weiter (als Sammelbegriff für die Nebenströmungen) Viktimologie unterschieden und ihre verschiedenen Themen darunter sortiert.

2.1 Enge Viktimologie

> „Victimology's objective should be the development of a body of general and verified principles and of other types of knowledge regarding the causes and prevention of victimisation, the victimisation process, the effects of victimisation and the efficacy of treatment for effects". (O´Connell 2008, S. 101)

Die konventionelle Viktimologie stellt insbesondere Fragen nach den Eigenschaften von Opfern und durch Opfer beeinflussbaren Faktoren der Tatbegehung. Dafür werden Häufigkeiten gemessen, Opfertypisierungen gebildet und praxisnahe Präventionskonzepte und Evaluationsarbeiten erstellt. Durch den Einfluss der „crime victims movement" auf die amerikanische Viktimologie werden außerdem die Folgen für die Betroffenen als ein wesentlicher Bestandteil in Betracht gezogen (vgl. Turvey und Ferguson 2013, S. 19). Nachfolgend werden relevante Themen der engen Viktimologie diskutiert, wobei insbesondere auch der Stand der Forschung zu Unternehmen als Opfer verdeutlicht wird.

2.1.1 Quantifizierung

Eine wesentliche Grundlage der konventionellen Viktimologie ist die zahlenmäßige Erfassung von Opfern in der Bevölkerung durch (zum Teil repräsentative) Befragungen (Wilson 2009, S. 94). Mit dem Aufkommen dieser Viktimisierungs-Surveys gewann die Kriminologie ein quantifizierendes Instrument neben den polizeilichen Kriminalstatistiken, um nun auch das Dunkelfeld – die der Polizei nicht gemeldete oder bekannt gewordene Kriminalität – zu erforschen (Wilson 2009). Taten des digitalen Raumes finden sich heute als Deliktgruppe auch in

[2]Das geht zum Teil so weit, dass Knudten fünf Viktimologien – von der kriminellen über die politische, ökonomische und familiäre bis hin zur medizinischen Opferwerdung zum Teil der Viktimologie erklärt (Knudten 1988; zit. nach Landau und Freeman-Longo 1990, S. 271).

klassischen Viktimisierungs-Surveys wieder (ein Überblick: Reep-van den Bergh und Junger 2018, S. 94). Um die Jahrtausendwende begannen sich Forscher in der internationalen Viktimologie verstärkt mit Unternehmen zu beschäftigen und Victim Surveys mit Unternehmen durchzuführen (Shury et al. 2005). Dennoch erfuhren diese nie eine Standardisierung oder Regelmäßigkeit (vgl. Hopkins 2016a, S. 162), wie es für haushaltsbezogene Victim Surveys international und im angloamerikanischen Raum der Fall ist (eine Aufstellung bei: Noack 2015, S. 77 ff.). Eine noch geringere Verbreitung haben Befragungen im Unternehmenskontext bezüglich Cybercrime gefunden (z. B. in Belgien Paoli et al. 2018a; in Deutschland hat die Erhebungsphase 2019 begonnen: Cyberangriffe gegen Unternehmen, KFN 2018).

Sowohl die Befragung von Unternehmen als auch die Opferforschung bezüglich Cybercrime weisen verschiedene methodische Schwierigkeiten auf: von der Zusammenstellung der Stichprobe (z. B. der Frage des Umgangs mit Tochterfirmen und Niederlassungen) über die Identifikation von Verantwortlichen (oder passenden Ansprechpersonen) in einem Unternehmen (Bussmann 2015) bis zur bearbeiteten Definition von Cybercrime und der allgemein verständlichen Vermittlung von digitalen Sachverhalten und Begriffen (Huber 2015). Zahlen zu Unternehmen als Opfer von Cybercrime kursieren dennoch viele. Der Großteil der Zahlen stammt aus der IT-Wirtschaft oder von Daten der Versicherungen und bringen entsprechende Probleme mit. Interessenkonflikte und methodische Schwierigkeiten, zum Beispiel durch problematische Operationalisierungen von Angriffen, machen diese Daten nur bedingt vergleichbar und kaum belastbar (vgl. zum Beispiel Fafinski et al. 2010, S. 12 ff.; Wall 2007, S. 18; s. a. Kap. „Ist der Begriff „Cyberkriminalität“ in Forschung und Praxis hinreichend konturiert und somit adäquater (Sozial-)Kontrolle zugänglich?“). Als weitere Quellen für entsprechende statistische Daten dienen Polizeistatistiken und staatliche Erfassungen. Doch auch diese Zahlen gelten als wenig aussagekräftig, da in diesem Deliktfeld von einer sehr geringen Anzeigebereitschaft der Unternehmen ausgegangen wird (vgl. Amir et al. 2018; Fafinski 2009, S. 51). Entsprechend gibt es nach wie vor eine problematische Datenlage (vgl. Lorkowski 2015). Eine Ausnahme stellen Unternehmen der kritischen Infrastruktur dar, welche gesetzlich verpflichtet sind, bestimmte Vorfälle an das Bundesamt für Sicherheit in der Informationstechnik zu melden (BSI 2016, S. 48). Inwieweit diese Daten belastbar sind und für Forschungen herangezogen werden, bleibt abzuwarten.

2.1.2 Typologien und Kategorisierungen

Auf Grundlage der Daten von Opferzahlen und tiefer gehender Analysen ihrer Merkmale sucht die Viktimologie nach Mustern und versucht durch die Gruppie-

rung der Opfer (mindestens indirekt) Ursachen für die Opferwerdung zu ermitteln (zu Beginn der Viktimologie z. B.: Hentig 1967; heute zu individuellen Opfern von Cybercrime z. B. van de Weijer und Leukfeldt 2017).

Dabei werden unterschiedliche Kategorien für die Analysen und Erklärungen herangezogen und verschiedene Vorschläge der Typisierung darauf basiert(vgl. Landau und Freeman-Longo 1990, S. 271): Opfer können nach ihrer soziologischen Einheit z. B. in Individuum, Gruppe, Organisation, Staat oder Menschheit unterschieden (Sellin und Wolfgang 1964) oder aufgrund des ihnen zugeschriebenen Beitrages zur Tat eingeteilt (Voss und Hepburn 1968; Weis und Borges 1973) werden. Verbreitet ist insbesondere die Betrachtung anhand von konkreten, potenziell risikosteigernden Charakteristika der Opfer, zum Beispiel Alter, Geschlecht, Herkunft, Wohnregion oder Bildung (Oberwittler und Kury 2015, S. 112). Daneben werden auch verschiedene stärker kriminologische Kategorien wie Tätermerkmale, die Intentionalität der Tat oder die Opfer-Täter-Beziehung für Gruppierungen von Opfern und zur Erklärung ihrer Opferwerdung herangezogen (vgl. Landau und Freeman-Longo 1990).

Kriminologische Typisierungen

Mit der englischsprachigen „Cybercriminology“ haben diese Systematisierungen bezüglich Deliktarten und Tätermerkmalen bereits einige Aufmerksamkeit erhalten. Durch die ständigen Veränderungen des Feldes werden jedoch für die digitalen Delikte immer neue „Landkarten“ notwendig (eine umfassende Übersicht: Donalds und Osei-Bryson 2014) – und entsprechend auch immer neue Abwägungen und Untersuchungen, welche Vorgänge bei Unternehmen relevant oder wahrscheinlich sind (Safa 2017, S. 16–18). Für die Typisierung von Tätern wird häufig der Angriffstyp oder die Fähigkeiten und Professionalität der Täter betrachtet (z. B.: Hald und Pedersen 2012; McGuire und Dowling 2013). Nur teilweise wird die betroffene Opfergruppe einbezogen (Kshetri 2013, S. 23). Auch die typische viktimologische Überlegung einer besonderen Beziehung zwischen Opfer und Täter findet sich in der Betrachtung von Cybercrime gegen Unternehmen nicht im klassischen Sinn, sondern eher als eine Ausprägung der Deliktart. Huber und Pospisil unterscheiden z. B. ungerichtete, gezielte, skalpellartige Angriffe (2018, S. 48):

> „Bei unterrichteten Angriffen wählt der Täter sein Opfer nicht persönlich. Ziel ist möglichst viele Opfer zu erreichen [z. B. SPAM, Viren, Würmer; Anm. Autor]. Gezielte Angriffe hingegen richten sich an ein bestimmtes Opfer. Es wird eine Methode des Angriffs gewählt, die das Opfer auf jeden Fall erreicht [z. B. Social-Engineering, Trojaner; Anm. Autor]. Bei skalpellartigen Angriffen bedienen

> sich die Täter mehrere Methoden, um das Opfer zu erreichen. Diese Angriffe sind komplex und werden strategisch lange vorbereitet [z. B. Zero-Days, Fälschung von Zertifikaten Anm. Autor]."

Eine Sondergruppe bilden Innentäter (z. B. Nykodym et al. 2005; Williams et al. 2018). Sie offenbaren das Spannungsverhältnis, welches sich bei der viktimologischen Betrachtung von Unternehmen ergibt: Die Dichotomie zwischen Täter und Opfer verschwimmt und ihr Verhältnis muss in diesem Kontext neu ausgelotet werden.[3] Vielfach wird auf die Schwierigkeit der Erfassung hingewiesen (siehe Abschn. 2.1.1), weshalb es keine genaue Aufstellung gibt, inwieweit sich die kriminologischen Merkmale zwischen betroffenen Unternehmen bzw. zwischen Unternehmen und Individuen unterscheiden.

Charakteristika

Insbesondere bei der Betrachtung der vulnerabilitätssteigernden Charakteristika wird schnell deutlich, dass die an Individuen extrahierten Größen (z. B. Alter, Geschlecht, räumliche Lage; Kesteren et al. 2014, S. 53) weder adäquat auf den Cyberspace noch auf Unternehmen übertragbar sind. Die existierende Forschung zu Unternehmen als Opfer (unabhängig vom Digitalen) hat stattdessen Faktoren wie den Geschäftsbereich (z. B. Verkauf, Produktion oder Dienstleistung), die Zahl der Angestellten, die Zugehörigkeit zu einer Unternehmenskette, den Umsatz, aber auch die räumliche Lage als relevant für das Risiko einer Viktimisierung formuliert (Hopkins 2016b).

Forschungen bezüglich viktimisierender Faktoren im Digitalen arbeiten zu individuellen Opfern meist unter Bezug auf das „Routine Activities Modell"[4] aus der klassischen Viktimologie (z. B. Bossler und Holt 2011; Choi 2011; Leukfeldt

---

[3]Allgemein zur Schwierigkeit der Trennung von Täter und Opfer bereits bei Individuen: *„Within positivist victimology, victims and offenders exist in a zero sum relationship with one another. The fact that as experiential categories they overlap, or that there may be delinquent victims (Miers 2007), is difficult for positivist victimology to embrace. Consequently positivism reflects a rather individualistic, passive and static understanding of the process of criminal victimisation and betrays an implicit acceptance of a functionalist view of society"* (Walklate 2012).

[4]Dieses sehr verbreite viktimologische Vorhersagemodell geht davon aus, dass die Wahrscheinlichkeit einer Viktimisierung steigt, wenn ein attraktives Ziel und fehlende Schutzmechanismen mit einem motivierten Täter zusammentreffen (Cohen und Felson 1979). Besonders durch das geringe notwendige Wissen über den Täter gilt es als produktiv für Cybercrime (Williams et al. 2018, S. 4).

und Yar 2016). Bisher gibt es jedoch nur eine Studie, die diesen Ansatz auf die Viktimisierung von Unternehmen überträgt – dort mit dem Fokus auf Insider-Taten (Williams et al. 2018). In den bisherigen größeren Untersuchungen zu Cyberangriffen auf Unternehmen wurden insbesondere die Faktoren Größe der Unternehmen, Branche, Angriffs- bzw. Deliktarten, Lage und Digitalisierungsgrad betrachtet (vgl. Bartsch et al. 2018; BSI 2018; Huber und Pospisil 2018; Paoli et al. 2018b). Insbesondere der letzte Punkt ist vielfach gekoppelt an die Frage nach aktiven Schutz- und Präventionsmaßnahmen in den Unternehmen. Wie schwierig die Datenlage und wie unklar die Einflussfaktoren sind, lässt sich anschaulich in den Arbeiten zu Cyberrisk (vgl. Eling und Schnell 2016; Peters et al. 2018) und Cyber-Policen sehen, welche die fehlende Datenlage und entsprechenden fehlenden Probabilitätsmodelle als ein zentrales Problem für diesen Bereich beschreiben (vgl. Tøndel et al. 2016; Wrede et al. 2018, S. 421 und 424).

2.1.3 Opferzentrierte Prävention

Eine weitere in der Viktimologie als Risiko verstandene und zur Typisierung verwendete Größe ist der „Beitrag des Opfers zur Tat“ (vgl. Landau und Freeman-Longo 1990, S. 280 ff.). Der Beitrag der Unternehmen wird vorrangig an der Frage von vorgenommenen Präventionsmaßnahmen diskutiert (vgl. Kopp et al. 2017, S. 8). Daher werden diese Aspekte hier zusammengefasst.

> „Victimologists assess the vulnerability of a target, regardless of whether it is tangible or non-tangible, after which the goal focuses on strategies for reducing crime and victimization risks through prevention.“ (Wilson 2009, S. 299)

Ähnlich dieser Ermächtigungsintention früher viktimologischer Forschungen durch die Konzentration auf Opfermerkmale mit dem Ziel vorbeugender Anpassungen (der Opfer) dominiert unter dem Stichwort „IT-Security“ ein industrie- und unternehmensnaher Fokus auf Schutzmaßnahmen derzeit die Forschung und Betrachtung von Opfern im Digitalen (Graham 2018; Huber 2015). Dabei gibt es unterschiedliche Konzepte zur Strukturierung der Schutzgüter, z. B. die RiSiKo-Management Pyramide von Müller (2015)[5]; die Kategorisierung in Vernetzungs- und Internetsicherheit, Digitale Unternehmenssicherheit, Client- und

[5] *„die Sicherheitsmanagementpyramide bietet ein strukturiertes, durchgängiges, strategisches und praxisorientiertes Top-down-Vorgehensmodell zum ganzheitlichen Aufbau und zur Weiterentwicklung des Sicherheits-, Kontinuitäts- und Risikomanagements.“* (Müller 2015, S. 137)

Serversicherheit und Mobile Security bei Steinmann (2018) oder die Orientierung an einem erweiterten OSI-Modell (Swire 2018).[6]

Unseres Erachtens ist daneben auch folgende, nicht auf das Schutzgut, sondern vielmehr an den handelnden bzw. für den Schutz adressierten Akteur ausgerichtete Strukturierung denkbar: Zu Beginn der Forschung zu diesem Themenfeld wurde IT-Security insbesondere als ein technisches Problem, d. h. als die Benutzung sicherer Software bzw. dem Einsatz von Schutzsystemen wie Firewalls verstanden und adressiert (vgl. Gao et al. 2015, S. 243; Klipper 2015, S. V). Aktuell werden auch das Management des Unternehmens und die individuellen Verhaltensweisen der Mitarbeiter als gleichermaßen wichtig erkannt. Bei den Mitarbeitern soll zum Beispiel mit *„awareness-raising activites“* (Pattabiraman et al. 2018, S. 162) ein Bewusstsein für die Gefahren geschaffen werden (Safa und Von Solms 2016). Auch auf der Management-Ebene spielt die Frage des Bewusstseins für das Thema eine Rolle, z. B. bei der Verteilung finanzieller Mittel (Fielder et al. 2016; Hausken 2006; Srinidhi et al. 2015). Andere Managementfaktoren, wie Informationssicherheitsrichtlinien, Compliance-Schulungen, effektive interne Kommunikationsprozesse und IT-Infrastrukturmanagement werden unter dem Stichwort einer *„holistischen organisationalen Betrachtung“* angemahnt (ein ausführliches Review: Soomro et al. 2016). Daneben kann die staatliche Ebene ebenso als Akteur für Prävention von Cybercrime betrachtet werden. Gesetzliche Rahmenbedingungen (z. B. Meldepflichten für Vorfälle im IT-Sicherheitsgesetz oder der Pflicht zu einem betriebsinternen IT-Sicherheitskonzept) haben einen Einfluss auch auf die Unternehmen und können eine verhütende Wirkung entfalten (Müller 2015, S. 29).

Insgesamt scheint die praktische Orientierung der frühen Viktimologie (vgl. Wilson 2009, S. 299) derzeit unter dem Stichwort IT-Security auch bezüglich Unternehmen als Opfer von Cybercrime prävalent.

[6]Das OSI-Modell (Open Systems Interconnection Model), auch ISO/OSI-Schichtenmodell genannt, ist ein Referenzmodell, welches die Kommunikation zwischen Computersystemen beschreibt. Das Modell besteht aus verschiedenen Schichten (Layers), welche jeweilig klar voneinander abgegrenzte Aufgaben ausführen. Neben diesen sieben technischen Ebenen, definiert Swire drei soziale. Mit der Erweiterung macht er deutlich, dass Kommunikation nicht nur auf der technischen, sondern auch auf sozialen Ebenen angreifbar, und entsprechend zu schützen ist.

2.1.4 Folgen

Die Selbst- und Fremdwahrnehmung der Opfer nach einer Tat rückten mit den „Victim Rights Movements“ und der Entstehung professioneller Opferhilfe in den Fokus. Besonders bekannt ist diesbezüglich das Karrieremodell der Viktimisierung (vgl. Condry 2010, S. 236). Demnach werden die direkten Verletzungen der Tat als primäre Viktimisierung besprochen, welche weitere Viktimisierungen durch den Umgang mit diesem ersten Vorfall zur Folge haben können. Die Reaktionen von Angehörigen, der Öffentlichkeit oder die Rolle der Betroffenen im Strafprozess kann diese erneut zum Opfer machen – es kommt zur sogenannten sekundären Viktimisierung (vgl. Haupt 2003, S. 36). Die tertiäre Viktimisierung ist der Theorie nach eine mögliche dritte Stufe der Viktimisierung, bei welcher Betroffene als Folge vielfacher Viktimisierungserfahrungen (primärer und sekundärer Art) eine Opferidentität annehmen. Erlernte Hilflosigkeit (Lebe 2003, S. 13 f.) oder die Verinnerlichung der Opferrolle verhindern die Rückkehr in ein normales Leben (Schwind 2013, S. 247).

Die Folgen von digitalen Schädigungen werden vorrangig monetär erfasst und gewichtet (Huber und Pospisil 2018, S. 74 f.) – insbesondere in Bezug auf Unternehmen (Anderson et al. 2013; Paoli et al. 2018b). Dabei legen diese ökonomischen Analysen unterschiedliche Einstufungen und Parameter an. Die Folgen von Imageverlust, Kundenreaktionen (Böhme und Moore 2012; Mikhed und Vogan 2018; Rosati et al. 2019; Syed 2018) und Börsenentwicklung (s. Review von Spanos und Angelis 2016) werden zum Teil in diesen Schadenskalkulationen ebenso einbezogen wie die Investitionen in Schutzmechanismen (Anderson et al. 2013; Detica 2011). Dies führt eine Übertragung des Karrieremodells der Viktimisierung an Grenzen, obwohl insbesondere die Reaktionen von Anlegern, Medien und Kunden durchaus im Sinne einer sekundären Viktimisierung verstanden werden können. Ökonomische Modelle und Strukturierungen (z. B.: Klahr et al. 2017; Paoli et al. 2018a) sind hier jedoch wesentlich präsenter.

Noch gravierender zeigen sich die Grenzen des Karrieremodells bei der Idee einer tertiären Viktimisierung von Unternehmen. Obwohl es durchaus denkbar wäre, dass Mitarbeiter nach einer Viktimisierung resignieren oder es zu vermehrtem Whistleblowing kommt, erscheint eine Organisation, welche sich über ihren Status als Opfer einer Cybercrime definiert – wie es die Idee der „Selbstviktimisierung“ (Kiefl und Lamnek 1986, S. 273) ist – in der Form kaum plausibel.

2.2 Weite Viktimologie

Die Nebenrichtungen der Viktimologie legen andere Definitionen von Opfer und Opferwerdung zugrunde und weiten Begriff und Forschungsbereich entsprechend auf. Die liberale Viktimologie bezieht zum Beispiel explizit auch Opfer von Unternehmenskriminalität (Corporate Crime) mit ein (Karmen 2012, S. 22). Dies ist zunächst eine Erweiterung, welche neue Themen, aber keine neuen Fragen setzt. Die kritische und radikale Viktimologie setzten bei der Wissensbildung an, indem sie fragen, was bei der (konventionellen) Viktimologie und den bisherigen Umgangsformen (des Staates) mit Opfern unsichtbar geblieben ist (Walklate 2008, S. 323 z. B. Opfer von Kriegen). Die Logik abweichenden Verhaltens aus der kritischen Kriminologie aufgreifend werden entsprechend auch Viktimisierungen durch gesellschaftliche Aushandlungen und Ausgrenzungen über das Strafrecht hinaus aufgegriffen.

Löst sich der enge Kriminalitätsbezug zugunsten eines Ansatzes abweichenden Verhaltens, werden neue Phänomene, zum Beispiel der Ausgrenzung, erfassbar. Aus dieser Richtung gibt es Ansätze ein breiteres Feld, als das der engen Cybercriminology (vgl. z. B. die Definition bei Ngo und Jaishankar 2017), zu öffnen (Powell et al. 2018). Statt individueller Merkmale und Zuweisungen an das Opfer steht hier das Rechtssystem und die gesellschaftliche Struktur im Zentrum. Der zentrale Bezugspunkt bildet die Zugriffsmacht und die entsprechende Frage: Wie ist die strukturelle Rahmensituation bei der digitalen Viktimisierung?

Der Fokus der kritischen Viktimiologie lag und liegt auf staatliche Stellen; so wird beispielsweise der staatliche Versuch der Kontroll- und Machtverstärkung auch im Digitalen fokussiert (Cavelty 2013, S. 106; Schulze 2016). Dies ist jedoch nur ein Teil: Im Digitalen liegt ein Teil struktureller Macht bei IT-Unternehmen, welchen Individuen aber auch andere Unternehmen mit dem Rückgriff auf technische Komponenten und Bedingungen der Geräte (zum Beispiel gegenüber Systemänderungen oder Lücken des Betriebssystems), entsprechend untergeordnet sind. Damit werden auch die ethischen Debatten und staatlichen Ambitionen bezüglich des Zwangs für Hintertüren in Software (zum Beispiel in Messenger Diensten) zum wichtigen Thema (Jenner 2018; Pfefferkorn 2018; Smith und Green 2017). Die geringe Bereitschaft der Unternehmen, sich an die staatlichen Stellen zu wenden, und die Bedeutung der technischen Rahmen (wie Software oder Hardware) und ihrer Anbieter führen im Bereich der Cybercrime zu einer erheblichen Veränderung der Akteursverteilung und ihrer Bedeutungen

(Cavelty 2015; Analysen z. B.: D'Elia 2016; Skibell 2002). Dies spiegelt sich auch in der zentralen Frage der kritischen Viktimologie nach der Definitionsmacht über den Opferstatus wieder. Es stellen sich Fragen, wie: Wer hat die Macht jemanden zum Opfer zu erklären oder jemandem diesen Status vorzuenthalten? Und wann wird diese Macht eingesetzt (Miers 1990, S. 224)? Anhand des Bildes eines idealen Opfers (Christie 1986; eine Übertragung des Ansatzes auf Unternehmen: Hopkins 2016b) wird aufgezeigt und kritisiert, wie durch (öffentliche) Darstellungen und gesellschaftliche Zuschreibungen in eine Opferrolle eingeschlossen oder von dem Opferstatus ausgeschlossen wird. Ein Beispiel ist das Problem der Attribution: So kann das Handeln einer Person in einer Situation oder auch einer Technik und deren Eigenschaften zugeschrieben (Hempel 2017, S. 471) werden. Obwohl Hempel (2017) die Verantwortungszuschreibung bezüglich der Täterschaft analysierte, ist dies ebenso für die Opferschaft denkbar und verdeutlicht die Veränderung der Akteurs- und Machtverteilungen. Hier kommt insbesondere den Medien – und den sozialen Medien – eine verstärkte Rolle zu: „In the digital age, news and social media debates are a key influence in shaping popular notions of who can rightly claim legitimate victim status" (Davies et al. 2017, S. 62).

2.3 Zwischenstand

Sowohl die Erforschung von Opfern im digitalen Raum als auch von Unternehmen als Opfer weicht deutlich von typischen viktimologischen Rahmen und Opfergruppen ab. Die grundlegenden Fragen bleiben jedoch die gleichen: Welche Faktoren beeinflussen das Viktimisierungsrisiko? Welche Präventionsmaßnahmen gibt es und greifen sie? Welche Folgen hat eine Viktimisierung? Und wer definiert, was als Verletzung zählt?

Allerdings unterscheiden sich, wie hier angedeutet, die erklärenden Dimensionen und Kategorien grundlegend. Entsprechend erscheint auch der Einbezug anderer Theorien und Disziplinen hilfreich: neben der Kriminologie und Psychologie erscheinen uns für das Digitale und im Falle von Unternehmen als Opfer insbesondere die Techniksoziologie und die Organisationsforschung wichtige Impulsgeber.

Grundsätzlich ist bei der Übertragungsarbeit Vorsicht geboten: Bereits früh wurden die Probleme der Übertragung von an Individuen aufgestellten Theorien auf Unternehmen festgehalten und angemahnt (Braithwaite und Fisse 2017; Cressey et al. 2017). Parallel stellt sich die Frage, inwieweit Theorien und

Erkenntnisse, welche anhand von Delikten in der physischen Welt beobachtet und aufgestellt wurden, auf digitale Vorgänge und Verhaltensweisen übertragbar sind (für eine Übertragung anerkannter kriminologischer Theorien: Grabosky 2001; dagegen: Yar 2013, S. 10 ff.).[7]

3 Cybercrime als Ereignis in einem sozialen System

Wir betrachten Cybercrime als einen besonderen Akt der Kommunikation, welcher zu Störungen und Veränderungen führt, in Unternehmen nicht vorgesehen ist und in diesem Sinne ihre eigene Gesetzmäßigkeiten angreift. Damit handelt es sich um einen Eingriff (meistens von Außen), bei welchem bestimmte Regeln absichtlich missachtet werden und wobei das Unternehmen gezwungen wird, sich anzupassen. Das Letztelement eines sozialen Systems nach Luhmanns Systembegriff ist Kommunikation (Luhmann 1984, S. 192). In diesem Sinne bietet die Nutzung des Systembegriffs eine produktive Annäherung an die digitale Viktimisierung von Unternehmen, da sie wesentlichen Elemente des Phänomens (Mitgliedschaft, Zweck, Hierarchie) berücksichtigt und fokussiert. Außerdem ermöglicht der Ansatz den Vergleich mit Prozessen der individuellen Opferwerdung, welche als soziale Interaktion eines physischen Systems (dem Menschen) verstanden werden. Entsprechend folgt eine knappe Einführung in die Systemtheorie und insbesondere bezüglich der sozialen Systeme und konkret der Organisationen wesentlicher Begrifflichkeiten.

[7]Yar argumentiert, dass die Umwelt einen wesentlichen Einfluss auf soziale Interaktionen hat und entsprechend die Neuartigkeit der digitalen Umgebung (mit dem Zusammenbruch der Zeit-Raum-Barrieren, der Viele-zu-Viele-Konnektivität und der Fluidität und Anonymität von Identitäten) auch völlig neue Formen und Muster des illegalen Verhaltens ermöglicht und entsprechend Cyberkriminalität zu etwas unverwechselbarem und originellem macht (Yar und Steinmetz 2019, S. 14). Grabosky argumentiert dagegen, dass mit der Digitalisierung zwar neue Bedrohungen (z. B. von persönlichen Daten) und Manifestationen von Kriminalität einhergehen, sich aber weder die Motivationen noch die Schutzstrukturen wesentlich unterscheiden („*The policing of terrestrial space is now very much a plualistic endavor. So too is the policing of cyberspace […] In cyberspace today, as on terrestrial space two millennia ago, the first line of defence will be self-defence*“ Grabosky 2001, S. 248) und es sich entsprechend nach wie vor um deutlich erkennbare Verbrechen, die nur auf eine ganz andere Weise begangen wurden, handelt (Grabosky 2001, S. 243).

3.1 Systemtheorie

Die Systemtheorie Luhmanns beschäftigt sich mit dem Gegenstand der Differenz von System und Umwelt und den damit verbundenen Problemen und Problemlösungen (Luhmann 1987, S. 38). Es besteht eine klare Trennung zwischen psychischen Systemen (Menschen) und sozialen Systemen (Kommunikationssystemen). Soziale Kontakte werden nach Luhmann als Systeme betrachtet, die sich von ihrer Umwelt abgrenzen (Luhmann 1984, S. 33). Um sich zu konstituieren und zu erhalten, müssen Systeme die Differenz zur Umwelt erzeugen und erhalten. Die Differenz von System und Umwelt muss dabei im System selbst produziert werden und wird an der Grenze reguliert (Luhmann 1984, S. 35; Weik und Lang 2003, S. 122): *„Systeme sind nicht nur gelegentlich und nicht nur adaptiv, sie sind strukturell an ihrer Umwelt orientiert und könnten ohne Umwelt nicht bestehen“* (Luhmann 1984, S. 35).

Luhmann (1987, S. 28) sieht den Unterschied zwischen System und Umwelt grundsätzlich als ein Komplexitätsgefälle. Dabei ist die Komplexität der Umwelt stets höher als die des Systems. Die Umwelt wird als deutlich komplexer gesehen und die Möglichkeiten, die sie bietet, unzählig (Luhmann 1987, S. 9). Vor diesem Hintergrund benötigen Systeme intern angefertigte Richtgrößen und ihre Beschreibungen, die sie befähigen, die Unterscheidung von System und Umwelt zu erkennen und sich daran zu orientieren. In diesen Beschreibungen wird unter anderem festgelegt, welche Ereignisse und Zustände zum System und welche zur Umwelt gehören (Luhmann 1987).

Zwei Faktoren – Komplexität und Kontingenz – sorgen dafür, dass Systeme mit einer Überfülle an Möglichkeiten konfrontiert werden, was von Luhmann (1984, S. 45–47) als ein Kardinalproblem beschrieben wird. Als Kontingenz wird zum einen die Abhängigkeit der Strukturen und Praktiken des Systems von der Art der Relevanz einer Umwelt für ein System beschrieben. Kontingenz bedeutet jedoch auch Unsicherheit darüber, inwieweit die Prämissen für das eigene Verhalten gegeben sind oder gegeben werden (Luhmann 1975, S. 40). Unter Komplexität ist die Vielzahl an verschiedene Systeme und Umwelten zu verstehen und somit die Gesamtheit der möglichen Ereignisse und Zustände (Kneer et al. 1993, S. 40). Nach Luhmann (1984, S. 16 f.) können vier Arten von Systemen unterschieden werden: Maschinen, Organismen, psychische Systeme und soziale Systeme. Alle Systeme operieren in Differenz zu ihrer Umwelt und sind autopoietisch (d. h. produzieren und reproduzieren sich selbst; Luhmann 1984, S. 46). Wir nutzen den analytischen Zugang zu diesen Systemen und konzentrieren uns – nach der Auseinandersetzung mit dem Menschen in den bisherigen

Überlegungen – auf Organisationen als einen der drei Typen sozialer Systeme Interaktionen, Organisationen und Gesellschaften.

3.2 Soziales System

Ein System kann als ein soziales System definiert werden, *„wenn Handlungen mehrerer Personen sinnhaft aufeinander bezogen werden und dadurch in ihrem Zusammenhang abgrenzbar sind von einer nicht dazu gehörigen Umwelt“* (Luhmann 1975, S. 9) Dabei ist es als Kommunikationssystem zu verstehen, da *„der basale Prozeß sozialer Systeme, der die Elemente produziert, aus denen diese Systeme bestehen, […] unter Umständen nur Kommunikation sein [kann]“* (Luhmann 1984, S. 194). *„Soziale Systeme konstituieren sich durch Prozesse der Selbstselektion und der damit einhergehenden Grenzdefinition auf der Basis selektiver Prozesse“* (Luhmann 1975, S. 22), wobei die Reduktion der Komplexität für ihre Entstehung und Erhaltung entscheidend ist (Luhmann 1975, S. 10). Ein soziales System *„vermag aus den (selbst der wieder sozial bedingten) Potentialitäten der Individuen seine eigene Erzeugung zu ‚katalysieren‘“* (Luhmann 1975, S. 22).

Die Kommunikation als basaler Prozess eines Systems besteht aus einem dreistufigen Selektionsprozess, an dem mindestens zwei Prozessoren beteiligt sind (Weik und Lang 2003, S. 141):

1. *Selektion der Information:* Hier nimmt der Sender diverse Informationen aus der Umwelt wahr (Berghaus 2011, S. 78) und ordnet diesen Informationen Bedeutung zu (Luhmann 1984, S. 194).
2. *Auswahl der Mitteilung des Mediums:* Die Mitteilung beinhaltet nur ein Teil der Information (Berghaus 2011, S. 81).
3. *Verstehen, Annahme oder Nichtannahme der Mitteilung:* Der wichtigste Schritt im Kommunikationsprozess (Berghaus 2011, S. 82; Luhmann 1984, S. 196) erfolgt auf der Seite des Empfängers mit dessen Selektion von Inhalten, die ihn tatsächlich erreichen.

3.3 Organisation als soziales System

Im diesem Abschnitt fokussieren wir uns auf die Organisation als soziales System. Der basale Prozess eines sozialen System ist Kommunikation (Luhmann 1984, S. 192) und die basale Operation der Organisation ist die Entscheidung

(Luhmann 1984, S. 339–340). Organisationen sind operativ geschlossen (lediglich auf die eigene Selbstorganisation angewiesen), umweltoffen (besitzen nach Außen offene Grenzen und importieren und exportieren über diese) und selbstreferenziell (reagieren selbstständig auf ihre Differenz zur Umwelt; Luhmann 1975, S. 35 ff.). Organisationen werden über drei Merkmale bzw. Elemente definiert:

1. Die *Mitgliedschaft* ist das zentrale Merkmal von Organisationen, welches über den Eintritt und Austritt von Personen entscheidet (Luhmann 1975, S. 99). Es ist an eine formale Regelbefolgung gebunden, die den Mitgliedern die Erwartung zur Erfüllung dieser Regeln stellt (Luhmann 2000, S. 50). Das System und die Umwelt werden hier durch Zugehörigkeit und Nichtzugehörigkeit abgegrenzt (Luhmann 2000, S. 212). Mitglieder werden durch Geld, Zwang oder Angebot attraktiver Zwecke und Handlung sowie Kollegialität zur Mitgliedschaft motiviert (Kühl 2011, S. 38–45).
2. Die *Zwecke* beschreiben die geschätzte Wirkung eines Handelns und sind entscheidend, um zwischen erstrebten und nicht erstrebten Zuständen zu entscheiden (Krause 2001, S. 237; Luhmann 1973, S. 46 und 88)
3. Die *Hierarchie* ist notwendig für den Aufbau komplexer Organisationen (Luhmann 2000, S. 20). Hier wird definiert, wer wem in der Organisation unterstellt ist. Außerdem dient sie zur Abstimmung des Verhaltens der Organisationsmitglieder (Luhmann 1999, S. 209).

Darüber hinaus können in einer Organisation zwei Arten von Strukturen unterschieden werden: Formale (Entscheidungsprogramme, Kommunikationswege und Personal) und informelle (auch Organisationskultur genannt; beschreibt alle Erwartungen, die keinen Bezug auf Mitgliedschaftsbedingungen haben und beeinflusst das Handeln der Mitglieder; Kühl 2011, S. 113 f.). Beide Strukturen dienen als Entscheidungsprämissen in der Organisation (Kühl 2011). Die Entscheidungen sind kontingent und werden als Wahl zwischen mehreren Alternativen definiert (Luhmann 1981, S. 337 ff.).

Eine weiteres Merkmal von Systemen ist ihre Offenheit gegenüber der Umwelt (Luhmann 1984, S. 35). Im Kontext dieser Offenheit entstehen gegenseitige Einflüsse und Wirkungen zwischen System und Umwelt, die als Irritationen bezeichnet werden (Krause 2001, S. 127 f.). System und Umwelt begegnen sich im System an sogenannten Grenzstellen. Diese agieren unter anderem als Filter der Irritationen, die durch die Umwelt ausgelöst werden; Grenzstellen absorbieren damit die Unsicherheit an der Systemgrenze (Luhmann 1999, S. 221–224) und interpretieren die Umwelt für das System. Sie sind jeweils für

einen bestimmten Teil der Umwelt zuständig (Luhmann 1999, S. 221 und 224). Sie erkennen und filtern Informationen aus der Umwelt, übertragen sie in die systemeigene Sprache, übernehmen Verantwortung für die Richtigkeit und für die Vollständigkeit der Information bezüglich der Relevanz der Umwelt für das System (Luhmann 1999, S. 224). Außerdem vertreten Grenzstellen das gesamte System nach Außen.

Die vorgestellte kurze theoretische Auseinandersetzung mit der Systemtheorie hat als Ziel, zentrale Annahmen und Elemente vorzustellen, die nachfolgend als Grundlage für die Strukturierung unserer Vorgehensweise für die Übertragung viktimologischer Ansätze von der individuellen auf die Unternehmensebene dienen. Zentrale Grundlage für die Überlegungen bildet die Fokussierung in der Systemtheorie auf die abstrakte Ebene von Ereignissen und Differenzen.

Wir gehen davon aus, dass ein Cybercrime Akt als ein Austausch bzw. Kommunikation zwischen der Organisation und der Umwelt zu betrachten ist, welcher die beschriebenen Elemente des Systems adressiert: Mitgliedschaft, Zwecke und Hierarchie. Die Organisation wird unter Umständen die Regeln ihrer Mitgliedschaft überdenken. Andererseits steht sie vor der Entscheidung, welche Bedeutung der Angriff für sie hat, wobei hierarchische Beziehungen bei der Entscheidungsfindung eine zentrale Rolle spielen.

4 Vorschlag zur Übertragung der Untersuchungsansätze für Individuen auf Unternehmen

Wie in der Einleitung verdeutlicht, sind die nachfolgenden Überlegungen als eine Anregung zur Betrachtung von Individuen und Unternehmen als Systeme und einer Strukturierung einer möglichen Übertragung der Analyseansätze zu sehen. Dabei verstehen wir Unternehmen und individuelle Opferwerdung als Systeme. Individuen (Opfer) werden als physische Systeme betrachtet, welche durch die Interaktion zum Zeitpunkt der Opferwerdung einer Störung von Außen ausgesetzt sind. Nach Anpassung des physischen Systems werden von der Opferseite her die Selbst- (systemintern) und Fremdreferenz (systemextern) und die Kommunikationsprozesse stark beeinflusst.

Hierbei ist unsere Bestrebung nicht, die Systemtheorie in ihrer Gesamtkomplexität zu adressieren. Vielmehr nutzen wir die oben vorgestellten Elemente, Prozesse und Merkmale als Rahmen für die Übertragung der Theorien und Ansätze aus der individuellen Opferforschung in die Betrachtung von Unternehmen. Die Übertragbarkeit wird ermöglicht durch den Rückbezug auf

Kommunikation als zentraler Prozess von sozialen Systemen (Organisation und Interaktion). Wie dabei die Unterschiede der Systeme berücksichtigt werden, skizzieren wir nachfolgend am Beispiel des Karrieremodells (Stufen der Viktimologie). Alle drei Stufen der Viktimisierung (primäre, sekundäre und tertiäre) sind mit spezifischen Kommunikations- und Austauschbeziehungen verbunden, die das System unter Umständen verändern.

4.1 Primäre Viktimisierung

Die primäre Viktimisierung kann als die Verletzung unmittelbar durch die eigentliche Tat beschrieben werden. Auf der Ebene des Individuums als Opfer wird auf dieser Stufe lediglich eine Instanz adressiert bzw. ist für die Betrachtung relevant – das Opfer in Gestalt einer einzelnen Person.

Für Unternehmen als soziale Systeme jedoch bedeutet das eine prozessuale und strukturelle Veränderung. Als Opfer von Cybercrime werden an erster Stelle hier ihre Kommunikationsprozesse geschädigt bzw. gehen verloren. Der Angriff führt zu einem direkten Daten- und Informationsverlust, greift jedoch auch die Art und Weise an, wie die Kommunikations-, Differenzierungs- und Entscheidungsfindungsprozesse im System ablaufen. Formelle und informelle Strukturen haben Bedeutung für die primäre Viktimisierung und die Reaktionen darauf. Es ist wichtig an dieser Stelle festzustellen, ob alle Mitglieder im System die Opfersituation wahrgenommen haben, ob sie sich darüber im Klaren sind, welche Bedeutung dies für die Zwecke der Organisation hat und ob sie sich bestehenden Hierarchien im Kontext der Entscheidungsfindung für weitere Schritte bewusst sind. Gleich für beide Systeme – Mensch und Unternehmen – ist die Tatsache, dass bei der primären Viktimisierung die Systemgrenzen bezüglich der Wahrnehmung als Opfer nicht überschritten werden (vgl. Tab. 1).

Tab. 1 Primäre Viktimisierung

Beschreibung der Stufe	Bedingungen für den Auftritt	
	Mensch	Unternehmen
Direkte Verletzungen durch die Tat	Keine zwingenden Kausalitäten, aber verschiedene Einflussfaktoren wie z. B. Prävention oder anderen spezifischen Verhaltensweisen	Keine zwingenden Kausalitäten, aber verschiedene Einflussfaktoren wie z. B. Prävention oder andere spezifische Verhaltensweisen

4.2 Sekundäre Viktimisierung

Im Gegensatz zur primären Viktimisierung ist die Überschreitung der Systemgrenzen nach Außen grundlegend für die sekundäre Viktimisierung: *„Sekundäre Viktimisierung durch eine Interaktion ist nicht möglich, wenn der/die Interaktionspartner*in nicht über die primäre Viktimisierung informiert ist“* (Metzner 2018, S. 53 Hervorhebung im Original). Die sekundäre Viktimisierung erweitert die Selbstwahrnehmung als Opfer durch die Fremdwahrnehmung und hat eine andere Auswirkung auf die Systemelemente verglichen mit der primären Viktimisierung.

Auf der Ebene des Individuums als Opfer wird die Intensivierung der Opferwahrnehmung als relevant untersucht. Für Unternehmen als soziale Systeme mit Schnittstellen nach Außen kann die eigene Opferwahrnehmung noch verstärkt werden dadurch, dass direkte Partner ebenso zu Opfer gemacht werden und das Unternehmen eventuell Mitschuld trägt. Auch hier wird der Kern des Systems – d. h., seine Kommunikationsprozesse – geschädigt bzw. gehen verloren. Der Angriff führt zuerst zu einer Überdenkung/Überprüfung der Zwecke der Organisation. An dieser Stelle kommen wichtige Fragen auf wie bestehende und notwendige moralische, vertragliche oder juristische Verpflichtungen. Bestehende Entscheidungswege werden genutzt und unter Umständen neue Entscheidungsstrukturen geschaffen. Insbesondere die Systemgrenzen werden kritisch betrachtet und der Selektionsprozess der (Außen)Kommunikation und Mitteilungen und Medien der Übermittlung von Informationen über die Systemgrenzen hinaus sorgfältig überprüft.

Die Reaktion der Außenwelt kann sowohl symbolische/non-tangible Effekte auf das System ausüben (Vertrauensverlust) als auch wirtschaftliche (Unterbrechung der Beziehungen) oder juristische Folgen (Anzeige) für das Unternehmen haben. Die Möglichkeit, unbewusst vom Opfer zum Täter zu werden durch eine direkte Übertragung des Akts, welcher das Unternehmen zum Opfer gemacht hat, auf weitere Systeme (z. B. Unternehmen), ist ein deutlicher Unterschied zu der Opferrolle des Menschen (vgl. Tab. 2).

4.3 Tertiäre Viktimisierung

Die tertiäre Viktimisierung ist wieder auf das Innere des Systems bezogen: *„Die Opferrolle wird in das Selbstbild übernommen“* (Metzner 2018, S. 54). Die Interaktionen der primären und sekundären Viktimisierung beeinflussen dauerhaft das psychische System.

Tab. 2 Sekundäre Viktimisierung

Beschreibung der Stufe	Bedingungen für den Auftritt	
	Mensch	Unternehmen
Die Reaktionen von Angehörigen, der Öffentlichkeit oder die Rolle des Betroffenen im Strafprozess kann diese erneut zum Opfer machen	Die Tat, die das Individuum zum Opfer gemacht hat, muss weiteren Akteuren bekannt und bewusst gemacht werden (Nahestehende, breitere Öffentlichkeit, Straffprozess). Dies kann freiwillig passieren, kann jedoch auch unfreiwillig oder unbewusst stattfinden, ist jedoch immer ein Bericht zum eigenen Zustand	Die Tat, die das Unternehmen zum Opfer von Cybercrime gemacht hat, muss weiteren Akteuren bekannt und bewusst gemacht werden (Unternehmenspartner, breitere Öffentlichkeit, Strafprozess). Dies kann freiwillig, unfreiwillig oder unbewusst passieren. Durch die digitale Vernetzung mit direkten Partnern kann das Unternehmen selbst gleichzeitig Opfer und „Mittäter“ werden. Durch den erreichten Zugang zum Unternehmen kann der Angreifer seine Tat auch auf direkte Partner ausbreiten

Unternehmen haben in diesem Sinne keine Psyche, ein Cybercrime-Akt könnte jedoch in diesem extremsten Fall Unternehmen dazu veranlassen, sich selbst handlungsunfähig zu machen.

Zuerst werden, wie bereits oben beschrieben, wichtige Prozesse und Systemgrößen intern infrage gestellt. Dies wird durch Einflüsse über die Systemgrenze

Tab. 3 Tertiäre Viktimisierung

Beschreibung der Stufe	Bedingungen für den Auftritt	
	Mensch	Unternehmen
Mögliche dritte Stufe der Viktimisierung, bei welcher Betroffene als Folge vielfacher Viktimisierungserfahrungen (primärer und sekundärer Art) eine Opferidentität bilden	Die Tatfolgen hinterlassen einen bleibenden Eindruck und verschieben die gesamte Selbstwahrnehmung des Individuums zu einem Bild als permanentes reales oder potenzielles Opfer („Selbst-viktimisierung“ nach Kiefl und Lamnek 1986, S. 273) ohne eigene Handlungsmacht (erlernte Hilflosigkeit)	Das Unternehmen war im Vorfeld der Tat oder aber danach nicht in der Lage, seine Systemelemente entsprechend anzupassen, sodass die Auswirkungen nicht verarbeitet und organisational eingeordnet werden konnten

hinaus (z. B. Beziehungen zu Kunden und Partnern) verstärkt. Des Weiteren lässt die durch den kriminellen Akt bewiesene Unvollkommenheit und Angreifbarkeit des eigenen Systems unter Umständen die Zwecke, die Entscheidungswege sowie die Mitgliedschaftsregeln ebenso angreifbar und unvollkommen erscheinen. Insbesondere wenn Mitglieder selbst verantwortlich für den Akt waren, wären alle Elemente im Unternehmenssystem zu überprüfen, was zu einer Blockade bzw. einem Stillstand führen kann. Gleichzeitig kann eine fehlende Anpassungsbewegung durch neue Angriffe das System ebenfalls grundlegend lähmen (vgl. Tab. 3).

5 Fazit

Am Anfang dieses Kapitels wurde die Wichtigkeit einer Übersetzung der bereits etablierten Viktimologieansätze vom Menschen auf Organisationen als Opfer verdeutlicht. Die Aktualität dieser Aufgabe ist insbesondere durch die steigende Kriminalität im digitalen Raum gegeben. In diesem Kontext wird die digitale Opferwerdung von Unternehmen zurzeit meistens ohne den Rückgriff auf viktimologische Ansätze analysiert, während sich viktimologische Betrachtungen digitaler Phänomene hingegen vorrangig auf spezifisch Individuen betreffende Delikte beziehen.

Um mögliche Parallelen für die Analyse von Mensch und Organisation aufzudecken und als Rahmenbedingungen für die Konzeptübertragung zu nutzen, wurde die Systemtheorie als geeignet in Betracht gezogen. Dies erscheint aus folgenden Gründen produktiv: Beim Menschen als psychisches System und bei Organisationen als soziale Systeme handelt es sich bei einem kriminellen Delikt um einen Angriff von Außen, welcher beide Systeme (negativ) beeinflusst und zur Anpassung und Veränderung veranlasst. Sowohl der Akt der Opferwerdung als auch die nachfolgende Anpassung werden mit der Systemtheorie auf Interaktionsebene als Kommunikationen analysiert. Dies ermöglicht die analoge Betrachtung von Kommunikationsprozessen auf der Ebene der Organisationen als soziale Systeme. Auf dieser Grundlage können viktimologische Ansätze neu strukturiert und für eine mehrstufige Betrachtung und Analyse von Kommunikationsströmen oder Merkmalen einer Organisation als System angewendet werden. Diese kann unserer Meinung nach ebenso risiko-prognostische Charakteristika wie Präventionsmöglichkeiten offenbaren. Der Beitrag baut damit einen ersten Rahmen für weiterführende Arbeiten, bei welchen z. B. ein Modell entwickelt werden kann, welches die Übertragung der Ansätze detailliert strukturiert, alle Systemelemente direkt adressiert, eine Auflistung der Erkennungsmerkmale für systeminterne

Veränderungen beinhaltet und für die Generierung von Handlungsanweisungen genutzt werden kann. Denkbar wäre es auch, den Fokus auf die Regelungen zur Mitgliedschaft und ihre Veränderungen auf allen drei Stufen des Karrieremodells zu legen, sowie auf die Auswirkungen eines Angriffs und die Folgen für die Zwecke der Organisation und für die Kommunikationsprozesse zwischen den Mitgliedern. Weiterhin ist es möglich, die Grenzen der Organisation als System und ihre Beziehungen zu und Irritationen der Umwelt (ähnlich der skizzierten sekundären Viktimisierung) neu zu stellen und zu beleuchten. Auch Fragen der kritischen Viktimologie (wie z. B. die Definitionsmacht) können mit diesen Elementen und den Stufen der Kommunikation als Hauptprozess eines Systems neu gefasst werden.

Der skizzierte Ansatz erweist sich unseres Erachtens nach als produktiv für eine weiterführende Betrachtung, welche, neben den Folgen von Cybercrime, auch andere Aspekte berücksichtigt. Eine geeignete Grundlage hierzu können weiterführende theoretische wie auch anwendungsorientierte Arbeiten liefern. Dies würde Unternehmen auch über den Bereich der Cyberkriminalität hinaus eine neue Bedeutung in der Kriminologie ermöglichen, indem ebenso Übertragungen von Modellen aus dem Unternehmensbereich auf die analoge, individuelle Opferwelt denkbar werden.

Insbesondere im anvisierten Kontext der Digitalisierung ist es relevant und notwendig, die kommunikationstheoretischen Überlegungen von Luhmann kritisch zu diskutieren und die Rolle neuer technischen Vermittler in Interaktionen anzuerkennen.

Literatur

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies, 23*(3), 1177–1206. https://doi.org/10.1007/s11142-018-9452-4.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Eeten, M. J. G. van, & Levi, M., et al. (2013). Measuring the cost of cybercrime. In R. Böhme (Hrsg.), *The economics of information security and privacy* (S. 265–300). Berlin: Springer. https://doi.org/10.1007/978-3-642-39498-0_12.

Bartsch, M., Gentemann, L., Kob, T., Krösmann, C., Mille, M., & Petri, A., et al. (2018). *Spionage, Sabotage, und Datendiebstahl. Wirtschaftsschutz in der Industrier*. Berlin: Bundesverband Industiewirtschaft, Telekommunikation und neue Medien e. V.

Berghaus, M. (2011). *Luhmann leicht gemacht*. Stuttgart: UTB GmbH.

Böhme, R., & Moore, T. (2012). How do consumers react to cybercrime? In *Proceedings of the 7th APWG eCrime Researchers Summit (eCrime)*. https://doi.org/10.1109/ecrime.2012.6489519.

Bossler, A. M., & Holt, T. J. (2011). Malware victimization a routine activities framework. In K. Jaishankar (Hrsg.), *Cyber criminology: Exploring internet crimes and criminal behavior* (S. 317–344). Boca Racon, USA: CRC Press. https://doi.org/10.1201/b10718.

Braithwaite, J., & Fisse, B. (2017). On the plausibility of corporate crime theory. In W. S. Laufer & F. Adler (Hrsg.), *Advances in criminological theory* (Bd. 2, S. 15–38).

BSI. (2016). *Die Lage der IT-Sicherheit in Deutschland 2016* (S. 68). Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI).

BSI. (2018). *Die Lage der IT-Sicherheit in Deutschland 2018* (S. 100). Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI).

Bussmann, K.-D. (2015). Organisationen als Opfer. In N. Guzy, R. Mischkowitz & C. Birkel (Hrsg.), *Viktimisierungsbefragungen in Deutschland – Band 1 – Ziele, Nutzen und Forschungsstand* (Bd. 1, S. 363–392). Bundeskriminalamt.

Cavelty, M. D. (2013). Gesellschaft im Daueralarm. Gefahrendarstellungen im Cybersecurity- Diskurs. In C. Daase, S. Engert & J. Junk (Hrsg.), *Verunsicherte Gesellschaft – überforderter Staat: Zum Wandel der Sicherheitskultur* (S. 19). Frankfurt a. M.: Campus.

Cavelty, M. D. (2015). "Cyber-security and private actors", in: Anna Leander and Rita Abrahamsen (eds), Routledge handbook of private security studies (Routledge, 2015), S. 89–99. In A. Leander & R. Abrahamsen (Hrsg.), *Handbook of private security studies* (S. 89–99). Routledge.

Choi, K. (2011). Cyber-routine activities empirical examination of online lifestyle, digital guardians, and computer-crime victimization. In K. Jaishankar (Hrsg.), *Cyber criminology: Exploring internet crimes and criminal behavior* (S. 229–252). Boca Racon, USA: CRC Press. https://doi.org/10.1201/b10718.

Christie, N. (1986). The ideal victim. In E. A. Fattah (Hrsg.), *From crime policy to victim policy: Reorienting the justice system* (S. 17–30). London: Palgrave Macmillan. https://doi.org/10.1007/978-1-349-08305-3_2.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608. https://doi.org/10.2307/2094589.

Condry, R. (2010). Secondary victims and secondary victimization. In P. Knepper, M. Kett & S. G. Shoham (Hrsg.), *International handbook of victimology* (S. 219–250). CRC Press.

Cressey, D. R., Adler, F., & Laufer, W. S. (2017). The poverty of theory in coporate crime. In W. S. Laufer & F. Adler (Hrsg.), *Advances in criminological theory* (Bd. 1, S. 31–56). New York: Transaction Publishers.

Davies, P., Francis, P., & Greer, C. (2017). *Victims, crime and society: An introduction*. London, Thousand Oaks, New Delhi, Singapore: SAGE.

D'Elia, D. (2016). The economics of cybersecurity: From the public good to the revenge of the industry. In A. Bécue, N. Cuppens-Boulahia, F. Cuppens, S. Katsikas & C. Lambrinoudakis (Hrsg.), *Security of industrial control systems and cyber physical systems* (S. 3–15). Springer International Publishing.

Detica. (2011). *The cost of cyber crime: A Detica report in partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office*. Guilford: Detica.

Donalds, C., & Osei-Bryson, K.-M. (2014). A cybercrime taxonomy: Case of the Jamaican jurisdiction. In *CONF- IRM 2014 proceedings* (S. 13). http://aisel.aisnet.org/confirm2014/5.

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance, 17*(5), 474–491. https://doi.org/10.1108/jrf-09-2016-0122.

EU Commission. (2007). Communication from the comission to the European parliament, the council and the commitee of the regions, towards a general policy on the fight against cybercrime (No. COM (2007) 267 final). Brüssel. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF.

Fafinski, S. (2009). Computer misuse: Response, regulation and the law. Taylor & Francis.

Fafinski, S., Dutton, W. H., & Margetts, H. Z. (2010). Mapping and measuring cybercrime (SSRN Scholarly Paper No. ID 1694107). Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=1694107. Zugegriffen: 30. Juli 2018.

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems, 86,* 13–23. https://doi.org/10.1016/j.dss.2016.02.012.

Gao, X., Zhong, W., & Mei, S. (2015). Security investment and information sharing under an alternative security breach probability function. *Information Systems Frontiers, 17*(2), 423–438. https://doi.org/10.1007/s10796-013-9411-3.

Grabosky, P. N. (2001). Virtual criminality: old wine in new bottles? *Social & Legal Studies, 10*(2), 243–249. https://doi.org/10.1177/a017405.

Graham, R. (2018). How cybersecurity and cybercrime are like wall street and main street. http://www.academia.edu/34589703/How_Cybersecurity_and_Cybercrime_are_Like_Wall_Street_and_Main_Street. Zugegriffen: 25. Juli 2018.

Hald, S. L. N., & Pedersen, J. M. (2012). An updated taxonomy for characterizing hackers according to their threat properties. In *2012 14th international conference on advanced communication technology (ICACT)* (S. 81–86). Gehalten auf der 2012 14th International Conference on Advanced Communication Technology (ICACT).

Haupt, H. (2003). *Handbuch Opferschutz und Opferhilfe* (2. Aufl.). Baden-Baden: Nomos Verlagsgesellschaft.

Hausken, K. (2006). Income, interdependence, and substitution effects affecting incentives for security investment. *Journal of Accounting and Public Policy, 25*(6), 629–665. https://doi.org/10.1016/j.jaccpubpol.2006.09.001.

Hempel, L. (2017). Verantwortungspolitiken im Kontext von IT-Sicherheit: Verantwortungszuschreibung als Kontingenzverschiebung. In *Politik und Verantwortung* (S. 454–476). Nomos Verlagsgesellschaft mbH & Co. KG.

Hentig, H. (1967). *The criminal and his victim: Studies in the sociobiology of crime* (1948., Repr. 1967 Aufl.). Hamden: Archon Books.

Hopkins, M. (2016a). The crime drop and the changing face of commercial victimization: Reflections on the commercial crime drop in the UK and the implications for future research. *Criminology and Criminal Justice, 16,* 410–430. https://doi.org/10.1177/1748895816628930.

Hopkins, M. (2016b). Business, victimisation and victimology: Reflections on contemporary patterns of commercial victimisation and the concept of businesses as ‚ideal victims‘. *International Review of Victimology, 22*(2), 161–178. https://doi.org/10.1177/0269758016628948.

Huber, E. (2015). Cybercrime gegen Privatpersonen. In N. Guzy, R. Mischkowitz & C. Birkel (Hrsg.), *Viktimisierungsbefragungen in Deutschland – Band 1 – Ziele, Nutzen und Forschungsstand* (Bd. 1, S. 393–420). Bundeskriminalamt.

Huber, E., & Pospisil, B. (2018). *Die Cyber-Kriminellen in Wien: Eine Analyse von 2006–2016*. Krems: Edition-Donau-Univ.

Jenner, L. (2018). Backdoor: How a metaphor turns into a weapon. Institut für Internet und Gesellschaft, Alexander von Humboldt. https://doi.org/10.5281/zenodo.1172718.

Karmen, A. (2012). *Crime victims: An introduction to victimology*. Cengage Learning.

van Kesteren, J., van Dijk, J., & Mayhew, P. (2014). The international crime victims surveys: A retrospective. *International Review of Victimology, 20*(1), 49–69. https://doi.org/10.1177/0269758013511742.

KFN, e. V. (2018). Cyberangriffe gegen Unternehmen. https://kfn.de/forschungsprojekte/cyberangriffe-gegen-unternehmen/. Zugegriffen: 21. Dez. 2018.

Kiefl, W., & Lamnek, S. (1986). *Soziologie des Opfers: Theorie, Methoden und Empirie der Viktimologie*. München: Fink.

Kirchhoff, G. F. (2010). History and a theoretical structure of victimology. In *International handbook of victimology* (S. 95–125). https://doi.org/10.1201/ebk1420085471-10.

Klahr, D. R., Shah, J. N., Sheriffs, P., Rossington, T., & Pestell, G. (2017). *Cyber security breaches survey 2017* (S. 66). Portsmouth: Department for Culture, Media and Sport.

Klipper, S. (2015). Was ist cyber security? In S. Klipper (Hrsg.), *Cyber Security: Ein Einblick für Wirtschaftswissenschaftler* (S. 9–27). Wiesbaden: Springer Fachmedien. https://doi.org/10.1007/978-3-658-11577-7_2.

Kneer, G., Massehi, A., & Luhmann, N. (1993). *Niklas Luhmanns Theorie*. München: Fink.

Knudten, R. D. (1988). The scope ofvictimology and victimization: Towards a reconceptualization of the field. In: Gehalten auf der 6th International Symposium of Victimology, Jerusalem, Israel.

Kopp, E., Kaffenberger, L., & Jenkinson, N. (2017). Cyber risk, market failures, and financial stability (No. 17/185). International Monetary Fund.

Krause, D. (2001). *Luhmann-Lexikon* (3. Aufl.). Stuttgart: Lucius & Lucius Verlagsgesellschaft GmbH.

Kshetri, N. (2013). Cyber-victimization and cybersecurity in China. *Communications of the ACM, 56*(4), 35. https://doi.org/10.1145/2436256.2436267.

Kühl, S. (2011). *Organisationen*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Landau, S. F., & Freeman-Longo, R. E. (1990). Classifying victims: A proposed multidimensional victimological typology. *International Review of Victimology, 1*(3), 267–286. https://doi.org/10.1177/026975809000100304.

Lebe, W. (2003). *Viktimologie – die Lehre vom Opfer. Entwicklung in Detschland. (No. 12)* (S. 8–19). Berlin: Landeskommission Berlin gegen Gewalt.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409.

Lorkowski, S. (2015). Kommunikation der IT-Sicherheitslage: Ein Index der Cyber-Sicherheit für den deutschsprachigen Raum (Position Paper), 15.

Luhmann, N. (1973). *Zweckbegriff und Systemrationalität*. Frankfurt a. M.: Suhrkamp.

Luhmann, N. (1975). *Soziologische Aufklärung 2*. Opladen: Westdeutscher.

Luhmann, N. (1981). *Organisation im Wirtschaftssystem*. Opladen: Westdeutscher.

Luhmann, N. (1984). *Soziale Systeme: Grundriss einer allgemeinen Theorie*. Frankfurt a. M.: Suhrkamp.

Luhmann, N. (1987). *Soziologische Aufklärung 4*. Opladen: Westdeutscher.

Luhmann, N. (1999). *Funktionen und Folgen formaler Organisation* (Bd. 9. Aufl). Berlin: Duncker & Humblot.

Luhmann, N. (2000). *Organisation und Entscheidung*. Opladen: Westdeutscher.

Mawby, R. I., & Walklate, S. (1994). *Critical victimology: International perspectives*. SAGE.

McGuire, M., & Dowling, S. (2013). Chapter 1: Cyber-dependent crimes. In *Cyber crime: A review of the evidence* (Bd. 75, S. 35). Home Office.

Metzner, C. (2018). Sekundäre Viktimisierung bei sexualisierter Gewalt.Strukturdynamiken und Präventionsansätze (Inauguraldissertation). Johann Wolfgang Goethe-Universität, Frankfurt a. M. Abgerufen von http://publikationen.ub.uni-frankfurt.de/frontdoor/index/index/docId/46814.

Miers, D. (1990). Positivist victimology: A critique part 2: Critical victimology. *International Review of Victimology, 1*(3), 219–230. https://doi.org/10.1177/026975809000100301.

Miers, D. (2007). Looking beyond Great Britain: The development of criminal injuries compensation. *Handbook of Victims and Victimology*, 337–379.

Mikhed, V., & Vogan, M. (2018). How data breaches affect consumer credit. *Journal of Banking & Finance, 88,* 192–207. https://doi.org/10.1016/j.jbankfin.2017.12.002.

Müller, K.-R. (2015). *Handbuch Unternehmenssicherheit: umfassendes Sicherheits-, Kontinuitäts- und Risikomanagement mit System* (3., aktualisierte u. erweiterte Aufl.). Wiesbaden: Springer Vieweg.

Ngo, F., & Jaishankar, K. (2017). Special article: Commemorating a decade in existence of the international journal of cyber criminology: A research agenda to advance the scholarship on cyber crime. *International Journal of cyber criminology*. https://doi.org/10.5281/zenodo.495762.

Noack, M. (2015). *Methodische Probleme bei der Messung von Kriminalitätsfurcht und Viktimisierungserfahrungen*. Wiesbaden: Springer VS.

Nykodym, N., Taylor, R., & Vilela, J. (2005). Criminal profiling and insider cyber crime. *Computer Law & Security Review, 21*(5), 408–414. https://doi.org/10.1016/j.clsr.2005.07.001.

Oberwittler, D., & Kury, H. (2015). Wissenschaftliche Perspektive. In N. Guzy, C. Birkel, & R. Mischkowitz (Hrsg.), *Viktimisierungsbefragungen in Deutschland – Band 1 – Ziele, Nutzen und Forschungsstand* (Bd. 1, S. 107–131). Wiesbaden: Bundeskriminalamt.

O'Connell, M. (2008). Victimology: A social science in waiting? *International Review of Victimology, 15*(2), 91–104. https://doi.org/10.1177/026975800801500202.

Paoli, L., Visschers, J., & Verstraete, C. (2018a). The impact of cybercrime on businesses: a novel conceptual framework and its application to Belgium. *Crime, Law and Social Change, 70*(4), 397–420. https://doi.org/10.1007/s10611-018-9774-y.

Paoli, L., Visschers, J., Verstraete, C., & van Hellemont, E. (2018b). The impact of cybercrime on Belgian businesses. BBC Project Report. https://bcc-project.be/surveys/wp4-2-the-impact-of-cybercrime-on-belgian.pdf.

Pattabiraman, A., Srinivasan, S., Swaminathan, K., & Gupta, M. (2018). Fortifying corporate human wall: A literature review of security awareness and training. In *Information technology risk management and compliance in modern organizations* (S. 142–175). https://doi.org/10.4018/978-1-5225-2604-9.ch006.

Peters, G., Shevchenko, P. V., & Cohen, R. (2018). Understanding cyber-risk and cyber-insurance (SSRN Scholarly Paper No. ID 3200166). Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=3200166. Zugegriffen: 27. Febr. 2019.

Pfefferkorn, R. (2018). *Security risks of government hacking* (S. 1–16). Stanford: The Center of Internet Society, Stanford Law School. http://cyberlaw.stanford.edu/files/publication/files/2018.09.04_Security_Risks_of_Government_Hacking_Whitepaper.pdf. Zugegriffen: 15. Aug. 2019.

Powell, A., Stratton, G., & Cameron, R. (2018). Digital criminology: Crime and justice in digital society. *Routledge*. https://doi.org/10.4324/9781315205786.

Reep-van den Bergh, C. M. M., & Junger, M. (2018). Victims of cybercrime in Europe: A review of victim surveys. *Crime Science*, 7(1). https://doi.org/10.1186/s40163-018-0079-3.

Rosati, P., Deeney, P., Cummins, M., van der Werff, L., & Lynn, T. (2019). Social media and stock price reaction to data breach announcements: Evidence from US listed companies. *Research in International Business and Finance, 47,* 458–469. https://doi.org/10.1016/j.ribaf.2018.09.007.

Safa, N. S. (2017). The information security landscape in the supply chain. *Computer Fraud & Security, 2017*(6), 16–20. https://doi.org/10.1016/s1361-3723(17)30053-2.

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior, 57,* 442–451. https://doi.org/10.1016/j.chb.2015.12.037.

Schneider, H. J. (2007). Die deutschsprachige Kriminologie der Gegenwart. In K. Liebl (Hrsg.), *Kriminologie im 21. Jahrhundert* (S. 145–174). Springer.

Schulze, M. (2016). (Un)Sicherheit hinter dem Bildschirm: Die Versicherheitlichung des Internets. In S. Fischer & C. Masala (Hrsg.), *Innere Sicherheit nach 9/11: Sicherheitsbedrohungen und (immer) neue Sicherheitsmaßnahmen?* (S. 165–185). Wiesbaden: Springer Fachmedien. https://doi.org/10.1007/978-3-658-02638-7_9.

Schwind, H.-D. (2013). *Kriminologie*. Heidelberg: C. F. Müller GmbH.

Sellin, T., & Wolfgang, M. E. (1964). *The measurement of delinquency*. New York: Wiley.

Shury, J., Speed, M., Vivian, D., Kuechel, A., & Nicholas S. (2005). Crime against retail and manufacturing premises: Findings from the 2002 Commercial Victimisation Survey (Online Report No. 37/05). UK: Home Office. https://sp.ukdataservice.ac.uk/doc/7143/mrdoc/pdf/7143_rdsolr3705.pdf. Zugegriffen: 15. Aug. 2019.

Skibell, R. (2002). The myth of the computer hacker. *Information, Communication & Society, 5*(3), 336–356. https://doi.org/10.1080/13691180210159292a.

Smith, M., & Green, M. (2017). *A discussion of surveillance backdoors:effectiveness, collateral damage and ethics* (S. 131–142). University of Bonn, Fraunhofer FKIE – Johns Hopkins University.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009.

Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security, 58,* 216–229. https://doi.org/10.1016/j.cose.2015.12.006.

Srinidhi, B., Yan, J., & Tayi, G. K. (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. *Decision Support Systems, 75,* 49–62. https://doi.org/10.1016/j.dss.2015.04.011.

Steinmann, C. (2018). IT-Sicherheit in Unternehmen – State of the Art, Gefahren und Trends. Informatics Inside gehalten auf der connect(IT), Reutlingen. http://www.hhz.de/fileadmin/user_upload/Fakultaet_INF/Bilder/Aktuelles/News/2018/010_Informatics_Inside/Tagungsband_InformaticsInside2018_digital_final_inhalt.pdf#page=57. Zugegriffen: 20. Juli 2018.

Swire, P. (2018). A pedagogic cybersecurity framework. *Communications of the ACM, 61*(10), 23–26. https://doi.org/10.1145/3267354.

Syed, R. (2018). Enterprise reputation threats on social media: A case of data breach framing. *The Journal of Strategic Information Systems*. https://doi.org/10.1016/j.jsis.2018.12.001.

Tøndel, I. A., Seehusen, F., Gjære, E. A., & Moe, M. E. G. (2016). Differentiating cyber risk of insurance customers: The insurance company perspective. In F. Buccafurri, A. Holzinger, P. Kieseberg, A. M. Tjoa & E. Weippl (Hrsg.), *Availability, reliability, and security in information systems* (S. 175–190). Springer International Publishing.

Turvey, B. E., & Ferguson, C. (2013). Victimology: A brief history with an introduction to forensic victimology. In B. E. Turvey (Hrsg.), *Forensic victimology: Examining violent crime victims in investigative and legal contexts*. Academic Press.

van de Weijer, S. G. A., & Leukfeldt, E. R. (2017). Big five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking, 20*(7), 407–412. https://doi.org/10.1089/cyber.2017.0028.

Voss, H. L., & Hepburn, J. R. (1968). Patterns of criminal homicide in Chicago (S. 267–286).

Walklate, S. (2008). Researching victims. In R. King & E. Wincup (Hrsg.), *Doing research on crime and justice* (S. 315–340). Oxford: OUP Oxford.

Walklate, S. (2012). Who is the victim of crime? Paying homage to the work of Richard Quinney. *Crime, Media, Culture: An International Journal, 8*(2), 173–184. https://doi.org/10.1177/1741659012444433.

Wall, D. (2007). Cybercrime: The transformation of crime in the information age. *Polity*.

Weik, E., & Lang, R. (2003). *Moderne Organisationstheorien*. Wiesbaden: Gabler.

Weis, K., & Borges, S. S. (1973). Victimology and rape: The case of the legitimate victim. In *Issues Criminology, 8*(2), 71–115.

Williams, M. L., Levi, M., Burnap, P., & Gundur, R. V. (2018). Under the corporate radar: Examining insider business cybercrime victimization through an application of routine activities theory. *Deviant Behavior*. https://doi.org/10.1080/01639625.2018.1461786.

Wilson, J. K. (Hrsg.). (2009). *The Praeger handbook of victimology*. Santa Barbara: Praeger.

Wrede, D., Freers, T., & Graf von der Schulenburg, J.-M. (2018). Herausforderungen und Implikationen für das Cyber-Risikomanagement sowie die Versicherung von Cyberrisiken – Eine empirische Analyse. *Zeitschrift für die gesamte Versicherungswissenschaft, 107*(4), 405–434. https://doi.org/10.1007/s12297-018-0425-2.

Yar, M. (2013). *Cybercrime and society*. SAGE.

Posterboys und Terrorpropaganda

Cybergrooming als terroristische Taktik zur Rekrutierung von (Ehe)Frauen für IS

Astrid Bötticher

This article deals with the phenomenon of terrorist recruiting under the perspective of cybergrooming. Instead of seeing terrorist recruiting as action of talent seeking, this article understands it as a form of grooming. The switch of perspective allows to analyse the recruitment process not as a professionalised Action, but as action of ideology driven predators that seek to groom in order to talk victims into entering a system of misuse. As consequence, this article combines the theory of Extremism and its methods for analysis with the criminal perspective of Cybergrooming.

Dieser Artikel beschäftigt sich mit dem Phänomen der terroristischen Rekrutierung unter der Perspektive des sog. Cybergrooming. Anstatt die Rekrutierung von Terroristen als eine Aktion der Nachwuchsgewinnung zu sehen, versteht dieser Artikel sie daher als eine Form des Groomings. Dieser Perspektivwechsel ermöglicht es, den Rekrutierungsprozess nicht als eine professionalisierte Handlungsweise zu analysieren, sondern als Handlungen ideologiegetriebener Predatoren, die wiederum versuchen, ihre Opfer durch einen Vertrauensaufbau im Rahmen eines Grooming-Prozesses in ein Missbrauchssystem einzubinden. Folglich kombiniert dieser Artikel die Theorie des Extremismus und seiner Analysemethoden mit einer kriminologischen Betrachtung und Perspektive des Phänomens Cybergrooming.

A. Bötticher (✉)
Fachbereich 5, Institut für Politikwissenschaft, Hochschule für Wirtschaft und Recht, Berlin, Deutschland
E-Mail: astridboetticher@web.de

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

T.-G. Rüdiger und P. S. Bayerl (Hrsg.), *Cyberkriminologie,*
https://doi.org/10.1007/978-3-658-28507-4_15

1 Einleitung

Mit dem Begriff „Cybergrooming“ wird normalerweise die gezielte Ansprache von meist minderjährigen Personen im Internet zum Zweck der Anbahnung übergriffiger sexueller Kontakte bezeichnet. Die Terrorgruppe IS (Islamischer Staat) hat eine sehr spezielle Form der Propaganda in Kombination mit persönlicher Ansprache junger Frauen und Mädchen entwickelt, die in Kriegs- und Krisengebiete zwecks Verheiratung gelockt werden sollen. Während andere islamistische Terrorgruppen, wie die in Afghanistan tätige Gruppe „Islamische Bewegung Usbekistan“ und deren Ableger „Islamische Djihad Union“ – und insbesondere ihr deutsches Gesicht Erik Breiniger – bereits vor mehr als zehn Jahren „unverheiratete Frauen“ aufforderten sich auf den Weg zum Hindukusch zu machen, so hat IS die Kombination aus terroristischer Propaganda und gezielter Ansprache von jungen Frauen und Mädchen perfektioniert und eine eigene Grooming-Systematik entwickelt, die bei propagandaempfänglichen Mädchen den Wunsch nach einer Djihad-Ehe auslöst (Flade 2014).

Sind die jungen Frauen oder Mädchen erst ausgereist, werden oft ihre Netzwerke aufgegriffen und die „Daheimgebliebenen“ werden von den weiblichen Djihadis zur Ausreise aufgefordert. Dabei wäre es blauäugig anzunehmen, dass es lediglich um eine Heirat der oft verniedlichend bezeichneten „Djihad-Bräute“ (Martini 2018) geht – denn sie unterstützen vor Ort oft Logistik oder andere organisatorische Aufgaben und nehmen eine wichtige Rolle in der Terrorpropaganda ein. Sie kämpfen aber auch oder sind Teil der Religionspolizei, einem wichtigen Element des Islamischen Staates, um die Bevölkerung vor Ort zu terrorisieren (Ramsauer 2017).

Der vorliegende Beitrag beschäftigt sich mit dem Begriff des Cybergroomings (s. a. Kap. „Grooming-Umgebungen von pädophilen und hebephilen Männern in Deutschland“), sowie seiner Anwendbarkeit auf Phänomene des Terrorismus. Weiterhin wird die gezielte Ansprache von jungen Mädchen und Frauen in ihrer Systematik dargestellt und im Rahmen des Cybergroomings analysiert. Das Cybergrooming wird als Werkzeug des terroristischen Extremismus eingeordnet und in seinen Bezügen dargestellt.

2 Extremistisches Cybergrooming – eine Begriffsbestimmung

Es ist nicht leicht, eine Sprache zu finden, die sich auf den Extremismus bezieht und gleichzeitig auf eine Form des sexuellen Missbrauchs hinweist. Oft ist es so, dass Phänomene wie weiblicher Terrorismus verniedlichend beschrieben

werden. Dann ist etwa von „Djihad-Bräuten“ die Rede oder Frauen werden zu „Mädchen“ (Speckhard 2015). Die Gewalt, die von diesen Frauen ausgeht, ihre Unterstützung von Kriegsverbrechen, wird teilweise auch in den Medien ausgeblendet. Die Kriegsverbrechen, die von irregulären Truppen, wie der von Frauen gestellten al-Khansâ'-Brigade von IS, finden oft kaum Erwähnung (Mendick und Verkaik 2014).

Der vorliegende Beitrag bezieht sich auf ein Phänomen, in dem jugendliche Frauen zunächst eine Rolle als Opfer spielen. Selbstverständlich hindert dies nicht, diese jungen Frauen (in Anlehnung an den Radikalisierungsverlauf) auch als Täterinnen zu verstehen. IS propagiert dennoch ein Frauenbild, in dem die Traditionelle Aufteilung von Haus und Markt wieder auflebt. Der Frau braucht nichts zu wissen, sie soll dem Mann untergeordnet leben, in ständiger Abhängigkeit und möglichst nicht hinaus gehen (Mohagheghi 2015).

Diese Frauen sind für ihre Taten verantwortlich. Wenngleich sie aus ihren Kinderzimmern gelockt wurden und anstelle von Boybands die Abbilder djihadistischer Posterboys an ihren Wänden hingen, sie von djihadistischen Cybergroomern angesprochen und ideologisiert wurden, haben sie sich dazu entschieden, in Kriegsgebiete zu reisen und von dort aus eine terroristische Organisation zu unterstützen, die weltweit für ihre schweren und systematisch verübten Kriegsverbrechen bekannt wurde. Sie sind nicht mehr einfach irgendwelche „Mädchen“ – das sind Extremistinnen in der Regel nicht. Es handelt sich um Befürworterinnen von politisch(-religiösen) Regimen, die im Kern menschenfeindlich sind. Terrorismus ist, ähnlich wie Populismus, lediglich eine Strategie von ExtremistInnen.

Was genau damit gemeint ist, wenn von ExtremistInnen die Rede ist, lässt sich anhand des Extremismusbegriffs ausloten.

2.1 Der Extremismus – eine Konsensdefinition

Vom Extremismus gehen symmetrische wie asymmetrische Bedrohungslagen aus, die äußerst umfassend bis hin zum Existenziellen reichen können. Viele politikwissenschaftliche Definitionen beschreiben den Extremismus als fundamental antidemokratisch und gegen die Volkssouveränität gerichtet. Es handele sich um politische Kräfte, die eine Diktatur errichten wollen, in der eine Interessenidentität zwischen Regierenden und Regierten herrschen soll. Der Extremismus konkretisiert sich auf der Wertachse als links-extreme, rechts-extreme oder religiös-extreme Position und ist eine anti-pluralistische und monistische Erscheinung, die Differenz und Abweichung bekämpft. In einer

dialogorientierten Sicht ist der Extremismus das Gegenteil des Dialogs. Es ist mithin eine indoktrinäre, gewaltverherrlichende Ideologie, die sich als Eindeutigkeitsangebot gegen die werteplurale und durch Ambiguität ausgezeichnete demokratische Sozialisation richtet, die Selbstbestimmung und die freie Wahl diverser Lebensentwürfe befürwortet. Der Extremismus stellt als Eindeutigkeitsangebot ein schwarz/weiß Bewertungsschema (z. B. haram-halal-Diskurs) zur Verfügung, dass die Begründung für die Ablehnung von Ambiguität, Pluralität und Diversität liefert und alleinige Deutungskompetenz beansprucht.

Die Rechtswissenschaft und die Kriminologie behandeln den Extremismus als Teil der politisch motivierten Kriminalität. Zum Extremismus gehört immer das Ziel, das System zu überwältigen, aber im Gegensatz zum Radikalismus ist der Extremismus sowohl in Ziel und Mitteln extrem. Es handelt sich um eine vorsätzliche, ernsthafte und nachhaltige Strategie zur Beseitigung oder Einschränkung grundlegender Werte und Strukturprinzipien des Grundgesetzes mit gewaltsamen Mitteln. Der Extremismus verhält sich aggressiv-kämpferisch und ist durch Ideologie geprägt, wobei der Extremist vor allem an die eigene Höherwertigkeit glaubt und sich in Motivation, Tat und Mittel von den gesetzlich verankerten demokratischen Verhaltensnormen abweicht. Der Extremismus liefert die Begründung für Hassverbrechen. Politisch-ökonomisch lässt sich der Extremismus als Spielstrategie verstehen, die sich durch besonderen Eifer und Verhaltenspolarität auszeichnet und Gewalt als Teil der erlaubten Macht-Strategie begreift. Es handelt sich um anti-individualistische Spieler, die nach innen auf Konformität bestehen, sodass eine hohe Kohärenz in den Spielzügen der Spielergemeinschaft durch Zwang hergestellt ist. Soziologisch gesehen, handelt es sich beim Extremismus um eine durch Eindimensionalität und geistige Starrheit ausgezeichneten menschlichen Zusammenschluss, der sich innerhalb der Gesellschaft bildet, aber vom demokratischen Mainstream abhebt und Gewalt als Handlungsstrategie bewusst ins Auge fasst. Ziel ist es, eine homogene Gemeinschaft nach den Standards der ausgerufenen Dogmen (auch mittels Gewalt) zu erschaffen und (mittels Zwang) dauerhaft zu erhalten. Damit wendet sich der Extremismus gegen jede Form der Diversität und gegen die offene Gesellschaft. Zwang und Intoleranz sind die Durchsetzungsstrategien; inhaltlich normiert ist der Extremismus durch eine Partikularmoral. Der kollektiven Homogenitätsvorstellung wird der Vorzug vor dem Individuum gegeben (Bötticher 2017).

2.2 Der Terrorismus – eine extremistische Strategie

Der Terrorismus ist demgegenüber eine Strategie, die von extremistischen Gruppen verfolgt wird. Der hypermoderne Djihadismus hat dabei besondere Merkmale, die ihn zu einem sogenannten „wicked problem“ machen, denn er ist ein Teil der Globalisierung. Der Terrorismus gilt als Ausdruck kontingenter Unsicherheit, als quasi unlösbares „wicked problem“. Im Zeitalter globaler Interdependenz hat sich der Terrorismus als „Verwaltungsproblem“ demnach weg von einem „tame problem“ hin zu einem „wicked-problem“ gewandelt. Der Terrorismus ist kein statisches Phänomen, sondern Ergebnis eines sozial tangierten und motivierten Verlaufs. Es handelt sich beim Terrorismus insbesondere um ein soziales Problem komplexer Natur. Neben der Wahrnehmung des Terrorismus als Aufgabenbereich des Politikfeldes der Inneren Sicherheit, wird das Phänomen zunehmend als Aufgabe des Sozialstaates wahrgenommen. Damit sind alternative Handlungsmöglichkeiten eröffnet worden und neue Problemlösungsstrategien, wie z. B. frühzeitige pädagogische Interventionen, werden eingesetzt.

Immer mehr rückt in den Fokus, wie stark die Cyberwelt den Terrorismus beeinflusst und wie stark diese Welt von ihm beeinflusst wird. Die Globalisierung ist durch technischen Fortschritt im Kommunikationsbereich, Liberalisierung der Märkte, neue und erstarkte Transporttechnologien und neue Beziehungsmuster gekennzeichnet und ist im Kern eine Verflechtung von Gesellschaften, Staaten, Individuen, Märkten und Kulturen. Die Globalisierung enthält durch ihre mannigfaltigen Verflechtungen ein Höchstmaß an Komplexität. Im Bereich der Politik hat die Globalisierung einen Wandel in der Problembewältigungsfähigkeit mit sich gebracht, indem sie vormals lösbare „tame problems“, mit einer klaren Aufgabendefinition, einer klaren Zielvorgabe und etablierten Lösungsmustern, zu unlösbaren „wicked problems“ transformierte. Heute überlagern und bedingen sich Probleme wechselseitig, sodass eine Benennung des Problems bereits nicht mehr eindeutig möglich ist. Auch die Frage, wer das Problem lösen soll, bleibt ungewiss. Unter diesen Umständen ist die Definition des Ziels in Form von administrativen Aufgaben und der klaren Angabe von Bearbeitungsprozessen kaum möglich. „Richtige“ und „falsche“ Maßnahmen können nicht abschließend und konkret benannt werden; auch ist das Resultat ungewiss, da Lösungen in anderen Gesellschafts- bzw. Politikbereichen neue Probleme aufwerfen können (Rittel und Webber 1973).

Der Islamismus, der von IS ausgeht, ist im Grunde globalisiert – so wie bereits AlQaida und andere terroristische Gruppen zuvor. Die Anschlagsorte reichen von Mali über Nigeria, USA, Frankreich, Spanien und England. Wenngleich durch

unterschiedliche, wenn auch zum Teil hochgradig vernetzte Gruppen durchgeführt, so handelt es sich der Wahrnehmung nach um terroristische Netzwerke mit gemeinsamer Prägung, deren Aktivitäten trotz Ferne als nationale sicherheitspolitische Gefahrenlagen verstanden werden und eine Reaktion der Politik erfordern. Der Anschlag von Christchurch 2019 führte zum Beispiel zum Anschlag am Ostersonntag auf Sri Lanka, so jedenfalls begründeten die Täter ihre Tat (Die ZEIT 2019). Die Logik von Anschlag zu Gegenanschlag ist eine wichtige Argumentationsschablone.

Insbesondere der islamistische Terrorismus wird als globale Bewegung wahrgenommen. Terroristische Ereignisse können unvorhergesehene Interdependenzen bis in unsere Gesellschaft zum Vorschein bringen. Die Beobachtung weit entfernt ausgetragener Konflikte mit Terrorgruppen ist dabei nicht nur zeitaufwendig und beansprucht für Politik und BOS hohe Kosten, sondern ist beinah unumgänglich, zumindest um den Anschein einer – wie auch immer gearteten – Sicherheitsleistung aufrecht zu erhalten (Junk und Offermann 2014). Der Islamische Staat (IS), Konfliktakteur im Syrienkonflikt, kann die globale Interdependenz beispielhaft verdeutlichen, denn die Flüchtlingskrise Europas hängt auch mit den Gräueltaten und Anschlägen von IS zusammen, die eine der Fluchtursachen sind. Ein nicht geringer Teil der Terroristen stammt aus Europa und hat keinen regionalen Bezug zu Syrien oder Nordirak. Der regionale Terrorismus in Syrien und Nordirak wird damit zu einem Problem, dass die Regierung und ihre Verwaltung in Deutschland herausfordert, regionale Wahlen beeinflusst und die Legitimität von Regierungshandeln auch auf transnationaler Ebene (Howorth 2012) infrage stellt. Der Terrorismus ist in seiner Komplexität, Diffusität und Globalität zu einem quasi unlösbaren Problem geworden; auch lassen sich die Folgen und Kosten kaum beziffern. Die den Terrorismus begünstigenden Begebenheiten, die nicht abschließend benannt werden können, wie auch die Auswirkungen des Terrorismus, die ebenfalls nicht abschließend benannt werden können, sind politikfeldübergreifend.

Während der Terrorismus in den 1970er Jahren noch hauptsächlich national organisiert war (z. B. Euzkadi Ta Askatasuna, Irish Republican Army, 17 November) und durch indigene Gruppen getragen wurde, die manchmal über internationale Kontakte verfügten (z. B. Baader-Meinhof Gruppe, Volksfront für die Befreiung Palästinas), so handelt es sich heute um eine Form des Terrorismus, der direkt auf das World Wide Web zurückgreift (Tech against Terrorism 2019). Die Cyberwelt wird zu einer Vorbedingung für terroristische Sicherheitsrisiken, die z. B. von IS ausgehen. Extremistisches Cybergrooming ist so nur ein Phänomenbaustein des weltweit agierenden hypermodernen Terrorismus. Die Entwicklung von den 1970er Jahren bis heute lässt sich durch die schrittweise Internationalisierung hin zu transnational organisierten terroristischen Gebilden

beschreiben, wenngleich dies nicht als Alleinstellungsmerkmal des 9/11 Terrorismus gelten kann. Die Akteure sind heute transnational organisiert, sie nutzen Kommunikationsmittel der global vernetzten Cyberwelt, rekrutieren sich nicht allein aus indigenen Bevölkerungsteilen, sondern sind durch ein globales radikales Milieu (Malthaner und Waldmann 2012) getragen, welches sich online vernetzt, und haben keine lokale Agenda mehr. Anschlagspläne werden an fernen Orten geschmiedet, während die Ausführungen der dezentralen Terrorzellen vor Ort stattfinden sollen. Insbesondere terroristische Beziehungsnetzwerke haben sich verändert, denn es braucht keine konkreten Freundschaftsnetzwerke mehr vor Ort, wie die zunehmende Problematik um einheimische, „sich selbst" radikalisierte Täter beweist.

Der moderne Terrorismus nutzt, wie auch schon die klassischen Vorbilder dies taten, die „Waffe der Wahrnehmung": Es geht um „die psychologische Manipulation" des Gegners, der dazu animiert werden soll seine Interessen – auf möglichst brachiale Weise – wahrzunehmen, und neue Interessen zu definieren, die dem Terrorismus zugutekommen (Neumann 2015). Die Kenntnisnahme der Bevölkerung über den derart gewandelten Terrorismus findet insbesondere über die Medien statt und hat zu der Wahrnehmung einer global operierenden islamistischen Verschwörung geführt, die quasi bis in Wohnzimmer reicht.

3 Cyberwelt und Terrorismus – eine glückliche Ehe

Wir leben in einer vernetzten Gesellschaft. Ein wichtiger Kanal für soziale Verbindungen ist heute das Internet. Akteure sind zu Vermittlern zwischen Offline- und Online-Welt geworden. Sie beteiligen sich an Online- und Offline-Diskussionen, bringen Themen zur Sprache und entwickeln politische Visionen und die dazugehörende Semantik, Symbole und Codes, die politische Aktionen auslösen können. Das Internet hat nicht nur die politische Debatte verändert, sondern auch den politischen Bereich, da politische Ideen, Visionen und Ideologien innerhalb von Sekunden ohne Filter weltweit ausgetauscht werden können – und für einige hat sich die Realität verändert: Websites, Blogs und Social-Media-Profile sind zu Wahrzeichen eines politischen Informationssystems geworden, das sich keiner Korrektur unterzieht; so sind Landschaften mit sich gegenseitig unterstützenden und bestätigenden Desinformationen entstanden. Die Informationen der etablierten Medien, der Institutionen wie der Polizei oder der Kirche sind den Informationskanälen eines sozialen Netzwerks extremistisch motivierter Akteure – zumindest für den ungeschulten User – gleichwertig. Gleichzeitig haben Unternehmen Social-Media-Plattformen wie Facebook,

v-kontakte, Google+ und andere entwickelt, die (politische) Echokammern auf Basis von Algorithmen entwickeln. Das Entstehen extremistischer Netzwerke wird von der Politikwissenschaft aufmerksam verfolgt. Diese Netzwerke haben virtuelle und physische Räume, sie bestehen aus losen Gruppen, Organisationen und Einzelpersonen, die in der physischen und Cyberwelt aktiv sind. Das Internet hat alles verändert, fast alles. Sie hat das gesamte Spektrum des politischen Verhaltens verändert. Seit der Einführung der elektronischen Kommunikation hat sich die Gesellschaft schnell von einer Gesellschaft funktional differenzierter Systeme zu einer Netzwerkgesellschaft gewandelt.

Rainie und Wellman (2014) sehen eine dreifache Revolution am Werk: 1) Sie verstehen die Art und Weise, wie man sich heute zusammenschließt, als eine Form von vernetztem Individualismus – das bedeutet, dass Menschen Teilmitgliedschaften in mehreren Netzwerken und nicht in engen Gruppen haben; 2) das Internet hat neue Wege der Kommunikation, der Informationssammlung und der Informationsverbreitung eröffnet – in den neuen Medien gibt es keine Gatekeeper, wie Redakteure oder Verlage, man lädt seine Inhalte einfach selbst hoch; 3) die mobile Revolution hat die Informations- und Kommunikationstechnologie in ein „body appendage", ein Körperanhängsel, verwandelt. Kurz gesagt, der Djihad kann in der Hosentasche überall hin mitgenommen werden. Djihadistische Inhalte sind leicht erhältlich, werden kaum durch Medien konterkariert, oftmals nicht gelöscht oder durch Gegennarrative bekämpft – und sie sind durch ihre körpernahe Aufbewahrung jederzeit erhältlich (Rainie und Wellman 2014).

Zwischen Cyberwelt und dem Terrorismus besteht somit ein intensives Verhältnis. Dies ist bei IS der Fall: Er basiert auf Mediennutzung und nutzt das Internet als Mittel der Kriegsführung. Das Internet bietet der Organisation eine mächtige, multimediale, kostengünstige und schnelle Plattform zur Meinungsverbreitung. IS verfügt über eine planvolle und sich auszahlende Kommunikationsstrategie und nutzt insbesondere Online-Medien als Instrumente zur Verbreitung seiner Propaganda (s. Kap. „Terrorismus und die Nutzung des Internet"). IS hat sämtliche Social-Media-Plattformen besiedelt und ein globales Netzwerk von Unterstützern angezogen, die ihre gewalttätigen extremistischen Botschaften artikulieren, vergrößern und weltweit verbreiten. Damit hat sich online ein breites Spektrum der Unterstützung etabliert, das das radikale Milieu verbreitert hat und den Zulauf zum Terrorismus vergrößert.

IS rekrutiert junge Männer und Frauen weltweit mit Hilfe von Streaming- und File-Sharing-Plattformen über Messenger-Anwendungen bis hin zu Social-Media-Services wie Facebook, YouTube, Twitter, Instagram, Whatsapp, AskFM, Telegram und geht dabei planvoll und strategisch vor (Liang 2015). Neue Plattformen werden dabei stetig ausgetestet und es hat sich ein ganzes System gebildet, sodass Inhalte stabil im Netz gehalten werden können:

> „Exploiting medium- to large-sized platforms as well as DWeb [Dark web] services is not the only problem. In fact, there are hundreds of small- and micro-platform exploited by IS. From file-sharing and streaming services to pastebins, these sites have become an integral part of the propaganda distribution ecosystem. Unlike the larger platforms, small- and micro-platforms lack the required resources to tackle this exploitation alone.“ (Tech against Terrorism 2019)

Die vielfältige Nutzung von Plattformen betrifft mittlerweile nicht mehr nur das World Wide Web, sondern auch das Dark web:

> „Decentralised services have already been exploited by IS and its supporters. Examples include DWeb services Riot, ZeroNet and most recently Minds, an open source and decentralised platform. If implemented successfully and accepted by the wider pro-IS audience, it will become difficult – if not impossible – to tackle IS presence on these decentralised services. That is because these services are independent from any intermediary or ‘middleman’ for receiving and sending messages.“ (Tech against Terrorism 2019)

Der IS bedroht aber auch seine Feinde über das Internet. Dazu nutzt er die hauseigene Nachrichtenagentur *Amaq,* über die sich der IS regelmäßig zu Anschlägen bekennt. Hier werden neue Narrative entwickelt und verbreitet. IS hat einen Terrorismus entwickelt, der sich auf Memplexe beziehen lässt und dessen Ansichten und propagandistische Taten viral sind (Baden 2019). Doch Amaq steht nicht allein; zum Medienimperium gehören das Magazin *Dabiq* und dessen Nachfolger *Rumiyah,* der Radiosender *Al-Bayan* und das *Al-Hayad Media Center.* Der Gegner wird verächtlich gemacht, Anschlagsdrohungen werden veröffentlicht und zahlreiche neue Narrative in die Welt gesetzt, die vor allem die Logik von Anschlag und Gegenanschlag verbreiten sollen (Remsky 2019). Der IS, so die eigene Darstellung, setzte sich lediglich zur Wehr, helfe den schwachen und armen Muslims, die auf den Schutz durch Terror angewiesen seien (Bayerisches Staatsministerium des Innern 2018). Die IS-Medienkampagne fungiert als Verbindungsstelle zu religiösen Führern in der Region und im Ausland. Die größte Stärke von IS, bezogen auf die Cyberwelt, ist die Fähigkeit, das Social Media Angebot zu dezentralisieren. Dies hat es ermöglicht, die Unterstützerbasis zu vergrößern und in Eigenregie dezentrale Inhalte zu entwickeln, zum Zweck der Förderung einer einheitlichen, getriebenen Botschaft (Nanninga 2018). Eine wichtige Zielgruppe sind Jugendliche. Extremistische Cybergroomer von IS haben sich darauf spezialisiert, in die Lebenswelt der Jugendlichen einzudringen und in ihre Sozialisation einzugreifen, indem über Online-Netzwerke der mögliche Nachwuchs ausgehorcht und versucht wird zu instrumentalisieren (Deutschlandfunk 2017).

3.1 Extremistisches Cybergrooming

Cybergrooming ist eigentlich ein Fachbegriff, der das gezielte Ansprechen von Kindern im Internet beschreibt, um sexuelle Kontakte aufzubauen. Der Begriff beschreibt die Täterstrategie: „Grooming“ heißt pflegen oder zurechtmachen. Es geht darum, Schritt für Schritt das Vertrauen des späteren Opfers zu gewinnen. Dabei spielt das Internet als besonderes Tatmittel eine wichtige Rolle. Cybergroomer sprechen ihre Opfer gezielt an, um sexuelle Kontakte herbeizuführen. Im eigentlichen Sprachgebrauch kann es sich dabei um eine sexuelle Belästigung handeln, meistens ist aber das Tatziel die Absicht, sexuellen Missbrauch online oder offline in der physischen Welt anzubahnen.

In für das Opfer harmlos wirkenden Portalen wie Facebook, sprechen die Täter ihre Opfer gezielt an. Sie werden vom Täter hofiert und umworben. Die Täter nutzen eine schmeichelnde Sprache, die Vertrauen wecken soll. Das alles dient dem Zweck, das spätere Opfer zu missbrauchen. Die Risiken Sozialer Medien sind weder den Opfern noch dessen Umfeld wirklich bekannt, obwohl es Aufklärungsversuche gibt. Wenngleich das Opfer mit seinem Device im globalen, öffentlichen Raum unterwegs ist, sitzt es im Wohnzimmer oder einer anderen bekannten Umgebung und fühlt sich „sicher“. Die Täter treten als „Freunde“ auf und erschleichen sich das Vertrauen der Opfer. Nicht alle Opfer sind „Kinder“, es trifft oft „Jugendliche“. Im Internet suchen sich die Täter junge Menschen, die z. B. mit den Problemen der Pubertät konfrontiert sind und sich in ihrem häuslichen Umfeld nicht mehr wohl fühlen. Oft ist der Sinn des Lebens infrage gestellt: Was soll ich mit meinem Leben machen?!

Wird vom extremistischen Cybergrooming gesprochen, so bezieht sich der Begriff insbesondere darauf, dass junge Frauen durch extremistisch motivierte Männer/Online-Profile dazu gebracht werden sollen, sich einem extremistischen Netzwerk anzuschließen. Im besonderen geht es hier darum, dass die Männer/Online-Profile eine ähnliche Kommunikation und eine gänzlich ähnliche Vorgehensweise wählen, wie die Cybergroomer. Dabei nutzen sie die gleichen Vorteile, wie die Sextäter. Das Kommunikations-Device ist heute oft das körpernahe Smartphone. Das Potenzial der Ansprache ist damit zeitlich fast unbegrenzt und wird durch die Körpernähe auch als „intim“ wahrgenommen. Um eine ideologische Nähe zu kreieren, werden neben den normalen Sozialen Medien auch Android-Apps genutzt (Flade 2016).

Es geht darum mit schmeichelnden Worten eine gemeinsame Zukunft zu besprechen, in der vollkommene Liebe und die biedere Sicherheit des kleinen Lebens hochgejubelt werden. Ziel sind junge Frauen, die das Gefühl haben,

isoliert zu sein. Ihnen wird eine wunderschöne, neue Welt versprochen. Freundinnen, gemeinsame Erlebnisse, die eine große Liebe, ein festes Netzwerk an Beziehungen, in dem die jungen Frauen aufgehen können, religiös erfüllt und mit der ethisch wichtigen Aufgabe, humanitäre Hilfe vor Ort zu leisten. Insbesondere IS hat diese Methode der Rekrutierung weiblicher Anhänger professionalisiert (Erelles 2015). Sie finden ihre Opfer auf Facebook, chatten mit ihnen auf Whatsapp und videotelefonieren über Skype. Die Täter betrachten die Online-Profile der Konsumenten der djihadistischen Netzkultur. Sie sind geschulte Beutegreifer, die junge Frauen dazu verleiten sollen, sich auf den Weg in Kampfgebiete zu machen. Zur Hilfe kommt ihnen dabei ein ganz besonderes Phänomen, welches sich Cybergroomer zunutze machen: Das Vertrauen in eine falsche Vorstellung über das Gegenüber ist das entscheidende Einfallstor. Die Userinnen gehen davon aus, dass es sich hier um „echtes" Verständnis, um eine „echte" und „verlässliche" Beziehung handelt. Die Userinnen gehen davon aus, dass es sich um „echte" Profile handelt und sie die einzigen Ehefrauen in einer von der Gemeinschaft getragenen friedlichen und harmonischen Umwelt werden, die von den kriegerischen Konflikten nur vermittelt tangiert ist. Die islamistische Realität der Vielehe wird ausgeblendet und der Täter transportiert sprachlich die Zweisamkeit. Das virtuelle Kalifat besitzt große Anziehungskraft und Krieg, Gewalt und Verbrechen dienen lediglich als Mittel zur Verfestigung von Gemeinschaft und Partnerschaft. Die Gewalt verkommt zu einem, wenngleich heroischen, Nebenaspekt. Die Wahrnehmung der Kontaktziele wird manipuliert. Künstlich wird eine gemeinsame Nähe hergestellt und echtes Interesse wird vorgegaukelt. Es dient dazu, die Hoffnung auf einen idealen Partner, die große Liebe, zu befeuern. Die Vorstellung eines umfassenden Glücks, von einem besseren Leben im Kriegsgebiet, wird geweckt.

3.2 Posterboys und Terrorpropaganda

Bereits die Nutzung der Kommunikationstechnik durch IS ist konsequent und hypermodern. Dezentrale Kommunikationskanäle stehen neben einer, wenngleich in seiner Brutalität und ideologischen Einfassung banalen Message, die ganz auf die Medienwelt zugeschnitten ist. Die Meme-Welt des cyber-basierten Terrorismus von IS lebt davon, eine modische Welle zu prägen. Terroristische Anschläge werden selbst gefilmt und kommen im Stil von Ego-Shootern ins Netz.

3.2.1 Die Rolle der Bilder

Bilder werden bearbeitet und ins Netz gestellt. Terroristen werden zu Hipstern. Sie sind die „Stars“ der Szene, die sich in anti-westlichen Narrativen formiert und dennoch der Inbegriff eines westlich geprägten Vorfelds des hypermodernen cyber-basierten Terrorismus bleibt. Die primäre rhetorische Aktivität der Terroristen ist die „Inszenierung von Image-Events für die Verbreitung in den Massenmedien“ (DeLuca 1999, S. 16). Mittels dieser Bilder wird die Identität der „Gemeinschaft“ des Islamischen Staates rhetorisch konstruiert. Die inhaltlich extremistischen Bilder, die in ihrer Aufmachung radikal wirken – und ihre (Re)Kontextualisierung – manifestiert und mobilisiert die IS-Identitäten von Mädchen und Frauen. Die Bildsprache, verstanden als primäre Kommunikation in diesen virtuellen Räumen, vermehrt sich durch das Teilen der Bilder bzw. der „Bildrhetorik“ in den Sozialen Medien und auch durch die Nutzung der Massenmedien. Das ultimative Ziel der Terrororganisation ist es, die Grenze der sozialen Ausgrenzung zu verschieben und Eingang zu finden in die Kommunikation der Dazugehörigen. Die ausgeschlossenen Gruppen Kommunizieren in Grenzräumen, in denen sie sich artikulieren und hinterfragen können. Hier ist das Einfallstor für die Bildrhetorik von IS. IS nutzt Bildmaterial, um Unterstützung für die Gruppe und für den von ihnen favorisierten sozialen und politischen Wandel zu erhalten. Die Nutzung von Social Media in mehreren Sprachen zieht Einzelpersonen weltweit an, um die Sache zu unterstützen. Zum Beispiel hat IS unzählige etablierte Twitter-Accounts und Facebook-Seiten, um die Ideologie zu teilen.

Bildereignisse sind für IS die wichtigste Möglichkeit, um ihre Ideologie zu teilen, und dafür sind die Accounts in den Sozialen Medien ihre wichtigsten Online-Tools. Die IS-Identitäten stecken in der Bildrhetorik; hier wird deutlich wofür sie stehen, was sie bedeuten, in welchem Namen der IS Gewalt begeht und wie IS sich durch die Identitäten der sich radikalisierenden Persönlichkeiten vermehrt, dort erneut konstruiert wird und von Neuem mobilisiert. All dies geschieht durch vermittelte Kommunikation im Netz. Meme werden auf verschiedenen Ebenen genutzt. Der IS hat eine „memplexe Kultur des Blutrausches“, der extremistischen und menschenverachtenden Einstellung geschaffen. Memes haben für Richard Dawkins die Funktion, sich als kulturelle Einheiten durch „Imitation“ und „Variation“ zu verbreiten. Der Mensch ist das zentrale Medium in diesem Prozess (Dawkins 2007). Diese memplexe Kultur kommt der heutigen Zeit des stetigen Konsums von Medien durch smart Devices sehr entgegen. Während es bei Al-Qaida noch komplizierte ideologische Auseinandersetzungen gab, wird bei ISIS komplett auf komplizierte Überlegungen verzichtet und sie werden durch Bilder ersetzt.

3.2.2 Hipster-Image von Posterboys

Einige Memes sollen den (Hipster)Alltag der IS-Mitglieder zeigen. Sie werden zu Menschen von Nebenan, denen man Vertrauen schenken kann, die „cool“ sind und denen man nacheifern kann. Ein Beispiel für diese Vorbildfunktion bietet Islam Yaken. Der – so die Netzbiographie – aus gutem Hause stammende Yaken, mehrsprachig und gebildet, ist ausgestattet mit modischer Brille und Six-pack; er wird in erotisierender Weise dargestellt. Von ihm gibt es islamistische Fitnessvideos, die den Kämpfer bei Bodybuilding-Übungen zeigen, aber auch bearbeitete Fotos, die ihn als Stilikone zeigen. In Abb. 1 etwa steht ein junger, wütender Mann, in einer Straßenszene. Der modisch gekleidete, gut frisierte Mann hält einen Säbel erhoben. Der Stil der Präsentation erinnert an Parfümwerbung und könnte in jedem Bahnhof hängen. Der westlichen, Konsum amalgamierten Ästhetik wird der islamistische Hipster-Endkampf aufoktroyiert. Der Held, der die ignorante Umwelt angreift und sich gegen die anonymisierende Konsumwelt wehrt, wird so selbst zu einem Konsumprodukt im Stile einer Boygroup-Ästhetik der 1990er Jahre (ElNaggar 2015).

Abb. 1 Beispiel ästhetisierter Bildsprache durch IS – Islam Yaken. (Quelle: Ein offizieller IS Account bei Twitter)

IS hat so eine Welt geschaffen, in der den verschiedenen Sprachgemeinschaften auf sie zugeschnittene Posterboys zugedacht sind. Die jungen Männer werden zu „Löwen“ gemacht. Sie sollen Anziehungspunkte in dem global ausgefochtenen Medienkrieg sein, den IS führt (Flade 2014). Die jungen Männer werden in verschiedenen Alltagsszenen gezeigt. Der Zuschauer kann ihren Alltag scheinbar verfolgen. Yaken wurde mit einem wiedererkennbaren Accessoire ausgestattet – der Säbel taucht immer wieder auf. Diese Technik findet sich auch in der westlichen Musikindustrie, wo der Wiedererkennungswert eine große Rolle spielt. Der Säbel deutet auf die IS-Praxis der massenhaften Enthauptung von vermeintlichen Kriegsgegnern hin. Gleichzeitig blickt Yaken auf einer anderen Abbildung cool und etwas spöttisch in die Kamera (vgl. Abb. 2). Es könnte einem Fantasy-Film entnommen sein (Helg 2014). Die reproduzierten Online-Identitäten sind von einem starken Dualismus geprägt. Der Transport der Inhalte ist hypermodern und an den Konsumgewohnheiten der westlichen Welt orientiert,

Abb. 2 Personifizierung des „Heldenethos“ bei IS – Islam Yaken. (Quelle: ein offizieller IS Account von Twitter)

während der Inhalt selbst eine Art Blutkult darstellt, der lediglich mit einem Islam-Versatz ausgestattet ist. Wichtigster Ideologie-Transporteur ist das Bild – dies unterscheidet IS zum Beispiel von Al-Qaida.

Die extremistischen Cybergroomer profitieren von dem Hipster-Image. Sie versuchen, junge Frauen in die Kampfgebiete zu locken. Dies hat einen praktischen Hintergrund, wie Karin Priester (2015) herausstellt:

> „Die westlichen Männer haben keinen Kontakt zu einheimischen Frauen und sprechen kein Arabisch. Also lassen sie gleichgesinnte junge Frauen nachkommen, die in ihnen Robin Hood oder den Märchenprinzen sehen. Nicht zu vergessen den Sexappeal dieser bärtigen Jünglinge, die mit Fahnen, Kalaschnikows und stolzgeschwellter Brust auf Panzern posieren.“ (Priester 2015, o. S.)

Neben der an Plakatwerbung orientierten Bildsprache, die einzelne Kämpfer in den Mittelpunkt stellt und sie zu „Löwen“ macht, die sich auflehnen und damit ihre tatsächliche Existenz als Kriegsverbrecher überdeckt und verniedlicht, diese aber auch surreal wirken lässt, steht die Bildsprache, die sich an Hollywood orientiert.

3.2.3 Hollywoodhelden und Anschlagsmeme

Eine wichtige Form der Propaganda sind die Memes, die nach Anschlägen in das Netz gestellt werden. Davon zu unterscheiden sind diejenigen Anschläge, die mit Bodycams aufgenommen werden und sich mehr an Computerspielen orientieren. Die kontinuierliche Präsenz djihadistischer Propaganda im Netz, ist ein wichtiger Faktor in der Aufmerksamkeitsökonomie:

> „Terroristische Akte zielen entsprechend auf die Symbolik ihrer medialen Wirksamkeit und setzen so ihren terroristischen Memplex durch. Terrorakte erzeugen überraschende Medienereignisse. Ihre Wirkung hängt vom medialen Multiplikationseffekt ab. Das heißt, der memetische Erfolg beruht auf der erzwungenen Anschlusskommunikation über den Akt der Gewalt. Auf diese Weise sollen Angst und Schrecken, der ‚Terror‘, verbreitet, aber auch SympathisantInnen rekrutiert werden.“ (Baden 2019, o. S.)

Ein interessantes Beispiel bildet dabei ein Poster, das sich der Ästhetik von Star-Wars bedient und die terroristischen Mörder von Paris/Bataclan 2015 in den Mittelpunkt stellt, während die Überschrift sich an einem erfolgreichen Werbespruch der Sportfirma NIKE abarbeitet (s. Abb. 3). Im Hintergrund sehen wir in schwarz/weiß das Bild von Paris. Farbig im Vordergrund sind Portraitaufnahmen der Attentäter. Am linken Bildrand ist das Dach eines Rettungswagens zu sehen.

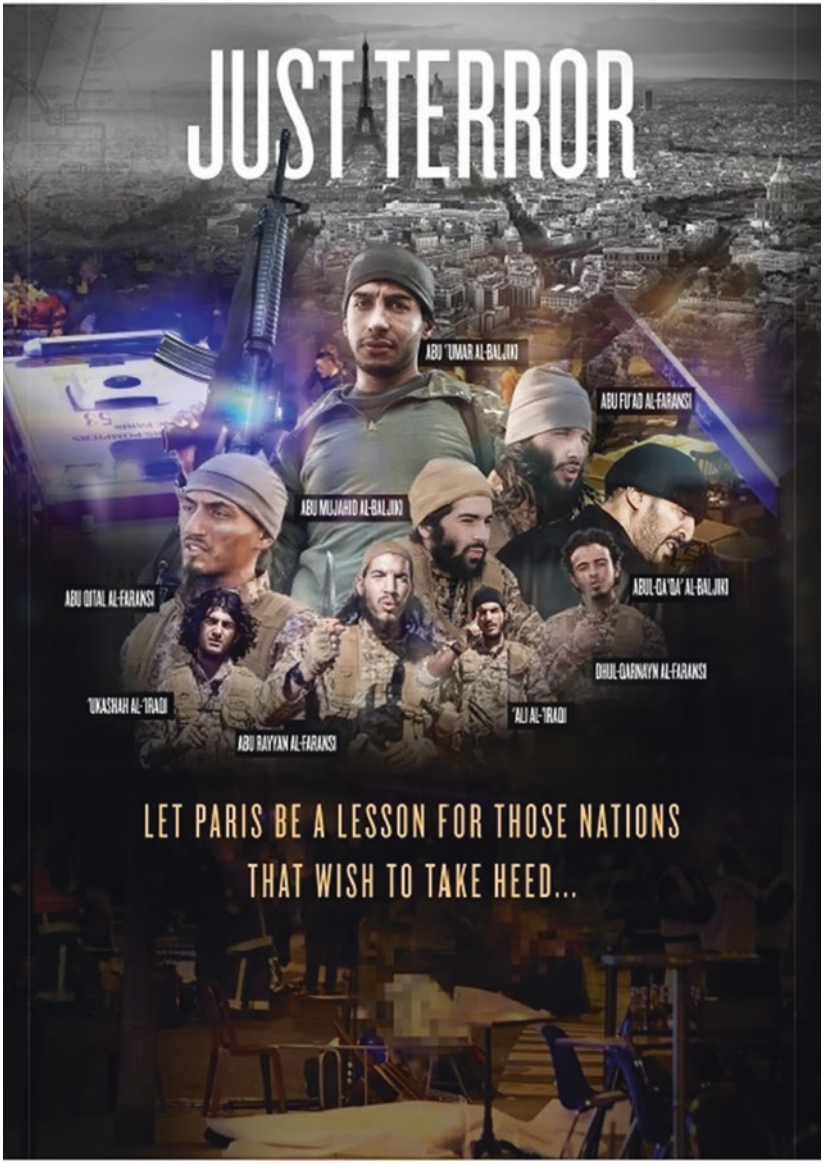


Abb. 3 IS-Poster von Attentätern des Anschlags in Paris 2015. (Quelle: Das IS Magazin Dabiq)

Direkt hinter den Tätern sind durchscheinende Fotos von einem Café, vermutlich einem Anschlagsort, zu sehen. Die Attentäter sind die „Stars“ von einem Ereignis, das wie die Episode eines Films dargestellt wird. Fiktion und Realität verschwimmen. Dieses Bild leistet rhetorische Arbeit, weil es wie eine mentale Bombe funktioniert. Auch hier orientiert sich die Bildsprache an den Konsumgewohnheiten westlicher Jugendlicher. Es geht darum, eine alternative Deutung des terroristischen Ereignisses zu bieten und an den Hipster-Diskurs anzuschließen. Die Unterschrift des Plakats weist darauf hin, das es nach Wunsch von IS tatsächlich nur eine Episode ist und ein zweiter, dritter, vierter … Film folgen soll.

Die Täter werden ebenfalls zu Posterboys gemacht. Sie sind in der Rhetorik des IS „Helden“ und hier werden Metaphern des Heldenkults geschaffen, die Räume des Jubels eröffnen. Die Propaganda von IS mittels Posterboys ist ein Baustein in der Strategie, AnhängerInnen anzuwerben. Ist die Propaganda erst konsumiert, ist es nicht mehr weit, auch den Zugang zu einem Chatforum zu suchen. In den Chatforen, per Skype oder anderen Messaging-Kanälen sind die extremistischen Cybergroomer aktiv. Die Frauen sollen möglichst schnell davon überzeugt werden, sich ins Ausland abzusetzen und ihren extremistischen Cybergroomer zu heiraten. Die Rolle, die den jungen Frauen zugedacht ist, ist Teil der Armee von Hausangestellten zu werden und alle notwendigen häuslichen Dienstleistungen zur Unterstützung des IS zu erbringen. Junge Frauen bieten auch die von Männern gewünschten sexuellen Dienste an. Die extremistischen Cybergroomer schmeicheln diesen Frauen, damit sie ihre Heimat verlassen, um auszureisen. Sie sollen sich diesen Männern anschließen. Gelockt werden sie mit Versprechungen eines hohen Status, einer klaren Rolle, einer wichtigen Bedeutung.

3.2.4 Imaginierte Community – die netten extremistischen Cybergroomerinnen von Nebenan

Neben den Posterboys, die es IS ermöglichen eine islamistische Netzkultur des Blutkults zu etablieren und extremistischen Cybergroomern erleichterten Zugang zu potenziellen Opfern zu verschaffen, stehen die Cybergroomerinnen. Dies sind Frauen, die dem Netzwerk der Daheimgebliebenen suggerieren, eine Ausreise ins Kriegsgebiet würde einen legitimen und realistischen Weg ins Lebensglück bieten. Sie bieten ihren ChatpartnerInnen die Idee von Gemeinschaft. Sie geben den jungen Frauen in ihren Heimatländern das Gefühl sie gehörten dazu, es handele sich um „echte Freundschaftsbande“. Ähnlich wie beim Nationalismus, geht es hier um eine gedachte Gemeinschaft (Anderson 2006). Virtuelle und erdachte Gemeinschaften haben als Figuren einen inneren Zusammenhang (Grădinaru 2016, o. S.):

> „The construction of the imaginary of a certain community does not include only the users' ideas about its structure, but also the expectances that they have about the atmosphere, the way of interaction, and the dynamic of relations. Thus, the imagined perception of community includes the technology, the content and representation, the history of members, the intertextuality of content, and the communication among users."

In diesen Diskussionsforen und Chatrooms können Veranstaltungen aufgegriffen werden, die über den regionalen und sprachlichen Kontext hinausgehen und einen Meinungsaustausch ermöglichen. Dies hat mentale Auswirkungen auf alle Teilnehmer. Common-Bond-Gruppen können leicht gebildet werden und werden später zu Common-Identity-Gruppen. Dies bedeutet, die Beziehungen werden intensiver, die Exklusivität wird erhöht und der soziale Druck nimmt zu. Es gibt mehrere Faktoren, die die Entwicklung der Gruppenkohäsion beeinflussen, so Spieß und von Rosenstiel (2010). Erstens, je mehr Zeit die Gruppenmitglieder zusammen verbringen, desto kohärenter werden sie. Zweitens, je mehr Gruppenmitglieder sich mögen, desto geschlossener ist die Gruppe. Drittens, Gruppen, die für ihre Mitglieder lohnender sind, sind geschlossener. Viertens können externe Bedrohungen für eine Gruppe die Kohäsion der Gruppe erhöhen. Fünftens, Gruppen sind geschlossener, wenn Leiter Gefühle der Wärme unter den Gruppenmitgliedern fördern.

Spieß und von Rosenstiel (2010) nennen mehrere Faktoren, die dazu beitragen, den Gruppenkohäsionsgrad zu erhöhen:

- Äußere Bedrohung
- Exklusivität
- Gruppenerfolge
- befriedigende Rollenverteilung
- Zeitaufwand für das Zusammensein
- Kleine Gruppengröße
- Die Gruppenmitglieder fühlen sich „gleich"

Auf diese Weise können sich Suchende, Mitglieder und Interessierte als Teil eines riesigen erfolgreichen Netzwerks, einer sozialen Bewegung, die islamische Renaissance genannt wird und zu dem IS gehört, interpretieren. Und das tun sie tatsächlich: Sie bilden derzeit ein globales Arbeitsnetzwerk des Extremismus.

Gerade für IS ist der Topos der „hijrah", der Emigration in das Staatsgebiet, sehr wichtig. Schon die dritte Ausgabe von Dabiq bespricht die hijrah als zentrales Thema und fordert Anhänger weltweit dazu auf, in das Staatsgebiet zu

kommen (Bunker und Bunker 2018). Cybergroomerinnen nehmen hier eine sehr wichtige Aufgabe wahr, da sie den Akt der Einwanderung mit einer Vorstellung der Heimkehr amalgamieren:

> „Frauen werden gebraucht, um Frauen zu rekrutieren. Als Mann kannst du nicht einfach so Frauen ansprechen. Frauen und Männer sollen außerhalb der Ehe keinen Kontakt haben.“ (Dantschke 2019)

Die „Schwesternnetzwerke“ sollen jungen Frauen vor Ort suggerieren, es sei „sicher“, in das Staatsgebiet des IS zu reisen. Das Angebot der Frauen gleicht ideologisch dem der Männer. Sie entwickeln Inhalte, die sich gezielt an Frauen richten (Frankfurter Allgemeine Zeitung 2017).

3.2.5 Postergirls und Cybergroomerinnen

Die Cybergroomerinnen nutzen eine Sprache, die die Grenze des Erträglichen verschiebt. Terroranschläge werden da mit „Lol“ oder „Hahaha“ kommentiert, aber auch der Tod des eigenen Ehemanns kann da mit einem „CU8ter“ bejubelt werden und dem „Westen“ wird angesichts seines Bemühens um die Zurückdrängung des menschenfeindlichen Djihadismus schon einmal ein „ROFL“ entgegen geschleudert. Die Cybergroomerinnen übernehmen die Sprache ihrer Kontakte. Interessierte oder Propagandakonsumentinnen werden aber auch ganz intim zu „Schwestern“; so wird quasi automatisch ein Bonding-Prozess initiiert.

In Europa bekannt geworden sind zum Beispiel die extremistischen Cybergroomerinnen Zahra und Salma Halane (Priester 2015). Jedoch unterhalten die meisten jungen Frauen Kontakt zu ihrem Familien-, Freundes- und Bekanntenkreis (Saltman und Smith 2016). Sie fördern terroristische Handlungen über Social-Media-Kanäle, rufen Familie und Freunde dazu auf, ebenfalls in das Gebiet des IS zu reisen, legen sich eigene Twitter-Accounts an oder sind bei Telegram aktiv. Sie zeigen ihren Alltag und bieten Vorstellungen von dem, was der Alltag für IS-Frauen bedeuten könnte. Die Frauen zeigen sich in alltäglichen Szenen, sie essen Pizza, tragen Turnschuhe oder fahren gemeinsam im Bus mit einem Kollektiv an Mitgliedern der speziellen weiblichen IS-Polizei, für die sie arbeiten, oder zeigen sich bei Schießübungen (s. Abb. 4). Die Erzählung dieser Frauen ist eine Metapher, die einen Raum des Jubels kreieren soll. Darin ist alles „normal“, der Alltag des Konsums bleibt, Frauenfreundschaften bleiben. Die Welt wird neu gedacht als ein Leben, in dem Mädchen und Frauen mächtig sind, obwohl sie ihre klare Rolle Zuhause haben. Dabei wird immer wieder auch der Topos der Selbstbestimmung aufgegriffen.

Abb. 4 Beispiel von frauen-spezifischer IS-Propaganda. (Quelle: Ein offizieller IS Account bei Twitter)

Während nun, nachdem der IS weitgehend militärisch geschlagen ist, viele Frauen ihre Rolle im IS klein reden, während sie in kurdischen Lagern auf Entscheidungen warten, die ihre Zukunft betreffen, so haben sich die Frauen vor ihrer Abreise intensiv mit der Ideologie auseinander gesetzt. Sie ließen sich vor ihrer Ausreise von den Mitgliedern der terroristischen Schwesternnetzwerke inspirieren und leisteten vor Ort eine intensive Medienarbeit, nahmen Teil an Spitzelaktionen, arbeiteten in der IS Sittenpolizei, usw. (Röhmel 2019). Es handelt sich demnach bei den Frauen die ausreisen, nicht einfach um „verführte" Frauen, sondern auch um verführende Frauen. Sie sind radikalisiert, sie haben eine Vorstellung von der Ideologie und sie sind gewaltbereit oder befürworten Gewalt:

> „Die Extremisten machen Frauen ein Angebot, das weit über die bekannten Gräueltaten hinausgeht. Das gilt in besonderem Ausmaß für den Islamischen Staat. Seine Botschaft an Frauen lautet: Wir behandeln euch nicht wie Sexobjekte. Wir respektieren euch. Für uns seid ihr die Mütter der nächsten Generation, Wächter unserer Ideologie, Verbreiter unserer Propaganda. Sie nützen dafür unter anderem Memes mit popkulturellen Referenzen. Ein besonders beliebtes Bild zeigt eine verschleierte Frau, und darunter steht: ‚Covered Girl: Because you're worth it.' Und das ist letztlich eine feministische Botschaft, die Frauen ermächtigen soll." (Henckel 2015, o. S.)

Die Halane-Zwillinge gelten als ein wichtiges Zentrum der IS Online-Aktivitäten. Besonders die Aktivitäten auf Ask.FM sind bereits analysiert worden. Hier wurden offen Ratschläge, die die Ausreise betreffend, gegeben. Auch ideologisch geprägte, gewaltorientierte Nachrichten wurden regelmäßig durch die Zwillinge abgesetzt. Sie nutzten zum Beispiel auch Twitter aktiv, um zu gewalttätigen Aktionen aufzurufen. ISIS-Unterstützer, die im Westen leben, werden zum Bespiel dazu angehalten, Zivilisten zu ermorden (Saltman und Smith 2016).

4 Fazit

Extremistisches Cybergrooming ist ein für den extremistischen Terrorismus wichtiges Werkzeug der Ansprache geworden. Neben der Rekrutierung neuer Anhänger, die hier im Fokus stand, steht das Einwerben von Geld und Sachmitteln, die Verbreitung der Ideologie, aber auch neue Gruppenkonfigurationen sind durch das Cybergrooming möglich geworden. Um im Jargon zu bleiben: Die Übertragungsrate extremistischer Ideologien hat sich durch das gezielt angewendete extremistische Cybergrooming erhöht. Sicher ist dies zusätzlich noch von verschiedenen anderen Faktoren abhängig.

Das extremistische Cybergrooming ist kostengünstig, dezentral organisiert und in absehbarer Zeit wohl eine der wichtigen Techniken, die der extremistische Terrorismus regelhaft anwenden wird. Dies lässt sich bereits bei Mikrophänomenen wie der rechtsextrem orientierten Identitären Bewegung ablesen, die hier allerdings nicht Thema war.

Extremistisches Cybergrooming geht von weiblichen und männlichen Tätern aus. Es handelt sich nicht um ein klassisches Sexualdelikt, wenngleich die Kontaktaufnahme sexuelle Ziele inkorporiert. Es ist aber auch keine klassische Anwerbung mit dem Ziel des Eintritts in eine Terrorgruppe. Wie genau dies einzuordnen ist und welche Konsequenzen sich daraus ergeben, wird weitergehend zu analysieren sein.

Der IS ist auf die starken Online-Aktivitäten nicht nur angewiesen, sondern bleibt ohne die Analyse der Cyberwelt unerklärlich. Gerade angesichts der Tatsache, dass der Rückgang der Cybergroomingaktivitäten des IS mit seinem militärischen Zusammenbruch zusammenfällt, zeigt, dass die Bekämpfung des extremistischen Terrorismus in der physischen Welt auch Bedeutung für die Cyberwelt besitzt. Wir können die Cyberwelt nicht vom restlichen Geschehen abkoppeln.

Cybergrooming ist für den IS ein zentrales Mittel der Rekrutierung, der Ideologieverbreitung und der Erweiterung der tatsächlichen Machtbasis. Durch die Cyberwelt gelangt der IS potenziell in jedes Wohnzimmer der entwickelten Welt. Das immer neue Aufkommen neuer Köpfe hat die Polizei und die Verfassungsschutzbehörden mindestens zeitweise überfordert. Mit dem Eindringen terroristischer Akteure hat die Cyberwelt eine neue Dimension an Gefährlichkeit erreicht. Es hat sich aber dadurch auch der extremistische Terrorismus gewandelt. Von einem für die national organisierten Behörden lösbaren „tame problem" hat sich der Terrorismus zu einem „wicked problem" entwickelt. Behörden allein sind gegen diese Form des Technikmissbrauchs nicht gewappnet. Es braucht eine koordinierte Anstrengung von verschiedenen nationalen Behörden und internationalen Organisationen wie den Technikanbietern aus der Privatwirtschaft. Bisher haben extremistische Cybergroomer jedoch noch immer einen Schwachpunkt in der Technik entdeckt, der die fortdauernde Kommunikation ermöglicht.

Literatur

Anderson, B. (2006). *Imagined communities – Reflections on the origin and spread of nationalism*. London: Verso. (1983).

Baden, S. (2019). Der „Memplex" Terrorismus. *kommunikation@ gesellschaft*, *19*, 1–19. https://www.ssoar.info/ssoar/bitstream/handle/document/56056/ssoar-ketg-2018-baden-Der_Memplex_Terrorismus.pdf?sequence=3. Zugegriffen: 10. Mai 2019.

Bayerisches Staatsministerium des Innern und für Integration. (2018). Verfassungsschutzinformationen Bayern im 1. Halbjahr 2018. http://www.verfassungsschutz.bayern.de/mam/islamismus/content/hjb_2018_islamismus.pdf. Zugegriffen: 09. Mai 2019.

Bötticher, A. (2017). Radikalismus und Extremismus: Konzeptualisierung und Differenzierung zweier umstrittener Begriffe in der deutschen Diskussion. https://openaccess.leidenuniv.nl/handle/1887/49257. Zugegriffen: 25. Mai 2019.

Bunker, R. J., & Bunker, P. L. (2018). *Radical Islamist English-language online magazines – Research guide, strategic insights, and policy response* (S. 94). Strategic Studies Institute and U.S. Army War College Press. https://ssi.armywarcollege.edu/pdffiles/PUB1381.pdf. Zugegriffen: 10. Mai 2019.

Dantschke, C. (2019). Beratungsstelle Hayat. Zitiert nach BR24: Hintergrund: Die Rolle der Frauen beim IS. https://www.br.de/nachrichten/deutschland-welt/die-rolle-der-frauen-beim-is,RN2mzMT. Zugegriffen: 02. Mai 2019.

Dawkins, R. (2007). *Das egoistische Gen*. Heidelberg: Spektrum, Akad. Verlag.

DeLuca, K. M. (1999). *Image politics: The new rhetoric of environmental activism*. New York: Guilford Press.

Deutschlandfunk. (2017). Frauen in der salafistischen Szene – Missionsarbeit im Sinne der Ideologie. Götz Nordbruch im Gespräch mit Stefanie Rohde. https://www.deutschlandfunk.de/frauen-in-der-salafistischen-szene-missionsarbeit-im-sinne.694.de.html?dram:article_id=406989. Zugegriffen: 27. Dez. 2017.

El-Naggar, M. (2015). From a private school in Cairo to IS killing fields in Syria. https://www.nytimes.com/2015/02/19/world/middleeast/from-a-private-school-in-cairo-to-IS-killing-fields-in-syria-video.html. Zugegriffen: 23. Apr. 2019.

Erelles, A. (2015). Undercover-Dschihadistin. Wie ich das Rekrutierungsnetzwerk des Islamischen Staats ausspionierte. München: Droemer Verlag.

Flade, F. (2014). Traum deutscher Mädchen von der Djihad Ehe. Die Welt. https://www.welt.de/politik/deutschland/article125275769/Traum-deutscher-Maedchen-von-der-Dschihad-Ehe.html. Zugegriffen: 06. Mai 2019.

Flade, F. (2016). IS veröffentlicht Handy-App für Kinder. https://ojihad.wordpress.com/2016/05/16/is-veroeffentlicht-handy-app-fuer-kinder/. Zugegriffen: 24. Apr. 2019.

Frankfurter Allgemeine Zeitung. (2017). Frau von Terrorzellen-Chef als Salafistin aktiv. https://www.faz.net/aktuell/gesellschaft/kriminalitaet/islamismus-frau-von-terrorzellen-chef-als-salafistin-aktiv-15361006.html. Zugegriffen: 18. Dez. 2017.

Grădinaru, C. (2016). The technological expansion of sociability – Virtual communities as imagined communities. http://www.academicus.edu.al/nr14/Academicus-MMXVI-14-181-190.pdf. Zugegriffen: 22. Apr. 2019.

Helg, M. (2014). Der Hipster als Jihadist. https://nzzas.nzz.ch/gesellschaft/der-hipster-als-jihadist-ld.146154?reduced=true. Zugegriffen: 21. Sept. 2014.

Henckel, E. (2015). Wenn der IS Frauen mit Waffen zeigt, macht uns das Angst. Neue Zürcher Zeitung. https://www.nzz.ch/frauen-als-terroristinnen-wenn-der-is-frauen-mit-waffen-zeigt-macht-uns-das-angst-ld.1295714. Zugegriffen: 4. Juli. 2015.

Hochschule der Polizei des Landes Brandenburg. https://www.youtube.com/watch?v=G3Kyk8K0Y90. Zugegriffen: 15. Juli 2019.

Howorth, J. (2012). *Security and defence policy in the European Union. Basingstoke, New York (2.Auflg.) 2014: Palgrave Macmillan. Sowie: Javier Argomaniz: The EU and counter-terrorism – Politics, polity and policies after 9/11*. London: Routledge.

Junk, J., & Offermann, P. (2014). Sicherheitskommunikation zwischen Alarmismus und Verharmlosung. In C. Daase, S. Engert, & G. Kolliarakis (Hrsg.), *Politik und Unsicherheit – Strategien in einer sich wandelnden Sicherheitskultur*. Frankfurt: Campus.

Liang C. S. (2015). Understanding and countering Islamic state propaganda. Geneva Centre for Public Security. https://www.gcsp.ch/publications/cyber-jihad. Zugegriffen: 23. Apr. 2019.

Malthaner, S., & Waldmann, P. (2012). Radikale Milieus. Das soziale Umfeld terroristischer Gruppen. In: Ders. (Hrsg.), *Das soziale Umfeld terroristischer Gruppen* (S. 11–42). Frankfurt a. M.: Campus.

Martini, A. (2018). Making women terrorists into "Jihadi brides": An analysis of media narratives on women joining IS. *Critical Studies on Terrorism*, *11*(3), 458–477.

Mendick, R., & Verkaik, R. (2014). British female jihadis sign up to the Islamic State's all-women police force. Sept. 2014. https://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/11079386/British-female-jihadis-sign-up-to-the-Islamic-States-all-women-police-force.html. Zugegriffen: 07. Mai. 2019.

Mohagheghi, H. (Hrsg.) (2015). Frauen für den Dschihad – Das Manifest der IS-Kämpferinnen. Freiburg im Breisgau: Herder Verlag.

Nanninga, P. (2018). Branding a caliphate in decline: The Islamic State's video output (2015–2018). https://icct.nl/publication/branding-a-caliphate-in-decline-the-islamic-states-video-output-2015-2018/. Zugegriffen: 19. Mai 2019.

Neumann, P. R. (2015). *Die neuen Dschihadisten: IS, Europa und die nächste Welle des Terrorismus* (S. 25). Berlin: Econ.

Priester, K. (2015). Schulmädchenreport – Das weibliche Gesicht des Dschihad. https://www.frankfurter-hefte.de/Archiv/2015/Heft_04/Zwischenruf/. Zugegriffen: 22. Apr. 2019.

Rainie, L., Wellman, B. (2014). *Networked – The new social operating system* (S. 11 f.). Cambridge: MIT Press.

Ramsauer, P. (2017). Die verlorenen Töchter. Wiener Zeitung. https://www.wienerzeitung.at/nachrichten/politik/welt/925483-Die-verlorenen-Toechter.html. Zugegriffen: 27. Okt. 2017.

Remsky, S. (2019). Wer ist für die Anschläge in Sri Lanka verantwortlich? https://www.zeit.de/gesellschaft/zeitgeschehen/2019-04/terrorismus-sri-lanka-anschlaege-explosionen-faq. Zugegriffen: 21. Apr. 2019.

Rittel, H. W. J., & Webber, M. M. (1973). Dilemmas in a general theory of planning. *Policy Sciences*, *4*(2), 155–169. http://www.sympoetic.net/Managing_Complexity/complexity_files/1973%20Rittel%20and%20Webber%20Wicked%20Problems.pdf. Zugegriffen: 07. Mai 2019.

Röhmel, J. (2019). Die Rolle der Frauen beim IS. BR24 – Hintergrund. https://www.br.de/nachrichten/deutschland-welt/die-rolle-der-frauen-beim-is,RN2mzMT. Zugegriffen: 20. Mai 2019.

Saltman, E. M., & Smith, M. (2016): ‚Till Martyrdom Do Us Part‘ Gender and the ISIS Phenomenon. Institute for Strategic Dialogue. https://www.isdglobal.org/wp-content/uploads/2016/02/Till_Martyrdom_Do_Us_Part_Gender_and_the_ISIS_Phenomenon.pdf. Zugegriffen: 07. Mai 2019.

Speckhard, A. (2015). *Bride of IS: One young woman's path into homegrown terrorism*. McLean: Advances Press.

Spieß, E., & Rosenstiel, L. von (2010). *Organisationspsychologie – Basiswissen, Konzepte und Anwendungsfelder* (S. 55). München: Oldenbourg Verlag.

Tech against Terrorism. (2019). IS use of smaller platforms and the DWeb to share terrorist content. https://www.techagainstterrorism.org/2019/04/29/analysis-IS-use-of-smaller-platforms-and-the-dweb-to-share-terrorist-content-april-2019/. Zugegriffen: 01. Juni 2019.

Wired Drug War

Wie lateinamerikanische Gangs und Kartelle die Digitalisierung nutzen

Julia Jaroschewski und Sonja Peteranderl

1 Einleitung und Überblick

Drogen, Waffen, Drohungen und Deals: Auch Gangs und Kartelle sind in sozialen Netzwerken wie Facebook, Twitter und Instagram aktiv. In Ländern wie Brasilien und Mexiko ist das Internet ein zunehmend wichtiger Schauplatz des Drogenkriegs. Gangs und Kartelle nutzen digitale Portale als PR-Plattform und prahlen mit Autos, Geld und Waffen. Online multipliziert sich die Reichweite von blutigen Botschaften: Bilder grausam verstümmelter Leichen, Videos von Hinrichtungen, in denen Rivalen vor laufender Kamera die Köpfe abgesägt werden, zirkulieren auf Plattformen wie YouTube, Twitter, Instagram, WhatsApp, Facebook und sogenannten Narcoblogs[1], die oft ungefiltert anonyme Einsendungen veröffentlichen. Kriminelle Organisationen spähen in sozialen Netzwerken Rivalen und Opfer aus, rekrutieren neue Mitglieder. In Mexiko professionalisieren sich kriminelle Netzwerke zudem, indem sie IT-Experten, Hacker oder

[1]Der Begriff „narco“ – abgeleitet von „narcotráfico“ (Spanisch für „Drogenhandel“) – repräsentiert in Mexiko Personen, Objekte und Bereiche, die direkt oder indirekt mit dem Drogensektor in Verbindung stehen (Heufelder 2011, S. 23).

J. Jaroschewski (✉)
BuzzingCities Lab, Berlin, Deutschland

S. Peteranderl
DER SPIEGEL, BuzzingCities Lab, Hamburg, Deutschland

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

T.-G. Rüdiger und P. S. Bayerl (Hrsg.), *Cyberkriminologie,*
https://doi.org/10.1007/978-3-658-28507-4_16

Elitesoldaten anheuern, die etwa Überwachungsnetzwerke installieren oder digitale Angriffe auf Rivalen ausführen.

Das Aktivitätenspektrum von kriminellen Gruppierungen lässt sich einteilen in 1) die strategische, öffentliche Kommunikation von kriminellen Gruppen sowie die Selbstdarstellung einzelner Mitglieder von kriminellen Gruppen sowie 2) die Unterstützung krimineller Operationen mit Internet- und Mobilkommunikation sowie anderen technologischen Mitteln.

Im Folgenden soll ein Überblick über die Nutzung von Online-Plattformen und technologischen Hilfsmitteln sowie Trends im Bereich lateinamerikanischer Gangs und Kartelle mit Schwerpunkt auf Brasilien und Mexiko gegeben werden.

2 Folter-Videos und Narco-PR: Die öffentliche Kommunikation krimineller Organisationen

Kriminelle Gruppen kommunizieren öffentlich, um ihre Botschaften zu verbreiten, Rivalen, den Staat, die Öffentlichkeit und andere Akteure einzuschüchtern oder ihr Image zu verbessern (Phillips und Rios 2019, S. 2). Ihre Botschaften verbreiten sie nicht nur mit Gang-Graffitis, auf Bannern, die im öffentlichen Raum wie an Brücken aufgehängt werden, oder auf Zetteln und Plakaten, die neben Leichen hinterlassen werden – sogenannten „Narcomensajes“, Narco-Botschaften. Zunehmend kommunizieren lateinamerikanische Gangs sowie Kartelle und einzelne Mitglieder auch online, auf Plattformen wie Twitter, Youtube, Facebook oder in WhatsApp-Gruppen (Peteranderl 2011, 2013b, 2014; Guevara 2013; Campbell 2014; Monroy-Hernández und Palacios 2014; Jaroschewski 2016; Phillips und Rios 2019).

Phillips und Rios zufolge, die 1800 Botschaften mexikanischer Kartelle aus dem Zeitraum 2007 bis 2010 ausgewertet haben, gewinnt die öffentliche Kommunikation normalerweise klandestin agierender krimineller Gruppen unter verstärkten Wettbewerbsbedingungen an Wert:

> „Public criminal communication should be likely when there is: antagonism among criminal groups, government crackdowns, what we call “information competition” with the news media, local drug consumption, and local drug production.“ (Phillips und Rios 2019, S. 2)

2.1 Drogenkrieg in Mexiko

Mexiko ist ein zentraler Korridor für Drogen und andere illegale Waren, aber auch eine Drogenproduktionsstätte; zudem sind die kriminellen Organisationen transnational vernetzt und in eine Vielzahl anderer illegaler und legaler Geschäftszweige involviert wie Entführungen, Schutzgelderpressung oder Ölhandel (Stuart 2019). Mexikos Kartelle sind die größten Zulieferer von Heroin, Methamphetamin und Kokain in die USA. Während der Großteil der Heroin-, Methamphetamin- und neuerdings auch Fentanyl-Produktion in Mexiko stattfindet, wird Kokain vor allem in Bolivien, Kolumbien und Peru produziert und dann durch Mexiko transportiert (Lee et al. 2019).

In Mexiko haben die Gewalt, die Mordrate sowie die absolute Zahl von Morden stark zugenommen, seitdem der damalige Präsident Felipe Calderón 2006 den Krieg gegen die Drogen ausrief und das Militär gegen Kartelle einsetzte – eine Strategie, die auch von den Nachfolgeregierungen verfolgt wurde und zur Zersplitterung krimineller Organisationen, zu zunehmenden Rivalitäten zwischen kriminellen Gruppen, aber auch zu brutalen Schlägen gegen staatliche Sicherheitskräfte führte:

> „In recent years, the nature of violence has changed as the country's major drug trafficking organizations, or cartels, have become more fragmented, decentralized, and diversified in their activities, this has contributed to a proliferation of smaller, regional and local criminal organizations and a more complex set of challenges for the Mexican government." (Calderón et al. 2019, S. 3 f.)

Angesichts der Verhaftung und Verurteilung des Sinaloa-Drogenbosses El Chapo und einem internen Machtkampf des Sinaloa-Kartells versucht derzeit das Cartel Jalisco Nueva Generación (CJNG) mit verschiedenen Allianzen die Vorherrschaft in Mexiko zu erlangen (Calderón et al. 2019, S. 25 f.).

Die Kartelle ringen seit Jahren sowohl offline als auch online um die Deutungshoheit: *„In Mexiko gibt es einen physischen Krieg, aber auch einen Krieg um Ideen, um Herzen und Köpfe"*, so der Sicherheitsexperte Antoine Nouvet über das Phänomen. *„Indem Kartelle den Cyberspace für sich nutzen, verwandeln sie sich in ihre eigenen Werbeagenturen"* (Peteranderl 2013b).

2.2 Drogenkrieg in Brasilien

Auch Brasiliens Drogengangs haben schon seit Anfang der 2000er Jahre den strategischen Nutzen der Onlineformate erkannt. Brasilianer sind sehr internetaffin: Allein in den zehn Jahren von 2007 auf 2017 ist die Zahl der Internetnutzer in Brasilien von 43 Mio. auf 139 Mio. Nutzer gestiegen (Internet World Stats 2019). Die schnelle Verbreitung des Internets und der anonyme Zugang über Cybercafés hat auch Gangmitglieder online aktiv werden lassen. Über die Jahre hinweg sind nicht nur soziale Medien wie Orkut, Messenger, MySpace und Facebook von Kartellen zur offiziellen Präsentation genutzt worden. Sie instrumentalisieren soziale Medien nicht nur, um ihre Macht gegenüber dem Staat und der Polizei zu demonstrieren, sondern auch, um sich untereinander einzuschüchtern.

Zwar gehen Brasiliens Regierungen gegen die erstarkende Vorherrschaft der kriminellen Drogengangs vor, doch Brasilien hat insbesondere für den Drogenhandel eine große Bedeutung. Das größte Land Südamerikas mit seinen 201 Mio. Einwohnern ist das Land mit dem höchsten Drogenkonsum auf dem Kontinent. Einerseits verbraucht Brasilien selbst das Kokain, das aus den Nachbarländern Bolivien, Kolumbien und Peru importiert wird (World Drug Report 2016). Andererseits ist das Land der größte Umschlagplatz für den Weitertransport nach Afrika und Europa.

Brasiliens Korruptionsskandale und die starke Interpenetration von Korruption, Politik und Wirtschaft geben der Organisierten Kriminalität im Land ausreichend Zeit und Platz, sich auszubreiten. Der im Oktober 2018 zum Präsidenten gewählte rechts-populistische Politiker Jair Bolsonaro setzte im Wahlkampf mit seiner Partei stark auf die Verbesserung der inneren Sicherheit und den Kampf gegen die Kriminalität, doch seit Amtsantritt im Januar 2019 muss sich Jair Bolsonaro für die Verquickungen von Familienmitgliedern und Parteikollegen erklären, die selbst mit kriminellen Akteuren kooperieren (Alessi 2019; Olliveira 2019). Insbesondere hat die Rolle der Milizen, paramilitärischer Einheiten, zugenommen, die besonders in Rio de Janeiro in den Armenvierteln zusätzlich zu den Drogengangs im Bereich des Drogenhandels agieren.

Wie in Mexiko besteht in Brasilien eine Wettbewerbssituation zwischen kriminellen Organisationen. Brasilien zählt Dutzende Drogengangs, viele ordnen sich den großen einflussreichen Kartellen wie dem „PCC“ (Primeiro Comando Capital) aus São Paulo, dem „CV“ (Comando Vermelho) aus Rio de Janeiro und der „Familia do Norte“ aus dem Norden Brasiliens unter. Digital veröffentlichte Fotos, Videos und Audios dienen der Präsentation und dem Ausbau der eigenen

tatsächlichen oder aber vermeintlichen Stärke und vergrößern den Einfluss in manchen Regionen.

Im Folgenden werden die wichtigsten Plattformen sowie Formen der öffentlichen Kommunikation von Gangs und Kartellen in Brasilien und Mexiko analysiert sowie die primären Funktionen der Plattformen für die kriminellen Organisationen und ihre Mitglieder dargestellt.

2.3 Narcoblogs, Crime-Seiten und WhatsApp-Gruppen als neue Gatekeeper

In Mexiko hat das Phänomen der sogenannten „Narcoblogs“ – Weblogs, die über Kartellkriminalität berichten – die Aufmerksamkeit auf die kriminellen Aktivitäten im Internet gelenkt. Seit Beginn des 21. Jahrhunderts sind im mexikanischen Drogenkrieg mehr als 332.000 Menschen ermordet worden (Calderón et al. 2019, S. 7). Auch die Medien sind Schauplatz des Drogenkriegs, in dem Akteure wie Staat, Politiker und Kartelle um die Deutungshoheit ringen (Reyes 2010). Angriffe auf Medienhäuser, die Bedrohung und Einschüchterung von Journalisten durch Politiker, Sicherheitskräfte und Kartelle hat in den vergangenen Jahren zu einer steigenden Selbstzensur der Medien geführt. Viele Zeitungen in besonders von Konflikten betroffenen Gebieten vermeiden die Berichterstattung über organisiertes Verbrechen (Freedom House 2019).

Angesichts der zunehmenden Zensur vor allem lokaler Medien begannen anonyme Blogs über Kartellkriminalität oder Schießereien zu berichten und veröffentlichten auch von Lesern anonym eingesandte Augenzeugenberichte und anderes Material, teils auch von Kartellen eingeschicktes Bild- und Videomaterial (Peteranderl 2011, S. 20). Im März 2010 launchte der bekannteste Blog „Blog del Narco“ dieses Genres, der schnell zu einer der 50 meistgelesenen Webseiten Mexikos avancierte (Monroy-Hernández und Palacios 2014, S. 85). Nachrichten und Bildmaterial zu Exekutionen und Leichenfunden nahmen mit 42 % den größten Anteil der Bloginhalte ein (Monroy-Hernández und Palacios 2014, S. 90). Die meisten Blogs wurden von anonymen Bloggern mit dem Selbstverständnis aufgesetzt, ein alternatives Forum zu sein, sie betrachten sich als Gegenöffentlichkeit zur Regierung und traditionellen Medien – werden aber eben auch als Propagandaplattform von kriminellen Gruppen instrumentalisiert (Peteranderl 2011, S. 20).

Auch auf anderen Plattformen wie Twitter, Facebook oder Youtube sind Seiten und Kanäle entstanden, die Nachrichten oder Augenzeugenberichte zu

Kartellkriminalität und Gewalt kuratieren. Forscher haben Kartellaktivitäten in Internet und sozialen Netzwerken wie MySpace, Youtube und Twitter seit 2005 beobachtet. Monroy-Hernández und Palacios (2014, S. 87) haben aber einen deutlichen Anstieg von Plattformen wie Narcoblogs seit 2008 festgestellt. Kanäle zu Kartellkriminalität und Schießereien in sozialen Netzwerken haben zugenommen: *„While early sites like NotiNarco and NarcoMexicano consisted solely of blogs, newer outlets often include Twitter, Facebook, and YouTube accounts“* (Monroy-Hernández und Palacios 2014).

Immer wieder gründen meist anonyme Betreiber auch in Brasilien Blogs und Micro-Blogs in sozialen Netzwerken, auf denen über die Gangs berichtet wird, lokal und regional. Crimenews-Seiten führen oftmals Profile auf Facebook und Youtube. In den Blogs finden sich unterschiedliche Beiträge: aktuelle Veränderungen innerhalb der Machtstrukturen der Banden, Polizeioperationen und damit einhergehende Morde und Verluste der Gruppierungen. Berichte über die Hierarchien der Gangs, der Bosse und Übergriffe auf gegnerische Gangs sind klassische Beiträge (Crime News 2019; Realidade das Favelas 2019). Einige der Blogs berichten über bekannte Drogenbosse oder die Entstehungsgeschichten und Legenden bestimmter Banden.

Oftmals werden jedoch auch Gerüchte aufgegriffen und verbreitet. Nicht immer ist deswegen deutlich nachzuvollziehen, welche Richtigkeit und damit Wertigkeit die entsprechenden Beiträge haben. Da die Betreiber dieser Seiten oft nicht bekannt sind, ist die Glaubwürdigkeit nicht oder nur schwer einzuschätzen. Zum Teil scheinen Informationen von Facebook-Gruppen von Polizisten oder den Sicherheitsbehörden nahestehenden Personen zu stammen, da Erfolge von Polizeioperationen gezeigt werden, Bilder und Videos von toten Kriminellen überwiegen.

Die neuen Plattformen der dezentralen Berichterstattung über Gangs, Kartelle und Verbrechen werden in Lateinamerika kontrovers diskutiert: Einerseits wird den Blogs und den Kanälen in sozialen Netzwerken Potential zugeschrieben, Bürger auf riskante, aktuelle Situationen in ihrer Umgebung hinzuweisen und Augenzeugenberichte zu veröffentlichen. Andererseits wird kritisiert, dass viele Falschinformationen oder Gerüchte zirkulieren und die neuen Medien auch als Plattform von Kartellen genutzt werden, die den Betreibern Videos, Fotos und Informationen zuspielen (Peteranderl 2011, S. 18). *„Das Problem mit den Narcobloggern ist, dass viele von ihnen [die Blogger] keine Journalisten sind und manche Narcoblogs sich in Knotenpunkte der Kommunikation von Kartellen verwandelt haben, die dort Drohungen veröffentlichen“,* sagt etwa die mexikanische Investigativjournalistin Anabel Hernández. *„Es besteht die Gefahr, dass*

Menschen Informationen glauben, die nicht aus verlässlichen Quellen stammen und nicht journalistisch aufbereitet worden sind.“[2]

Wie in Mexiko übernimmt in Brasilien das Publikum der Seiten eine wichtige Funktion – Leser und deren Wissen sind mit der Transition der Crimenews-Seiten von Websites und Blogs hin zu Facebook und anderen sozialen Medien zunehmend relevanter geworden. Leser kommentieren tendenziöse Berichte und tragen zum Teil Insiderwissen bei. Unter den Kommentatoren sind Bürger, von der Gewalt Betroffene, aber auch Sicherheitskräfte, Kriminelle und Experten, die die Gewalt diskutieren. Beiträge werden von Mitgliedern oder Unterstützern der lokalen Gang oder deren Kontrahenten oftmals stark meinungsgeladen kommentiert.

In Brasilien sind Kommentare von Bewohnern aus den von besonders von Gangkriminalität betroffenen und geprägten Regionen oder Favelas sehr wertvoll im Prozess des Factcheckings, also der Überprüfung von lokalen Informationen und Gerüchten. Diese Form des Crowdsourcing hilft Bürgern und Kriminellen ebenso wie Sicherheitskräften – die Plattformen können trotz des Risikos von Gerüchten eine wichtige Quelle für Informationen darstellen, die etwa bei der Lagebewertung helfen (Muggah und Diniz 2013, S. 9 f.; Milhorance 2018).

Auch „Disque Denuncia“ hilft mit Crowdsourcing bei der Suche nach und teils auch Festnahme von Kriminellen. Vom Genre her ist „Disque Denuncia“ eine Spezialform und unterscheidet sich von den von anonymen Bürgern betriebenen Crime-Blogs und -Seiten. „Disque Denuncia“ ist eine Organisation sowie ein gleichnamiges Denunziationsportal, das 1995 von dem brasilianischen Unternehmer Zeca Borges gegründet wurde, Unterstützung von der Stadt Rio de Janeiro erhält und mit der Polizei kooperiert (Jaroschewski 2015a). Über das Portal können Bürger kriminelle Handlungen anonym melden.

„Disque Denuncia“ ist mittlerweile über diverse Messenger, soziale Medien wie Instagram, Facebook, Twitter erreichbar und betreibt unter anderem das Online-Portal „Procurados“, bei dem Kriminelle aller Drogengangs und Milizen gelistet sind, die bei Polizeioperationen festgenommen wurden und gegen die ein Verfahren läuft (Procurados 2019). „Procurados“ – übersetzt „Gesuchte“ – sammelt die entsprechenden Täter und veröffentlicht Profile mit Nicknames, bürgerlichen Namen, persönlichen Daten, ihrer Gangzugehörigkeit, Straftaten, laufenden Verfahren und der Kopfgeldsumme, die auf die jeweilige Person ausgesetzt ist. „Procurados“ postet zudem regelmäßig Profile von gesuchten mutmaßlichen Kriminellen auf Facebook. *„Ein Großteil unserer Leser sind Kriminelle selbst,*

[2]Interview mit Anabel Hernández in Berlin am 7. Juni 2011.

denn sie nutzen Disque Denuncia als Informationsquelle über die gegnerischen Gangs", erklärte Borges in einem Video-Interview 2015.[3]

2.4 Youtube: Foltervideos und Sozialkampagnen

Wie Terrororganisationen nutzen Gangs und Kartelle in Lateinamerika die virale Wirkung blutiger Propaganda-Bilder im Internet aus (s. a. Kap. „Posterboys und Terrorpropaganda"). Mit Videos wenden sich kriminelle Gruppen oder einzelne Mitglieder auf Youtube an Regierung, Bevölkerung oder Rivalen – die Videos werden sowohl auf Youtube selbst veröffentlicht, als auch über Narcoblogs, Crime-Seiten in sozialen Netzwerken oder WhatsApp-Gruppen weiterverbreitet. Inzwischen sind Gangs und Kartelle aber nicht mehr zwingend darauf angewiesen, fremden Plattformen oder sozialen Netzwerken ihr Material zuzuspielen – sie betreiben teils eigene reichweitenstarke Twitterkanäle, Facebookseiten oder WhatsApp-Gruppen, um ihre Perspektiven, Nachrichten, sowie Bild- und Videomaterial direkt zu verbreiten.

Lange vor der online-affinen Terrororganisation Islamischer Staat (IS) haben Mexikos Kartelle begonnen, die Folter mutmaßlicher Mitglieder rivalisierender Kartelle und andere Videos auf Kanälen wie Youtube zu veröffentlichen. Dem Soziologieprofessor Howard Campbell von der University of Texas in El Paso war ein Foltervideo der Beginn des mexikanischen Online-Drogenkriegs zugeschickt worden. Im Jahr 2005 zirkulierte ein Video auf Youtube, das zeigte, wie ein Mörder vier Mitglieder des Zetas-Kartells verhörte und folterte:

> „Es war das erste große Social-Media-Event und schien den Stil von Al-Qaida nachzuahmen. Das Phänomen explodierte und verbreitete sich wie ein Lauffeuer – heute gibt es Tausende von ähnlichen YouTube-Videos und andere Arten der Nutzung von Social Media." (Peteranderl 2014)

In Brasilien zelebrieren Gangmitglieder Folter, meistens mit dem Handy gefilmt. Im Mai 2016 wurde die Doppelhinrichtung von zwei Teenagern im Alter von 14 und 16 Jahren in einem Video festgehalten. Die Jugendlichen hatten eine Favela in Niteroi bei Rio de Janeiro angeblich nur besucht, um dort ein Pferd zu kaufen. Als sie in eine Schießerei gerieten, rannten sie der lokalen Drogengang direkt in die Arme. Deren Mitglieder hielten die beiden für Mitglieder einer rivalisierenden

[3]Interview mit Zeca Borges in Rio de Janeiro am 12. Mai 2015.

Gang. In dem Video, das etwa über WhatsApp-Gruppen weiterverbreitet wurde, sehen die beiden Jungen verstört in die Kamera, einem läuft Blut über das Gesicht, auch sein Kapuzenpulli ist blutverschmiert. Sie müssen dem Mann nachsprechen, der sie mit einer Pistole bedroht, dem Boss der Drogengang huldigen, die die Favela beherrscht. Mit den Händen bilden die Teenager die Buchstaben „C“ und „V“, die Initialen des „Comando Vermelho“, einer von Rios mächtigsten Drogengangs. Erschossen werden sie trotzdem (Jaroschewski 2016).

Bevor sie getötet werden, sind gefangene Rivalen in Brasilien wie Mexiko oft gezwungen, zu gestehen, welcher kriminellen Organisation sie angehören, wen sie entführt und ermordet haben. Ein Katalog ihrer Verbrechen wird verlesen. Die erzwungenen Geständnisse vor der Kamera haben eine Signalwirkung – sie sollen Stärke gegenüber der eigenen, aber auch gegenüber der rivalisierenden Organisation vermitteln, senden aber auch eine Botschaft an die Öffentlichkeit.

> „Es ist eine Art politisches Statement, oft geht es um den Einfluss der Kartelle in bestimmten Regionen. Die Narcos wollen zeigen, dass sie die Guten sind, die gegen die Mächte des Bösen kämpfen; dass sie die Gesellschaft vor ihren Feinden schützen, die wirklich abscheuliche Taten begangen haben.“ (Peteranderl 2014)

Dieses Narrativ spiegelt sich in vielen kriminellen Social-Media-Strategien. In Mexiko hat sich etwa das Kartell der Caballeros Templarios (Tempelritter) in sozialen Netzwerken und mit eigenen Facebook-Seiten sowie Youtube-Kanälen als Kämpfer für soziale Gerechtigkeit und Frieden in Michoacán positioniert – und als beste Option, um angesichts eines machtlosen Staates, korrupter Sicherheitskräfte und brutaler rivalisierender Kartelle Sicherheit herzustellen. *„Es ist korrekt, dass wir Waffen haben – um unseren Staat vor den Zetas zu beschützen und vor dem Cártel de Jalisco Nueva Generación“,* sagte der inzwischen festgenommene Tempelritter-Chef Servando Gómez Martínez alias „La Tuta“ in einem mittlerweile von Youtube entfernten 14-min Video, das mehr als 1,2 Mio. Mal angesehen wurde. Er forderte die Regierung zudem auf, gegen die Bürgerwehren vorzugehen, hinter denen angeblich das Cártel de Jalisco Nueva Generación (CJNG) stecke, und bot dem Staat seine Unterstützung an (Peteranderl 2014).

In Brasilien spielen Frauen in Videos eine große Rolle. Frauen und Mädchen, die sich mit den vermeintlich falschen Personen einlassen, der Drogenbande zu viel geredet oder gegen andere Verhaltensregeln der Gangs verstoßen haben, werden öffentlich gefoltert, gedemütigt oder missbraucht. Damit die Schande möglichst breite Wirkung erzeugt, filmen die Peiniger ihre Opfer dabei. Rasant verbreiten sich solche Nachrichten über Messengerdienste wie Whatsapp und Telegram (Jaroschewski 2016).

So wurde im Jahr 2014 eine 18-Jährige in einer Favela von mehreren Männern vor laufender Kamera drangsaliert (O Globo 2014). Der sichtbar eingeschüchterten Jugendlichen wurden mit einem langen Messer die Träger des Oberteils durchgeschnitten, um somit ihren Oberkörper zu entblößen, mit einem Rasierer und Schere wurden ihre langen Haare abrasiert, immer wieder von Beleidigungen und Schlägen der Männer unterbrochen. Selbst als sie bereits blutend und erschöpft am Boden lag, schütteten ihr die Männer Wasser ins Gesicht, zwangen sie, der Folter wach beizuwohnen. Das Mädchen erlag Tage später ihren Verletzungen im Krankenhaus. Das Abrasieren der Haare von Frauen hat eine lange Tradition in der Geschichte der Demütigung (Frevert 2017). Fast archaisch sind diese Rituale in kriminellen Strukturen erhalten geblieben und erfüllen ihren Zweck: Sie verbreiten Angst, zementieren die Macht der Peiniger und senden eine Warnung an die Bevölkerung, sich dem Willen der kriminellen Organisationen unterzuordnen.

Die Verbreitung von Nachrichten aus dem kriminellen Milieu in Brasilien funktioniert oft in Form einfach geschnittener Videos. Fotos, Mitschnitte und Screenshots werden in Brasilien häufig aus offiziellen Medienberichten zusammengeschnitten und mit Nachrichten über Gangs und ihre Aktivitäten vertont (Facções News 2019). Weil sich die Produzenten dieser Videos schützen wollen, wählen sie dabei häufig die Anonymisierung durch Computerstimmen.

Eine andere Form der Werbung für die eigene Gang und zugleich dem künstlerischen Genre zuzuordnen sind musikalische Videos, die die Handlungen einer bestimmten Drogengang oder einer bestimmten kriminellen Führungsfigur publik machen – die eigene Macht, Auseinandersetzungen oder Gebietsgewinne werden thematisiert, aber auch alltägliche Themen wie soziale Ungleichheit, Unterdrückung und Gewalt durch Sicherheitskräfte oder den Staat werden besungen.

Sogenannte „Narcocorridos“ in Mexiko und „Funk Proibidão“ als ein spezielles Rap-Subgenre in Brasilien werden durchaus nicht nur von Kriminellen gehört (Cymrot 2011, S. 48), sind aber ebenfalls fester Bestandteil der kriminellen Kultur. Sie sind:

> „mehr als ein bloßes Medium der Nachrichtenvermittlung. Sie sind Teil der Drogenkultur und reproduzieren diese wiederum, indem sie gleichermaßen zur Würdigung von alternativen Normen und Werten beitragen sowie die Anerkennung und Verankerung dieser in der Bevölkerung forcieren. Darüber hinaus sind sie ein extrem erfolgreiches Mittel der Glorifizierung von mehr oder weniger populären Narcos“ (Wickert 2013).

In Mexiko reicht die Tradition dieser Volksmusik bis ins 19. Jahrhundert zurück (Wickert 2013), heute werden die Lieder auch auf Plattformen wie Youtube, über Facebook oder Messenger weiterverbreitet.

In Brasilien bestimmen Funk-MCs insbesondere in Rio de Janeiro und Rapper in São Paulo die musikalische Szene. In den harmloseren Videos rappen die meist jungen Männer über den Alltag in den Favelas und beschreiben den Werdegang der aktuellen Drogenbosse. MCs stammen zumeist aus der Favela, die sie besingen. In der Hierarchie aufgestiegen bespielen sie lokale Baile Funks, Parties in den Favelas. Sofern die Polizei nicht eine kontrollierende Machtfunktion in der jeweiligen Favela ausübt, repräsentiert der Baile Funk oft ein soziales Unterhaltungsevent für die Favela, auf der der lokale Drogenboss und seine Männer die VIPs darstellen, die Regeln bestimmen, oft auch den Drogenhandel ankurbeln und ebenso Einfluss auf die Musik haben (Cymrot 2011, S. 51).

Sowohl in Brasilien als auch in Mexiko beauftragen hochrangige Kriminelle Bands oder Rapper, bestimmte Lieder anzufertigen. In den Proibidão-Funks und ihren Online-Videos schlagen MCs auch schärfere Töne an, sie provozieren die Gegner in ihren Songs, beschreiben die Macht der jeweiligen Gang (Sneed 2003, S. 82). Nicht selten werden dabei Drohungen ausgesprochen, direkt Nachrichten an Feinde gesendet. Loyalität gegenüber der eigenen Gang ist sehr wichtig, negative Kommentare über diese können für MCs ein Todesurteil bedeuten.

Videos werden mitunter auch für Imagekampagnen genutzt, die das soziale Engagement der Gangs und Kartelle vermitteln sollen und etwa dokumentieren, wie kriminelle Organisationen nach Naturkatastrophen spenden. Das Sinaloa-Kartell dokumentierte nach Hurrikan-Verwüstungen mit YouTube-Videos, aber auch auf Instagram Hilfeleistungen für zerstörte Gebiete. Nach den Tropensturm-Verwüstungen im September 2013 präsentierte sich auch das Golfkartell als Wohlfahrtsorganisation, mit einem Video, in dem mehrere mit Lebensmitteln beladene Pick-ups in einem betroffenen Gebiet abgeladen werden (Proceso 2013, Peteranderl 2013b). Die Hilfe für die Hurrikan-Opfer wurde nicht nur in sozialen Netzwerken diskutiert und weiterverbreitet, sondern auch von traditionellen Medien: *„Drug cartels seized the opportunity to provide aid and influence community sentiment in their favor“* (Sullivan 2013).

Brasiliens Drogengangs verbreiten Bilder und Videos von Events, bei denen die Bewohner von Armenvierteln, insbesondere Kinder und Jugendliche, beschenkt werden – häufig mit Spielzeug wie Spielen, Bällen, Puppen oder mit Fahrrädern. In großen Stückzahlen werden diese Gaben an die arme Bevölkerung vermeintlich verschenkt. Auch der ehemalige Drogenboss Rogerio 157 von Rio

de Janeiros größter Favela Rocinha verbreitete bis zu seiner Festnahme 2018 auf Twitter Videos, wenn er für die Kinder Geschenke oder Essenspakete an Bedürftige verteilte – sie wurden von anderen Favelabewohnern meist mit Wohlwollen in den sozialen Netzwerken weiter geteilt und kommentiert.[4]

Die Botschaft der Gangs: Nicht der Staat, sondern die Gangs kümmern sich um die vernachlässigten, einkommensschwachen Bevölkerungsgruppen. Dies ist jedoch in doppelter Hinsicht scheinheilig, da diese Geschenke oft aus dem Diebesgut von Fracht-/Lasterüberfällen stammen. Zudem basiert das Patronagesystem der Gangs nicht nur auf Nächstenliebe: In vielen Regionen müssen Bewohner monatliche Schutzgelder an die Gangs zahlen.

2.5 Präsentation in sozialen Netzwerken

Gangs und Kartelle sind in zahlreichen sozialen Netzwerken aktiv wie Twitter, Facebook und Instagram; früher auch Hi5, MySpace oder Orkut. Im Folgenden sollen vor allem die Aktivitäten auf den drei heute zentralen sozialen Netzwerken Twitter, Facebook und Instagram, sowie Messengerdienste analysiert werden.

Es ist vor allem die jüngere Generation, die in sozialen Netzwerken präsent ist. Während die alten Drogenbosse sich wie Phantome bewegten und lange etwa von dem inzwischen inhaftierten Sinaloa-Boss El Chapo kaum ein Foto existierte, sind ihre Söhne und Nachfolger Social-Media-Fans. Sie präsentieren ihr Geld, Autos, Drogen und Waffen in sozialen Netzwerken und verbreiten Propaganda, um die Kartelle zu verherrlichen und Gegner einzuschüchtern. Auch Facebook-Fanseiten feiern die Gangs und Kartelle, zu deren Anhängern harmlose junge Menschen zählen, die den Drogenlebensstil verherrlichen, aber auch echte Kartellmitglieder.

Einige Mitglieder krimineller Organisationen haben sich einen Influencer-Status mit teils Hunderttausenden von Followern aufgebaut. El Chapos Söhne Ivan und Alfredo und andere junge Männer aus dem Sinaloa-Kartell waren etwa lange auf Twitter aktiv und posteten Autos, Raubtiere, und Sturmgewehre. Die Gúzman-Brüder zogen sich dabei Basecaps ins Gesicht, machten ihre Gesichter auf Fotos mit Photoshop unkenntlich; andere Kriminelle waren weniger vorsichtig. Broly Banderas vom Tempelritter-Kartell präsentierte sich dagegen mit Maschinengewehren, Patronen oder Geldbündeln, ohne sein Gesicht zu verdecken. Auch sein inzwischen verhafteter Chef, der Boss der Tempelritter „La

[4]Das Twitter-Profil ist mittlerweile inaktiv.

Tuta“, veröffentlichte regelmäßig PR-Videos auf YouTube, die Hunderttausende von Klicks erhielten. Auch dank ihrer sehr aktiven, strategischen Online-Kommunikation und Influencern wie „La Tuta“ oder „Broly Banderas“ ist es den Tempelrittern – einem vergleichsweise kleinen Kartell – gelungen, eine nationale Präsenz aufbauen (Abb. 1; Peteranderl 2013b).

José Rodrigo Aréchiga Gamboa, ehemaliger Kopf und Gründer des Killerkommandos „Los Ántrax“ des Sinaloa-Kartells, postete auf seinem Instagram-Konto „miauuuuuu5_7“ Fotos von Louis Vuitton-Gepäck, aber auch Selfies an Bord einer Yacht, vor einem Luxushotel in Monaco, oder in Tarnmontur im Wald mit einem Sturmgewehr. Er benutzte zwar Photoshop, um sein Gesicht unkenntlich zu machen, aber auf den meisten Fotos und Videos war er durch seinen Ring mit dem Totenschädel identifizierbar, dem Logo des Ántrax-Killerkommandos. Vermutlich haben die Instagram-Fotos von seinen Reisen dazu beigetragen, dass er verhaftet wurde: Im Dezember 2013 wurde er in Amsterdam

Abb. 1 Der mexikanische Narco-Influencer „Broly Banderas“ vom Kartell der Tempelritter präsentierte sich auf Facebook regelmäßig mit Waffen – und offenem Visier. (Foto: Broly Banderas/Facebook – Profil inzwischen gelöscht)

auf dem Flughafen verhaftet – auch damals trug er seinen Schädelring (Peteranderl 2014).

Brasiliens Drogengangster zeigen sich ebenso gerne online – mit Gütern wie Goldketten, Markenkleidung, Autos, Motorrädern, Waffen, teurem Alkohol. Bestimmte Whiskeysorten und Energydrinks in „Party-Eimern“ zählen zu den elementaren Objekten, die Gangmitglieder auf ihren Profilen teilen. In Brasilien wurde der inzwischen getötete Drogenboss Celso Pinheiro Pimenta alias „Playboy“ von der Gang A.D.A., Amigos dos Amigos, auch durch seine Online-Auftritte bekannt. In den sozialen Netzwerken präsentierte er sich mit Frauen, Autos, Motorrädern und Waffen (Jaroschewski 2015b). Auch Fotos von seinem Schmuck, einer eigens für ihn aus Gold angefertigten Comic-Figur mit Gewehr, stellte er online. Als Provokation an Staat und Rivalen veröffentlichte er zudem Bilder von sich und seiner Gang, wie sie schwer bewaffnet in einem öffentlichen Freibad schwimmen und ihre Maschinengewehre in die Luft strecken (Abb. 2).

Abb. 2 Die Bilder der Mitglieder der Drogengang, die ihre Waffen in einem öffentlichen Schwimmbad in Rio de Janeiro provokant nach oben streckten, waren Aufmacher in vielen brasilianischen Medien, wie hier bei „extra“ aus Rio de Janeiro. (Foto: Screenshot extra-online) (https://extra.globo.com/casos-de-policia/traficantes-ostentam-fuzis-dentro-da-piscina-da-vila-olimpica-de-honorio-gurgel-14298499.html. Zugegriffen: 12. Mai 2019)

Waffen und deren Präsentation für die Öffentlichkeit zählen zu den wichtigsten Formen der Inszenierung in den sozialen Medien. Das Posieren der Männer und zum Bandenmilieu gehörender Frauen mit ihren Gewehren sowie Fotos und Videos, auf denen mit Kriegsgerät geschossen wird, sind ein Teil der kriminellen Kultur. Waffen sollen Macht, Einfluss und Status demonstrieren. Tatsächlich erhalten Bilder davon viele Likes und huldigende Kommentare von den Followern. Früher war das Posieren im Selfie-Stil mit Waffen besonders beliebt, doch haben auch die Sicherheitsbehörden ihren Arbeitsstil geändert.

Über die vergangenen Jahre hinweg hat sich aufgrund der verstärkten digitalen Ermittlungen das Verhalten der Gangmitglieder verändert. Mehrere Anpassungsphänomene, die die Identifikation von Kriminellen erschweren, lassen sich daher mittlerweile feststellen.

In seltener gewordenen Postings zeigen Kartellmitglieder in Brasilien größtenteils Waffenansammlungen (Leitão 2019), ohne Gesichter, ohne Körperteile oder Objekte, die die dahinterstehenden Personen identifizierbar machen könnten. So ist es sehr beliebt, einen Teil der Gewehre, aus der Perspektive eines Schießenden zu zeigen – das Zielrohr auf eine Favela gerichtet. Stellten sich Bandenmitglieder früher gern mit ihren Waffen in die Luft gestreckt für ein Gruppenfoto auf, stehen dafür nun repräsentativ Gewehre an die Wand gereiht (Abb. 3).

Anstatt selbst aufgenommener Fotos, auf denen sie etwa mit Waffen posieren, zeigen Kriminelle nun etwa Bilder und Screenshots aus bekannten Filmen wie „Cidade de Deus“ („City of God“) – als Memes, die das Gangsterleben verkörpern. Viele der Social Media-Profile von Kriminellen in Brasilien und Mexiko sind zudem inzwischen inaktiv. Kriminelle haben ihre Social Media-Profile teils selbst gelöscht oder betreiben diese nicht mehr aktiv weiter – zum Teil wurden die Seiten auch von den sozialen Netzwerken selbst gesperrt. Insbesondere hochrangige Bosse gehen mit ihren Daten und ihren Online-Auftritten vorsichtiger um.

Die virtuelle Freizügigkeit von Narcos, die Fotos von Missionen posten und Aufenthaltsorte verraten, können nicht nur aufgrund digitaler Ermittlungen riskant sein – sondern auch, wenn rivalisierende Kartelle die Spuren auswerten. 2017 wurde ein Drogendealer in Rio de Janeiro ermordet aufgefunden, wenige Tage nachdem er die Eroberung eines Favelaterritoriums einer rivalisierenden Gang live über sein Smartphone gestreamt hatte. Mit den Aufnahmen, die er online veröffentlichte, hatte er zugleich weitere Mitglieder seiner Bande enttarnt (Bottari 2017).

Digitale Ermittlungen werden auch dadurch erschwert, dass inzwischen Fans von Gangs und Kartellen zahlreiche Profile anlegen, auf denen sie aus dem Internet kopierte Fotos und Videos veröffentlichen. So ist es schwieriger geworden, echte Kriminelle von Fans zu unterscheiden (Jaroschewski und Peteranderl 2014).

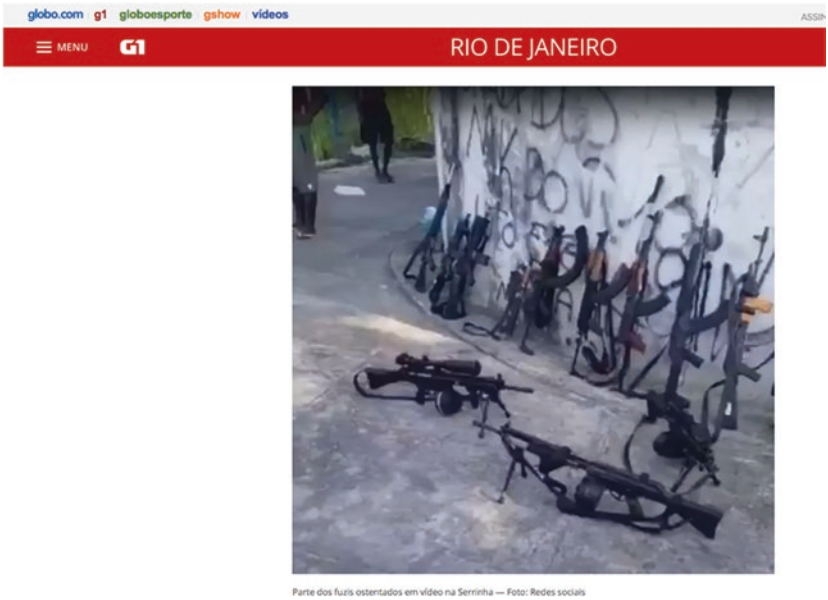


Abb. 3 Früher Selfies, jetzt nur noch Waffen: Mitglieder der Drogenbanden in Rio de Janeiro stellen ihre Waffen aufgereiht an eine Hauswand, um ihre „Kriegsmacht" zu demonstrieren. Bilder wie solche übernehmen brasilianische Medien aus den sozialen Netzwerken. (Foto: Screenshot G1 O Globo/Leitão 2019) (https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/02/03/trafico-exibe-arsenal-em-morro-da-zona-norte-do-rio.ghtml. Zugegriffen: 3. Aug. 2019)

Zunehmend verschiebt sich Kommunikation zudem in Messenger und Chat-Gruppen. In Brasilien haben sich mit dem Mobiltelefon aufgenommene Audio-Nachrichten als Form der kriminellen Kommunikation und Propaganda etabliert. Messengerdienste wie WhatsApp oder Telegram sind in Brasilien weit verbreitet und für Gangmitglieder ein schneller und einfacher Weg zu kommunizieren, sowie Bilder und Videos zu verbreiten, ohne großen logistischen Aufwand zu betreiben.

Nummern und Profile sind austauschbar, die Kommunikation schnell und kostengünstig. Sie senden Botschaften an die Bevölkerung und gegnerische Banden. Selbst bei schlechter Netzabdeckung schicken Drogenbosse und Unterhändler so Nachrichten an die eigenen Gangmitglieder, die diese wiederum

anderweitig lancieren, etwa in WhatsApp-Gruppen oder sozialen Medien. So geraten Botschaften ebenfalls an die Polizei und die Medien (Dlmusicas 2019) – die Skandalisierung in den Medien trägt wiederum zur Verstärkung der kriminellen Propaganda bei.

3 Unterstützung krimineller Operationen mit digitalen Mitteln

Die digitalen Aktivitäten der Gangs und Kartelle dienen nicht nur der öffentlichen Kommunikation, sie unterstützen auch konkrete Operationen. Im Folgenden soll ein Überblick über das Aktivitätenspektrum gegeben werden.

3.1 Digitale Rekrutierung

Per Internet rekrutieren mexikanische Kartellmitglieder auch Mitarbeiter jenseits der mexikanischen Grenze: Die amerikanische Drogenfahndungsbehörde DEA warnte bereits 2012 davor, dass die Zetas, das Sinaloa-Kartell, das Golfkartell, das Juárez-Kartell und La Familia Michoacana über soziale Netzwerke wie Facebook versuchen, Jugendliche zwischen 14 und 20 Jahren aus den USA zu rekrutieren – um sie als Kartellmitglieder, Spione, Auftragsmörder oder Schlepper von Migranten anzuwerben (Peteranderl 2014).

2015 wurde etwa ein 14-jähriger Schüler über Facebook für einen Mordauftrag in der mexikanischen Grenzstadt Tijuana angeworben. Vor Ort erhielt er die Tatwaffe von einem Taxifahrer, er erschoss das Opfer, wurde aber anschließend festgenommen. Seine Prämie konnte er so nicht mehr kassieren. 31.000 mexikanische Pesos, umgerechnet knapp 1700 EUR, waren ihm in Aussicht gestellt worden (Peteranderl 2015).

Dem US-Justizministerium zufolge ist auch die Zahl der Vorfälle, bei denen Drogen von Minderjährigen an der Grenze zu Kalifornien beschlagnahmt wurden, deutlich gestiegen. Von 2016 auf 2017 gab es einen Anstieg der registrierten Fälle von Drogenschmuggel durch Minderjährige um 153 %, von 39 auf 99 Vorfälle. Kriminelle Organisationen versprechen den Minderjährigen Geld oder Elektrogeräte als Belohnung:

> „They have been known to recruit children at schools, but also may approach them at after-school functions, camps, libraries, on public transportation, via social media outlets, and over electronic communications like gaming consoles, text messages or chat rooms.“ (United States Department of Justice 2018)

Minderjährige schmuggeln mittlerweile zudem Fentanyl, was in den Vorjahren nicht der Fall war (United States Department of Justice 2018).

3.2 Vorbereitung von Straftaten

Die kriminellen Organisationen spionieren zudem Unternehmen für Schutzgelderpressungen aus oder suchen nach potentiellen Opfern für Identitätsdiebstahl, Erpressung, Entführungen oder Menschenhandel. *„Facebook und IP-Adressen sind für die mexikanischen Kartelle genauso wertvoll wie Waffen und Panzer“,* so der US-Sicherheitsexperte Brad Barker (Gomora 2012). Soziale Netzwerke dienen auch der Anbahnung von Kontakten zu zukünftigen Zwangsprostituierten: Auf Facebook flirten zudem sogenannte „Loverboys“ mit jungen Frauen und versuchen sie zu einem persönlichen Treffen zu überreden – kommt es zu einem Treffen, werden sie entführt, unter Druck gesetzt oder mit einem lukrativen Jobangebot dazu verleitet, ihrem vermeintlichen neuen Freund an einen anderen Ort zu folgen.

Auch Migranten sind für die Kartelle ein Geschäft, in Mexiko haben die kriminellen Gruppen inzwischen weitgehend das Schlepper-Geschäft übernommen. Migranten, die Mexiko durchqueren, werden aber auch entführt und müssen Lösegeld zahlen, zum Teil auch Zwangsarbeit verrichten. In Mexiko entführte Migranten berichteten, dass die Kidnapper nicht nur die Telefonnummern der Angehörigen forderten, um Lösegeld zu erpressen, sondern auch das Passwort für das Facebook-Profil der Migranten – um das Profil zu durchforsten und die Familienmitglieder unter den virtuellen Freunden zu kontaktieren (Peteranderl 2013a).

Auch per Facebook Messenger oder WhatsApp werden Familienmitglieder von tatsächlichen oder nur angeblichen Entführungsopfern bedroht und zu Zahlungen genötigt – die Kriminellen schicken auch ihre Bankdaten per Messenger, an die die Lösegelder überwiesen werden sollen (Plevin und Ornelas 2019).

3.3 Drogen- und Waffenhandel online

Über Facebook- und WhatsApp-Gruppen werden in ganz Lateinamerika kleinere Drogenmengen und mitunter auch Waffen vertrieben (Diario Extra 2017).

In Brasilien werden Drogendeals häufig über verschlüsselte Messenger und unter Nutzung von Codewörtern vereinbart – die Ware wird dann persönlich ausgeliefert, insofern es sich um kleinere Mengen handelt. Über eine von Drogendealern gegründete WhatsApp-Gruppe wurden etwa synthetische Drogen wie MDMA in fünf brasilianischen Bundesstaaten verkauft. Die Gruppe, die zuletzt rund 200 Mitglieder hatte, wurde Anfang des Jahres 2019 ausgehoben, indem sich Ermittler unter die Online-Kunden mischten (Carlos 2019).

Waren es früher überwiegend Telefonmitschnitte, die zu Fahndungserfolgen führten, ist die Überwachung von Messengern heute ein wichtiger Bestandteil der brasilianischen Polizeiarbeit geworden. Belege für kleinere Drogendeals werden über Messenger ebenso entdeckt wie Mordaufträge, Waffenhandel und andere kriminelle Geschäfte (De Sales Dias 2018). WhatsApp musste sich bereits mehrfach mit der brasilianischen Justiz auseinandersetzen, weil der Messengerdienst keinen Zugang zu bestimmten Daten von Nutzern geben wollte, gegen die Ermittlungen liefen. Der Dienst wurde daraufhin mehrmals für kurze Zeit im ganzen Land gesperrt (Spiegel Online 2016).

Teilweise experimentieren kriminelle Gruppen in verschiedenen lateinamerikanischen Ländern auch mit dem Drogenhandel per Drohne – allerdings können nur kleinere Mengen so verschickt werden, was sich bisher allenfalls in unzugänglichen Gebieten oder gut kontrollierten Grenzregionen lohnt (Peteranderl 2019a).

Auch der Online-Verkauf von Drogen im Darknet ergänzt die klassischen Kanäle für den Drogenvertrieb, spielt aber eine sehr untergeordnete Rolle im Vergleich zu traditionellen Vertriebswegen (s. a. Kap. „Von der Straße ins Netz“). Aussagen von IT-Experten zufolge haben sich alle großen Kartelle in Mexiko zumindest mit dem Darknet und Kryptowährungen wie Bitcoin vertraut gemacht. *„Die Kartelle nutzen das Deep Web in erster Linie für Narcumenudeo, also den Verkauf kleinerer Drogenmengen, aber auch als Schauplatz für große Lieferungen“,* so ein mexikanischer Hacker (Peteranderl 2014). Kartellmitglieder würden dabei Codes verwenden – etwa ein „Lastwagen voller Zitronen“ als Metapher für einen Drogendeal.

Dennoch ist der Anteil des Drogenhandels, der über Darknet-Plattformen abgewickelt wird, vergleichsweise gering. Darknetplattformen sind für Konsumentenländer attraktiver als für Produzentenländer:

> „Anstatt bestehende Lieferketten zu beseitigen oder zu ersetzen, werden in einigen wenigen, hochaktiven Verbraucherländern Darknet-Märkte für den Einzelhandel genutzt – auch, da transnationale Drogenlieferungen per Post ein sehr hohes Risiko sind.“ (Dittus et al. 2018)

3.4 Überwachung

In Brasilien und Mexiko zerstören Mitglieder von Gangs und Kartellen nicht nur Überwachungskameras von Polizei oder Militär, sie installieren auch eigene Kameras im öffenlichen Raum. Mitunter verwanzen mexikanische Kartelle ganze Stadtteile und installieren Überwachungskameras an strategischen Punkten wie Straßen oder in der Nähe von Grenzübergängen. Die Kameras übertragen live, so dass Polizeioperationen oder Rivalen schneller erkannt werden können oder die Route von Drogentransportern aus der Ferne überwacht werden können. In Reynosa hat die Polizei im Mai 2019 ein Netzwerk von Überwachungskameras entdeckt, die in Ampelanlagen, in Stromkästen oder in falschen Straßenlaternen versteckt waren. 2015 waren bereits zwei Männer in Reynosa festgenommen worden, als sie gerade versteckte Kameras installierten (Peteranderl 2019b).

Teils kontrollieren die Kartelle sogar die Überwachungszentren der Polizei. In Gómez Palacio im Bundesstaat Durango kontrollierte das Cártel del Poniente bis etwa Ende Januar 2013 das polizeiliche Nachrichten- und Kommandocenter (Peteranderl 2014). El Chapo ließ seine Mitarbeiter, ebenso wie seine Frau und Geliebten zudem mit Spionagesoftware ausspionieren, die er auf Smartphones und Laptops installieren ließ (Peteranderl 2019b). Auch Drohnen werden in Mexiko zunehmend für die Überwachung unzugänglicher Gebiete, von Rivalen oder Sicherheitskräften eingesetzt (Peteranderl 2019a).

Brasilien setzte gerade im Kontext der Großereignisse wie der Fußballweltmeisterschaft 2014 und Olympia 2016 auf modernste Überwachungstechnologien in den Großstädten, wie einer neuen Kommandozentrale der Sicherheitskräfte in Rio de Janeiro mit großflächigen Bildschirmen und Echtzeitübertragung von zahlreichen, in der Stadt verteilten Kameras. Auch die Gangs ließen die Aufrüstung nicht an sich vorüberziehen. In der größten Favela Rocinha zerstörten die Mitglieder der Drogenbanden nicht nur gezielt die von der Polizei installierten Überwachungskameras, sie verkabelten die Favela selbst mit eigenen Audio- und Videoaufnahmegeräten. So konnten sie insbesondere die zahlreich in der Rocinha stationierten Polizeitruppen überwachen und ihren Drogenhandel trotz der Besetzung des Viertels durch die Polizei weiterführen.[5]

In Brasilien gehören auch Drohnen mittlerweile zum Repertoire einiger Drogenkartelle. Das Terceiro Comando Puro (TCP) in Rio de Janeiro nutzt

[5]Interview mit der Unidade de Polícia Pacificadora (UPP) Rocinha in Rio de Janeiro am 16. Juni 2015.

Drohnen, um Rivalen auszuspähen (O Globo 2018a). Ebenso hat die Polizei in Einzelfällen Drohnen zur Beobachtung und Lokalisierung von Mitgliedern der Drogenbanden eingesetzt. Ende 2018 sagte der neu gewählte konservative Gouverneur von Rio de Janeiro, Wilson Witzel, dass die Sicherheitskräfte darüber nachdenken sollten, bewaffnete Drohnen für die Arbeit in den Favelas einzusetzen, um gegen Gangmitglieder vorzugehen (O Globo 2018b).

In Mexiko wurde zudem eine erste Attacke mit einem Sprengsatz per Drohne registriert. Die Attacke in Tecate wird dem Drogenkartell Jalisco Nueva Generación (CJNG) zugerechnet, das als besonders brutal gilt und den Staat immer wieder herausfordert (Peteranderl 2019a).

4 Fazit und Trends

Kriminelle Organisationen in Brasilien und Mexiko nutzen neue Technologien, um ihre Macht zu demonstrieren und ihren Einfluss zu erweitern. Sie experimentieren mit digitalen Innovationen und setzen eine Vielzahl von technischen Hilfsmitteln und Plattformen für Propaganda, Kommunikation sowie die Unterstützung von Operationen ein.

Digital verbreitete Propaganda spielt mittlerweile eine erhebliche Rolle bei der Außendarstellung und der versuchten Einflussnahme auf Akteure wie Staat, kriminelle Rivalen, aber auch Bürger. Gangs und Kartelle sind nicht mehr auf Gatekeeper wie traditionelle Medien angewiesen – sie betreiben eigene Social Media-Konten oder Chat-Gruppen, deren Inhalte dann wiederum von Medien, Narcoblogs oder anderen Mikro-Seiten aufgegriffen und weiterverbreitet werden.

Portale wie Facebook oder Twitter werden nach wie vor von Kriminellen genutzt, die unbeschwerte Frühzeit des Social Media-Booms ist allerdings vorbei. Mitgliedern krimineller Organisationen ist bewusst geworden, dass sie sich verletzlich machen, wenn sie zu viele Informationen online veröffentlichen und versuchen sich inzwischen mit einer zurückhaltenderen Posting-Strategie, der Anonymisierung von Profilen, aber auch mittels digital verfremdeter Stimmen und der zunehmenden Nutzung weniger öffentlicher Kanäle wie Messenger und eigener Kommunikationsnetzwerke zu schützen.

Die semantische Verschlüsselung interner Kommunikation von kriminellen Banden in Form von Codewörtern wird zunehmend durch den Einsatz von Verschlüsselungstechnologien ergänzt. Auch neue Technologien wie Drohnen werden für Überwachung, Drogenhandel oder sogar zum Transport von Sprengsätzen genutzt, sie befinden sich aber noch im Experimentierstadium.

Technologie verändert nicht die Grundmechanismen der kriminellen Geschäfte – Gangs und Kartelle fokussieren sich weiterhin auf traditionelle Geschäftsfelder wie Drogenhandel, Schutzgelderpressung, Entführungen oder Geldwäsche. Digitale Hilfsmittel unterstützen aber die traditionellen Aktivitäten, etwa durch die Gewinnung von Informationen über Rivalen oder Opfer, digitale Rekrutierung oder die Kontaktaufnahme zu späteren Opfern.

In bisher geringerem Ausmaß bilden sich rein digitale Kriminalitätsformen wie virtuelle Entführungen heraus, bei denen eine Entführung nur vorgetäuscht wird und die Erpressung und die Bezahlung von Lösegeld völlig über Kanäle wie Facebookmessenger oder WhatsApp abgewickelt wird.

Cybercrime im engeren Sinn wie Hacking oder digitale Erpressung durch die Verschlüsselung von Computern und anderen Geräten mit Ransomware, könnte auch für traditionelle kriminelle Gruppen zukünftig ein interessantes Geschäftsfeld darstellen. Schätzungen zufolge richtet Cybercrime weltweit fast 600 Mrd. US$ Schaden an (Center for Strategic und International Studies 2018).

Brasilien rangiert weltweit bereits auf Platz 2 der Länder mit Cybercrime-Aktivitäten – da Brasiliens Regierung relativ spät auf die Herausforderung Cybercrime reagierte, hatten Kriminelle dort freien Spielraum, ihre Aktivitäten ungehindert auszuweiten (Glenny 2012). Allein im Jahr 2013 verzeichnete Brasilien eine Summe von 4,7 Mrd. US$ Verluste aufgrund von Onlinebetrug (Thompson und Muggah 2015), McAfee schätzt den Verlust für brasilianische Firmen aufgrund von Cybercrime mittlerweile auf zehn Milliarden Dollar pro Jahr (Center for Strategic und International Studies 2018). Auch Brasiliens traditionelle kriminelle Organisationen haben Cybercrime als neues Geschäftsfeld für sich entdeckt, wie etwa das massenhafte Kopieren von Geldkarten-Daten (Muggah et al. 2014).

Dennoch sind die klassischen Drogengangs und -kartelle weit davon entfernt den Cybercrime-Markt zu übernehmen (Lusthaus 2018). Hochspezialisierte, technisch versierte kriminelle Entrepreneure oder Hacking-Gruppen dominieren den globalen Cybercrime-Markt, deren Dienste traditionelle Drogenhandelsgruppen teils zukaufen – „Crime-as-a-Service“. Selbst Darknet-Drogenhandelsplattformen werden nicht von traditionellen Drogenhandelsgruppen betrieben, sondern von IT-Experten – Gangs und Kartelle nutzen höchstens die Infrastruktur (Aiken et al. 2016; Europol 2016).

Ermittlungen in den Niederlanden haben gezeigt, in welchem Umfang Drogenhandelsgruppen etwa mit der Hilfe von externen Hackern logistische Systeme manipulieren und sich einen Vorteil verschaffen können. Den beauftragten Hackern gelang es, in die Hafen-Sicherheitssysteme einzudringen und die PIN-Nummern von Containern zu stehlen – so konnten die Kriminellen ihre

Drogentransporte bereits vor den Hafenkontrollen abfangen und abladen (Leyden 2013).

Während nicht alle Gang- und Kartellmitglieder IT-Experten sind, verfügen kriminelle Gruppen zunehmend über professionelle IT-Experten – mit vielen jungen Mitgliedern haben die Organisationen zudem zahlreiche Digital Natives in ihren Reihen, die neue Technologien selbstverständlich nutzen und experimentierfreudig sind.

Auch in Mexiko ist in den letzten Jahren eine starke Professionalisierung im technischen Bereich feststellbar. Mexikanische Kartelle bauen ihre eigenen IT-Teams auf, die etwa Überwachungsnetzwerke installieren, Mobiltelefone und Computer verwanzen oder die Computernetzwerke von Rivalen, Opfern oder Sicherheitskräften hacken. Dafür werden IT-Experten entführt oder angeworben. Teils versuchen Kartelle auch Spezialisten des Militärs zu rekrutieren (Peteranderl 2014, 2019b). *„Sie sind relativ professionell und nutzen gute Systeme, auch wenn sie längst nicht so professionell wie etwa ein Geheimdienst oder das Militär sind“,* sagt die Sicherheitsexpertin Vanda Felbab-Brown vom Washingtoner Think Tank Brookings über die technische Expertise der Kartelle (Peteranderl 2019b); *„Die Technik entwickelt sich, und die Kartelle bringen sich auf den neuesten Stand.“*

Literatur

Alessi, G. (2019). O elo entre Flávio Bolsonaro e a milícia investigada pela morte de Marielle. El Pais. https://brasil.elpais.com/brasil/2019/01/22/politica/1548165508_401944.html. Zugegriffen: 3. Mai 2019.

Aiken, M. et al. (2016). Youth pathways into cybercrime. http://www.ucd.ie/geary/static/publications/Pathways_White_Paper.pdf. Zugegriffen: 10. Aug. 2019.

Bottari, E. (2017). Miliciano é morto após divulgar invasão em transmissão ao vivo. O Globo. https://oglobo.globo.com/rio/miliciano-morto-apos-divulgar-invasao-em-transmissao-ao-vivo-21831877. Zugegriffen: 15. Aug. 2019.

Calderón, L. et al. (2019). 2019 organized crime and violence in Mexico report. University of San Diego. https://justiceinmexico.org/publications/reports/. Zugegriffen: 1. Juni 2019.

Campbell, H. (2014). Narco-propaganda in the Mexican “Drug War”. An anthropological perspective. *Latin American Perspectives, 41*(2), 60–77. https://doi.org/10.1177/0094582X12443519.

Carlos, C. (2019). PF detona esquema de venda de drogas sintéticas realizada pelo WhatsApp. Cerca de 200 pessoas faziam parte do grupo de vendas de drogas dos traficantes no WhatsApp. Diario da Jaragua. https://www.diariodajaragua.com.br/seguranca/pf-detona-esquema-de-venda-de-drogas-sinteticas-realizada-pelo/435163/. Zugegriffen: 5. Aug. 2019.

Center for Strategic and International Studies. (2018). Economic impact of cybercrime – No slowing down. global cybersecurity report. https://www.csis.org/analysis/economic-impact-cybercrime. Zugegriffen: 3. Aug. 2019.

Crime News. (2019). https://crimesnewsrj.blogspot.com. Zugegriffen: 5. Aug. 2019.

Cymrot, D. (2011). A criminalização do funk sob a perspectiva da teoria crítica. Faculdade de Direito da Universidade de São Paulo. www.teses.usp.br/teses/disponiveis/2/2136/tde…/Danilo_Cymrot_ME.pdf. Zugegriffen: 3. Mai 2019.

De Sales Dias, L. (2018). O acesso às mensagens armazenadas em softwares de comunicação de smartphones, frente ao direito à intimidade. Jus. https://jus.com.br/artigos/65639/o-acesso-as-mensagens-armazenadas-em-softwares-de-comunicacao-de-smartphones-frente-ao-direito-a-intimidade. Zugegriffen: 14. Aug. 2019.

Diario Extra. (2017). Grupo de WhatsApp ofrece armas a narcos. https://www.diarioextra.com/Noticia/detalle/340202/grupo-de-whatsapp-ofrece-armas-a-narcos. Zugegriffen: 3. März 2019.

Dittus, M. et al. (2018). Platform criminalism: The ‚Last-Mile‘ geography of the darknet market supply chain. ACM The Web Conference 2018, Lyon. https://arxiv.org/abs/1712.10068. Zugegriffen: 4. Apr. 2019.

Dlmusicas. (2019). Áudios do Tiroteio na Cidade Alta 2018. https://dlmusicas.pw/mp3/audio-de-tiroteio-na-cidade-alta.html. Zugegriffen: 2. Febr. 2019.

Europol. (2016). IOCTA 2016. Internet organised crime threat assessment. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016. Zugegriffen: 15. Aug. 2019.

Facções News. (2019). https://www.youtube.com/channel/UCmmZB48WWbD4UBGdXo-HytAA. Zugegriffen: 2. Aug. 2019.

Freedom House. (2019). Mexico. https://freedomhouse.org/report/freedom-world/2019/mexico. Zugegriffen: 2. Juni 2019.

Frevert, U. (2017). *Die Politik der Demütigung. Schauplätze von Macht und Ohnmacht*. Frankfurt a. M.: Fischer.

Glenny, M. (2012). *CyberCrime. Kriminalität und Krieg im digitalen Zeitalter*. München: DVA.

Gomora, D. (2012). Los cárteles mexicanos usan Facebook para reclutar jóvenes. La DEA para atraparlos. Cosecha Rocha/El Universal. http://cosecharoja.org/los-carteles-mexicanos-usan-facebook-para-reclutar-jovenes-la-dea-para-atraparlos. Zugegriffen: 5. Juni 2019.

Guevara, A. Y. (2013). Propaganda in Mexico's drug war. *Journal of Strategic Security, 6*(5), 131–151. https://doi.org/10.5038/1944-0472.6.3S.15.

Heufelder, J. E. (2011). *Drogenkorridor Mexiko*. Berlin: Transit.

Internet World Stats. (2019). Brazil internet stats and telecom market report. https://www.internetworldstats.com/sa/br.htm. Zugegriffen: 3. Febr. 2019.

Jaroschewski, J. (2015a). Verbrecherjagd per Kurznachricht. Gewalt in Rio de Janeiro. Spiegel Online. https://www.spiegel.de/netzwelt/web/rio-de-janeiro-crowdsourcing-bei-der-verbrecherjagd-a-1052786.html. Zugegriffen: 5. Apr. 2019.

Jaroschewski, J. (2015b). Playboy und der Drogenkrieg von Rio. Stern Online. https://www.stern.de/panorama/stern-crime/getoeter-drogenboss-in-brasilien–playboy-und-der-drogenkrieg-von-rio-de-janeiro-6424274.html. Zugegriffen: 6. Juni 2019.

Jaroschewski, J. (2016). Der Drogenkrieg als Handyvideo. Spiegel Online. https://www.spiegel.de/netzwelt/web/rio-de-janeiro-der-drogenkrieg-als-handyvideo-a-1098605.html. Zugegriffen: 6. Juni 2019.

Jaroschewski, J., & Peteranderl, S. (2014). Social criminals – Dealer, gangs und Kartelle im Internet. Vortrag 05.07.2014. Netzwerk Recherche. https://nr14.sched.com/event/51a8f316f42f76f37722feb628481e1f.

Lee, B. et al. (2019). Mexico's drug war. Council on foreign relations. https://www.cfr.org/backgrounder/mexicos-drug-war. Zugegriffen: 5. Juni 2019.

Leitão, M. (2019). Trafico exibe arsenal em morro da zona norte do Rio. https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/02/03/trafico-exibe-arsenal-em-morro-da-zona-norte-do-rio.ghtml. Zugegriffen: 3. Aug. 2019.

Leyden, J. (2013). Drug gang hacks into Belgian seaport, cops seize Tonne of smack. https://www.theregister.co.uk/2013/06/18/drug_smugglers_using_hackers. Zugegriffen: 6. Feb. 2019

Lusthaus, J. (2018). Is the mafia taking over cybercrime?*. Department of Sociology University of Oxford. https://i.blackhat.com/us-18/Wed-August-8/us-18-Lusthaus-Is-The-Mafia-Taking-Over-Cybercrime-wp.pdf. Zugegriffen: 10. Juli 2019.

Milhorance, F. (2018). The apps that map violence – And keep Rio residents out of the crossfire. The Guardian. https://www.theguardian.com/cities/2018/apr/05/the-apps-that-map-violence-and-keep-rio-residents-out-of-the-crossfire. Zugegriffen: 3. Mai 2019.

Monroy-Hernández, A., & Palacios, L. D. (2014). Blog del Narco and the Future of Citizen Journalism. *Culture & Society*, 85–96. https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/BlogdelNarco.pdf (Summer/Fall 2014).

Muggah, R., & Diniz, G. (2013). Digitally enhanced violence prevention in the Americas. *Stability: International Journal of Security & Development*, *2*(3), 1–23. https://doi.org/10.5334/sta.cq.

Muggah, R., Diniz, G., & Glenny, M. (2014). Deconstructing cyber security in Brazil. Threats and responses. Igarapé Publication. Strategic Paper 11. https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf. Zugegriffen: 2. Juni 2019.

O Globo. (2014). Morre jovem filmada por traficantes durante sessão de tortura em favela da Zona Norte do Rio. https://extra.globo.com/casos-de-policia/morre-jovem-filmada-por-traficantes-durante-sessao-de-tortura-em-favela-da-zona-norte-do-rio-14087762.html. Zugegriffen: 3. Mai 2019.

O Globo. (2018a). Imagens mostram drone usado por traficante para vigilar faccao rival em comunidade da Zona Norte do Rio. https://g1.globo.com/rj/rio-de-janeiro/noticia/imagens-mostram-drone-usado-por-traficante-para-vigiar-faccao-rival-em-comunidade-da-zona-norte-do-rio.ghtml. Zugegriffen: 1. Aug. 2019.

O Globo. (2018b). Planos de Witzel de usar drone que faz disparos em ações policiais no Rio são criticados por especialistas. https://extra.globo.com/noticias/rio/planos-de-witzel-de-usar-drone-que-faz-disparos-em-acoes-policiais-no-rio-sao-criticados-por-especialistas-23209073.html. Zugegriffen: 1. Aug. 2019.

Olliveira, C. (2019). As Ligacoes dos Bolsonaros com as Milícias. The Intercept. https://theintercept.com/2019/01/22/bolsonaros-milicias/. Zugegriffen: 5. Juni 2019.

Peteranderl, S. (2011). *„Leaking secrets, leaking blood". Narcoblogs als Gegenöffentlichkeit in Mexiko*. Unveröffentlichte Masterarbeit. Ludwig-Maximilians-Universität München.

Peteranderl, S. (2013a). Die Sklaven der Kartelle. Zeit Online. https://www.zeit.de/politik/ausland/2013-11/mexiko-migranten-kartelle. Zuegriffen: 7. Juni 2019.

Peteranderl, S. (2013b). Drogenkrieg im Internet. Wie mexikanische Kartelle Facebook und Twitter nutzen. Spiegel Online. https://www.spiegel.de/netzwelt/web/mexikanische-drogenkartelle-image-pr-im-internet-a-940256.html. Zugegriffen: 5. Juni 2019.

Peteranderl, S. (2014). Die Geeks der Kartelle. Zeit Online. https://www.zeit.de/politik/ausland/2014-09/mexiko-drogenkartelle-internet-darknet. Zugegriffen: 5. Juni 2019.

Peteranderl, S. (2015). Mordauftrag per Facebook. In Mexiko wurde ein 14-Jähriger als Killer angeheuert. Wired. https://glocalreporting.com/2015/10/20/mordauftrag-per-facebook-in-mexiko-wurde-ein-14-jaehriger-als-killer-angeheuert. Zugegriffen: 6. Juni 2019.

Peteranderl, S. (2019a). So setzen Kartelle Drohnen als Waffen ein. Spiegel Online. https://www.spiegel.de/netzwelt/netzpolitik/drogenkrieg-in-mexiko-so-setzen-kartelle-drohnen-als-waffen-ein-a-1257400.html. Zugegriffen: 10. Aug. 2019.

Peteranderl, S. (2019b). Spionage im Drogenkrieg. Wie Mexikos Kartelle ganze Städte überwachen. Spiegel Online. https://www.spiegel.de/netzwelt/netzpolitik/mexikos-drogenkrieg-wie-kartelle-ganze-staedte-ueberwachen-a-1268656.html. Zugegriffen: 10. Aug. 2019.

Phillips, B., & Rios, V. (2019). Narco-messages: Competition and public communication by criminal groups. *Latin American Politics and Society.* https://freedomhouse.org/report/freedom-world/2019/mexico (Forthcoming).

Plevin, R., & Ornelas, O. (2019). Mexican cartels turn social media into tools for extortion, violence. Desert Sun. https://www.desertsun.com/in-depth/news/2019/02/27/mexican-drug-cartels-use-social-media-for-extortion-threats-violence-facebook-whatsapp-youtube/2280756002/. Zugegriffen: 3. Apr. 2019.

Proceso. (2013). Cártel del Golfo reparte toneladas de despensas a afectados por ‚Ingrid' en Tamaulipas. https://www.proceso.com.mx/353468. Zugegriffen: 18. Juni 2019.

Procurados. (2019). https://www.procurados.org.br. Zugegriffen: 15. Aug. 2019.

Realidade das Favelas. (2019). https://realidadedasfavelas.blogspot.com/. Zugegriffen: 15. Aug. 2019.

Reyes, I. (2010). Los frentes mediáticos de la guerra contra el narcotráfico en México. BBC Mundo México. https://www.bbc.com/mundo/noticias/2010/11/101117_101117_mexico_violencia_cobertura_medios_debate_irm. Zugegriffen: 15. Aug. 2019.

Sneed, P. M. (2003). *Machine Gun Voices: Favelas and Utopia in Brazilian Gangster Funk. Dissertation University of Wisconsin-Madison*. Seoul: Seoul National University Press.

Spiegel Online. (2016). Erneute WhatsApp-Sperre in Brasilien. https://www.spiegel.de/netzwelt/netzpolitik/whatsapp-erneute-sperre-in-brasilien-a-1103772.html. Zugegriffen: 12. Aug. 2019.

Stuart, S. (2019). Tracking Mexico's Cartels in 2019. Startfor. https://worldview.stratfor.com/article/tracking-mexicos-cartels-2019. Zugegriffen: 8. Juni 2019.

Sullivan, J. P. (2013). Mexican Cartel Strategic Note No. 15: Skullduggery or Social Banditry? Cartel Humanitarian Aid. https://smallwarsjournal.com/blog/mexican-cartel-strategic-note-no-15-skullduggery-or-social-banditry-cartel-humanitarian-aid. Zugegriffen: 12. Juni 2019.

Thompsons, N., & Muggah, R. (2015). Brazil's cybercrime problem. Time to get tough. https://igarape.org.br/en/brazils-cybercrime-problem/. Zugegegriffen: 13.Juni 2019.

United States Department of Justice. (2018). Youth are smuggling drugs on behalf of cartels; law enforcers launch education campaign. https://www.justice.gov/usao-sdca/pr/youth-are-smuggling-drugs-behalf-cartels-law-enforcers-launch-education-campaign. Zugegriffen: 10. Juni 2019.

Wickert, C. (2013). Narcocorridos – Mexikanische Drogenballaden. Criminologia. https://criminologia.de/2013/07/narcocorridos-mexikanische-drogenballaden. Zugegriffen: 13. Aug. 2019.

World Drug Report. (2016). United Nations World Drug Report 2016. https://www.unodc.org/wdr2016/. Zugegriffen: 15. Aug. 2019.

Phänomenologie von digitalen Delikten

Eine Tat- und Täteranalyse von Hackern

Christoph Einzinger

1 Täteranalyse – Hacker

Bei dem Begriff „Hacker“ handelt es sich in der heutigen Zeit um einen negativ behafteten Begriff. Im allgemeinen Sprachgebrauch wird mit Hackern zumeist eine entsprechende Gruppierung verbunden, die in Computersysteme eindringen kann und deren Hauptaugenmerk auf dem monetären Schaden anderer Leute und dem daraus resultierenden eigenen finanziellen Mehrwert liegt. Die ursprüngliche Bedeutung des Wortes „hacking“ könnte dieser Begriffsdefinition nicht ferner sein.

Neben einer Betrachtung des Ursprungs der Hacker und deren Ideologien, soll eine Analyse der Hackerethik und ihrer Kultur an die Thematik heranführen und vermitteln, dass der gemeine Hacker nicht zwangsläufig Straftaten begeht oder in Computersysteme eindringt.

Abschließend werden die einzelnen Ideologien aus kriminologischer Sicht betrachtet und mit medialen Beispielen belegt. Dabei wird herausgestellt, dass die ideologische Ausprägung von Hackern durch bereits bekannte kriminologischen Theorien erklärt werden können, es aber subsidiär wirkende Faktoren, wie beispielsweise die im Internet vorherrschende Anonymität und die allgemeine Zugänglichkeit des Internets einen nicht von der Hand zu weisenden Einfluss innehaben.

C. Einzinger (✉)
Biebelnhein, Deutschland
E-Mail: ChrEinz@web.de

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

T.-G. Rüdiger und P. S. Bayerl (Hrsg.), *Cyberkriminologie,*
https://doi.org/10.1007/978-3-658-28507-4_17

2 Ursprung der Hacker

Seit den 1950er Jahren existiert an der amerikanischen Universität „Massachusetts Institute of Technology“ (MIT) eine studentische Gruppe, die sich mit Modelleisenbahnen bzw. den dazu verwendeten Signalen und Relais beschäftigt (Levy 2010, S. 2). Dort wurde für die kreative Lösung eines herausfordernden Problems der Begriff „hack“ geschaffen (Levy 2010, S. 8). Die Mitglieder dieser Gruppe nannten sich selbst erstmalig „Hacker“ und verbanden mit dem Begriff lediglich einen raffinierten Tüftler mit erheblichem technischem Sachverstand. Mit dieser Intension waren Hacker bis in die 1980er Jahre die treibende Kraft der Entwicklung der Computertechnik und der Distribution von Computern an die breite Masse.

Seit dem Aufkommen der ersten Raubkopierer bzw. „Cracker“ im Jahr 1982 verschwammen die sprachlichen Grenzen zwischen Tüftlern und Tätern immer mehr.

2.1 Differenzierung von Hackern

Bereits bei der Begriffsbestimmung des Hackens ist ersichtlich, dass es sich bei Hackern um Experten im technischen Bereichen handelt. Lediglich ein kleiner Teil dieser Experten missbraucht das erlernte Fachwissen und fügt anderen Schaden zu. Grundsätzlich hängt es also von der Ideologie eines Hackers ab, ob er seine Fachkenntnisse missbraucht oder nutzt. Für den Bereich der IT-Sicherheit differenzieren sich Hacker in drei verschiedene Ideologien.[1]

2.1.1 White Hats

Cybersicherheit und das legale Aufdecken von Sicherheitslücken sind White Hat Hackern wichtiger als der persönliche finanzielle Gewinn. Sie ermitteln Schwachstellen in IT-Systemen und setzen die hinter den Produkten stehenden Firmen über selbige in Kenntnis. Produkte von beispielsweise Microsoft, Google und Co. sollen somit sicherer und die Digitalisierung vorangetrieben werden. Die

[1]Die farbliche Unterscheidung der Ethiken entsprang amerikanischen Western aus den 1920er Jahren. Dort trugen die Protagonisten bzw. Gesetzeshüter weiße Hüte. Die entsprechenden Antagonisten trugen schwarze Kleidung bzw. schwarze Hüte.

Intention eines White Hat Hackers ist es eine noch nicht identifizierte Sicherheitslücke zu entdecken und zu schließen. Die Parallelen zu den Tüftlern des MIT sind hier am prägnantesten (Rouse n. d. a; Symantec n. d.).[2]

2.1.2 Grey Hats

Grey Hat Hacker sind die Robin Hoods der digitalen Welt. Sie nutzen ihre Fachkenntnisse und verfolgen damit höhere Ziele, wie beispielsweise das Publizieren von verschwiegenen Sicherheitslücken in IT-Systemen oder der gewerbliche Betrug ganzer Unternehmen. Ähnlich wie Robin Hood rechtfertigen Grey Hat Hacker das Übertreten der Grenze zur Strafbarkeit mit der Verfolgung eines höherwertigen Ziels. Beispiele für Grey Hat Hacker sind u. a. hacktivistische Gruppierungen wie Anonymous oder LulzSec, die Straftaten begingen, um gegen die Terrororganisation IS oder Pädophile vorzugehen (Rouse n. d. c; Symantec n. d.).

2.1.3 Black Hats

Im Gegensatz zu White Hat oder Grey Hat Hackern, die durch einen ehrbaren Hintergedanken angetrieben werden, verfolgen Black Hat Hacker hauptsächlich destruktive Ziele (Rouse n. d. b; Symantec n. d.).

Bei der kriminologischen Betrachtung von Black Hat Hackern bietet sich eine feinere Untergliederung an, da diese nicht ausschließlich aus monetären Beweggründen angetrieben werden. So können diese in die Bereiche Cybercrime, Cyberterror und Cyberwar untergliedert werden. Das bloße Interesse an „schnellem Geld“ ist markant für den Bereich Cybercrime. Dabei wird keinerlei Rücksicht auf die Opfer genommen und ohne Reue gehandelt. Unter Cyberterror ist das Konzept der reinen Zerstörung zu verstehen. Dem auserkorenen Ziel soll möglichst viel Schaden zugefügt werden. Dabei kann der Beweggrund politisch, religiös oder ideologisch motiviert sein. Davon abzugrenzen sind Black Hat Hacker, die Kombattanten in einem Cyberwar sind. Diese handeln mit staatlichem Auftrag und verfolgen eher selten persönliche Ziele.

[2]Da gemäß Definition von White Hat Hackern keine strafbaren Handlungen vorgenommen werden, wird auf eine kriminologische Betrachtung verzichtet.

3 Die Hackerethik

Im Jahr 1984 veröffentlichte der amerikanische Journalist Steven Levy das Buch „Hackers: Heroes of the Computer Revolution“. Neben der Auflistung der, seiner Meinung nach, „wahren Hacker“ zu denen unter anderem Steve Wozniak[3], John McCarthy[4], Richard Stallman[5] und Fred Moore[6] zählen, prägt er in Kap. „Ist der Begriff „Cyberkriminalität“ in Forschung und Praxis hinreichend konturiert und somit adäquater (Sozial-)Kontrolle zugänglich?“ den Begriff der Hackerethik.

3.1 Hackerethik nach Levy

Die Hackerethik manifestiert sich in sechs Doktrinen, die impulsgebend für das Handeln eines Hackers sein sollen. Nachdem Levy diese publizierte, erachteten viele Hacker diese als Grundsteine der Hackerkultur (Nagenborg und Sell 2016, S. 344):

> „Access to computers – and anything that might teach you something about the way the world works – should be unlimited and total. Always yield to the Hands-On Imperative!“ (Levy 2010, S. 23 f.)

Laut Levy sind Hacker davon überzeugt, dass man etwas über Dinge bzw. die Welt lernen kann, wenn man sie dekonstruiert, die Funktionsweise rekonstruiert und das Erlernte nutzt, um neue interessantere Dinge zu schaffen. Dabei lehnen sie sich gegen jede Person, physische Barriere oder Gesetzgebung auf, die versucht sie daran zu hindern. Den Ursprung dieser These sieht Levy im bereits erwähnten Modellbauclub des MIT. Dort soll es das sog. „Midnight Requisitioning Committee“ gegeben haben. Deren Aufgabe war es, für eigene Projekte benötigte Materialien während Nacht und Nebel zu akquirieren. Dabei spielte es weniger eine Rolle, woher die gewonnenen Materialien stammten. Levy beschreibt, dass es von keinem der sonst sehr gewissenhaften Mitglieder als Stehlen angesehen wurde:

> „All information should be free.“ (Levy 2010, S. 24 f.)

---

[3]Mitbegründer von Apple.

[4]Mitbegründer des MIT Artificial Intelligence Lab.

[5]Gründer der Freien Software Bewegung und Mitbegründer des GNU-Projects.

[6]Mitbegründer des Homebrew Computer Club.

Die zentrale Fragestellung dieses Grundsatzes ist, wie Dinge verbessert werden können, wenn man nicht alle benötigten Informationen besitzt oder Zugriff auf selbige hat. Daher sollten alle Informationen insbesondere Programmcode für jedermann frei zur Verfügung stehen:

> „Mistrust Authority—Promote Decentralization." (Levy 2010, S. 24 f.)

Aufbauend auf den genannten zwei Doktrinen darf, nach der Interpretation von Levy, nichts zwischen einem Hacker und Informationen bzw. Gegenständen, die der Wissensakkumulation dienen, stehen. Inbegriff eines solchen Hindernisses ist die Bürokratie und die Verwaltung durch überdimensionierte Behörden und Unternehmen. Der zur damaligen Zeit größte Kontrahent eines Hackers war das Unternehmen „International Business Machines" (IBM). Aus Sicht von IBM-Mitarbeitern sollte der Zugriff zu Computern streng limitiert und nur den Fähigsten ermöglicht werden. Zudem konterkarierte die von Hackern geforderte Dezentralisation den Unternehmensplan von IBM, da die Computer von IBM als zukunftsweisend und unumgänglich im Bereich der Informatik angesehen wurden. Als Folge dessen formte sich bei vielen Hackern eine Abneigung gegen das Unternehmen IBM, die damit verbundene Autorität und die angestrebte Zentralisierung.

> „Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position." (Levy 2010, S. 26 f.)

Innerhalb der Hackerkultur konnte Ansehen nur durch raffinierte Bedienung der Konsole eines Computers verdient werden. Ein Doktortitel oder sonstige Referenzen wogen weit weniger, als die Vorführung der Fähigkeiten. Hintergrund ist der stetige Drang der Weiterentwicklung von Fähigkeiten und Computern. Dabei konnten Titel weniger erreichen als ausgeklügelte neue Programme.

> „You can create art and beauty on a computer." (Levy 2010, S. 26 f.)

Unter Kunst und Schönheit – im Sinne Levys – ist nicht die Malerei oder Bildhauerei zu verstehen. Kunst und Schönheit bezieht sich auf den Programmcode. In den 1960er Jahren war die limitierende Größe bei der Entwicklung von Programmen die Leistungsfähigkeit des Computers. Daher mussten Programme effizient und mit so wenig Codezeilen wie möglich entwickelt werden. Als Beispiel führt Levy ein Programm auf, das Binärzahlen in Dezimalzahlen umwandelt. Ein unerfahrener Nutzer konnte die Umwandlung mit ca. 100 Codezeilen erreichen. Hoch angesehene Hacker schafften es mit ca. 50 Codezeilen. Dies galt lange Zeit

als apodiktisch beste Lösung des Problems. Als ein Hacker namens Jensen den Algorithmus umschrieb und die Transformation mit 46 Zeilen entwickelte, wurde es ungewöhnlich still in der Hackerkultur. Jensens Code wurde als das Nirvana der Programme angesehen, der Inbegriff von Schönheit.

> „Computers can change your life for the better.“ (Levy 2010, S. 28 f.)

Für viele Hacker war der Computer eine lebensverändernde Erfindung. Er gab ihnen einen neuen Fokus und machte ihr Leben abenteuerlich. Innerhalb von kürzester Zeit waren sie Meister in einem neuen noch größtenteils unerforschten Gebiet. Sie waren fest davon überzeugt, dass Computer auch das Leben anderer zum Besseren verändern konnten, wenn man es nur zuließe.

Computer wie beispielsweise der IBM 7094 kosteten zu der damaligen Zeit mehrere Millionen Dollar und füllten ganze Räume (IBM n. d.). Daher sollten sie nur für aufwendige Rechenoperationen genutzt werden. Die Hacker dieser Zeit wollten Computer aber zu allem nutzen, was ihr Leben einfacher machte. So entstanden die ersten „teuren Taschenrechner“, „teuren Schreibmaschinen“ oder die erste künstliche Intelligenz, die Schach spielt. Hoch angesehene Professoren proklamierten öffentlich, dass ein Computer niemals einen menschlichen Schachspieler schlagen könne. Diese These sahen Hacker als Ansporn (Levy 2010, S. 30 f.).

Das in den beschriebenen Doktrinen inhärente Verhalten kann anhand der Theorie von Becker zu Außenseitern (Becker 2014) und der Neutralisierungsthese von Sykes und Matza (1957) erklärt werden. Hacker in den 1960er Jahren fühlten sich trotz ihrer sozialen Vormachtstellung, durch ein Studium am MIT, als Außenseiter in einer von IBM und Bürokratie dominierten Welt (Levy 2010, S. 24 f.). Sie wurden von den eigenen Professoren für die innovative Nutzung von Computern belächelt und das als deviant angesehene Verhalten wurde geahndet.

Becker beschreibt in seinem 1963 erschienenen Buch „Outsiders“ die Vorgänge, die dazu führen, dass Verhalten von Personen oder Gruppen kriminalisiert wird. Er geht dabei auf Moralunternehmen ein, die den Marihuana-Konsum kriminalisierten. Hier ergeben sich Parallelen zu den Professoren am MIT (Levy 2010). Diese definierten – durch ihre eigenen Ansichten und Moral geprägt – das Verhalten von Hackern als deviant. Die Kriminalisierung erfolgte durch die Ahndung (Vergabe von schlechten Noten) der Nutzung von Computern zu einem nicht etablierten Einsatzzweck. Dies führte dazu, dass Hacker sich als eigene Subkultur sahen, deren Aufgabe es war, sich über bestehende Normen und Werte hinwegzusetzen, gegen Autorität und Bürokratie zu rebellieren und die lebensverändernde Erfindung des Computers der breiten Masse verfügbar zu machen.

Als Manifestation kann u. a. die Ablehnung des Unternehmens IBM und dem Aberkennen von Titeln oder Referenzen, solange die jeweiligen Fähigkeiten nicht bewiesen wurden, gesehen werden. Das Verhalten gipfelt in beispielsweise der kriminellen Beschaffung von Materialien oder dem Beugen von Regeln, um einen Lerneffekt zu erzielen, wobei dieses Verhalten von Hackern nicht als Unrecht angesehen wurde. Diese Technik der Neutralisation wurden 1957 in dem Artikel „Techniques of neutralization: a theory of delinquency“ von Sykes und Matza beschrieben. Nach ihrer Theorie suchen Außenseiter nach einer Rechtfertigung für ihr deviantes Verhalten. Diese Rechtfertigung kann u. a. die Verneinung des Unrechts, also die Verharmlosung bzw. Bagatellisierung des Handelns sein.

3.2 Zusätze des Chaos Computer Clubs

Im September 1981 wurde der Chaos Computer Club (kurz CCC) in Berlin gegründet (CCC n. d. b). Die Intention war es ein Sprachrohr für Hacker in Deutschland zu schaffen und sich zu einer größeren Gruppe zusammenzuschließen. Nachdem zwischen 1985 und 1989 Mitglieder des CCC im Auftrag des KGB weltweit Unternehmen infiltrierten und Informationen verkauften (Zota 2017), erweiterte der CCC die Hackerethik von Levy (CCC n. d. a). Dabei wurde zwei neue Doktrinen verfasst und ein bestehender Punkt ergänzt:

> „Mülle nicht in den Daten anderer Leute.“ (CCC n. d. a)

Während des 35. Chaos Communication Congress (35C3) stellt Frank Rieger die Hackerethik vor (Media CCC.de 2018). Dabei geht er auch auf den Grundsatz *„Mülle nicht in den Daten anderer Leute“* ein. Kern seiner Ausführung ist dabei, dass ein Hacker seine Fähigkeiten nicht missbrauchen sollte. Er stellt dabei eine zentrale Frage, die an Thesen von Kant erinnert: „Was wäre, wenn jemand das Gleiche tun würde, was Du gerade vorhast, nur das Du betroffen wärest?“ Diese Frage soll dazu motivieren, sein eigenes Handeln zu hinterfragen und dabei helfen den schmalen Grat des ethischen Hackens zu beschreiten.

> „Öffentliche Daten nützen, private Daten schützen.“ (CCC n. d. a)

Rieger startet seinen Vortrag mit dem Kernsatz: *„Privatsphäre ist Handlungsfreiheit“*. Es gilt die Privatsphäre und damit verbunden private Daten zu schützen und dennoch den Grundsatz von Levy, dass alle Informationen frei verfügbar sein sollen, zu wahren. Er zeigt auf, dass große Datenkraken wie Facebook und

Google private Daten sammeln und an Höchstbietende verkaufen. Weiterhin appelliert er an Hacker, die Zugriff auf eine große Menge privater Daten haben, damit ethisch umzugehen. Rieger weist auf die Hackerethik-Hotline des CCC hin und rät, dass der Weg des geringsten Schadens für betroffene Personen gewählt wird, aber gleichwohl sichergestellt wird, dass die entsprechende Sicherheitslücke geschlossen wird.

> „Beurteile einen Hacker nach dem, was er tut, [!sic] und nicht nach üblichen Kriterien wie Aussehen, Alter, Herkunft, Spezies, Geschlecht oder gesellschaftlicher Stellung.“ (CCC n. d. a)

Der Grundsatz von Levy, dass Hacker nach ihren Leistungen beurteilt werden sollten und nicht nach den üblichen Kriterien, wird durch den CCC der Zeit angepasst und um das Geschlecht erweitert. Der CCC hat damit in den 1980er Jahren die Emanzipation der Frau im Bereich der Informatik berücksichtigt und in dieser Doktrin vorantreiben wollen.

4 Hacktivismus

Der Neologismus des „Hacktivismus“ setzt sich aus den Worten Hacken und Aktivismus zusammen. Es soll ausgedrückt werden, dass politisch, sozial oder ideologisch motivierter Aktivismus in der digitalen Welt durch Hacker ausgeübt wird. Der Ursprung des Begriffs geht auf die 1984 gegründete Hackergruppierung *Cult of the Dead Cow* (cDc) zurück. Das cDc-Mitglied *Omega* nutze 1998 erstmals in einer E-Mail an cDc-Mitglieder den Begriff des Hacktivismus im Kontext des Hackens und der politischen Befreiung (Delio 2004).

Jordan und Taylor interviewten in ihrem Buch „Hactivism and Cyberwar Rebels with a cause“ ein Mitglied der o. g. Hackergruppe:

> „I know from personal experience that there is a difference between street and on-line protest. I have been chased down the street by a baton-wielding police officer on horseback. Believe me, it takes a lot less courage to sit in front of a computer.“ (Ruffin 2000, Auszug aus dem Interview Jordan und Taylor 2004, S. 80)

Seiner Aussage nach bedarf es wesentlich weniger Mut einen Computer als Protestmittel zu nutzen, als physisch an Protesten teilzunehmen und beispielsweise von Polizisten gejagt zu werden. Hinzu kommt, dass neben der geringeren Schwelle an Protesten teilzunehmen, im Internet eine gewisse Anonymität

herrscht. Diese kann mit entsprechendem Wissen maximiert werden, sodass eine Identifikation des Nutzers nahezu ausgeschlossen ist.

Nach § 17a Abs. 2 Nr. 1 Versammlungsgesetz ist es in Deutschland verboten, an Veranstaltungen unter freiem Himmel – dazu zählen u. a. gewisse Ausprägungen von Demonstrationen – teilzunehmen, wenn die getragene Kleidung die Feststellung der Identität verhindert. Dies soll u. a. die anonyme Begehung von Straftaten und damit Straftaten in einer großen Menschenmasse verhindern. Im Internet kann zwar nicht an einer massenhaften Ansammlung von Menschen teilgenommen werden, dennoch können politisch, sozial oder ideologisch motivierte Ziele demonstriert werden. Dies erfolgt u. a. durch das gezielte Ausschalten von Diensten wie beispielsweise einer Webseite eines Unternehmens durch sogenannte DDOS-Angriffe.[7]

Füllgraf (2016) hat in einer wissenschaftlichen Arbeit zu der Thematik „Hacktivismus“ im Auftrag des Bundeskriminalamts im Jahr 2016 eine analytische Definition geschaffen, die auf die Ziele von Hacktivisten eingeht:

> „Hacktivismus setzt sich aus den Konzepten des Hackings und des Aktivismus zusammen. Die Schnittstelle beider Konzepte erklärt hacktivistische Ausrichtungen. Es handelt sich demnach um ideologisch, sozial und/oder politisch motivierte Aktionen unter Nutzung von Hacking-/IuK-Tools. Computer und Netzwerke sind Tatmittel und Angriffsziele zugleich. Sie werden als Protestmittel zur Verdeutlichung politischer und/oder gesellschaftlicher Ideologien eingesetzt. Die Taten sind nicht profitorientiert, es geht nicht um das missbräuchliche Erlangen von materiellem und/oder finanziellem Gewinn.“ (Füllgraf 2016, S. 6)

4.1 Phänomene des Hacktivismus

Diese Ziele können nur erreicht werden, wenn Hacktivisten aktiv ihre Position ausdrücken. Dazu unterscheidet Füllgraf (2016) in verschiedenen Modi Operandi, die in sechs verschiedenen hacktivistischen Phänomenen gebündelt werden können.

[7]DDOS steht für „Distributed Denial of Service“. Bei einem DDOS Angriff auf bspw. die Webseite eines Unternehmens kann der inhärente Service nicht mehr genutzt werden. Ziel ist es dabei nicht Zugriff zum System zu erlangen, sondern den Service des Servers zu stören.

4.1.1 Defacement[8] von Webseiten

Defacement ist das widerrechtliche Infiltrieren eines Webservers und das anschließende Verändern der Startseite. Bei Hackern ohne politische, soziale oder ideologische Motivation wird die Startseite zumeist mit pornographischem Inhalt gefüllt, um den Inhaber bloßzustellen. Bei Hacktivisten beinhaltet die Startseite nach einem Defacement eine politische Aussage, die Kritik an der gehackten Organisation üben soll. Als Beispiel kann das Defacement der Webseite der CDU-Hessen aus dem Jahr 2002 genannt werden. Dort wurde das Pesthörnchen[9] mit nachfolgender Nachricht hochgeladen:

> „Vielleicht hätten Sie jemanden fragen sollen, der sich damit auskennt – da hilft auch keine Rasterfahndung!“ (Quintessenz 2002)

4.1.2 Parodieren von Webseiten

Hierbei werden Domains[10] angemietet, die der Domain der Zielorganisation zum Verwechseln ähnlich sind. Anschließend wird dort eine satirische Webseite zum Abruf bereitgestellt, die der eigentlichen Webseite nachempfunden ist, jedoch widerläufige und sarkastische Aussagen enthält. Die wohl bekannteste Parodie ist die des WTO aus dem Jahr 1999. Die Hackergruppe ®™ark veröffentlichte die Webseite www.gatt.org (GATT = General Agreement on Tariffs and Trade) und parodierte den Inhalt der Webseite und kritisierte damit die WTO (Walker 2002).

4.1.3 Denial of Service

Bei Denial of Service-Angriffen soll durch fortwährende Anfragen an einen Server der darauf angebotene Service beispielsweise einer Webseite gestört werden. Dadurch kann dem Ziel des DDOS-Angriffs teilweise ein erheblicher finanzieller Schaden entstehen. Im Jahr 2010 antwortete Anonymous auf die Festnahmen eines 16-jährigen Mitglieds mit massenhaften DDOS-Angriffen auf Webseiten der niederländischen Staatsanwaltschaft und Polizei (Spiegel 2010).

---

[8]Defacement: engl. für Entstellen oder Verunstalten.

[9]Ein Logo des CCC, mit dem Kritik an der Deutschen Post geübt werden soll. Die Auseinandersetzung zwischen CCC und der Deutschen Post geht auf den BTx-Hack des CCC aus dem Jahr 1984 zurück.

[10]Vereinfacht: Die Adresse einer Webseite (Erdogan 2014).

4.1.4 Daten-Diebstahl

Daten-Diebstahl hat zum Ziel den häufig unzureichenden Umgang mit IT-Sicherheit eines Unternehmens aufzudecken und so für negative Pressemitteilung bzgl. des Unternehmens zu sorgen. Dazu werden Sicherheitslücken in den Systemen des Ziels ausgenutzt und Daten gestohlen. Diese widerrechtlich erworbenen Daten können anschließend veröffentlicht werden, um je nach Inhalt, weitere negative Pressemitteilungen zu provozieren. So wurde im Jahr 2001, als Protest gegen die Globalisierung, die Datenbank des World Economic Forum (WEF) in der Schweiz gehackt. Die erlangten Daten wurden anschließend an eine Schweizer Zeitung gesandt und enthielten u. a. persönliche Daten von Bill Gates oder Kofi Annan (Matsakis 2016).

4.1.5 Virtuelle Sit-Ins

Bei virtuellen Sit-Ins wird eine Webseite öffentlich demonstriert und ähnlich wie bei DDOS-Angriffen vielfach pro Sekunde aufgerufen. Dabei geschehen die Aufrufe nicht durch sogenannte Bot-Netze[11], sondern durch eine Vielzahl von Protestteilnehmern. Der bekannteste Organisator von virtuellen Sit-Ins ist die Gruppe *Electronic Disturbance Theatre,* die in einem Protest namens „Flood-Net“ Webseiten des damaligen mexikanischen Präsidenten Ernesto Zedillo, der Frankfurter Börse und des US Department of Defense störten (Lecher 2017). Es sind auch Mischformen von virtuellen Sit-Ins und DDOS-Angriffen bekannt. Das Programm Low Orbit Ion Cannon (LOIC) wurde in einer modifizierten Form von Anonymous u. a. im Dezember 2010 dazu genutzt, mit Hilfe von ca. 30.000 Nutzern Webseiten der Firmen Mastercard, Visa, PayPal und PostFinance anzugreifen (Beuth 2012; Schmidt et al. 2010).

4.1.6 Virtuelle Sabotage

Wie der Name bereits suggeriert, wird bei der virtuellen Sabotage ein Ziel beschädigt und dabei eine meist politische Nachricht hinterlassen. Dabei kann das Ausmaß der Beschädigung von Ziel zu Ziel variieren. Der Virus InJustice aus dem Jahr 2001 beispielsweise beschädigte die infizierten Systeme nicht, verbreitete sich aber ähnlich zu bereits bekannter E-Mail Schadsoftware. Nach erfolgreicher Installation des Virus wurde dem Nutzer eine Nachricht angezeigt:

[11]Mit Schadsoftware infizierte IT-Systeme, die meist unter der Kontrolle eines Hackers oder eine Hackergruppierung stehen. Die infizierten Systeme werden dazu genutzt, um massenhaft Anfragen an Dienste eines Servers zu stellen (DDOS) und diesen Dienst zu stören.

> „Do not worry. This is a harmless virus. It will not do anything to your system. The intension [!sic] is to help Palestinian people live in PEASE [!sic] in their own land.“ (Meserve 2001)

Zusätzlich zu der angezeigten Nachricht wurden sechs Pro Palästina Webseiten geöffnet (Meserve 2001).

4.2 Hacktivismus-Gruppierungen

Zu den wohl bekanntesten Hacktivismus-Gruppierungen zählen LulzSec und Anonymous.[12] Die Gruppierung Anonymous formierte sich im Jahr 2004 aus Mitgliedern des Imageboards 4chan und machte es sich fortan zur Aufgabe gegen Zensur im Internet vorzugehen (Olson 2013). Später kamen Ziele wie die Bekämpfung von Terrorismus (BR n. d.), Kinderpornographie (Meusers 2012) oder Rassismus (Woolf 2015) hinzu. Obwohl die hier verfolgten Ziele als ehrbar interpretiert werden könnten – siehe Grey Hat Hacker – stellen die aufgeführten Operationen der Gruppierung strafbare Handlungen dar. Im Laufe des Bestehens von Anonymous wurden die Ziele zunehmend politisch motivierter. Dies veranlasste eine kleinere Gruppe von Anons[13] zu der Gründung von LulzSec[14] im Jahr 2011. Erklärtes Ziel war es, Chaos zu stiften und Spaß zu haben – *„we do it for the lulz“* (Greis 2015). Nach nur 50 Tagen löste sich die Gruppe wieder auf. Mediale Aufmerksamkeit zog LulzSec nach Angriffen auf u. a CIA, US-Senat, Sony, The Sun oder Nintendo auf sich. Fünf der sechs Kernmitglieder wurden mittlerweile teilweise zu mehrjährigen Freiheitsstrafen verurteilt (FBI 2012).

Wie bereits in der Definition des BKA angedeutet, ist das Motiv von Hacktivisten keinesfalls der materielle oder finanzielle Gewinn. Es handelt sich nun mal um eine Fusion des Hackings mit Aktivismus. Daher ist es wenig verwunderlich, dass Motive aus beiden Bereichen erkennbar sind. Als Hauptmotive können politische, soziale oder ideologische Propaganda und Protest genannt werden. Nebenmotive können u. a. Spaß, Rebellion gegen Autorität und Bürokratie oder das Bloßstellen von Akteuren, um den wirtschaftlichen oder politischen Einfluss zu behindern, sein. Ein Erklärungsansatz für das deviante Verhalten kann wie

[12] Auf eine detaillierte Auseinandersetzung mit der Formierung der genannten Gruppen und deren Aktivitäten wird verzichtet. Es wird auf einschlägige Fachliteratur verwiesen.

[13] Mitglieder der Gruppe Anonymous.

[14] Neologismus aus Lulz (abgewandelter Plural von lol = laugh out loud) und Security.

bereits zuvor in der Neutralisationstheorie von Sykes und Matza (1957) gefunden werden. Neben den ursprünglichen fünf Neutralisationstechniken[15] wurden durch Studien von Moore und Dretsch aus dem Jahr 2009 drei weitere Techniken[16] hinzugefügt.

In den Beispielen der bereits vorgestellten Phänomene können Hinweise auf die Ablehnung von Unrecht (siehe InJustice oder Hack der CDU Hessen), die Ablehnung des Opfers (siehe Bekämpfung von Terrorismus, Kinderpornographie und Rassismus durch Anonymous oder das Manifest von LulzSec) und die Verdammung der Verdammenden (siehe DDOS der niederländischen Staatsanwaltschaft und Polizei, FloodNet, Hack des WEF oder WTO) gefunden werden. Bisher existieren jedoch keine empirischen Studien zu angewandten Neutralisationstechniken von Hacktivisten, daher kann die aufgestellte These nicht hinreichend belegt werden.

5 Cyberwar/Cyberkriegsführung

Nach der Definition der Arbeitsgemeinschaft Kriegsursachenforschung (AKUF) ist Krieg ein gewaltsamer Massenkonflikt, an dem mindestens zwei bewaffnete Streitkräfte teilnehmen, von denen mindestens einer im Auftrag einer Regierung handeln muss. Zudem muss ein Mindestmaß an zentralgelenkter Organisation und eine gewisse Kontinuität von bewaffneten Operationen erkennbar sein (Universität Hamburg 2016). Anhand dieser Definition ist der Begriff „Cyberwar“ irreführend und nichtzutreffend. Bei der inhärenten Aussage von Cyberwar handelt es sich eher um Hacker mit staatlichem Auftrag bzw. staatliche Akteure, die u. a. an Kriegen oder bewaffneten Konflikten teilnehmen können. Diese sind nach Motiv und Auswahl von Zielen eindeutig von Hacktivisten oder Cyberkriminellen abzugrenzen (s. a. Kap. „Terrorismus und die Nutzung des Internet“).

Staatliche Hacker handeln mit dem Auftrag, die geopolitische Situation des eigenen Staates zu stärken oder die eines anderen Staates zu schwächen. Als eine der ersten Teilnahmen von staatlichen Hackern an bewaffneten Konflikten, kann das massenhafte Versenden von E-Mails im Jahr 1999 während des Kosovokonflikts gesehen werden (Pollock und Peternsen 1999). Als weiteres Beispiel

[15] 1) Ablehnung von Verantwortung, 2) Verneinung von Unrecht, 3) Ablehnung des Opfers, 4) Verdammung des Verdammenden, 5) Berufung auf höhere Instanzen.

[16] 6) Ablehnung von Schaden, 7) Ablehnung eines Opfers, 8) Alle anderen machen es auch (Bock 2019).

kann der im Jahr 2010 durchgeführte Angriff auf iranische Atomkraftwerke genannt werden. Dort hatten Zentrifugen in der iranischen Atomanlage Natans Fehlfunktionen und zerstörten sich augenscheinlich selbst. Nach einer Analyse gab der damalige iranische Präsident Mahmud Ahmadinedschad bekannt, dass die Supervisory Control and Data Acquisition (SCADA) Systeme durch den Virus Stuxnet infiziert und die Geschwindigkeit der Elektromotoren veränderten wurden. Dies führte zu Fehlfunktionen in den Zentrifugen und teilweise zu der Zerstörung selbiger (Peters 2016). Später wurde gemutmaßt, dass US-Geheimdienste für die Entwicklung des Virus Stuxnet mitverantwortlich waren (dpa 2013; Spiegel 2013).

Stuxnet und der Nachfolger Duqu sind nach einer Studie von Kaspersky (Gostev 2012) die ersten ernstzunehmenden Cyberwaffen der USA, deren erfolgreiche Nutzung zu einer atomaren Katastrophe hätte führen können. Kaspersky nennt in der Studie weitere Cyberwaffen wie Flame oder Gauss, deren erfolgreiche Nutzung erhebliche Auswirkungen hätten. Da bei beiden Cyberwaffen (Flame und Gauss) Ähnlichkeiten im Sourcecode zu Stuxnet bzw. Duqu ersichtlich sind, spricht Kaspersky in der Folge von Cyberkriegsführung und der gezielten Infizierung und Infiltrierung von diplomatischen, militärischen oder wirtschaftlichen interessanten Zielen einer Regierung.

5.1 Staatliche Hackergruppen

Dank der von Edward Snowden durchgesickerten Erkenntnisse zu den Hackern der NSA sind die Fähigkeiten selbiger hinreichend bekannt (Appelbaum et al. 2013). Die USA sind jedoch nicht das einzige Land mit staatlichen Hackern.

Fancy Bear (APT28, STRONTIUM) ist der Name einer russischen Hackergruppe, der nachgesagt wird, mit dem russischen Militärgeheimdienst Glavnoje Razvedyvatel'noje Upravlenije (GRU) zusammenzuarbeiten. Die Gruppe soll u. a. für die Hackerangriffe auf die Demokraten während der US Präsidentschaftswahl im Jahr 2016 verantwortlich sein (Buchert 2017) und bei der Sabotage der Midtermwahlen im Jahr 2018 mitgewirkt haben (FireEye n. d.; O'Flaherty 2018). Zudem soll die Hackergruppierung im Jahr 2015 das Computernetzwerk des Bundestags infiltriert und somit u. a. E-Mails von Bundeskanzlerin Angela Merkel ausspioniert haben (Beuth et al. 2017).

Büro 121 (Electronic Reconnaissance Bureau's Cyber Warfare Guidance Bureau) ist eine nordkoreanische Behörde, die sich mit Cyberkriegsführung auseinandersetzt und für Operation Hidden Cobra (United States Computer Emergency Readiness Team 2017) verantwortlich sein soll. Ihr wird nachgesagt mit der Hackergruppierung Lazarus Group (Guerrero-Saade und Moriuchi 2018; Jun et al. 2015) zusammenzuarbeiten und u. a. für Teile des Sourcecodes der Ransomware WannaCry verantwortlich zu sein (Mjolnir Security 2018). Häufige Ziele von Büro 121 und der Lazarus Gruppe sind südkoreanische Unternehmen bzw. Behörden (United States Computer Emergency Readiness Team n. d.).

Comment Crew (APT1, PLA Unit 61398) ist eine chinesische Gruppierung, die unter der Leitung der chinesischen Peoples Liberation Army (PLA) agieren soll. Diese staatliche Hackergruppierung soll für mehr als 100 Angriffe auf amerikanische Unternehmen verantwortlich sein. Im Jahr 2013 wurde die Gruppierung durch ein amerikanisches Sicherheitsunternehmen enttarnt und ein ausführlicher Bericht zu vergangenen Operationen veröffentlicht (Mandiant 2013).

Die vorgestellten staatlichen Hackergruppierungen bilden nur die Spitze des Eisbergs. Nach dem niederländischen Cyber Security Assessment (CSAN) aus dem Jahr 2018 ist die Gefahr von Cyberangriffen durch staatliche Hackergruppierungen so groß wie noch nie zuvor (National Coordinator for Security and Counterterrorism – Ministry of Justice and Security – Netherlands 2018).

5.2 Völkerrecht und Kombattanten

Sobald Begriffe wie „Krieg“ oder „bewaffneter Konflikt“ im Zusammenhang mit zivilen Kräften wie Hackern genutzt werden, muss zwingend auch das humanitäre Völkerrecht betrachtet werden. Das humanitäre Völkerrecht schützt, nach der Genfer Konvention, Teilnehmer an bewaffneten Kriegshandlungen und nennt diese Kombattanten (Art. 43 ZP I der Genfer Konvention). Der Kombattantenstatus wird jedoch nur Angehörigen von Streitkräften erteilt, die auch als solche erkennbar sind (Art. 44 Abs. 3 ZP I der Genfer Konvention 1977). Dies erfolgt im Regelfall durch das Tragen von Uniformen bzw. das offene Führen von Waffen. Ausnahmen dazu bildet die Haager Landkriegsordnung. Demnach darf sich bei unzureichendem Schutz durch das staatseigene Militär auch die zivile Bevölkerung offen bewaffnen und das Land verteidigen, ohne eine Uniform zu tragen, und trotzdem den Schutzstatus eines Kombattanten innehaben (Art. 1 und 2 der Anlage zur Ordnung der Gesetze und Gebräuche des Landkriegs).

Übertragen auf die aktuelle moderne Kriegsführung bedeutet dies, dass ein staatlicher Hacker bei einem Angriff auf feindliche Infrastruktur eine Uniform tragen muss, um in den Status eines Kombattanten zu gelangen. Sollte die zivile Bevölkerung gemäß der Haager Landkriegsordnung an Kampfhandlungen teilnehmen, so dürfen zivile Hacker nicht digital daran teilnehmen. Das bedeutet, dass ein ebensolcher Hacker sich durchaus bewaffnen darf, jedoch beispielsweise keine Drohne kapern und diese in feindliche Kräfte steuern darf. Jegliche Kampfhandlungen der zivilen Bevölkerung, die gemäß der Haager Landkriegsordnung als Kombattanten geschützt werden wollen, müssen offen ausgetragen werden, andernfalls sind sie als Straftäter anzusehen.

In der Bundesrepublik Deutschland sind Hacker meist als zivile Kräfte bei der Bundeswehr angestellt. Sie sind somit nicht den Streitkräften, die an Kampfhandlungen teilnehmen dürfen, zuzurechnen und zählen somit im Regelfall nicht zu den Kombattanten. Sollten sie dennoch den Status eines Kombattanten benötigen, so werden diese in kürzester Zeit – ähnlich wie bei der Bundeswehr beschäftigte Juristen – zu Soldaten ausgebildet (Pake 2012). Sie werden also „als Kombattanten qualifiziert“ und erhalten anschließend eine Uniform, die während der Verrichtung des Dienstes getragen werden muss (Bundesregierung 2015; Monroy 2015). Wie andere Staaten das Anheben der zivilen Kräfte in den Kombattantenstatus erreichen, ist nicht bekannt.

Wie bereits zu Beginn beschrieben, handeln staatliche Hacker mit einem staatlichen Auftrag und begehen damit – solange sie dem Kombattantenstatus unterliegen – keine in ihrem Land sanktionierbare Straftat. Es ist also der Beruf eines staatlichen Hackers, andere Regierungen oder Organisationen digital anzugreifen bzw. zu sabotieren. Dabei ist die persönliche Motivation des Hackers zur Erfüllung des Auftrags nebensächlich, wobei sie durch politische Einflüsse geprägt häufig der des handelnden Staates entspricht.

5.3 Cyberterror

Von der gezielten digitalen Kriegsführung eines Staates gegen andere Regierungen ist der sogenannte „Cyberterror“ abzugrenzen. Terroristen werden von ideologischen oder religiösen Zielen motiviert und getrieben. Im Jahr 2008 beschrieb Stephen Cummings[17] Cyberterrorismus als Mythos (Trevelyan 2008). Auch im

[17]Direktor des Centre of the Protection of National Infrastructure.

bereits referenzierte CSAN aus dem Jahr 2018 wird die Gefahr von Cyberterrorismus als gering eingeschätzt, da beispielsweise jihadistischen Terrororganisationen das benötigte Fachwissen für ernstzunehmende Cyberangriffe fehlen würde. Nichtsdestotrotz gibt es wissenschaftliche Publikationen, die mit Nachdruck darauf hinweisen, Cyberterrorismus ernst zu nehmen und sich auf eine solche Gefahr vorzubereiten (Cambridge Centre for Risk Studies 2017, S. 33).

5.4 Cybercrime

Wie bereits bei der Begriffsdefinition von Hackern beschrieben, gibt es einen eklatanten Unterschied zwischen Hackern und Crackern. Raymond (2001)[18] beschreibt in seiner Anleitung „How to become a Hacker?“ den Unterschied wie folgt: *„The basic difference is this: hackers build things, crackers break them.“* Hacker – orientiert an den ersten Hackern des MIT – schaffen Dinge, Cracker zerstören sie. Sie versuchen in Computer einzudringen, Telefonnetze zu stören oder Schutzmechanismen zu überwinden, jedoch nicht um diese anschließend an den Hersteller zu melden, sondern vielmehr aus Spaß, Profitgier oder Zerstörungswut. Sie sind Black Hat Hacker bzw. Cyberkriminelle, die für Phishing, Ransomware oder digitale Erpressung verantwortlich sind.

Nach dem Bundeslagebild des BKA aus dem Jahr 2017 sind diese Cyberkriminellen für einen Schaden von ca. 71,4 Mio. EUR, und für 251.617 Fälle (4,4 % aller in der PKS[19] erfassten Straftaten) verantwortlich (Bundeskriminalamt 2017, 2018). Dem gegenüber stehen statistische Berichte von der BITKOM[20] aus dem Jahr 2017 und dem amerikanischen IT-Sicherheitsunternehmen Norton, ebenfalls aus dem Jahr 2017, wonach ca. 43 % der Bevölkerung Opfer von Straftaten wurden – mit dem Tatmittel Internet – und ein Schaden von ca. 2,2 Mrd. EUR entstanden sein soll. Die erhebliche Diskrepanz der offiziell durch Strafverfolgungsbehörden erfassten Straftaten und der durch Unternehmen empirisch ermittelten Zahlen kann lediglich anhand eines enormen Dunkelfeldes erklärt werden. Somit liegt der Schluss nahe, dass nur ein sehr geringer Teil der Straftaten im Bereich Cybercrime bei Strafverfolgungsbehörden angezeigt werden.

[18] US-amerikanischer Autor und Softwareentwickler.

[19] Polizeiliche Kriminal Statistik.

[20] Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. ist der Branchenverband der deutschen Informations- und Telekommunikationsbranche.

5.5 Cybercrime im engeren Sinne

Entsprechend der Definition des BKA wird Cybercrime in zwei Bereiche unterteilt. Cybercrime im engeren Sinne umfasst dabei die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (Bundeskriminalamt n. d.). Dazu zählen im Detail:

- Computerbetrug als Cybercrime im engeren Sinne (§ 263a StGB)
- Sonstiger Computerbetrug (§ 263a Abs. 1 und 2 StGB sowie Vorbereitungshandlungen gem. § 263a Abs. 3 StGB)
- Ausspähen und Abfangen von Daten einschließlich Vorbereitungshandlungen und Datenhehlerei (§§ 202a, 202b, 202c, 202 d StGB)
- Fälschung beweiserheblicher Daten bzw. Täuschung im Rechtsverkehr (§§ 269, 270 StGB)
- Datenveränderung/Computersabotage (§§ 303a, 303b StGB)
- Missbräuchliche Nutzung von Telekommunikationsdiensten (§ 263a StGB)

Nach einer Arbeit von Meier aus dem Jahr 2012 gibt es:

> „keinen Anlass […] davon auszugehen, dass die Internetkriminalität […] anderen Regelmäßigkeiten folgt [!sic] als sie aus der allgemeinen Kriminologie bekannt sind.“ (Meier 2012, S. 197)

Dementsprechend werden bei der Analyse von Cybercrime in der Literatur klassische kriminologische Theorien angewandt:

- Bindungstheorie und Theorie der Selbstkontrolle (Bachmann 2010)
- Lerntheorie (Fisk 2006)
- Neutralisationstheorie (Majid 2005)
- Theorie des rationalen Wahlhandelns (Chiesa et al. 2009)
- Routine-Aktivitätstheorie (Chon und Broadhurst 2014)
- Space Transition Theorie (Jaishankar 2007)

5.6 Cybercrime im weiteren Sinne

Der zweite Bereich der Unterteilung bei Cybercrimedelikten umfasst jede Straftat, bei der als Tatmittel eine Art der Informationstechnik eingesetzt wurde. Dabei werden auch klassische Delikte wie Betäubungsmittelkriminalität, Verstöße

gegen das Urheberrecht oder Kinderpornografie erfasst. Somit werden auch Delikte in Darknetmarktplätzen oder Underground Economy Foren erfasst (s. a. Kap. „Strafverfolgung digital“, „Darknet – die dunkle Seite des Internets?“ und „Von der Straße ins Netz“). Dort werden neben bspw. Betäubungsmitteln und Kreditkartendaten auch Dienste wie Crime as a Service (CaaS) angeboten. Basierend auf dem Cloud Modell Software as a Service (SaaS), bei dem Kunden die Software online nutzen können[21], wird bei CaaS die Begehung von Straftaten (u. a. mieten von Ransomware oder DDOS-Angriffe) outsourced (Krempel 2016). Es ist wenig verwunderlich, dass der Anteil an Delikten in diesem weiter gefassten Bereich deutlich höher ist.

Bei Cybercrime im weiteren Sinne handelt es sich um Delikte, deren Begehung bereits seit langer Zeit bekannt ist. Lediglich der Modus Operandi hat sich durch das Tatmittel Internet geändert. Bei einer kriminologischen Analyse können also alle bekannten Theorien angewandt werden.

6 Differenzierung

Es konnte aufgezeigt werden, dass die kriminologische Erklärung delinquenten Verhaltens von rechtswidrig agierenden Hackern immens von deren Ideologie abhängt (s. a. Kap. „Identitätsbildung im digitalen Zeitalter“). Dabei konnte herausgestellt werden, dass das Handeln von Grey Hats, zu denen ein Großteil der Hacktivisten zählen, durch Neutralisationstechniken von Sykes und Matza erklärt werden können.

Bei Black Hats hingegen gilt es zu differenzieren, da hier unterschiedliche Ideologien aufeinandertreffen. Das Handeln eines klassischen cyberkriminellen Hackers kann mit ebenfalls klassischen kriminologischen Theorien erklärt werden. Dabei gibt es einige multiplikativ wirkende Faktoren, wie z. B. die Space Transition Theory von Jaishankar (2007). Die im Internet und speziell im Darknet vorhandene Anonymität – und damit verbunden auch flexible und austauschbare Identitäten – senken die Schwelle zu delinquentem Verhalten.[22] Staatliche

[21]Beispielsweise Google Docs.

[22]Eine wissenschaftliche Studie von Rost und Stahel aus dem Jahr 2016 zeigt auf, dass die im Internet herrschende Anonymität kein förderlicher Faktor für die Häufigkeit von sogenannten Trollen ist. Diese Studie bezieht sich jedoch speziell auf aggressive Kommentare in Social Media Beiträgen und kann daher nicht standardmäßig auf im Darknet befindliche Straftäter oder gar Grey oder Black Hats angewandt werden.

Hacker hingegen handeln mit einem Auftrag, der durchaus der Ideologie des Hackers entsprechen kann, jedoch nicht muss. Demgegenüber stehend, handeln Cyberterroristen durch ideologisch oder religiös motivierte Ziele. Doch in diesem Farbenspiel der Cyberaktivisten und Cyberkriminellen zeigt sich deutlich, dass Hacker nicht gleich Cracker ist, diese nicht grundsätzlich Straftäter sind und eine Unterscheidung der Graustufen lohnend ist, da ethische Hacker proaktiv die Sicherheit in IT Systemen fördern.

Literatur

Appelbaum, J., Horchert, J., & Stöcker, C. (29. Dezember 2013). *Spiegel*. https://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html.

Bachmann, M. (2010). The risk propensity and rationality of computer hackers. *International Journal of Cyber Criminology, 4,* 643–656.

Becker, H. S. (2014). *Außenseiter: Zur Soziologie abweichenden Verhaltens*. Frankfurt a. M.: Springer VS.

Beuth, P. (14. Juni 2012). *Zeit Online*. https://www.zeit.de/digital/internet/2012-06/bka-razzia-gema-anonymous.

Beuth, P., Biermann, K., Klingst, M., & Stark, H. (11. Mai 2017). *Zeit*. https://www.zeit.de/2017/20/cyberangriff-bundestag-fancy-bear-angela-merkel-hacker-russland.

BITKOM. (10. Oktober 2017). *Bitkom.* https://www.bitkom.org/Presse/Presseinformation/Cybercrime-Jeder-zweite-Internetnutzer-wurde-Opfer.html. Zugegriffen: 10. März 2019.

Bock, M. (2019). *Kriminologie* (5. Ausg.). München: Vahlen.

BR. (n. d.). *BR*. https://www.br.de/puls/themen/welt/anonymous-greift-is-an-und-hackt-hunderte-twitter-accounts-100.html.

Buchert, H. (10. März 2017). *Zeit*. https://www.zeit.de/politik/ausland/2017-03/donald-trump-russland-us-wahl-einfluss-hacker-wikileaks/seite-2.

Bundeskriminalamt. (2017). *BKA*. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2017.pdf?__blob=publicationFile&v=4.

Bundeskriminalamt. (27. September 2018). *Bundeskriminalamt*. https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html;jsessionid=9247D6333B20468CE076528B99E57826.live0602.

Bundeskriminalamt. (n. d.). *Bundeskriminalamt*. https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html.

Bundesregierung. (6. Februar 2015). *Bundestag.* http://dip21.bundestag.de/dip21/btd/18/039/1803963.pdf.

Cambridge Centre for Risk Studies. (2017). *Cambridge Centre for Risk Studies.* https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/pool-re-cyber-terrorism.pdf.

Chaos Computer Club e. V. (n. d. a). *CCC*. https://www.ccc.de/de/hackerethik. Zugegriffen: 03. März 2019.
Chaos Computer Club e. V. (n. d. b). *CCC*. https://www.ccc.de/de/club.
Chiesa, R., Ducci, S., & Ciappi, S. (2009). *Profiling hackers. The science of criminal profiling as applied to the world of hacking*. Boca Raton: Auerbach Publication.
Chon, S., & Broadhurst, R. (2014). *SSRN*. https://www.ssrn.com/abstract=2379201.
Delio, M. (14. Juli 2004). *Wired*. https://web.archive.org/web/20160103174237/http://archive.wired.com/techbiz/it/news/2004/07/64193. Zugegriffen: 4. März 2019.
Digitalwelt. (n. d.). *Digitalwelt*. https://www.digitalwelt.org/themen/hackerethik/der-begriff-hacker. Zugegriffen: 3. März 2019.
dpa. (28. 06 2013). *Heise*. https://www.heise.de/newsticker/meldung/Stuxnet-Berichte-ueber-weiteren-Geheimnisverrats-Fall-in-den-USA-1902235.html.
Erdogan, J. (13. November 2014). *Spiegel*. http://www.spiegel.de/einestages/btx-hack-1984-angriff-der-ccc-hacker-gegen-die-bundespost-a-1002443.html.
FBI. (2012). *FBI*. https://archives.fbi.gov/archives/newyork/press-releases/2012/six-hackers-in-the-united-states-and-abroad-charged-for-crimes-affecting-over-one-million-victims.
FireEye. (n. d.). *FireEye*. https://www.fireeye.com/current-threats/apt-groups/rpt-apt28.html?utm_source=FEcom&utm_campaign=intel-apt28&utm_medium=ctireports.
Fisk, N. (13. November 2006). *Scholarworks*. https://scholarworks.rit.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=5134&context=theses.
Füllgraf, W. (2016). *BKA*. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/Forschungsergebnisse/2016HacktivistenqAbschlussbericht.html. Zugegriffen: 4. März 2019.
Genfer Konvention. (8. Juni 1977). Zusatzprotokoll zu den Genfer Abkommen vom 12. August 1949 über den Schutz der Opfer internationaler bewaffneter Konflikte. Genf.
Gostev, A. (18. Dezember 2012). *Securelist*. https://securelist.com/kaspersky-security-bulletin-2012-cyber-weapons/36762/.
Greis, F. (11. Februar 2015). *Golem*. https://www.golem.de/news/studie-zu-hacktivisten-bka-sieht-naehe-zu-cyberterrorismus-1502-112299.html. Zugegriffen: 4. März 2019.
Guerrero-Saade, J., & Moriuchi, P. (16. Januar 2018). *Recorded Future*. https://web.archive.org/web/20180116170903/https://www.recordedfuture.com/north-korea-cryptocurrency-campaign/.
IBM. (n. d.). *IBM FAQ*. https://www.ibm.com/ibm/history/reference/faq_0000000011.html.
Jaishankar, K. (2. Juli 2007). *Cybercrimejournal*. http://www.cybercrimejournal.com/Editoriaijccjuly.pdf. Zugegriffen: 10. März 2019.
Jordan, T., & Taylor, P. A. (2004). *Hacktivism and cyberwar*. Rebels with a cause: Routledge.
Jun, J., LaFoy, S., & Sohn, E. (2015). *North Korea's cyber operations – Strategy and response*. CSIS – Center for Strategic International Studies.
Krempel, S. (05. Oktober 2016). *Heise*. https://www.heise.de/newsticker/meldung/Europol-warnt-vor-Crime-as-a-Service-aus-der-Cloud-3341301.html.
Lecher, C. (14. April 2017). *The Verge*. https://www.theverge.com/2017/4/14/15293538/electronic-disturbance-theater-zapatista-tactical-floodnet-sit-in.
Levy, S. (2010). *Hackers: Heroes of the computer revolution – 25th anniversary edition*. Beijing: O'Reilly.

Majid, Y. (2005). Computer hacking: Just another case of juvenile delinquency? *Howard Journal of Criminal Justice, 44,* 387–399.

Mandiant. (2013). *Mandiant.* https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf. Zugegriffen: 5. März 2019.

Matsakis, L. (1. Februar 2016). *Motherboard*. https://motherboard.vice.com/en_us/article/kb78kn/15-years-ago-hackers-attacked-davos-in-one-of-the-first-acts-of-hacktivism-world-economic-forum.

Media CCC.de. (27. Dezember 2018). *Youtube*. https://www.youtube.com/watch?v=OBFJiUG9IgU. Zugegriffen: 3. März 2019.

Meier, B.-D. (2012). Sicherheit im Internet. Neue Herausforderungen für Kriminologie und Kriminalpolitik. *Monatsschrift für Kriminologie und Strafrechtsreform, 95*(3), 184–204.

Meserve, J. (20. März 2001). *CNN*. http://edition.cnn.com/2001/TECH/internet/03/20/injustice.virus.idg/index.html.

Meusers, R. (10. Juli 2012). *Spiegel*. http://www.spiegel.de/netzwelt/web/anonymous-hat-ein-neues-ziel-paedophile-a-843549.html.

Mjolnir Security. (30. Mai 2018). *Mjolnir Security*. https://mjolnirsecurity.com/north-korean-malicious-cyber-activity-hidden-cobra-joanap-backdoor-trojan-and-brambul-server-message-block-worm/.

Monroy, M. (12. Februar 2015). *Netzpolitik*. https://netzpolitik.org/2015/bundeswehr-darf-nach-ansicht-der-bundesregierung-bei-deutschen-cyberangriffen-deren-herkunft-verschleiern/.

Moore, R., & Dretsch, E. (2009). Neutralizations and rationalizations of digital piracy: A qualitative analysis of university students. *International Journal of Cyber Criminology, 3*(1), 441–451.

Nagenborg, M., & Sell, S. (2016). Hackerethik. In J. Heesen (Hrsg.), *Handbuch Medien- und Informationsethik* (S. 344–351). Stuttgart: J.B. Metzler.

National Coordinator for Security and Counterterrorism – Ministry of Justice and Security – Netherlands. (2018). *NCSC*. Abgerufen am 05. 03 2019 von CSAN: https://www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/cyber-security-assessment-netherlands/cyber-security-assessment-netherlands-2018/1/cyber_security_assessment_netherlands_2018.pdf.

Norton by Symantec. (2017). *Symantec*. https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf. Zugegriffen: 10. März 2019.

O'Flaherty, K. (23. August 2018). *Forbes*. https://www.forbes.com/sites/kateoflahertyuk/2018/08/23/midterm-election-hacking-who-is-fancy-bear/#16c336322325.

Olson, P. (2013). *We are anonymous: Inside the hacker world of LulzSec, anonymous, and the global cyber insurgency*. New York: Little, Brown and Company.

Pake, S. (25. Januar 2012). *Legal Tribune Online*. https://www.lto.de/recht/job-karriere/j/juristen-bei-der-bundeswehr-vergaberecht-in-flecktarn/.

Peters, R. (31. August 2016). https://www.n-tv.de/leute/film/Die-scharfe-Cyber-Atombombe-im-Iran-article18535516.html.

Pollock, E., & Petersen, A. (8. April 1999). *The Wallstreet Journal*. http://www.dragomirdimitrijevic.rs/media/wsj.pdf.

Quintessenz. (29. Dezember 2002). *Quintessenz*. http://www.quintessenz.org/cgi-bin/index?funktion=view&id=000100002372.

Raymond, E. S. (2001). *Catb*. http://catb.org/~esr/faqs/hacker-howto.html.

Rost, K., & Stahel, L. (17. Juni 2016). *PLOS*. https://journals.plos.org/plosone/article?id=10.1371%2Fjournal.pone.0155923.

Rouse, M. (n. d. a). *TechTarget – Search Security*. https://searchsecurity.techtarget.com/definition/white-hat.

Rouse, M. (n. d. b). *TechTarget – Search Security*. https://searchsecurity.techtarget.com/definition/black-hat.

Rouse, M. (n. d. c). *TechTarget – Search Security*. https://searchsecurity.techtarget.com/definition/gray-hat.

Schmidt, J., Kuri, J., & Janssen, J.-K. (9. Dezember 2010). *CT*. https://www.heise.de/ct/artikel/Operation-Payback-Proteste-per-Mausklick-1150151.html.

Spiegel. (10. Dezember 2010). *Spiegel*. http://www.spiegel.de/netzwelt/netzpolitik/cyber-kampf-um-wikileaks-angriff-auf-die-angreifer-a-733972.html.

Spiegel. (28. Juni 2013). *Spiegel*. http://www.spiegel.de/politik/ausland/us-general-james-cartwright-soll-stuxnet-virus-verraten-haben-a-908298.html.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Association, 22,* 664–670.

Symantec. (n.d.) What is the difference between black, white and gray hat hackers? https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html.

Trevelyan, M. (16. April 2008). *Reuters*. https://www.reuters.com/article/us-security-cyber-space/security-experts-split-on-cyberterrorism-threat-idUSL1692021220080416?feedType=RSS&feedName=technologyNews.

United States Computer Emergency Readiness Team. (kein Datum). *United States Computer Emergency Readiness Team*. https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity.

United States Computer Emergency Readiness Team. (13. Juni 2017). *United States Computer Emergency Readiness Team*. https://web.archive.org/web/20180121184131/https://www.us-cert.gov/ncas/alerts/TA17-164A.

Universität Hamburg – Professur Politikwissenschaften. (1. September 2016). *Universität Hamburg*. https://www.wiso.uni-hamburg.de/fachbereich-sowi/professuren/jakobeit/forschung/akuf/kriegsdefinition.html.

Walker, A. (24. Mai 2002). *BBC*. http://news.bbc.co.uk/2/hi/business/2006536.stm.

Woolf, N. (6. November 2015). *The Guardian*. https://www.theguardian.com/technology/2015/nov/06/anonymous-ku-klux-klan-name-leak.

Zota, V. (12. September 2017). *Heise*. https://www.heise.de/newsticker/meldung/Zahlen-bitte-CCC-Virtueller-Bankraub-fuer-134-634-88-DM-3824653.html.

Identitätsbildung im digitalen Zeitalter

Hacking und der Labeling Approach

Martina Althoff, Wytske van der Wagen und René van Swaaningen

1 Einleitung

Heutzutage wird Hacking vor allem kriminalisiert. Insbesondere in den Medien werden Hacker[1] als *Vandalen* dargestellt oder als Urtyp eines *Kriminellen* beschrieben. Das war nicht immer so. In den 1960er und 70er Jahren genossen Hacker viel Ansehen; sie galten als geschickte technologische *whizzkids,* die über magische Kräfte verfügen. Wie kam es zu dieser veränderten Wahrnehmung? Ist diese das Ergebnis einer moralischen Panik über Hacker oder Hacking, und falls ja, wer waren die Moralunternehmer? Und kann die Entwicklung des Phänomens Hacking als Schulbeispiel für die soziale Konstruktion von Kriminalität und den Etikettierungsprozess verstanden werden (Steinmetz 2015; Yar 2005; s. a. Kap. „Phänomenologie von digitalen Delikten“)?

[1]Aus Platzgründen und zugunsten der Lesbarkeit wird im Folgenden auf eine inklusive Schreibweise, was Personen- oder Funktionsbezeichnungen betrifft, verzichtet. Die Leser*innen mögen diese freundlicherweise jeweils mitdenken.

M. Althoff (✉)
Rijksuniversiteit Groningen, Groningen, Niederlande
E-Mail: m.althoff@rug.nl

W. van der Wagen · R. van Swaaningen
Erasmus Universiteit Rotterdam, Rotterdam, Niederlande
E-Mail: vanderwagen@law.eur.nl

R. van Swaaningen
E-Mail: vanswaaningen@law.eur.nl

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

T.-G. Rüdiger und P. S. Bayerl (Hrsg.), *Cyberkriminologie,*
https://doi.org/10.1007/978-3-658-28507-4_18

Eine Frage, die sich in diesem Zusammenhang stellt, ist, wie Hacker sich selbst und ihre Aktivitäten beschreiben. Wie erfahren sie die gesellschaftlichen Zuschreibungen? Wie nehmen Hacker sich selbst und andere Hacker wahr? Fühlen sie sich stigmatisiert und falls ja, behindert dies ihre Entwicklung als gesetzestreuer Bürger?

Die Bedeutung derartiger Zuschreibungen und der gesellschaftlichen Etikettierung von Hackern für die Betroffenen ist kaum erforscht. Eine der wenigen empirischen Studien – die von Turgeman-Goldschmidt (2008) – zeigt, dass Etikettierungsprozesse bei Hackern anders als beim klassischen Außenseiter von Becker (1963) funktionieren. Hacker – als „anders" etikettiert – versetzen sich gegen das Stigma des Kriminellen, erfahren ansonsten aber kaum negative Gefühle, unabhängig davon ob sie sich selbst als „good" oder „bad guys" sehen. Ungeachtet der negativen Zuschreibungen, betrachten sie sich als sogenannte positive Deviante, die über einzigartige Fähigkeiten verfügen. Eine interessante und kriminologisch relevante Frage ist dann, inwiefern der traditionelle Etikettierungsansatz, der sogenannte *Labeling Approach* (Becker 1963; Goffman 1959, 1963), der sich vor allem auf die negativen Implikationen der Zuschreibungen (negatives Selbstbild, sekundäre Devianz und soziale Ausschließung) richtet, auch anwendbar und von Bedeutung ist für das *Verstehen* des Phänomens Hacking.

Auf den ersten Blick scheint diese Frage möglicherweise etwas ungewöhnlich; schließlich stammen die symbolisch-interaktionistischen Theorien aus dem prä-digitalen Zeitalter und wurden zudem in einer Zeit entwickelt, in der soziale Gruppen und Gemeinschaften sich eher lokal definierten, und Identitäten viel weniger fluide und hybride waren (Bauman 2000; Turkle 2005). Eigene Forschung (Van der Wagen und Pieters 2015), die sich auf die nicht-menschlichen Akteure und auf mögliche Cyborg-Dimensionen richtet, macht jedoch die Bedeutung von Zuschreibungsprozessen sichtbar. Vor allem in unseren Interviews mit Hackern zeigt sich, wie stark gesellschaftliche Etikettierungen die Art und Weise, wie Hacker sich selbst definieren und der Wirklichkeit Bedeutung zuschreiben, beeinflussen. Eine Frage, die sich hieraus ergibt, ist, ob der Labeling Approach im digitalen Zeitalter noch immer von Bedeutung ist und inwiefern er eines digitalen Impulses bedarf. Hat die Etikettierung als „Hacker" bei den Betroffenen möglicherweise einen weniger stigmatisierenden Effekt wie bei anderen Außenseitern, hat sie vielleicht sogar einen eher positiven Effekt oder spielen hier ganz andere Prozesse eine Rolle für die Identitätsbildung? Und falls ja, wie lässt sich Identitätsbildung im digitalen Zeitalter dann erklären?

In dem hier vorliegenden Beitrag wollen wir diesen Fragen auf der empirischen Grundlage von Interviews, die mit Hackern geführt wurden und der (qualitativen) Analyse einer kleinen Anzahl von Strafakten, nachgehen. Ziel

dieses Kapitels ist es, Etikettierungsprozesse am Beispiel einer kleinen aber diversen Gruppe von Hackern zu explorieren. Im Anschluss hieran soll die Frage beantwortet werden, inwiefern der Etikettierungsansatz im digitalen Zeitalter noch relevant ist. Schließlich soll in einem letzten Schritt diskutiert werden, welche Bedeutung die Technologie für das Verstehen von Hacking hat und welche Konsequenzen hiermit für die kriminologische Theoriebildung verbunden sind.

Zunächst folgt eine kurze Übersicht zum Stand der Forschung über Hacking und eine Diskussion der Etikettierungstheorie. Anschließend werden das empirische Material vorgestellt und die Ergebnisse seiner Analyse besprochen. Dabei richtet sich der Fokus auf drei Aspekte der Identitätsbildung: 1) Wie denken Hacker, dass sie durch die Außenwelt wahrgenommen werden; 2) wie sehen sie sich selbst; und 3) wie sehen sie ihre eigene Rolle innerhalb und außerhalb der Hackergemeinschaft? Die Erklärungskraft des Labeling Approach für diese spezifische Gruppe von (digitalen) Außenseitern wird anschließend diskutiert. Schließlich stellt sich zum Schluss die Frage, inwieweit die Bedeutung, die Hacker selbst dem Phänomen Hacking zuschreiben, im Kontext ihrer spezifischen Beziehung zur Technologie zu begreifen ist. Inwiefern bestimmen ihre technologischen Interaktionen ihre devianten Handlungen, ihre Wahrnehmungen und ihre Intentionen?

2 Hacker: vom „Helden“ zum „Verbrecher“

„It was only a matter of time before they started to believe themselves as bad as they sounded. And no time at all before everyone else did.“ (Barlow, in: Skibell 2002, S. 347).

In den 1960er und 1970er Jahren, auch das goldene Zeitalter der Hacker genannt (Blankwater 2011; Halbert 1997), galten Hacker als „Helden“ des Cyberspace (Levy 1984) oder als technologische *whizzkids,* die die Möglichkeiten der Computertechnologie erkunden. Hacker beschäftigten sich damals vor allem mit der Verbesserung und Entwicklung (bestehender) Hard- und Software und entwickelten neue Algorithmen und Anwendungen, die wiederum in die folgende Computergeneration integriert wurden (Halbert 1997; Jordan 2008; Nissenbaum 2004). Von finanziellem Gewinn war hier keine Rede (Halbert 1997). In jener Zeit bezog sich Hacking nicht auf den „unbefugten Zugriff“ auf Systeme (woran wir vor allem gegenwärtig denken), sondern darauf, neue Wege zu finden, um Probleme oder Hindernisse innerhalb von Systemen zu lösen. Der „Hack“ verwies auf ein Spielen mit „dem System“ (Blankwater 2011).

Hacker erforschten die Computersysteme von Dritten, jedoch mit dem Ziel hiervon zu lernen und dieses Wissen anschließend mit anderen zu teilen. Das Beschädigen von Systemen wurde als inkompetent und unethisch betrachtet (Yar 2005). Hacker waren damals stark ihrer eigenen Ethik verhaftet, die eine antiautoritäre Haltung, eine deutliche Befürwortung des freien Zugangs zu Informationen (einschließlich Computerprogrammen) und die Bedeutung von Computern in Bezug auf Kunst und Schönheit betonte (vgl. Levy 1984). Sie waren eine Art Mikro-Gesellschaft mit einer eigenen Ideologie, eigenen Regeln und Werten (Blankwater 2011, S. 41). Obwohl Hacker nicht zum Mainstream-Establishment gehörten, wurden sie toleriert. Sie galten als Mitglieder einer bestimmten Subkultur und wurden für ihre Fähigkeiten im Umgang mit Computern bewundert (Nissenbaum 2004). Im Laufe der Zeit, seit den 1980er und vor allem seit den 1990er Jahren, wich diese Bewunderung Angst und Abneigung. Hacker wurden zunehmend als „Kriminelle", „gefährliche Anarchisten" oder „Terroristen" betrachtet (Halbert 1997; Nissenbaum 2004; Skibell 2002). Für diese Umkehrung des Bildes vom Hacker werden in der Literatur verschiedene Erklärungen gegeben.

Eine erste Erklärung bezieht sich darauf, dass der Begriff „Hacking" ebenso wie die Hackergemeinschaft selbst sich über die Zeit hinweg verändert hat (Nissenbaum 2004). So entstand schon im Laufe der 1970er Jahre eine zweite Generation Hacker, die viel Geld mit Computertechnologie verdienen wollte und das Kopieren von Software als „Diebstahl" qualifizierte. Bill Gates, einer der bekanntesten Hacker dieser zweiten Generation, wurde diesbezüglich auch durch die erste Generation, für die individueller Reichtum kein Motiv bzw. Ziel war, als Verräter gesehen. Er trug dazu bei, dass Eigentumsrechte und Patente im Zusammenhang mit Software zum Big Business wurden, was im Widerspruch zur klassischen Hacker-Ethik stand (Blankwater 2011). Auch Apple basierte sich ursprünglich auf die Ethik des Hackers (z. B. im Hinblick auf die offene Struktur), entwickelte sich aber nach und nach zu einer Firma, die sich für das große Geschäft interessierte (Blankwater 2011). Zugleich schritt die Technologie in dieser Zeit enorm voran (man denke nur an den Aufstieg von Telekommunikations- und Computernetzwerken); Computer wurden allgemein zugänglich und vermarktet (Levy 1984; Turgeman-Goldschmidt 2008). In den 1980er Jahren tauchte eine dritte Generation von Hackern auf, die versuchte Systeme zu knacken *(cracken)* oder Computersysteme zu sabotieren. In dieser Zeit wurde der einflussreiche Hackerfilm *War Games,* in dem ein rebellischer Teenager versucht, in Computersysteme einzudringen, enorm populär und inspirierte junge Hacker (Blankwater 2011). Obwohl diese Gruppe von Hackern das Hacken völlig anders interpretierte, war

ihre Berufsethik immer noch der der früheren Hackergenerationen sehr ähnlich (Halbert 1997; Turgeman-Goldschmidt 2008). Die Zunahme der digitalen Einbrüche führte jedoch zu der Notwendigkeit einer besseren Sicherheit der Systeme und Netze (Blankwater 2011; Nissenbaum 2004).

Eine zweite Erklärung für die Umkehrung des Hacker-Bildes hängt mit der oben beschriebenen Kommerzialisierung des Internet und der damit einhergehenden und zunehmenden Bekämpfung von Cyberkriminalität zusammen, sowie dem problematischen Konfliktverhältnis zwischen Hackern und der Computerindustrie (vgl. Skibell 2002; Taylor 1999; Yar 2005). Taylor (1999), der in den 1990er Jahren das Phänomen des Hackens erforschte (und hierfür Hacker interviewte), erklärt das negative Bild des Hackers in dieser Zeit vor allem als eine Folge der konflikthaften Beziehung zwischen dem „Hacker-Untergrund" und der aufstrebenden Computerindustrie. War die Computerindustrie anfangs noch begierig darauf, mit Hackern zusammen zu arbeiten, weil es ihr selbst an Wissen und praktischer Erfahrung mangelte, zögerte sie letztendlich, diese Zusammenarbeit anzugehen. Letztendlich hat, so Taylor (1999), das Stigma, dass Hackerinformationen zugewiesen bekamen, zu einer weiteren Kriminalisierung und Marginalisierung von Hackern in dieser Zeit geführt, wobei nicht unterschieden wurde zwischen „verantwortlichen Hackern" und sogenannten „Vandalen". *Alle* Hacking-Aktivitäten wurden jetzt als kriminell etikettiert. Die Sicherheitsindustrie hat demnach eine große Rolle gespielt bei der Bildung von negativen Einstellungen gegenüber bzw. dem negativen Diskurs über Hacker (vgl. auch Churchill 2016).

Eine dritte Erklärung bezieht sich auf die Rolle der Medien und Filme, in denen Hacker als pathologisch, computersüchtig oder gefährliche *Nerds* dargestellt werden (vgl. Halbert 1997; Jordan und Taylor 1998; Nissenbaum 2004). Während in Filmen wie *War Games* aus dem Jahr 1983 Hacker noch romantisiert (Halbert 1997) oder als diejenigen dargestellt werden, die den Staat überlisten, werden Hacker in späteren Filmen zunehmend als „gefährliche Cyberkriminelle" präsentiert (Wall 2008). Eine Illustration der Vielfältigkeit dieser negativen Zuschreibungen liefert Thomas (in: Blankwater 2011, S. 54) mit einer Auswahl von Labels aus Zeitungen und Fernsehsendungen der 80er Jahre in den USA:

> Modem-Macho Übeltäter – elektronischer Hausfriedensbrecher – durchgeknallte Kinder, die sich dem Unfug verschrieben haben – elektronische Vandalen – Saboteure – Monster – Geheimgesellschaft Krimineller – böswillige, böse, böse Täter, die die Bildschirme von Amateur-Computer-Nutzern mit Pornografie füllen – Schädlinge – Bastarde – High-Tech-Straßenbanden.

Diese Labels zeigen, dass die Anomalie von Hackern zunehmend betont wird und dass Hacker als zu besiegende Feinde dargestellt werden (Halbert 1997).

Obwohl Hacker im Laufe der Zeit ein zunehmend negatives Image zugeschrieben bekommen, sehen sie sich selbst nicht als gesellschaftsschädliche Außenseiter, sondern betrachten sich als positive Andere ungeachtet dieser Dämonisierung und Sündenbockzuschreibung: „Sie neigen dazu ihre Andersartigkeit zu umarmen, so dass diese sie von anderen unterscheidet“ (Halbert 1997, S. 363, Übers. der Autoren). Zu einer vergleichbaren Einschätzung kommt Turgeman-Goldschmidt (2008) in ihrer Studie. Die von ihr interviewten Hacker betrachten sich selbst als positive Abweichler: sie seien talentiert, überlegen und brillant. Den Befragten sei es gelungen, den negativen Folgen von Etikettierung und sekundärer Abweichung zu entgehen, ihre devianten Erfahrungen in Sozialkapital umzuwandeln und einen guten Platz auf dem Arbeitsmarkt zu erlangen. Die Tatsache, dass Hacker qua Bildungsstandards eher aus dem höher gebildeten Teil der Gesellschaft kamen, wird hier als mögliche Erklärung genannt. Auch wird angenommen, dass Hacker sich schneller sozialen Konventionen oder moralischen Grenzen widersetzten, wodurch sie besser in der Lage seien, Stigmatisierungen zu bewältigen. Holt (2010) verweist in diesem Zusammenhang darauf, dass Hacker in der Szene ihre eigenen (moralischen) Grenzen zwischen sich und den anderen kreieren, und so Kategorien wie Hacker versus Cracker und *black hat* Hacker versus *white hat* Hacker konstruieren.[2]

3 Etikettierung, Selbstbild und beschädigte Identität

Wie verhält diese Entwicklung sich nun zu den Ideen des kriminologischen Etikettierungsansatzes? Der klassische Labeling Approach beschreibt die Art und Weise, in der die gesellschaftliche Reaktion – formell durch Sanktionierung oder informell durch Stigmatisierung – (negativen) Einfluss ausübt auf das Selbstkonzept und die soziale Identität der Etikettierten (Becker 1963). So sind

[2]*White hat* Hacker sind in der Regel Hacker, die sich damit befassen, Schwachstellen in Systemen zu finden. Sie suchen nach unbefugtem Zugriff auf diese Systeme und wollen deren Sicherheit verbessern. Auch *black hat* Hacker suchen nach solchen Schwachstellen, dringen aber in die Systeme ein, um z. B. Informationen zu erhalten oder Systeme zu schädigen. Sogenannte *grey hat* Hacker liegen hier (unbestimmt) dazwischen. Ihre Motive sind oft nicht ganz klar und situationsabhängig (Holt und Kilger 2008).

zum Beispiel ein negatives Selbstbild, der Ausschluss aus der Gemeinschaft und den sozialen Netzwerken oder das Nicht-Finden einer Arbeit mögliche Konsequenzen. Wird das zugeschriebene Etikett bzw. das Stigma durch die Betroffenen internalisiert, kann dies, so Goffman (1963), zu einer Beschädigung der Identität führen. Dies wiederum kann in der Folge zu abweichender Gruppenbildung und weiterem deviantem Verhalten führen, auch Sekundärabweichung genannt.

So wie man von einer am symbolischen Interaktionismus orientierten Perspektive erwarten darf, wird Devianz im Labeling Approach nachdrücklich als eine soziale Konstruktion betrachtet, die entsprechend den Standards und Regeln „mächtiger" Individuen gestaltet wird und denjenigen zugeschrieben wird, die jene Standards und Regeln nicht einhalten (Becker 1963; Lemert 1967; Mead 1934; Tannenbaum 1938). Tannenbaum (1938) hat als einer der ersten diesen Etikettierungsprozess als eine öffentliche Botschaft von und an die Gesellschaft beschrieben. Während mit dem Etikett „abweichendes Verhalten" zunächst nur die *Tat* verurteilt wird, folgt danach oft eine „Dramatisierung des Bösen", womit auch der *Täter* als *Person* als schlechter Mensch stigmatisiert wird (Tannenbaum 1938). Die öffentliche Identifizierung als „Verbrecher" führt zu einer Segregation, einer Abgrenzung als *anders* und einer Etikettierung als „Außenseiter" (Becker 1963; Tannenbaum 1938). In dieser Phase erhält das deviante Etikett einen sogenannten Master-Status, der alle anderen Eigenschaften des etikettierten Individuums überlagert (Hughes 1945). So führt die Etikettierung von jemandem als Außenseiter zu einer Verallgemeinerung, Vereinfachung und Verzerrung hin zu einem „kriminellen Status".

Das heißt jedoch nicht, dass dieser Status durch die Betroffenen auch immer internalisiert wird. Nach Lemert (1967), der das Konzept Sekundärabweichung entwickelt hat, beginnt der Prozess sekundärer Devianz mit dem Gefühl der Betroffenen, dass die Etikettierung ungerechtfertigt ist. Erst dann bildet diese im weiteren Verlauf auch die Basis für die Entwicklung einer neuen Identität. So betrachtet löst jemand durch sogenannte sekundäre Abweichung auch ein mögliches Identitätsproblem. Die stärkste Variante einer solchen sekundären abweichenden Identität ist die des Inhaftierten, eine Identität, der sich die Betroffenen kaum entziehen können.

Lemert sieht jedoch auch fließende Formen der Sekundärabweichung, bei der die Mitglieder einer Subkultur beispielsweise von einer abweichenden zur einen sozial akzeptierten Identität „driften".[3] Insbesondere diese letzte Form der Sekundärabweichung scheint bei Hackern relevant zu sein. In der Literatur

[3]Den Begriff „driften" verwendet Lemert hier unter Bezug auf *Delinquency and Drift* von Matza (1964).

wird dem Einfluss des digitalen Kontexts für das Entwickeln von sekundärer Abweichung bisher kaum Aufmerksamkeit gewidmet. In dem vorliegenden Kapitel soll diese Dimension mit einbezogen werden. Es wird deshalb untersucht, ob die virtuelle Dimension des Internet es für Hacker einfacher macht, sich den negativen Etikettierungen zu entziehen oder etwa zwischen einer abweichenden und einer nicht abweichenden Identität hin und her zu „driften".

Da das empirische Material dieser Studie hauptsächlich Einblicke in das Selbstbild von Hackern gibt und in geringerem Maße Aspekte wie Ausgrenzung, Beschäftigungsmöglichkeiten und sekundäre Abweichungen sichtbar macht, nehmen wir das Konzept des „abweichenden Selbst" des symbolischen Interaktionismus (Mead 1934; Goffman 1959, 1963) als Ausgangspunkt für diese Studie, um das Selbstbild von Hackern zu analysieren.

Die in unserer Studie interviewten Hacker erfahren sich vom „Normalbürger" als „anders" etikettiert, jedoch wird diese Zuschreibung selten internalisiert und führt deswegen auch nicht zu einem negativen Selbstbild oder Sekundärabweichung. Folgt man den Grundlagen des klassischen Labeling Approach, ist dies aber auch nicht zu erwarten, weil hier davon ausgegangen wird, dass Etikettierung immer eine vertikale Dimension impliziert. Jemanden effektiv zu etikettieren, bedeutet, dass man sozusagen *über* jemandem steht; eine Beziehung, die nicht beliebig umgekehrt werden kann. Etikettierung drückt ein vertikales Verhältnis aus: eine Status bestimmende Eigenschaft *(status determining trait)* wie Hughes (1945) das genannt hat. Ist dies nicht der Fall, können die Etiketten sozusagen nicht „haften" bleiben. Dies erklärt, warum der Labeling Approach vor allem angewendet wurde, um Etikettierungsprozesse von Gruppen mit einem geringen sozialen Status zu erklären: So hat Becker (1963) sich vor allem mit Marihuana-Benutzern beschäftigt, Goffman (1963) mit Inhaftierten. Sowohl der Zuschreibungsprozess als auch die Möglichkeit eine solche Etikettierung zu vermeiden, erfordert eine gewisse soziale Macht. Dadurch funktioniert der Etikettierungsprozess wie ein Kontrollinstrument und zielt auf die Stärkung der Machtstrukturen in der Gesellschaft. In diesem Sinne steht der Labeling Approach im Einklang mit Durkheims Idee, dass das „Verbrechen" dazu dient, den Unterschied zwischen „Gut" und „Böse" festzustellen und damit das gesellschaftliche System aufrecht zu erhalten und zu bestätigen. Etikettierung erfordert demnach eine gewisse hierarchische Struktur. Interessant scheint uns die Frage, inwieweit sich diese Struktur auch bei Hackern finden lässt.

Gleichzeitig scheint es uns sinnvoll, nicht nur die Etikettierung des Hackers als Außenseiter durch die Gesellschaft, sondern auch die Prozesse der Etikettierung innerhalb der Gruppe der Außenseiter selbst zu betrachten. So weist Matza darauf hin, dass Außenstehende oft Selbstkategorisierungen in der Gruppe vornehmen, der sie zugeschrieben werden:

> „From the outside, deviant persons … tend to look alike. From the inside, there is bound to be assortment and variety, observable, known, and usually designated by those who inhabit that world“ (Matza 1969, S. 28).

Ebenso kann hier die Rede sein von einem Vergleich mit anderen („externen“) Gruppen, eine Dimension, die möglicherweise gerade für Hacker eine wichtige Rolle spielt. So wird Latour (2005, S. 32) zufolge jede Bindung immer im Vergleich zu anderen konkurrierenden Bindungen betont und wird von daher für jede zu definierende Gruppe auch eine Liste von Anti-Gruppen erstellt. Mit anderen Worten, um das Selbstbild des Hackers aus der Perspektive des Etikettierungsansatzes zu verstehen, sind drei Aspekte relevant: 1) wie Hacker (als „andere“) denken, dass sie von der Außenwelt wahrgenommen werden; 2) wie Hacker sich selbst sehen und wie sie ihr eigenes Handeln bewerten und 3) wie Hacker als „Außenseiter“ sich selbst in Bezug zu allen anderen sehen.

4 Empirische Grundlage

Grundlage der folgenden Analyse ist empirisches Material[4], das im Rahmen einer Promotionsstudie durch die Zweitautorin gesammelt wurde (Van der Wagen 2018a). Theoretischer Ausgangspunkt und zentraler Forschungsansatz dieser Studie ist die *Actor-Network Theory* (ANT) von Bruno Latour. ANT basiert auf einer Forschungsmethode, die ziemlich eng mit der *verstehenden* Perspektive der kulturellen Kriminologie verbunden ist (Ferrell 1997). Latour zufolge ist für das Verstehen sozialer Phänomene unabdingbar, dass die Perspektive der Forschungsobjekte selbst soweit wie möglich im Vordergrund steht. Laut Latour (2005) sind diese nicht nur in der Lage, ihre eigene soziale Realität zu konstruieren und zu definieren, sondern ist zudem mit einer „agnostischen“ Forschungsperspektive mehr über deren Wahrnehmungen bzw. Erlebniswelt zu erfahren als mittels eines vorab festgelegten Rahmens. Latour schließt hier an die Tradition des symbolischen Interaktionismus an, aus dem der Labeling Approach sich entwickelt hat.

Im Rahmen unserer Studie wurden zehn semi-strukturierte Interviews mit Hackern geführt, in denen verschiedene Aspekte wie Motivation, Lernprozesse, Selbstbild, moralische Wahrnehmung und die Erfahrung des Hacks thematisiert

[4]Das empirische Material wurde schon an anderer Stelle, jedoch viel weniger ausgebreitet und in einem anderen Kontext besprochen und publiziert (vgl. Van der Wagen et al. 2016).

wurden.[5] Kontakt zu den Befragten wurde über *Hackerspaces* oder über Studierende hergestellt; gesucht wurde außerdem mittels der Schneeballmethode. Die Suche nach Hackern, die bereit waren, an einem Interview mitzuarbeiten, gestaltete sich sehr schwierig. In erster Linie scheint dies durch die vielen Interviewanfragen, die Hacker erhalten, und einer damit verbundenen Medien- und Forschungsmüdigkeit verursacht zu werden. So wurde uns über *Hackerspaces* mitgeteilt, dass sie täglich Anfragen von Journalisten oder Forschern erhalten. Zweitens spielte die Vorstellung „hier ist wieder so ein Forscher, der nichts von unserer Welt versteht", eine wichtige Rolle in der geringen Kooperationsbereitschaft. Drittens schien die Befürchtung zu bestehen, mit Cyberkriminalität assoziiert zu werden. So erhielten wir die folgende Antwort aus einem der *Hackerspaces:*

> „Um vorab Deutlichkeit zu schaffen, was verstehen Sie unter ‚Hacking'? Ein großer Teil der Außenwelt denkt hier nämlich an verschiedene Formen der Online- und Computer-orientierten Kriminalität. Je nachdem welche Art Hackers Sie suchen, werden wir Ihre Nachricht und Antwort gerne unter unseren Teilnehmern verbreiten."

Das Beispiel zeigt, wie negative Zuschreibungen und Kennzeichnungen sich auch negativ auf die Datenerfassung auswirken und diese beeinträchtigen können, was möglicherweise auch einen Einfluss auf die Zusammensetzung der interviewten Gruppe hatte. Letztendlich konnte nur mit einem Hacker direkt über einen *Hackerspace* Kontakt aufgenommen werden; drei Befragte wurden über die Schneeballmethode rekrutiert und der Rest der Befragten wurde über Kontakte mit Studierenden gefunden.

Alle Befragten sind (junge) erwachsene Männer, haben die niederländische Nationalität (mit Ausnahme eines Australiers) und ein durchschnittliches bis hohes Bildungsniveau im Bereich der Informationstechnologie. Dass die Befragten alle Männer sind, ist kein Zufall. Auch aus der Forschungsliteratur geht hervor, dass Hacking hauptsächlich von Männern dominiert wird (Yar 2005) und dass Hacker – Jordan und Taylor (1998, S. 767) zufolge – eine intensivere

[5]Acht der zehn Interviews wurden *face to face* geführt, eines über Skype und eines über E-Mail. Die Hälfte aller Interviews wurden im Zeitraum von Mai 2013 bis Mai 2015 durch die Zweitautorin abgenommen. Sie betreute auch die Gruppe Studierender, die im Rahmen einer Lehrveranstaltung zu Cybercrime an der Universität Groningen die zweite Hälfte der Interviews im Frühjahr 2013 führte.

maskuline Variante der bereits bestehenden männlichen Voreingenommenheit in den Computerwissenschaften konstruieren.

Hinsichtlich ihrer Erfahrungen und Motive ist die Gruppe jedoch sehr divers. Fünf der zehn Befragten betrachten sich in erster Linie als ethische oder *white hat* Hacker. Sie sind auf der Suche nach Schwachstellen in Systemen, teils auf eigene Initiative, teils im Namen eines Unternehmens (unabhängig davon, ob es sich um einen Auftrag handelt oder nicht), melden diese und machen diese in einigen Fällen auch öffentlich bekannt. Die andere Hälfte der Befragten ist mehr oder weniger in der *black hat* Szene aktiv. Zwei der Interviewten haben mehrere große Unternehmen oder Organisationen gehackt und erhielten hierfür auch eine Freiheitsstrafe. Derzeit verstehen sie sich als *(ex-)black hat* oder *grey hat* Hacker: Sie geben an, dass sie gelegentlich noch die Grenzen ausloten und nicht mit der *white hat* Szene verbunden sind. Zwei andere Befragte waren als *black hat* Hacker aktiv und berichten aber, nicht mehr illegal zu hacken. Ein letzter Befragter, der sich selbst nicht als Prototyp-Hacker versteht, war vier Jahre lang mit virtuellem Diebstahl beschäftigt, hackte Konten von Mitspielern und leerte diese. Er ist der einzige Befragte, der angibt (auch) ein finanzielles Motiv gehabt zu haben.

Zusätzlich zu den Interviews mit Hackern werden fünf Akten der niederländischen Staatsanwaltschaft in die Analyse mit einbezogen, in denen Computerverletzung der zentrale Punkt der Anklage ist.[6] Es betrifft vier Fälle, in denen ein individueller Hacker ein oder mehrere größere Unternehmen oder Organisationen gehackt hat. In einem der Fälle wurden die Hacks von einer Hacker-Gruppe durchgeführt. Die untersuchten Akten enthielten polizeiliche Vernehmungen oder aber Gespräche mit den Verdächtigen (zum Beispiel mit der Bewährungshilfe) und teilweise auch umfangreiche Chat-Gespräche unter Hackern. Aus jeder dieser Akten wird deutlich, wie Hacker ihre begangenen Straftaten betrachten und sich selbst als Hacker sehen; ein wichtiger Grund, diese Akten in die hier vorliegende Studie mit einzubeziehen. Bei der Analyse der Akten muss selbstverständlich berücksichtigt werden, dass die Befragungen und Gespräche im Rahmen einer strafrechtlichen Untersuchung durchgeführt wurden und möglicherweise nur eingeschränkt den Bedeutungszuschreibungen der Verdächtigen entsprechen. Eine Bezugnahme auf Ergebnisse der Aktenanalyse wird deshalb im Folgenden immer explizit erwähnt.

[6]Die Aktenanalyse fand im Zeitraum Juli und August 2015 bei der Staatsanwaltschaft in Rotterdam statt. Es handelt sich dabei nicht um die Strafakten der interviewten Personen.

Die Beschreibung des der Studie zugrunde liegenden empirischen Materials zeigt, dass es sich um eine kleine aber auch sehr unterschiedliche Gruppe von Befragten handelt, deren einziges gemeinsame Merkmal darin besteht, dass sie sich selbst als Hacker verstehen. Jenseits davon unterscheiden sie sich erheblich hinsichtlich ihrer ethischen Perspektive, ihrer normativen Position in Bezug auf Hacking und ihrer strafrechtlichen Vergangenheit. Generalisierende Aussagen über die Hacker Gemeinschaft sind im Rahmen dieser Forschung nicht möglich. Unser Vorhaben zielt vielmehr darauf, einen Einblick in die Erfahrungswelt von Hackern zu geben.

Die festgestellte große Diversität und Erfahrungsvielfalt der interviewten Hacker unterstützt den theoretischen Zweck dieser Studie, den Mehrwert des Etikettierungsansatzes für die Analyse von Hacking zu untersuchen, wodurch auch die wechselseitigen Zuschreibungen offengelegt werden können. In der folgenden Analyse wird anhand der Aussagen der interviewten Hacker die Art und Weise, in der sie ihre Realität konstruieren, herausgearbeitet.

Die Ergebnisse werden in drei Abschnitten präsentiert. Der erste Abschnitt befasst sich damit, wie Hacker denken, dass sie von der Außenwelt wahrgenommen werden; der sich anschließende Abschnitt damit, inwiefern Hacker sich selbst als *anders* verstehen; schließlich wird untersucht, wie Hacker sich selbst innerhalb und außerhalb der Hackergemeinschaft wahrnehmen und sich gegenseitig etikettieren.[7]

5 Perzeption durch die Außenwelt

Auf die Frage, was sie denken, wie die Außenwelt Hacker wahrnehmen, verweisen die Befragten zu allererst auf mangelndes Verständnis. Außenstehende würden „ihre Welt“ nicht verstehen und könnten diese möglicherweise auch nicht richtig verstehen. Dieses Unverständnis oder Unvermögen wird von einigen Befragten mit der bestehenden Kluft erklärt, die zwischen Hackern und Durchschnittsbürgern bestehe, was digitales Wissen betrifft. Eric (ein ehemaliger *black hat* Hacker) denkt, dass die gesellschaftliche Angst vor Hackern groß ist und viele Menschen Cyberspace als ein großes Mysterium betrachten. Andere Befragte verweisen auf Vorurteile, wonach Hacker ihre Fähigkeiten grundsätzlich

[7]Um die Anonymität zu gewährleisten, haben wir den interviewten Hackern fiktive Namen gegeben und soweit erforderlich strafrechtliche Informationen weggelassen.

für bösartige Zwecke einsetzen würden, indem sie überall „einbrechen“. Darüber hinaus geben einige Befragte an, dass aufgrund dieses Missverständnisses alle möglichen Stereotypen bestünden, variierend von Hackern als Sonderlinge bis zu Hackern als gefährliche Personen, wobei diese Stereotypen von den Medien bestätigt oder verstärkt würden. Das typische Bild eines Hackers ist laut Paul (einem ehemaligen *black hat* Hacker) das Folgende:

> „Nerdy Typen, die in kleinen Dachgeschosskammern im Dunkeln sitzen und den ganzen Tag am Computer Dinge kaputtmachen. Verschiedene Medien beschreiben das wirklich so. Ich denke, dass die Medien und die meisten Leute, wenn sie an Hacker denken, das genauso denken; das sind Nerds mit schlechten Absichten, asozial, die den ganzen Tag nichts anderes machen. Obwohl, dieses Image verändert sich allmählich, weil vielmehr an die Öffentlichkeit kommt und zum Beispiel, Hacker mehr und mehr Publizität erhalten.“

Jack, ein Hacker aus dem *Hackerspace* weist auch noch auf das negative Image in Medien und Filmen. Zugleich geben die interviewten Hacker an, dass es für Außenstehende auch schwierig sei „ihre Welt“ zu verstehen und dass das Unverständnis und die Angst gegenüber Hackern auch eine gewisse Grundlage habe. Sie beschreiben die Hacker-Szene als eine separate Gemeinschaft, die sich sehr wohl als „geheimnisvoll“, „unterirdisch“ oder „schwer zugänglich“ charakterisieren lasse. Die bestehenden Stereotypen könnten nur aufgebrochen werden, wenn Hacker mehr nach Außen treten würden, erklärt Paul; die Welt des Hackers würde dann weniger bedrohlich und geheimnisvoll sein.

Neben dem Gefühl als eine Art mysteriöse oder gefährliche Person betrachtet zu werden, erfahren Hacker vor allem die Zuschreibung als „kriminell“. Das Bild von Hackern als „Kriminelle“ oder als eine „kriminelle Organisation“ ist zentraler Gegenstand der Interviews, das durch alle Befragten selbst thematisiert wird. Ein Faktor, der als mögliche Erklärung für dieses negative Image gesehen wird, ist die Zunahme von Cyberkriminalität. David (ein *white hat* Hacker, der in einer Sicherheitsfirma arbeitet) verweist darauf, dass in den letzten Jahren viele neue Akteure und kriminelle Organisationen entstanden seien, die sich mit Hacken beschäftigten und so für den schlechten Ruf von allen Hacker gesorgt hätten. Einige der Befragten (z. B. Paul) machen vor allem die Medien verantwortlich, die durch ihre selektive Berichterstattung über Hacker als Kriminelle, dieses Image noch verstärken würden:

> „Lesen Sie irgendwas über ‚Hacker findet in jeder Windows-Version ein Loch‘? Sie lesen nur, ‚Hacker hackt Unternehmen X und stiehlt 3 Millionen Kreditkartendaten‘; das ist was du findest. Ja natürlich schafft dies ein negatives Image, das verstehe ich auch: diese Scheißkerle, die mein Konto plündern.“

Laut Jan, einem ethischen Hacker, zufolge, werden Hacker, auch wenn sie gute Absichten haben, immer mit Misstrauen begegnet und gilt bei diesen nicht die Unschuldsvermutung: *„Anstelle des Vorteil des Zweifels geht die Staatsanwaltschaft immer aus vom Nachteil des Zweifels.“* Jan hat zudem den Eindruck, dass hier eine Umdrehung stattfinde, denn eigentlich seien die Unternehmen, die gehackt werden viel „krimineller“, da sie mit ihren Daten nachlässig umgingen, was genau das ist, was durch Hacker erst sichtbar gemacht würde. Hacker riskierten jedoch eine seriöse strafrechtliche Verfolgung.

Ethische Hacker würden sich ziemlich über die schlechte Systemsicherung aufregen und fühlten sich oft nicht ernst genommen. Dies könne sogar dazu verführen, dass Hacker mit guten Absichten über's Ziel hinausschießen. So erzählt Jan von einem Vorfall, in dem ein Hacker entdecke, dass man in einem Webshop gratis bestellen kann. Als nach seiner Meldung nichts durch die Firma unternommen wird, bestellt er (als eine Art Witz-Aktion) (kostenlos) ein Sofa und lässt dieses an das Büro des betroffenen Unternehmens liefern.

6 Selbstwahrnehmung von Hackern als *anders*

Viele Hacker betrachten ihre Szene als eine besondere Gemeinschaft und verweisen darauf, dass sie sich selbst als anders als die anderen betrachten. Dabei charakterisieren sie sich als Menschen, die eine besondere Affinität für und ein besonderes Interesse an Technologie haben. Zwei Merkmale sind hier zu unterscheiden: Zum einen schreiben die meisten Befragten sich selbst eine neugierige Haltung gegenüber Computersystemen und Technologien zu, welche sie erkunden, knacken oder sichern wollen. Die Befragten sprechen hier weniger von Fähigkeiten, sondern beschreiben dies mehr als eine Art Hingabe und Faszination für die Funktionsweise von Computersystemen und Technologien. Dies spiele oft schon eine Rolle, wenn sie noch sehr jung seien. Jan, ein ethischer Hacker, erzählt zum Beispiel:

> „Als Kind wollte ich alle möglichen Knöpfe betätigen, nur um zu sehen, was passieren würde. Ich denke, es gibt ein angeborenes Bedürfnis, wenn es um den Umgang mit Technologie geht, dass man was hat mit dem Phänomen Technologie.“

Die interviewten Hacker sprechen von Systeme „durchschauen“, „untersuchen“ und „hinterfragen“, um zu beschreiben, was sie tun, und unterstreichen damit ihre besondere Beziehung und Haltung gegenüber der Technologie. Eric spricht in diesem Kontext sogar von „Empathie“. Empathie wird normalerweise mit der

Sensibilität für die Emotionen anderer Menschen in Verbindung gebracht, doch Eric verwendete das gleiche Wort in Bezug auf technische Systeme. Technische Systeme so gut zu verstehen, dass dies in Empathie für Technologie resultiere, steht beispielhaft hierfür und zeigt die tiefe und fast innere Verbindung, die manche Hacker mit Technologie angeben zu haben.

Zum zweiten beschreiben sich die befragten Hacker als Akteure, die eine nicht-instrumentelle Beziehung zur Technologie haben. Sie machen geltend, dass sie anders als „gewöhnliche" Menschen oder „passive Nutzer" gerade an den zugrunde liegenden Prozessen interessiert seien, wodurch ein System arbeite, wie dies funktioniere und wie nicht. In diesem Zusammenhang erklärt Jan: *„‚Starten Sie den Computer neu' ist doch der bescheuertste Kommentar, den du kriegen kannst, weil man dann nämlich noch immer keine Ahnung hat, was los ist."* Die Befragten scheinen auch Vergnügen zu haben an der Ziel-Mittel-Rhetorik von Geräten oder Technologien, die die Frage, wie diese wirken außer Betracht lassen – ein Aspekt, der manchmal explizit in die Definition von Hacking mit einbezogen wird; so zum Beispiel Kevin: *„Ein Hacker ist jemand, der Systeme und ihre Einrichtung für Zwecke einsetzt, für die sie ursprünglich nicht entwickelt wurden."*.

Verbunden mit ihrer nicht-instrumentellen Beziehung zur Technologie sei das Bedürfnis nach gegenseitigem Kontakt, sei es online oder in der physischen Welt: „Leute wie uns" oder mit einem ähnlichen Interesse aufzusuchen, wird mit der stärkeren Bindung, die man gegenseitig fühle, begründet. Dabei geben die Befragten an, dass es für sie enorm wichtig sei, Wissen zu teilen und mit Leuten reden zu können, die verstehen würden, worum es geht – oder wie Paul es formuliert, *„die dich nicht angucken wie ein Schaf, nach dem Motto, ‚worüber redest du?'"* Verschiedene Befragte erzählen, dass sie deshalb ihre *online*-Freunde und ihre *online*-Welt strikt trennen würden von den *offline*-Freunden und deren Welt, oder sie zumindest als zwei getrennte Kategorien betrachten würden. Mit den *offline*-Freunden gingen sie in die Kneipe oder würden sie *gamen,* jedoch kaum oder gar nicht über Computer-relevante Themen sprechen.

Die befragten Hacker fühlen sich nicht nur als anders und als Teil einer Gruppe anderer, sondern verstehen sich auch als positive Andere. So machen die interviewten Hacker deutlich, dass man Hacken vor allem in Begriffen wie Kreativität, Fantasie, *out of the box*-Denken, Kunst oder Genialität denken muss. So ist laut Jack ein Hacker jemand, der „spielerisch kluge Dinge tut". Jan definiert Hacken als „state of mind", als ein Denken jenseits der üblichen Pfade. Hacker würden Signale aufgreifen, die „normale Menschen" nicht sehen, was wiederum eine Kluft zwischen Hackern und der Gesellschaft schaffe:

> „Nicht gehört zu werden, wenn Dinge nicht gelöst werden, dass man ausgelacht wird, aber auch dass man sich nicht verstanden fühlt. Warum siehst du nicht, dass die ganze Welt grün ist? Warum sehe ich das sehr wohl, warum seht ihr das nicht?“

Hacker sehen sich demnach selbst als mit einem extra Sinn ausgestattet bzw. als jemand, der über einen Sensor oder eine spezielle Brille verfüge, der sie befähige, Dinge sehen zu können, wofür andere Menschen blind seien.

Für manche (ehemalige) *black hat* oder *grey hat* Hacker sind Beschreibung wie „jenseits der üblichen Pfade“ jedoch zu weitgehend. Sie definieren Hacking eher als „Kontrolle über fremde Systeme“ oder als „Übernahme eines Servers“. So wird zum Beispiel die Idee, dass das „Kreieren einer Zapfanlage“ unter Hacking fallen könnte, von Eric (einem ehemaligen *black hat* Hacker) lächerlich gefunden.

Eric bezieht sich hier auf *Hackerspaces,* in denen Hacker mit allerlei Dingen basteln und Objekte umfunktionieren. Dies kann alles sein. Wenn ein Hacker ein bestehendes Objekt in etwas anderes verwandelt (z. B. eine Bier-Zapfanlage aus einem Gartenschlauch konstruiert), kann dies auch als „Hack“ betrachtet werden Sie verwenden das Objekt für etwas, für das es ursprünglich nicht vorgesehen war. Das ist eine weit gefasste Definition von Hacking. Eric hält eine solche Definition für viel zu weit; für ihn bedeutet Hacking die Kontrolle über den Computer eines anderen.

Einige *black hat* Hacker betonen jedoch auch, dass Hacker „Querdenker“ seien. Und so beschreibt Eric es folgendermaßen:

> „Du musst eine Art Mensch sein, die mit etwas Seltsamem, Unbestimmtem und Neuem aufwarten kann, über das zuvor noch nie jemand nachgedacht hat. Du musst anders denken. Manchmal betrete ich einen Raum und weiß sofort, wie ich alle Türen öffnen kann, während die anderen nichts sehen.“

Eine andere Qualität, die Hacker sich selbst zuschreiben, ist die eines „Helfers“. Für ethische Hacker ist dies offensichtlich. Sie weisen darauf, dass ihre Hacks den Unternehmen helfen würden, Schwachstellen zu schließen oder anders – in Jans Worten – formuliert: „Fehlverhalten in der Gesellschaft aufzuzeigen“ und die Gesellschaft zu warnen oder zu schützen vor solchem Fehlverhalten. Jedoch spielt das Bild des Hackers als Helfer auch eine Rolle in der Art und Weise, in der *black hat* Hacker oder *grey hat* Hacker manchmal ihren Aktionen einen Sinn verleihen. Dylan, der lange in der *black hat* Hacker Szene aktiv war, erklärt zum Beispiel, dass er den Unternehmen, die er hackte, eigentlich geholfen habe:

> *„Wenn wir, also die mehr* mid- or low-level hackers *nicht wären, um Betriebe hinsichtlich ihrer Sicherheit zu erziehen, würden diese lebend aufgefressen werden.“*

Die Unternehmen, in die eingebrochen wird, werden hier nicht als Opfer gesehen, sondern als diejenige, die nicht für Sicherheit und Ordnung sorgen und dadurch den Hack selbst herausfordern. Dies ist übrigens ein Aspekt, den auch die Verdächtigen in allen untersuchten Strafakten betonen. So kommentiert einer von ihnen beispielsweise:

> „Es ist unfassbar, dass Leute all ihre persönlichen Daten angeben und dann können Leute wie ich, diese Daten einfach so abrufen. Bei der Veröffentlichung werden diese Daten online gestellt, um Menschen zu schockieren und Bewusstsein zu schaffen, was mit ihren Daten passieren kann. Das Ziel ist vor allem, das Unternehmen bloß zu stellen. Es wird viel Geld für schöne Bilder ausgegeben, aber die Systemsicherheit ist anscheinend unwichtig."

Die Tatsache, dass die Effekte von Hacking für die Gesellschaft auch positiv sein können, müsse sich auch im Verhältnis zu der verhängten Strafe widerspiegeln, findet Paul:

> „Meine Verurteilung ist nicht ungerechtfertigt. Ich denke aber zu schwer. Zumal ich die Systeme nicht zerstört habe. Ich habe sie eigentlich sogar besser gemacht; so fühlte ich mich damals, ja, ich habe diesen Leuten eigentlich geholfen."

Schließlich sehen sich Hacker auch als eine Art Moralritter oder als Menschen, die über dem Gesetz stehen. Unabhängig davon, ob es sich um legales oder illegales Hacking handelt, halten sich die Befragten im Allgemeinen an ihre eigenen moralischen Regeln oder Prinzipien, an die sie fest glauben. Dies erlaubt ihnen auch, dass sie Regeln brechen oder das System „abzocken", wenn sie nicht damit einverstanden sind oder etwas unfair finden. In diesem Zusammenhang erzählt Kevin (ein ehemaliger *black hat* Hacker) von einem eher ungewöhnlichen Beispiel:

> „Es gab dieses ‚free-to-play'-Spiel, bei dem die Benutzer durch das Bezahlen von Geld Vorteile im Spiel erhalten konnten. Ich hasste diese Idee, dass jemand in einem wettbewerbsorientierten Umfeld besser ist, nur weil er Geld hat. Also habe ich das, was im Spiel wirklich wichtig sein sollte, eingesetzt, nämlich *Skills*. Ich habe mich in die Site gehackt und abrufbare Codes generiert für die *in-game* Währung."

7 Gegenseitige Wahrnehmungen und Etikettierungen

Nicht jeder kann sich den Befragten zufolge als Hacker bezeichnen. Möglich sei es schon („es ist kein geschützter Titel"), aber es bestehe auch eine gewisse Exklusivität. Ein Hacker müsse fähig sein, etwas Geniales oder Kreatives zu schaffen. „Brillant sein" hat nichts damit zu tun, ob etwas legal oder illegal ist. Jan zufolge können einige Handlungen auch ziemlich brillant sein, obwohl sie nicht legal sind. Daniël (ein *white hat* Hacker) verweist in diesem Zusammenhang auf den Unterschied zwischen jemandem, der weiß, wie man den Tresor in einer Bank hackt, und einem Einbrecher, der einfach den Schlüssel unter der Haustürmatte findet. Den Befragten zufolge genießen sogenannte „Scriptkiddies" in der Hackerszene ein negatives Ansehen, da diese vorhandene Tools verwenden bzw. den Schlüssel unter der Matte gefunden hätten, also nicht wirklich wüssten, was sie tun. So betrachtet, machen die Befragten einen deutlichen Unterschied zwischen dem *echten* Hacker und dem Amateur oder *Möchtegern*-Hacker, den Scriptkiddies, die durch die Hacking-Kits, die man online ohne Probleme erstehen kann, am Zunehmen sind. Hier wird die oben besprochene Bedeutung der vertikalen Struktur und die Status-bestimmende Eigenschaft *(status determing trait)* für eine erfolgreiche Etikettierung deutlich. Demgegenüber findet Eric es „fucking bullshit", dass Scriptkiddies in der Szene so negativ angesehen werden würden, weil schließlich jeder so anfange. Vincent, derjenige Befragte, der am virtuellen Diebstahl beteiligt war, distanziert sich wiederum gerade von Hackern, die *alles* über die Systeme wissen wollen. *„Sie haben nichts Besseres zu tun, das finde ich ‚nerdig'. Ich finde das auch Zeitverschwendung."* Er erzählt, vielmehr daran interessiert zu sein, herauszubekommen, was man mit den Programmen machen könne, vor allem wie man Computer von Dritten unter seine Kontrolle bringen könne. So fand er z. B. sogenannte „Remote Access Tools", mit denen er den Computer und die Webcam von anderen Benutzern übernehmen konnte.

Fachkenntnisse und den Zugang hierzu spielen eine wichtige Rolle in der Hackerszene. Neben den offenen Foren, auf denen Hacker aktiv sind, verbringen sie, den Interviews zufolge, viel mehr Zeit auf privaten Chat-Kanälen (z. B. IRC oder personal messaging via fora), und für diese bekomme man nicht so einfach Zugang. Laut Kevin handelt es sich um eine auserwählte Gruppe von Freunden, mit denen man Wissen und „exploits"[8] austausche. Außenstehende, auch „Publikum"

[8] *Exploits* sind sogenannte Sicherheitslücken in Steuersystemen.

genannt, würden hier ausgeschlossen werden. Für viele der Kanäle müsse man explizit eingeladen werden, um Zutritt zu erhalten. Kevin (ein ehemaliger *black hat* Hacker) verweist darauf, dass der schwierige Zugang und die damit verbundene Heimlichkeit ihn besonders angezogen habe: *„Sie lassen nicht jeden zu, und ganz bestimmt lehren sie Neulingen nicht, wie es funktioniert. Das machte es für mich viel aufregender und interessanter, es selbst zu versuchen.“* Paul stellt fest, dass die Kriterien, um zugelassen zu werden jetzt völlig andere seien, als zu der Zeit, als er in der *black hat* Szene aktiv war:

> „Jemand stellt eine Frage, egal was für eine Frage und du kannst sie beantworten, dann kannst du zeigen, puhh der weiß das! Der kennt sich aus. Das ist dann keine Angeberei im Sinne von, seht, ich habe heute 400 Websites gehackt und ich gehöre dazu.“

Mit anderen Worten, Hacker scheinen sich selbst als eine Art *exklusive Andere* zu erfahren oder meinen einer exklusiven Gruppe anzugehören.

Genauso wichtig für die Art und Weise wie Hacker sich selbst wahrnehmen, ist – wie schon oben angedeutet – die Distanzierung von sogenannten Cyber-Kriminellen (als Anti-Gruppe). Um sich gegen dieses Label zu wehren und dagegen zu verteidigen, weisen sie nachausdrücklich auf die Unterschiede zwischen „Hackern“ und „Cyber-Kriminellen“ *(„den Scheißkerlen, die dein Konto plündern“).* Ein wichtiger Unterschied bezieht dabei sich auf die Absichten von Hackern. Paul zufolge sind *„Hacker nur Leute mit einem Hobby, die alles über das System wissen wollen, die wissen wollen, wie es funktioniert, wie man es zerstören kann, was es tut, wenn ich dies oder jenes tue.“* Manchmal gerate das Hobby außer Kontrolle, wie dies bei ihm selbst der Fall gewesen sei, aber auch dann könne man einen Hacker nicht mit einem Kriminellen vergleichen, der Dinge verkaufe oder stehle. Bei Paul und auch bei anderen Befragten markiert vor allem der finanzielle Gewinn die Trennlinie zwischen der Zuschreibung „kriminell“ oder „nicht-kriminell“. Eine zweite Trennlinie, die mehrere schon „erwischte“ Hackern beschreiben, ist mit der Unterstellung verbunden, dass Hacker sich überhaupt nicht wissentlich schuldig machen an „(Cyber)kriminalität“ und keine „kalkulierenden Kriminellen“ seien. In einer der Strafakten finden wir die folgende Aussage eines Verdächtigen:

> „Du stiftest ein bisschen Chaos mit ein paar Mann, aber das ist kein organisiertes Verbrechen! Aus meiner Sicht würden wir dann nur im Voraus planen und darüber nachdenken, wie man Geschäfte macht und was man mit den Daten tut. Aber das machen wir nicht, wir haben einfach Spaß, mit dem etwas zu tun, was man findet, aber es gibt keinen Plan dahinter.“

Einige der Befragten, darunter auch ein von der Staatsanwaltschaft Verfolgter, verweisen auf die Bedeutung des Gruppeneinflusses und dass Grenzen innerhalb einer *(black hat)* Gruppe leicht verschwömmen; so z. B. Eric: „Es gibt niemanden, der zu dir sagt, hey dies ist vielleicht strafbar“, was dazu führt, dass „viele Jungs darin untergehen.“ Hacker seien oft talentierte Jungens, die noch Suchende seien und nicht wüssten, wie sie ihr Talent einsetzen sollen, stellt Simon fest. Am Ende werde jedoch auch ein *black hat* Hacker auf der „guten Seite“ landen, so die Befragten. Der Spaß und die Herausforderung würde zu einem bestimmten Zeitpunkt abnehmen, ebenso wie ein Moment komme, dass jemand ein normales Einkommen erzielen möchte. In der Tat weisen viele Befragte unter den ehemals *black hat* Hackern darauf, dass ihre Vergangenheit sogar positiv für ihre Berufskarriere gewesen sei. Nach ihrer Inhaftierung fanden sie direkt eine Arbeit und konnten hier ihre Fachkenntnis und Kompetenzen gut einsetzen.

Der Modus Operandi markiert eine dritte Trennlinie, der Hackern zufolge sich deutlich unterscheide von dem eines „Kriminellen“. So berichtet Eric zum Beispiel, dass Schutzmaßnahmen durch Hacker oft nur halbherzig durchgeführt würden und dass sie oft auch sehr unvorsichtig seien:

> „Jemand, der beabsichtigt, finanziellen Gewinn zu erzielen, der sorgt von Anfang an dafür, keine Spuren zu hinterlassen und hinterlässt nicht überall seinen Namen, weil er eben kein Interesse hat, bekannt zu werden. Gerade Jungens, die die technischen Möglichkeiten ausloten, machen aber total blöde Fehler. Sie geben ihren Namen einfach überall und irgendwo an, aber inzwischen sind sie dabei alle Menschen zu infizieren.“

Im Gegensatz zu Cyber-Kriminellen prahlten Hacker auch gerne in Chat-Kanälen, wodurch sie Vincent zufolge schneller gefasst würden. Paul spricht von „mediengeilen“ Typen, die so dumm seien, dass sie sogar ihre Adresse hinterließen. Er glaubt auch, dass dies typisch für die Hacker unserer Zeit sei. Seiner Meinung nach nimmt die „Prahlerei“ in den letzten Jahren enorm zu und gebe es Gruppen, die nur hacken, um damit anzugeben.

Neben den beschriebenen Prozessen des *Othering* bzw. des „Zu Anderen machen“ bezüglich wer oder was sich ein Hacker nennen kann, gibt es auch Etikettierungsprozesse zwischen den verschiedenen Hacker-Gruppen. Ein Beispiel dafür ist die Weise, wie *black hat* und *white hat* Hacker sich gegenseitig wahrnehmen. Die Mehrheit der Befragten verweist darauf, dass beide Gruppen sich deutlich unterscheiden und sprechen in diesem Zusammenhang von den „guten“ oder „schlechten“ Absichten oder von Legalität und Illegalität. Paul erklärt:

> „Ein *white hack* Hacker ist wirklich jemand, der es gut meint, nichts falsch machen will, nichts Illegales, im Sinn von, wir haben einen Bug gefunden und melden diesen der Person, die den Bug hat. Ein *black hat* Hacker würde dies missbrauchen, im Sinne von schauen wir einfach mal hinein, melden tun wir aber nichts."

In diesem Zusammenhang findet Kevin auch den Begriff des *grey hat* Hacker unsinnig:

> „Eine Person kann nicht gut und schlecht sein. Jemand hackt entweder für Geld, behält es für sich, verkauft es auf dem Schwarzmarkt oder verursacht Schaden (black hat). Oder er ist ein guter Kerl und hackt professionell."

Jan zufolge bedeutet dies nicht, dass nicht auch ein *black hat* Hacker gute Dinge tue (oder vice versa). Als Beispiel nennt er einen Mafia-Boss, der Geld an eine Wohltätigkeitsorganisation gespendet habe.

Eric spricht von einem ständigen Kampf zwischen *black hat* und *white hat* Hackern, der mit dem diskutierten schlechten Image des Hackers zusammenhänge:

> „Auf Twitter oder so machen sie sich alle gegenseitig schlecht. Alle *black hats* hassen die *white hats* und alle white hats hassen die *black hats*, weil die nur mit kriminellen Sachen beschäftigt sind, und das ist für das Ansehen des Hackers nicht gut."

Betrachtet man, wie die ethischen Hacker in den Interviews *black hat* Hacker beschreiben, dann können wir feststellen, dass hier nur in Begriffen von „Gut" und „Böse", Moral oder Schaden gesprochen wird. *Black hat* Hacker gelten als „Menschen, die hacken, um andere zu irritieren", „Schaden verursachen", „Bösewichte", „Einbrecher", „Hacker mit anderen moralischen Standards" und die „bösartig" seien. Umgekehrt wird nicht nur referiert an „Gut" und „Böse", sondern auch verwiesen auf unterschiedliche Charaktere und Gefühle. So beschreibt Eric *white hat* Hackers als „nette Schlappschwänze", „die sich an die Regeln halten", „total anständige zivilisierte Jungens", „die weiß geboren werden", „übermäßig brav", „die bei jedem Leck, das sie sehen, ausflippen" und „die eine klare Grenze sehen zwischen dem, was darf und was nicht darf", während er die *black hats* als die „stursten Jungens in der Gruppe" sieht, die auf der Suche nach Spannung seien.

8 Diskussion

Zwei zentrale Fragen bildeten den Ausgangspunkt für die vorliegende Studie: Inwieweit Hacker als *digitale Andere* negative Folgen aus ihrer Etikettierung als Außenseiter erleiden und ob der klassische Etikettierungsansatz auch im digitalen Zeitalter von Bedeutung ist. Drei Dimensionen des Selbstkonzeptes einer kleinen, aber vielfältigen Gruppe von Hackern wurden hierfür untersucht. In Übereinstimmung mit den Erkenntnissen von Turgeman-Goldschmidt (2008) erfahren die hier interviewten Hacker zwar eine negative Etikettierung, sehen sich selbst jedoch vor allem als *positive Andere.* Aus ihrer Perspektive sind sie weniger durch Unzulänglichkeiten, sondern eher durch außergewöhnliche Merkmale im Vergleich zu anderen Menschen charakterisiert, was Fähigkeiten, Intelligenz und einen Geisteszustand betrifft, mit dem sie „brillante Dinge" realisieren. Sie beschreiben sich selbst als Individuen mit einer angeborenen Faszination und Affinität für Gegenstände und Technologie, die eine deutliche Verbundenheit mit Technik empfinden, was zugleich ein wesentliches Element ihrer Definition des „anders sein" ist (Van der Wagen 2018a, b).

Die Befragten verstehen sich als Helden oder Moralritter mit eigenen und sehr spezifischen Vorstellungen von Gut und Böse. (Bestehende) Grenzen sowohl in technischer als auch in moralischer Hinsicht werden als unnatürlich betrachtet. Sie wollen diese durchbrechen und verschieben sowie eigene Grenzen setzen. Sie scheinen beinahe davon überzeugt, dass sie über bestimmte sensorische Fähigkeiten oder Kräfte verfügen, die ihnen ermöglicht bestimmte Dinge zu sehen, zu bemerken oder ergründen zu können, wofür normale Menschen blind sind. In diesem Sinne verstehen sie sich auch als eine Art „Supermensch" oder „Cyborgs", weil ihr Körper und ihr Geist sich in anderen und größeren Sphären bewegen (Van der Wagen 2018b). Basierend auf unserer Analyse des empirischen Materials können wir hier also nicht von einer verletzten Identität sprechen.

Die empirische Studie hat zudem gezeigt, dass Etikettierung *innerhalb* der Gruppe von Hackern zwingender ist als die Etikettierung von außen. Wir können konstatieren, dass mit Beginn des neuen Jahrhunderts die Massenmedien zunehmend als Moralunternehmen aufgetreten sind und mit einer sensationellen Berichterstattung über Hacking auch ein negatives Bild von Hackern konstruiert haben. Diese negative Berichterstattung hat jedoch ebenso wie negative Aussagen von Politikern die Betroffenen kaum erreicht, da diese als nicht maßgeblich betrachtet werden. Da die moralische Empörung über Hacker immer von außen kommt, bleibt sie an der Oberfläche und wird sie von den Betroffenen kaum internalisiert. Autorität und Kenntnis *innerhalb* der Gruppe von Hackern

sind Status-bestimmende Eigenschaften, die dazu führen, dass Etiketten effektiv zugeschrieben werden können. Deswegen hat die Etikettierung von Hackern kaum stigmatisierende Effekte und resultiert auch nicht in der Internalisierung einer devianten Identität. Obwohl Hacker vom „Publikum“ häufig als „kriminelle Andere“ betrachtet werden, verringert die Exklusivität der Gruppe selber die Bedeutung öffentlicher oder rechtlicher Reaktionen. Eine ähnliche Feststellung wurde übrigens bereits von Goffman (1963) gemacht, der einräumte, dass einige Individuen trotz ihrer Stigmatisierung „gedeihen“ könnten.

Die Tatsache, dass Etikettierungsprozesse bei Hackern weniger stigmatisierende Effekte zu haben scheinen als bei den „traditionellen“ Devianten, die üblicherweise Gegenstand des Labeling Approach sind, lässt sich auch auf Merkmale des Phänomens Hacking selbst zurückführen. Das Phänomen des Hackens, das mit den je eigenen Fähigkeiten, der Denkweise und Moral verbunden ist, ist die Domäne einer exklusiven Gruppe von „Insidern“, die als Online-Gruppe im World Wide Web aktiv ist. Um ein „exklusiv Anderer“ zu werden, muss man nicht nur die Fähigkeiten erlernen, sondern sich auch beweisen. Ohne Interaktion mit und Bestätigung durch die anderen in der Szene (dem Publikum), sind Hacker eigentlich im Cyberspace verloren. Durch brillante Hacks können sie jedoch einen heroischen Status erlangen. Wie in der „echten Welt“ darüber durch die weniger bedeutend Anderen gedacht wird, ist unwichtig. In diesem Sinne haben Außenstehende auch nicht den sozialen Status, um Hacker effektiv etikettieren zu können.

Mit anderen Worten: Das positive Selbstbild, das Hacker von sich selbst haben, die (Online-)Gemeinschaft, auf die sie zählen, und der deutliche moralische Rahmen, innerhalb dessen sie ihren Handlungen Sinn zuschreiben, können möglicherweise erklären, warum Hacker sozusagen *über* den negativen Urteilen der (Offline-)Außenwelt stehen, die die Welt der Hacker sowieso nicht begreifen. Eine Rolle spielt hier auch, dass Hacking ein Phänomen ist, das für Außenstehende relativ unsichtbar ist. Hacker können mehr oder weniger im Geheimen operieren und so Online-Zuschreibungen leichter vermeiden. Sie werden dadurch nicht als Person negativ stigmatisiert (es sei denn, sie werden strafrechtlich verfolgt), sondern mehr allgemein als Gruppe (vor allem durch die Medien) negativ beurteilt. Die Etikettierung ist sozusagen auf das Phänomen beschränkt und erreicht selten das Stadium der individuellen Zuschreibung.

In gewisser Weise existiert das positive Bild von Hackern aus den 1970er Jahren, als die Industrie gerne mit Hackern zusammenarbeitete, noch immer. Weil sie über IT-Fähigkeiten verfügen, die in der gegenwärtigen Gesellschaft dringend gebraucht werden, genießen sie auch eine gewisse Anerkennung. Nicht nur arbeiten IT-Firmen noch immer gerne mit ihnen zusammen, auch werden (erwischte)

illegale Hacker (z. B. in den Niederlanden durch die Polizei) eingeladen, mit den Strafverfolgungsbehörden zusammenzuarbeiten.[9] Auch das scheint uns ein wichtiger Grund zu sein, warum die negativen Etiketten im Fall von Hackern nicht haften bleiben und nicht zu sekundärer Devianz führen.

Unsere Analyse weist auch darauf hin, dass einige Hacker eine Unterscheidung vornehmen zwischen ihrer Online- und Offline-Identität, was ihnen ermöglicht, zwei Identitäten nebeneinander zu managen und zwischen diesen – einer devianten und einer nicht-devianten Identität – hin und her zu „driften". So erhält auch Goffmans Bühnenansatz, mit einer Vorderbühne, auf der man sich mit einem bestimmten Charakter salonfähig präsentiert, und einer Hinterbühne, auf der man sich entspannen kann und die Vorderseite sowie das dazu gehörende Skript fallen lassen kann, im Cyberspace eine neue Dimension und Relevanz (Goffman 1959). Für einige *black hat* Hacker scheint Hacken dann auch vielmehr ein „kriminelles Rollenspiel" zu sein, da sie letztendlich der Gesellschaft nur Gutes tun, indem sie die mangelnde Sicherheit von Unternehmen und Organisationen aufdecken, die aus ihrer Perspektive die eigentlichen „Kriminellen" sind. Die bekannten Neutralisierungstechniken (Sykes und Matza 1957) wie Zurückweisung eigener Verantwortung oder eines Schadens und die Abwertung von Opfern kommen hier zum Einsatz. Es stellt sich jedoch die Frage, ob hier von Neutralisierung im Sinne von *moral holiday* entsprechend des klassischen Etikettierungsansatzes gesprochen werden kann. Angesichts ihrer ausgeprägten eigenen Moral denken Hacker nicht, dass sie ihr Verhalten legitimieren müssen. Sie betrachten diese Erklärungen eher als eine Verteidigungsstrategie und weniger als Neutralisierung.

Obwohl sich die moralischen Grenzen zwischen *black* und *white hat* Hackern deutlich unterscheiden, sind sich beide einig, dass man Hacker nicht mit den „echten Cyberkriminellen" vergleichen kann, die durch finanzielle Motive getrieben seien. Das bringt uns auch zu dem Punkt, dass das „anders sein" nicht nur auf eine Assoziation mit „gleichgesinnten Anderen" zielt, sondern auch auf eine ausdrückliche Dissoziation mit anderen Gruppen. In diesem Kontext

[9]Die niederländische Polizei hat auf dieser Grundlage sogar ein alternatives oder zusätzliches Strafverfahren eingeführt, Hack_Right genannt, wobei erwischte Hacker den verursachten Schaden wieder reparieren müssen, Schulung in den Regeln der ethischen Internetnutzung erhalten und dabei durch ethische Hacker gecoacht werden und lernen sollen, wie sie ihre Fähigkeiten positiv nutzen können (siehe https://www.politie.nl/themas/hack_right.html).

scheint uns Latours Begriff der „Anti-Group“ relevant, um das Verhältnis zwischen Hackern und sogenannten Kriminellen, aber auch zwischen *black hat* und *white hat* Hackern zu beschreiben. Die Tatsache, dass also auch innerhalb der als „anders“ stigmatisierten Gruppe Etikettierungsprozesse stattfinden, neutralisiert möglicherweise das negative Image. Zusammenfassend würde das bedeuten, dass nicht nur die digitale Dimension, sondern auch eine solche (Anti)Gruppendimension den Etikettierungsansatz bereichern könnte.

Die Idee, dass die zugeschriebenen Labels nur haften bleiben und dass eine deviante Identität nur verinnerlicht werden kann, wenn diejenigen, die sie zuschreiben, über ausreichende Autorität verfügen, ist integraler Bestandteil des Etikettierungsansatzes. Bei der späteren Rezeption der Theorie wurde dieser Aspekt jedoch meist vernachlässigt. Eine Schlussfolgerung ist dann auch nicht, dass der Etikettierungsansatz veraltet ist, sondern dass wir uns den ursprünglichen Quellcode noch einmal genau ansehen müssen und dass der Etikettierungsansatz sehr wohl ein Update verdient. Nur so kann dieser auch in Zukunft seine Bedeutung für (cyber)kriminologische Forschung erhalten.

Literatur

Bauman, Z. (2000). *Liquid modernity*. Cambridge: Polity.

Blankwater, E. (2011). *Hacking the field. An ethnographic and historical study of the Dutch hacker field*. Master’s Thesis Sociology. University of Amsterdam.

Becker, H. S. (1963). *Outsiders. Studies in the sociology of deviance*. New York: The Free Press.

Churchill, D. (2016). Security and visions of the criminal: Technology, professional criminality and social change in victorian and Edwardian Britain. *British Journal of Criminology, 56,* 857–876.

Ferrell, J. (1997). Criminological verstehen: Inside the immediacy of crime. *Justice Quarterly, 14,* 3–23.

Goffman, E. (1959). *The presentation of self in everyday life*. London: Penguin.

Goffman, E. (1963). *Stigma. Notes on the management of spoiled identity*. Englewood Cliffs: Prentice-Hall.

Halbert, D. (1997). Discourses of danger and the computer hacker. *The Information Society, 13,* 361–374.

Holt, T. J. (2010). Examining the role of technology in the formation of deviant subcultures. *Social Science Computer review, 28,* 466–481.

Holt, T. J., & Kilger, M. (2008). Techcrafters and Makecrafters: A comparison of two populations of hackers. *Presentation 2008 WOMBAT Workshop on Information Security Threats Data Collection and Sharing*. Amsterdam, Nederland.

Hughes, E. C. (1945). Dilemmas and contradictions of status. *American Journal of Sociology, 50,* 353–359.

Jordan, T. (2008). *Hacking. Digital media and technological determinism*. Cambridge: Polity Press.
Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review, 46,* 757–780.
Latour, B. (2005). *Reassembling the social. An introduction to actor-network-theory*. New York: Oxford University Press.
Lemert, E. (1967). *Human deviance, social problems and social control.* Englewood Cliffs: Prentice Hall.
Levy, S. (1984). *Hackers heroes of the information age*. New York: Doubleday.
Matza, D. (1964). *Delinquency and drift*. New York: Wiley.
Matza, D. (1969). *Becoming deviant*. Englewood Cliffs: Prentice Hall.
Mead, G. H. (1934). *Mind, self and society: From the standpoint of a social behaviorist*. Chicago: Chicago University Press.
Nissenbaum, H. (2004). Hackers and the contested ontology of cyberspace. *New Media Society, 6,* 195–217.
Skibell, R. (2002). The myth of the computer hacker. *Information, Communication and Society, 5,* 336–356.
Steinmetz, K. F. (2015). Craft(y)ness. An ethnographic study of hacking. *British Journal of Criminology, 55,* 125–145.
Sykes, G. M., & Matza, D. (1957). Techniques of neutralization. A theory of delinquency. *American Sociological Review, 22,* 664–670.
Tannenbaum, F. (1938). *Crime and the community*. New York: Colombia University Press.
Taylor, P. A. (1999). *Hackers. Crime in the digital sublime*. London: Routledge.
Turgeman-Goldschmidt, O. (2008). Meanings that hackers assign to their being a hacker. *International Journal of Cyber Criminology, 2,* 382–396.
Turkle, S. (2005). *The second self: Computers and the human spirit*. Cambridge: MIT press.
Van der Wagen, W. (2018a). *From cybercrime to cyborg crime: An exploration of high-tech cybercrime, offenders and victims through the lens of actor-network theory*. PhD diss., University of Groningen.
Van der Wagen, W. (2018b). The cyborgian deviant. An assessment of the hacker through the lens of actor-network theory. *Journal of Qualitative Criminal Justice and Criminology, 6,* 157–178.
Van der Wagen, W., Althoff, M., & Van Swaaningen, R. (2016). De andere ‚anderen'. Een exploratieve studie naar processen van labelling van, door en tussen hackers. *Tijdschrift over Cultuur & Criminaliteit, 6,* 27–41.
Van der Wagen, W., & Pieters, W. (2015). From cybercrime to cyborg crime: Botnets as hybrid criminal actor-networks. *British Journal of Criminology, 55,* 578–595.
Wall, D. (2008). Cybercrime and the culture of fear. Social science fiction(s) and the production of knowledge about cybercrime. *Information, Communication & Society, 11,* 861–884.
Yar, M. (2005). Computer hacking: Just another case of juvenile delinquency? *The Howard Journal, 44,* 387–399.

Grooming-Umgebungen von pädophilen und hebephilen Männern in Deutschland

Erste Ergebnisse einer qualitativen Befragung

Daniela Stelzmann, Till Amelung und Laura F. Kuhle

1 Problemstellung

Nach Strafgesetzbuch § 176 liegt der Tatbestand des sexuellen Missbrauchs von Kindern dann vor, wenn sexuelle Handlungen an einer Person unter vierzehn Jahren vorgenommen werden bzw. diese zu sexuellen Handlungen animiert wird, wobei dies auch mittels Informations- und Kommunikationstechnologien geschehen kann (Herrmann 2008). Nach Schätzungen geht circa der Hälfte aller sexuellen Missbräuche von Kindern ein sogenannter Grooming-Prozess voran (Canter et al. 1998). Unter dem sexuellen Groomen von Kindern[1] (kurz: Grooming) versteht man den Prozess, bei dem eine Person Kontakt zu einem Kind

[1]Die Begriffe Sexual Grooming, Sexual Grooming of Children oder Solicitation werden in der Literatur synonym verwendet.

D. Stelzmann (✉)
Institut für Publizistik- und Kommunikationswissenschaft, Freie Universität Berlin, Berlin, Deutschland
E-Mail: daniela.stelzmann@fu-berlin.de

D. Stelzmann · T. Amelung · L. F. Kuhle
Institut für Sexualwissenschaft und Sexualmedizin, Charité – Universitätsmedizin Berlin, Berlin, Deutschland

T. Amelung
E-Mail: till.amelung@charite.de

L. F. Kuhle
E-Mail: laura.kuhle@charite.de

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

T.-G. Rüdiger und P. S. Bayerl (Hrsg.), *Cyberkriminologie,*
https://doi.org/10.1007/978-3-658-28507-4_19

aufbaut, um es nach und nach für einen sexuellen Missbrauch vorzubereiten, indem sie das Vertrauen des Kindes gewinnt und eine Offenbarung der Taten seitens des Kindes mit Hilfe von Manipulation unterbindet (Craven et al. 2006). Da die Täter unterschiedliche Strategien nutzen, ist Grooming vielfältig in seiner Erscheinungsweise (Kloess et al. 2017; Black et al. 2015; Quayle et al. 2014; Akhtar 2014). Durch diese Varianz kann Grooming nur schwer von Kindern als Gefahrensituation identifiziert werden (Williams 2015), zumal sich in der Anfangsphase Grooming für das Kind selbst kaum von einer normalen Interaktion mit einer erwachsenen Person unterscheiden lässt (Winters und Jeglic 2017).

Grooming findet sowohl in Offline-Umgebungen (z. B. in der Familie, in pädagogischen Einrichtungen, etc.) als auch in Online-Umgebungen (z. B. Online-Gaming, digitale soziale Netzwerke, etc.) statt (Akhtar 2014). Für letztere attestieren Forscher einen alarmierenden Anstieg von sexuellem Kindesmissbrauch (Gupta et al. 2012). Prävalenzstudien aus den USA und Deutschland quantifizieren diese Problematik: Zwischen 10 % und 27 % der Kinder und Jugendlichen geben an, unterschiedlichste Formen von sexuellen Kontaktanbahnungen im Internet erlebt zu haben (Polizeiliche Kriminalstatistik 2018; Sklenarova et al. 2018; Staksrud 2013; Wolak et al. 2008; Ybarra et al. 2004).

Um präventiv gegen Grooming in den verschiedenen Umgebungen vorzugehen, müssen Kenntnisse über (potenzielle) Groomer gewonnen werden, mit deren Hilfe präventive Strategien abgeleitet werden können. Bisherige Studien über Grooming-Täter untersuchten forensische Stichproben und verglichen die Gruppe der „Online-Täter“ im Allgemeinen (Nutzer von Missbrauchsabbildungen, Groomer) mit der Gruppe der „Offline-Täter“ (sexuelle Kindesmissbraucher). Diese Ergebnisse zeigen, dass es sich bei den „Online-Tätern“ um eine heterogene Gruppe handelt, die sich in demographischen, ökonomischen und sozialen Merkmalen unterscheidet (Babchishin et al. 2011).

Unabhängig vom Grooming ist bekannt, dass Täter, die sexuellen Kindesmissbrauch begehen, unterschiedliche Risikoprofile haben (Bonta und Andrews 2007). So stellt die sexuelle Präferenz für das kindliche (Pädophilie) oder frühpubertäre (Hebephilie) Körperschema einen bedeutenden Risikofaktor dar, der die Wahrscheinlichkeit der Tatwiederholung erhöht (Hanson und Morton-Bourgon 2005). Gegenwärtig gibt es nur wenige Studien, die Grooming in Hinblick auf die sexuelle Präferenz der Täter untersuchen (Kuhle und Stelzmann 2018). Durch die erhöhte Wahrscheinlichkeit der Tatwiederholung stellen Menschen mit einer Präferenz für Kinder (Pädophilie und/oder Hebephilie) jedoch eine wichtige Gruppe für präventive Maßnahmen dar. Um die entsprechenden Maßnahmen am Risiko zu orientieren, braucht es Untersuchungen an groomenden Präferenztätern. Dies ermöglicht auch den Fragen nachzugehen, wie sich diese Tätergruppe von anderen Tätergruppen unterscheidet, welche Grooming-Strategien sie nutzen und in welchen Umgebungen sie groomen.

2 Ziel der Studie

Da die meisten Studien die Täter unabhängig von ihrer sexuellen Präferenz betrachten, ist das Ziel dieser Studie die Erfassung und Beschreibung der Grooming-Umgebungen von Männern, die aufgrund ihrer Präferenz für kindliche oder frühpubertäre Körperschemata ein erhöhtes Risiko für wiederholten sexuellen Kindesmissbrauch haben. Die gewonnenen Erkenntnisse sollen der besseren Identifikation von Grooming durch Kinder, ihren Bezugspersonen und der Justiz dienen und die Einrichtung juristischer (und präventiver) Maßnahmen und Behandlungsansätze unterstützen.

3 Methode[2]

Da die empirischen Erkenntnisse zum Grooming-Verhalten von Männern mit einer Präferenz für Kinder bisher gering sind, wurde im Rahmen dieser Studie eine qualitative Befragung pädophiler und hebephiler Täter durchgeführt. Diese hatte zum Ziel, die subjektiven Sinnstrukturen der Befragten zu erfassen und so die Erkundung des neuen und noch nicht belegten Forschungsgegenstandes zu ermöglichen (Lamnek 2008). Insgesamt wurden drei pädophile und vier hebephile Männer[3], die in der Vergangenheit wiederholt als Groomer aktiv waren, befragt. Die Befragten waren im Durchschnitt 41,29 Jahre alt ($SD = 12{,}57$ Jahre, *Range:* 23–58 Jahre); zwei Befragte waren in Partnerschaften und fünf Befragte waren berufstätig. Bei zwei der Männer wurden die Taten juristisch entdeckt – spiegeln sich also im sogenannten Hellfeld wider, fünf verblieben im sogenannten Dunkelfeld.

Die Interviewten waren Teilnehmer am „Präventionsprojekt Dunkelfeld“ (PPD)[4] und wurden in diesem Rahmen für die Teilnahme an der Studie aus den

[2]Die hier präsentierten Ergebnisse sind Teilergebnisse einer Studienreihe (mehr dazu: Kuhle und Stelzmann 2020).

[3]Die Stichprobe umfasste sowohl Männer mit exklusiver als auch mit nicht-exklusiver Pädophilie und Hebephilie.

[4]Im Jahr 2005 startete das Projekt „Prävention von sexuellem Kindesmissbrauch im Dunkelfeld“, kurz „Präventionsprojekt Dunkelfeld (PPD)“. Seitdem wird dort für Menschen, die sich sexuell zu Kindern hingezogen fühlen und freiwillig und ohne juristische Auflagen Hilfe suchen, spezifische Diagnostik und Therapie unter Schweigepflicht angeboten. Ziel des Präventionsprojektes war und ist es, Sexualstraftaten an Kindern sowie die Nutzung von Missbrauchsabbildungen (sogenannte Kinderpornographie) durch die therapeutische Behandlung von Menschen, die sich sexuell zu Kindern hingezogen fühlen, bereits im Vorfeld zu verhindern. Weitere Informationen unter: https://www.kein-taeter-werden.de.

bestehenden Therapie- bzw. Nachsorgegruppen rekrutiert. Die sexuelle Präferenz der Befragten wurde bereits in der Eingangsdiagnostik des Projektes erhoben, wobei die diagnostizierte Präferenz für Kinder durch einen zweiten Rater basierend auf den Interviewaufzeichnungen verifiziert wurde. Die Tiefeninterviews zum bisherigen Grooming-Verhalten, die dann im Rahmen der vorliegenden Studie durchgeführt wurden, dauerten im Schnitt eine halbe bis eine Stunde und wurden zwischen Juli und Oktober 2018 face-to-face oder per Telefon von zwei geschulten Therapeuten des PPD durchgeführt. Das Interview umfasste mehrere Frageblöcke zum Thema Grooming, wie beispielsweise Strategien der Kontaktinitiierung oder Geheimhaltung. Die Antworten wurden via Diktiergerät aufgenommen und im Anschluss transkribiert. Die Transkripte wurden qualitativ inhaltsanalytisch, orientiert an Mayring, mithilfe der Software f4 ausgewertet.

4 Ergebnisse

4.1 Übersicht der Grooming-Umgebungen

Um präventiv gegen Grooming vorgehen zu können und Kinder für risikoreiche Situationen zu sensibilisieren, ist es wichtig zu wissen, in welchen Umgebungen Männer mit einer sexuellen Präferenz für Kinder[5] groomen. Dazu sollten die Befragten zu Beginn des Interviews berichten, wie konkrete Grooming-Situationen bzw. Kontaktinitiierungen[6] gestaltet wurden. Tab. 1 zeigt, in welchen Umgebungen die Täter, unterteilt nach sexueller Präferenz und Umgebung, agierten. Die befragten pädophilen und hebephilen Täter hätten sowohl in Offline- als auch Online-Umgebungen agiert, um ein Kind zu groomen. Jedoch haben die Befragten, in Abhängigkeit ihrer sexuellen Präferenz, unterschiedliche Fokusse bei den Grooming-Umgebungen. Von den drei interviewten Pädophilen gaben zwei an, in Offline-Umgebungen Kinder gegroomt zu haben. So beschreibt ein pädophiler Befragter (kurz: PB) den Beginn des Groomings, der in seinem Bekanntenkreis stattgefunden habe. PB: *„Das Kind war […] mir halt für einen längeren Zeitraum anvertraut.“* Doch neben dem Grooming innerhalb seines Bekanntenkreises habe er auch versucht, Kontakte zu Kindern in

[5]Der Begriff *Kinder* umfasst alle, die unter 14 Jahre sind und ein kindliches oder frühpubertäres Körperschema aufweisen.

[6]Es ist anzumerken, dass nicht aus jedem Grooming ein sexueller Missbrauch hervorging, jedoch die beschriebenen Grooming-Prozesse mit dieser Zielintention geführt wurden. Aus diesem Grund wurden auch diese für die Auswertung berücksichtigt.

Tab. 1 Grooming-Umgebungen von pädophilen und hebephilen Tätern in Deutschland

	Pädophile Täter	Hebephile Täter
Offline-Umgebung	Alltagssituationen Bekanntenkreis/Nachbarn Familiärer Kontext	Freizeit/Hobby
Online-Umgebung	Soziale Medien Online-Spiele Erotikforen/-chats	Soziale Medien Online-Spiele Erotikforen/-chats

Alltagssituationen aufzubauen: *„ich war auf dem S-Bahnhof, hab' auf den Zug gewartet, ein Mädchen wartete auch auf den Zug […] wir hatten irgendwie Augenkontakt […] später sprach sie mich an und bat um Hilfe."* Ein weiterer PB beschreibt eine Grooming-Situation in einer Offline-Umgebung, in welcher er das Nachbarskind gegroomt habe: *„Also zuvor […] waren meistens die Eltern dabei […], aber danach kam es halt auch öfter zu Kontakten, wo ich speziell […] versucht habe, sie alleine zu erwischen."* Einschlägige Gründe, wieso sie primär in Offline-Umgebungen gegroomt hätten, gaben die beiden nicht an.

Neben den pädophilen Befragten schilderten auch hebephile Befragte (kurz: HB), wie sie in Offline-Umgebungen gegroomt hätten. Ein HB beschreibt Situationen, in denen er als Trainer im Volleyballverein Kontaktsituationen initiiert habe: *„weil ich im Volleyballverein bin und dort hat man natürlich auch Kontakt mit jüngeren Personen […] da denke ich, kamen schon so ein paar Momente, die nicht wirklich okay waren."* Des Weiteren schilderte er, dass er auch online sexuelle Kontakte zu den Kindern aus seiner Mannschaft gehabt habe, die durch Begegnungen in Online-Spielen oder sozialen Medien zustande gekommen seien: *„Automatisch dadurch, dass ich sehr viel in Online-Spielen und halt Social Media unterwegs bin. Da kommt es halt relativ schnell automatisch zustande. Da ist es nicht gezielt, sondern einfach […] das passiert dann meistens einfach."* Ein HB beschrieb, dass er über einen längeren Zeitraum offline Kontakt zu einem Mädchen gehabt hätte, welches er durch die Ausübung seines Hobbys kennengelernt hätte. Bei diesem Kontakt sei es wiederholt zu sexuellen Übergriffen gekommen. Nach Angaben des HB sei es zu Berührungen des Mädchens gekommen, die nach Angaben des Befragten *„zu intim"* gewesen seien.

Die Offline-Umgebungen wurden in den meisten wiedergegebenen Grooming-Prozessen auch um Interaktionen in Online-Umgebungen ergänzt. So standen die Befragten nach kurzer Zeit über Messenger oder soziale Medien in Kontakt mit den entsprechenden Kindern. Demnach finden Grooming-Prozesse, die in Offline-Umgebungen begonnen haben, aufgrund der zunehmenden

Vernetzung auch immer mehr in Online-Umgebungen wie den sozialen Medien statt bzw. werden dorthin verlagert.[7] Aus diesem Grund werden Online-Umgebungen im Folgenden gesondert betrachtet.

4.2 Online-Umgebungen

Unabhängig davon, ob die Kontaktinitiierung teilweise auch offline stattfindet, ist das Grooming in Online-Umgebungen bei beiden Gruppen, den pädophilen und hebephilen Tätern, ein ausgeprägtes Phänomen. Die Befragten gaben an, die Kinder über soziale Medien, Online-Spiele und Erotikforen/-chats zu kontaktieren, wobei es zwischen den beiden Tätergruppen in dieser Hinsicht keine Unterschiede zu geben scheint (siehe Tab. 2).

Dass das Internet eine dynamische Umgebung darstellt, beschreibt ein PB: *„Damals war es Knuddels, Jappy, vor 10, 12, 13 Jahren, heute ist es halt Instagram oder irgendwelche Spiele […] über Facebook werden sie heutzutage nichts mehr anmachen können oder nichts mehr finden.“* Demnach haben die Präferenztäter eine klare Vorstellung, wo sie potenzielle Opfer in den digitalen Medien kontaktieren können.

Bezüglich der Frage, warum die pädophilen und hebephilen Täter primär in Online-Umgebungen und nicht in Offline-Umgebungen Kontakte initiieren, nannten diese 1) ein zu hohes Risiko der Entdeckung in Offline-Umgebungen *(„Auf der Straße ist man ja der Situation ausgeliefert.“),* 2) eine einfachere Kontaktinitiierung *(„In der Online-Welt, zumindest hatte ich die Erfahrung gemacht, […] geht das Ansprechen einfacher.“)* und eine damit verbundene 3) niedrigere Hemmschwelle *(„Weil online, wenn keine weitere Reaktion kommt, fragt man […] gar nicht mehr. […] man bekommt keinen Korb, […] dann folgt man dem einfach nicht mehr oder blockiert [den Kontakt].“).* Selbst wenn die Täter eine direkte Abweisung durch die Kinder erfahren hätten *(„Was willst Du, Du bist doch bestimmt pädophil.“),* hätten sie aufgrund der Anonymität der Online-Umgebung keine Angst vor Konsequenzen gehabt. Auf die Frage, wieso sich so viele Kinder auf den fremden Kontakt einlassen, nannten die Befragten Neugierde aufseiten der Kinder und 4) die Einfachheit der Manipulation der Opfer als Gründe *(„Viele haben ein geringes Selbstvertrauen […] bei Tumblr ist es halt so, dass halt sehr viele Mädchen sehr leicht zu manipulieren sind.“).*

[7]Voraussetzung hierfür ist die materielle Ausstattung (z. B. Smartphone) und die Aktivität in Online-Welten (z. B. Account bei Instagram) der Kinder. Diese Voraussetzung trifft auf einen Großteil der Kinder zu.

Tab. 2 Online-Umgebungen von pädophilen und hebephilen Tätern in Deutschland

Online-Umgebung	Soziale Medien	Online-Spiele	Erotikforen/-chats
	Instagram	Fortnite	Nicht spezifiziert
	Facebook	Diabolo	
	YouNow	Minecraft	
	Snapchat	World of Warcraft	
	Tumblr		
	WhatsApp		

Neben den Online-Umgebungen (siehe Tab. 2), die die Befragten primär für ihre Grooming-Absichten nutzen, kommt es auch zu Grooming in Online-Umgebungen, die die Befragten laut eigenen Angaben nicht für die Kontaktinitiierung mit Kindern aufgesucht hätten. Gerade bei Online-Spielen bestünde das Interesse, seinen Spielpartner zu kennen, so die Befragten. Wenn Sympathie auf beiden Seiten bestehe, hätten die Täter versucht, den Kontakt auf einen gängigen Messenger zu verschieben: *„Wenn man sich sympathisch ist und vielleicht ein paar Mal miteinander gezockt hat, dann kann man ja auch mal versuchen zu fragen ‚Hey, hast Du Bock Nummern zu tauschen' […] und dann geht man halt über WhatsApp."* Ein weiterer PB berichtete, dass er regelmäßig in Erotikforen sei, um mit erwachsenen Frauen zu schreiben. Das Schreiben mit Kindern in den Erotikchats habe *„sich irgendwie so ergeben."* Ein anderer PB erzählte, dass er Instagram nutze, weil er sich für Fotografie interessiere und es automatisch durch das Posten und Kommentieren von Bildern zu Kontakten kommen würde. Ein weiterer HB gab an, dass er grundsätzlich viel online sei und dadurch Kontakte *„halt relativ schnell"* zustande kommen würden.

Zusammenfassung und zukünftige Forschung

Die vorliegende Studie untersuchte erstmals, in welchen Umgebungen Männer mit einer sexuellen Präferenz für Kinder Kontakte zu Kindern initiieren und ausbauen. Dabei zeigt sich, dass die Grooming-Umgebungen bei den Befragten sowohl offline (Alltagssituationen, Bekanntenkreis/Nachbarn und familiärer Kontext) als auch online (soziale Medien, Online-Spiele & Erotikchats) sind. In Abhängigkeit der spezifischen Phänomenologie der sexuellen Präferenz für Kinder zeigt sich, dass hebephile Täter vermehrt die Kontakte in Online-Umgebungen initiieren, um frühpubertäre Kinder zu groomen. Ein Grund hierfür könnte die höhere Wahrscheinlichkeit und Frequenz des Aufenthalts in

Online-Umgebungen bei frühpubertären Kindern sein, die eine Kontaktinitiierung in den angegebenen Online-Umgebungen erleichtert. Zusätzlich verfügen diese auch über die entsprechende materielle Ausrüstung wie Smartphone und Laptop, die unabhängig von der Erlaubnis der Eltern genutzt werden können. Dies trifft in Deutschland auf einen Großteil der 6–13-Jährigen Kindern zu (mpfs 2018).

Grundsätzlich begünstigen Online-Umgebungen auch aus Sicht unserer Befragten die Initiierung und Aufrechterhaltung des Grooming-Prozesses. Dabei nennen sie folgende Faktoren: 1) Geringes Risiko der Entdeckung, 2) Einfachheit der Kontaktinitiierung, 3) niedrige Hemmschwelle der Kontaktinitiierung und 4.) leichte Manipulation der Kinder. Vereinzelt gaben die Befragten an, dass es zu Kontaktinitiierungen kam, die ursprünglich nicht als Grooming intendiert gewesen seien, sondern durch ähnliche Online-Nutzungsmuster (z. Bsp. das Spielen des gleichen Online-Spiels) hervorgerufen wurden. Dies wirft die ethische Frage auf, inwieweit Erwachsene und Kinder gemeinsam Online-Spiele spielen sollten, wenn diese Interaktion nicht durch eine Aufsichtsperson überwacht werden kann. Rüdiger schlägt aus diesem Grund vor, dass Betreiber von sozialen Medien oder Online-Spielen sicherstellen müssen, dass Kinder wirksam vor den bestehenden Risiken durch Erwachsene geschützt werden oder, wenn dies nicht möglich ist, dass keine Erwachsenen oder im Umkehrschluss keine Kinder diese Seiten nutzen können (Rüdiger 2016).

Die weitgehende Unreguliertheit von Online-Umgebungen und speziell den sozialen Medien lässt den sexuellen Kindesmissbrauch, vermittelt durch das Internet, zu einem massiven Problem werden. Damit einhergehend ist die Rate der justiziell unentdeckten Taten und damit die Dunkelziffer enorm hoch. Laut Polizeilicher Kriminalstatistik (PKS) aus dem Jahr 2018 kam es zu 1391 Anzeigen wegen Online-Grooming. Gleichzeitig belegt die Studie des Instituts für Jugendkulturforschung, dass 30 % der 11–18-Jährigen mit sexuellen Belästigungen konfrontiert werden, weshalb von einer absoluten Konfrontationszahl im sechsstelligen Bereich auszugehen ist (Rüdiger 2019). Um dieser Entwicklung entgegen zu wirken, sind zum einen vor allem die Betreiber von Online-Plattformen gefordert, proaktiv und regulierend gegen Online-Grooming vorzugehen. Dabei erscheint die Installierung von Sicherheits- oder Warnsystemen relevant. So könnten automatisierte Inhaltsanalysen das Monitoring erleichtern und dabei helfen, sexuell missbräuchliche Kontakte zu unterbinden. Diese Technologie wird schon vereinzelt von Messenger-Programmen wie WhatsSafe eingesetzt, um Online-Grooming zu identifizieren und reduzieren. Die Installation von Warnsystemen wie WhatsSafe erfolgt über die Eltern. Dies setzt voraus, dass Eltern über die Problematik des Grooming aufgeklärt sind und über Wissen zu den Präventionsmöglichkeiten verfügen. Dies wiederum führt zu dem

Punkt, dass grundsätzlich Eltern und Kinder für das Thema des sexuellen Missbrauchs im Internet und des sexuellen Grooming sensibilisiert und entsprechende Hilfsstrukturen (z. B. Medienscouts wie Juuuport, Messenger-Warnsysteme wie WhatsSafe) kommuniziert werden müssen. Zum anderen müssen auf der Seite der (potenziellen) Täter präventive Maßnahmen und Behandlungsansätze geschaffen bzw. ausgeweitet werden, wie sie für pädophile und hebephile Täter durch das PPD schon existieren. Gleichzeitig müssen bestehende juristischen Maßnahmen verbessert und ausgebaut werden. So erscheint die Einrichtung von Polizeipräsenz in den digitalen Medien, welche über die Präsenz durch Accounts in sozialen Medien hinausgeht, sinnvoll, um eine schnellere Entdeckung der Taten zu ermöglichen und so die Dunkelzifferrelation zu senken. Ebenso ist die Ausweitung der Strafbarkeit auf das Versuchsdelikt im Bereich des online Grooming eine Möglichkeit, um (potenzielle) Täter abzuschrecken.

Einordnung und Limitationen der Studie

Die vorliegende Studie hat die Grooming-Umgebungen pädophiler und hebephiler Täter, die selbst-motiviert am PPD teilgenommen haben, untersucht. Die Ergebnisse der Studie stehen im Einklang mit bereits gefundenen Erkenntnissen aus der Literatur. So belegt diese Studie, dass es sich auch bei pädophilen und hebephilen Täter um eine heterogene Gruppe handelt (Babchishin et al. 2011), die unterschiedliche Grooming-Strategien nutzt (Kloess et al. 2017; Black et al. 2015; Quayle et al. 2014; Akhtar 2014). Dies spiegelt sich u. a. auch in der Nutzung der unterschiedlichen Offline- und Online-Umgebungen wider (Akhtar 2014). Wobei ein Großteil Online-Umgebungen nutzt, da diese aus Sicht der Befragten hohe Anonymität und ein geringes Risiko der Entdeckung gewährleisten (Briggs et al. 2011).

Trotz der Übereinstimmung mit dem Forschungsstand unterliegen die Ergebnisse Limitationen, die im Folgenden dargelegt werden: 1) Da es sich um eine explorative Stichprobe mit kleiner Fallzahl handelt, besitzen die Aussagen keine allgemeine Gültigkeit, sondern dienen vielmehr dem tiefer gehenden und beispielhaften Verständnis der Thematik. Um allgemein gültige Aussagen treffen und präventiv gegen Grooming vorgehen zu können, muss in zukünftiger Forschung eine größere Fallzahl untersucht werden. 2) In dieser Studie wurden ausschließlich männliche Täter mit einer Pädophilie und Hebephilie untersucht, die aufgrund ihrer sexuellen Präferenz ein erhöhtes Risiko für wiederholten sexuellen Kindesmissbrauch aufweisen. Da nur ein Teil aller sexuellen Missbrauchsdelikte gegen Kinder durch pädophile oder hebephile Täter verübt werden (Beier et al. 2015; Imhoff 2015) muss zukünftige Forschung sich auch mit männlichen und weiblichen Ersatzhandlungstätern auseinandersetzen. 3) Die Befragten wurden

über das PPD rekrutiert, was zu einer Einschränkung der Generalisierbarkeit auf die Gesamtpopulation von Menschen mit einer sexuellen Präferenz für Kinder führt. Die Teilnehmer des PPD erleben aufgrund ihrer Präferenz einen Leidensdruck und damit eine Störung ihrer sexuellen Präferenz, der sie zur Therapie motiviert. Somit sind sie nicht vergleichbar mit pädophilen und/oder hebephilen Menschen, die nicht unter ihrer sexuellen Präferenz leiden, es keine Gefahr für Selbst- oder Fremdgefährdung gibt oder die nicht problembewusst sind.

Literatur

Akhtar, Z. (2014). Child sex grooming: ‚Culture' crime, racial stereotyping and the environment. *European Journal of Crime, Criminal Law and Criminal Justice, 22*(2), 167–196. https://doi.org/10.1163/15718174-22022045.

Babchishin, K. M., Karl Hanson, R., & Hermann, C. A. (2011). The characteristics of online sex offenders: A meta-analysis. *Sexual Abuse A Journal of Research and Treatment, 23*(1), 92–123. https://doi.org/10.1177/1079063210370708.

Beier, K. M., Scherner, G., Gieseler, H., Siegel, S., Wagner, J., Kossow, S., Amelung, T., Grundmann, D., & Kuhle, L. (2015). Primärpräventive Therapieangebote bei Pädophilie und Hebephilie – Teil der Prävention sexuellen Kindesmissbrauchs im Dunkelfeld. *Interdisziplinäre Fachzeitschrift, 18*(2), 140–159.

Black, P. J., Wollis, M., Woodworth, M., & Hancock, J. T. (2015). A linguistic analysis of grooming strategies of online child sex offenders: Implications for our understanding of predatory sexual behavior in an increasingly computer-mediated world. *Child Abuse and Neglect, 44,* 140–149. https://doi.org/10.1016/j.chiabu.2014.12.004.

Bonta, J., & Andrews, D. A. (2007). *Risk-need-responsivity model for offender assessment and rehabilitation*. Ottawa: Public Safety Canada.

Briggs, P., Simon, W. T., & Simonsen, S. (2011). An exploratory study of internet-initiated sexual offenses and the chat room sex offender: Has the internet enabled a new typology of sex offender? *Sexual Abuse A Journal of Research and Treatment, 23*(1), 72–91. https://doi.org/10.1177/1079063210384275.

Canter, D., Hughes, D., & Kirby, S. (1998). Paedophilia: Pathology, criminality, or both? The development of a multivariate model of offence behaviour in child sexual abuse. *The Journal of Forensic Psychiatry, 9*(3), 532–555. https://doi.org/10.1080/09585189808405372.

Craven, S., Brown, S., & Gilchrist, E. (2006). Sexual grooming of children: Review of literature and theoretical considerations. *Journal of Sexual Aggression, 12*(3), 287–299. https://doi.org/10.1080/13552600601069414.

Gupta, A., Kumaraguru, P., & Sureka, A. (2012). Characterizing pedophile conversations on the internet using online grooming. arXiv:1208.4324 *[cs]*. Abgerufen von http://arxiv.org/abs/1208.4324.

Hanson, R. K., & Morton-Bourgon, K. E. (2005). The characteristics of persistent sexual offenders: A meta-analysis of recidivism studies. *Journal of Consulting and Clinical Psychology, 73*(6), 1154–1163. https://doi.org/10.1037/0022-006X.73.6.1154.

Herrmann, B. (Hrsg.). (2008). *Kindesmisshandlung: medizinische Diagnostik, Intervention, und rechtliche Grundlagen*. Heidelberg: Springer Medizin.

Imhoff, R. (2015). Punitive attitudes against pedophiles or persons with sexual interest in children: Does the label matter? *Archives of Sexual Behavior, 44*(1), 35–44. https://doi.org/10.1007/s10508-014-0439-3.

Kloess, J. A., Hamilton-Giachritsis, C. E., & Beech, A. R. (2017). Offense processes of online sexual grooming and abuse of children via internet communication platforms. *Sexual Abuse*, 1079063217720927. https://doi.org/10.1177/1079063217720927.

Kuhle, L. F., & Stelzmann, D. (2018, 08.-31.08). *Pedophilia and online sexual grooming of children in the Dunkelfeld*. Gehalten auf der International Association for the Treatment of Sexual Offenders, Vilnius.

Lamnek, S. (2008). *Qualitative Sozialforschung: Lehrbuch* (4., vollst. überarb. Aufl., [Nachdr.]). Weinheim: Beltz PVU.

mpfs. (2018). KIM-Studie 2018. Kindheit, Internet, Medien. https://www.mpfs.de/fileadmin/files/Studien/KIM/2018/KIM-Studie2018_Web.pdf.

Polizeiliche Kriminalstatistik Bundesrepublik Deutschland, Jahrbuch. (2018). https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2018/pks2018_node.html.

Quayle, E., Allegro, S., Hutton, L., Sheath, M., & Lööf, L. (2014). Rapid skill acquisition and online sexual grooming of children. *Computers in Human Behavior, 39,* 368–375. https://doi.org/10.1016/j.chb.2014.07.005.

Rüdiger, T.-G. (2016). Onlinespiele – Ein kritisches Spielfeld für Kinder und Erwachsene? Eine kriminologische Betrachtung auf das alterslose Zusammenspiel in Onlinespielen. Digitale Spiele im Diskurs. http://www.fernuni-hagen.de/KSW/portale/ifbm/bildung_medien/medien-im-diskurs/digitale-spiele-im-diskurs/.

Rüdiger, T.-G. (2019). Polizei im digitalen Raum. http://www.bpb.de/apuz/291183/polizei-im-digitalen-raum?p=all.

Sklenarova, H., Schulz, A., Schuhmann, P., Osterheider, M., & Neutze, J. (2018). Online sexual solicitation by adults and peers – Results from a population based German sample. *Child Abuse and Neglect, 76,* 225–236. https://doi.org/10.1016/j.chiabu.2017.11.005.

Staksrud, E. (2013). Online grooming legislation: Knee-jerk regulation? *European Journal of Communication, 28*(2), 152–167. https://doi.org/10.1177/0267323112471304.

Williams, A. (2015). Child sexual victimisation: Ethnographic stories of stranger and acquaintance grooming. *Journal of Sexual Aggression, 21*(1), 28–42. https://doi.org/10.1080/13552600.2014.948085.

Winters, G. M., & Jeglic, E. L. (2017). Stages of sexual grooming: Recognizing potentially predatory behaviors of child molesters. *Deviant Behavior, 38*(6), 724–733. https://doi.org/10.1080/01639625.2016.1197656.

Wolak, J., Finkelhor, D., Mitchell, K. J., & Ybarra, M. L. (2008). Online „predators“ and their victims: Myths, realities, and implications for prevention and treatment. *American Psychologist, 63*(2), 111–128. https://doi.org/10.1037/0003-066X.63.2.111.

Ybarra, M. L., Leaf, P. J., & Diener-West, M. (2004). Sex differences in youth-reported depressive symptomatology and unwanted internet sexual solicitation. *Journal of Medical Internet Research, 6*(1), e5. https://doi.org/10.2196/jmir.6.1.e5.

Normenkontrolle und digitale Polizeiarbeit

Kriminalität und Unsicherheit im virtuellen Raum

Perspektiven aus Kriminologie und Medienpädagogik

Stefan Piasecki und Dorothee Dienstbühl

1 Einleitung

Die Sozialisation junger Menschen geschieht heute vor allem und immer stärker durch Medien. Dies ergibt sich aus dem Wandel der Bevölkerungsstruktur und einer zunehmend geringeren Zahl von Menschen in ihrer jeweiligen Alterskohorte, aus der mobilen Gesellschaft und resultiert weiterhin aus einer starken Konsumneigung und -orientierung. Eltern sind ganz oder teilweise berufstätig oder Kinder wachsen in Haushalten von Alleinerziehenden und/oder Patchworkfamilien auf, Sozialkontakte ergeben sich weniger durch Gleichaltrige in unmittelbarer Nachbarschaft als vielmehr online. Die „peer group“ setzt sich nicht mehr alleine aus einer physischen „Clique“ zusammen, sondern der „Onlinecommunity“. Lebenserfahrungen werden somit seltener im direkten Gespräch erörtert als durch Social-Media-Kanäle, zu denen Kommunikations-Apps wie Whatsapp und auch Selbstdarstellungsplattformen wie Facebook oder Videoportale zählen. Entsprechend erfolgt die Suche nach Freunden, vor allem aber nach Partnern, seit Jahren immer häufiger durch Online-Angebote (vgl. z. B. JIM-Studie 2016). Somit generieren menschliche Bedürfnisse nach sozialen Kontakten, Freundschaft und Liebesbeziehungen entsprechende

S. Piasecki (✉)
Fachhochschule für öffentliche Verwaltung NRW, Mülheim, Deutschland
E-Mail: stefan.piasecki@fhoev.nrw.de

D. Dienstbühl
FHöV NRW, Mülheim an der Ruhr, Deutschland
E-Mail: dorothee.dienstbuehl@fhoev.nrw.de

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

T.-G. Rüdiger und P. S. Bayerl (Hrsg.), *Cyberkriminologie,*
https://doi.org/10.1007/978-3-658-28507-4_20

Kriminalitätspotenziale. Doch auch privates Geschäftsgebaren hat sich immer weiter in den virtuellen Raum verlagert: Käufe werden online getätigt, die Kontoführung via Onlinebanking eigenständig vorgenommen. Entsprechend lukrativ sind Verfahren zum Phishing von Daten und den unterschiedlichsten Formen von Betrug.

Nutzer von sozialen Medien sind bedroht von Kommunikation und Inhalten, denen sie realweltlich möglicherweise nicht ausgesetzt wären, weil sie nicht Teil einer bestimmten Subkultur sind oder ihre Vorlieben und Interessen sie normalerweise nicht in Kontakt bringen mit Pornografie, anstößigen Bildern und Videos oder radikalen bzw. extremen Texten. Das, was bis vor einigen Jahren bei der Beschaffung mit einem gewissen individuellen Risiko der Entdeckung bzw. Strafbarkeit durch Besitz versehen war, findet sich nunmehr leicht auffindbar im Internet. Weder müssen Erzeugnisse wie Snuff-Filme oder harte Pornos unter dem Ladentisch gekauft, noch müssen Szenetreffs besucht werden, um Kontakt zu einschlägigen Kreisen zu bekommen. Hierbei war man in der Vergangenheit physisch sichtbar, konnte das individuelle Risiko der Entdeckung jedoch durch das Ausweichen in eine andere Stadt oder gewisse Geschäftszeiten minimieren.

Aufgrund der direkten Zurechenbarkeit aller Onlineaktivitäten und der Sichtbarkeit individueller Profile und ihrer Follower bzw. erteilter „Likes“ ist es leicht möglich, von anderen eingeschätzt und in den eigenen Charaktereigenschaften bewertet zu werden. Sie werden zum Ziel einschlägiger Angebote oder auch von Angriffen durch Gegner bestimmter Positionen (Tierschützer, politische Extremisten etc.). Andererseits erweitert Social Media den Kreis möglicher Gleichgesinnter schnell und effektiv, die wiederum aktivierbar sind (rbb24 2019). Die theoretische Unbegrenztheit der Reichweite von Kommunikation und Teilnehmern bei aufrecht zu erhaltener Anonymität (zumindest aus Sicht von Laien) bildet die spezifische Herausforderung von Täter-Opfer-Beziehungen in der Virtualität (s. a. Kap. „Digitaler Vigilantismus“) und verdeutlicht den Grad von Verwundbarkeit und Betroffenheit:

> „Despite the fact that traditional bullying can occur elsewhere in the community than school, cyberbullies can by using communication technology in an anti-social way penetrate the walls of the victim’s home environment. If the victimized teen prefers not to switch off the cellular phone at night, he or she may be a perpetual target for cyberbullies, whereas the victim of traditional bullying can find a safe retreat at home.“ (Heirman und Walrave 2008)

2 Ausgewählte Formen von Cyberkriminalität

Zu den häufig berichteten und öffentlich diskutierten Cyberdelikten zählen Verletzungen von Cyberidentität und Beeinträchtigungen der Onlinesozialisation. Dazu gehören Identitätsdiebstähle oder -fälschungen zum Zwecke des Betruges oder der Erpressung und Bedrohung („blackmailing"). Ebenso relevant sind Cybermobbing/-bullying, Cyberstalking und Cybergrooming, während Aktivitäten mit Aufforderungscharakter, die sich an die bekannten Kettenbriefe anlehnen, seltener sind, aber nicht weniger Aufmerksamkeit erzeugen (s. a. Kap. „Grooming-Umgebungen von pädophilen und hebephilen Männern in Deutschland"). Vor allem die multimedialen und Netzwerkfähigkeiten moderner mobiler Plattformen können gezielt instrumentalisiert und eingesetzt werden, wie die sog. „Blue Whale Challenge", mittels derer Teilnehmende zu späteren Selbstmorden herangeführt wurden.

2.1 Cybermobbing und Cyberbullying

Cybermobbing und Cyberbullying werden als Begriffe häufig synonym verwendet. Im Gegensatz zum interpersonalen Mobbing erstreckt sich Cybermobbing über den Ort der direkten Konfrontation hinaus in die Privatsphäre. Nicht mehr der Arbeitsplatz oder die Schule sind Schauplatz, sondern alle jene Orte und Zeiten, zu denen ein Mensch online ist und erreichbar für verletzende Inhalte. Einige Erklärungsansätze differieren zwischen den Phänomenen Bullying und Mobbing, indem sie die beabsichtigte längerfristige Beeinträchtigung einer Person (Präventionsportal „Lilli" 2019) oder eine körperliche Schädigung als Ziel einbeziehen (Präventionsportal „Mobbing-out" 2019).

Cyberbullying ist:

> „an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend him or herself. […] Some cyberbullying can combine the anonymity of the aggressor found in conventional indirect aggression with the targeted attack on the victim found in conventional direct aggression" (Smith et al. 2008, S. 376).

Cyberbullying ereignet sich stets zwischen mindestens zwei Personen in einer sozio-strukturellen Konstellation unter Menschen, die sich meistens bereits kennen (Festl und Quandt 2015, S. 109 f.). Hier werden daher digitale Kommunikationskanäle zur Ansprache von Personen und ihres näheren Umfeldes

genutzt, ohne notwendig eine breitere Rezeption anzustreben (Festl und Quandt 2015). Gleichwohl ist die Zahl möglicher Adressaten hoch, ebenso wie die Qualität der sozialen Bedeutung:

> „Except for family, school and classes are the most stable social contexts in adolescent's life. They not only spend most of their time in school but also find a large portion of their social contacts in this setting" (Festl und Quandt 2015, S. 110).

Festl und Quandt (2015) fanden sechs Merkmale von Cyberbullying, die von den Teilnehmenden ihrer Untersuchung besonders häufig berichtet wurden:

1. gesendete verletzende Botschaften (insulting messages),
2. geschriebene verletzende Inhalte auf einer Webseite (write insulting things on a public website),
3. verletzende Bilder von jemandem hochladen (upload embarassing pictures of someone),
4. Botschaften unter einer falschen Identität schreiben (write messages using a fake identity),
5. Gerüchte über das Internet verbreiten (spread rumors in the Internet) und
6. persönliche Informationen an andere senden (forward personal information to others).

22,5 % der Befragten berichteten, von einem der genannten Phänomene in der Vergangenheit Opfer gewesen zu sein (Festl und Quandt 2015). Die Befragten konnten zudem drei Kategorien zugeordnet werden: 11,7 % (n = 602) berichteten von Viktimisierungserfahrungen, 11,1 % von aktiven Täterhandlungen (n = 627) und 33,4 % (n = 1889) von Betroffenheitserlebnissen durch Cyberbullying (Festl und Quandt 2015).

Eine weitere Form der Bedrohung/Beeinträchtigung ist das Cyberstalking. Darunter wird das Nachstellen einer Person verstanden, wobei häufig die gleichen Technologien und Verfahren zum Einsatz kommen wie bei Cyberbullying und -mobbing. Um den Aufenthaltsort einer Person herauszufinden oder diese zu überwachen und ihr Kommunikationsverhalten auszuspähen wird verzeichnet, wann die Person online ist, ob sie Nachrichten liest und mit wem sie Kontakt hat. Dies kann durch Kontrollfragen an die Person oder mutmaßlich mit ihr bekannte andere Personen geschehen. Ebenso können Persönlichkeitsprofile, Interessen oder Standorte ausgelesen und verwendet werden. So kann ein Individuum belastet und sein Umfeld in Mitleidenschaft gezogen werden, wenn dieses des Vorganges gewahr wird und sich bspw. durch eigene Ängstigung abwendet.

Formen virtuellen Fehlverhaltens müssen nicht immer mit destruktiver Absicht verübt werden, sondern haben bisweilen schlicht die Festigung des Status des Tatausführenden in der eigenen *peer group* zum Ziel (Festl 2015, S. 281) bzw. ergeben sich aus vorhandener „peer pressure“, um u. U. für jemand anderen tätig zu werden oder einen vermeintlichen Schaden zu rächen.

2.2 Cybergrooming

Cybergrooming umschreibt den zielgerichteten Versuch, über ICT Kontakt mit Kindern oder Minderjährigen aufzunehmen zum Zwecke der sexuellen Annäherung (Wachs et al. 2012, S. 628). Das Ziel kann ein körperlicher ebenso wie seelischer Missbrauch sein oder die Inaugenscheinnahme von Bildern und Videos (Rüdiger 2012, S. 31). Etwa ein Viertel der Internetnutzer (Statista 2018) sind in den „letzten 12 Monaten“ mit Grooming oder sexueller Gewalt im Netz in Kontakt gekommen (Regelmäßig: 2 %, Manchmal: 6 %, Selten: 17 %) (Rüdiger 2012). Charakteristisch für das Grooming sind der Aufbau längerer Beziehungen und die Schaffung von Vertrauen, damit das Gegenüber sich öffnet, Informationen teilt und letztlich Bilder sendet oder sogar bereit wird zu einer Beziehung. So gut wie alle Formen von Onlinekriminalität finden sich hier: Fake Identities zur Vortäuschung von Alter, Geschlecht oder Interessen bis hin zum Stalking oder der Kontaktaufnahme mit tatsächlichen Bekannten der Zielperson, die dann als unfreiwillige Zeuge/Bestätigungsperson der Fakeidentität des Täters dienen kann. Mathiesen zählt die Einwirkung auf „eine Person unter 14 Jahren“ sowie die „Einflussnahme auf den Willen des Opfers“ zu eindeutigen Merkmalen, wenn diese sich durch „Hartnäckigkeit“ auszeichnet und durch „Schriften“ erfolgt (Mathiesen 2014, S. 19; siehe dort auch zur juristischen Diskussion des Wesens einer „Schrift“).

Tätern dienlich wird das oft geringe Anzeigeverhalten durch Kinder aufgrund von Scham oder weil sie den Ermittlungsbehörden eine Aufklärung nicht zutrauen (a. a. O., S. 23). Katzer (2014, S. 39) hält Mädchen online sogar für ehrlicher als Jungen. Wachs et al. (2012, S. 632) zählen weitere Faktoren auf, die als Bedingungen für Cybergrooming vorausgesagt werden können: Mädchen zu sein, eine grundsätzliche Offenheit und Bereitschaft, Fremde in der Realwelt zu treffen wie erlebte Cybermobbingerfahrungen. Sie verweisen jedoch auf zusätzlich gefährdete Zielgruppen, für die ICT- und Social Media-Systeme eine besondere Bedeutung haben mögen, die jedoch von der Forschung noch nicht ausreichend berücksichtigt worden seien:

> „Such understudied groups are adolescents with special needs or lesbian, gay, bisexual, and transgender (LGBT) adolescents. ICTs may have a key function for LGBT adolescents and adolescents with disabilities to get in contact with consensual partners and also may be used for crossing physical borders.“ (Wachs et al. 2012)

Erkennbar wird an dieser Anmerkung auch die Notwendigkeit, präventiv und aufklärend tätig zu werden und breite gesellschaftliche Gruppen und Milieus in ihrer spezifischen Gefährdung zu berücksichtigen.

2.3 Romance-Scamming

Love- oder Romance-Scamming bezeichnet Betrugsverfahren, bei denen bewusst mit dem Bedürfnis nach einer Liebesbeziehung Gelder vom Opfer erbeutet werden (s. a. Kap. „Liebesschwindel im Cyberspace“). Die Täter tummeln sich entsprechend in Online-Partnerbörsen und besitzen zudem ein Profil in einschlägigen sozialen Netzwerken wie Facebook (Bundeskriminalamt Österreich o. J.). Zur Kontaktaufnahme verwenden sie Fake-Profile, häufig mit fremden oder gestohlenen Bildern (ProPK o. J.), und treten als Singles mit interessanten Lebensgeschichten und den gleichen Ansichten wie die des Opfers auf. Sie finden heraus, was sich ihre Opfer von einem Partner wünschen und konstruieren damit ihre falsche Identität. Dabei gibt es Unterschiede zwischen den Geschlechtern: Männliche Scammer behaupten, sie seien Ingenieur, Architekt, IT-Fachmann oder Arzt, regelmäßig im humanitären Einsatz, beispielsweise in Afrika. Ihre Hauptzielgruppe sind Frauen ab 40. Weibliche Scammer suchen gezielt nach wohlhabenden Männern und geben sich bevorzugt als Krankenschwester, Ärztin, Lehrerin oder Schauspielerin aus. Es handelt sich somit um Berufe, die auf das andere Geschlecht besonders attraktiv wirken.

Bei dieser Form des Betruges geht es darum, das Opfer in eine emotionale Abhängigkeit zu bringen. Mittels „love-bombing“, also dem Überschütten mit Komplimenten, Liebesbezeugungen und ständigem Kontakt wird eine psychische Kontrolle über das Opfer erlangt (ProPK o. J.). Nach Kontaktaufnahme erfolgt der Vertrauensaufbau. Die Täter präsentieren sich als interessiert, humorvoll, sensibel und zuverlässig. Gleichzeitig erzählen sie viel von sich, angeblichen Erlebnissen und persönlichen Schicksalsschlägen. Das Opfer soll sich einerseits geschmeichelt von der Person und andererseits für deren Wohlergehen verantwortlich fühlen. Wenn die emotionale Bindung aufgebaut ist, betätigen sich die Scammer in emotionaler Erpressung, die mit Geldforderungen einhergeht:

Eine kranke Mutter, eine missliche Situation, Erpressung usw., werden als Anlass genommen, um Geld vom Opfer zu fordern (Bundeskriminalamt Österreich o. J.). Das Geld soll dabei bevorzugt via Money-Transfer-Diensten angewiesen werden, da diese Methode nur schwer für Ermittler nachzuvollziehen ist (Bundeskriminalamt Österreich o. J.). Sobald kein Geld mehr vom Opfer gezahlt werden kann, erfolgt der Kontaktabbruch. Whitty und Buchanan (2012, S. 8) verweisen auf die doppelte Viktimisierung der durch den Verlust ihres Vertrauten und dem Geld entsteht, zudem sei die Scham bei dieser Opfergruppe besonders hoch.

2.4 Internetphänomene wie Blue Whale Challenge

Die schnellen und direkten Kommunikationsmöglichkeiten der Mobiltelefonie, verbunden mit ihren multimedialen Fähigkeiten zur Erstellung von Bildern und Videos sowie den technischen Funktionen wie Positionserkennung (GPS) ermöglichten die Etablierung gänzlich neuer Aktivitätsformen oder die Abwandlung bekannter. Ähnlich der traditionellen Kettenbriefe können ICT-Nutzer auf „Challenges“ geschickt werden. Sie suchen verborgene Schätze (Geo-Caching) oder unternehmen Mutproben. Als „Blue Whale Challenge“ wurde ab 2015 eine destruktive Form der kettenbriefartigen Mutprobe bekannt, die dazu führen sollte, dass Teilnehmer Suizid begingen. Teilnehmende unternehmen bestimmte Aufgaben (bspw. sich einritzen oder mehrere Stunden auf einem Balkon stehen) (Singh et al. 2018, S. 1). Ferrero de Sousa et al. (2017, S. 796) verorten den Beginn der Selbstmordwelle 2015 in Russland und zählten bis 2017 eine Zahl von 130 Selbstmorden alleine dort, die sich auf die *Challenge* zurückführen ließen; sie geben jedoch zu bedenken, dass diese Zahlen nicht offiziell bestätigt sind (a. a. O., 797). Singh et al. betonen, dass es trotz der breiten Medienberichterstattung lange keinen in der medizinischen Fachliteratur dokumentierten Fall gegeben habe (2018, S. 1) – aber berichten den Fall eines Betroffenen in ihrer eigenen klinischen Praxis, der von seinem Vater gebracht wurde und bereits sechs der Challenges durchgeführt hatte (Singh et al. 2018). Der Vater löschte die Applikation und der Junge berichtete, dass er sie nicht mehr installiert hätte und auch nicht weiter teilnehmen wolle, gleichwohl aber neugierig sei auf die weiteren Aufgaben, die auf ihn gewartet hätten.

In der Challenge kommen mehrere Elemente zur Wirkung, die einzigartig für moderne Mediengesellschaften sind: Gleichzeitigkeit und Unmittelbarkeit verbinden sich mit einer quasi unbegrenzten Teilnehmerzahl, Selbstwirksamkeitserfahrungen, individuellen Motiven nach Geltung und Leistung sowie Neugierde. Spielende erreichen, wie bei Computerspielen auch, einen „Flow“-Zustand, in

welchem sie spüren, dass neue Herausforderungen leistbar sind, denen sie sich stellen und die auf einer höheren Herausforderungsstufe wieder das Gefühl von Erfolg vermitteln (Piasecki 2018, S. 290 ff.). Social-Media-Kanäle, die im Minutentakt neue Bilder und Nachrichten posten, setzen dann manche Jugendliche unter Druck, dabei mithalten zu müssen: *„It is depressing to watch friends having fun and posting selfies and the temptation to compare their own life to the perfectly depicted life that friends portray online"* (Shakir et al. 2018, S. 380).

Shakir und Sharma listen Selbstmordfälle aus 11 Ländern auf und stellen eine Relation zwischen *realer* Einsamkeit/Unbetreutheit her und *virtueller* Eingebundenheit in Netzwerke und Aktivitäten, die Betroffene langsam von den üblichen Gewohnheiten und Kontakten entfremden. Sie rufen insbesondere Schulen auf, Informationen und Aufklärung über schädliche Internetphänomene zu bieten (a. a. O., 384).

3 Opfererfahrungen und Kriminalitätsfurcht

Vulnerable Situationen und Opfererfahrungen werden in ebensolchem Maße online gemacht, wie sich das Leben von Menschen aus ihren realweltlichen Lebensinseln (Baacke 1984) in die „Scheinräume" (so Zeiher bereits 1983) der Virtualität verlagert. Die sich darbietende Vielfalt der Möglichkeiten, Heterogenität und Multioptionalität bieten eine große Bandbreite an Repräsentation der individuellen Identität – aber auch der Grenzüberschreitungen. Opfer werden oder sind nicht selten auch Täter oder andersherum. Die Virtualität und ihre vermeintliche Anonymität sowie die gegenüber direkter Kommunikation veränderte Wahrnehmung von Nähe bei Online-Kommunikation verleiten zu einem veränderten Wahrnehmungs- und Schutzverhalten (Ben-Ze'ev 2004, S. 55 f.). Deutlich gemacht werden muss, dass von den genannten und auszuführenden Problemkonstellationen nicht nur Jugendliche, „digital natives", betroffen sind, sondern alle Altersgruppen und nicht zuletzt auch Senioren, die sogenannten „digital mellowed" – welche sich spätestens seit der Verbreitung von mobilen Endgeräten (Smartphones, Tablets) mit moderner ICT (Information and Communication Technology) beschäftigen, selbst wenn ihnen dies kaum bewusst ist und sie nur den Kommunikations- oder Shopping-Aspekt sehen. So sind denn auch Emails und die Suche nach Produktinformationen oder Finanzdienstleistungen die häufigsten Anwendungen bei älteren Nutzern (Suhr und Statista 2017).

Die Bedingungen für Vulnerabilität sind jedoch unterschiedlich. Während Adoleszente ihre eigene Identität in Abgleich bringen mit der Umwelt und

Spielräume zur Entwicklung suchen, austesten, erweitern und verändern, wollen ältere Nutzer selbst- und eigenständig bleiben sowie bestehende Kontakte nicht verlieren. Jüngere sind über ihre Identitätsunsicherheiten eher anfällig für moderne Phänomene wie Cybermobbing und -bullying; ältere für virtualisierte Formen klassischer Betrugsmuster. Beiden Opfergruppen gemein ist jedoch eine teilweise Hilflosigkeit und Scham nach eingetretener Viktimisierungserfahrung: Anstatt sich realen Bezugspersonen anzuvertrauen, versuchen sie häufig, ihre Opfererfahrungen alleine zu verarbeiten und die Taten gegen sie zu vertuschen.

Berichte über das Ausmaß von Cyberkriminalität zeigen, dass jeder Mensch zum Opfer werden kann. Dies hat wiederum Einfluss auf die Wahrnehmung von Kriminalität und damit einhergehend mit der persönlichen Kriminalitätsfurcht. Zum einen erfahren Menschen gerade aus dem Internet von Kriminalität, zum anderen ist Internetnutzung jedoch auch ein Risikofaktor.

Kriminalitätsfurcht kann hinsichtlich einer gesellschaftlich/sozialen und einer personalen Komponente unterschieden werden. Soziale/gesellschaftliche Kriminalitätsfurcht bezieht sich auf die Einschätzung der Bedeutung, des Ausmaßes und der Entwicklung der Kriminalität als soziales Problem einer Gesellschaft im Kontext zu anderen Problemen wie Arbeitslosigkeit, Inflation, etc. (LKA NRW 2006, S. 3). Häufig steht die Sorge über Kriminalität als gesellschaftliches Problem hinter sozialen Problemen zurück; es sei denn, es gab gravierende Kriminalitätsformen, wie beispielsweise Terroranschläge. So zeigte die 25. Befragung der R&V Versicherungen, dass die Sorge vor Terroranschlägen erstmals auf dem ersten Platz lag, gefolgt von Angst vor Extremismus und Spannungen durch den Zuzug von Ausländern (R&V 2016). Dies konnte unmittelbar auf die Terroranschläge in Europa im Sommer 2016 bezogen werden. Entsprechend hoch blieb das Angst-Niveau hinsichtlich Terrorismus noch in der Befragung 2017, bei welcher nun der Terroranschlag von Berlin im Dezember 2016 berücksichtigt werden musste (vgl. R&V 2017). Die personale Komponente bezieht sich auf eigene Opfererfahrungen.

Das subjektive Sicherheitsempfinden ist ein wichtiger Parameter der Sicherheitspolitik, entsprechend häufig werden Befragungen zur Kriminalitätsfurcht durchgeführt und mit Dunkelfeldstudien gekoppelt (Baier et al 2011, S. 45 f.; Clages und Zeitner 2016, S. 188; Bock 2013, S. 325). Internetkriminalität wirkt sich vor allem auf die personale Kriminalitätsfurcht aus: Persönliche Erfahrungen oder solche von Angehörigen, Freunden und Bekannten verunsichern Internetnutzer. Nicht nur die entstehende Furcht, sondern auch die Opferwerdungsprozesse zu erläutern, ist Gegenstand der Kriminologie.

4 Internetkriminalität als Forschungsfeld der Kriminologie

Die Kriminologie befasst sich mit sämtlichen Facetten kriminellen Verhaltens. Es gibt diverse Ansätze für Definitionen, die allesamt ihre Stärken und Schwächen haben (Pientka 2014, S. 146 ff.). Als empirische Wissenschaft basieren sämtliche Analysen auf systematisch erfasstem Erfahrungswissen. Daher muss die Kriminologie als interdisziplinärer Forschungsbereich verstanden werden, da sie auf sämtlichen empirischen Wissenschaften basiert, die Erkenntnisse über das Zusammenleben und menschliches Verhalten bieten (Schwindt 2016, S. 8 f.). Bedürfnisse und Verhaltensweisen, die Menschen zum Opfer machen, sind Gegenstände der Kriminologie und damit Grundlage für die kriminalistische Ermittlungsarbeit (Schwarz in: Artkämper und Clages 2015, S. 305). Insbesondere der Opferwerdungsprozess, Verhalten und Anteil der Opfer, sowie die Auswirkungen der Kriminalität auf die Opfer sind Gegenstand der Viktimologie, einem Teilbereich der Kriminologie (s. a. Kap. „Cyber-Viktimisierung von Unternehmen“). Untersuchungen von Martin P. Seligman ergaben durch Nutzung umstrittener Tierversuche, dass Menschen nach einem traumatisierenden Erlebnis eine passive Haltung einnehmen, die, beeinflusst durch mangelndes Selbstwertgefühl und Hilflosigkeit, sie schneller wieder zu Opfern werden lassen („Theorie der erlernten Hilflosigkeit“, vgl. Pientka 2014, S. 226). Gerade beim (Cyber-)Mobbing lässt sich eine solche Haltung an Opfern beobachten: Sie können durch ihre passive Haltung immer wieder zur Zielscheibe entsprechender Attacken werden.

Die Theorie des „Lebensstilkonzepts“ legt ihr Augenmerk auf die Verhaltensweisen von Menschen, die ihr Risiko erhöhen, Opfer von Straftaten zu werden (Pientka 2014, S. 225). Hierbei geht es vor allem um leichtsinniges Verhalten, wie beispielsweise seinen Computer nicht mit Virenschutz zu versehen, Passwörter offen liegen zu lassen oder auch sich auf sozialen Netzwerken offen jegliche persönlichen Daten, Lebensumstände und Aktivitäten mitzuteilen. Die Betrachtung der Lebensgewohnheiten, die einen Menschen zu einem attraktiven Ziel für Täter werden lassen, untersucht der Ansatz der Routine-Activity-Theory (BKA 2015, S. 63 f.).

Gerade die Möglichkeiten des Internets und insbesondere sozialer Netzwerke machen zunächst Milliarden User zu potenziellen Zielen krimineller Bestrebungen. Dabei rückt aber nicht nur die Frage in den Vordergrund, was einen User zum geeigneten Opfer macht, sondern auch, welche Schutzfaktoren fehlen, die die Opferwerdung erschweren würden. Genau diese Frage ist ein besonders wichtiger Ansatz für die Präventionsarbeit, der insbesondere in

Informationsmaterialien aufgegriffen wird (BKA 2015, S. 65; s. a. Kap. „Alter Wein in Neuen Medien?“). Warum gerade ältere Menschen auf mitunter sehr grobe und durchschaubare Betrugsmaschen hereinfallen, kann mit der Neurobiologischen Opfertheorie besser nachvollzogen werden. Shelley E. Taylor stellte in vergleichenden Untersuchungen zwischen Gruppen mit älteren (Durchschnittsalter 68 Jahre) und jüngeren Probanden mit einem Durchschnittsalter von 23 Jahren fest, dass die Gruppe der Älteren eine Nicht-Vertrauenswürdigkeit bei ihrem Gegenüber nicht einschätzen konnten, während die jüngeren Probanden damit kein Problem hatten (Pientka 2014, S. 227). Tylor nahm zur Ergründung der Frage, warum die Fähigkeit eines gesunden Misstrauens im Alter offensichtlich nicht mehr ausgeprägt ist, ein MRT zu Hilfe. Dabei stellte sie fest, dass das Zeigen wenig Vertrauen erweckender Gesichter bei den jüngeren Probanden deutliche Aktivitäten in der Inselrinde (einem Teil der Großhirnrinde) aufwies, während diese bei den älteren Probanden inaktiv blieb (a. a. O., S. 228). Dieser Umstand kann möglicherweise auch auf virtuelle Betrugsmaschen angewandt werden, die für ältere Menschen trotz offensichtlich unseriöser Inhalte nicht erkennbar sind, weil sie kein Misstrauen empfinden.

5 Medienpädagogische Perspektiven

Virtuelles Fehlverhalten ist, wie auch reales, eine Form sozial nicht akzeptierter Devianz (Festl 2015, S. 201, 281). Festl empfiehlt eine soziale Netzwerkanalyse, um die sozialen und Mobbingstrukturen eines Umfeldes sichtbar zu machen (a. a. O., S. 284). Die Schule als, wenn schon nicht Tatort, so doch häufig Ort des gemeinsamen Treffens von Tätern und Opfern, gilt als *„sozialer Komplex und bietet Ansatzpunkt für entsprechende Maßnahmen auf unterschiedlichen Ebenen“* (a. a. O., S. 288). Gerade Schulen sieht Katzer hier jedoch wenig gut vorbereitet, denn nicht nur gebe es dort grundsätzlich wenige Informationsveranstaltungen zu „neuen Medien“ (Katzer 2014, S. 158), Themen wie Mobbing/Bullying oder Grooming fehlten sogar vollständig (Katzer 2014). Allerdings berichten Wachs und Wolf (2011, S. 742), dass *„einen Lehrer bzw. eine Lehrerin aufzusuchen“* überhaupt nur für *„einen verschwindend geringen Teil (2,4 %) der Betroffenen in Frage“* käme (Wachs und Wolf 2011). Dies spräche dafür, dass gerade Schulen und ihr Personal Nachholbedarf haben und um ihre Akzeptanz ringen müssen.

Einen Lösungsansatz sieht Katzer in verbesserten Anforderungen an Anbieter von Kinder- und Jugendforen zur Daten- und Kundensicherheit (Katzer 2014, S. 207 f.); dabei dürften allerdings die meisten ihrer Vorschläge wie jener einer Ausweispflicht für Forenteilnehmer zur Verringerung von Anonymität kaum

durchsetzbar sein, denn gerade jene Anonymität stellt für viele den besonderen Reiz dar und ist einer der Gründe, warum sich Menschen so bereitwillig öffnen. In der Anonymität bzw. der Gewissheit anonym zu agieren sehen Schiller et al. (2014, S. 54) auch einen der Gründe für einen positiven hohen Zusammenhang zwischen Spielern altersunangemessener und gewalthaltiger Spiele und Cyberbullying-Tätern. Die Medienwirkungsforschung bemüht sich schon lange um den Nachweis erhöhter Gewaltbereitschaft und -toleranz bei Nutzern von entsprechenden Bildschirmspielen. Schiller et al. sehen durch ihre Replikation einer früheren Studie von Lam et al. (2013) ihre Vermutung des Zusammenhanges von Spielgewalt und Online-Gewaltbereitschaft bestätigt und erklären ihn dadurch, dass der Transfer von aggressivem Verhalten im Spiel auf andere ICT-Bereiche übertragen wird. Weiterhin könnten sich Mediennutzer in Spielumgebungen ausprobieren – da dies dort folgenlos bleibe, würde der Wirkungsgrad von entsprechendem Verhalten gegenüber *realen* Personen, aber auch ICT-Plattformen, durch die Täter u. U. unterschätzt werden (Schiller et al. 2014, S. 54). Auch wenn die Autoren die Aussagekraft ihrer Replikationsstudie selber begrenzen, so zeigt der Kontext gleichwohl die Notwendigkeit, Phänomene von Cyberdevianz oder -kriminalität multiprofessionell zu bekämpfen.

6 Bewertung und Fazit

Mit kriminologischer Forschung kann sowohl der Opferwerdungsprozess nachvollziehbar gemacht wie auch eine Einordnung von Taten und Tätern vorgenommen werden, welche wiederum Einfluss auf die Präventions- und Ermittlungsarbeit nehmen. Auf Basis kriminologischer Untersuchungen stellt sich in der Kriminalistik zudem die Frage nach Ermittlungsmöglichkeiten von Tätern und der strafrechtlichen Einordnung von Taten – bereits Mathiesen hat auf die großen Herausforderungen bei der eindeutigen Zuordnung strafbarer Handlungen hingewiesen (Mathiesen 2014, S. 19 ff.); Katzer fragt dennoch nach einem Cybermobbinggesetz und wünscht, analog zum Beispiel der Schweiz (dort allerdings wieder abgeschafft), verdeckte Ermittlungen (Katzer 2014, S. 208). Die Rechtslage hat sich in den letzten Jahren allerdings entwickelt und so sind nicht mehr nur allgemein zugängliche Daten durch Ermittlungsbehörden nutzbar (§ 161 Abs. 1 StPO) und das Verschweigen der Beamtenrolle eines Ermittlers gilt als probat, sondern ggfls. auch die Anlage von „Fake Accounts“ oder, mit Zustimmung der Staatsanwaltschaft, die Erstellung einer „ausgefeilten Legende“ (§ 110b Abs. 1 StPO) (siehe hierzu auch Beck (o. J.) oder Kochheim 2012).

Problematisch für die kriminologische Beurteilung ist eine zuvor so nicht gekannte Herausforderung, die sich ergibt sich aus dem Lebensstilansatz, nach dem potenzielle Täter mit einer umso höheren Wahrscheinlichkeit auf potenzielle Opfer treffen, je mehr sich ihre Lebensstile gleichen:

> „Mit Lebensstil ist hier die charakteristische Art und Weise gemeint, wie ein Mensch im Tagesverlauf seine Zeit (…) aufteilt, an welchen Orten er sich zu welcher Zeit für welche Aktivitäten aufhält und welches Muster an Begegnungen und Interaktionen mit anderen Menschen daraus folgt. Die an bestimmte Orte und Zeiten gebundene Struktur der Aktivitäten einer Person hat Konsequenzen für die Wahrscheinlichkeit, in Opfersituationen hinein zu geraten. […] Das Erklärungsmodell basiert also auf der Überlegung, daß zahlreiche Delikte nur dann entstehen können, wenn Täter und Opfer räumlich zusammentreffen oder in eine Interaktion miteinander treten. […] Die Wahrscheinlichkeit nun, daß ein potentielles Opfer mit einem potentiellen Täter unter solchen situativen Umständen zusammentrifft, wird als umso höher eingeschätzt, je mehr sich die Lebensstile des Täters und des Opfers gleichen.“ (Schindler 1998, S. 268)

Lebensstile oder, um den älteren Begriff der „Lebensinseln“ von Baacke zu nutzen, lassen sich online aber mühelos wechseln bzw. fälschen, Milieuzugehörigkeiten vortäuschen, sodass (vermeintliche) Nähe auf vielfache Weise hergestellt werden kann und damit die Voraussetzung für Vertrauen. Hinsichtlich der Gefährdung Jugendlicher, zu *realweltlichen (!)* Opfern von Schlägereien zu werden, kommen Willems und van Santen (2014) zu der Überzeugung, dass bei Menschen mit Opfererfahrungen häufig weitere Problemlagen vorliegen, die eine Vulnerabilität erhöhen. Sie bilanzieren, dass Geschlecht, Religiosität, familiäre Stabilität und Zusammenhalt im Freundeskreis die Gefährdung verringern; Schulabsentismus, Alkohol- oder Drogenkonsum, ein schlechteres Familienklima und eine erhöhte Kontrollüberzeugung die Gefahren vergrößern (Willems und van Santen 2014, S. 104 f.) – was mithin für die Gültigkeit gewachsener und traditioneller Familien- und Persönlichkeitsbilder spricht, die heute oft als altmodisch oder sogar reaktionär gelten (auch Wachs, Wolf und Pan sehen in einem erhöhten Grad von persönlicher Zurückhaltung eine Bedingung für eine geringere Vulnerabilität; Wachs et al. 2012, S. 632).

Dieser Befund spricht für aktive Schul-, Gemeinde- und Sozialarbeit sowie nicht zuletzt für verstärkte Ansätze des *community policing,* also der gemeinschaftlich koordinierten Zusammenarbeit von Sozialarbeit und polizeilicher Kriminalitätsprävention. Diese können auch die Bystanderproblematik bearbeiten, die zumindest auf Fälle von virtuellen Halböffentlichkeiten zutrifft (siehe auch: Obermaier et al. 2015, S. 33). Vielfach werden Dritte einbezogen

oder sogar gezielt adressiert, bspw. bei der Weiterleitung diffamierender Bilder oder Texte. Ihr passives hinnehmendes oder aktiv widersprechendes (bzw. sogar bejahendes) Verhalten spielt im Weiteren eine wesentliche Rolle in der Fortführung oder Beendigung des Vorfalls. Ihre Rolle als „Bystander“ und damit Partei in einem sich zuspitzenden Konflikt ist vielen allerdings nicht bewusst.

Hinsichtlich *virtueller Gefährdungslagen* sind insbesondere in einem stärkeren Maße medienpädagogische Ansätze heranzuziehen bzw. Medienpädagogen in eine über den realweltlichen Rahmen hinausgreifende *virtual community policing* Programmatik einzubinden. Internetkriminalität zeichnet sich durch ein hohes Maß an Flexibilität und Anonymität aus. Intensivtäter finden durch ICT eine Vielzahl neuer Aktionsmöglichkeiten ebenso wie Täter oder Banden aus dem Ausland heraus wirken können und sich so einer möglichen inländischen Strafverfolgung in Deutschland gar nicht erst stellen müssen.

Alle Maßnahmen, um Kriminalität auch im virtuellen Raum zu bekämpfen, beginnen mit dem Verständnis für die Art der jeweiligen kriminellen Methode und dem hinsichtlich der Täter. Die Kriminologie muss die Themen aktuell und am Puls der Zeit aufgreifen, Medienpädagogische Lehrkonzepte wiederum sollten die Elemente der Kriminologie für Praktiker umsetzen. Die Taktiken im Cyberspace verändern sich sehr schnell, entsprechend wichtig ist eine praktisch orientierte und regelrecht tagesaktuelle Forschung. Denkbar sind systematische Fallaufarbeitungen komplexer Sachverhalte (z. B. Fälle von Love-Scamming durch Tätergruppen), die in Kategorien unterteilt und verglichen werden (z. B. Daten zu den Tätern, den Opfern, der Dauer des Scammings, Höhe des Betruges, Art der Kontaktaufnahme, Kommunikationsschema, etc.). Diese Informationen können – wie dies bereits die Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) praktisiert – als Information und Aufklärung zur Verfügung gestellt werden. Darüber hinaus könnte medienpädagogisch Handlungskonzepte beispielsweise für soziale Medien erstellt werden, bzw. als eingebaute Elemente im Schulunterricht, um die Schüler für den Umgang im Internet fachlich zu sensibilisieren. Der Aufwand ist vor allem angesichts der Notwendigkeit zur Aktualität natürlich hoch, doch die Schäden der Kriminalität sollten entsprechende Investitionen in die Prävention rechtfertigen.

Literatur

Artkämper, H., & Clages, H. (Hrsg.). (2015). *Kriminalitätsbekämpfung – Ein Blick in die Zukunft*. Stuttgart: Boorberg.

Baacke, D. (1984). *Die 6- bis 12-jährigen. Einführung in die Probleme des Kindesalters*. Weinheim: Beltz.

Baier, D., Kemme, S., Hanslmaier, M., Doering, B., Rehbein, F., & Pfeiffer, C. (2011). *Kriminalitätsfurcht, Strafbedürfnisse und wahrgenommene Kriminalitätsentwicklung. Ergebnisse von bevölkerungsrepräsentativen Befragungen aus den Jahren 2004, 2006 und 2010*. Hannover: KFN.

Beck, S. (o. J.). Verdeckte Ermittlungen in sozialen Netzwerken. https://www.pa.polizei-nds.de/download/72621. Zugegriffen: 26. Apr. 2019.

Ben-Ze'ev, A. (2004). *Love online. Emotions on the internet*. Cambridge: Cambridge University Press.

Bock, M. (2013). *Kriminologie* (4. Aufl.). München: Vahlen.

Bundeskriminalamt (Hrsg.). (2015). Täter im Bereich Cybercrime. Eine Literaturanalyse. Teil I – Eine phänomenologische und tätertypologische Betrachtung. Teil II – Kriminologische Erklärungen und Handlungsmöglichkeiten. https://cdn.netzpolitik.org/wp-upload/BKA-Studie_Taeter-im-Bereich-Cybercrime_Eine-Literaturanalyse.pdf. Zugegriffen: 1. Mai 2019.

Bundeskriminalamt Österreich (Hrsg.). (o. J.). Schutz vor Love-Scam. https://www.bundeskriminalamt.at/202/Betrug_verhindern/files/InformationsblattLoveScam.pdf. Zugegriffen: 1. Mai 2019.

Clages, H., & Zeitner, I. (2016). *Kriminologie. Für Studium und Praxis* (3. Aufl.). Hilden: VDP.

Ferrero de Sousa, D., de Deus Quirino Filho, J., de Cassia Pires Bezerra Cavalcanti, R., dos Santos, A. B., & Neto, M. L. R. (2017). The impact of the ‚Blue Whale' game in the rates of suicide: Short psychological analysis oft he phenomenon. *International Journal of Social Psychiatry, 63*(8), 796–797.

Festl, R., & Quandt, T. (2015). Cyberbullying at schools: A longitudinal research project. *Diskurs Kindheits- und Jugendforschung, 1,* 109–114.

Festl, Ruth. (2015). *Täter im Internet. Eine Analyse individueller und struktureller Erklärungsfaktoren von Cybermobbing im Schulkontext*. Wiesbaden: Springer VS.

Heirman, W., & Walrave, M. (2008). Assessing Concerns and Issues about the Mediation of Technology in Cyberbullying. Cyberpsychology. *Journal of Psychosocial Research on Cyberspace 2*(2). https://cyberpsychology.eu/article/view/4214/3256. Zugegriffen: 28. Apr. 2019.

Katzer, C. (2014). *Cybermobbing – Wenn das Internet zur W@ffe wird*. Berlin: Springer Spektrum.

Kochheim, D. (2012). Verdeckte Ermittlungen im Internet. Strafverfahrensrechtliche Voraussetzungen und Grenzen beim Einsatz von Überwachungstechnik und bei verdeckten Ermittlungen zur Bekämpfung der Cybercrime. Version 1.2, März 2012. http://www.cyberfahnder.de/doc/Kochheim-Internet-Ermittlungen.pdf. Zugegriffen: 28. Apr. 2019.

Lam, L. T., Cheng, Z., & Liu, X. (2013). Violent online games exposure and cyberbullying/victimization among adolescents. *Cyberpsychology, Behavior, and Social Networking, 16*(3), 159–165.

LKA NRW (Hrsg.). (2006). Individuelle und sozialräumliche Determinanten der Kriminalitätsfurcht. Sekundäranalyse der Allgemeinen Bürgerbefragungen der Polizei in Nordrhein-Westfalen. Kriminalistisch-Kriminologische Forschungsstelle Forschungsberichte Nr. 4/2006.

Mathiesen, A. (2014). *Cybermobbing und Cybergrooming. Neue Kriminalitätsphänomene im Zeitalter moderner Medien*. Publikationsreihe des Kriminalwissenschaftlichen Instituts der Leibniz Universität Hannover. Hannover: Eigenverlag.

Medienpädagogischer Forschungsverbund Südwest (mpfs). (2016). JIM 2016. Jugend, Information, (Multi-) Media. Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland. https://www.mpfs.de/fileadmin/files/Studien/JIM/2016/JIM_Studie_2016.pdf. Zugegriffen: 20. Juli 2019.

Obermaier, M., Fawzi, N., & Koch, T. (2015). Bystanderintervention bei Cybermobbing. Warum spezifische Merkmale computervermittelter Kommunikation prosoziales Eingreifen von Bystandern einerseits hemmen und andererseits fördern. *SCM Studies in Communication/Media 4*(1), 28–52.

Piasecki, S. (2018). *Credere et ludere. Computer- und Videospiele aus religionspädagogischer Perspektive*. Baden-Baden: Tectum.

Pientka, M. (2014). *Kriminalwissenschaften II*. Berlin: Beck.

Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK). (o. J.). Scamming. https://www.polizei-beratung.de/themen-und-tipps/betrug/scamming/#panel-17221-2. Zugegriffen: 1. Mai 2019.

Präventionsportal „Lilli“. https://www.lilli.ch/stalking_mobbing_bullying. Zugegriffen: 26. Apr. 2019.

Präventionsportal „Mobbing-out“. https://mobbing-out.blogspot.com/p/bullying.html. Zugegriffen: 26. Apr. 2019.

R&V Versicherung. (2016). Ergebnisse der Ängste-Studie 2016. https://www.ruv.de/presse/aengste-der-deutschen/presseinformation-aengste-der-deutschen-2016 vom 12.07.2016, 30.04.2019.

R&V Versicherung. (2017). Ergebnisse der Ängste-Studie 2017. https://www.ruv.de/presse/ruv-infocenter/pressemitteilungen/ruv-aengste-der-deutschen-2017-ergebnisse vom 07.09.2017, 30.04.2019.

rbb24. (2019). Massenschlägerei am Alexanderplatz nach Youtube-Aufruf. https://www.rbb24.de/panorama/beitrag/2019/03/massenschlaegerei-auf-alexanderplatz-nach-youtube-aufruf.html. Zugegriffen: 28. Apr. 2019.

Rüdiger, T.-G. (2012). Cybergrooming in virtuellen Welten – Chancen für Sexualtäter? *Deutsche Polizei, 2,* 29–35.

Schiller, E.-M., Gradinger, P., & Strohmeier, D. (2014). Nutzung gewalthaltiger Bildshirmspiele als längsschnittlicher Risikofaktor für Cyberbullying in der frühen Adoleszenz. *Diskurs Kindheits- und Jugendforschung, 1,* 39–59.

Schindler, V. (1998). Strukturen der Verwicklung in Delinquenz bei Jugendlichen und jungen Erwachsenen: Ergebnisse einer Auswertung des National Survey. In DVJJ (Hrsg.), *Kinder und Jugendliche als Opfer und Täter: Prävention und Reaktion: Dokumentation*

des 24. Deutschen Jugendgerichtstages vom 18. bis 22. September 1998 in Hamburg (S. 265–293). Mönchengladbach: Forum Verlag Godesberg.

Schwindt, H.-D. (2016). *Kriminologie und Kriminalpolitik. Eine praxisorientierte Einführung mit Beispielen* (23. Aufl.). Heidelberg: Kriminalistik Verlag.

Shakir, M., & Sharma, S. (2018). Adolescents under stress: The blue whale game challenge. *Research Review International Journal of Multidisciplinary, 03*(7), 379–386.

Singh, B., Bhargava, R., Pakhre, A., Bhati, N. (2018). The „Blue Whale Challenge"?: The first report on a consultation from a health care setting for carrying out „tasks" accessed through a mobile phone application. *Asia-Pacific Psychiatry.* https://doi.org/10.1111/appy.12317. Zugegriffen: 25. Apr. 2019.

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Neil, Tippet. (2008). Cyberbullying – Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry, 49*(4), 376–385.

Statista.(2018). Statista Dossier „Cybermobbing". https://de.statista.com/statistik/studie/id/24611/dokument/cybermobbing-statista-dossier/. Zugegriffen: 26. Apr. 2019.

Suhr, F., & Statista (2017). Was Senioren im Internet treiben. https://de.statista.com/infografik/9002/alte-menschen-im-internet. Zugegriffen: 28. Apr. 2019.

Wachs, S., & Wolf, K. D. (2011). Zusammenhänge zwischen Cyberbullying und Bullying – Erste Ergebnisse aus einer Selbstberichtsstudie. *Praxis der Kinderpsychologie und Kinderpsychiatrie 60*(9), 735–744.

Wachs, S., Wolf, K. D., & Ching-Ching, P. (2012). Cybergrooming: Risk factors, coping strategies and associations with cyberbullying. *Psicothema, 24*(4), 628–633.

Whitty, M. T., & Buchanan, T. (2012). the online dating romance scam: A serious crime. *CyberPsychology, Behavior, and Social Networking, 15*(3), 181–183.

Willems, D., & Santen, E. van. (2014). Verletzliche Jugend – Jugendliche als Opfer von Schlägereien: Empirische Ergebnisse des DJI-Surveys „Aufwachsen in Deutschland: Alltagswelten". *Diskurs Kindheits- und Jugendforschung, 1,* 93–108.

Zeiher, H. (1983). Die vielen Räume der Kinder. Zum Wandel räumlicher Lebensbedingungen seit 1945. In U. Preuss- Lausitz, P. Büchner (Hrsg.), *Kriegskinder. Konsumkinder. Krisenkinder. Zur Sozialisationsgeschichte seit dem Zweiten Weltkrieg* (S. 176–195). Weinheim: Beltz.

Strafbedürfnis und Kriminalitätsfurcht im Cyberspace

Stefanie Kemme und Maximilian Querbach

1 Einleitung

Individuelle Strafbedürfnisse sind von erheblicher Bedeutung, da sie zu weitreichenden gesellschaftlichen Veränderungen führen können. So muss sich die Politik verstärkt mit bestimmten Straftaten bzw. mit ihrer Verhütung auseinandersetzen, wenn sie im öffentlichen Diskurs besondere Aufmerksamkeit erlangen. Einschätzungen und Meinungen in der Bevölkerung werden dann nicht selten als Rechtfertigung für Gesetzesverschärfungen herangezogen. (vgl. Kemme und Doering 2015). Zu nennen ist hier beispielhaft das Sexualstrafrecht, das aufgeheizt durch eine Reihe von Ereignissen wie bspw. in der Kölner Silvesternacht 2015/2016 von der Bevölkerung und in den Medien als zu „lasch" dargestellt wurde, sodass Verschärfungen als notwendig angesehen wurden (vgl. dazu Kreuzer 2018).

Obwohl zahlreiche Erkenntnisse zum Strafbedürfnis in der Forschung existieren, wurde bisher nicht untersucht, inwiefern sich Strafbedürfnisse in Hinblick auf die klassischen Delikte in der realen Welt wie bspw. sexuelle Nötigung, Raub oder Ladendiebstahl von solchen im Cyberspace wie bspw. Cyberstalking, Passwort-Hacking oder illegale Downloads unterscheiden. Seit Beginn der 2000er und der Weiterentwicklung des virtuellen Raumes und dessen Bedeutung für kommerzielle Zwecke, aber auch für die Bildung eines sozialen Interaktionsraumes,

S. Kemme (✉)
Hamburg, Deutschland
E-Mail: stefanie.kemme@polizei-studium.org

M. Querbach
Landeskriminalamt Niedersachsen, Hannover, Deutschland
E-Mail: maximilian.querbach@polizei.niedersachsen.de

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

T.-G. Rüdiger und P. S. Bayerl (Hrsg.), *Cyberkriminologie,*
https://doi.org/10.1007/978-3-658-28507-4_21

sind die Bedrohungspotenziale, Opfer einer Straftat im Internet zu werden, stetig gewachsen. Daher ist von Interesse, ob sich die Bevölkerung durch Straftaten im Cyberspace auch tatsächlich bedroht fühlt. Zuverlässiger Prädiktor des Strafbedürfnisses ist die Kriminalitätsfurcht. Doch auch diese kann in der realen Welt anderen Einflussfaktoren ausgesetzt sein als in der virtuellen Welt. Bevor nachfolgend auf die spezifischen Erkenntnisse zu Strafbedürfnis und Kriminalitätsfurcht im Cyberspace eingegangen wird, werden zunächst die Ergebnisse bisheriger Studien in Bezug auf klassische Delikte dargestellt. Abschließend werden Daten einer Hamburger Studie vorgestellt, die erstmals Strafbedürfnisse im Cyberspace untersucht hat.

2 Punitivität und Kriminalitätsfurcht

Punitivität ist ein vielschichtiges Konzept. So kann sowohl die Höhe der Gefangenenraten, die nationale Gesetzgebung, die mediale Berichterstattung aber auch das individuelle Strafbedürfnis gemeint sein (Baier et al. 2011; Kury et al. 2004; Simonson 2009). Es sind daher verschiedene Ebenen zu unterscheiden. Auf der Makroebene lässt sich Punitivität innerhalb des öffentlichen gesellschaftlichen, politischen und medialen Diskurses identifizieren (vgl. Baier et al. 2011, S. 43; Kury et al. 2004, S. 52). Zur Makrobene zählt auch die justizielle Punitivität, die die Strafhärte der sanktionierenden oder gesetzgebenden Institutionen im Blick hat. Die Mikroebene meint dagegen die Einstellungen zu Strafen, also das individuelle Strafbedürfnis der einzelnen Personen (vgl. Kury und Obergfell-Fuchs 2006, S. 125). Begreift man Einstellungen als die „individuelle Stellungnahme auf allgemeine soziale Inhalte“ bzw. als Bewertungsdisposition, so stellt Punitivität auf der Individualebene eine Strafeinstellung dar, welche die Tendenz kennzeichnet, im Falle von Normverstößen schärfere und vergeltende Sanktionen den milderen vorzuziehen (Lautmann und Klimke 2004, S. 9).

Die Abhängigkeit des Strafbedürfnisses von Geschlecht, Alter, Bildung, sozioökonomischem Status und Wohnort war zunächst zentraler Gegenstand erster Erklärungsansätze (vgl. Baier et al. 2011, S. 73 ff. m. w. N.). Männer tendieren oftmals zu härteren Strafen (u. a. Borg 1997; Kühnrich und Kania 2005), der sozioökonomische Status bzw. ein hoher Bildungsstatus weist einen strafmildernden Effekt auf (u. a. Borg 1997; Hartnagel und Templeton 2008) und älteren Menschen kann teilweise ein höheres Strafbedürfnis nachgewiesen werden (Baier et al. 2011, S. 79). Trotzdem kann das Strafbedürfnis nur in einem geringen Maße durch soziodemografische Faktoren erklärt werden (vgl. King und Maruna 2009; Kury et al. 2002; Van Kersteren 2009). Schon früh musste

entgegen aller Erwartungen zur Kenntnis genommen werden, dass eine direkte Beziehung zwischen Viktimisierung und Punitivität nicht zu belegen ist (bspw. Taylor et al. 1979). Eine Reihe von Untersuchungen zeigte keine oder nur geringe Zusammenhänge zwischen Opferstatus und Punitivität (u. a. Applegate et al. 2000; Cullen et al. 1985; Hartnagel und Templeton 2008; Langworthy und Whitehead 1986; Mascini und Houtman 2006; Reuband 2010). Zum Teil ließen sich sogar gegenläufige Beziehungen belegen (Van Kesteren 2009). Der stellvertretenden Viktimisierung konnte ebenfalls lediglich ein geringfügiger Effekt nachgewiesen werden (vgl. Schwarzenegger 1992; Tyler und Weber 1982). Hingegen erwies sich, dass die kindliche Sozialisation in einem besonders rigiden und gewaltgeprägten familiären Umfeld die späteren Strafeinstellungen prägt (Kemme und Hanslmaier 2010; Kemme et al. 2014). Daneben haben auch fundamentalistische religiöse Einstellungen sowie politisch konservative Einstellungen einen starken Einfluss auf das individuelle Strafbedürfnis (vgl. Applegate et al. 2000; Britt 1998; Cook und Powell 2003; Johnson 2009; Mascini und Houtman 2006; Tyler und Boeckman 1997). Ebenso zeigte sich beim Konsum kriminalitätsbezogener Medienberichterstattung eine erhöhte Strafeinstellung der Rezipienten (vgl. Dowler 2003; Kleck und Jackson 2017; Pfeiffer et al. 2005), insbesondere beim vermehrten Konsum von Boulevardzeitungen (vgl. Baier et al. 2011, S. 152; Hanslmaier und Kemme 2011; Kemme und Hanslmaier 2012, S. 12).

Darüber hinaus wurden Einflüsse kriminalitätsbezogener Furcht auf die individuelle Strafeinstellung weitreichend untersucht (bspw. Hirtenlehner 2010). Es wird auf individueller Ebene zwischen kognitiver, affektiver und konativer Kriminalitätsfurcht unterschieden (vgl. Bilsky et al. 1992; Boers 1991; Skogan 1993; Wetzels et al. 2001). *Kognitive Kriminalitätsfurcht* beschreibt die persönliche Einschätzung der Wahrscheinlichkeit, selbst Opfer von Straftaten zu werden. Die *affektive* Komponente bezieht sich auf die individuelle Sorge bzw. Befürchtung des Opferwerdens bzw. die Häufigkeit und Intensität dieser Befürchtungen. Beide Komponenten können unter das Konstrukt der personalen Kriminalitätsfurcht subsumiert werden. Hinzu kommt die *konative bzw. behaviorale* Komponente, womit verschiedene Verhaltensweisen gemeint sind, mit denen das Individuum glaubt, mögliche Opferwerdung vermeiden zu können (vgl. Baier et al. 2011). Wie das Strafbedürfnis wird auch die Kriminalitätsfurcht von verschiedenen soziodemografischen Variablen beeinflusst. Frauen, ältere Personen und Personen mit geringem Bildungsstand weisen eine höhere konative und personale Kriminalitätsfurcht auf (Baier et al. 2011, S. 74; Hale 1996). Auch die Mediennutzung hat sich als Einflussfaktor der Kriminalitätsfurcht erwiesen (bspw. Eschholz 1997). Eine Reihe von Studien berichte zudem einen Zusammenhang zwischen Viktimisierung und erhöhter Kriminalitätsfurcht (bspw. Dreißigacker 2017; Tseloni und Zarafonitou

2008). Allerdings haben Viktimisierungserfahrungen einen geringeren Einfluss auf Kriminalitätsfurcht als zunächst angenommen (Kury und Würger 1993; Kury et al. 2000).

In verschiedenen Analysen wird der Kriminalitätsfurcht eine zentrale Rolle bei der Erklärung punitiver Einstellungen zugesprochen (vgl. Applegate 1997; Baier et al. 2011; Kühnrich und Kania 2005). Hinsichtlich des Zusammenhangs zwischen personaler Kriminalitätsfurcht und Strafbedürfnis liegen dennoch inkonsistente Ergebnisse vor. So konnte zum Teil bestätigt werden, dass eine hohe personale Kriminalitätsfurcht mit der Forderung nach härteren Strafen einhergeht (vgl. Baier et al. 2011; Pfeiffer et al. 2005; Windzio et al. 2007), wohingegen teilweise auch keine Zusammenhänge gefunden wurden (vgl. Armborst 2017; Costelloe et al. 2009; Dowler 2003; Wynterdyk und Hincks 2013).

Die gefundenen Korrelationen zwischen Viktimisierung und Kriminalitätsfurcht einerseits und die Auswirkungen der Kriminalitätsfurcht auf Punitivität andererseits (bspw. Applegate 1997) führten zu der weiteren Annahme eines über die Kriminalitätsfurcht vermittelten Einflusses der Viktimisierung auf die Punitivität. Die Annahme einer indirekten Wirkung der Opferwerdung auf das Strafverlangen über die Erhöhung der Kriminalitätsfurcht bestätigte sich nicht durchgängig. Zum Teil wurden leicht positive, zum Teil keine Zusammenhänge entdeckt (Kury und Ferdinand 1999; Kleck und Jackson 2017). Andere Autoren (vgl. Langworthy und Whitehead 1986) fanden sowohl für die direkte als auch für die indirekte Viktimisierung über die Erhöhung der Kriminalitätsfurcht Effekte auf die Punitivität.

Auf der Ebene der *sozialen Kriminalitätsfurcht,* welche die Sorge um allgemeine Entwicklungen der inneren Sicherheit oder bezüglich vermeintlich steigender Kriminalität beschreibt (vgl. Bornewasser 2012, S. 1), konnten punitivitätssteigernde Einflüsse durch eine erhöhte Kriminalitätswahrnehmung auf sozialer Ebene nachgewiesen werden (vgl. Baier et al. 2011, S. 68; Costelloe et al. 2009; Pfeiffer et al. 2005).

Ein weiterer aktueller Erklärungsansatz beschreibt Kriminalitätsfurcht und Punitivität als Resultat des Wandels sozialer Strukturen und den damit verbundenen tradierten und vertrauten Lebensformen (vgl. Hirtenlehner 2011, S. 27). In diesem Fall manifestiert sich ein Teil einer diffusen Angst in einem höheren Strafbedürfnis von Individuen. Innerhalb der Forschungslandschaft haben bereits mehrere Studien den Einfluss einer allgemeinen Verunsicherung im Kontext der Entstehung von Kriminalitätsfurcht und Punitivität untersucht und bestätigt (vgl. Dowler 2003; Ewald 2000; Garland 2001; Hirtenlehner 2009; Hirtenlehner und Farrall 2013; Hummelsheim-Doss et al. 2011).

3 Punitivität und Kriminalitätsfurcht im Cyberspace

Alle dargelegten Zusammenhänge im Bereich von Strafbedürfnissen und Kriminalitätsfurcht beziehen sich auf Delikte in der realen Welt. Das Cyberspace hat in dieser Hinsicht in der Forschung bisher kaum Aufmerksamkeit erlangt. Fraglich ist jedoch, ob sich gefundene Erklärungsansätze auch auf den Cyberspace übertragen lassen. Nachfolgend werden zunächst einige Entwicklungen auf der Makroebene der Punitivität erläutert, um im Anschluss die Erkenntnisse auf der individuellen Ebene zu skizzieren.

3.1 Die Makroebene der Punitivität im Cyberspace – Gesetzesanpassungen und -verschärfungen

Die neuen Möglichkeiten der sozialen Vernetzung im digitalen Raum, aber auch die dadurch neu entstandenen Gefahren im Cyberspace Opfer kriminelller Handlungen zu werden, mussten durch die Gesetzgebung zeitnah adressiert werden. Erste gesetzliche Veränderungen wurden bereits Ende der 1980er Jahre vorgenommen. Jedoch galten diese, etwaigen Gesetzeslücken in der Datenverarbeitung im Kontext von Wirtschaftskriminalität zu begegnen, und weniger unserem heutigen Verständnis von Cybercrime entgegenzuwirken (vgl. Eisele 2016, S. 255). Der Grundstein für heutige cyberspezifische Strafrechtsanpassungen und die Strafverfolgung wurde zunächst auf europäischer Ebene im Jahr 2001 gelegt. In der Vereinbarung, die 30 Länder unterzeichneten, wurde die Notwendigkeit einer internationalen polizeilichen Zusammenarbeit mit der *Convention on Cybercrime* vereinbart (vgl. Council of Europe 2001). Aber auch der Rahmenbeschluss der Europäischen Union über Angriffe auf Informationssysteme bildete einen weiteren Baustein für die Schaffung einer übergreifenden nahen Zusammenarbeit der involvierten Strafverfolgungsbehörden (Amtsblatt der Europäischen Union 2005). Um die justizielle Zusammenarbeit bei grenzübergreifenden Delikten zu erleichtern, wurde 2016 das European Judicial Cybercrime Network (EJCN) ins Leben gerufen. Ziel der Gründung des EJCN war es, eine Plattform des internationalen Austausches zu schaffen, bei der sich Praktiker und Experten der Strafverfolgung und Justiz sowie weitere Sicherheitsakteure hinsichtlich der Strafverfolgung von Cybercrime austauschen und beraten können. Die europäische Justizbehörde EUROJUST fungiert als zentraler Koordinationspartner des

informationellen Austauschs, organisiert die jeweiligen Treffen des Netzwerkes und berät die jeweiligen Partner zur Thematik.[1]

Seit Anfang der 2000er wurden auf nationaler Ebene die rechtlichen Anforderungen an die Strafverfolgung des Cybercrime weiter angepasst. Es wurde beispielsweise die Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen geregelt (§ 201a StGB). Darüber hinaus ist mit der Anpassung des Strafrechts zur Bekämpfung der Computerkriminalität im Jahr 2007 (vgl. BGBl. I, S. 1786 41. StrÄndG vom 7. August 2007) das Abfangen und Ausspähen von Daten sowie die Vorbereitung dieser Taten neu geregelt worden (§§ 202a – c StGB). Mit dem 49. StrÄndG (vom 21. Januar 2015 BGBl. I S. 10) wurden Delikte strafrechtlich angepasst, die zuvor nur außerhalb des Internets in Erscheinung traten und nun durch die Möglichkeiten des Cyberspace eine neue Dimension bekamen. Dazu zählen beispielsweise das Zugänglichmachen und das Abrufen von kinder- und jugendpornografischen Inhalten (§ 184d StGB) oder das Verleiten eines Kindes zu sexuellen Handlungen mittels Kommunikationstechnologie (§ 176 Abs. 4 Nr. 3 StGB), die Verbreitung rassistischer oder gewaltverherrlichender Inhalte (§§ 130, 131 StGB) sowie die Verbreitung und Verwendung verfassungswidriger Symbole (§§ 86, 86a StGB) in Online-Medien oder der Aufruf zu und die Anleitung von Straftaten (§§ 111, 130a StGB) in sozialen Netzwerken oder Foren. Zusätzlich wurden die Befugnisse der polizeilichen Strafverfolgung angepasst. So gehören Fahndungsmaßnahmen in Online-Foren oder sozialen Netzwerken sowie Online-Durchsuchungen und die Beschlagnahme von digitalen Datenträgern, der Zugriff auf private E-Mails und die Aufzeichnung oder Entschlüsselung privater Kommunikationsdaten zum adaptierten Maßnahmenkatalog der Strafverfolgungsbehörden zur Bekämpfung internetbasierter Kriminalität (vgl. Eisele 2013, S. 229 f.), gleichwohl eine Anpassung der gefahrenabwehrrechtlichen Grundlagen in diesem Bereich nicht in gleichem Maße stattgefunden hat (Krischok 2018). Daneben wurden entsprechende Ausbildungs- und Weiterbildungsmaßnahmen der Polizisten im IT-Bereich sowie Einstellungen von Fachpersonal teilweise vorgenommen (vgl. Herbst 2017; Honekamp 2019, S. 55 ff.).

2011 kam es zur Verabschiedung der Cyber-Sicherheitsstrategie der Bundesregierung. Anlass war die als immer stärker anwachsend wahrgenommene Gefährdungslage von Angriffen auf sensible IT-Strukturen, die Staat, Wirtschaft und Gesellschaft maßgeblich schädigen könnten. Zu den Kernpunkten der Strategie zählen die Schaffung eines sicheren Cyber-Raums durch Stärkung und

[1]EUROJUST – The European Union's Judicial Cooperation Unit unter http://www.eurojust.europa.eu/Practitioners/Pages/EJCN.aspx (zuletzt abgerufen am 24.05.2019).

Verbesserung der IT-Sicherheitssysteme in Form von Beratungsangeboten oder der kostenfreien Verfügbarkeit von Sicherheitsprodukten für private Personen, Wirtschaft und die Öffentliche Verwaltung, der Schutz kritischer Infrastrukturen und der Einsatz neuer gesicherter Informationstechnologien. Zusätzlich wurde 2011 auf Basis dieser Sicherheitsstrategie das Nationale Cyber-Abwehrzentrum (NCAZ) gegründet, angesiedelt beim Bundesamt für Sicherheit und Informationstechnik (BSI) in Zusammenarbeit mit dem Bundesamt für Verfassungsschutz (BfV) sowie dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK). Durch die Gründung des Abwehrzentrums soll ein schneller und enger Informationsaustausch im Falle einer Gefährdungslage zwischen den zuständigen Behörden (Bundeskriminalamt, Bundespolizei, Bundesnachrichtendienst, Bundeswehr, Zollkriminalamt) und wirtschaftlichen Vertretern ermöglicht werden. Das NCAZ soll dabei die Federführung in der Analyse haben und Handlungsempfehlungen für die beteiligten Partner bereitstellen (Bundesministerium des Innern 2011). Darüber hinaus wurde 2011 der Nationale Cyber-Sicherheitsrat gegründet, zu dessen Hauptaufgaben die Koordination der Politik für Cybersicherheit zwischen Staat und Wirtschaft zählt. Der Rat besteht aus Vertretern der Politik und Wirtschaft (z. B. Bundeskanzleramt, Digitalverband BITKOM, Deutscher Industrie- und Handelskammerverband) (Bundesministerium der Verteidigung o. D.).

3.2 Die Mikroebene – das individuelle Strafbedürfnis und Kriminalitätsfurcht im Cyberspace

Zwar lässt sich bisher keine Studie finden, die sich mit den individuellen Strafeinstellungen im Cyberspace beschäftigt, jedoch wurden in den letzten Jahren vermehrt Studien publiziert, die Opferwerdung im Cyberspace und Furcht vor computerbezogener Kriminalität untersuchten (bspw. Karuppannan 2012; Vozmediano et al. 2013). Die im Folgenden dargestellten Studien stellen einen zentrierten Kern der für die Untersuchung relevanten Forschungserkenntnisse und Ergebnisse dar.

Eine erste größer angelegte Untersuchung führte Alshalan (2006) durch. Die Studie analysierte die individuellen Einflussfaktoren der Furcht vor Cybercrime. Die Grundlage der Studie bildete dabei eine Stichprobe von 987 Personen, die im Rahmen des *National Cybercrime Victimization Survey* der Universität von Mississippi, USA, untersucht wurden. Die Ergebnisse wiesen darauf hin, dass ältere Menschen mehr Furcht als jüngere Menschen davor hatten, Opfer einer Straftat im Internet zu werden, obwohl sie sich weniger im Internet aufhielten. Zudem wiesen Frauen eine generell höhere Furcht vor Cybercrime auf

als Männer, was durch eine bereits erfahrene Viktimisierung nochmals verstärkt wurde. Hingegen konnten keine Effekte bezüglich der ethnischen Zugehörigkeit oder stellvertretender Viktimisierungserfahrungen auf die Furcht vor Cybercrime gefunden werden. Überdies untersuchten Henson et al. (2013) anhand einer Stichprobe von 838 amerikanischen Studenten die Zusammenhänge zwischen der Risikoeinschätzung, Opfer von Beleidigung, Stalking oder Bedrohung im Internet durch Partner, Freund oder Fremde zu werden, der erlebten Viktimisierung dieser Delikte und wiederum der Angst vor interpersonaler Online-Viktimisierung (OIPV) durch Partner, Freunde oder Fremde. Die Ergebnisse deuteten darauf hin, dass das wahrgenommene Risiko der Opferwerdung einen signifikanten Einfluss auf die Angst vor der Opferwerdung für alle Täter-Opfer-Beziehungen hatte. Zudem zeigte sich zwar ein positiver Zusammenhang von bereits erlebter Viktimisierung und der Furcht vor interpersonaler Viktimisierung im Internet, jedoch nur für die Täterkategorien „Partner“ und „Bekannte“. Darüber hinaus wurde kein Einfluss der Online-Aktivität der Probanden und der Opferwerdung durch Partner, Freund oder Fremde im Internet festgestellt.

Weitere Einflussfaktoren der Viktimisierung untersuchten Lenhart et al. (2016) mit einer Stichprobe von 3002 Amerikanern. Fast drei Viertel der Befragten Internetnutzer wurden bereits Opfer von Online-Belästigungen. Die am stärksten betroffene Gruppe waren Personen unter 30 Jahren und solche, die sich als homosexuell oder bisexuell identifizierten sowie Menschen mit dunklerer Hautfarbe. Mehr als ein Viertel der Befragten zeigte eine erhöhte konative Kriminalitätsfurcht, indem sie weniger Inhalte in Online-Foren veröffentlichten. Personen, die bereits Opfer von Beleidigung im Internet wurden, tendierten eher dazu, weniger aktiv im Netz zu sein. Unter den Personen, die Online-Beleidigung erlebt hatten, war die Wahrscheinlichkeit, dass die Erfahrung Angst hervorbrachte oder Besorgnis erregte, bei Frauen dreimal höher als bei Männern, wohingegen Männer vermehrt dazu tendierten, die Erfahrungen als nicht störend anzusehen. Die DIVSI-U25-Studie in Deutschland zeigt, dass ca. zwei Drittel der Jugendlichen eine Beleidigungskultur im Internet wahrnehmen und ca. ein Drittel der Jugendlichen deswegen auf eigene Posts verzichten (DIVSI 2018, S. 13).

Yu (2014) analysierte, inwiefern der wahrgenommene Schweregrad von Cybercrime das Risiko der Opferwerdung und die erfahrene Viktimisierung die Furcht vor Cybercrime beeinflussen. Eine Stichprobe von 270 Studenten bildete die Basis der Untersuchung, in der sich herausstellte, dass die jeweiligen Prädiktoren je nach Deliktart variierten und kein einziger Prädiktor die Angst vor allen untersuchten Deliktarten vorhersagen konnte. So war die Furcht vor Online-Scams durch eine erhöhte Risikowahrnehmung, ein verstärktes Online-Kaufverhalten und eine erhöhte Wahrnehmung der Schwere des Deliktes bedingt, wohingegen die Angst

vor Cyber-Bullying durch eine erhöhte soziale Interaktion im Online-Bereich, Viktimisierungserfahrungen und das Geschlecht – Frauen wiesen eine erhöhte Furcht auf – erklärt werden konnte. Die Risikowahrscheinlichkeit hatte keinen Einfluss auf die Furcht vor Digitaler Piraterie und Computerviren, verstärkte aber die Furcht vor Online-Scams und Cyber-Bullying. Dahingegen wies der gefühlte Schweregrad des Deliktes nur für die Furcht vor Online-Scams und Computerviren einen positiven Effekt auf. Die Viktimisierungserfahrung konnte nur als Prädiktor für die Angst vor Computerviren und Cyber-Bullying bestätigt werden.

Mit dem Einfluss der Selbstkontrolle der Nutzer sozialer Netzwerke auf Online-Kriminalitätsfurcht befasste sich eine Studie von Higgins et al. (2008). Die Basis der Studie bildeten 224 Studenten der Southeastern University in Florida, USA, die einen Facebook-Account besaßen. Anhand einer Pfadanalyse zeigte sich, dass Selbstkontrolle keinen direkten Effekt auf die Angst vor Online-Viktimisierung hatte. Die Risikoeinschätzung, Opfer zu werden, wies jedoch einen direkten positiven Effekt auf die Angst vor Online-Viktimisierung aus. Darüber hinaus war der Effekt der Selbstkontrolle auf die individuelle Furcht voll durch die individuelle Risikoeinschätzung mediiert. Mit einer erhöhten Selbstkontrolle gingen somit eine erhöhte Risikoeinschätzung und damit eine erhöhte Furcht vor Online-Viktimisierung einher.

Anhand einer Stichprobe von 573 Befragten Internetnutzern des Staates Florida untersuchten Reisig et al. (2009) den Einfluss der Vulnerabilität und der Selbstkontrolle auf die individuelle Risikoeinschätzung, Opfer eines Kreditkartenbetrugs im Internet zu werden. Es stellte sich heraus, dass vulnerablere Gruppen, definiert durch einen niedrigen sozioökonomischen Status oder die Zugehörigkeit zu einer ethnischen Minderheit, eine erhöhte Risikoeinschätzung zeigten. Ähnliche Ergebnisse zeigten sich auch für finanziell impulsivere Menschen, die in die Kategorie der geringeren Selbstkontrolle fielen. Eine erhöhte Risikoeinschätzung führte zu einer verminderten Nutzungszeit des Internets und einem verringerten Kaufverhalten. Jedoch investierten finanziell impulsivere Befragte trotz erhöhter Risikoeinschätzung immer noch mehr Zeit und Geld online als Personen mit einer erhöhten Selbstkontrolle.

Eine Studie mit 18.133 befragten Internetnutzern des Eurobarometers von 2012 von Böhme und Moore (2012) untersuchte wiederum den Einfluss der Online-Viktimisierung, der Befürchtung der Opferwerdung und der medialen Berichterstattung zu Cybercrime auf das Einkaufsverhalten, das Onlinebanking und die Online-Partizipation in sozialen Netzwerken und Foren. Individuelle Viktimisierungserfahrungen hatten demnach nur einen geringfügigen negativen Effekt auf die Onlineaktivitäten. Personen, denen durch die Medienberichterstattung die Risiken im Internet bekannt waren, tendierten eher seltener dazu,

Onlinebanking zu nutzen, als Personen, die medial weniger oder gar nicht mit der Thematik in Berührung kamen.

Die Datengrundlage der Untersuchung von Virtanen (2017) bildete der Eurobarometer von 2013 mit 18.711 Befragten. Hier ergab sich, dass Personen mit Viktimisierungserfahrungen im Netz, Frauen und Personen mit einem geringeren sozialen Status sowie solche mit einer geringen Internetnutzungskompetenz ein höheres Maß an Angst vor der Opferwerdung aufwiesen. Es wurde darüber hinaus festgestellt, dass ein niedriger sozialer Status und ein geringes Vertrauen in die eigenen Online-Kompetenzen einen signifikanten Interaktionseffekt mit früheren Viktimisierungserfahrungen in Bezug auf die Angst vor Cyberkriminalität hatten. Frühere Viktimisierungserfahrungen mit Online-Betrug schienen die Angst vor Cyberkriminalität bei Personen mit niedrigem Sozialstatus stärker zu erhöhen als bei anderen Gruppen. Erfahrungen mit gehackten Online-Accounts oder Cyberangriffen verstärkten auch die Angst derjenigen mit geringem Vertrauen in ihre Online-Kompetenzen mehr als derjenigen mit einem höheren Maß an Vertrauen. Die Ergebnisse dieser Studie konnten zeigen, dass soziale und physische Vulnerabilität sowie Viktimisierungserfahrungen direkte und indirekte Auswirkungen auf die Angst vor Cyberkriminalität haben und somit ähnliche Effekte aufwiesen, wie sie bei traditionellen ortsbezogenen Delikten und klassischer Kriminalitätsfurcht gefunden wurden.

Eine aktuelle Auswertung der Dunkelfeldstudien der Jahre 2015 und 2017 des Landeskriminalamtes Schleswig-Holstein (Dreißigacker und Riesner 2018) zeigte, dass sich über die Hälfte der befragten privaten Internetnutzer unsicher im Internet fühlen. Jüngere Frauen fühlten sich unsicherer als jüngere Männer und ältere Menschen hatten eine allgemein geringere Furcht im Internet als jüngere Menschen. Daneben wurde deutlich, dass vor allem die Art der Internetnutzung einen maßgeblichen Einfluss auf das individuelle Sicherheitsgefühl hatte. Des Weiteren wurden die drei Ebenen der computerbezogenen Kriminalitätsfurcht erhoben. Auf der affektiven Ebene konnte eine erhöhte Risikoeinschätzung für Frauen sowie jüngere Menschen, auf der kognitiven Ebene nur für Frauen nachgewiesen werden. Ebenso konnte ein positiver Effekt der Opfererfahrung auf die kognitive Kriminalitätsfurcht nachgewiesen werde. Männer wiesen ein höheres Schutzverhalten als Frauen auf, wohingegen bei Frauen ein erhöhtes Vermeidungsverhalten festgestellt werden. Bei älteren Menschen waren sowohl das Schutz- als auch das Vermeidungsverhalten geringer ausgeprägt als bei jüngeren. In Anbetracht bereits erlebter Viktimisierung konnte bei Personen mit einer hohen konativen Kriminalitätsfurcht kein Unterschied zu Nicht-Opfern beobachtet werden.

Neben den Viktimisierungserfahrungen, der Vulnerabilität und der Internetnutzung wurde versucht, die klassische Kriminalitätsfurcht als Prädiktor der Kriminalitätsfurcht vor Cybercrime zu untersuchen. Roberts et al. (2013) nutzten dafür die Daten von 1550 erwachsenen Australiern des AuSSA *(Australian Survey of Social Attitudes)* von 2007. Darin sollte der Einfluss der sozialen Einstellungen und des Verhaltens der Befragten auf die Furcht, Opfer von Identitätsdiebstahl im Internet zu werden, untersucht werden. Für Personen mit einem erhöhten Einkommen und somit einem erhöhten Schadenspotenzial konnte kein Zusammenhang zur Angst vor Online-Identitätsdiebstahl festgestellt werden. Jedoch hatten Befragte mit einer erhöhten affektiven Furcht vor der klassischen Opferwerdung auch eine höhere Furcht vor Online-Identitätsdiebstahl; die klassische Kriminalitätsfurcht stellte sich als stärkster Prädiktor heraus. Daneben konnte auch nachgewiesen werden, dass eine erhöhte Internetaktivität mit einer erhöhten Furcht der Opferwerdung einhergeht.

Eine der aktuellsten Studien zur Thematik stammt von Brunton-Smith (2018) mit einer Stichprobe von 6685 Befragten des *Crime Survey for England and Wales* von 2014/2015. Brunton-Smith untersuchte sowohl klassische soziodemografische Faktoren, Viktimisierungserfahrungen online und offline, als auch den Einfluss der klassischen Kriminalitätsfurcht auf die Ausprägung der Online-Kriminalitätsfurcht. Die Ergebnisse verdeutlichten, dass Personen mit einer erhöhten Furcht vor klassischen Kriminalitätsdelikten auch eine erhöhte Furcht vor Cybercrime aufwiesen. Des Weiteren ließ sich wiederum bestätigen, dass Frauen, ältere Menschen, ethnische Minderheiten und Personen mit einem höheren Bildungsabschluss stärker besorgt waren, Opfer von Cybercrime zu werden. Unter den Personen, die bereits Opfer einer Straftat im Internet waren, stellten eine hohe Internetnutzung, ein finanzieller Schaden, der unautorisierte Zugang zu persönlichen Daten durch Fremde und die Beleidigung den stärksten Einfluss auf die Online-Kriminalitätsfurcht dar. Auch das allgemeine Sicherheitsgefühl nachts in der eigenen Wohngegend hatte einen maßgeblichen Einfluss auf die individuelle Online-Kriminalitätsfurcht, was Brunton-Smith (2018) letztendlich als Anzeichen einer generellen Kriminalitätsfurcht, welche nicht online von offline unterscheidet, ansah.

Im Anschluss an die beschriebenen Erkenntnisse bisheriger Studien wird nachfolgend angenommen, dass Kriminalitätsfurcht online (im Cyberspace) und offline (in der realen Welt) zusammenhängen.

▶ H1: Personen mit einer hohen Kriminalitätsfurcht offline weisen auch eine hohe Kriminalitätsfurcht online auf.

Da über das Strafbedürfnis online bisher keine Erkenntnisse vorliegen, wird vorliegend davon ausgegangen, dass auch das Strafbedürfnis online und offline zusammenhängen.

▶ H2: Personen mit einem hohen Strafbedürfnis offline weisen auch ein hohes Strafbedürfnis online auf.

Des Weiteren weisen Studien darauf hin, dass sowohl im Offline- als auch im Online-Bereich Verbindungen von Viktimisierung und Kriminalitätsfurcht bestehen. Zudem gibt es Hinweise darauf, dass auch Offline-Viktimisierung die Kriminalitätsfurcht im Netz beeinflusst. Viktimisierung scheint hingegen mit Punitivität nicht in Verbindung zu stehen (vgl. Abschn. 2).

▶ H3:
1. Opfer in der realen Welt und Opfer im Cyberspace haben eine höhere Kriminalitätsfurcht als Nichtopfer.
2. Opfer in der realen Welt und Opfer im Cyberspace haben kein höheres Strafbedürfnis als Nichtopfer.

Entsprechend der Erkenntnisse, dass sich Kriminalitätsfurcht offline auf das Strafbedürfnis auswirkt, wird angenommen, dass dies auch für die Kriminalitätsfurcht online gilt.

▶ H4: Sowohl hohe Kriminalitätsfurcht offline als auch hohe Kriminalitätsfurcht online führen zu einem erhöhten Strafbedürfnis.

4 Eine Befragung zu Strafbedürfnissen im Cyberspace in Hamburg

4.1 Durchführung

Die Grundlage für die vorliegende Untersuchung bildet eine Dunkelfeldbefragung der Universität Hamburg aus dem Jahr 2016. Im Fokus der Befragung waren Erkenntnisse zur Viktimisierung, zur Kriminalitätsfurcht und zur Punitivität jeweils in Bezug auf klassische Delikte und zu Delikten im Cyberspace. Um eine Vergleichbarkeit der individuellen Einstellungen im Bereich der klassischen Delikte und der Delikte im Cyberspace zu ermöglichen, wurde versucht, jeweils

ähnliche Delikte in beiden Bereichen abzubilden. Es handelt sich um eine Querschnittsbefragung, die über einen Zeitraum von einem Monat (Februar-März 2017) in deutscher sowie in englischer Sprache online zugänglich war. Die Befragung wurde mittels der Umfragesoftware „Unipark“ erstellt und über soziale Netzwerke – maßgeblich Facebook – öffentlich gepostet oder an Freunde und Bekannte mit der Bitte um Teilnahme und Weiterleitung gesendet. Es ist ein selektives Schneeballverfahren gewählt worden. Auf diese Weise konnte in der kurzen Erhebungszeit eine möglichst breite Masse an Internetnutzern erreicht werden. Es bestand nicht die Intention, Viktimisierungserfahrungen repräsentativ abzubilden und Populationsparameter zu schätzen. Ziel und Zweck war vielmehr, einen ersten exemplarischen Beitrag zum Strafbedürfnis und zur Kriminalitätsfurcht im Cyberspace im Vergleich zur realen Welt zu leisten und Korrelationszusammenhänge herauszufiltern. In diesem Fall ist die fehlende Repräsentativität der Stichprobe weniger bedeutsam. Zum Ende der Erhebungsphase ergab sich eine Stichprobe aus 468 Internetnutzern.

4.2 Ergebnisse

4.2.1 Soziodemografische Variablen

Das durchschnittliche Alter der Befragten beträgt 34 Jahre. 55 % sind weiblich und 45 % männlich. 4,3 % der Befragten leben nur vorübergehend in Deutschland (bspw. Erasmus-Studierende), 5,6 % sind aus dem Ausland nach Deutschland zugewandert und 8,5 % sind in Deutschland geboren, aber mindestens ein Elternteil ist zugewandert, sodass 18,4 % der Befragten einen Migrationshintergrund haben (vgl. Tab. 1).

14 % der Befragten weisen eine niedrige Bildung auf, d. h. sie haben einen Realschulabschluss oder einen geringeren Schulabschluss oder keinen bzw. noch keinen Schulabschluss. In der Kategorie der mittleren Bildung sind die Befragten, die ein Abitur als höchsten Bildungsabschluss aufweisen (32 %) und in der Kategorie der hohen Bildung solche mit einem Hochschulabschluss (54 %). 71 % der Befragten habe keine bzw. noch keine Kinder (vgl. Tab. 1).

4.2.2 Internetnutzung

Wie sich aus Tab. 1 ergibt, beträgt die durchschnittliche Nutzung des Internets 4,63 h täglich. Wird die Nutzungszeit kategorisiert, so zeigt sich, dass von 27,4 % der Befragten das Internet nach wie vor wenig genutzt wird (zwischen 0,25 und 2 h täglich), von 42,5 % im mittleren Maße (zwischen 2 und 5 h täglich) und von 30,1 % in extremen Maße (zwischen 5 und 18 h täglich). Den hohen Nutzungszeiten

Tab. 1 Übersicht über die soziodemografischen Variablen

Variable	Beschreibung	N	Mean	S.D.	Min	Max
Alter	Alter in Jahren	468	34,28	12,87	15	83
Geschlecht	Dummyvariable ♀ = 0 (54,5 %) ♂ = 1 (45,5 %)	468	0,46	0,50	0	1
Migrationshintergrund	Dummyvariable Deutsch = 1 (81,6 %) Migration = 2 (18,4 %)	468	1,18	0,39	1	2
Bildung	Dummyvariable Niedrige Bildung 13,8 % Mittlere Bildung 32,0 % Hohe Bildung 54,2 %	 465 465 465	 0,14 0,32 0,54	 0,34 0,47 0,50	 0 0 0	 1 1 1
Kinder	Anzahl	468	0,54	0,99	0	6
Internetnutzung	Nutzung in Stunden täglich	468	4,63	3,24	0,25	18,00

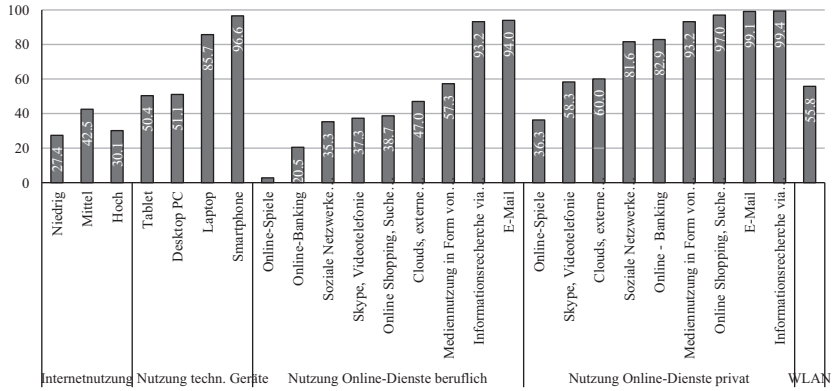


Abb. 1 Internetnutzung, Nutzung technischer Geräte, Nutzung von Online-Diensten beruflich und privat sowie Nutzung öffentlicher, nicht gesicherter Netzwerke (N = 468)

entsprechend sind die Befragten technisch ausgestattet. 96,6 % verfügen über ein Smartphone, 85,7 % über einen Laptop, 51,1 % über einen Desktop PC und 50,4 % über ein Tablet (vgl. Abb. 1).

Abb. 1 zeigt zudem das Nutzungsverhalten der Befragten in Hinblick auf Online-Dienste beruflich und privat. Während beruflich lediglich Emails und

Informationsrecherchen im Internet von fast allen Befragten (94 % bzw. 93 %) genutzt werden, dehnt sich die private Nutzung auf viele weitere Bereiche aus. Über die Nutzung von Emails und Suchmaschinen wie bspw. Google hinaus (jeweils 99 %) wird intensiv online eingekauft (97 %) und werden Videos, Musik und Filme online gestreamt (93 %) sowie soziale Netzwerke wie bspw. Facebook oder Twitter (82 %) genutzt.

Nach einer Statista Umfrage zur Nutzung von Online-Diensten („Werbung & Datenschutz 2017“ vom 17. Mai 2017 bis 19. Mai 2017)[2] an 1009 Befragten ab 16 Jahren nutzen 99 % der Befragten Emails, 94 % Online-Shopping-Portale und 76 % Social Media wie bspw. Facebook und Twitter. Demnach weist die vorliegende Stichprobe ein etwas stärkeres Online-Nutzungsverhalten auf als die Allgemeinbevölkerung, was mit dem geringeren Durchschnittsalter der Befragten erklärt werden kann.

4.2.3 Kriminalitätsfurcht und Unsicherheitsgefühl

Die kognitive und die affektive Kriminalitätsfurcht im realen und virtuellen Raum wurden mit jeweils fünf Items erhoben. Kognitive Furcht bedeutet die eingeschätzte Wahrscheinlichkeit, Opfer eines bestimmten Delikts zu werden, während affektive Furcht die Höhe der Befürchtung misst. Die Antwortkategorien bei der Wahrscheinlichkeitseinschätzung reichten von „1 = sehr unwahrscheinlich“ bis „6 = sehr wahrscheinlich“, bei der Befürchtungseinstufung von „1 = nie“ bis „6 = immer“. Es wurde versucht, die realen Delikte auf den virtuellen Raum zu übertragen (vgl. Abb. 2). Während im Internet psychische Gewalt („dass ich im Internet bedroht oder beleidigt werde“ = Cybermobbing) abgefragt wurde, war die Entsprechung in der Realität physische Gewalt („dass ich geschlagen oder verletzt werde“). Für den Wohnungseinbruchdiebstahl wurde ein Item zum Hacking gebildet.

Das Vermeidungsverhalten (konative Kriminalitätsfurcht) meint spezifische Verhaltensweisen, um einer Viktimisierung in einem bestimmten Deliktsbereich zu entgehen. Schutzmaßnahmen, die getroffen werden können, um Online-Delikte zu vermeiden, haben eine andere Qualität als solche, die gegen Kriminalität im realen Raum unternommen werden können (vgl. Tab. 2). So wurde das Vermeidungsverhalten online über sechs Einzelitems erfasst, die den Umgang mit persönlichen Daten im Netz, mit Schutzprogrammen und Passwörtern erfragten.

[2]Statista-Umfrage unter https://de.statista.com/statistik/studie/id/45554/dokument/statista-umfrage-werbung-und-datenschutz-2017 (abgerufen am 05 Juni 2019).

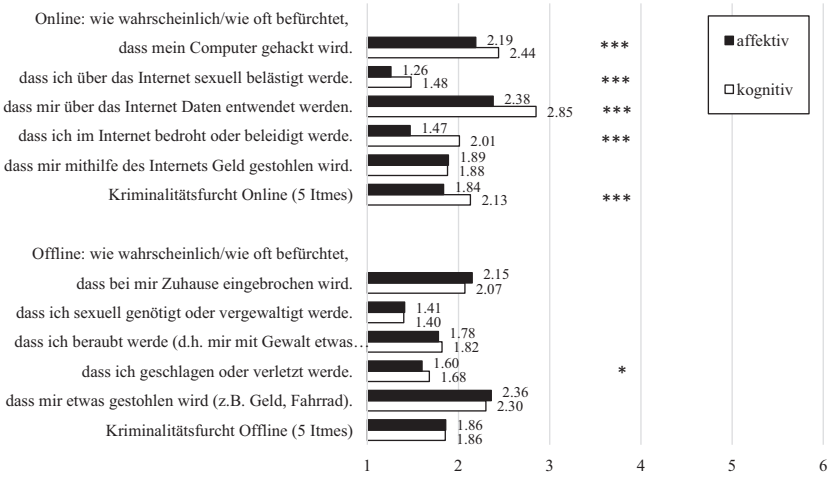


Abb. 2 Mittelwerte der Einzelitems der Skalen zur affektiven und kognitiven Kriminalitätsfurcht online und offline

Tab. 2 Skala konative Kriminalitätsfurcht online und offline

ONLINE
Konativ: Persönliche Maßnahmen zum Schutz vor Risiken beim Umgang mit dem Computer und im Internet
Ich wäge stets ab, ob ich online Daten von mir preisgebe
Ich achte darauf, dass meine Schutzprogramme (Anti-Virus, Firewall etc.) auf dem neuesten Stand sind
Ich achte darauf, möglichst unterschiedliche und sichere Passwörter zu benutzen
Ich besuche im Internet keine Seiten, denen ich nicht vollends vertraue
Ich sichere meine Daten regelmäßig auf verschiedenen Speichermedien
Ich gebe viel Geld für Schutzprogramme aus
OFFLINE
Konativ: Persönliche Maßnahmen, um sich im Alltag vor Kriminalität zu schützen
…Ich vermeide es, bestimmte Straßen, Plätze, Parks zu besuchen
…Ich vermeide es, abends öffentliche Verkehrsmittel zu benutzen
…Ich vermeide es, das Haus bei Dunkelheit zu verlassen
…Ich sichere meine Wohnung in meiner Abwesenheit besonders, indem ich z. B. zusätzliche Riegel vorlege oder eine Alarmanlage einschalte
…Ich trage Abwehrspray, ein Messer und/oder eine andere Waffe bei mir, um mich verteidigen zu können
…Ich trainiere (z. B. in einem Selbstverteidigungskurs), um mich in kritischen Situationen wehren zu können

Das Vermeidungsverhalten im realen Raum wurde ebenfalls durch sechs Einzelitems erfragt, die sich mit dem Meiden bestimmter Plätze und Gegenden zu bestimmten Zeiten, dem Nutzen öffentlicher Verkehrsmittel oder dem Sichern der Wohnung befassten.

Die Antwortkategorien reichten von „1 = trifft überhaupt nicht zu“ bis „6 = trifft voll und ganz zu“. Auch hier ließen sich Verhaltensweisen auf die virtuelle Welt übertragen. So entspricht etwa das Meiden bestimmter Plätze und Gegenden in der Wirklichkeit dem Meiden von Internetseiten, denen nicht vollends vertraut werden kann. Oder eine Absicherung durch Schutzprogramme im Internet kann in der realen Welt als ein Beisichtragen von Abwehrspray etc. oder die Teilnahme an Selbstverteidigungskursen verstanden werden. Neben den Skalen zur Kriminalitätsfurcht wurden die Probanden noch generell nach ihrem Unsicherheitsgefühl in ihrer Wohngegend bzw. im Internet befragt. Auf einer Skala von „1 = sicher“ bis „4 = unsicher“ konnten die Probanden angeben, wie unsicher sie sich fühlen, wenn sie sich in ihrer Wohngegend nachts draußen alleine aufhalten bzw. wie unsicher sie sich fühlen, wenn sie das Internet nutzen.

Abb. 2 zeigt die Mittelwerte der Items der zwei abgefragten Skalen zur affektiven und kognitiven Furcht im Internet und im realen Raum. Es zeigt sich, dass die Furcht vor einer Datenentwendung bzw. eines Datenmissbrauchs am größten ist, gefolgt von der Furcht des Computerhackings. Dies deckt sich mit den Ergebnissen der Dunkelfeldbefragung des LKA Schleswig-Holsteins (Dreißigacker und Riesner 2018, S. 26).

Die Angst, mithilfe des Internets bestohlen zu werden, ist im Vergleich zur Angst, Opfer eines Diebstahls in der realen Welt zu werden, erstaunlich gering. Ängste hinsichtlich sexueller Belästigung im Netz oder real sowie hinsichtlich Cybermobbing im Netz oder physischer Gewalt real sind in etwa gleich stark ausgeprägt. Auffällig ist, dass es kaum Unterschiede in der realen Welt zwischen kognitiver und affektiver Angst gibt. Hingegen sind hinsichtlich fast aller Deliktsbereiche die affektiven Befürchtungen, im Internet Opfer zu werden, signifikant geringer als die kognitiven Einschätzungen, Opfer werden zu können.

Tab. 3 gibt an, wie die einzelnen Skalen zur Kriminalitätsfurcht und zum Unsicherheitsgefühl zusammenhängen. Erwartungsgemäß hängen alle drei Aspekte der Furcht und das Sicherheitsgefühl in der realen Welt (offline) eng zusammen. Personen, die hohe Kriminalitätsbefürchtungen haben und auch die Wahrscheinlichkeit hoch einstufen, viktimisiert zu werden, zeigen ein hohes Vermeidungsverhalten und fühlen sich nachts allein in ihrer Wohngegend auch unsicher. Unklar ist, ob das Verhalten eine Folge der (kognitiven/affektiven) Furcht ist oder ob die Verhaltensweisen wiederum das Ausmaß der Furcht bedingen (vgl. Gibson et al. 2002, S. 540; Wetzels et al. 1995, S. 213 f.).

Tab. 3 Korrelationsmatrix der Skalen zur Kriminalitätsfurcht und zum Unsicherheitsgefühl (N = 468)

	Kognitiv Online	Affektiv Online	Konativ Online	Unsicherheitsgefühl Internet	Kognitiv Offline	Affektiv Offline	Konativ Offline
Affektiv online	,644**	1					
Konativ online	−,111*	−,101*	1				
Unsicherheitsgefühl Internet	,275**	,330**	,103*	1			
Kognitiv offline	**,495****	,372**	−0,015	,266**	1		
Affektiv offline	,400**	**,547****	−0,06	,212**	,637**	1	
Konativ offline	,201**	,285**	**,205****	,276**	,400**	,412**	1
Unsicherheitsgefühl Wohngegend	,175**	,288**	0,021	**,229****	,322**	,420**	,475**

*p<,05, **p<,01, ***p<,001

Im Cyberspace zeigt sich hingegen ein anderes Muster. Hier sind es die Personen, die ein geringes Vermeidungsverhalten zeigen, also kaum Schutzprogramme, sichere Passwörter, verschiedene Speichermedien, etc. anwenden, die hohe Befürchtungen haben, bzw. die Wahrscheinlichkeit hoch einstufen, Opfer im Netz zu werden. Offensichtlich können Schutzmaßnahmen in der realen Welt als Ausdruck von Angst betrachtet werden, während Schutzmaßnahmen in der virtuellen Welt eher geeignet scheinen, Ängste der Nutzer zu nehmen. Zwar lässt sich aus den Korrelationen nichts über die Kausalität aussagen, doch scheint es plausibel, dass nicht die hohe Angst im Netz zu einem geringen Vermeidungsverhalten führt, sondern eher ein hohes Vermeidungsverhalten Ängste reduzieren kann. Dies spräche dafür, dass Schutzmaßnahmen im Netz eine Effektivität zur Senkung der Kriminalitätsfurcht im Netz zugesprochen werden kann.

Betrachtet man die Zusammenhänge der Kriminalitätsfurchtskalen online mit jenen offline, so gehen sowohl kognitive und affektive Furcht als auch das

Unsicherheitsgefühl online mit hohen Ausprägungen auf denselben Skalen offline einher. Lediglich das Vermeidungsverhalten weist ein anderes Muster auf. Zwar zeigen Personen mit einem hohen Vermeidungsverhalten offline auch eher vermeidendes Verhalten online (d. h. Personen schützen sich gleichermaßen in der realen wie in der virtuellen Welt), allerdings haben kognitive und affektive Furcht in der realen Welt sowie das Unsicherheitsgefühl in der Wohngegend nichts damit zu tun, ob eine Person zu Schutzmaßnahmen im Netz greift.

Tab. 4 zeigt, dass signifikante Unterschiede hinsichtlich realer und virtueller Angst auf der affektiven Ebene nicht zu finden sind. Personen haben sowohl im Netz als auch in der realen Welt relativ geringe affektive Kriminalitätsfurcht. Allerdings sind die eingeschätzte Wahrscheinlichkeit hinsichtlich einer Online-Viktimisierung, das Unsicherheitsgefühl und die konative Furcht im Netz signifikant größer als in der realen Welt (vgl. Tab. 4).

Aufgrund der hohen Zusammenhänge zwischen der kognitiven und der affektiven Kriminalitätsfurcht ist es sinnvoll, beide als Subdimensionen eines übergeordneten Konstrukts, der personalen Kriminalitätsfurcht, zu betrachten (vgl. Baier et al. 2011; Windzio et al. 2007). So können Personen der Meinung sein, dass Übergriffe sehr wahrscheinlich sind, vor diesen aber keine Furcht haben, oder aber eine hohe Furcht aufweisen, die Wahrscheinlichkeit des Eintritts eines Übergriffs aber als gering einstufen. Ihre personale Furcht wäre im mittleren Bereich. Je höher sowohl kognitive als auch affektive Furcht ausgeprägt sind, desto höher ist die personale Furcht. Kognitive und affektive Furcht werden jeweils hinsichtlich eines Delikts abgefragt und anschließend multipliziert, um die Höhe der personalen Furcht zu bestimmen (vgl. Tab. 4).

Hypothese 1 lässt sich also nicht durchgängig bestätigen. Zwar gehen affektive, kognitive und konative Furcht offline sowie das Unsicherheitsgefühl in der Wohngegend auch jeweils mit affektiver, kognitiver und konativer Furcht online und mit einem Unsicherheitsgefühl im Netz einher. Allerdings gehen affektive und kognitive Furcht offline sowie das Unsicherheitsgefühl in der Wohngegend nicht mit einer konativen Furcht online einher. Hier lassen sich keine Zusammenhänge finden. Im Netz werden sehr viel höhere Vermeidestrategien angewendet als in der realen Welt und es herrscht ein sehr viel größeres Unsicherheitsgefühl. Allerdings wird eine Person, die im Netz hohe Sicherheitsmaßnahmen ergreift, auch in der realen Welt Sicherheitsmaßnahmen ergreifen.

4.2.4 Strafbedürfnis

Aussagen zur Erfassung des allgemeinen Strafbedürfnisses sind in Tab. 5 aufgeführt. Die Befragten konnten auf einer Skala von „1 = stimme gar nicht zu“ bis „4 = stimme voll und ganz zu“ antworten.

Tab. 4 Übersicht über die Variablen zum Strafbedürfnis und zur Kriminalitätsfurcht

Variable	Beschreibung	n	Mean	S.D.	Min	Max	Sign.[+]
Punitivität	4 Items Cronbachs α = ,87	468	2,79	0,75	1,00	4,00	
Strafzumessung offline	3 Items Cronbachs α = ,55	465	5,23	1,78	1,67	9,67	***
Strafzumessung online	3 Items Cronbachs α = ,45	465	4,22	1,59	1,33	9,67	
Kriminalitätsfurcht							
Kognitive Kriminalitätsfurcht offline	5 Items Cronbachs α = ,87	468	1,86	0,71	1,00	6,00	***
Kognitive Kriminalitätsfurcht online	5 Items Cronbachs α = ,73	468	2,13	0,75	1,00	5,20	
Affektive Kriminalitätsfurcht offline	5 Items Cronbachs α = ,82	468	1,86	0,72	1,00	5,20	ns
Affektive Kriminalitätsfurcht online	5 Items Cronbachs α = ,74	468	1,84	0,68	1,00	4,80	
Personale Kriminalitätsfurcht offline	5 Items Cronbachs α = ,86	468	4,03	3,30	1,00	32,20	***
Personale Kriminalitätsfurcht online	5 Items Cronbachs α = ,72	468	4,72	3,45	1	25,40	
Konative Kriminalitätsfurcht offline[a]	5 Items Cronbachs α = ,70	468	2,04	0,94	1,00	5,40	***
Konative Kriminalitätsfurcht online[b]	6 Items Cronbachs α = ,71	468	3,95	0,85	1,67	6,00	
Unsicherheitsgefühl offline	1 Item	468	1,75	0,70	1,00	4,00	***
Unsicherheitsgefühl online	1 Item	468	2,20	0,66	1,00	4,00	

[+]Level of significance: ***p < ,001, ns: non-significant

[a]Die interne Konsistenz war lediglich für die Skala „Konative Kriminalitätsfurcht offline" fragwürdig. Durch Weglassung des letzten Items (vgl. Tab. 2) hat sich Cronbachs Alpha von ,66 auf ,70 erhöht, sodass eine akzeptable interne Konsistenz erreicht werden konnte.

[b]Die internen Konsistenzen für die Kriminalitätsfurchtskalen (persönlich und konativ) online sind lediglich akzeptabel. Dass die einzelnen Items der Skalen online weniger stark miteinander übereinstimmen als im Offline-Bereich deutet darauf hin, dass hier eher unterschiedliche Aspekte der Furcht erhoben werden.

Tab. 5 Konfirmatorische Faktorenanalyse (Hauptkomponenetenanalyse; Rotation: Varimax; Faktorladungen)

	F I	F II
Täter sollten hart bestraft werden, um klar zu zeigen, dass Recht und Gesetz gelten	**0,807**	
Täter werden nur durch harte Strafen abgeschreckt, erneut Straftaten zu begehen	**0,783**	
Auf Straftaten sollte mit härteren Strafen reagiert werden, als das bisher der Fall ist	**0,817**	
Täter sollten für das, was sie getan haben, auch richtig büßen	**0,815**	
Allein durch Schadenswiedergutmachung und Gespräche mit dem Opfer lassen sich Täter nicht abhalten, Straftaten zu begehen	0,270	
Bestrafung ist nicht so wichtig. Täter sollten vor allem Schadensersatz an Opfer zahlen		0,791
Geringe Strafen führen eher zu einer Besserung eines Täters als hohe Strafen		0,652
Generell sollte von Gerichten die mildeste gesetzliche Bestrafung gewählt werden		0,603
Auch wenn jemand Anderen absichtlich Schaden zugefügt hat, sollte Nachsicht mit ihm geübt werden		0,511
Eigenwert	**4,279**	**0,989**
Erklärte Varianz	**47,5**	**10,9**

F = Faktor; fett: Items in Skalenbildung berücksichtigt

Faktorenanalysen deuten nur vage auf eine Zwei-Faktoren-Struktur hin.[3] Im Rahmen einer Reliabilitätsanalyse steigt Cronbachs Alpha von ,84 (5 Strafhärte-Items) auf ,87 unter Verzicht des Items zur Schadenswiedergutmachung. Insofern ist es sinnvoll, im Folgenden eine 4-Item-Skala der Strafhärte zugrunde zu legen

[3]Eine explorative Faktorenanalyse extrahiert nur einen Faktor, der höchste Ladungen auf den Strafhärte-Items aufweist. Eine konfirmatorische Faktorenanalyse, bei der eine Extraktion von zwei Faktoren gefordert wird, extrahiert einen ersten Faktor, der als Strafhärte bezeichnet werden kann, und einen zweiten Faktor der Strafmilde. Allerdings fallen die Faktorladungen dieses zweiten Faktors insgesamt deutlich geringer aus. Und auch die interne Konsistenz dieser Skala ist relativ gering (Cronbachs Alpha = ,68). Die ersten vier Items in Tab. 5 weisen sehr hohe Faktorladungen auf, nicht hingegen das Item zur Schadenswiedergutmachung (,270). Als Kriterium wird angelegt, auf Items zu verzichten, die eine geringere Ladung als ,60 aufweisen, um die interne Konsistenz zu erhöhen.

(Cronbachs Alpha = ,87). Die Items bilden verschiedene Strafzwecke ab, die mit Strafhärte im Zusammenhang stehen (vgl. Kemme 2012). So sollen Täter hart bestraft werden, um zu büßen (Vergeltungstheorie), um abgeschreckt zu werden (negative Spezialprävention) und um zu demonstrieren, dass Recht und Gesetz gelten (positive Generalprävention).

Über die allgemeine Strafhärte bzw. Strafmilde hinaus wurden den Befragten sechs kurze Fallvignetten vorgelegt. In diesen hat jeweils ein 25-Jähriger, nicht vorbestrafter Mann mit einem Netto-Monatseinkommen von 2000 € drei „reale" Delikte (1. Diebstahl [4 DVDs im Wert von 40 €], 2. Wohnungseinbruch [Gegenstände im Wert von 2000 €], 3. Stalking [3 Monate Nachstellung auf der Straße]) und drei Cyberdelikte (1. Illegale Downloads [4 Filme im Wert von 40 €], 2. Passwort-Hacking [Schaden in Höhe von 2000 €], 3. Cyberstalking [3 Monate unerwünschte Emails] begangen. Es sollte entschieden werden, ob hier „1 = keine Strafe", „2 = Schadenwiedergutmachung", „3 = Geldstrafe" oder „4 = Freiheitsstrafe" zu verhängen sei. Zudem sollte die Höhe der zu verhängenden Geldstrafe und die Höhe der zu verhängenden Freiheitsstrafe angegeben werden. Aus diesen Angaben wurde eine 11-stufige Skala gebildet.[4] Bei der Konstruktion der Fälle wurde versucht, die Delikte im Cyberspace mit denen in der realen Welt hinsichtlich der Schwere und des verursachten Schadens zu parallelisieren.

Offensichtlich streut der Strafrahmen bei Cyberdelikten deutlich weiter (vgl. Abb. 3). Beim Passwort-Hacking verhängen 0,4 % keine Strafe bzw. 31,8 % lediglich eine geringe Geldstrafe und 20,1 % eine Freiheitsstrafe, während der Wohnungseinbruchdiebstahl von der weit überwiegenden Anzahl der Befragten mit einer hohen Geldstrafe bzw. Freiheitsstrafe versehen wird. Die Verletzung der digitalen Privatsphäre wird als weniger gravierend und strafwürdig betrachtet als die häusliche Privatsphäre.

Insbesondere im Vergleich zum Ladendiebstahl wird ersichtlich, dass illegale Downloads eher als Kavaliersdelikt betrachtet werden.[5] 23,1 % verhängen keine Strafe und 71,7 % entscheiden sich für den Schadensausgleich bzw. eine geringe

[4] 0 = keine Strafe; 1 = Geldstrafe 1 bis 100 €; 1 = Schadensausgleich; 3 = Geldstrafe 101 bis 1000 €; 4 = 1001 bis 2000 €; 5 = 2001 bis 5000 € und/oder 1 Monat Freiheitsstrafe; 6 = 5001 bis 10000 € und/oder 2 Monate Freiheitsstrafe; 7 = Geldstrafe über 10.000 € und/oder 3 bis 5 Monate Freiheitsstrafe; 8 = 6 bis 12 Monate Freiheitsstrafe; 9 = 13 bis 24 Monate Freiheitsstrafe; 10 = 25 und mehr Monate Freiheitsstrafe.

[5] Vgl. eine Emnid-Umfrage zu Kavaliersdelikten unter https://www.presseportal.de/pm/112295/3027047 (Zugriff am 7. Mai 2019): Illegale Downloads sind auf Platz 3 der verzeihlichsten Delikte.

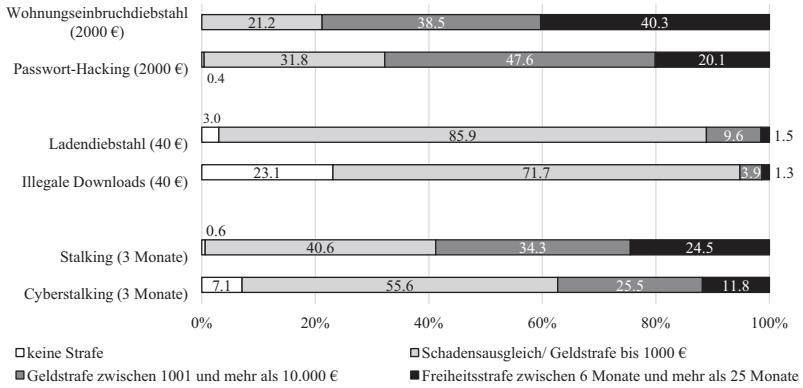


Abb. 3 Zumessung der Strafe zu sechs Fallvignetten, „reale“ Delikte und Cyberdelikte

Geldstrafe. Der Ladendiebstahl hingegen wird lediglich von 3 % als nicht strafwürdig betrachtet, aber von über 11 % mit einer hohen Geldstrafe und sogar mit Freiheitsstrafe belegt.

Abb. 4 zeigt die drei erhobenen Skalen zum Strafbedürfnis kategorisiert.[6] Erkennbar ist, dass Personen bei der Einstufung von allgemeinen Aussagen zur Strafhärte ein sehr hohes Strafbedürfnis zeigen. Knapp 80 % der Befragten sind als eher hoch bis hoch punitiv zu bezeichnen. Vergleicht man die allgemeine Strafhärte mit der Einstufung der drei Delikte (Wohnungseinbruch, Diebstahl und Stalking), so hat nur knapp die Hälfte der Befragten ein eher hohes und sehr hohes Strafbedürfnis. Das Strafbedürfnis im Rahmen der Cyberdelikte (Passwort-Hacking, illegale Download und Cyberstalking) fällt mit Abstand am geringsten aus; nur 23 % verlangen hier die volle Härte der Justiz.

Tab. 6 gibt die Korrelationen zwischen den einzelnen Strafzumessungseinstufungen für die Online- und die Offline-Delikte wieder sowie die Korrelationen zwischen dem Online- und dem Offline-Bereich. Zunächst zeigt sich, dass die allgemeine Strafhärte mit einem höheren Strafen für Online- wie auch für Offline-Delikte einhergeht. Eine Person, die hohe Strafen für die drei realen

[6]Die Werte der vier einzelnen Strafhärte-Items wurden in ein 11-stufiges Format umgerechnet. Zudem wurden die Antworten zu den drei realen Delikten und zu den drei Cyberdelikten gemittelt. Im Anschluss sind Personen mit Werten bis 2,75 als „sehr gering“ eingestuft worden, Personen mit Werten über 2,75 bis 5,50 als „eher gering“, Personen mit Werten über 5,50 und 8,25 als „eher hoch“ und Personen mit Werten über 8,25 als „sehr hoch“.

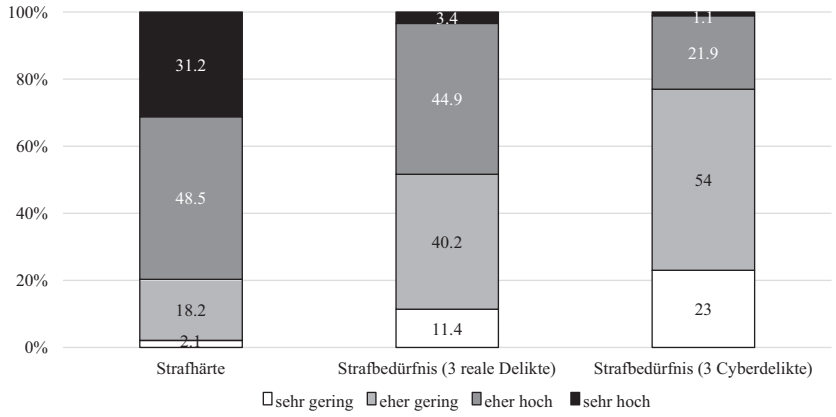


Abb. 4 Punitivität und Strafbedürfnis (reale und Cyberdelikte)

Delikte verhängt hat, hat ebenso im Cyberspace höhere Strafen verhängt ($r = ,674$; $p < ,001$).

Insgesamt lässt sich Hypothese 2 bestätigen. Ein hohes allgemeines Strafbedürfnis geht nicht nur mit dem Bedürfnis für höhere Strafen bei Realdelikten sondern auch bei Delikten im Cyberspace einher. Es lässt sich sagen, dass Personen, die eher zu hohen Strafen für Wohnungseinbruchdiebstahl, Ladendiebstahl und Stalking greifen, auch höhere Strafen für Passwort-Hacking, Illegale Downloads und Cyberstalking wählen. Dabei sind die Korrelationen der miteinander vergleichbaren Delikte online und offline am höchsten (vgl. Tab. 6). Dennoch ist das Niveau des Strafbedürfnisses unterschiedlich, denn es werden signifikant höhere Strafen für die drei Realdelikte im Vergleich zu den drei Cyberdelikten gewählt (vgl. Tab. 4).

Bei Betrachtung der Ergebnisse für das Strafbedürfnis und die Kriminalitätsfurcht ist interessant, dass signifikant härtere Strafen für die realen Delikte verhängt werden, sowohl die personale und die konative Kriminalitätsfurcht als auch das Unsicherheitsgefühl in der realen Welt aber signifikant niedriger sind als im virtuellen Raum (vgl. Tab. 4). Das höhere Furchtniveau im Cyberspace geht demnach nicht einher mit der Verhängung höherer Strafen für Cyberdelikte.

4.2.5 Viktimisierung

Eine wichtige Variable im Zusammenhang mit Kriminalitätsfurcht ist die Viktimisierung. Die Probanden wurden nach elf Cyberdelikten befragt und nach fünf

Tab. 6 Korrelationsmatrix der Skalen und Items zum Strafbedürfnis (N = 468)

	Strafhärte	3 Realdelikte	WED	Ladendiebst.	Stalking	Drei Cyberdelikte	Passwort-Hacking	Illegale Downloads
Strafzumessung 3 Realdelikte	**,275 *****							
Wohnungseinbruchdiebstahl	,244 ***	,795 ***						
Ladendiebstahl	,150 **	,590 ***	,361 ***					
Stalking	,200 ***	,786 ***	,352 ***	,211 ***				
Strafzumessung 3 Cyberdelikte	**,266 *****	**,674 *****	,484 ***	,480 ***	,532 ***			
Passwort-Hacking	,245 ***	,568 ***	**,577 *****	,401 ***	,301 ***	,761 ***		
Illegale Downloads	,125 **	,254 ***	,124 **	**,451 *****	,105 *	,506 ***	,192 ***	
Cyberstalking	,172 ***	,522 ***	,249 ***	,223 ***	**,606 *****	,776 ***	,309 ***	,152 **

**p<,01, ***p<,001

Delikten in der realen Welt. Zu den Delikten wurde angegeben, ob sie überhaupt einmal im bisherigen Leben erlebt wurden (Lebenszeitprävalenz), und wie häufig sie in den letzten 12 Monaten erlebt wurden. Aus der Inzidenz des letzten Jahres wurde die 12-Monats-Prävalenz errechnet.

Das am häufigsten erlebte reale Delikt ist nach wie vor der Diebstahl (vgl. Abb. 5). Ca. 60 % der Befragten wurden mindestens einmal in ihrem Leben bestohlen und ca. 14 % allein im letzten Jahr. Jemals Opfer eines Einbruchs bzw. eines versuchten Einbruchs geworden zu sein, berichteten rund 18 % der Befragten. Die Gesamt-Lebensprävalenz (alle fünf Delikte) liegt bei knapp 70 %. Auch im Cyberspace berichtet fast jeder Befragte, mindestens einmal im Leben Opfer gewesen zu sein (86 %). Diese hohen Gesamt-Lebens- und 12-Monats-Prävalenzen

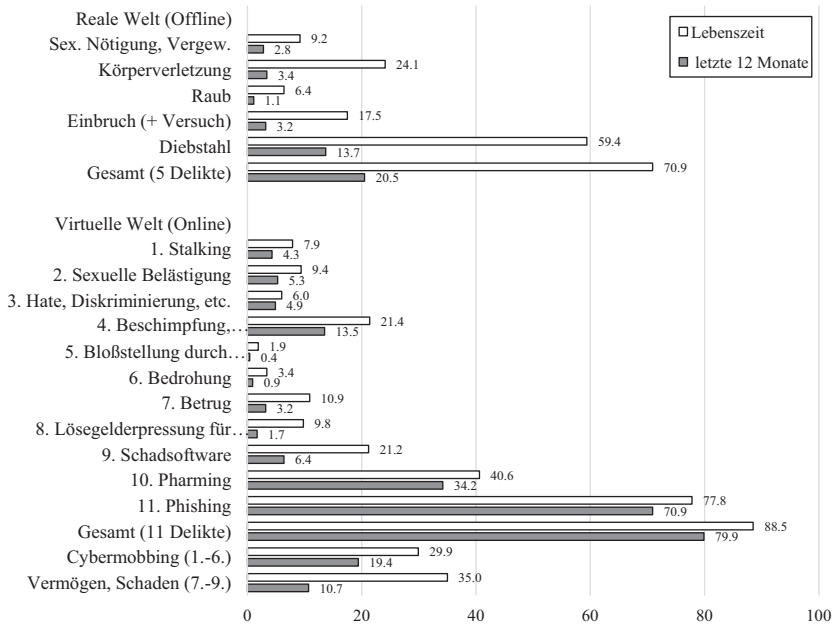


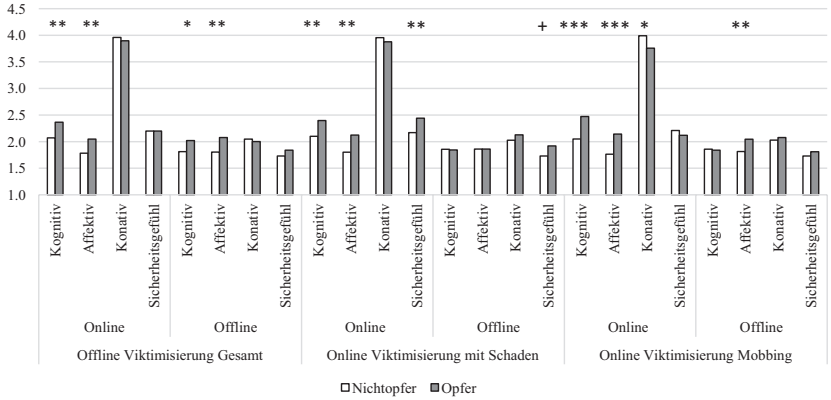
Abb. 5 Lebenszeit- und 12-Monats-Prävalenzen der Viktimisierung online und offline

beruhen auf den hohen Angaben im Bereich des Phishings und Pharmings. Fragen[7] waren so formuliert, dass auch Versuche mitinbegriffen waren, sodass nicht deutlich wird, ob die Befragten tatsächlich ihre Kontodaten, Passwörter oder Zugangsdaten preisgegeben oder eingegeben und einen Schaden erlitten haben. Tatsächlich hat fast jeder Internetnutzer heutzutage schon einmal Phishing-Mails erhalten.

Betrachtet man nur die Items, bei denen es tatsächlich zu einem Schaden aufgrund einer Infizierung, einer Sperrung oder eines Betruges (Items 7 bis 9)[8]

[7]„Ich wurde in einer gefälschten E-Mail dazu aufgefordert, vertrauliche Daten, wie z. B. Kontodaten oder Passwörter, preiszugeben (sog. Phishing-Mail).“; „Ich wurde auf eine gefälschte Seite umgeleitet, welche wie eine Website eines von mir genutzten Dienstes (z. B. PayPal, Ebay) aussah, und dort dazu aufgefordert, meine Zugangsdaten (Login-Daten) einzugeben (sog. Pharming).“

[8]Item 7: „Ich wurde im Internet Opfer eines Betrugs und erlitt dadurch einen finanziellen Schaden.“; Item 8: „Mein Computer wurde durch nicht autorisierte Fremdeinwirkung über das Internet gesperrt, um ein Lösegeld zu erpressen.“; Item 9: „Mein Computer wurde mit Schadsoftware infiziert, sodass dadurch Datenverluste oder finanzielle Schäden entstanden sind.“



+ <0.10, * p <0.05, ** p<0.01. *** p <0.001

Abb. 6 Mittelwertsvergleiche der Kriminalitätsfurcht online und offline zwischen Opfern und Nichtopfern (in den letzten 12 Monaten)

gekommen ist, fallen die Prävalenzen deutlich geringer aus (Lebenszeit 35 % bzw. 12 Monate 11 %). Auch alle Cybermobbing-Items[9] wurden zu einer Skala zusammengefasst. 30 % gaben an, im Internet bereits mindestens einmal in ihrem Leben beschimpft, bedroht, beleidigt, bloßgestellt, gestalkt oder sexuell belästigt worden zu sein. Diese Opfererlebnisse mussten ca. 20 % der Befragten im letzten Jahr machen.

4.2.6 Strafbedürfnis, Kriminalitätsfurcht und Viktimisierung

Opfer weisen nicht generell eine höhere Kriminalitätsfurcht auf (vgl. Abb. 6). Bivariat bestätigt sich allerdings Hypothese 3.1 teilweise: Opfer in der realen Welt und Opfer im Cyberspace haben eine höhere kognitive und affektive Kriminalitätsfurcht. Ist es zu einer Viktimisierung im Netz gekommen, bei der das Opfer einen finanziellen Schaden erlitten hat, so sind lediglich die Einschätzung und Befürchtung, Opfer im Netz zu werden, signifikant höher. Eine erhöhte Kriminalitätsfurcht in der realen Welt lässt sich nicht feststellen. Allerdings fühlen sich diese Opfer nicht nur im Netz sehr viel unsicherer als Nichtopfer, sondern auch die Unsicherheit in der realen Welt ist leicht erhöht.

[9]Auch die Frage zur sexuellen Belästigung wird hier als Cybermobbing i.w.S. kategorisiert: „Ich wurde über das Internet gegen meinen Willen gezielt sexuell bedrängt, zum Beispiel durch anzügliche Nachrichten oder Bilder.“

Die massivsten Unterschiede können zwischen Opfern und Nichtopfern von Cybermobbing festgestellt werden. Waren die Befragten Opfer von Cybermobbing in den letzten 12 Monaten, so ist ihre kognitive und affektive Furcht im Cyberspace signifikant höher, und darüber hinaus auch ihre affektive Furcht in der realen Welt. Die konative Kriminalitätsfurcht (Vermeidungsverhalten) ist bei den Opfern geringer. Hierin zeigt sich, dass es die Cybermobbing-Opfer sind, die in geringerem Maße Sicherheitsvorkehrungen im Netz betreiben, wie bspw. Schutzprogramme, häufige Passwortwechsel oder das Meiden unsicherer Seiten. Insofern wird im Cyberspace durch diese Items lediglich ein Schutzverhalten gemessen. Hierin kommt nicht, wie in der realen Welt, eine höhere Furcht zum Ausdruck. Vielmehr zeigen die Korrelationen (vgl. Tab. 3) in Verbindung mit Abb. 6, dass vor allem Nichtopfer höhere Schutzmaßnahmen ergreifen und auch weniger personale Furcht zeigen.

Zwischen Viktimisierung und Strafhärte bzw. Strafbedürfnis ergeben sich keine Zusammenhänge. So hat es auf die allgemeine Strafhärte oder die Strafzumessung bei den realen oder den Cyberdelikten keinen Einfluss, ob der Befragte schon einmal selbst Opfer einer realen oder virtuellen Straftat geworden ist. Auch bei Betrachtung der Einzelitems ergeben sich kaum Zusammenhänge. Ist eine Person Opfer eines Wohnungseinbruchdiebstahls geworden, so ist ihre allgemeine Strafhärte leicht erhöht (WED: $t = -1{,}808$; $p = {,}071$), allerdings bemisst sie die Strafe bei der Fallvignette zum Wohnungseinbruchdiebstahl nicht höher als Nichtopfer eines WED. Zum Teil zeigen die Ergebnisse in die entgegengesetzte Richtung. So sind bspw. die Nicht-Opfer eines Diebstahls insgesamt strafhärter als die Opfer. Es lässt sich entsprechend Hypothese 3.2 bivariat keine Verbindung zwischen Opferwerdung und Strafbedürfnis feststellen. Die zu Realdelikten festgestellten Befunde eines nicht nachweisbaren Zusammenhangs (vgl. Abschn. 2. Strafbedürfnisse und Kriminalitätsfurcht) sind nach der vorliegenden Stichprobe auch auf den Cyberspace zu übertragen.

Zusammenhänge zwischen Kriminalitätsfurcht und Strafhärte sind allerdings ersichtlich (vgl. Tab. 7). So sind Personen mit hoher affektiver und kognitiver Kriminalitätsfurcht und mit hohem Vermeidungsverhalten offline sowie einem hohen Unsicherheitsgefühl in der eigenen Wohngegend insgesamt strafhärter. Allerdings geht nur ein hohes Vermeidungsverhalten in der realen Welt damit einher, sowohl reale Delikte als auch Cyberdelikte mit höheren Strafen zu versehen. Interessant ist, dass auch Online-Kriminalitätsfurcht und allgemeine Strafhärte zusammenhängen, allerdings sind die Zusammenhänge bezüglich des Vermeidungsverhaltens (bzw. Schutzverhalten im Internet) und des Sicherheitsgefühls im Internet weniger stark ausgeprägt. Zudem hat die kognitive Furcht online (also die Einschätzung der Opferwahrscheinlichkeit) keinen Einfluss auf

Tab. 7 Korrelationen zwischen Strafbedürfnis und Kriminalitätsfurcht

	Strafhärte allgemein 4 Items		Strafzumessung 3 reale Delikte		Strafzumessung 3 Cyberdelikte	
Kognitiv Online	−,010		,071		,046	
Affektiv Online	**,107**	*	**,130**	**	,075	
Konativ Online	**,173**	**	,057		,083	
Unsicherheitsgefühl Internet	**,184**	**	,059		**,095**	*
Kognitiv Offline	**,152**	**	,046		,053	
Affektiv Offline	**,103**	*	,054		,037	
Konativ Offline	**,344**	**	**,108**	*	**,131**	**
Unsicherheitsgefühl Wohngegend	**,255**	**	0,083		0,074	

*p<,05, **p<,01, ***p<,001

die Strafhärte, sondern lediglich die emotionale Befürchtung Opfer zu werden. Dies ist plausibel damit zu erklären, dass Gefahren im Netz über Schutzmaßnahmen gut vermieden werden können und demnach leichter einzuschätzen sind als Gefahren, die von der Kriminalität in der realen Welt ausgehen. Personen mit hoher affektiver Furcht in der virtuellen Welt verhängen höhere Strafen für reale jedoch nicht für Cyberdelikte; dies lässt sich zunächst nicht erklären. Hingegen nachvollziehbar verhängen Personen mit einem hohen Unsicherheitsgefühl im Netz höhere Strafen für Cyberdelikte. Personen mit einer hohen Kriminalitätsfurcht online und offline haben ein höheres Strafbedürfnis (Ausnahme kognitive Kriminalitätsfurcht online).

4.2.7 Einflussfaktoren der Strafbedürfnisse und der Kriminalitätsfurcht

Nachfolgend sollen anhand von multivariaten Modellen einerseits die Einflussfaktoren der Kriminalitätsfurcht online und andererseits die Einflussfaktoren auf die Punitivität untersucht werden. Tab. 4 gibt einen Überblick über die Variablen zum Strafbedürfnis und zur Kriminalitätsfurcht. In Tab. 8 sind für die personale und die konative Furcht online sowie das Unsicherheitsgefühl im Netz jeweils lineare Regressionen gerechnet worden.

Es sollte jeweils untersucht werden, wie stark eine Furchtkomponente von der Viktimisierung online und offline sowie von den anderen Furchtaspekten online

Tab. 8 Einflussfaktoren der Kriminalitätsfurcht im Netz (OLS-Regression; abgebildet: Beta)

	Personale Furcht Im Netz				Konative Furcht Im Netz				Unsicherheitsgefühl Im Netz			
	Modell 1		Modell 2		Modell 1		Modell2		Modell1		Modell 2	
Männer (Ref. Frauen)	−0,031		−0,004		0,021		0,090	+	−0,005		0,001	
Alter	**−0,130**	**	**−0,110**	**	**0,322**	***	**0,282**	***	0,091	+	0,096	*
Migrationshintergrund (Ref. ohne)	0,014		0,036		0,043		0,020		0,025		0,022	
Bildung hoch (Ref. niedrig)	0,069		0,054		−0,013		0,022		−0,068		−0,070	
Internetnutzung	0,049		0,024		0,065		0,063		**−0,104**	*	**−0,103**	*
Viktimisierung Netz (Ref. Nichtopfer)	**0,093**	*	**0,105**	**	0,063		0,056		−0,023		−0,032	
Viktimisierung Real (Ref. Nichtopfer)	0,088	*	0,050		−0,006		−0,002		0,003		0,000	
Personale Furcht Netz					**−0,127**	*	**−0,129**	*	**0,331**	***	**0,331**	***
Personale Furcht Real			**0,520**	***	0,049		−0,018		−0,008		−0,031	
Konative Furcht Netz	**−0,125**	**	**−0,088**	*					0,071		0,076	
Konative Furcht Real	0,205	***	0,028				**0,264**	***	0,127	*	0,089	
Unsicherheit Netz	**0,301**	***	**0,236**	***	0,099	*	0,079					
Unsicherheit Real	0,081	+	−0,029		0,014		−0,059				**0,104**	*
N	**465**		**465**		**465**		**465**		**465**		**465**	
Korr. R^2	**,217**		**,412**		**,101**		**,139**		**,169**		**,175**	

*p<,05, **p<,01, ***p<,001

und offline beeinflusst wird (Modell 1).[10] Modell 2 schließt darüber hinaus die jeweils zu erklärende Furchtkomponente in der realen Welt ein. Es zeigt sich, dass die personale Furcht in der realen Welt die größte Kraft zur Erklärung der personalen Furcht im Netz aufweist. Weiterhin können ein hohes Unsicherheitsgefühl im Netz und vorherige Viktimisierung im Netz sowie geringe Sicherungsmaßnahmen im Netz die Befürchtung, Opfer im Netz zu werden, erklären.

Die Einflussfaktoren der konativen Furcht im Netz divergieren erheblich. Allerdings können die hier erhobenen Variablen insgesamt nur ca. 14 % der Varianz erklären, während die personale Furcht im Netz zu 41 % und das Unsicherheitsgefühl im Netz zu 17 % erklärt werden können. Der größte Teil der Varianz geht auf das Alter zurück; je älter die befragten Personen, desto mehr Sicherungsmaßnahmen im Netz werden angewendet. Personen, die sich in der realen Welt vor Kriminalität schützen, schützen sich auch im Netz, sodass die konative Furcht offline ebenfalls einen hohen Erklärungswert für die konative Furcht online aufweist.

Die Internetnutzungsdauer hat lediglich im Rahmen des Unsicherheitsgefühls im Netz eine Bedeutung. Je mehr Personen das Internet nutzen, desto sicherer fühlen sie sich. Interessant ist, dass das Unsicherheitsgefühl in der realen Welt zwar ebenfalls einen Einfluss auf die Unsicherheit im Netz hat; jedoch sind es vor allem Personen mit einer hohen personalen Furcht im Netz, die sich gleichfalls unsicher fühlen.

Während die allgemeine Strafhärteskala eine sehr hohe interne Konsistenz aufweist, gilt dies nicht für die Strafzumessungsskalen online und offline (vgl. Tab. 4).[11] Dies ist nicht verwunderlich, da für sehr unterschiedliche Delikte Strafen zu verhängen waren.

Tab. 9 zeigt drei Modelle zur Erklärung des Strafbedürfnisses. In Modell 1 flossen lediglich die Kontrollvariablen ein (5,4 % Varianzaufklärung). Modell 2 überprüft den Einfluss der Viktimisierung und der Furcht in der realen Welt (signifikante Änderung in F auf 18 % aufgeklärte Varianz). Und im letzten Schritt werden die Viktimisierung und die Furcht im Cyberspace berücksichtigt. Wie auch in anderen Studien haben Bildung, Alter und Geschlecht einen

[10]Da die Prädiktoren untereinander zum Teil korrelieren (vgl. Tab. 3), wurden alle hinsichtlich Multikollinearität untersucht. Sowohl die Toleranzwerte als auch die VIF-Werte liegen durchgehend im nicht kritischen Bereich (Urban und Mayerl 2006, S. 232).

[11]Insofern eigneten sich die Skalen zum Strafbedürfnis für Cyber- und für reale Delikte nicht als abhängige Variablen. Auch für die Einzelitems der Strafzumessung konnten keine zuverlässigen Modelle geschätzt werden.

Tab. 9 Einflussfaktoren des Strafbedürfnisses (OLS-Regression; abgebildet: Beta)

	Modell 1		Modell 2		Modell 3	
Männer (Ref. Frauen)	−0,029		**0,140**	**	**0,132**	**
Alter	**0,168**	**	**0,119**	*	**0,095**	*
Migrationshintergrund (Ref. ohne)	0,020		−0,028		−0,033	
Bildung hoch (Ref. Bildung niedrig)	**−0,168**	***	**−0,112**	*	**−0,111**	*
Internetnutzung	−0,037		−0,047		−0,045	
Viktimisierung Real (Ref. Nichtopfer)			**−0,111**	*	**−0,113**	**
Personale Furcht Real			−0,030		−0,048	
Konative Furcht Real			**0,350**	***	**0,277**	***
Unsicherheitsgefühl Wohngegend			**0,164**	**	**0,161**	**
Viktimisierung Netz (Ref. Nichtopfer)					−0,002	
Personale Furcht Netz					0,026	
Konative Furcht Netz					0,074	
Unsicherheit Netz					0,064	
N	**465**		**465**		**465**	
Korr. R^2	**,054**		**,180**		**,182**	

*p<,05, **p<,01, ***p<,001

signifikanten Einfluss auf die Punitivität. Modell 2 zeigt, dass Viktimisierung sogar einen gegenteiligen Effekt auf die Punitivität hat (vgl. Abschn. 2), sodass Nichtopfer realer Kriminalität punitiver als Opfer sind. Zudem schlägt sich die Kriminalitätsfurcht in der realen Welt stark auf das allgemeine Strafbedürfnis nieder, mit Ausnahme der personalen Kriminalitätsfurcht, was sich auch in anderen Studien zeigte (vgl. Abschn. 2). Vor allem Personen mit einem hohen Vermeidungsverhalten in der realen Welt und einem hohen Unsicherheitsgefühl in der eigenen Wohngegend sind punitiver. Durch Hinzunahme der Viktimisierung online und der Furcht im Netz kann keine Verbesserung des Modells erzielt werden (keine signifikante Änderung in F; 18,2 % aufgeklärte Varianz). Insofern kann die Hypothese 4 nicht bestätigt werden. Kriminalitätsfurcht im Netz trägt nicht zur Erklärung von allgemeiner Strafhärte bei. Lediglich eine hohe Kriminalitätsfurcht offline kann ein hohes Strafbedürfnis erklären.

5 Zusammenfassung

Zunächst ist festzuhalten, dass sich ein Teil der Ergebnisse aus bisherigen Studien bestätigen ließ. Befunde zum Alter waren bisher widersprüchlich. Während einige Studien mit zunehmendem Alter eine höhere Kriminalitätsfurcht online fanden (bspw. Alshalan 2006; Brunton-Smith 2018), waren es vorliegend wie auch bei Dreißigacker und Riesner (2018) die jüngeren Personen, die eine höhere personale Kriminalitätsfurcht aufwiesen. Vermeidestrategien werden allerdings eher von älteren Menschen angewendet. Des Weiteren konnten Studien zeigen, dass Frauen höhere Furcht im Cyberspace aufweisen (Alshalan 2006; Henson et al. 2013; Pereira et al. 2016; Yu 2014). Dieser Zusammenhang ließ sich vorliegend auf der bivariaten Ebene für die personale und die konative Furcht ebenfalls zeigen. Beide Befunde lassen sich zum Teil mit der sehr viel höheren Opferwerdung jüngerer Frauen im Bereich des Cybermobbing erklären (Bergmann et al. 2019).

Der Viktimisierung konnte in einigen Studien Effekte auf die Kriminalitätsfurcht online nachgewiesen werden (Henson et al. 2013; Lenhart et al. 2016; Brunton-Smith 2018; Dreißigacker und Riesner 2018). Vorliegend zeigte sich lediglich für die Opferwerdung im virtuellen Raum ein Effekt auf die personale Furcht online. Viktimisierung in der realen Welt scheint in geringerem Maße mit der personalen Furcht online zusammenzuhängen.

Der beste Prädiktor für personale Furcht im Netz war vorliegend die personale Furcht in der realen Welt. Diese Ergebnisse scheinen die These zu bestätigen, dass es ein allgemein existierendes Konstrukt von Furcht gibt, welches vom eigentlichen Risiko der Opferwerdung entkoppelt ist (vgl. Roberts et al. 2013; Brunton-Smith 2018). Eine solche generelle Kriminalitätsfurcht unterscheidet nicht zwischen realer und virtueller Welt.

Im Rahmen des Strafbedürfnisses lassen sich die Ergebnisse nicht mit bisherigen Studien vergleichen. Es wurde angenommen, dass hier die Furcht online und offline gleichermaßen zu einem höheren allgemeinen Strafbedürfnis führt. Die allgemeine Strafhärte hängt allerdings lediglich von allen Furchtkomponenten in der realen Welt ab. Kriminalitätsfurcht im Cyberspace wirkt sich nach vorliegenden Ergebnissen nicht auf Punitivität bzw. eine allgemeine Strafhärte aus. Insgesamt ist das Bedürfnis, Delikte im Cyberspace zu bestrafen, noch sehr gering ausgeprägt. Auch wenn der Schaden, der durch die sich entsprechenden realen und virtuellen Verhaltensweisen hervorgerufen wird, gleich hoch ist, werden sehr viel mildere Strafen im Cyberbereich gegeben. Die Delikte scheinen als weniger strafwürdig angesehen zu werden. Hierin spiegelt sich, dass nach wie vor Anzeigequoten im Online-Bereich gering sind (Birkel et al. 2019). Warum Strafbedürfnisse im Netz wesentlich geringer sind als in der realen Welt,

vermag die Untersuchung nicht abschließend zu beantworten. Es handelt sich bisher um ein zu wenig erforschtes Feld. Dargelegte Ergebnisse sind lediglich als erste explorative Schritte zu bezeichnen. Weitere Studien zu Einflussfaktoren der Strafhärte bzw. Strafmilde im Cyberspace könnten wichtige Hinweise auf gesetzgeberische Nachbesserungen liefern.

Literatur

Alshalan, A. (2006). Cyber-crime fear and victimization: An analysis of a national survey. http://www.ibrarian.net/navon/paper/CYBER_CRIME_FEAR_AND_VICTIMIZATION_AN_ANALYSIS_O.pdf?paperid=5920587. Zugegriffen: 16. Apr. 2019.

Armborst, A. (2017). How fear of crime affects punitive attitudes. *European Journal of Criminal Policy and Research, 23*(3), 461–481.

Amtsblatt der Europäischen Union. (2005). Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:DE:PDF. Zugegriffen: 6. Apr. 2019.

Applegate, B. (1997). *Specifying public support for rehabilitation: A factorial survey approach*. Ohio: University of Cincinnati.

Applegate, B., Cullen, F., Fisher, B., & Vander Ven, T. (2000). Forgiveness and fundamentalism: Reconsidering the relationship between correctional attitudes and religion. *Criminology, 38,* 719–753.

Baier, D., Kemme, S., Hanslmaier, M., Doering, B., Rehbein, F., & Pfeiffer, C. (2011). *Kriminalitätsfurcht, Strafbedürfnisse und wahrgenommene Kriminalitätsentwicklung. Ergebnisse von bevölkerungsrepräsentativen Befragungen aus den Jahren 2004, 2006 und 2010 (KFN-Forschungsbericht Nr. 117).* Hannover: KFN.

Bergmann, M., Kliem, S., Krieg, Y., & Beckmann, L. (2019). *Jugendliche in Niedersachsen. Ergebnisse des Niedersachsensurveys 2017 (KFN-Forschungsbericht Nr. 144).* Hannover: KFN.

Bilsky, W., Mecklenburg, E., & Wetzels, P. (1992). *Persönliches Sicherheitsgefühl, Angst vor Kriminalität und Gewalt, Opfererfahrung älterer Menschen. Skalenanalyse und Skalenkonstruktion zur KFN-Opferbefragung 1992 (KFN-Forschungsbericht Nr. 13).* Hannover: KFN.

Birkel, C., Church, D., Hummelsheim-Doss, D., Leitgöb-Guzy, N., & Oberwittler, D. (2019). *Der Deutsche Viktimisierungssurvey 2017: Opfererfahrungen, kriminalitätsbezogene Einstellungen sowie die Wahrnehmung von Unsicherheit und Kriminalität in Deutschland*. Wiesbaden: Bundeskriminalamt.

Brunton-Smith, I. (2018). Fear 2.0. Worry about cybercrime in England and Wales. In M. Lee & G. Mythen (Hrsg.), *International handbook on fear of crime*. London: Routledge.

Boehme, R., & Moore, T. (2012). How do consumers react to cybercrime. https://ieeexplore.ieee.org/document/6489519/. Zugegriffen: 15. Dez. 2018.

Boers, K. (1991). *Kriminalitätsfurcht: Über den Entstehungszusammenhang und die Folgen eines sozialen Problems*. Pfaffenweiler: Centaurus.

Borg, M. (1997). The Southern subculture of punitiveness? Regional variation in support for capital punishment. *Journal of Research in Crime and Delinquency, 34,* 25–45.

Bornewasser, M. (2012). Kriminalitätsfurcht – Ein Phänomen mit abnehmender Bedeutung? https://www.bpb.de/politik/innenpolitik/innere-sicherheit/76648/kriminalitaetsfurcht?p=all#footnodeid10-10. Zugegriffen: 3. März 2019.

Britt, C. (1998). Race, religion, and support for the death penalty. A Research Note. *Justice Quarterly, 15,* 175–191.

Bundesministerium des Innern. (2011). Cyber-Sicherheitsstrategie für Deutschland. Berlin.

Bundesministerium der Verteidigung. (o. D.). Cybersicherheitsrat. https://www.bmvg.de/de/themen/cybersicherheit/partnerschaften-zur-cybersicherheit/cyber-sicherheitsrat. Zugegriffen: 05. Apr. 2019.

Cook, K., & Powell, C. (2003). Christianity and punitive mentalities: A qualitative study. *Crime, Law and Social Change, 93,* 69–89.

Costelloe, M., Chiricos, T., & Gertz, M. (2009). Punitive attitudes toward criminals. Exploring the relevance of crime salience and economic insecurity. *Punishment & Society, 11,* 25–49.

Council of Europe. (2001). Convention on cybercrime. http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf. Zugegriffen: 05. Apr. 2019.

Cullen, F. T., Clark, G. A., Cullen, J. B., & Mathers, R. A. (1985). Attribution, salience, and attitudes toward criminal sanctioning. *Criminal Justice and Behavior, 12,* 305–331.

Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI). DIVSI U25-Studie. Euphorie war gestern. Die „Generation Internet“ zwischen Glück und Abhängigkeit. https://www.divsi.de/wp-content/uploads/2018/11/DIVSI-U25-Studie-euphorie.pdf. Zugegriffen: 1. Juli 2019.

Dreißigacker, A. (2017). *Befragung zu Sicherheit und Kriminalität. Kernbefunde der Dunkelfeldstudie 2017 des Landeskriminalamtes Schleswig-Holstein.* Hannover: KFN.

Dreißigacker, A., & Riesner, L. (2018). *Private Internetnutzung und Erfahrung mit computerbezogener Kriminalität – Ergebnisse der Dunkelfeldstudien des Landeskriminalamtes Schleswig-Holstein 2015 und 2017*. Hannover: KFN.

Dowler, K. (2003). Media consumption and public attitudes toward crime and justice. The relationship between fear of crime, punitive attitudes, and perceived police effectiveness. *Journal of Criminal Justice and Popular Culture, 10,* 109–126.

Eisele, G. (2013). *Computer- und Medienstrafrecht*. München: Beck.

Eisele, G. (2016). Cyberkriminalität. In J. Heesen (Hrsg.), *Handbuch Medien und Informationsethik* (S. 255–261). Stuttgart: J.B. Metzler.

Eschholz, S. (1997). The media and fear of crime: A survey of the research. *Journal of Law and Public Policy, 9,* 37–59.

Ewald, U. (2000). Criminal Victimisation and social Adaption in Modernity. Fear of Crime and Risk Perception in the New Germany. In T. Hope & R. Sparks (Hrsg.), *Crime, risk and insecurity: Law and order in everyday life and political discourse* (S. 166–199). London: Routledge.

Garland, D. (2001). *The culture of control. Crime and social order in contemporary society*. Oxford: Clarendon.

Gibson, C. L., Zhao, J., Lovrich, N. P., & Gaffney, M. J. (2002). Social integration, individual perceptions of collective efficacy, and fear of crime in three cities. *Justice Quarterly, 19,* 537–564.

Hale, C. (1996). Fear of crime: A review of the literature. *International Review of Victimology, 4,* 79–150.

Hanslmaier, S., & Kemme, S. (2011). Kriminalität in der öffentlichen Wahrnehmung: Welchen Einfluss hat die Mediennutzung? *Zeitschrift für Rechtssoziologie, 32*(1), 129–152.

Hartnagel, T. F., & Templeton, L. (2008). Perceptions, Emotions and Experiences of Crime: Effects on Attitudes Toward Punishment in a Canadian Sample. In H. Kury (Hrsg.), *Fear of crime – Punitivity: New developments in theory and research. Crime and crime policy* (S. 349–370). Bochum: Dr. N. Brockmeyer.

Henson, B., Reyns, B. W., & Fisher, B. S. (2013). Fear of crime online? Examining the effect of risk, previous victimization, and exposure on fear of online interpersonal victimization. *Journal of Contemporary Criminal Justice, 29*(4), 475–497.

Herbst, M. (2017). Alter Wein in neuen Schläuchen? Neue Formen der Fortbildung im Deliktsfeld Cybercrime bei der Polizeiakademie Niedersachsen. In W. Honekamp & R. Povalej (Hrsg.), *Polizei-Informatik 2017* (S. 51–60). Remscheid: Re Di Roma.

Higgins, G., Ricketts, M., & Vegh, D. T. (2008). The role of self-control in college student's perceived risk and fear of online victimization. *American Journal of Criminal Justice, 33,* 223–233.

Hirtenlehner, H. (2009). Kriminalitätsangst – klar abgrenzbare Furcht von Straftaten oder Projektionsfläche sozialer Unsicherheitslagen? Ein Überblick über den Forschungsstand von Kriminologie und Soziologie zur Natur kriminalitätsbezogener Unsicherheitsgefühle der Bürger. *Journal für Rechtspolitik, 17,* 13–22.

Hirtenlehner, H. (2010). Instrumentell oder expressiv? Zu den Bestimmungsfaktoren individueller Straflust. *Soziale Probleme, 21*(2), 192–224.

Hirtenlehner, H. (2011). The Origins of Punitive Mentalities in late modern Societies. Testing an Expressive Explanatory Model. In H. Kury & E. Shea (Hrsg.), *Punitivity – International developments. Vol. 1: Punitiveness – A global phenomenon?* (S. 27–52). Bochum: Dr. Brockmeyer.

Hirtenlehner, H., & Farrall, S. (2013). Anxieties about modernization, concerns about community, and fear of crime: Testing two related models. *International Criminal Justice Review, 23*(1), 5–24.

Honekamp, W. (2019). Cybercrime: Aktuelle Erscheinungsformen und deren Bekämpfung. In H. J. Lange, T. Model, & M. Wendekamm (Hrsg.), *Zukunft der Polizei – Trends und Strategien* (S. 47–59). Wiesbaden: Springer VS.

Hummelsheim-Doss, D., Hirtenlehner, H., Jackson, J., & Oberwittler, D. (2011). Social insecurities and fear of crime: A cross-national study on the impact of welfare state policies on crime-related anxieties. *European Social Review, 27*(3), 327–345.

Johnson, D. (2009). Anger about crime and support for punitive criminal justice policies. *Punishment & Society, 11,* 51–66.

Karuppannan, J. (2012). Victimization in the cyberspace: patterns and trend. In S. Manacorda (Hrsg.), *Cybercriminality: Finding a balance between freedom and security* (S. 91–106). Milan: ISPAC.

Kemme, S. (2012). *Harsh penalties, deterrence and retribution: Indicators of a growing need of security?* Paper presented at the 12th Annual Conference of the European Society of Criminology, Bilbao, Spain (12.–15. September 2012).

Kemme, S., & Doering, B. (2015). Viktimisierung und Strafeinstellungen. In N. Guzy, C. Birkel, & R. Mirschkowitz (Hrsg.), *Viktimisierungsbefragungen in Deutschland. Ziele, Nutzen und Forschungsstand Band 1* (S. 543–571). Wiesbaden: Bundeskriminalamt.

Kemme, S., & Hanslmaier, M. (2010). Elterliches Strafen und eigenes Strafbedürfnis: Die Bedeutung frühkindlicher Viktimisierungserfahrung. *Praxis der Rechtspsychologie, 20*(2), 256–277.

Kemme, S., & Hanslmaier, M. (2012). Recht, Strafe und Kriminalität in der öffentlichen Wahrnehmung. In H.-G. Soeffner (Hrsg.), *Transnationale Vergesellschaftungen. Verhandlungen des 35. Kongresses der Deutschen Gesellschaft für Soziologie in Frankfurt am Main 2010* (S. 1–16). Wiesbaden: VS Verlag & CD-ROM.

Kemme, S., Hanslmaier, M., & Pfeiffer, C. (2014). Experience of domestic violence in childhood and ado-lescence and its effect on punitiveness. *Journal of Familiy Violence, 29*(2), 129–142.

King, A., & Maruna, S. (2009). Is a conservative just a liberal who has been mugged? Exploring the origins of punitive views. *Punishment & Society, 11,* 147–169.

Kleck, G., & Jackson, D. (2017). Does crime cause punitiveness? *Crime & Delinquency, 63*(12), 1572–1599.

Kreuzer, A. (2018). Kriminalpolitische Kurskorrekturen durch die neue Bundesregierung? Kein Weiter-So mit steten Strafrechtsausweitungen. *Neue Kriminalpolitik, 30*(2), 141–156.

Krischok, H. (2018). Das Internet in der polizeilichen Gefahrenabwehr. In T. G. Rüdiger & P. Bayerl (Hrsg.), *Digitale Polizeiarbeit*. Wiesbaden: Springer VS.

Kühnrich, B., & Kania, H. (2005). *Attitudes towards punishment in the European Union. Results from the 2005 European Crime Survey (ECSS) with focus on Germany.* Freiburg/Breisgau: Max Planck Institute for Foreign and International Criminal Law.

Kury, H., & Ferdinand, T. (1999). Public opinion and punitivity. *International Journal of Law and Psychiatry, 22,* 373–392.

Kury, H., & Würger, M. (1993). Opfererfahrungen und Kriminalitätsfurcht. Ein Beitrag zur Viktimisierungsperspektive. In G. Kaiser & H. Kury (Hrsg.), *Kriminologische Forschung in den 90er Jahren* (S. 411–462). Freiburg: Max-Planck-Institut für ausländisches und internationales Strafrecht.

Kury, H., Obergfell-Fuchs, J., & Würger, M. (2000). *Gemeinde und Kriminalität. Eine Untersuchung in Ost- und Westdeutschland*. Freiburg: Max-Planck-Institut für ausländisches und internationales Strafrecht.

Kury, H., Obergfell-Fuchs, J., & Smartt, U. (2002). The evolution of public attitudes to punishment. In Western and Eastern Europe. In J. Roberts & M. Hough (Hrsg.), *Changing Attitudes to Punishment. Public Opinion, Crime and Justice* (S. 93–114). Cullompton: Willan.

Kury, H., Obergfell-Fuchs, J., & Würger, M. (2002). *Strafeinstellungen. Ein Vergleich zwischen Ost- und Westdeutschland*. Freiburg i. Br.: Max-Planck-Institut für ausländisches und internationales Strafrecht.

Kury, H., Kania, H., & Obergfell-Fuchs, J. (2004). Worüber sprechen wir, wenn wir über Punitivität sprechen? Versuch einer konzeptionellen und empirischen Begriffsbestimmung. *Kriminologisches Journal, 36*(8), 51–88.

Kury, H., & Obergfell-Fuchs, J. (2006). Zur Punitivität in Deutschland. *Soziale Probleme, 17*(2), 119–154.

Langworthy, R. H., & Whitehead, J. T. (1986). Liberalism and fear as explanations of punitiveness. *Criminology, 24*(3), 575–591.

Lautmann, R., & Klimke, D. (2004). Punitivität als Schlüsselbegriff für eine kritische Kriminologie. In R. Lautmann, D. Klimke, & F. Sack (Hrsg.), *Punitivität. Kriminologisches Journal*, *8. Beiheft* (S. 9–29). Weinheim: Juventa.

Lenhart, A., Ybarra, M., Zickuhr, K., & Price-Feeney, M. (2016). *Online Harassment, Digital Abuse, and Cyberstalking in America*. New York: Data & Society Research Institute.

Mascini, P., & Houtman, D. (2006). Rehabilitation and repression. Reassessing their ideological embeddedness. *British Journal of Criminology, 46,* 822–836.

Pereira, F., Spitzberg, B.H., & Matos, M. (2016). Cyber-harassment victimization in Portugal: Prevalence, fear and help-seeking among adolescents. *Computers in Human Behavior, 62,* 136–146.

Pfeiffer, C., Windzio, M., & Kleimann, M. (2005). Media use and its impact on crime perception, sentencing attitudes and crime policy. *European Journal of Criminology, 2,* 259–285.

Reisig, M. D., Pratt, T. C., & Holtfreter, K. (2009). Perceived risk of internet theft victimization: Examining the Effects of social vulnerability and financial impulsivity. *Criminal Justice and Behavior, 36*(4), 369–384.

Reuband, K. (2010). Einstellungen der Bevölkerung gegenüber jugendlichen Straftätern. Eine empirische Analyse ihrer Erscheinungsformen und Determinanten. In B. Dollinger & H. Schmidt-Semisch (Hrsg.), *Handbuch Jugendkriminalität. Kriminologie und Sozialpädagogik im Dialog* (S. 507–531). Wiesbaden: Springer Verlag für Sozialwissenschaften.

Roberts, L. D., Indermaur, D., & Spiranovic, C. (2013). Fear of cyber-identity theft and related fraudulent activity. *Psychiatry. Psychology and Law, 20*(3), 315–328.

Schwarzenegger, C. (1992). *Die Einstellung der Bevölkerung zur Kriminalität und Verbrechenskontrolle*. Freiburg im Br.: Max-Planck-Institut für ausländisches und internationales Strafrecht.

Simonson, J. (2009). Punitivität: Methodische und konzeptionelle Überlegungen zu einem viel verwendeten Begriff. *Zeitschrift für Jugendkriminalrecht und Jugendhilfe, 20,* 30–37.

Skogan, W. G. (1993). The various meanings of fear. In W. Bilsky, C. Pfeiffer, & P. Wetzels (Hrsg.), *Fear of crime and criminal victimisation* (S. 131–140). Stuttgart: Enke.

Taylor, D. G., Scheppele, K. L., & Stinchcombe, A. (1979). Salience of crime and support for harsher criminal sanctions. *Social Problems, 26*(4), 413–424.

Tseloni, A., & Zarafonitou, C. (2008). Fear of crime and victimisation: A multivariate multilevel analysis of competing measurements. *European Journal of Criminology, 5,* 387–409.

Tyler, T. R., & Boeckman, R. J. (1997). Three strikes and you are out, but why? *Law and Society Review, 31*(2), 237–266.

Tyler, T., & Weber, R. (1982). Support for the death penalty. Instrumental response to crime or symbolic attitude? *Law & Society Review, 17,* 21–45.

Urban, D., & Mayerl, J. (2006). *Regressionsanalyse: Theorie, Technik und Anwendung*. Wiesbaden: Springer VS.

Van Kersteren, J. (2009). Public attitudes and sentencing policies across the world. *European Journal on Criminal Policy and Research, 15,* 26–46.

Virtanen, S. M. (2017). Fear of cybercrime in Europe: Examining the effects of victimization and vulnerabilities, psychiatry. *Psychology and Law, 24*(3), 323–338.

Vozmediano, L., San-Juan, C., Vergara, A. I., & Lenneis, A. (2013). Risk perception in digital contexts: Questionnaire and pilot study. *International E-journal of Criminal Sciences, 7*(4), 1–18.

Wetzels, P., Enzmann, D., Mecklenburg, E., & Pfeiffer, C. (2001). *Jugend und Gewalt. Eine repräsentative Dunkelfeldanalyse in München und acht anderen deutschen Städten*. Baden-Baden: Nomos.

Wetzels, P., Greve, W., Mecklenburg, E., Bilsky, W., & Pfeiffer C. (1995). *Kriminalität im Leben alter Menschen*. Stuttgart: Kohlhammer.

Windzio, M., Simonson, S., Pfeiffer, C., & Kleimann, M. (2007). *Kriminalitätswahrnehmung und Punitivität in der Bevölkerung – Welche Rolle spielen die Massenmedien? Ergebnisse der Befragungen zu Kriminalitätswahrnehmung und Strafeinstellungen 2004 und 2006*. Hannover: KFN.

Wynterdyk, J., & Hincks, C. (2013). Fear of crime and punitivity: A Canadian overview. In H. Kury & J. Winterdyk (Hrsg.), *Fear of crime and punitiveness – Results from international student surveys* (S. 21–38). Bochum: Universitätsverlag Dr. Brockmeyer.

Yu, S. (2014). Fear of cyber crime among college students in the United States: An exploratory study. *International Journal of Cyber Criminology, 8*(1), 36–46.

Digitaler Vigilantismus

Kerrin-Sina Arfsten

1 Einleitung

Immer öfter scheinen Privatpersonen in den letzten Jahren auf eigene Faust Fahndungsaufrufe im Netz und in den Sozialen Medien[1] zu veröffentlichen oder abweichendes Verhalten anderer zu ahnden, indem sie die Personen öffentlich anprangern, bloßstellen, oder ihnen gar Gewalt androhen. Besonders spektakuläre Fälle generieren mediale Aufmerksamkeit und gelangen so ins öffentliche Bewusstsein. Andere Fälle bleiben in ihrer Sichtbarkeit für die breite

[1] „Soziale Medien" sind „onlinebasierte Programme, die eine Kommunikation oder Interaktion der Nutzer untereinander ermöglichen" (Rüdiger 2017, S. 214; siehe auch Milivojevic und McGovern 2014, S. 24; Salter 2017, S. 14; Sallavaci 2018, S. 3). Mit dem Aufkommen der sog. „Sozialen Medien" seit Anfang der 2000er Jahre hat sich die Kommunikation online stark verändert: sie ist seither interaktiver und kollaborativer geworden (Stratton et al. 2016, S. 21). Soziale Medien sind stark partizipativ ausgerichtet und unterscheiden sich von den „traditionellen" Medien dadurch, dass Inhalte nicht hierarchisch von einigen, wenigen AutorInnen an ein breites Publikum kommuniziert werden, welches diese passiv konsumiert (Powell 2015, S. 573). Stattdessen können in den „Sozialen Medien" Inhalte jederzeit von jedermann erstellt und an ein ebenso breites Spektrum an Empfängern vermittelt werden. Diese wiederum können mit den Inhalten interagieren und sie,

Ich danke Prof. Dr. Dr. h.c. mult. Hans-Jörg Albrecht, Max-Planck-Institut für ausländisches und internationales Strafrecht, für seine konstruktive Kritik und weiterführenden Anmerkungen zu einem ersten Entwurf dieses Kapitels.

K.-S. Arfsten (✉)
Freiburg i.Br., Deutschland

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

T.-G. Rüdiger und P. S. Bayerl (Hrsg.), *Cyberkriminologie,*
https://doi.org/10.1007/978-3-658-28507-4_22

Öffentlichkeit begrenzt. Offizielle Statistiken zu diesem Phänomen gibt es nicht – Selbstjustiz an sich ist kein eigenständiges, strafbewehrtes Delikt. Lediglich mit dem Phänomen in Zusammenhang stehende Handlungen, wie z. B. ein öffentlicher Aufruf zur Körperverletzung, das Veröffentlichen von Gewaltdarstellungen oder das Veröffentlichen eines Fotos einer Person ohne deren Erlaubnis, sind (straf-)rechtlich relevant. Kriminalstatistiken können daher zur Bestimmung des Umfangs des Phänomens nur wenig beitragen. Vor zwei Jahren stellte der Kriminologe Thomas-Gabriel Rüdiger (2017, S. 227) jedoch fest: *„Selbstjustiz-Handlungen im Internet sind ein so relevantes Phänomen, dass es bereits zu Aufrufen gegen Selbstjustiz im Internet kommt“*. Der SPIEGEL Blogger Sascha Lobo (2019) widmete dem Phänomen jüngst einen eigenen Podcast und auch im Abendprogramm des öffentlich-rechtlichen Fernsehens ist das Thema bereits angekommen: So strahlte die ARD im November 2018 eine Folge der populären Fernsehsendung *Tatort* aus, in der wütende BürgerInnen Fotos und Adressen der in einem Mordfall ermittelnden Kommissare in den Sozialen Medien publizierten, um gegen diese online zu hetzen und sie unter Druck zu setzen.

Mit dem Begriff der „Selbstjustiz“ werden umgangssprachlich Situationen erfasst, in denen private Akteure „das Recht in die eigenen Hände nehmen [und] eigenmächtig Gewalt gegenüber Dritten anwenden, um gegen diese vorzugehen oder um eigene Anliegen durchzusetzen“ (Schmidt-Lux 2013, S. 99). In Verbindung mit dem Internet wird Selbstjustiz auch als „digitaler Vigilantismus“ bzw. „Digilantismus“ (Martin 2007; Byrne 2013), „Cyber-Vigilantismus“ (Altheide 2004; Smallridge et al. 2016), „elektronischer Vigilantismus“ (Katyal 2001), „virtueller Vigilantismus“ (Dennis 2008), „mobiler Vigilantismus“ (Morozov 2009) oder „Online-Vigilantismus“ (Salter 2017; Myles und Trottier 2017) bezeichnet. Ein weiterer in der Literatur verwendeter Begriff ist „Netilantismus“ – ein Neologismus aus den Worten „Internet“ und „Vigilantismus“ (Chang und

z. B. redigieren oder kommentieren. Nutzer werden zu dem was Salter (2017, S. 228) als „consumer-producers“ bezeichnet. Die prominentesten Beispiele Sozialer Medien sind sog. „social networking“-Seiten wie Facebook oder Instagram und Seiten, deren Inhalte von den Nutzern selbst generiert werden, wie YouTube oder Wikipedia (Van Dijk 2013, S. 8; Sallavaci 2018, S. 3). Im Zusammenhang mit der Entwicklung und Verbreitung Sozialer Medien hat sich nicht nur die Art und Weise verändert, wie Wissen über Kriminalität und abweichendes Verhalten produziert und vermittelt wird; auch die Möglichkeiten für Empfänger dieses Wissen zu rezipieren haben sich verändert. Neue Möglichkeiten der kollektiven Bedeutungszuschreibung sind entstanden (vgl. Powell et al. 2018).

Poon 2017). Diese Bezeichnungen sind allerdings umstritten (vgl. bspw. Yardley et al. 2018, S. 84; Salter 2017, S. 27).[2] Allein die Vielfalt an Begrifflichkeiten zeigt jedoch, dass das Phänomen nicht leicht zu konzeptualisieren ist. Was sich hinter diesen Begriffen verbirgt, bleibt bislang vage: *„While much has been written on vigilantism in offline contexts, there is little scholarly coverage of similar practices in online domains"* (Jane 2017, S. 3; siehe auch Arvanitidis 2016, S. 19; Dunsby und Howes 2019, S. 2). Der Stand der Forschung zu Selbstjustiz im Internet oder unter Verwendung Sozialer Medien ist gering, insbesondere auch aus kriminologischer Sicht (vgl. auch Stratton et al. 2016, S. 18; Yardley et al. 2018, S. 81; Powell et al. 2018, S. 141 ff.). Zudem gibt es noch keine fundierten, empirischen Studien zu dem Phänomen im deutschsprachigen Raum. Die wenigen wissenschaftlichen Beiträge, die es gibt, stammen aus China (z. B. Skoric et al. 2010; Chang und Poon 2017), Australien (z. B. Milivojevic und McGovern 2014; Jane 2017; Salter 2017; Powell et al. 2018), Kanada (z. B. Schneider und Trottier 2012; Trottier 2017; Myles und Trottier 2017) und den USA (z. B. Powell 2015; Lally 2017; Nhan et al. 2017).

Die Entwicklung neuer, sozialer Technologien verändert Formen der Kommunikation und Interaktion; Wissensbestände werden anders vermittelt; neue

[2]Problematisiert werden in der Literatur insbesondere solche definitorischen Ansätze, die versuchen, eine Dichotomie zwischen „virtueller" und „realer", „online" und „offline" Welt aufrechtzuerhalten. Eine solche Unterscheidung gilt als überholt (Powell et al. 2018, S. 7 f.; vgl. auch Stalder 2017). Walls und Williams (2007, S. 395) beispielsweise argumentieren, dass empirische Studien bereits mehrfach gezeigt haben, dass Nutzer verschiedener online Dienste ihre Erfahrungen nicht als „virtuell" oder getrennt von ihren „echten" Lebenswelten wahrnehmen. Zudem seien online Phänomene intrinsisch mit kulturellen und sozialen Prozessen offline verbunden (Walls und Williams 2007, S. 396). Eine Trennung von „online" und „offline" bei der Konzeption digitaler Phänomene decke sich daher nicht mit der Praxis und sei wenig ertragreich. Auch Salter (2017, S. 27) zeigt auf, dass Präfixe wie „virtuell" oder „cyber" weder einem besseren Verständnis der zu beschreibenden technosozialen Phänomene, noch dem besseren Verständnis ihrer Auswirkungen auf die Wahrnehmungen und Erfahrungen von Nutzern zuträglich sind. Stattdessen suggerierten sie die Existenz einer Art parallelen Realität und trivialisierten damit Ereignisse, die online geschehen. Stratton et al. (2016, S. 22) vertreten eine ähnliche Ansicht. Yardley et al. (2018, S. 84) hingegen problematisieren die Verwendung des Begriffs „Vigilantismus" um das Phänomen im techno-sozialen Kontext zu beschreiben, denn dieser beziehe sich auf eine sehr limitierte und spezifische Art von Aktivitäten. Sie postulieren die Notwendigkeit, eine neue Begrifflichkeit für die Fälle zu finden, in denen nichtstaatliche Akteure sich quasi-polizeilich im Netz betätigen und versuchen TäterInnen auf eigene Faust zu überführen.

Foren für die Austragung sozialer Konflikte sowie die Aushandlung sich wandelnder gesellschaftlicher Werte und Normen entstehen. Wie diese Technologien die Wahrnehmung und Bedeutung abweichenden Verhaltens, sowie den alltäglichen Umgang mit Abweichung, prägen, ist daher eine zentrale Frage für eine digital ausgerichtete Kriminologie. Ziel des vorliegenden Kapitels ist es, Elemente für einen theoretischen Ansatz herauszuarbeiten, der ein besseres Verständnis des Phänomens des Vigilantismus im digitalen Kontext ermöglicht. Welche Fälle werden unter der diskursiven Rahmung eines „digitalen Vigilantismus" öffentlich diskutiert? In medialen und wissenschaftlichen Diskursen wird dem Phänomen eine wachsende gesellschaftliche Bedeutung zugeschrieben (vgl. Salter 2017; Nhan et al. 2017; Powell et al. 2018); doch handelt es sich tatsächlich um ein relativ „neues" Phänomen, wie es z. B. Arvanitidis (2016, S. 19) postuliert? Gibt es Unterschiede zwischen Selbstjustiz in der „realen" und der „digitalen" Welt, zwischen „Vigilantismus" und „Digilantismus"? Kurzum, wie stellt sich Selbstjustiz im techno-sozialen Kontext dar? Welche Erklärungen für das Entstehen digilanter Gewalt im Internet werden offeriert? Und welche Legitimationsmuster lassen sich identifizieren, d. h., wie rechtfertigen digilante Akteure ihre Handlungen?

Meine Überlegungen in diesem Beitrag stützen sich auf direktes Wissen aus der Forschungsliteratur und auf indirektes Wissen aus der Medienberichterstattung. Letzteres nutze ich in Form von Fallbeispielen, welche ich zur Illustration verschiedener Aspekte heranziehe. Beginnen möchte ich mit einer kurzen Vorstellung konzeptioneller Ansätze zum klassischen Vigilantismus. Von diesen Ansätzen werde ich dann den digitalen Vigilantismus (im Folgenden auch „Digilantismus" genannt) abgrenzen, in dem ich einige Kernelemente problematisiere und zur Diskussion stelle.

2 Was ist Vigilantismus?

Bevor sich der Rest des Kapitels mit den Unterschieden zwischen Vigilantismus und Digilantismus beschäftigt, möchte ich zunächst einmal klären, was der Begriff des „Vigilantismus" überhaupt bedeutet und wie das Phänomen klassischerweise konzeptioniert wird. Das Wort „Vigilantismus" geht zurück auf das lateinische Wort *vigilare,* welches „wachsam sein" bedeutet (Abrahams 1998, S. 4). In der Kriminologie, sowie in den Sozialwissenschaften generell, ist der Begriff des „Vigilantismus" umstritten, denn er bezeichnet ein konzeptionell nur schwer zu greifendes Phänomen: zu vielseitig erscheinen seine konkreten Ausprägungen; zu unterschiedlich erscheinen Akteure, Aktivitäten, Motive, Organisationsformen, Strategien, Entstehungsbedingungen und gesellschaftliche

Auswirkungen (Powell et al. 2018, S. 139 ff.; vgl. auch Johnston 1996; Abrahams 1998). Im Deutschen wird der Begriff des „Vigilantismus“ zudem eher selten verwendet; wie bereits erwähnt, wird im Alltag eher von „Selbstjustiz“ gesprochen (Schmidt-Lux 2018, S. 146).[3]

Vigilantismus ist ein Phänomen, bei dem es in erster Linie um soziale Kontrolle und die Schaffung bzw. Erhaltung von sozialer Ordnung geht. Der Kulturwissenschaftler Thomas Schmidt-Lux (2013, S. 100) definiert klassischen „Vigilantismus“ als die *„gewaltsame bzw. unter Androhung von Gewalt erfolgende Bestrafung, Erzwingung oder Verhinderung eines abgelehnten bzw. erwünschten Handelns Anderer durch nicht-staatliche bzw. private Akteure“. Er schreibt, vigilanten Akteuren gehe es „immer um das Verhalten Anderer […], das aus ihrer Perspektive als ‚abweichend‘ zu verurteilen, zu verhindern oder zu bestrafen ist.“* (Schmidt-Lux 2013, S. 100; siehe auch Johnston 1996, S. 229; Kowalewski 2002, S. 426).

Vigilante Aktivitäten richten sich demnach gegen jene Personen, die sich nicht an die in einer Gemeinschaft vereinbarten und festgelegten, sowie als legitim erachteten Regeln halten (vgl. Hitzler 1993). Dabei stehen das Bestrafen bzw. der Wunsch, Gerechtigkeit für ein wahrgenommenes Unrecht zu erwirken immer im Vordergrund vigilanter Aktivitäten (Schmidt-Lux 2018, S. 152). Eine vigilante Tat soll etwas wieder in Ordnung oder in ein Gleichgewicht bringen, was durch ein Unrecht aus der Balance geraten zu sein scheint (Schmidt-Lux 2018, S. 152). Es geht vigilanten Akteuren also nicht darum, grundlegende strukturelle und gesellschaftliche Veränderungen herbeizuführen, sondern einen bestimmten Status quo wiederherzustellen und aufrechtzuerhalten (Quent 2016a, S. 14). Klassischer Vigilantismus ist in diesem Sinn systemstabilisierend: eine „alte“ Ordnung soll verteidigt werden (Quent 2016b).

Mit seiner Konzeption greift Schmidt-Lux Elemente der in der Literatur wohl am häufigsten zitierten und verwendeten Definition von Vigilantismus auf. Diese entstammt dem Aufsatz *What is Vigilantism?* des britischen Soziologen Les Johnston (1996). In diesem Aufsatz schlägt Johnston eine kriminologische Definition von Vigilantismus vor, die mehrere Kernelemente beinhaltet. Für Johnston (1996, S. 232 ff.) zeichnen sich vigilante Bewegungen dadurch aus, dass 1) sie ein

[3]Manche Vigilantismus-Forscher unterscheiden zwischen „Selbstjustiz“ und „Vigilantismus“ (vgl. z. B. Johnston 1996; Quent 2016b). Sie sprechen von „Selbstjustiz“ in Bezug auf Handlungen einzelner Personen und von „Vigilantismus“, wenn es um Bürgerwehren mit einem gewissen Grad an Organisiertheit geht.

Minimum an Planung und einen gewissen Grad an Organisiertheit aufweisen; 2) die vigilanten Akteure freiwillig und unabhängig vom Staat und seinen Institutionen agieren; 3) vigilante Aktivitäten autonom, d. h. ohne (implizite oder explizite) staatliche Unterstützung erfolgen; 4) vigilante Aktivitäten eine Reaktion auf (tatsächliche, wahrgenommene oder antizipierte) Kriminalität und/oder sozial abweichendes Verhalten darstellen; und 5) das Ziel, welches vigilante Akteure mit ihren Taten zu erreichen versuchen, die Wiederherstellung bzw. der Schutz einer sozialen Ordnung und/oder der Ausgleich eines wahrgenommenen Sicherheitsdefizits ist.

Zwei Aspekte von Johnstons Definition des konventionellen Vigilantismus sind noch besonders hervorzuheben. Zum einen ist anzumerken, dass Johnston (1996, S. 232, 233) es – im Gegensatz zu beispielsweise Haas (2010), Moncada (2017) und e Silva (2018) – nicht für zwingend notwendig erachtet, dass die auslösenden Taten illegal sind. Seine Definition ist weiter und erfasst auch verschiedene, lediglich als „abweichend“ zu klassifizierende Verhaltensweisen. Einer vigilanten Tat muss somit kein Rechtsbruch vorausgehen (Johnston 1996, S. 222). Zum anderen müssen vigilante Aktivitäten aus Johnstons Sicht auch selbst nicht zwingend illegal sein. Für Juliano (2012, S. 46) gilt: *„To be a vigilante, one must break the law“*. Nur solche Aktivitäten, die gegen geltende Gesetze verstoßen, fallen für sie unter den Begriff des Vigilantismus. Johnston (1996, S. 227) hingegen nimmt eine derartige Abgrenzung nicht vor. So reicht für ihn die bloße Androhung von Gewalt aus – es muss beispielsweise nicht zu einer tatsächlichen Körperverletzung kommen (siehe auch Quent 2016a, S. 14; Moncada 2017, S. 408).

3 Fallbeispiele eines digitalen Vigilantismus („Digilantismus“)

Der kurzen Vorstellung theoretischer Ansätze zur Konzeptionierung von klassischem Vigilantismus, möchte ich nun drei Fälle gegenüberstellen, die in jüngerer Zeit in den deutschsprachigen Medien Erwähnung gefunden haben und unter dem Begriff der digitalen „Selbstjustiz“ thematisiert wurden. Ich habe sie ausgewählt, weil sie das Phänomen illustrieren, welches hier als „digitaler Vigilantismus“ bzw. „Digilantismus“ erörtert werden soll, und zeigen, wie unterschiedlich es in seinen konkreten Ausprägungen sein kann. Die Fälle stellen somit eine gute Hinführung zum Thema dar, die zugleich auf seine Komplexität hinweist.

Das erste Beispiel ist der Fall Ariane Friedrich. Im April 2012 schickte ein Mann der deutschen Rekordhalterin im Hochsprung ein Foto seines Geschlechtsteils. Friedrich wehrte sich gegen die sexuelle Belästigung, indem sie die (vermeintliche) Identität des Mannes auf Facebook veröffentlichte:

> „Liebe Followers, eben erreichte mich folgende Facebookmail: Thorsten D., wohnhaft in A. schrieb: ‚Willst du mal einen schönen Schw*** sehen. Gerade geduscht und frisch rasiert'. Zusätzlich hat er noch eine Datei mitgeschickt, die ich nicht öffnen werde. NEIN HERR D., ich möchte weder Ihr Geschlechtsteil, noch die Geschlechtsteile anderer Fans sehen. Anzeige folgt." (zitiert in Jüttner 2012)

In Zeitungsinterviews erklärte sie später, sie habe jahrelang Belästigungen dieser Form ertragen müssen (vgl. DIE ZEIT 2013). Jetzt habe sie eine Grenze aufzeigen wollen. Durch das *„Herausnehmen aus der Anonymität"* habe sie verdeutlichen wollen, dass sie bereit sei, *„aktiv zu handeln, und dass ich eben nicht mehr solche Sachen überlese und mich im Stillen mehr als darüber ärgere"* (zitiert in Hungermann 2012).

Noch im selben Jahr erregte ein weiterer Fall die öffentlichen Gemüter: Nach dem gewaltsamen Tod eines elfjährigen Mädchens im niedersächsischen Emden verhaftete die Polizei wenig später einen siebzehnjährigen Verdächtigen. Nachbarn fotografierten die Festnahme und verbreiteten das Bild des vermeintlichen „Kindermörders" über das Internet. Ein junger Mann postete bei Facebook: *„Aufstand! Alle zu den Bullen! Da stürmen wir! Lasst uns das Schwein tot hauen!"* (zitiert in Thissen 2012). 33 Leute klickten den „Gefällt mir"-Button (Thissen 2012). Auch in der „realen" Welt hatte der Aufruf Konsequenzen. In der Folge versammelte sich ein wütender Mob von etwa 50 Personen vor dem Emdener Polizeikommissariat. Sie skandierten *„Hängt ihn auf, steinigt ihn!"* und forderten die Herausgabe des „Täters" (Thissen 2012; Saliger 2013). Der verdächtigte Junge stellte sich später als völlig unschuldig heraus. Eine Woche nach Entdeckung der Leiche nahm die Polizei den wahren Täter fest (Saliger 2013).

Ein drittes Beispiel stammt aus Hamburg. Dort fand im Juli 2017 der G20-Gipfel statt. Im Umfeld der Veranstaltung kam es zu massiven Ausschreitungen. Um Randalierer schneller identifizieren zu können, richtete die Polizei Hamburg zusammen mit dem Bundeskriminalamt (BKA) ein Hinweisportal ein, über welches eigene, noch nicht veröffentlichte Fotos und Videos von Straftaten anonym oder namentlich gekennzeichnet hochgeladen werden konnten (Krempl 2017). Zeitgleich starteten Privatpersonen eine eigene „Internet-Fahndung." Im Zuge dieser privaten Fahndung kam es zu Falschmeldungen. Mindestens eine unschuldige Person wurde öffentlich verdächtigt, einen Polizisten schwer verletzt zu haben (Krempl 2017). Ein großformatiges Bild des Mannes mit unverpixeltem Gesicht verbreitete sich in den Sozialen Medien. Unter dem Bild wurde die Bevölkerung dazu aufgerufen, den Mann zu lokalisieren, damit er seiner gerechten Strafe zugeführt werden kann: *„Das ist der ‚Demonstrant', der mit einem Böller einem Polizisten fast das Augenlicht nahm. Findet ihn! Bitte teilen"* (zitiert in Krempl 2017).

4 Öffentlichkeit als Mittel zur Selbstverteidigung

So unterschiedlich diese drei Fälle in ihren Details auch sein mögen, sie teilen zwei Gemeinsamkeiten. Erstens, wie bereits erwähnt, verbindet die soeben angeführten Fälle ihre diskursive Rahmung in den Medien als Fälle von Selbstjustiz. Zweitens nutzten in allen drei Fällen private, nichtstaatliche Akteure die kommunikativen Möglichkeiten des Internets – und insbesondere der Sozialen Medien, um tatsächliche oder wahrgenommene Devianz Anderer publik zu machen und die vermeintlichen TäterInnen über diesen Prozess der Sichtbarmachung von einem spezifischen Handeln abzuhalten oder sie dafür zu bestrafen. Um sich selbst oder andere Personen vor dem schädigenden Verhalten anderer zu schützen, nutzten die vigilanten Akteure die Sozialen Medien, um eine über den situativ-lokalen Kontext hinausgehende Aufmerksamkeit zu generieren, die den oder die vermeintliche TäterIn dem verurteilenden Blick eines mehr oder weniger anonymen Publikums zuführte. Das Publizieren der zu ahndenden Taten bzw. TäterInnen folgte dabei einer denunziatorischen bzw. akkusatorischen Logik. Die resultierende Sichtbarkeit wiederrum sollte garantieren, dass eine entstandene Schädigung auch tatsächlich (formell oder informell) geahndet wird oder zumindest Betroffenheit und Empathie aufseiten der Öffentlichkeit hervorruft. Die auslösenden Taten variieren zwischen den Fällen, aber stets erscheint die vigilante Handlung als eine Reaktion auf ein wahrgenommenes Unrecht, welches es auf diese Weise auszugleichen bzw. vor dem es sich zu schützen gilt (siehe auch Trottier 2017). Der Wunsch über eine gezielt hergestellte Sichtbarkeit eine informelle Ahndung des/der TäterIn zu erwirken, ist im Prinzip nichts Neues. Die drei Fälle zeigen jedoch, dass sich unter den Bedingungen der Sozialen Medien die Steuerbarkeit und Nachhaltigkeit dieser Sichtbarkeit verändert (darauf, wie sie sich verändert, gehe ich noch genauer in Abschn. 5.5 ein).

Aufgrund der Ähnlichkeit, die diese Art von Vorkommnissen mit klassischen Formen des Vigilantismus aufweist (nichtstaatliche Akteure, die das „Recht in die eigene Hand nehmen“, um ein falsches Verhalten anderer Personen zu ahnden) und der zentralen Rolle, die das Internet bzw. die Sozialen Medien spielen, wird in der einschlägigen Literatur regelmäßig der Begriff des „digitalen Vigilantismus“ verwendet, um sie zu beschreiben (vgl. Byrne 2013; Trottier 2017; Jane 2017; Dunsby und Howes 2019; Powell et al. 2018). Unter dem Begriff des „digitalen Vigilantismus“ versteht Trottier (2017, S. 55) einen Prozess *„where citizens are collectively offended by other citizen activity, and respond through coordinated retaliation on digital media“*. Dunsby und Howes (2019, S. 2) beschreiben digitalen Vigilantismus als *„a citizen's reaction to another person's transgression of social norms in the online space“*. Jane (2017, S. 3) beschreibt das Phänomen

kurz und bündig als *„do-it-yourself attempts to secure justice online“,* und für Powell (2015, S. 579) ist es *„technology-mediated informal justice“*. Gemeinsam ist den genannten Definitionen ein zugrunde liegendes Verständnis von digitalem Vigilantismus als eine Form der Ausübung informeller Sozialkontrolle bzw. Suche nach „Gerechtigkeit“ in und unter Verwendung Sozialer Medien – und hier insbesondere der durch sie offerierten Möglichkeit eine gezielte Öffentlichkeit zu generieren. In diesem Sinn verwende ich den Begriff des „digitalen Vigilantismus“ im Folgenden.

Gleichzeitig möchte ich an dieser Stelle jedoch darauf hinweisen, dass es bislang keine einheitliche Definition von „digitalem Vigilantismus“ gibt (vgl. Powell et al. 2018). Zudem existieren noch andere Ansätze, die im vorliegenden Kapitel diskutierten Fälle von Selbstjustiz im Internet zu konzeptualisieren. So werden sie, u. a., auch als „civilian policing“ (vgl. Schneider und Trottier 2012); „citizen-initiated cyber-policing“ bzw. „digital paedophile hunting“ (Campbell 2015); „websleuthing“ (vgl. Yardley et al. 2018); oder „(feminist) digital activism“ (Jane 2017) besprochen – je nachdem in welchem spezifischen Kontext sich das Phänomen manifestiert und welche konkreten Aktivitäten es umfasst. Hinzu kommt, dass manche AutorInnen unter „digitalem Vigilantismus“ nur solche Selbstjustizhandlungen verstehen, die sich vollständig online abspielen, d. h. als eine digitale Reaktion auf eine digitale Tat. Bei ihnen geht es z. B. um Fälle von hacktivism (s. a. Kap. „Phänomenologie von digitalen Delikten“) oder scambaiting (vgl. Katyal 2001; Jane 2017; e Silva 2018) oder auch um digitale Selbstjustiz zwischen Staaten (s. a. Kap. „Wie Cyberterrorismus stattfindet – und warum wir ihn nicht sehen“). Diese Fälle, die sich gewissermaßen online/online ereignen, diskutiere ich hier nicht. Sie haben m. E. eine andere Qualität und folgen einer anderen Logik als die sozio-technischen, online/offline Phänomene, die sich zwischen privaten BürgerInnen abspielen und Gegenstand dieses Kapitels sind.

5 Elemente des Digilantismus

Nachdem ich das Phänomen des Digilantismus nun beispielhaft dargestellt und kurz definitorisch umrissen habe, möchte ich in den folgenden Abschnitten einigen Gemeinsamkeiten und Unterschieden zwischen konventionellem und digitalem Vigilantismus nachgehen. Ich orientiere mich dabei an den von Johnston (1996) vorgeschlagenen Kernelementen des klassischen Vigilantismus. Mein Augenmerk liegt dabei auf jenen Elementen, die im Kontext eines digitalen Vigilantismus zu problematisieren und überdenken sind. Auf diese Weise möchte ich versuchen, die oben genannten Definitionen weiter auszudifferenzieren.

Allerdings möchte ich anmerken, dass sich das Phänomen des Vigilantismus auch im soziotechnischen Kontext vielschichtig und facettenreich präsentiert. Jeder Versuch, ein komplexes gesellschaftliches Phänomen in eine Definition zu übersetzen, stellt immer eine Form von Reduktion dar, die sich darauf beschränkt, idealtypische Muster und Merkmale abzubilden. Abweichungen von einer Definition bedeuten deshalb nicht zwangsweise, dass sie nicht tragfähig ist. Sie besagen vielmehr, dass gesellschaftliche Realitäten sich stets zu einem gewissen Grad einer ordnenden – und damit auch limitierenden bzw. eine Bedeutung fixierenden – Sprache entziehen. Die folgenden Aspekte stellen in diesem Sinn Elemente verschiedener Spielarten von digitalem Vigilantismus dar, die in einem konkreten Fall zu beobachten sein können, es aber nicht müssen. In Bezug auf konventionellen Vigilantismus konstatieren Pratten und Sen (2008, S. 19): *„Vigilantism is a shifting concept that articulates to ever-changing social realities“*. Diese Beobachtung trifft ebenso für das Konzept des digitalen Vigilantismus zu. Letztendlich muss ein bestimmter Fall von Digilantismus immer in seinem spezifischen Kontext und somit in seiner Singularität, d. h. in seiner spezifischen Konstellation von Akteuren, Aktivitäten, Motiven, etc., betrachtet werden.

5.1 Auslösende Taten

Vigilantismus und Digilantismus geht immer eine auslösende Tat voraus, die gegen eine – formelle oder informelle – Norm verstößt (vgl. Haas 2010; Moncada 2017). Sowohl vigilante als auch digilante Akteure reagieren mit ihrem Handeln auf eine als bedrohlich wahrgenommene Situation der Gefährdung oder Belästigung (Hitzler 1993, S. 16) oder auf wahrgenommenes Unrecht (vgl. Johnston 1996; Schmidt-Lux 2013, 2018). Sie handeln aus ihrer Sicht nicht initiativ, sondern bewerten ihre Handlungen als rein reaktiv (Schmidt-Lux 2018, S. 152). Hierbei ist es unwesentlich, ob die auslösende Tat online oder offline stattgefunden hat. Auch die Schwere der Tat ist nicht maßgeblich. Auslöser für digilante Aktivitäten können simple Verstöße gegen soziale Gepflogenheiten (z. B. Falschparken, das Nicht-entfernen von Hundekot oder das Twittern eines politisch nicht korrekten Witzes, vgl. Kohm 2009; Clune 2013; Ronson 2015a, b), aber auch Kindesmissbrauch oder die Teilnahme an gewalttätigen Auseinandersetzungen im Rahmen von Demonstrationen sein (vgl. Campbell 2015; Trottier 2017). In manchen Fällen kommt es zu digitalem Vigilantismus als Reaktion auf lediglich moralisch fragwürdiges oder sozial unerwünschtes Verhalten und in anderen Fällen als Reaktion auf tatsächlich strafbares Verhalten (vgl. Skoric et al. 2010; Moncada 2017). *„[A]ny public (and sometimes private) behavior is open*

to published scrutiny", schreibt Martin (2007, S. 124). Eine ganze Reihe von begründeten oder unbegründeten Missständen kann zum Auslöser für digilante Aktivitäten werden und jeder scheint „fair game" zu sein (Clune 2013). Clune (2013) stellt fest: *„There are thousands of Facebook pages and many stand-alone websites dedicated to accusing people of just about anything you care to think about."* Denn gerade weil es (fast) nichts kostet, sind solche Webseiten schnell eingerichtet. Sie lassen sich außerdem relativ leicht, ohne viel Aufwand, betreiben.

Was die auslösenden Taten zu verbinden scheint ist, dass sie in ihrem jeweils spezifischen Kontext eine besondere emotionale Wirkung entfalten. Ereignisse, die digilante Aktivitäten nach sich ziehen, scheinen zum einen solche zu sein, die mit einem Begriff von Innes (2004) als sog. „signal crimes" bezeichnet werden können (vgl. auch Warren 2009). Sie sind Schlüsselereignisse, denen eine Warnwirkung und damit eine übergeordnete gesellschaftliche Bedeutung zugesprochen wird, die über den Kreis unmittelbar betroffener Personen (Täter, Opfer, Zeugen) hinausgeht. Diese Warnwirkung ergibt sich daraus, dass die Ereignisse symbolhaft für eine Schieflage in der Gesellschaft insgesamt zu stehen scheinen. Dies ist selbst dann der Fall, wenn es sich um eigentlich singuläre Vorkommnisse handelt (vgl. Hitzler 1993; Kaiser 2002). Warren (2009, S. 275) beobachtet hierzu: *„it appears ‚vigilantism' is a pertinent signifier of public anxiety over the timing, location and antecedents of some serious violent crimes".* Zudem scheinen auslösende Taten im Zusammenhang mit Digilantismus solche zu sein, bei denen sich die Bevölkerung besonders leicht mit einem Opfer identifizieren kann (Shotland 1976, S. 31 ff.; Powell et al. 2018, S. 11). Hier handelt es sich um Fälle, bei denen der Eindruck entsteht, es hätte einen auch selbst oder eine Person, die einem nahesteht, treffen können. Das Opfer scheint zufällig ausgewählt worden zu sein und/oder wird als so „normal" wahrgenommen, dass es auch, beispielsweise, die eigene Tochter, Freundin, oder Ehefrau hätte sein können (Milivojevic und McGovern 2014, S. 27, 33). Relativität („relatability") ist das entscheidende Stichwort. Eine gewisse räumliche Nähe („proximity") zur auslösenden Tat scheint ein weiterer Faktor zu sein, der emotionalisierend wirken und somit eine Rolle beim Entstehen von Digilantismus spielen kann (vgl. Yardley et al. 2018, S. 97). Und schließlich ist noch an solche Ereignisse zu denken, die stark affektiv mobilisieren, in dem sie Gefühle hervorrufen, die sich mit kulturellen Labels wie Wut, Angst oder Trauer aber auch Empathie oder Hilflosigkeit beschreiben lassen (vgl. Jane 2017; Powell et al. 2018).

Der junge Mann, der in Emden 2012 dazu aufrief, die Polizeiwache zu stürmen, in der sich der vermeintliche Mörder eines elfjährigen Mädchens befand, sagte in seiner Vernehmung bei der Polizei später aus, *„der Tod des Mädchens*

habe ihn emotional stark berührt" und *„dass es bei Facebook kaum noch ein anderes Thema gegeben habe"* (Thissen 2012). Als 2014 im baden-württembergischen Freiburg ein achtjähriger Junge tot aufgefunden wurde und kurze Zeit später gefälschte Phantombilder des mutmaßlichen Täters auf Facebook kursierten unter denen dazu aufgefordert wurde, *„die Fäuste fliegen zu lassen, wenn der Mann angetroffen wird",* erklärte Polizeisprecherin Laura Riske diese Aktion u. a. damit, dass an diesem Fall *„alle Menschen emotional beteiligt"* waren (zitiert in Drutschmann 2014). Ein weiteres Beispiel stammt aus Ravensburg. Im Netz kursierte 2014 eine Videoaufzeichnung, die mehrere junge Männer dabei zeigt, wie sie in einem leeren Silo minutenlang eine Katze grausam zu Tode quälen (DIE WELT 2014). Die Szenen lösten im Netz einen wahren Sturm der Entrüstung (einen sog. „shitstorm") aus. Tierschützer hatten auf ihrer Facebook Seite auf die Tat aufmerksam gemacht und darum gebeten, Hinweise zu den Tätern öffentlich zu machen. In nur 24 Stunden wurde der Post 80.000 Mal geteilt (DIE WELT 2014). Darunter entlud sich der Groll der Bevölkerung: *„ich schneide dir die Kehle durch", „pass auf, dass du nicht überfahren wirst"* oder *„abschlachten sollte man so was"* sind nur einige Beispiele für die stark emotionalisierten Reaktionen einiger Facebook Nutzer auf das veröffentlichte Video (zitiert in DIE WELT 2014). Ein weiterer Fall von Tierquälerei in Neubrandenburg ging 2018 ebenfalls mit solchen Aufrufen zur Gewaltanwendung im Internet einher (vgl. Beigang und Langer 2018).

Ob es bei diesen auslösenden Taten die Gewalt selbst war, die letztendlich die digilanten Akteure emotionalisiert und mobilisiert hat (zu Emotionen als Auslöser von Gewalthandlungen bzw. Rachegelüsten, vgl. z. B. Elias 1997; Heitmeyer und Hagan 2002; Tripp et al. 2007) oder die mediale Berichterstattung (z. B. durch dramatisierende oder skandalisierende Narrative, vgl. Hitzler 1993, Powell et al. 2018; die Möglichkeit, den Verlauf von Ereignissen dank ubiquitärer mobiler und sozialer Technologien quasi in Echtzeit und interaktiv miterleben zu können[4], vgl.

[4]Rose und Fox (2014, S. 785) z. B. haben in einer Studie den Zusammenhang zwischen dem Verfolgen von Berichterstattung über Kriminalität in den Sozialen Medien und vigilanten Einstellungen untersucht. Ihr Ergebnis zeigt, *„that those who use social networking sites to follow high-profile criminal trials are much more likely to wish they could seek revenge."* Sie schreiben, das Verfolgen und Lesen von Berichten über Kriminalfälle in den Sozialen Medien, stelle *„a significant predictor of vigilante attitudes"* dar. Personen, die sich regelmäßig mit Kriminalitätsberichterstattung in und über die Sozialen Medien beschäftigten, demonstrierten *„a heightened tendency to feel more vengeful and even wanted to take matters into their own hands against perpetrators of crime"* (Rose und Fox 2014, S. 787).

Presser und Sandberg 2014, Powell et al. 2018; bestimmte Täterzuschreibungen, vgl. Brückweh 2006; oder Opferdarstellungen, vgl. Peelo 2006), sei an dieser Stelle offengelassen. Eine eigenständige Betrachtung der Rolle von Emotionen im Vigilantismus steht, wie Schmidt-Lux (2017, S. 177) kürzlich anmerkte, bislang noch aus: *„In den bisherigen Arbeiten zum Vigilantismus haben Emotionen keine systematische Beachtung gefunden“*. Gerade eine solche Untersuchung wäre jedoch wünschenswert, stellt Warren (2009) doch die These auf, Vigilantismus sei eher Ausdruck gesellschaftlicher Unsicherheitsgefühle und Ängste, denn eine konkrete Maßnahme zur Kriminalitätsprävention (ähnlich siehe auch Quent 2016a, S. 12). In Gesellschaften monopolisierter Gewalt ist der Staat für die formelle Aufarbeitung und Sanktionierung eines Unrechts zuständig; BürgerInnen werden von der Regelung oder Lösung ihrer eigenen Konflikte in gewisser Weise verdrängt (vgl. Christie 1977). Das Publizieren von Unmutsäußerungen (wie z. B. der Ruf nach Todesstrafe) bzw. von stigmatisierenden, beschämenden Äußerungen ist somit das einzig (legitim) verfügbare Ventil für Opfer und andere betroffene Personen, ihre Unrechtserfahrungen selbst zu verarbeiten.

5.2 Aktivitäten und Ziele

Im soziotechnischen Kontext lassen sich – etwas vereinfacht – drei Arten von digilanten Aktivitäten beobachten: investigativ-kontrollierende Aktivitäten, appellative Aktivitäten und strafende bzw. rächende Aktivitäten (vgl. Yardley et al. 2018, S. 82, 93 f.; siehe auch Smallridge et al. 2016; Trottier 2017; Rüdiger 2017; Nhan et al. 2017; Powell et al. 2018; Dunsby und Howes 2019). Investigativ-kontrollierende Aktivitäten beinhalten das gezielte Suchen im Netz und in sozialen Netzwerken nach Informationen über Personen; das Kommentieren, Analysieren und Diskutieren digitaler Artefakte wie Dokumente, Fotos oder Videos; das Sammeln von digitalen Artefakten als „Beweismittel“ in Form von Screenshots, Chatprotokollen, etc.; das Identifizieren und öffentliche Hervorheben von verdächtigten Personen; und das Interagieren mit Vertretern der Polizei und/oder Justiz, sowie, in Ausnahmefällen, den Opfern bzw. ihren Familien. Appellative Maßnahmen sind beispielsweise das Weiterleiten offizieller Fahndungsaufrufe oder das Veröffentlichen eigener Fahndungsaufrufe. Strafende bzw. rächende Maßnahmen beinhalten das Hochladen und Teilen von Fotos und Videos sowie das Publizieren anderer personenbezogener Daten (Name, Anschrift, Arbeitsplatz, etc. – sog. „doxing“) mit dem Ziel die dargestellten Personen zu demütigen oder zu stigmatisieren; das Anfeinden, Beleidigen und Bedrohen von Personen; und, in einzelnen Fällen, das physische Bestrafen von

vermeintlichen TäterInnen, sind sie erst einmal identifiziert und lokalisiert (z. B. durch Verprügeln). Die meisten dieser digilanten Aktivitäten finden online statt, doch es kommt auch vor, dass das *„Hervorheben aus der Anonymität“*, wie es Ariane Friedrich ausdrückte, investigative Tätigkeiten oder Gewalt im „echten“ Leben nach sich zieht (auf diesen Aspekt gehe ich in Abschn. 5.4. noch ausführlicher ein). Zusammengefasst lässt sich also sagen, manche digilante Aktivitäten finden ausschließlich im digitalen Raum bzw. online statt; andere erfolgen teils online und teils offline (Trottier 2017, S. 58).

Ziele digilanter Aktivitäten sind i. d. R. Individuen, die mit den digilanten Akteuren über ihre Tat in einer unmittelbaren oder wenigstens mittelbaren Beziehung stehen. Entweder reagiert das „Opfer“ einer Schädigung selbst, wie im Fall der Ariane Friedrich, oder, wenn das Opfer selbst sich nicht wehrt oder nicht mehr wehren kann, wie im Fall der 2014 in Australien getöteten Jill Meagher, eine dem „Opfer“ nahestehende Person (vgl. Milivojevic und McGovern 2014; siehe auch der Fall Chloe Rubenstein in den USA, vgl. Hess 2010). Seltener kommt es vor, dass eine Person auf ein wahrgenommenes Unrecht reagiert, die selbst weder unmittelbar noch mittelbar betroffen ist, sondern aus anderen Gründen – z. B., weil sie der sachliche Kern eines Themas besonders berührt – gezielt die Aufmerksamkeit der Öffentlichkeit auf eine Tat bzw. einen Täter/eine Täterin zu lenken versucht (vgl. Zetter 2007; Levy 2013; Penny 2013; Kushner 2013, 2014). Das Handeln digilanter Akteure wiederum richtet sich direkt gegen die Personen, von denen der Schaden ausgegangen ist bzw. ausgegangen zu sein scheint (vgl. Jane 2017, S. 4). Es kommt aber auch vor, dass nicht nur die vermeintlichen Normbrecher selbst zum Ziel werden: Personen, die Verständnis für deren Handeln zeigen oder sich unterstützend für sie aussprechen, sowie Personen, die mit den Zielpersonen zu sympathisieren scheinen oder die vigilanten Handlungen Anderer kritisieren, können ebenfalls zu Zielen werden (Schmidt-Lux 2017, S. 182; vgl. auch Bosker 2013; Malone 2017). Und manchmal beginnt Digilantismus mit einer einzelnen, gegen eine bestimmte Person gerichteten Aktion, mit der auf eine konkrete Tat reagiert wird. Sie weitet sich dann aber zu einer größeren Bewegung aus, die mehrere Akteure vereint, welche sich gegen all jene wenden, die symbolisch für das wahrgenommene Unrecht zu stehen scheinen (man denke hier z. B. an den Fall Zoë Quinn und die Ereignisse rund um den „#gamergate“ Eklat, vgl. Malone 2017).

Des Weiteren können vigilante Akteure selbst zur Zielscheibe werden. Auf einer Konferenz für Software-Entwickler im kalifornischen Santa Clara kam es 2013 zu folgendem Vorfall, der unter dem Hashtag „#donglegate“ bekannt wurde: Die US-Amerikanerin Adria Richards schoss ein Foto zweier Männer und postete es auf Twitter mit den Worten, *„Not cool. Jokes about … ‚big‘ dongles*

right behind me" (zitiert in Ronson 2015a, b). „Dongles" ist das englische Wort für einen Kopierschutzstecker; umgangssprachlich wird es jedoch auch als Bezeichnung für das männliche Geschlechtsteil verwendet. Die beiden Männer hatten diese Zweideutigkeit des Wortes für einen Witz genutzt und Richards hatte sie gehört, obgleich sie sich nur leise miteinander unterhielten. Sie nahm Anstoß an den aus ihrer Sicht sexistischen Äußerungen der Männer und veröffentlichte deren Vergehen im Netz – allerdings ohne die Männer zuvor auf ihr Verhalten anzusprechen. In der Folge fand sich einer der beiden Männer – ein dreifacher Familienvater – nicht nur mit den wüsten Beschimpfungen und Beleidigungen einer Horde anonymer Internetnutzer konfrontiert; er wurde einen Tag später auch von seinem Arbeitgeber entlassen. Diese Tatsache wiederum machte der junge Mann in einem Online-Forum für Entwickler öffentlich. Kurz darauf wendete sich das Blatt: Aktivisten der Männerrechtsbewegung sowie verschiedene anonyme Trolle griffen nun Adria Richards an. Sie drohten ihr über Facebook und Twitter; ein Nutzer veröffentlichte sogar ihre Adresse, zusammen mit dem Foto einer enthaupteten Frau, der man den Mund mit Klebeband verschlossen hat; und ein Anderer startete eine *Distributed-Denial-of-Service* (DDoS) Attacke gegen die Webseite ihres Arbeitgebers mit dem Hinweis, diese erst beenden zu wollen, wenn Frau Richards nicht mehr für ihn arbeitet (vgl. Ronson 2015a, 2005b). Noch am selben Tag erhielt Adria Richards ihre Kündigung. Dieser Fall demonstriert eindrücklich die interaktiv-kommunikative Dimension digilanter Aktivitäten und die Aushandlungsprozesse über gesellschaftliche Normen und Werte, welche hier stattfinden. Er zeigt aber auch, wie sprunghaft das Phänomen des digitalen Vigilantismus sein kann. Wer TäterIn und wer Zielperson ist, kann sich schnell ändern.

5.3 Organisiertheit und Reichweite

Aus Johnstons (1996) Definition geht hervor, dass er Vigilantismus als eine Art soziale Bewegung versteht, die einen gewissen Grad an Organisiertheit aufweisen kann. Er unterscheidet Vigilantismus von spontanen Akten der Selbstverteidigung, die unmittelbar nach einer Schädigung erfolgen und denen somit keine Planung vorausgeht (ähnlich siehe auch Dumsday 2009; Quent 2016b; e Silva 2018). Dieser minimale Grad an Organisiertheit trennt für ihn Vigilantismus von Notwehr.

Digitaler Vigilantismus weist eine ganze Bandbreite an verschiedenen Organisiertheitsgraden auf. Digilante Akteure können Individuen oder Gruppierungen sein. Hill (2017) unterscheidet zwischen *„lone-wolf vigilantism"*

und *„crowdsourced vigilantism“* (ähnlich siehe auch Moncada 2017). Manchmal handeln digilante Individuen oder formieren sich digilante Gruppierungen *ad hoc* im Angesicht einer wahrgenommenen Bedrohung (vgl. Jane 2017); manchmal entstehen sie nach längerfristiger, gezielter Planung (vgl. Myles und Trottier 2017); und manchmal beginnen sie als spontane Reaktion auf ein wahrgenommenes Unrecht, aber nehmen mit der Zeit ein verbindlicheres Format an. Manchmal verfügen digilante Gruppierungen nur über eine kurze Lebensdauer und verschwinden ebenso schnell wieder wie sie aufgetaucht sind; die auslösende Tat bietet ihnen einen Anlass, der sie temporär zusammenfinden lässt, weil sie sich durch ihre Betroffenheit vereint fühlen oder ein gemeinsames Ziel teilen, den oder die Verantwortlichen für eine Schädigung zu identifizieren und/oder zur Rechenschaft zu ziehen (vgl. Nhan et al. 2017; Trottier 2017). Fällt die Betroffenheit weg oder wird das Ziel (durch sie oder die staatliche Ordnungsmacht) erreicht, löst sich die Gruppierung wieder auf. In anderen Fällen sind digilante Gruppierungen recht beständig (vgl. Myles und Trottier 2017; Zadrozny 2019).[5]

Auch der Grad der Regulierung innerhalb digilanter Gruppierungen variiert. Teilweise sind sie recht informell organisiert; dann wiederum gibt es Gruppierungen, die eigene Verhaltensregeln für ihre Mitglieder aufstellen und Verstöße mit einem Ausschluss aus der Zweck- bzw. Schutzgemeinschaft ahnden – was z. B. über ein Löschen des Nutzers von der Mitgliederliste oder ein Blockieren des Nutzers von den Kommentarfunktionen erfolgen kann. Des Weiteren gibt es digilante Akteure, die als Reaktion auf eine spezifische Tat aktiv werden und ihre Aktivitäten auf diese fokussieren, während andere eine ganze Reihe von Anliegen haben und z. B. über die Ahndung einer konkreten Tat hinaus noch weitergehende politische Ziel verfolgen (Yardley et al. 2018, S. 92; siehe auch Powell 2015; Salter 2017).

Das Internet mit seinen technischen Möglichkeiten, trägt dazu bei, dass sich Individuen und Gruppierungen schneller und leichter mobilisieren, als es bei

[5]Dies scheint insbesondere für solche Gruppierungen zuzutreffen, die sich der „Jagd nach Pädophilen“ verschrieben haben, wie z. B. *Prey on Predators, Predator Hunters* oder *Perverted Justice* aus den USA, *Judge Beauce* oder *Creep Catchers* aus Kanada, und *Dark Justice, Daemon Hunter* oder *Letzgo Hunting* aus England. Diese Organisationen sehen sich selbst allerdings nicht als vigilante Vereinigungen und distanzieren sich von derartigen Zuschreibungen aufgrund der mit diesem Begriff verbundenen negativen Konnotation eines gewaltbereiten und gewaltausübenden „Mobs“ (vgl. Campbell 2015; Perraudin 2017). Stattdessen bezeichnen sie sich als politische Aktivisten, die sich für den Schutz von Kindern einsetzen, da es der Staat nicht ausreichend tut bzw. lokale Polizeibehörden nicht über ausreichend (finanzielle und personelle) Ressourcen verfügen, um effektiv gegen die wahrgenommene Bedrohung vorzugehen.

konventionellen vigilante Bewegungen der Fall ist (Trottier 2017, S. 58). Digilante Gruppierungen sind i. d. R. *„horizontal organisiert“*, *„führerlos“* und *„rhizomatisch“* (Powell et al. 2018, S. 154). Klassische vigilante Bewegungen zeichnen sich oftmals durch einen – wenn auch nicht besonders rigorosen – Auswahlprozess aus, durch den potenzielle Mitglieder vor ihrer Aufnahme auf ihre Motivation und Gesinnung hin überprüft werden (Marx und Archer 1976, S. 140 f.; vgl. auch Arfsten 2010). Diese Hürde hängt bei digilanten Gruppierungen deutlich niedriger – im Prinzip kann jeder, der über einen Internetzugang verfügt, zum Digilante werden, in dem er sich entweder ein eigenes Profil einrichtet und darüber seine Nachrichten verbreitet oder sich in einem Forum anmeldet, welches sich digilanten Zielen verschrieben hat (Yardley et al. 2018, S. 82; Salter 2017, S. 133). Manche dieser Foren sind nur semi-öffentlich, d. h. um bestimmte Beiträge sehen oder sich aktiv beteiligen zu können, ist es notwendig zuvor eine Aufnahmeanfrage zu versenden, die von einem Administrator oder Moderator bestätigt werden muss (geschlossene, rein private Foren sind selten, da es ja gerade eines der Hauptziele dieser Gruppierungen ist, Öffentlichkeit für ihr Anliegen zu generieren). Glaubt man Salter (2017), dann ist diese Bestätigung jedoch häufig nur eine Formalie (vgl. auch Kushner 2013).

Darüber hinaus verändern die technischen Möglichkeiten des Internets die Reichweite digilanter Zusammenschlüsse. Bezeichnete Johnston (1996, S. 231) Vigilantismus noch als *„invariably local“*, so können Mitglieder digilanter Gruppierungen aus der ganzen Welt stammen und geografisch an verschiedenen Orten leben (Noble 2017, S. 48; Myles und Trottier 2017, S. 5). Sie stellen *„networks of shared interest“* (Salter 2017, S. 131) dar, die – Wiedemann (2014, S. 322) folgend – eher „Schwärmen“ ähneln, denn sozialen Bewegungen. Ein Nachteil dieser schwarmartigen, globalen Netzwerkstrukturen ist jedoch, dass die Verbindungen zwischen den Mitgliedern vigilanter Gruppierungen oft schwach und flüchtig sind (Salter 2017, S. 131). Gerade für jene Gruppierungen, die auf kollektiver Ebene nachhaltig für politische oder rechtliche Veränderungen sorgen wollen, stellt dies ein Problem dar: *„[It] has the potential to disperse and dilute momentum towards collective action and exarcerbate dynamics of exclusion and alienation“* (Salter 2017, S. 131).

Aus theoretischer Sicht interessant an den schwarmartigen digilanten Netzwerken ist, dass hier Taten, die sich offline und in einem spezifischen, situativ-lokalen Kontext ereignet haben, in einem digitalen Raum zur Diskussion gestellt werden, der diesen Rahmen bei weitem überschreitet und in dem kulturell unterschiedliche Werte und Vorstellungen von Recht und Ordnung aufeinandertreffen (können). Dieser Aspekt ist deshalb spannend und gibt Anlass zu Reflektion, da Vigilantismus klassischerweise mit historisch und lokal geprägten, d. h. eher

national-spezifischen, Verständnissen von Bürgerschaft, Gemeinschaft („community"), Recht, Ordnung und Moral verbunden wird, als deren Beschützer sich vigilante Akteure präsentieren (vgl. Abrahams 1998; Wall und Williams 2007; Trottier 2017). Für Quent (2016b) ist Vigilantismus deshalb ein „hausgemachtes" („homegrown") Phänomen: seine Akteure sind StaatsbürgerInnen, die ihr „Heim" (ihre Gemeinschaft, ihren Status quo, ihre Moralvorstellungen, etc.) verteidigen wollen.

Was aber bedeuten Konzepte wie „Staatsbürgerschaft", „Ordnung" oder „Gemeinschaft" in einem globalen, digitalen Raum wie dem Internet? Trottier (2017, S. 63) betont: *„on digital media, these elements by definition exceed the scope and jurisdiction of any nation"*. An dieser Stelle möchte ich nur ein Beispiel für die Problematik anführen, die damit entsteht: In der Literatur zum klassischen Vigilantismus besteht die Annahme, dass die Wahrscheinlichkeit seines Auftretens höher in homogenen, geschlossenen (kohäsiven) Gemeinschaften ist, weil sie Normen und moralische Standards miteinander teilen (vgl. Silke 2001: S. 123). Virtuelle Gemeinschaften zeichnen sich aber i. d. R. durch einen hohen Grad an Heterogenität aus. Der beim konventionellen Vigilantismus beobachtete Zusammenhang zwischen der Homogenität einer Gemeinschaft und seinem Entstehen muss im digitalen Kontext also hinterfragt und überdacht werden. Stegbauer (2001, S. 67) bezweifelt zudem, ob aus einer *„internetbasierten Kommunikationsgruppe"*, selbst wenn sie eine interne Struktur herausbildet, je eine Gemeinschaft werden kann.

5.4 Anwendung bzw. Androhung von Gewalt

Die Anwendung bzw. Androhung von (physischer) Gewalt durch private Akteure in Räumen, in denen sich ein staatliches Gewaltmonopol (noch) nicht durchgesetzt hat, ist ein zentrales Element klassischer Definitionen von Vigilantismus. Schmidt-Lux (2018, S. 146) beschreibt klassischen Vigilantismus als eine „Gewaltform", die *„von – wie auch immer motivierten – nicht-staatlichen Akteuren eingesetzt oder mindestens angedroht wird"*. Moncada (2017, S. 407) spricht von *„repertoires of violence"*, die tödliche und nicht-tödliche Gewalt umfassen. Und auch Johnston (1996) sieht mindestens die Androhung von Gewalt als ein zentrales Merkmal des klassischen Vigilantismus an. Sowohl die Androhung als auch Anwendung von Gewalt sind im Digilantismus ebenfalls zu beobachten. Während sich Androhungen von Gewalt häufiger finden lassen, kommt es allerdings seltener zu tatsächlicher physischer Gewalt: *„physical violence is rarely a component of digital attacks"* (Smallridge et al. 2016, S. 65; siehe auch Myles

und Trottier 2017, S. 59). Selten folgt auf einen Aufruf zur Gewalt im Netz auch tatsächlich gewaltsames Handeln in der nicht-digitalen Welt; selten führt selbstjustizielles Gebaren online auch zu „realer“ Selbstjustiz offline. Die Anwendung von Gewalt ist also ein Element, welches sich – zumindest im physischen Sinne – nicht ohne weiteres in eine Konzeption von Vigilantismus im digitalen Kontext übertragen lässt.

Der Fall des 2011 im Zusammenhang mit dem Mord an einem elfjährigen Mädchen fälschlich verdächtigten Jungen aus Emden zeigt, dass Aufrufe zur Gewalt im Netz durchaus „reale“ Konsequenzen nach sich ziehen können – immerhin hatte sich aufgrund des Facebook Posts bereits eine Menschenmenge vor der Polizeiwache versammelt, die zumindest Gewaltbereitschaft verbal signalisierte, als sie seine Auslieferung verlangte (vgl. Thissen 2012). Und ein Fall aus Gütersloh aus dem Jahr 2016 zeigt, dass private Fahndungsaufrufe im Netz auch tatsächlich physische Gewalt nach sich ziehen können: nach einer Schlägerei in einem Bistro, bei der ein Kellner verletzt wurde, luden Angehörige des Kellners ein Foto der Auseinandersetzung bei Facebook hoch mit der Aufforderung den Angreifer zu identifizieren (Menzel 2016). Ausgestattet mit Namen und Adresse suchten die Angehörigen den Mann schließlich auf und verletzten ihn so schwer, dass er mit einem Rettungswagen in ein Krankenhaus gebracht werden musste (Menzel 2016). Diese beiden Fälle unterstreichen Schmidt-Luxs (2018, S. 149) Argument, dass die verbale Legitimation von vigilanter Gewalt deren Ausübung vorbereiten und stimulieren kann.

Aufgrund der Seltenheit von tatsächlicher Gewaltanwendung plädieren Myles und Trottier (2017, S. 59) dennoch dafür, dieses Element des klassischen Vigilantismus-Konzeptes für den Online-Kontext zu modifizieren. Sie schlagen vor, den Begriff der „Gewalt“ durch den der „Schädigung“ zu ersetzen: *„the causation of harm or threat thereof“* (ähnlich siehe e Silva 2018). In erster Linie ginge es den digilanten Akteuren nämlich nicht einfach um die Anwendung von physischer Gewalt, sondern um die Stigmatisierung der Zielperson(en) und die Realisierung informeller (nicht verbotener) Sanktionen. Auf den ersten Blick scheint dieser Vorschlag das Gewaltpotenzial, welches sich in digilanten Äußerungen online immer wieder zeigt, verharmlosen zu wollen. Dies scheint insbesondere bei jenen Fällen zuzutreffen, bei denen die gewaltindizierenden oder beschwörenden Aussagen digilanter Akteure in keinem Verhältnis zu ihren auslösenden Taten zu stehen scheinen: wenn es z. B. zu Morddrohungen als Reaktion auf einen Twitter-Post kommt (vgl. Ronson 2015a). Angedrohte Vergewaltigungen (sog. „rape threats“) – eine hochgradig genderisierte Form der Gewaltandrohung online, die sich fast ausschließlich gegen Frauen richtet – sind ein weiteres Beispiel (vgl. Hess 2010; Schaschek 2014; Salter 2017;

Molloy 2018).[6] Trotzdem erscheint Myles und Trottiers Adaption sinnvoll, trägt sie doch der Tatsache Rechnung, dass es als Folge digilanter Aktivitäten auch zu Schädigungen kommen kann, die nicht allein physischer Natur sind. In den einschlägigen Studien, die bislang zum digitalen Vigilantismus existieren, lassen sich ganz unterschiedliche Konsequenzen feststellen, die digilante Aktivitäten nach sich ziehen können. Sie lassen sich – auch hier wieder vereinfacht – in vier Kategorien ordnen: 1) Konsequenzen für die Reputation/Identität der beschuldigten Personen; 2) Konsequenzen für das Leben bzw. den Lebensstil der Betroffenen; 3) Konsequenzen für mittelbar betroffene Angehörige; und 4) Konsequenzen für die „Opfer" einer Digilantismus auslösenden Tat.

In erster Linie können digilante Aktivitäten negative Auswirkungen auf die Identität bzw. Reputation der öffentlich beschuldigten oder gedemütigten Personen haben (vgl. Massaro 1991; HLRA 2003; Dittmeyer 2013; Ronson 2015a, b; Kaser 2017). Martin (2007, S. 126) spricht in diesen Fällen von *„online character assassination"*. Beleidigende und herabwürdigende Äußerungen können die Ehre einer Person verletzen (vgl. Dittmeyer 2013) und das ungenehmigte Veröffentlichen persönlicher Daten oder eines Bildnisses kann das Recht auf informationelle Selbstbestimmung der betroffenen Person tangieren (vgl. Baur et al. 2011). Ein weiterer Kernaspekt digilanten Handelns ist, dass ihm kein rechtsstaatliches Verfahren vorweg geht, in dem u. a. die Schuld eines Täters gerichtlich festgestellt wird (Rüdiger 2017, S. 228). Wenn nun also eine Person im Rahmen digilanter Aktivitäten öffentlich „an den Pranger" gestellt wird, dann ist das aus rechtsstaatlicher Sicht problematisch. Das Prinzip der Unschuldsvermutung besagt, dass jeder bis zum gesetzlichen Nachweis seiner Schuld als unschuldig zu gelten hat (vgl. Saliger 2013).[7] Aus diesem Grund sind die traditionellen Medien

[6]Laut einer Ipsos-Mori-Umfrage aus dem Jahr 2017 (n = 500) ist jede vierte Frau schon einmal Opfer von Anfeindungen in sozialen Netzwerken geworden. In knapp der Hälfte der Fälle waren die Hassbotschaften frauenfeindlichen oder sexistischen Inhalts (vgl. IPSOS-MORI 2017). Auch eine FORSA Umfrage der Landesanstalt für Medien NRW von 2018 zeigt, dass Frauen geringfügig mehr Erfahrungen mit Hass Kommentaren machen (78 %) als Männer (76 %) (vgl. FORSA 2018).

[7]Im Kontext dieses Kapitels ist es interessant, dass die Idee der Unschuldsvermutung im deutschsprachigen Raum erstmalig im Jahr 1631 von Friedrich Spee von Langenfeld in einer umfangreichen Schrift gegen die Praxis der Hexenverfolgungen (der *Cautio Criminalis*) aufgegriffen und entwickelt wurde; vgl. http://www.rheinische-geschichte.lvr.de/Persoenlichkeiten/friedrich-spee-von-langenfeld/DE-2086/lido/57c9537ab741e1.30560080. Zugegriffen: 23. Februar 2019.

auch durch einen Pressekodex dazu angehalten, die Persönlichkeit und das Privatleben von Personen zu achten und nur in besonderen Fällen individualisierende Informationen zu veröffentlichen (vgl. Saliger 2013).[8] Vor allen Dingen darf die Berichterstattung nicht präjudizierend bzw. vorverurteilend wirken, d. h., es darf nicht der Eindruck entstehen, der Beschuldigte sei der ihm vorgeworfenen Tat bereits überführt (Saliger 2013, S. 178). Wäre dies der Fall, würde die Veröffentlichung den gesetzlichen Nachweis der Schuld quasi aushebeln und somit eine gravierende Verletzung der Persönlichkeitsrechte der beschuldigten Person bedeuten, denn es besteht die Gefahr einer Stigmatisierung, die selbst durch einen Freispruch später nicht mehr ausgeräumt werden kann, zumal einmal in das Internet gestellte Informationen kaum wieder aus diesem zu entfernen und grundsätzlich auch Jahre später noch, weltweit, auffindbar sind (Saliger 2013, S. 177; Voskamp und Kipker 2013, S. 788; vgl. auch Wettlaufer 2015). Diese Stigmatisierung wiederum kann faktisch den Ausschluss aus der sozialen Gemeinschaft bedeuten, mit weitreichenden Folgen für das Leben der betroffenen Person:

[8]Wann eine Berichterstattung zulässig ist, richtet sich nach der Art derselben und nach dem Bereich, dem die veröffentlichten Informationen angehören, d. h., ob sie dem Kernbereich höchstpersönlicher privater Lebensgestaltung angehören (Intimsphäre) oder der bloßen Privatsphäre (vgl. Saliger 2013, S. 175; siehe auch Dittmeyer 2013). Informationen, die letzterem Bereich zugeordnet werden, können nach einer Abwägung unter Beachtung des Verhältnismäßigkeitsgrundsatzes der Öffentlichkeit zugänglich gemacht werden, sofern hier – z. B. aufgrund der besonderen Schwere der Straftat – ein Informationsinteresse besteht. Für eine bloße Verdachtsberichterstattung liegen die rechtlichen Anforderungen für eine Veröffentlichung individualisierender Informationen noch höher. Nach Ansicht des Bundesgerichtshofs für Zivilsachen *„kommt eine Namensnennung grundsätzlich nur in Fällen schwerer Kriminalität oder bei Straftaten mit besonderer Öffentlichkeitsberührung in Betracht. Eine zulässige Verdachtsberichterstattung setzt darüber hinaus einen Mindestbestand an Beweistatsachen für den Wahrheitsgehalt der Information voraus, wobei die Medien eine umso höhere Sorgfalt trifft, je schwerer und nachhaltiger die Veröffentlichung das Ansehen des Beschuldigten beeinträchtigt“* (Saliger 2013, S. 177). Über eine *mittelbare Drittwirkung* ist die Unschuldsvermutung zudem auch im Verhältnis von Privatpersonen zueinander anwendbar (vgl. Saliger 2013, S. 186; Zabel 2011, S. 360). Gerade auch der Emdener Fall von Digilantismus, schreibt Saliger (2013, S. 186), zeige, wie notwendig es ist, mit der Unschuldsvermutung *„auch im Verhältnis der Bürger untereinander für eine Atmosphäre der Anständigkeit“* zu sorgen und *„gezielte Öffentlichkeit“* zu unterbinden. Aber nicht nur ehrverletzende Äußerungen oder eine öffentliche Namensnennung können rechtlich problematisch sein, auch die ungenehmigte Weitergabe an Dritte von bestimmten Informationen, z. B. wenn der Inhalt von E-Mails, SMS, etc. veröffentlicht wird, kann unzulässig sein (vgl. Dittmeyer 2013, S. 783).

sie kann zu ihrem *„sozialen Tod“* führen (Baur et al. 2011, S. 131). Das Veröffentlichen personenbezogener Daten, um einer Person die Begehung einer unrechten Tat zu unterstellen und sie damit gezielt zu demütigen bzw. ihren Ruf zu schädigen, wie es beim Digilantismus regelmäßig praktiziert wird, ist rechtlich also durchaus fragwürdig – nicht nur in Fällen, bei denen sich später herausstellt, dass der oder die Verdächtigte unschuldig war (vgl. Wehmhoener 2010; Rose und Fox 2014; Arvanitidis 2016; Nhan et al. 2017; Jane 2017; Noble 2017).[9] Prekär sind in diesem Zusammenhang außerdem Fälle, in denen die beschuldigten Personen noch minderjährig sind, aber dennoch durch eine Namensnennung und/oder eine Abbildung klar identifizierbar gemacht werden, denn Minderjährige genießen i. d. R. einen besonderen Schutz (vgl. Saliger 2013, S. 176; siehe auch Arvanitidis 2016).

Zweitens, kann Digilantismus Konsequenzen für das Leben bzw. den Lebensstil der betroffenen Person bedeuten: wie ebenfalls der Fall Adria Richards bereits aufgezeigt hat, können öffentliche Anschuldigungen gegen eine Person (aber auch vigilante Aktivitäten selbst) zum Verlust des Jobs und darüber hinaus zu einer (zeitweisen) Verschlechterung beruflicher Karriereperspektiven führen (vgl. Ronson 2015a, 2005b; Arvanitidis 2016; Molloy 2018). Beschimpfungen, Beleidigungen und Drohungen, die auf eine öffentliche Anschuldigung folgen, können es außerdem erforderlich machen, dass die Zielpersonen (sowie ggf. deren Angehörige) nicht nur ihren Arbeitgeber, sondern auch ihren Wohnort wechseln müssen (vgl. Arvanitidis 2016; Myles and Trottier 2017). Zudem kann

[9]Wenn Beschuldigte, wie in dem anfangs genannten Fall aus Hamburg oder im Fall Adria Richards, ohne ein möglicherweise klärendes Gespräch (oder, in schwerwiegenden Fällen, ohne ein polizeiliches Ermittlungsverfahren bzw. ein offizielles Strafverfahren) sofort im Netz landen, um von einer digitalen *„citizen jury“* vorverurteilt zu werden, wird ihnen außerdem noch die Gelegenheit genommen, wie Jane (2017, S. 4) anmerkt, *„to tell their – potentially exculpatory – sides of the story“*. Hätte Adria Richards vor ihrem Twitter-Post den beiden jungen Männer eine Gelegenheit gegeben, zu erklären, dass sie nur einen – zugegebenermaßen etwas unreifen und durchaus sexistischen – Witz gemacht haben und, nachdem Richards ihren Unmut darüber geäußert hätte, sich dafür in aller Form zu entschuldigen, dann hätten möglicherweise auf allen Seiten größere Schäden verhindert werden können, die eben gerade durch die gezielte Veröffentlichung des Vorfalls entstanden sind. Ronson (2015a) vermutet allerdings, dass Adria Richards den Vorfall bewusst nutzte, um an den beiden Männern ein Exempel zu statuieren und Aufmerksamkeit auf Sexismus und Diskriminierung von Frauen in der Tech-branche an sich zu lenken – ein Thema, mit welchem sie sich zuvor auch schon auf ihrem Blog *butyoureagirl* befasste.

negative Öffentlichkeit zu sozialer Ausgrenzung und Isolation führen (vgl. Goffman 1963, S. 30; Katyal 1997, S. 2458; Wergin 2017). Goffman (1963, S. 30) schreibt hierzu: *„In general, the tendency for a stigma to spread from the stigmatized individual to his close connections provides a reason why such relations tend either to be avoided or to be terminated, where existing"*. Und Katyal (1997, S. 2458) vermerkt, *„[n]ormal people do not want to be seen with the stigmatized"* denn der Umgang, den eine Person pflegt, sage auch etwas über ihre soziale Identität aus.

Der 2013 öffentlich einer Vergewaltigung bezichtigte, aber in einem internen Untersuchungsverfahren für unschuldig erklärte Columbia University Student Paul Nungeßer berichtet dementsprechend über seine Erfahrungen:

> „Ich war weitestgehend isoliert. Viele Leute, die vorher Freunde gewesen waren, haben mich von einem Tag auf den anderen gemieden. Wenn ich das Gespräch gesucht habe, kam oft die Antwort: Paul, wir glauben dir, dass an diesen Anschuldigungen nichts dran ist, aber wir können es in diesem öffentlichen Klima nicht erlauben, weiter mit dir in Verbindung gebracht zu werden" (zitiert in Wergin 2017).

Ähnliche Erfahrungen machte Justine Sacco, die 2014 für einen politisch inkorrekten Witz, den sie über ihren Twitter-Account veröffentlichte, online geächtet wurde. Sie stellte bald fest, dass sich Freunde von ihr distanzierten. Auch Dating wurde unmöglich in einer Welt, in der jeder einen potenziellen Partner erst einmal googelt, bevor er ihn trifft (vgl. Ronson 2015a, 2005b). Trotz der kurzen Aufmerksamkeitsspanne, die den Medien und ihrem Publikum heutzutage regelmäßig attestiert wird (vgl. z. B. Maiaroto 2013), und einer öffentlichen Entschuldigung, dauerte es Monate bevor Justine Sacco wieder in ein einigermaßen normales Leben zurückfand (vgl. Ronson 2015a, b).

Die mit einer öffentlichen Demütigung einhergehende Stigmatisierung kann also nachhaltig das Leben der betroffenen Personen beeinflussen – nicht zuletzt, weil das Internet nichts vergisst; die Vorwürfe stehen für immer im virtuellen Raum, auch wenn sie längst entkräftet oder widerlegt wurden. Im Einzelfall kann das Leben der Zielperson von Digilantismus daher sogar so weit als beeinträchtigt empfunden werden, dass es zum Suizid kommt (vgl. Kohm 2009; Booth 2013; Baraniuk 2014; Campbell 2015; Noble 2017; Zadrozny 2019). In jedem Fall aber ist die Erfahrung des öffentlichen Hervorhebens, Beschuldigens und Beschimpfens unangenehm, wenn nicht traumatisch. Diesen Schluss legt zumindest Jon Ronson (2015a) nahe. In seinem Buch *So You've Been Publicly Shamed* verarbeitet der britische Journalist die Geschichten einiger Personen, die in den letzten Jahren zum Ziel von Digilantismus geworden sind. Er beschreibt

die betroffenen Personen allesamt als „broken somehow“, als *„deeply confused and traumatized“* (Ronson 2015b).[10]

Drittens ist bei den Konsequenzen digilanter Aktivitäten mittelbar an die Familien der betroffenen Personen zu denken. Auch sie können zur Zielscheibe von Beschimpfungen, Beleidigungen und Drohungen werden. In dieser Hinsicht stellen auch sie – indirekt – „Opfer“ dar, denn sie sind Unbeteiligte, die in diesen Prozess des Digilantismus unfreiwillig hineingezogen werden, denen aber ebenfalls (emotionaler und/oder physischer) Schaden zugefügt werden kann (vgl. Linkins 2013; Shontell 2013; Lee 2015; Malone 2017; Nhan et al. 2017). Ein eindrückliches Beispiel ist der Fall Sunil Tripathi. Tripathi wurde nach den Anschlägen beim Boston Marathon 2013 von selbsternannten Privatermittlern auf den Internet-Plattformen Reddit und 4chan zunächst verdächtigt, einer der beiden Attentäter zu sein. Der Junge galt zum Zeitpunkt der Anschläge bereits als vermisst, doch als ein vom FBI veröffentlichtes Fahndungsfoto vermeintlich Ähnlichkeit mit dem Vermissten aufweist, wird er schnell zur Zielscheibe. Seine Familie muss miterleben, wie über die Sozialen Medien Nachrichten wie diese verbreitet werden: *„Oh hey Sunil Tripathi, wenn Du gerade auf Twitter bist und siehst, wie wir auf deinen Tod warten, beeil dich, ich will schlafen“* (zitiert in Dorfer und Schulz 2013). Sie selbst werden ebenfalls beschimpft und erhalten sogar Morddrohungen (vgl. Schmoll 2013); ihnen wird unterstellt, den *„Attentäter“* zu decken (vgl. Lee 2015). Kurze Zeit später stellt sich heraus, Tripathi hatte mit den Anschlägen nichts zu tun. Er litt an Depressionen und hatte bereits Tage zuvor sein eigenes Leben beendet (Lee 2015). Im Nachgang beschreibt seine Familie die Aufmerksamkeit, die ihnen und ihrem Sohn zu Teil wurde, als *„tremendous and painful“* (zitiert in Dorfer und Schulz 2013) und ihre Erlebnisse als „a nightmare unimaginable“ (zitiert in Linkins 2013).

Schließlich müssen noch negative Auswirkungen anerkannt werden, die digilante Aktivitäten auf die „Opfer“ von auslösenden Taten haben können, denn nicht immer stehen die „Opfer“ hinter den Veröffentlichungen oder sind mit ihnen einverstanden (vgl. Levy 2013; Fuchs, Kelley und Lubin 2013; Petersen 2014a, b). Vor knapp fünf Jahren zirkulierte ein Video auf Facebook, welches zeigte, wie

[10]Eine für Amnesty International von dem britischen Marktforschungsinstitut Ipsos-Mori im Jahr 2017 durchgeführte Umfrage zeigt, dass Betroffene von Anfeindungen in sozialen Netzwerken in der Folge an Stress, Angst, Panik-Attacken und Schlafstörungen leiden können (vgl. Ipsos-Mori 2017). Befragt wurden für diese Studie 500 Frauen in acht Ländern. Die Umfrage zeigt, dass das Internet gerade auch für Frauen zu einer Art „Angstraum“ werden kann.

eine Jugendliche von anderen Jugendlichen geschlagen und getreten wurde. Als Grund für die Veröffentlichung wurde „Selbstjustiz“ genannt (Petersen 2014b). Die Polizei Stuttgart, die für den Fall zuständig war, bat über ihre Webseite darum, das Video nicht weiter zu verbreiten. Das Teilen oder Verbreiten von Gewaltdarstellungen sei nicht nur eine Straftat gemäß § 201a StGB; sie baten die Öffentlichkeit darüber hinaus zu bedenken, dass jeder, der das Video verbreitet, *„auch das im Video gezeigte Opfer der Gewalt in der Öffentlichkeit zeigt und der bereits geschädigten Person somit erneut Schaden zufügt“*.[11]

Ähnliche Bedenken wurden auch in den USA laut, als im Jahr 2012 Fotos und Videos durch eine Bloggerin öffentlich gemacht wurden, welche mehrere Jugendliche dabei zeigten, wie sie eine stark alkoholisierte 16-Jährige, die kaum noch bei Bewusstsein war, mehrfach sexuell missbrauchten und vergewaltigten. Das Mädchen hatte Anzeige gegen die Jungen erstattet, als es von den Darstellungen Kenntnis erlangte. Während des anschließenden Gerichtsverfahrens machten mehrere große Nachrichtensender sowie ein Vertreter der digilanten Gruppe *Anonymous* die Namen der (damals noch minderjährigen) Verfahrensbeteiligten publik (Levy 2013). Am Ende der Verhandlungen kannte eine breite Öffentlichkeit den Namen und das Gesicht des Opfers: sie war zum Gesicht einer nationalen Debatte über eine US-amerikanische „Vergewaltigungskultur“, über die Autonomie von Frauen und ihr Recht auf Sicherheit geworden (vgl. Penny 2013; Levy 2013). Levy (2013) zitiert die zuständige Staatsanwältin in dem Fall mit den Worten: *„What the bloggers did was to make sure that five hundred million people saw those pictures of her [the victim]. I wouldn’t want that picture to be seen by one person.“*

Studien zur Erforschung der Wirkungen von Kriminalitätsberichterstattung bieten Anlass zu der Annahme, dass ein derartiges mediales Spektakel für ein ohnehin bereits traumatisiertes „Opfer“ einer Gewalttat zu einer Art sekundären Viktimisierung führen kann.[12] Sekundäre Viktimisierung bezeichnet die Reaktionen der Umwelt der Opfer – und damit auch der Medien – auf eine Tat, wodurch zusätzlicher Schaden zugefügt wird (Kunczik 2016, S. 152). Eine primäre Viktimisierungserfahrung kann durch entsprechende (Fehl)Reaktionen des

[11]Siehe: https://www.polizei-praevention.de/aktuelles/polizei-stuttgart-auf-facebook-bittet-um-teilen-des-hinweises.html?type=98. Zugegriffen: 9. März 2019.

[12]Im deutschsprachigen sind bislang allerdings nur drei Studien bekannt (Kunczik und Bleh 1995; Maercker und Mehr 2006; Otto 2002). Diese beschäftigen sich mit der Kriminalitätsberichterstattung in den traditionellen Medien, nicht in den Sozialen Medien (vgl. Kunczik 2016). Hier besteht eine Forschungslücke.

Umfelds eines Opfers verlängert, verdichtet und verschlimmert werden (Condry 2010, S. 236). Wie das Opfer die öffentliche bzw. veröffentlichte Meinung wahrnimmt, spielt hierbei eine wesentliche Rolle (Kunczik 2016, S. 161). Außerdem kann es für ein Opfer belastend sein, ein Leben lang namentlich mit einem solchen Fall verbunden zu bleiben. Wenn ein Opfer identifizierbar ist, kann eine Veröffentlichung auch hier eine Prangerwirkung nach sich ziehen (Kunczik 2016, S. 156; vgl. auch Fuchs et al. 2013; Kepplinger 2016).

Darüber hinaus zeigt der eben beschriebene Fall aus Steubenville, dass digilante Aktivitäten polizeiliche Ermittlungsverfahren gefährden können, wenn Verdächtigungen öffentlich und vorab im Netz publiziert werden: *„many of the teens who tweeted and took pictures that night deleted their digital records as anxiety began to set in“,* schreibt Levy (2013; ähnlich siehe auch e Silva 2018). Die Möglichkeit, digitale Artefakte zu manipulieren oder verschwinden zu lassen, kann also ein Problem darstellen, welches den Weg zu einem fairen Verfahren und zu einer Wahrheitsfindung für ein Opfer einer auslösenden Tat erschweren kann – zumal, wenn die Öffentlichkeit noch vor einem offiziellen Ermittlungsverfahren hergestellt wird. Des Weiteren besteht die Möglichkeit, dass ein Strafprozess durch große öffentliche Aufmerksamkeit negativ beeinflusst wird (vgl. Kunczik 2016; Kepplinger 2016). Diese Formen der Schädigung müssen bei einer umfassenden Betrachtung der möglichen Konsequenzen von digilantem Handeln erfasst werden.

Zusammenfassend lässt sich also sagen, dass die entscheidende Taktik digilanter Akteure, um ihre Ziele zu erreichen, nicht die Anwendung physischer Gewalt zu sein scheint; stattdessen scheint es sich, wie Trottier (2017, S. 58) überzeugend argumentiert, vielmehr um die Ausübung einer Art kulturellen Gewalt zu handeln, die vermeintliche TäterInnen sichtbar macht und zugleich begleitende Formen der Gewalt bzw. der Schädigung legitimiert. Für Myles und Trottier (2017, S. 6) ist es diese gezielte Instrumentalisierung einer medial hergestellten und vermittelten Öffentlichkeit, die das Element der Gewalt im klassischen Vigilantismus ersetzt: *„the new dynamics of mediated vigilantism might be better understood as the instrumentalization of power imbalances rather than as the use of physical force in a stricter sense“*. Wenn digilante Akteure Sichtbarkeit gezielt als eine Art „Waffe“ zur Ausübung von Selbstjustiz einsetzen (vgl. Trottier 2017), dann erfüllt dies zwar nicht das von klassischen Definitionsansätzen zum Vigilantismus geforderte Kriterium der Anwendung physischer Gewalt; diese Aktivitäten können aber dennoch sehr reale und durchaus schwerwiegende emotionale/psychologische, soziale, und ökonomische Auswirkungen für unmittelbar und mittelbar betroffene Personen haben (vgl. Powell et al. 2018, S. 143, 148). Daher erklären Smallridge et al. (2016) zu Recht, das Fehlen einer Anwendung von Gewalt im

engen Sinne, d. h. als physische Gewalt, sei kein Grund nicht von Digilantismus zu sprechen.

5.5 Öffentliches Beschämen als zentrales Element des Digilantismus

Das systematische und öffentliche Beschämen bzw. Vorführen von Personen spielt beim digitalen Vigilantismus eine zentrale Rolle (vgl. z. B. Wall und Williams 2007; Kohm 2009; Skoric et al. 2010; Powell et al. 2018). Elemente der von Ahmad (2015) beschriebenen *„call-out culture“* oder von Hai-Jews (2014) *„vengeance culture“* spiegeln sich hier wieder.

Das Ziel von Digilantismus als eine Strategie des Sichtbarmachens ist das Bloßstellen von Personen, die sich aus Sicht der digilanten Akteure sozial unerwünscht oder abweichend verhalten haben, als eine Form der virtuellen Bestrafung bzw. eines „trial by media“ (vgl. Dennis 2008; Kohm 2009; Cheung 2014; Trottier 2017; Dunsby und Howes 2019). In erster Linie geht es den Akteuren dabei aber nicht um die Herstellung von (Straf-)Verfahrensgerechtigkeit, d. h. um eine gesetzlich festgelegte Verarbeitung der Tat, sondern um eine Ansehensminderung der TäterInnen: *„The new breed of digilante aims less to take cases to court than to shame the shameless“* (Martin 2007, S. 124). Diese sanktionierende Stigmatisierung von Personen erfolgt losgelöst von jedwedem formalrechtlichen Prozess der Konfliktlösung, also außerjustiziell oder informell (vgl. Powell et al. 2018; Zabel 2011). Sie erfolgt durch Blogeinträge, Tweets oder Postings von privaten Personen im Internet und unter Verwendung Sozialer Medien. Dabei wird den zu diesem Zweck hochgeladenen Screenshots, Fotos oder Videos der Status digitaler „Beweise“ zugeschrieben: ihre Authentizität wird nicht hinterfragt. Sie werden als eindeutige und authentische Repräsentationen der auslösenden Tat in den digilanten Narrativ eingefügt (vgl. Mallén 2016).

Im Kontext von Digilantismus sind Postings in den Sozialen Medien folglich nicht bloß Inhalte, sondern performative Akte (Wall und Williams 2007, S. 404; Salter 2017, S. 106). Sie benennen ein Handeln als offensichtlich „falsch“ („naming“) und lenken Aufmerksamkeit auf die vermeintlich für dieses Handeln verantwortliche Person („shaming“). Sie definieren die Situation für das Publikum und binden dieses in das Geschehen als virtuelle „Zeugen“ ein. Diesen Akten des öffentlichen Beschuldigens und Beschämens wird sowohl eine einschüchternde oder repressive, als auch eine abschreckende Wirkung attestiert (Smallridge et al. 2016, S. 63; siehe auch Trottier 2017). Einerseits sollen sie dazu führen, dass die beschuldigten Personen, durch die ihnen zuteilwerdende

negative Aufmerksamkeit zur Rechenschaft gezogen werden und Verantwortung für ihre Taten übernehmen (vgl. Jane 2017).[13] Andererseits soll durch das gezielte Hervorheben von falschen Verhaltensweisen und deren öffentliche Verurteilung bzw. Missbilligung ein präventiver Effekt entstehen und „richtiges" Verhalten befördert werden (Skoric et al. 2010, S. 188; Dunsby und Howes 2019, S. 13). Durch den Akt des Beschämens sollen bestehende und als legitim erachtete Normen und Werte, sowie Vorstellungen von Recht und Ordnung, in einer Gemeinschaft symbolisch verdeutlicht werden. Darüber hinaus soll über die Angst vor Stigmatisierung und sozialer Ausgrenzung, die auf einen Akt des öffentlichen Beschämens folgen kann, Konformität hergestellt werden.[14] In dieser Hinsicht ähneln Praktiken des Beschämens im Rahmen von Digilantismus früheren Formen der Sozialkontrolle in lokalen Gemeinschaften (vgl. Mallén 2016, S. 12).

Aufgrund der gezielten Öffentlichkeit von beschämenden Schuldzuschreibungen ist im Zusammenhang mit Digilantismus deshalb auch immer wieder von einem „Internet-*Pranger*" die Rede. Der Begriff „Pranger" bezeichnet laut Duden eine *„Stelle auf einem öffentlichen Platz mit einem Pfahl, einer Säule, wo jemand wegen einer als straf-, verachtenswürdig empfundenen Tat angebunden stehen muss und so der allgemeinen Verachtung ausgesetzt ist"*.[15] Es ist ein Ort, *„an dem Menschen der Kundgabe der Verachtung durch die Masse schutzlos ausgesetzt sind"* (Voskamp und Kipker 2013, S. 788). Das Bewusstsein, den (missbilligenden, wütenden, verachtenden, etc.) Blicken Anderer ungeschützt und wehrlos ausgesetzt zu sein, kann ein Gefühl der Scham hervorrufen. Scham ist in diesem Sinn *„ein regulativer Affekt",* der einen Anreiz liefern kann, sein eigenes Verhalten zu überdenken und zu modifizieren (Hilgers 2012, S. 17). Dieser Affekt entsteht in direkter (oder imaginärer) Interaktion oder Konfrontation und bedarf daher einer gewissen Publizität (Karstedt 1996, S. 23; vgl. auch Zabel 2011). Aber die Öffentlichkeit von Anschuldigungen induziert nicht nur Scham als Affekt, indem sie die wahrgenommenen Schwächen und Defekte einer Person sichtbar macht. Öffentlichkeit verstärkt auch den schmerzhaften Effekt von Scham: *„an insult, a look of contempt, a physical humiliation, an insult on one's character and standing, a rudeness is nearly always far more injurious when it is inflicted before an audience"* (Scott zitiert in Tankebe 2009, S. 249).

[13]Skoric et al. (2010, S. 189) und Powell (2015, S. 582 f.) stellen diesen Effekt jedoch in Frage.

[14]Obgleich sich dieser Zusammenhang nicht zwingend ergibt (vgl. Braithwaite 1989, 1993, 2000; HLRA 2003; Wall und Williams 2007; Skoric et al. 2010).

[15]vgl: https://www.duden.de/rechtschreibung/Pranger.

Die gezielte Verachtungsbekundung nimmt an einem „Internet-Pranger“ durch ihre Qualität bzw. Quantität besondere Ausmaße an (vgl. Voskamp und Kipker 2013, S. 788). Dabei stehen der Umfang des Beschämens und seine destruktive bzw. stigmatisierende Wirkung nicht immer im Verhältnis zur auslösenden Tat (vgl. z. B. Gottschalk 2014; Malone 2017).[16] Ronson (2015b) schreibt: *„It almost [feels] as if shamings [are] now happening for their own sake“*. Während die Reichweite eines Prangers zu früheren Zeiten begrenzt war, ist heute mithilfe moderner Medien und Techniken zudem eine weltweite virtuelle Anprangerung möglich (Baur et al. 2011, S. 131). Trottier (2017, S. 55) beschreibt die Sichtbarkeit, die durch digilante Aktivitäten produziert wird, als *„unwanted (the target is typically not soliciting publicity), intense (content like text, photos and videos can circulate to millions of users within a few days) and enduring (the vigilantism campaign may be top search item linked to the target, and even become a cultural reference).“* Dieser unerwünschten, intensiven und dauerhaften Sichtbarkeit, der TäterInnen durch den Prozess des öffentlichen Beschämens ausgesetzt werden, wird eine disziplinierende und Ordnung wiederherstellende Funktion zugeschrieben, eben weil sie eine Form der Sozialkontrolle darstellt, die die Freiheit und das Wohlbefinden der Person einschränken kann (Dunsby und Howes 2019, S. 5; vgl. auch Braithwaite 1989, 1993, 2000; Hilgers 2012; Trottier 2017).

Digilante Akteure machen sich den negativen Effekt einer öffentlichen Beschämung und das Unbehagen, welches sie auslöst, gezielt zunutze: *„Don’t*

[16]Ein Beispiel zur Illustration: In 2014 wurde die Videospieldesignerin Zoë Quinn zum Ziel massiver digilanter Attacken. Sie hatte sich von ihrem damaligen Freund getrennt, der sich daraufhin für die Zurückweisung an ihr rächte, indem er sie auf seinem Blog der Untreue bezichtigte (vgl. Malone 2017). Er beschuldigte sie u. a. mit einem einflussreichen Journalisten geschlafen zu haben, der dafür eine positive Rezension über ein von Quinn designtes Computerspiel geschrieben haben soll. Kurz nach Veröffentlichung der Anschuldigungen erhielt Quinn Nachrichten wie diese: *„If I ever see you are doing a pannel [sic] at an event I am going to, I will literally kill you. You are lower than shit and deserve to be hurt, maimed, killed, and finally graced with my piss on your rotting corpse a thousand times over“* (zitiert in Malone 2017). Hier geht es längst nicht mehr nur darum, einen vermeintlichen Normverletzer zu beschämen; die Nachrichten, die Quinn im Rahmen der digilanten Aktivitäten erhielt, gingen weit darüber hinaus: sie bedrohten Quinn in ihrer körperlichen Unversehrtheit und zielten darauf ab, ihr Angst einzujagen. In einem Interview mit *Boston Magazine,* sagte Quinns Ex-Freund später aus, er habe gewusst, er könne mit seiner Geschichte ein größeres Publikum innerhalb der Gaming-Community erreichen und habe diese Öffentlichkeit gezielt herstellen wollen, obgleich er die Wahrscheinlichkeit, dass Quinn nach seiner Veröffentlichung zum Ziel von Belästigungen und Drohungen werden würde auf ungefähr 80 % einschätzte (vgl. Jason 2015; Malone 2017).

let him have any feeling of anonymity or security. Rapists don't get the luxury of feeling comfortable"– mit diesen Worten erklärte z. B. ein Nutzer der Plattform Tumblr, warum er den Namen eines vermeintlichen Vergewaltigers mit seinem Posting publik machte (Young 2015). Die absichtlich herbeigeführte Öffentlichkeit im Rahmen digilanter Aktivitäten soll steuernd auf die vorgeführten Personen einwirken und sie psychisch zwingen, ein unerwünschtes, als abweichend erachtetes Verhalten zu unterlassen (vgl. Baur et al. 2011). Dies soll über den Effekt des Beschämens geschehen, denn das Erleben von Scham, so erklärt es der Psychologe Micha Hilgers (2012, S. 20), besitzt grundsätzlich einen negativen Charakter. Es geschieht aber auch dadurch, dass die Sichtbarkeit nicht symmetrisch ist: während die Zielpersonen mit Namen oder gar Abbild klar erkennbar wird, bleiben die digilanten Akteure i. d. R. hinter Pseudonymen und in der Anonymität versteckt.

Darüber hinaus dient die Sichtbarkeit dazu, die Außenseiterpositionen der TäterInnen symbolisch und öffentlichkeitswirksam zu manifestieren (Quent 2016a, S. 14). Ein Akt des Beschämens und Demütigens ist stets eine Ausübung von Macht; er stellt ein Sich-Erheben über denjenigen, der beschämt und gedemütigt wird, dar, und kommt somit einem Akt der Selbst-Aufwertung bzw. Selbst-Affirmation gleich (vgl. Kohm 2009, S. 198).[17] Dem Anderen wiederrum wird durch den herabwürdigenden Akt des Beschämens ein Dasein auf Augenhöhe verwehrt. Ihm wird „sein Gesicht genommen" und er wird in seinem sozialen Geltungsanspruch herabgesetzt (vgl. Zabel 2011; Hilgers 2012; Mallén 2016). Dies zeigt sich auch darin, dass sich beim Digilantismus immer wieder diskursive Strategien des „Othering" erkennen lassen, die dazu dienen, die Zielpersonen digilanter Taten als „nicht menschlich" zu etablieren, um die Gewalt bzw.

[17]Der Journalist, der Justine Saccos Tweet auf seinem Profil teilte und damit maßgeblich zur Eskalation der Situation beitrug, erklärte in einem Interview, es sei gerade ihr beruflicher Status gewesen, der ihr Fehlverhalten so delikat und in gewisser Weise „newsworthy" gemacht hätte: *„The fact that she was a PR chief made it delicious. It's satisfying to be able to say ‚OK, let's make a racist tweet by a senior IAC employee count this time.' And it did. I'd do it again"* (zitiert in Ronson 2015a, S. 78). Es ging ihm folglich nicht nur darum, den fragwürdigen Inhalt von Saccos Tweet zu problematisieren, sondern auch um die Gelegenheit, eine Person zu Fall zu bringen bzw. herabzuwürdigen, die zuvor eine bestimmte gesellschaftliche Position innehatte, welche sich durchaus als privilegiert bezeichnen ließe. Ronson (2015a) zeigt zudem auf, dass Missgunst oder Neid auf Saccos vermeintlich höheren sozialen Status oder ihren beruflichen Erfolg auch die Motivation einiger MitläuferInnen gewesen zu sein scheint, sich an ihrer öffentlichen Demütigung zu beteiligen.

Schädigung, die ihnen zugefügt werden soll, auf diese Weise zu rechtfertigen. Die Personen werden als „Monster“, „Scheusale“, „Abschaum“ oder als „(Raub-) Tiere“ bezeichnet – in jedem Fall aber als nicht zu der Gemeinschaft gehörig, die es zu schützen gilt (vgl. Kohm 2009; Schneider und Trottier 2012; Arvanitidis 2016). Durch diese „Dämonisierung“ und „Entmenschlichung“ verlieren die Personen spezifische Rechte und können damit auch gewaltsam behandelt werden (Schmidt-Lux 2018, S. 153; vgl. auch MacDonald 2014).

Problematisch ist dies nicht nur deswegen, weil Stigmatisierungen nicht allen Menschen gleichermaßen anhaften. Wie Goffmann (1963) in seinem Buch *Stigma: Über Techniken der Bewältigung beschädigter Identität* zeigt, greifen sie überwiegend bei jenen, die ohnehin schon marginalisiert oder machtlos sind (vgl. auch Salter 2017). Problematisch ist dies auch, weil eine stigmatisierende Beschämung, die der Person selbst angeheftet wird und nicht nur ihrem devianten Verhalten, sich mit ihrem Selbst verbinden kann, d. h., sie macht die Person in ihrer Identität dann aus (vgl. Wettlaufer 2015, S. 36). Eine solche Beschämung kann in der Folge desintegrativ wirken (vgl. Braithwaite 1989, 1993, 2000; Cheung 2014). Eine Reintegration der TäterInnen in die Gesellschaft kann durch diese Art der Beschämung erheblich erschwert werden und – im schlimmsten Falle – weitere Devianz hervorbringen (Cheung 2014). Darüber hinaus zeigen Studien zum strafenden Effekt von Beschämungen, dass dieser nur eintritt, wenn sich die Person, deren Schamgefühl hervorgerufen werden soll, auch mit den Werten und Normen der Gemeinschaft, die sie bloßstellt, identifiziert (vgl. Wettlaufer 2015, S. 36). Für Gemeinschaften, die sich durch einen eher flüchtigen Charakter auszeichnen, postuliert die *Harvard Law Review Association* (2003, S. 2194 ff.) hingegen, sie seien zu diffus und komplex, als das „shaming punishments“ effektiv funktionieren könnten (siehe auch Massaro 1991; Wettlaufer 2015). Eine empirische Analyse der Wirksamkeit von „shaming punishments“ im digitalen Kontext liegt bislang allerdings nicht vor.

5.6 Rechtfertigung(en)

Digilante Aktivitäten werden immer wieder über eine Rahmung als schützende Tat gerechtfertigt (Schmidt-Lux 2018, S. 152). Auf einer individuellen Ebene wird der digilante Akt als „das einzig Richtige“ aus Sicht des Akteurs erklärt, um die eigene Person verteidigen zu können (Moncada 2017, S. 408). Auf einer kommunalen Ebene rechtfertigen digilante Akteure ihre Handlungen damit, eine andere Person oder eine – wie auch immer definierte – „Gemeinschaft“ jetzt oder in der Zukunft vor einer Gefahr schützen zu wollen (Moncada 2017, S. 408; siehe

auch Powell 2015, S. 221; Dunsby und Howes 2019, S. 10). Hier stellt das öffentliche Anprangern von Normverletzern gleichsam eine Praktik dar, *„that reflect[s] a moral obligation for those with a sense of social responsibility“* (Dunsby und Howes 2019, S. 10; siehe auch Skoric et al. 2010, S. 195). In beiden Varianten soll der schützende Effekt durch ein „naming und shaming“ des Täters erzielt werden, welches als legitim angesehen wird, da es der „Gerechtigkeit“ dient. Eine mögliche Schädigung der Zielperson wird dabei billigend in Kauf genommen und lediglich als ein ausgleichendes Übel betrachtet (Schmidt-Lux 2018, S. 152 f.). Manchmal soll der schützende Effekt aber auch dadurch entstehen, dass die Veröffentlichung der Informationen zu einer Verhaltensänderung potenzieller „Opfer“ führt. Durch die Bekanntgabe bestimmter in der Vergangenheit liegender, sozial unerwünschter Verhaltensweisen sollen sich zukünftige „Opfer“ besser wappnen und sichernde Maßnahmen ergreifen können (vgl. Baur et al. 2011, S. 131).

Im April 2010 beispielsweise veröffentlichte eine Studentin der American University in den USA die Namen von zwei Kommilitonen auf ihrer Facebook-Seite und beschuldigte die beiden jungen Männer der Vergewaltigung:

> „ATTENTION WOMEN, we should all be aware! Stay away at all costs. They are predators and will show no remorse for anyone. If you have been effected [sic] by either one of these sickos please feel free to talk to me. With enough help we can take them down!“ (zitiert in Hess 2010).

Sie rechtfertigte ihre Entscheidung, die Anschuldigungen öffentlich zu machen, mit dem Wunsch Andere zu warnen: *„I felt like I needed to warn everyone else about these guys“* (zitiert in Hess 2010). Über Facebook erreichte sie mit einem Klick zeitgleich 986 ihrer Online-FreundInnen; diese wiederum konnten die Warnung teilen und sie an ihre jeweiligen Kontakte weiterleiten. Die Nachricht verbreitete sich rasant schnell. Auch die Bloggerin Sarah Wells, die die Namen der Personen öffentlich machte, die im Fall Megan Meier durch ihr Handeln den Suizid des gerade mal 13-jährigen Mädchens herbeigeführt hatten, rechtfertigte ihr Posting damit, es bestehe ein Interesse der Öffentlichkeit an dieser Information und sie wolle mit der Namensnennung die Gemeinschaft im weiteren Sinne schützen (vgl. Conan 2007).

Wie auch im klassischen Vigilantismus verbindet sich diese Form der Legitimation von Digilantismus *„häufig mit dem Verweis darauf, dass die eigentlich für den Schutz zuständige Instanz, nämlich der Staat, diesen Schutz nicht oder nicht mehr gewährleistet“* (Schmidt-Lux 2018, S. 152; siehe auch Silke 2001, S. 126; Kowalewski 2002, S. 428). Entweder setzt der Rechtstaat vorhandene Regeln aus

Sicht der Vigilanten nicht effektiv um oder ein nicht durch den Staat reguliertes Verhalten wird aus Sicht der Handelnden als Rechtsbruch angesehen (Rüdiger und Bayerl 2018, S. 281). Aus diesem Grund wird es aus Sicht der digilanten Akteure erforderlich, das Recht in die eigenen Hände zu nehmen, denn sie fühlen sich allein gelassen bzw. auf sich selbst gestellt (Schmidt-Lux 2018, S. 149). Es ist ein wiederkehrendes Muster, dass Digilantismus in Situationen entsteht, in denen ein sicherheitsbedürftiger Bürger auf einen Rechtsstaat trifft, der nicht präsent oder nicht handlungsfähig (bzw. -willig) erscheint (vgl. Silke 2001; Rüdiger 2017). Wahrgenommene Sicherheitsdefizite sowie eine wahrgenommene Untätigkeit oder Ineffektivität bei der Rechtsdurchsetzung werden regelmäßig zur *raison d'être* digilanter Akteure erklärt (Campbell 2015, S. 353). Hinzu kommt ein vermeintliches Fehlen von Verfahrensgerechtigkeit (vgl. Tankebe 2009).

Auch hier zwei Fallbeispiele: Im April 2018 wird bereits zum dritten Mal in diesem Jahr in ein Restaurant in Magdeburg eingebrochen (Ellrich 2018). Die ersten beiden Male hat der Betreiber noch die Polizei alarmiert. Dieses Mal jedoch entscheidet er sich dafür, Videoaufnahmen seiner Überwachungskameras im Internet zu veröffentlichen und die Öffentlichkeit bei der Identifizierung der Täter um Hilfe zu bitten: *„Für die Bekanntgabe, wer unser nächtlicher Besucher ist, gibt es eine Belohnung"* (zitiert in Ellrich 2018). Auf Nachfrage begründet der Betreiber seine Entscheidung damit, dass er sich von der Polizei allein gelassen fühlt hat: er habe die beiden Male zuvor vergeblich auf eine Rückmeldung gewartet (Ellrich 2018). Eine ähnliche Rechtfertigung findet sich in dem Vergewaltigungsfall aus Steubenville in den USA, der von einer britischen Feministin auch als *„Abu Ghraib der Rape Culture"* tituliert wurde (Penny 2013). Hier war ebenfalls eine konstatierte Untätigkeit des Staates bzw. seiner Rechtsdurchsetzungsorgane der Auslöser für die digilanten Handlungen einer Bloggerin, die mit ihren Postings für eine breite Medienöffentlichkeit sorgte und den Fall erst richtig ins Rollen brachte: in einem Interview gab sie an, das „Beweismaterial" deshalb zusammengetragen zu haben, weil sie davon ausgegangen sei, die Polizei würde nicht akribisch genug suchen (Süddeutsche Zeitung 2013; vgl. auch Levy 2013).

In diesem Sinne ist Digilantismus ein kommunikativer Akt, der Aufschluss über wahrgenommene Missstände oder Ungerechtigkeiten bei der formellen Rechtsdurchsetzung gibt (vgl. Quent 2016a, 2016b). *„Wenn Vertrauen und Verlässlichkeit schaffende Ordnungskonzepte brüchig werden, dann wachsen Schutzbedürfnisse und die individuelle wie kollektive Wehrbereitschaft",* schreibt Hitzler (1993, S. 19). Es ist aber nicht bloß ein tatsächliches oder vermeintliches „Versagen" der Polizei oder Justiz, welches zum Entstehen von Digilantismus beitragen kann. Eine Studentin der Columbia University in New York, die 2015

öffentlich einen Kommilitonen der Vergewaltigung bezichtigte, erklärte: *„I went public with my story because I wanted to show the world how flawed the college process for handling cases of sexual assault is“* (zitiert in Ryan 2015). Der Kommilitone war zuvor nach einer universitätsinternen Untersuchung von den Vorwürfen freigesprochen worden (vgl. Ryan 2015). Der Fall zeigt, dass auch als unfair oder ungerecht wahrgenommene Entscheidungen anderer Kontrollorgane digilante Aktivitäten auslösen können. Außerdem spielen empfundene Spannungen innerhalb einer sich verändernden Gesellschaft eine Rolle. Sowohl Vigilantismus als auch Digilantismus treten häufig entlang sog. „social fissure lines“ auf, d. h. dort wo es um Themen wie Religion, Ethnizität, Gender, Sexualität, etc. geht, denn neue Überzeugungen und/oder Verhaltensweisen in diesen Bereichen können zu Stör-, Bedrohungs- oder Frustrationsgefühlen bei (Teilen) der Bevölkerung führen (Kowalewski 2002, S. 429; vgl. auch MacDonald 2014). *„[D]igital vigilantism is tapping into, and identifies with an affective mood of public frustration and concern“*, beobachtet Campbell (2015, S. 353). Als Antwort auf diese affektiven (Ver-)stimmungen reagieren digilante Akteure dann *„[by] acting in a way they believe the state should“* (Trottier 2017, S. 63). Digitaler Vigilantismus wird zu einem diskursiven *„flashpoint upon which moral boundaries may be formed and reformed“* (Mallén 2016, S. 15).

Gerade bei Normverletzungen, die im Internet und unter Verwendung sozialer Technologien geschehen, ist es nicht leicht, eine Ahndung für die Nutzer spürbar und Kontrollinstanzen sichtbar werden zu lassen (vgl. Rüdiger 2017; Rüdiger und Bayerl 2018). Dafür gibt es verschiedene Gründe, von denen hier nur einige beispielhaft angeführt werden sollen. Da ist zum einen, dass das Internet als ein „virtueller“ Raum, der zeitliche und geografische Grenzen überwindet, die staatlichen Strafverfolgungsbehörden immer wieder vor neue Herausforderungen stellt: so, z. B. greifen nationale Anstrengungen zur Normenregulierung in einem solchen, globalen Raum nur bedingt (Rüdiger 2017, S. 217; vgl. ebenso Katyal 2001, S. 1091 f.; Juliano 2012, S. 57; Rose und Fox 2014, S. 787). Hier ist besonders hervorzuheben, dass es kulturelle und linguistische Unterschiede bei der Definition bestimmter Phänomene zwischen Ländern gibt (Wall und Williams 2007, S. 401; siehe auch Robertz et al. 2016). Auch die juristischen Zuständigkeiten (Zivilrecht? Strafrecht?) können differieren (Wall und Williams 2007, S. 401). Die grenzübergreifende Struktur des Internets macht es also problematisch, Online-Materialien und Handlungen durch die Gesetzgebung zu kontrollieren (Robertz et al. 2016, S. 9). Computertechnologien entwickeln sich außerdem schnell (weiter), was es den Ermittlungsbehörden und der Justiz schwermachen kann, Schritt zu halten (Nhan et al. 2017, S. 343; siehe auch Wall und Williams 2007, S. 400; Brodowski und Freiling 2011, S. 15). Und selbst

wenn entsprechende (Straf-)Gesetze existieren und Anwendung finden, so lassen sie sich faktisch nicht immer erfolgreich bzw. für private BürgerInnen spür- oder sichtbar implementieren (Brodowski und Freiling 2011, S. 93; Rüdiger 2017, S. 229; vgl. auch McCarthy 2014; Rüdiger und Bayerl 2018). Um jeden Verstoß zu ahnden, fehlen den Strafverfolgungsbehörden oftmals die personellen und finanziellen Ressourcen oder schlichtweg das technische Knowhow (Noble 2017).

Darüber hinaus können die Möglichkeiten TäterInnen zur Rechenschaft zu ziehen auch deshalb begrenzt bleiben, weil diese nicht unter ihrem Klarnamen sondern anonym handeln (vgl. McCarthy 2014; Hess 2010). Verwendete Identitäten müssen in keinem Zusammenhang mit der realen Identität eines Nutzers stehen, was die Zuordnung einer schädigenden oder illegalen Aktivität zu einer Person mindestens schwierig gestaltet (Brodowski und Freiling 2011, S. 55). Nutzer beschreiben zudem immer wieder Desinteresse, Verharmlosung und fehlendes Verständnis aufseiten der Polizei, was davon zeugt, dass nach wie vor zwischen bloß „virtuellen" Ereignissen und Ereignissen im „echten" Leben unterschieden wird (Salter 2017, S. 18, 154; siehe auch Hess 2010; BITKOM Studie 2017).[18] Schließlich stellt es für die Polizei noch eine Herausforderung dar, in den Sozialen Medien die Deutungshoheit bei Kriminalitätsereignissen zu bewahren und Kontrolle über ihre diskursive Rahmung sowie Wahrnehmung innerhalb der Gesellschaft auszuüben (vgl. Schneider und Trottier 2012). Wie Trottier (2017, S. 62) hervorhebt, können Online-Plattformen wie *Reddit* oder auch Facebook eine entscheidende Rolle dabei spielen, das Vertrauen der Öffentlichkeit in die ordnungssichernde Fähigkeit des Staates zu erodieren, weil sie es schwieriger machen, Informationsflüsse bei Kriminalitätsereignissen effektiv zu managen.

Derzeit versucht die Bundesregierung die Betreiber sozialer Netzwerke, wie Facebook oder Twitter, stärker in die Verantwortung zu nehmen und mit Maßnahmen wie dem Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen

[18]In einer Umfrage des *Pew Research Center* (Duggan 2017) gaben 43 % der befragten US-Amerikaner (n = 4248) an, die staatlichen Strafverfolgungsbehörden nähmen Vorfälle von Online-Belästigungen („harassment") derzeit nicht ernst genug. Der Begriff „harassment" umfasste in der Studie folgende Handlungen: *„offensive name-calling", „purposeful embarassment", „physical threats", „sustained harassment", „stalking"* und *„sexual harassment"*. Eine repräsentative Befragung von 1017 Internetnutzern ab 14 Jahren im Auftrag des Digitalverbands Bitkom für das Jahr 2017 zeigt, dass etwa 13 % der Opfer von Cybercrime sagen, Polizei und Staatsanwaltschaft nähmen Cybercrime nicht ernst. 12 % gaben zudem an, sie seien sich nicht sicher, ob ihr Fall überhaupt von den Behörden verfolgt würde. 8 % glaubten, die Ermittler würden sich mit dem Thema schlicht nicht auskennen.

Netzwerken (NetzDG) das Vorgehen gegen Hass und Hetze im Netz zu privatisieren.[19] Wenn staatliche Institutionen einen privaten Anbieter zu quasi hoheitsstaatlichen Aufgaben aufrufen, dann kann allerdings ebenfalls der Eindruck erweckt (oder auch verstärkt) werden, der Staat – und insbesondere die Justiz – sähe sich nicht in der Lage, selbst erfolgreich gegen entsprechende Taten im Internet vorzugehen (Rüdiger 2017, S. 229). Der Staat kann auch hier als nicht leistungsfähig oder überfordert erscheinen. Davon abgesehen ist das zugrunde liegende Problem mit einer teilweisen Abgabe der Verantwortung längst nicht gelöst, denn die Medienunternehmen tun sich ebenfalls schwer mit ihren Selbstkontrollmechanismen Normverstöße ausreichend zu unterbinden – vor allen Dingen, weil sie versuchen müssen eine Balance zu finden, zwischen der Sicherheit ihrer Nutzer und den Idealen freier demokratischer Meinungsäußerung und Selbstregulierung für die das Internet steht (vgl. Keller 2015; Tiku und Newton 2015).

Mittlerweile können Nutzer Inhalte, die ihrer Meinung nach gegen Gemeinschaftsstandards verstoßen, dem Netzwerk melden (Twitter hat z. B. einen „Missbrauch-melden"-Button). Die Betreiber der Netzwerke können (oder, in besonderen Fällen, müssen) dann die entsprechenden Inhalte löschen oder stumm schalten und/oder die Verfasser blockieren. Um gegen online basierte Hassrede vorzugehen, gibt es zudem seit 2017 zumindest in NRW eine Initiative mit dem Namen *„Verfolgen statt nur Löschen – Rechtsdurchsetzung im Internet"*. Ziel der Initiative ist es, „eine effektive Strafverfolgung im Netz zu gewährleisten und so der zunehmenden Verrohung der Netzkommunikation entgegenzutreten" (Landesanstalt für Medien NRW 2018). Dabei verfolgen die Initiatoren einen generalpräventiven Ansatz: Strafbare Äußerungen sollen nicht nur gelöscht, sondern die Verfasser auch im Online-Umfeld konsequent zur Verantwortung gezogen werden (Landesanstalt für Medien NRW 2018). Insbesondere wenn es um Phänomene wie Stalking, Mobbing oder sexuelle Belästigungen im Netz geht, werden die zur Verfügung stehenden Maßnahmen aber trotz aller Bemühungen noch oft von den Betroffenen als mangelhaft empfunden (Salter 2017, S. 18; vgl. auch Ipsos-Mori 2017; Duggan 2017; Noble 2017; Jane 2017).

Eine Erklärung dafür ist, dass die Übergänge von sozial anerkanntem Verhalten über lästige Erscheinungen bis hin zu kriminellen Verhaltensweisen i. d. R. fließend und situationsbezogen beurteilt werden (Brodowski und Freiling 2011, S. 93). Es kann schwierig sein einzuschätzen, wann eine online geäußerte Bedrohung glaubwürdig ist oder ein geschriebener Kommentar einen direkten

[19]Vgl: https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html. Zugegriffen: 12. Februar 2019.

Angriff darstellt, der eine rechtsstaatliche Intervention zwingend erforderlich macht. Ein Beispiel: Haben sich z. B. auf einer bestimmten Internetplattform raue Umgangsformen entwickelt und werden dort zwischen den Beteiligten dieser Plattform den Umgangsformen entsprechende Äußerungen regelmäßig getätigt, dann muss eine Beleidigung nicht zwingend den Ehrbegriff der §§ 185 ff. StGB verletzen, selbst wenn der Ausdruck in anderen Situationen durchaus als Ausdruck der Missachtung oder Nichtachtung verstanden werden könnte (Brodowski und Freiling 2011, S. 102). Die Voraussetzungen für eine strafrechtliche Reaktion sind dann nicht gegeben, was für die betroffenen Personen nicht immer nachvollziehbar sein kann.

Vertrauen in die Institutionen und ihre ordnungssichernden Fähigkeiten wird als unabdingbar für die Legitimität eines Rechtsstaates angesehen (vgl. Tyler 2006; Rose und Fox 2014). Für die Aufrechterhaltung der Ordnung einer demokratischen Gesellschaft ist es wichtig, dass die BürgerInnen dem Staat (und insbesondere der Justiz) zutrauen, mit wahrgenommenen Bedrohungen effizient und fair umzugehen (vgl. Abrahams 1998; Quent 2016a; Schmidt-Lux 2018). Aufgrund der Problematik seiner Kontrollierbarkeit und einer gefühlten Machtlosigkeit gegenüber bestimmten Formen der Devianz wird das Internet jedoch häufig als ein „rechtsfreier“ oder „gesetzloser“ Raum beschrieben bzw. wahrgenommen. Manche AutorInnen sprechen – anknüpfend an die *frontier*-Mythologie Amerikas, dem „Heimatland“ des Vigilantismus – vom Internet auch als *„Wild West Web“* (Keller 2015) oder *„digitalem Wilden Westen“* (McLure 2000; Martin 2007). Genau dieser nicht bzw. noch nicht ausreichend regulierte Raum bietet laut Rose und Fox (2014, S. 787) ideale Bedingungen für das Aufkommen von Digilantismus, denn dort, wo Ordnungsmacht weitestgehend unsichtbar bleibt und Normbrüche nicht spürbar geahndet werden, fühlen sich digilante Akteure geradezu dazu berufen, anstelle des Staates zu handeln und selbst für ihre Sicherheit zu sorgen (vgl. auch Katyal 2001; Arvanitidis 2016; Rüdiger 2017; Noble 2017; Salter 2017; Schmidt-Lux 2018). Im Internet bedeutet dies, dass sie entweder ihre eigenen Regularien in Form einer sog. „Netiquette“ entwickeln oder auf Grenzüberschreitungen mit der Etablierung von Selbstjustizgruppen oder – handlungen reagieren (vgl. Rüdiger und Bayerl 2018, S. 280).

5.7 Verhältnis zum Staat

Der Anspruch auf die Monopolisierung von Gewalt und von (gewaltsamer) Bestrafung ist ein zentraler Pfeiler moderner Staatlichkeit (Schmidt-Lux 2018, S. 146). Der Staat beansprucht für sich die Kompetenz, Gewalt gegen seine

BürgerInnen anzuwenden, um (vermeintliche) Verstöße gegen staatliche Normen zu ahnden (Winter 2003, S. 519). Nach Webers berühmter Definition zeichnet sich ein vollwertiger Staat gerade durch diese monopolisierte Gewaltkompetenz aus (Winter 2003, S. 519). Private Gewalt ist verboten; nur der Staat und seine für diesen Zweck eingerichteten Organisationen – und hier an erster Stelle: die Polizei – sind für ihre Ausübung legitimiert, denn ihre Kontrollierbarkeit und Dosierbarkeit stehen im Vordergrund (Winter 2003, S. 519, 520). Wenn vigilante Akteure Gewalt anwenden, um das abweichende Verhalten anderer zu ahnden, dann beanspruchen sie also eine Kernkompetenz moderner Staaten, *ohne* selbst staatliche Akteure zu sein (Silke 2001, S. 126; Schmidt-Lux 2013, S. 103). Sie agieren quasi-staatlich und fordern damit den Staat heraus, denn in gewisser Weise stellt ihr Handeln eine Infragestellung seiner Fähigkeit, für Recht und Ordnung sorgen zu können, dar (Schmidt-Lux 2013, S. 103; siehe auch Quent 2016a, S. 3). Das Auftauchen von Vigilantismus indiziert eine Art Vertrauensverlust in den Staat und lässt sich, wie eben dargelegt, als ein Misstrauensvotum in seine Effizienz begreifen (Hitzler 1993, S. 16; Quent 2016a, S. 9). Nicht zuletzt deshalb ist das Verhältnis zwischen Staat und digilanten Akteuren von Ambivalenz geprägt. Und obgleich Vigilantismus eine Form der Status-quo-orientierten bzw. -erhaltenden Gewalt darstellt, wird er oftmals als antagonistisch zum Staat und seinen Institutionen wahrgenommen (vgl. Arfsten 2012; Schmidt-Lux 2013, 2018).

Für Johnston (1996) ist es ein charakteristisches und vor allen Dingen auch entscheidendes Merkmal von Vigilantismus, dass die Akteure autonom, d. h. ohne (expliziten oder impliziten) staatlichen Auftrag und oft sogar ausdrücklichen Warnungen von Polizei und Justiz zum Trotz, handeln (vgl. Johnston 1996, 2001; Quent 2016a). Es sind nur diese Formen „autonomer“ bzw. „aktiver Bürgerschaft“, die er als Vigilantismus klassifiziert. Aus seiner Sicht können Polizeibeamte deshalb z. B. niemals Vigilanten sein, denn sie können sich nicht von ihrer Rolle lösen, als „private Personen“ auftreten und wahrhaft unabhängig vom Staat agieren:

> „the notion that one should define off-duty police officers as ‚private persons‘ is a peculiar one since, whether on duty or not, they continue to enjoy full police powers. In that respect, their off-duty actions cannot be demarcated from their public status, functions, and responsibilities.“ (Johnston 1996, S. 224; anders siehe Kotecha und Walker 1976; Kowalewski 2002; Dumsday 2009)

Die Diskussion um das digilante Handeln Ariane Friedrichs unterstreicht Johnstons Interpretation. Als die Hochspringerin den Mann, von dem sie annahm, er hätte ihr die anzüglichen Nachrichten über Facebook gesendet, öffentlich an den

Pranger stellte, wurde ihr Handeln auch deshalb so kontrovers diskutiert, weil sie eine ausgebildete Polizeikommissarin ist (vgl. Lichtenberg 2012; DIE ZEIT 2013). Für viele schien ihre Entscheidung, den Mann in den Sozialen Medien bloßzustellen, im Widerspruch zu ihrer Rolle als Polizistin – und somit Repräsentantin des Rechtstaates – zu stehen.

Im Kontext von Digilantismus lässt sich Johnstons Differenzierung allerdings nicht mehr so leicht aufrechterhalten. Trottier (2017, S. 58) stellt fest: Manche digilanten Akteure seien selbst-autorisiert und handelten autonom, andere wiederum *„may (indirectly) inform police and state actions"*. Angesichts der zunehmenden Dezentralisierung und Privatisierung staatlicher Kontrollaufgaben, die sich in westlichen Gesellschaften in den letzten Jahrzehnten im Rahmen des sog. „neoliberal turn" beobachten lässt, fällt eine strikte konzeptionelle Trennung zwischen autonomer und responsibilisierter Bürgerschaft, d. h. zwischen unabhängigem und staatlich unterstütztem Handeln, zunehmend schwer (vgl. MacDonald 2014). Der Sozial- und Rechtsstaat zieht sich nämlich immer mehr von seinen Kernaufgaben zurück (Quent 2016a, S. 10). Private BürgerInnen werden im Zuge dieses Wandels hingegen immer öfter (bzw. wieder vermehrt, vgl. Zedner 2006) in klassische Aufgaben des Polizierens eingebunden. Sicherheitspartnerschaften sind hierfür ein Beispiel. Pluralisierte Formen der sozialen Kontrolle und Intervention bilden heute eine Art *„crime control assemblage"*, durch die Kriminalität und Devianz „aus-der-Distanz" regiert werden (vgl. Yar 2012). In diesen Formationen verbinden sich private Aktivitäten zur Sicherheitsherstellung verstärkt mit denen der staatlichen Rechtsdurchsetzungsorgane: *„[they] connect and align with existing networks of authorized and legitimate policing provision"* (Campbell 2015, S. 347). Die britische Kriminologin Jessica Evans (2003, S. 165) argumentierte deshalb jüngst, eine strikte Trennung zwischen unabhängiger Selbsthilfe privater Bürger in Form von Vigilantismus und staatlich begrüßter – oder zumindest geduldeter – Selbsthilfe in Form von Vigilanz, d. h. Wachsamkeit gegenüber potenziellen Bedrohungen, sei nicht länger sinnvoll. Ähnlich konzedieren Smallridge et al. (2016, S. 63): *„individuals and groups can potentially drift between vigilantism and proactive citizenship"*.

Die Ergebnisse einer Studie zu „naming and shaming" Aktivitäten in den Sozialen Medien während der gewaltsamen Ausschreitungen nach einem Eishockeyspiel in Vancouver im Sommer 2011 stützen Evans Einschätzung. Sie zeigen, dass die digilanten Akteure in diesem Fall *„ultimately supportive of the state"* waren und die staatliche Durchsetzung von Recht und Ordnung überwiegend befürworteten (Schneider und Trottier 2012, S. 63). Sie wollten den Staat keinesfalls abschaffen oder entmachten; sie wollten ihm vielmehr temporär bei der Ausübung seiner Schutzaufgaben helfen. Ähnliches ließ sich auch in

Boston nach den Anschlägen beim Marathon 2013 beobachten: eine signifikante Anzahl an Postings von Nutzern der Online-Plattform *Reddit,* die sich in einem eigens kreierten Forum darum bemühten, die Attentäter zu identifizieren, zeugte davon, dass die digilanten Akteure die laufenden Ermittlungen der offiziellen Rechtsdurchsetzungsorgane lediglich unterstützen wollten (Nhan et al. 2017, S. 342; vgl. auch Arfsten 2018). Sie verstanden sich nicht als Kritiker oder Gegner des Staates, sondern positionierten sich diskursiv als seine zivilen und wachsamen Partner bei der Aufklärung eines furchtbaren Verbrechens. In Zeiten, in denen private BürgerInnen zunehmend in die Verantwortung genommen und über staatliche Responsibilisierungsdiskurse in die Herstellung von Sicherheit eingebunden werden, rahmten sie ihre Tätigkeiten als eine natürliche Reaktion guter und besorgter BürgerInnen, die es, angesichts der außergewöhnlichen und bedrohlichen Situation, als ihre Aufgabe ansahen, dem Staat unter die Arme zu greifen.

Weiterhin zeigt das eingangs angeführte Beispiel aus Hamburg, dass manche Digilanten sich durch offizielle Fahndungsaufrufe in den Sozialen Medien ermutigt fühlen können, quasi-polizeilich zu handeln (siehe auch Schneider und Trottier 2012, S. 69; Rose und Fox 2014, S. 787; Dunsby und Howes 2019, S. 15). Durch die Bitte um Mithilfe bei der Aufklärung von Straftaten können sie sich aufgefordert fühlen, eigenständig investigative Tätigkeiten vorzunehmen (vgl. Trottier 2017). Ihre Narrative weisen deshalb auch nicht selten Konsistenten mit denen staatlicher Akteure auf. Viele ihrer Vorgehensweisen ähneln zudem jenen von Polizeibeamten während ihrer Ermittlungen (Schneider und Trottier 2012, S. 62). Wie Salter (2017, S. 231) beschreibt, lassen digilante Akteure sich bis zu einem gewissen Grad von den offiziellen Strafverfolgungsbehörden in ihrem Handeln inspirieren und imitieren sie sogar. Insbesondere in organisierter Form demonstrieren digilante Gruppierungen immer wieder, dass sie die rechtlichen Grundlagen und Grenzen ihres Handelns kennen und mit Prozessen der offiziellen Strafverfolgung und Kriminalitätsaufklärung vertraut sind (vgl. Huey et al. 2012; Campbell 2015). Der Gründer von *Judge Beauce,* einer digilanten Organisation aus Kanada, deren Mission es ist, vermeintliche Pädophile zu identifizieren und bloßzustellen, argumentiert deswegen, er und seine KollegInnen agierten nicht außerjustiziell, sondern als *„extension of the law“* (Myles und Trottier 2017, S. 1).

Manche digilanten Akteure kooperieren tatsächlich offen mit anerkannten Medienanstalten, um vermeintliche TäterInnen öffentlichkeitswirksam bloßzustellen und sie dann an die Polizei zu übergeben (vgl. Leonard und Morin 2002; Straziuso 2004; Stengel 2018); andere wiederum kooperieren (mehr oder weniger offiziell) direkt mit lokalen Polizeibehörden. Sie bieten den Ermittlern z. B.

freiwillig ihre Dienste oder ihr Wissen als kulturelles Kapital im Bourdieuschen Sinne an (vgl. Huey et al. 2012). Altheide (2004, S. 239) zufolge gilt: *„Police officers may decry such cyber-vigilantism, but they enlist the help of the public routinely.“* Milivojevic und McGovern (2014, S. 29) betonen darüber hinaus, dass die Reichweite Sozialer Medien ein enormes Potenzial für die Strafverfolgungsbehörden birgt: *„global connectivity is unprecedented and law enforcement can tap into this knowledge pool to find vital information.“* Ähnlich argumentieren Huey et al. (2012, S. 95), *„the general public can be a vital partner in the provision of security online“* obgleich sie derzeit noch *„a much-undervalued nodal cluster in the cyber-space security network“* darstellt.

Auch aktuelle Debatten über sog. „crowdsourced policing“ zeigen, dass zumindest den investigativ-kontrollierenden Tätigkeiten von digilanten Akteuren eine gewisse Legitimität zugesprochen wird. Dies ist insbesondere dann der Fall, wenn ihre Ziele und politischen Diskurse weitestgehend mit denen der staatlichen Institutionen übereinstimmen, denn dann können digilante Aktivitäten nichtstaatlicher Akteure durchaus eine Reihe instrumenteller (und variabler) Zwecke für den Staat erfüllen – gerade auch, weil sie nicht denselben rechtsstaatlichen Limitierungen unterliegen oder Anforderungen genügen müssen (Moncada 2017, S. 414). Aufgrund dieser Beobachtungen kommt Trottier (2017, S. 63) zu dem Schluss: *„While both DV [digital vigilantism] and conventional vigilantism are typically framed as a critical response against the state, DV's relation to a given state's socio-political climate is more complex.“* Und im Anschluss an Moncada (2017, S. 413) lässt sich festhalten: *„the nature and extent of state involvement in vigilantism can vary across both time and space.“* Digilantismus muss nicht zwingend in einem antagonistischen Verhältnis zum Staat und seinen Akteuren stehen bzw. durch die von Johnston (1996) geforderte Autonomität privater Akteure gekennzeichnet sein.

5.8 Motive

Der Kriminologe Steven Kohm erklärt die Beteiligung an digilanten Aktivitäten mit einem Bedürfnis nach Rache: *„People are yearning to reconnect with the punitive emotional core of the justice system“* (zitiert in Zadrozny 2019). Rache ist ein klassisches Motiv für die Ausübung von Selbstjustiz. Sie wird ausgelöst von einem Impuls *„sich für eine körperliche oder seelische Verletzung, eine persönliche Kränkung, ein Unrecht, einen ungerechtfertigten Angriff, eine Herabsetzung oder eine Beleidigung an ihrem (oder seinem) Urheber rächen zu wollen“* (Paul 2005, S. 240; vgl. auch Tripp et al. 2007). Allerdings geht es

den selbstjustizierenden Akteuren nicht immer darum, einen digitalen Gegenschlag auszuführen, der ein wahrgenommenes Unrecht vergelten und wieder ausgleichen soll. In der einschlägigen Literatur sowie in Fallbeispielen aus den Medien lässt sich noch eine ganze Reihe anderer Motive für digitalen Vigilantismus finden (vgl. z. B. Huey et al. 2012, S. 89; Yardley et al. 2018, S. 97 f.). Diese Motive lassen sich grob zu folgenden Kategorien zusammenfassen: 1) Suche nach Gerechtigkeit; 2) ein Wunsch, wahrgenommene Ungerechtigkeiten oder Mängel im System aufzuzeigen und eine Änderung herbeizuführen; 3) Katharsis; 4) Empowerment; 5) Entertainment und 6) ein Streben nach Aufmerksamkeit bzw. Geltungsdrang. Insbesondere die letzten beiden Motive sind eng verbunden mit der algorithmischen Logik und dem besonderen technischen Design Sozialer Medien, sowie heute vorherrschenden Medienkulturen (vgl. bspw. Franck 2019). Eine Unterscheidung zwischen Rechtfertigungen bzw. Legitimationsmustern digilanter Akteure und ihren Motiven ist sinnvoll, da die Gründe, warum sie auf außerjustizielle Strategien rekurrieren, um Normverstöße zu ahnden, nicht unbedingt deckungsgleich sein müssen, mit denen, die sie öffentlich – z. B. gegenüber Medienvertretern oder staatlichen Akteuren – äußern (Moncada 2017, S. 408). Motive sind *„fluid, dynamic and not necessarily readable off of the justification“,* schreibt Moncada (2017, S. 408). Hervorzuheben ist außerdem, dass das Vorliegen eines Motivs ein anderes nicht ausschließt; mehrere Motive können gleichzeitig präsent und miteinander verflochten sein.

5.8.1 Suche nach Gerechtigkeit und Bedürfnis nach Normenanpassung

Neben dem Wunsch nach Rache wird hauptsächlich die Suche nach Gerechtigkeit als ein Motiv für digilante Aktivitäten angeführt (vgl. Schneider und Trottier 2012; Rose und Fox 2014; Powell et al. 2018). Hier können im Wesentlichen zwei Faktoren eine Rolle spielen: erstens, die Einschätzung der digilanten Akteure, dass das von ihnen als abweichend wahrgenommene Verhalten auf offiziellem Wege überhaupt durch ein faires Verfahren einer Strafe zugeführt wird und zweitens, die Schwere der zu erwartenden Strafe. Glauben die Akteure, ihr Anliegen würde offiziell nicht verfolgt (beispielsweise, weil ein wahrgenommenes Unrecht nicht unter Strafe steht wie im Fall Sigi Maurer, vgl. SPIEGEL 2018), ein Verfahren würde nicht fair verlaufen oder eine Strafe würde schlussendlich zu gering ausfallen, erscheint es ihnen womöglich zielführender, das Recht in die eigenen Hände zu nehmen und selbst für ausgleichende Gerechtigkeit zu sorgen (vgl. Tripp et al. 2007; Keller 2015).

Manchmal wird die Suche nach Gerechtigkeit aber auch diskursiv mit einem Wunsch, Ungerechtigkeiten oder Mängel im System als solches aufzuzeigen und

zu beseitigen, verbunden. In diesem Fall können digilante Aktivitäten von Personen ausgehen, die am sachlichen Kern einer auslösenden Tat interessiert sind und die Ursache dafür in gesellschaftlichen Missständen oder durch Machtverhältnisse reproduzierten Ungleichheitsbeziehungen sehen, die sie adressieren und gegen die sie vorgehen wollen.[20] Sie schließen sich digilanten Bewegungen an, weil sie etwas Gutes tun und für ein Thema, z. B. die Anerkennung von Opfern sexualisierter Gewalt, die Öffentlichkeit mobilisieren oder zumindest sensibilisieren wollen (vgl. Jane 2017; Powell und Henry 2017). Die Suche nach Gerechtigkeit ist ein Motiv, welches sich oftmals auch in den begleitenden Hashtags eines Postings ablesen lässt: #justiceforsarah oder #justiceforjill steht dort dann beispielsweise (vgl. Powell et al. 2018, S. 150).

Mit ihrem Handeln zeigen die digilanten Akteure in beiden Fällen zumindest bei ihnen selbst ein vorhandenes Interesse an einer staatlichen Normenregulierung bzw. angepassten Normenkontrolle auf (vgl. Rüdiger und Bayerl 2018, S. 281). Nicht selten sind sie bereits selbst, oder eine ihnen nahestehende Person, einmal Opfer einer ähnlichen Tat geworden oder haben Erfahrungen mit Unterdrückung, Diskriminierung und/oder Hass gemacht (vgl. Levy 2013; Kushner 2013, 2014; Keller 2015; Yardley et al. 2018). Nun versuchen sie, durch einen öffentlich aufgebauten Druck die Politik zu verschärfter Gesetzgebung anzuregen oder Vertreter der Ordnungsmacht zu einem härteren Durchgreifen zu animieren (Dunsby und Howes 2019, S. 14; Arvanitidis 2016, S. 10). Nach Quent (2016a, S. 14) ließe sich Digilantismus in diesem Kontext deshalb auch als eine *„Form des unkonventionellen Protestes“* verstehen. Powell et al. (2018, S. 143 ff.) bezeichnen ihn als eine Form von politischem Aktivismus (ähnlich siehe auch Phillips 2017); und Fileborn (2014, S. 32) sieht in ihm einen *„informal justice mechanism“* (vgl. auch Powell 2015).

5.8.2 Katharsis

Ein drittes Motiv für digilante Aktivitäten kann ihre kathartische Wirkung sein. Als Beispiele hierfür können Fälle angesehen werden, in denen digilante Akteure handeln, um ihren eigenen Gefühlen Ausdruck zu verleihen oder Erfahrungen

[20] In der Diskussion um das politische Moment und partizipatorische oder demokratisierende Potenzial von Digilantismus wirft Campbell (2015, S. 351) allerdings zurecht die Frage auf, inwieweit dialogische Praktiken, die ihre kommunikative Wirkung über die Provokation von Reaktionen wie Angst, Ekel, Schock oder Wut entfalten, und Akte öffentlicher Demütigung zur Abschreckung nutzen, tatsächlich die Art Dialog hervorbringen können, *„which move[s] justice (or policing) forward“*.

kollektiv zu verarbeiten (vgl. Martin 2007; Kohm 2009; Skoric et al. 2010; Powell 2015; Powell et al. 2018). Nach dem Mord an Jill Meagher in Sydney, Australien, im Jahr 2012 untersuchten Powell, Overington und Hamilton (2017, S. 14) die öffentliche Kommunikation zu dem Fall bei Twitter und stellten fest, dass viele Nachrichten, die unter dem Hashtag #jillmeagher veröffentlicht wurden, therapeutischer Natur zu sein schienen: *„individuals vented their emotions, enabling them to feel united in a shared grief“*. Martin (2007, S. 125) machte in einem anderen Kontext eine ähnliche Beobachtung: digilante Akteure schienen sich „besser zu fühlen“, nachdem sie ihre Geschichten online mit anderen geteilt hatten – vor allen Dingen, wenn diese ihnen Empathie entgegenbrachten oder sie in ihren Ansichten unterstützten (vgl. auch Huey et al. 2012). Sie kommt zu dem Schluß: *„At times, digilante websites function more like support groups than pillories“* (Martin 2007, S. 125). Auch Kohm (2009, S. 192) berichtet in seiner Analyse der digilanten Organisation *Perverted Justice* aus den USA, dass einige Mitglieder in Interviews angaben, für sie sei *„rooting out and publicly humiliating online predators […] a personally cathartic experience“*. Online-Plattformen können also ein Medium darstellen, welches bei der Verarbeitung von Taterlebnissen, sowie der Bereitstellung von gegenseitiger Unterstützung und Empathie helfen kann (vgl. Mallén 2016, S. 14). Sie können virtuelle Orte zum Austausch von Gedanken und Erfahrungen darstellen und Opfern eine Gelegenheit bieten, ihre Seite der Geschichte mit ihren eigenen Worten präsentieren zu können. Sie können dazu beitragen, die eigene Situation anderen verständlich zu machen, oder Menschen mit ähnlichen Erfahrung zu finden und dadurch eine heilsame Wirkung für die betroffenen Personen entfalten.

Für andere wiederum können digilante Aktivitäten eine Möglichkeit bedeuten, die eigenen Ängste und Sorgen in tatkräftige Maßnahmen zu übersetzen. In diesem Sinn bezeichnet Hill (2017) digitalen Vigilantismus als einen *„virtual coping process, indicative of the current global, social, and interactive contexts of the digital age.“ „The contributory potential of social media environments enable [sic] a form of simulated conclusivity which caters to the innate human drive for control“,* schreibt er. Gerade jenen BürgerInnen, die *„comfort in fantasies of control“* suchten, würde ein Rückgriff auf digilante Handlungsmuster angesichts einer wahrgenommenen Bedrohungslage helfen, ihre Bedürfnisse zu adressieren und auf diese Weise Sicherheitsgefühle herzustellen (s. a. Kap. „Kriminalität und Unsicherheit im virtuellen Raum“ und „Strafbedürfnis und Kriminalitätsfurcht im Cyberspace“). Einer kollektiv empfundenen Hilflosigkeit nach medial-vermittelten, traumatischen Ereignissen, wie den Anschlägen beim Boston Marathon 2013, könne digitaler Vigilantismus einen kollektiven Aktionismus gegenüberstellen, der dem Gefühl durch die Illusion von Kontrolle Abhilfe verschafft, weil

er es den Akteuren ermöglicht, „irgendetwas zu tun“, d. h., ihnen ermöglicht, den Ereignissen nicht bloß passiv ausgeliefert zu sein. Er bietet den digilanten Akteuren tatkräftige Maßnahmen, um ihr Ordnungsbedürfnis zu befriedigen. Allerdings stellt Hill (2017) auch fest, dass die genaue Rolle, welche der Impuls eine chaotische und scheinbar nicht überschaubare Situation kontrollieren zu wollen, bei Ritualen des digitalen Vigilantismus spielt, noch zu wenig beforscht ist, um empirisch gesicherte Aussagen zu treffen. Er konstatiert hier weiteren Forschungsbedarf.

5.8.3 Empowerment

Viertens können digilante Akteure mit dem Veröffentlichen eigener Viktimisierungserfahrungen und dem Anprangern von vermeintlichen TäterInnen eine Art „empowerment“ anstreben (vgl. Rose und Fox 2014; Keller 2015; Jane 2017; Salter 2017). Die Literatur fokussiert sich hier zumeist auf Fälle von sexualisierter Gewalt gegen Frauen – wie z. B. Cyber-Stalking, Cyber-Harassment oder sog. *„Revenge Porn“* (vgl. Fileborn 2014; Powell 2015; Powell und Henry 2017; Salter 2017; Jane 2017). Selbstjustizielles Handeln, welches sich gegen diese Taten richtet, wird als ein Digilantismus diskutiert, der zugleich eine Art „feministischen Aktivismus“ darstellt (siehe z. B. Powell 2015; Jane 2017). Jane (2017) beschreibt unter dem Begriff des „feministischen Digilantismus“ beispielsweise Online-Foren, die Frauen, welche Opfer von sexueller Belästigung geworden sind, eine Gelegenheit bieten, sich selbst wieder als Subjekte zu behaupten und gleichzeitig eine Kritik an den dahinterliegenden sozial-strukturellen Ursachen ihrer Diskriminierung zu formulieren, *„because they can ‚talk back‘ – not only to their individual assailants but to misogyny in the broader culture“* (Jane 2017, S. 5; siehe auch Fileborn 2014). Mit dieser Art Veröffentlichungen grenzen sich feministische, digilante Plattformen bewusst von der herkömmlichen Medienberichterstattung ab, die aus ihrer Sicht durch traditionelle Normen und Rollenerwartungen geprägt erscheint. Sensationelle Aspekte würden hier oft überbetont und gerade männliche Journalisten würden Gewalt gegen Frauen oftmals nicht als Problem sehen – Argumente, für die sich in Analysen zur Medienberichterstattung über Gewalt gegen Frauen durchaus Belege finden lassen (vgl. z. B. Meloy und Miller 2010).

Ein prominentes Beispiel für feministischen Digilantismus ist die Webseite *ihollaback*. Auf dieser Seite werden Frauen, die in der Öffentlichkeit sexuell belästigt worden sind, dazu ermutigt, die Täter zu fotografieren und das Bild zu Zwecken des Beschämens online verfügbar zu machen (vgl. Smith 2006; Martin 2007; Fileborn 2014; Powell 2015). Auf diese Weise soll ein öffentliches Bewusstsein für das Ausmaß eines sexualisierten und diskriminierenden

Umgangs mit Frauen geschaffen werden. Das Bloßstellen und Vorführen der Personen, durch die die Frauen zuvor emotionale und/oder physische Gewalt erfahren haben, erniedrigt und objektifiziert worden sind, soll es ihnen darüber hinaus ermöglichen, Kontrolle über ihr Leben zurückzugewinnen und gleichzeitig ein empfundenes Ungleichgewicht wieder auszubalancieren. Durch ein Publizieren eines erlittenen Unrechts wird die Möglichkeit geschaffen, sich gegen eine gesellschaftliche Zuschreibung als *„ideales Opfer“* (Christie 1986) sowie eine Selbstwahrnehmung als *„hilfloses Opfer“* (vgl. Kunczik 2016, S. 10) zu wehren. Auch Ariane Friedrich postete auf Facebook, um sich gegen das unerwünschte Verhalten eines anderen zu wehren und sich nicht länger wie ein „Opfer“ zu fühlen: *„Ich wurde in der Vergangenheit beleidigt, sexuell belästigt, und einen Stalker hatte ich auch schon. Ich bin allerdings nicht mehr bereit, mich doppelt zum Opfer zu machen und stets zu schweigen – ich bin es schlicht leid“* (zitiert in DPA 2012; Graff 2012). Digilantismus diente auch ihr dazu, aus einer subjektiven Ohnmacht angesichts einer als bedrohlich empfundenen Situation auszubrechen und sich durch eine tatkräftige Maßnahme von der Belastung zu befreien: *„Das war für mich ein persönlicher Befreiungsschlag“,* sagte sie im Nachhinein (zitiert in DIE ZEIT 2013).

5.8.4 Entertainment

Ein fünftes Motiv für Digilantismus kann darin zu finden sein, dass die Teilnahme an einer Online- „Jagd“ nach vermeintlichen Normverletzern Spaß und Abenteuer verspricht (vgl. Grigoriadis 2007; Skoric et al. 2010; Quent 2016a; Yardley et al. 2018; Chang und Poon 2017). Die technischen Gegebenheiten des Internets und der Sozialen Medien, sowie die ubiquitäre Verfügbarkeit von Handykameras und Tablets, ermöglichen eine Teilnahme an Prozessen der Kriminalitätsaufklärung, die zuvor in dieser Form nicht möglich war (vgl. Stratton et al. 2016, S. 23; Powell et al. 2018, S. 13). Normverstöße können über die Ton- und Bildaufnahmefunktionen der Geräte live dokumentiert und schnell mit anderen Nutzern über das Netzwerk in der ganzen Welt geteilt werden; die Identitäten verdächtigter Personen lassen sich dank der Verfügbarkeit vielfältiger persönlicher Informationen auf Webseiten und Online-Portalen offenlegen (Arvanitidis beschreibt Nutzerkonten bei sozialen Netzwerken deshalb auch als *„repositories of potentially incriminating information“*, vgl. 2016, S. 24); „digitale Beweise“ können per Screenshot gesammelt und in entsprechenden Foren kollaborativ-kollektiv ausgewertet werden (vgl. Schneider und Trottier 2012, S. 62).

Nutzer konsumieren Kriminalitätsereignisse nicht mehr nur passiv über die traditionellen Medienformate; in den sozialen Medien können sie Nachrichten selbst produzieren und den Verlauf von Ereignissen in diesem Sinn aktiv und

partizipatorisch mitgestalten – sie werden zu dem was Salter (2017, S. 228) als *„prosumer“* bezeichnet. Das alles trägt dazu bei, dass Normbrüche nicht nur medienwirksam in Szene gesetzt, sondern auch zu einer Art *„entertainment commodity“* (Kohm 2009, S. 191) werden können (vgl. auch Zabel 2011; Yardley et al. 2018). Laut Fox und Rose (2014, S. 775) sind es gerade diese Elemente, die BürgerInnen dazu befähigen und verleiten können, eine Rolle als „citizen detectives“ anzunehmen. Das öffentliche Beschämen und Vorführen von Personen wird zu einem inszenierten Spektakel für das Publikum mit einem gewissen Unterhaltungswert. Gesellschaftliche Realitäten werden vereinfacht dargestellt, Menschen auf Archetypen reduziert: der Digilante wird zum Helden, der Normverletzer zum Bösewicht (vgl. z. B. Shaw 2014). Projektionsflächen für moralisierende und skandalisierende Diskurse gibt es ausreichend.

Über das öffentliche Anprangern vermeintlicher TäterInnen schreibt der Philosoph Guy Aitchison außerdem: *„It's a relatively low cost way to feel like you are doing something noble. But there are also darker motivations at work: the psychic pleasure in seeing someone else brought low and humiliated“* (zitiert in Molloy 2018).[21] Bei der Teilnahme an digilanten Aktivitäten kann es um Neugierde oder Enthüllungslust, um Voyeurismus oder das Erleben eines kleinen Abenteuers im Alltag, um ein Bedürfnis nach Auflösung („closure“) oder gar um einen Wettstreit zwischen Akteuren, die sich gegenseitig ihre technischen Fähigkeiten unter Beweis stellen wollen, gehen (vgl. Chang und Poon 2017, S. 1915; Snyder et al. 2017; Malone 2017; Hombach 2019). Befördert werden kann dieser digilante „Spieltrieb“ dadurch, dass die Reaktionen der Zielpersonen online nicht mehr länger direkt sichtbar sind und soziale Hinweisreize fehlen (Wettlaufer 2015, S. 39; Wall und Williams 2007, S. 394).[22] Wenn ein digilanter Akteur nun einer Frau wünscht, sie solle vergewaltigt oder ermordet werden, dann sieht er nicht, wie die Frau reagiert (vgl. Suler 2004; Gruber 2018). Die Emotionen der betroffenen

[21]Im Jahr 2018 hat das Meinungsforschungsinstitut FORSA eine Online-Befragung (n = 1008) zur Wahrnehmung von Hasskommentaren in Deutschland durchgeführt (vgl. FORSA 2018). Erhoben wurde u. a. warum sich Nutzer mit Hasskommentaren beschäftigen. Obgleich sich nur eine Minderheit der befragten Internetnutzer mit Hasskommentaren im Netz beschäftigt, weil sie diese unterhaltsam finden (19 %), tun dies Männer häufiger als Frauen. Frauen hingegen beschäftigen sich eher mit Hasskommentaren, weil sie Hasskommentare entsetzen.

[22]In der Literatur werden diese Wirkmechanismen bisweilen kontrovers diskutiert, und sie stellen auch keinesfalls unumgängliche Regeln dar, weshalb sie hier im Anschluss an Kaspar (2017) im Konjunktiv formuliert werden.

Person – ob sie z. B. enttäuscht, verletzt, wütend, verängstigt oder traurig ist – können nicht durch die TäterInnen registriert werden; Gestiken und Mimiken fehlen in der Interaktion. Dadurch kann eine größere emotionale Abgrenzung zur potenziellen Zielperson erfolgen: sie wird nicht als realer, fassbarer Mensch wahrgenommen. Das Fehlen identitätsstiftender Merkmale kann zudem diesen Effekt noch verstärken (vgl. Kaspar 2017, S. 64 f.). Durch die wahrgenommene (technische und soziale) Anonymität und die physische Distanz kann es zu einer Erosion der sonst vorzufindenden Umgangsformen oder auch sozialen Urteilsfähigkeit kommen – ein Prozess, der in der Literatur als Deindividuation beschrieben wird (Brodowski und Freiling 2011: S. 102; vgl. auch Kaspar 2017, S. 64). Beide Faktoren können zu einer Art Enthemmung und höheren Bereitschaft zur Begehung digilanter Aktivitäten führen (Rüdiger 2017, S. 222). Sie machen es leichter, zu drohen und zu beleidigen (vgl. Moore et al. 2012; Gruber 2018).

5.8.5 Wunsch nach Aufmerksamkeit bzw. Geltungsdrang

Ein Streben nach Aufmerksamkeit ist schließlich das letzte denkbare Motiv, welches in diesem Abschnitt Erwähnung finden soll. Im Internet können Nutzer sich selbst zum Urheber, Multiplikator oder Meinungsmacher erheben. Es bietet somit die Möglichkeit, sich selbst durch einen einzelnen Eintrag auf einem viel gelesenen Blog oder ein Posting auf einer Seite populärer Sozialer Netzwerke zu einem „Star“ zu machen (Brodowski und Freiling 2011, S. 58). Öffentliches Beschämen kann hier eine wirkungsvolle Strategie darstellen. Salter (2017, S. 74) schreibt: *„Repudiating or humiliating other social media users can constitute a highly salient form of content generation that, in and of itself, invites attention and interaction from other users.“* Das liegt u. a. daran, dass das Ungewöhnliche, das von der Norm Abweichende, besonderen Aufmerksamkeitswert besitzt (Kunczik 2016, S. 151). Und Negativität erhöht ebenfalls die Wahrscheinlichkeit, dass ein Ereignis zur Nachricht wird (Galtung und Ruge zitiert in Kunczik 2016, S. 151). Kurzum, *„[p]eople can gain influence by creating opportunities for the derogation of others“* (Salter 2017, S. 60).

Das öffentliche Anprangern und Demütigen von Personen stellt einen performativen Akt dar, der sich laut Kohm (2009, S. 189) gut verkaufen und vermarkten lässt. Davon zeugen nicht nur populäre Infotainment-Sendungen wie *To Catch a Predator* in den USA oder hierzulande *Tatort Internet* (vgl. auch Grigoriadis 2007; Zabel 2011; Saliger 2013). Auch eine Reihe von digilanten Akteuren hat durch ihre Veröffentlichungen bereits eine gewisse Berühmtheit erlangt – selbst wenn das Streben nach Ruhm (zunächst) kein Beweggrund für ihr Handeln gewesen sein mag: Alexandra Goddard, die Bloggerin, die den Steubenville-Vergewaltigungen zu ihrer notorischen Bekanntheit verholfen hat, war

im Nachhinein ein gerngesehener Gast in verschiedenen US Nachrichten- und Unterhaltungssendungen (Levy 2013). Der ultra-konservative Blogger Milo Yiannopoulus wiederum nutzte die #gamergate Affäre als ein Sprungbrett für seine Karriere: er wurde zeitweise als „Popstar des Hasses“ und als „Superbösewicht des Internets“ gefeiert (vgl. Moore 2016; Lynskey 2017). Aitchison (zitiert in Molloy 2018) erklärt: *„More outrage means more clicks“* (vgl. auch Salter 2017. Mehr Klicks bedeuten *„more revenue through advertising“* (vgl. Molloy 2018). Öffentliche Aufmerksamkeit kann sich also auszahlen.

Das Internet mit seinen Sozialen Medien bietet aber nicht nur die Möglichkeit ein „Star“ oder „Held“ zu werden; es offeriert zudem neue Möglichkeiten der Selbstdarstellung und des Reputationsmanagements. Der Drang nach sozialer Geltung, danach *„gesehen, bewundert und gefeiert zu werden“,* wie es Yar (2012, S. 252) formuliert, kann einen weiteren Anreiz dafür liefern, sich als Digilant zu betätigen. Hierbei geht es um das Verlangen nach Status und Respekt innerhalb einer Online-Community, und es geht um das Bedürfnis, sein transgressives Selbst zu zelebrieren und zur Schau zu stellen, welches sich mit breiteren gesellschaftlichen Trends zur Selbstvermarktung verbindet (Yar 2012, S. 252; vgl. auch Kushner 2013; Salter 2017). Dabei können das Design und die Algorithmen-basierte Logik der Plattformen dazu beitragen, jenen Beiträgen zu mehr Aufmerksamkeit zu verhelfen, die provozieren und aktivierende Emotionen, wie Wut oder Hass, schüren. Wenn ein Beitrag viele Kommentare oder „likes“ erntet, sorgen die Empfehlungsalgorithmen, z. B. bei Facebook, nämlich dafür, dass dieser noch mehr Menschen gezeigt wird – d. h., die Plattform „belohnt“ Beiträge, die Wut oder Hass säen (vgl. Salter 2017, S. 13, 57). Salter (2017, S. 60) konstatiert: *„Through abuse and harassment, users can increase their profile and status“*. Keller (2015) kommt zu einem ähnlichen Schluß: *„Triumphs over adversity are good for clicks“*. Mehr „clicks“ – oder auch „likes“ – und mehr „Follower“ können wiederum ein höheres Ansehen innerhalb einer Online-Community bedeuten und somit zu einem Gefühl persönlicher Befriedigung beitragen (vgl. Keller 2015). Und dieses Gefühl kann dann weiter dazu motivieren noch mehr solcher „negativen“ Beiträge, die dem Bloßstellen von normabweichenden Verhalten dienen, zu posten.

6 Fazit

Das Phänomen der Selbstjustiz im Internet polarisiert sowohl in öffentlichen als auch wissenschaftlichen Debatten. In seinem Podcast spricht sich der SPIEGEL Blogger Sascha Lobo (2019) für eine Art *„Social-Media-Notwehr“* aus.

Er argumentiert, die Möglichkeit, Missetaten gegen sich oder eine andere einem nahestehende Person öffentlich zu machen, könne Täter in die Verantwortung zwingen, abschreckend wirken, oder eine Art Schutz für weitere potenzielle Opfer bieten, da diese durch die nun zugänglichen Informationen gewarnt werden können. Öffentlichkeit könne in diesem Sinne als eine Art *„Selbstschutz-Waffe“* fungieren. Der Rechtstaat müsse sich angesichts neuer sozialer Technologien weiterentwickeln, betont Lobo. Ähnliche Argumente lassen sich, z. B. auch bei Powell (2015) finden, die sich mit der Veröffentlichung von Erfahrungen sexueller Gewalt durch *„victim-survivors“* beschäftigt. Sie hebt hervor, dass durch Praktiken informeller Sozialkontrolle in Online-Räumen und unter zur Hilfenahme von Kommunikationstechnologien nicht nur individuelle und kollektive Gewalterfahrungen validiert, sondern darüber hinaus auch patriarchale Machtstrukturen, die in westliche Gesellschaften (oftmals unsichtbar) eingeschrieben sind, aufgebrochen und herausgefordert werden können. Dadurch ließen sich Vorstellungen von Recht und Ordnung neu und vor allen Dingen partizipatorisch verhandeln.

In diesem Sinne stellten digilante Handlungen eine Form von Aktivismus dar, die systematische Ungerechtigkeiten aufdecken und den „Opfern“ eine Stimme verleihen kann. Auf diesem Weg könnten sie sich gegen ihre Viktimisierung wehren. Kritiker von Digilantismus indessen verweisen zum einen auf die Gefährdung grundlegender, rechtsstaatlicher Prinzipien, wie die Unschuldsvermutung, die ihren Ursprung in vergangenen Unrechtserfahrungen haben und einen Grundpfeiler der bestehenden Rechtsordnung darstellen, und zum anderen auf das Gewaltpotenzial, welches unkontrollierte „Hetzjagden“ durch virtuelle „Mobs“ mit sich bringen können – mit Konsequenzen online *und* offline. Auch das Spannungsverhältnis zwischen dem Schutz der Persönlichkeit, welcher in Art. 2 Abs.1 i. V. m. Art. 1 Abs.1 GG geregelt ist, und dem Recht auf Meinungsfreiheit aus Art. 5 Abs.1 GG ist immer wieder Thema kritischer Auseinandersetzung und Diskussion.

Dass private Akteure das Recht in die eigenen Hände nehmen, ist kein neues Phänomen. Nicht erst seit Einführung des Internets kommt es vor, dass Menschen angesichts eines wahrgenommenen „falschen“ Verhaltens Anderer regulierend eingreifen. *„Vigilantism is at heart a reaction of normal people“,* stellt Silke (2001, S. 129) fest. Dennoch verleiht das Internet dem Phänomen des Vigilantismus eine neue Qualität, die sich über die Eigenheiten der digitalen Kommunikationsmedien erklären lässt. Heute ermöglichen es die beinahe ubiquitär verfügbar sozialen Technologien, jeden Fehltritt einer anderen Person sofort zu dokumentieren und millionenfach im Internet zu teilen. Sie offerieren eine anonyme, schnelle und weitreichende Verbreitung von Inhalten. Insbesondere

die partizipatorisch ausgerichteten Sozialen Medien bringen zudem Äußerungsformen und Reaktionsmöglichkeiten hervor, die es zuvor in dieser Form nicht gab. Sie bieten einen neuen Raum, sowie neue kommunikative Möglichkeiten für Auseinandersetzungen über gesellschaftliche Konflikte (Salter 2017, S. 129). Neue Formen der (Durch-)Setzung von (Ge-)Recht(igkeit) werden hier verhandelt und handlungspraktisch umgesetzt. Das sog. *Trolling* oder auch *„Revenge Porn“* sind Formen der Devianz, die mit der Digitalität erst entstanden und ohne sie nicht denkbar sind; ältere Formen von Devianz, wie Hass-Kommentare oder sexuelle Belästigungen, erhalten im digitalen Raum neue Dimensionen. Obgleich eigenständige Phänomene, so gibt es, zumindest in Teilbereichen, konzeptionelle Überschneidungen mit dem Digilantismus. Im hiesigen Kontext werden sie zu Werkzeugen und Strategien digilanter Akteure, die mit ihnen eigene Vorstellungen von Moral und (Un)Recht eigenmächtig und wirkmächtig umzusetzen versuchen.

Im vorliegenden Kapitel habe ich einige der Elemente konventioneller Definitionen von Vigilantismus thematisiert und problematisiert, die m. E. im digitalen Kontext überdacht werden müssen. Mein Ziel war es, auf diese Weise eine Grundlage für ein besseres Verständnis des Digilantismus zu legen und weiterführende Diskussionen sowie Forschung anzuregen. Wie zu Anfang erwähnt, mangelt es bislang noch an empirischer Forschung zu verschiedenen Aspekten und Ausprägungen des Phänomens. Vor allen Dingen fehlen im deutschsprachigen Raum bislang Studien, die über Medienberichte mit ihrem inhärenten *Bias* hinausgehen, denn diese sind in der Art und Weise ihrer Darstellung in hohem Maß von journalistischen Standards und Selektionsmechanismen beeinflusst (vgl. Roberz und Kahr 2016, S. 13). Es wäre daher sinnvoll, die Wahrnehmungen, Erfahrungen und Ansichten von digilanten Akteuren (n)ethnographisch in den Blick zu nehmen. Beispielsweise ist über die Tatsache hinaus, dass es sich bei Digilanten um private, nichtstaatliche Akteure handelt, noch wenig darüber bekannt, wer sie sind. Daher lassen sich derzeit noch so gut wie keine Aussagen über Alter, Herkunft, Bildungsgrad, etc. digilanter Akteure treffen (vgl. Yardley et al. 2018). Spannend wäre es ebenfalls, jene Fälle empirisch zu erfassen, die nicht spektakulär genug sind, um es in die nationale oder internationale Medienberichterstattung zu schaffen oder große Aufmerksamkeit in den Sozialen Medien zu generieren. Ich spreche hier von den eher alltäglichen Fällen, die zwar auch in und unter Verwendung Sozialer Medien stattfinden, die aber in ihrer medialen Reichweite auf bestimmte Nutzergruppen, z. B. Mitglieder einer Kontaktliste oder eines geschlossenen Online-Forums, beschränkt bleiben. Interessant wäre es weiterhin genauer zu erkunden, inwiefern die neuen Kommunikationstechnologien und Medien mit ihrer spezifischen Logik und ihren

partizipatorischen Möglichkeiten eine Motivation für digilantes Handeln erst hervorbringen bzw. diese befördern. Inwiefern werden sie, z. B. selbst zum Motor von individuellen und/oder gesellschaftlichen Ängsten?

Auch hinsichtlich der Rolle, die die Sozialen Medien bei einer Suche nach Gerechtigkeit als *„informal justice mechanism“* (Powell 2015) spielen können, besteht, wie gesagt, noch Forschungsbedarf. In diesem Zusammenhang wäre es aufschlussreich, sich auch Fälle anzusehen, in denen das Streben nach Gerechtigkeit wiederum eigene Ungerechtigkeiten, z. B. bei falschen Verdächtigungen, produziert hat, denn hier stellt sich eine Reihe von ethischen Fragen. Im Anschluss daran könnte beispielsweise darüber nachgedacht werden, wie eine größere Sensibilität der Internetnutzer für denkbare negative Auswirkungen von Online „Shamings“ erreicht werden kann. Ließen sich z. B. ethische Maßstäbe – ähnlich denen im journalistischen Bereich – kodifizieren und implementieren? Oder ließe sich eine Art *„kollektive Publikumsethik“*, wie sie Kunczik (2016, S. 166) unter Verweis auf Christians zur Debatte stellt, entwickeln, die Nutzer in eine moralische Pflicht nimmt, Fehlverhalten im Online-Bereich untereinander anzuzeigen? Die bereits erwähnte FORSA Umfrage aus dem Jahr 2018 zeigt z. B., dass die überwiegende Mehrheit der Befragten (78 %) schon einmal Hassrede bzw. Hass-Kommentare im Internet gesehen hat. 42 % der Befragten gaben jedoch an, sich beim Wahrnehmen eines Hass-Kommentars weder näher mit diesem beschäftigt noch diesen bzw. dessen Verfasser gemeldet zu haben (FORSA 2018, S. 3). Und nur 1 % hat aufgrund eines Hass-Kommentars Anzeige bei der Polizei erstattet (FORSA 2018, S. 3). Wie ließe sich also ein größeres Verantwortungsbewusstsein für ein respektvolles Miteinander auch im digitalen Raum entwickeln?

Und zu guter Letzt stellt sich die Frage nach dem offiziellen Umgang mit dem Phänomen des Digilantismus: Wie kann/soll sich das Verhältnis zwischen BürgerInnen und Staat bei der Aufklärung und Ahndung von Vergehen und Straftaten in und unter Verwendung sozialer Technologien gestalten? Muss sich der Rechtsstaat weiterentwickeln, wie es der anfangs zitierte SPIEGEL Blogger Sascha Lobo (2019) fordert, und die Möglichkeit einer offiziellen „Social-Media-Notwehr“ anerkannt werden? Nhan et al. (2017, S. 358) sind der Ansicht, *„the police should develop strategic policies and practices aimed at proactively recognizing and employing members of the public as additional crime detectors“*. Sie berufen sich mit ihrer Aussage auf Fälle, in denen private Akteure durch investigative Tätigkeiten im Internet tatsächlich erfolgreich zur Aufklärung von Straftaten beigetragen haben (vgl., z. B. Murphy 2013; Li 2014; Baraniuk 2014; Dewey 2015). Allerdings stellt sich dann die Frage, *„where boundaries of citizen involvement in policing affairs might be drawn“* (Campbell 2015, S. 347). Offen bleibt

außerdem, wie der Rechtsstaat seine eigene Sichtbarkeit und Präsenz im Netz erhöhen und somit Tendenzen zur Selbstjustiz präventiv entgegenwirken kann. Nicht alle Initiativen privater BürgerInnen werden sich schließlich für die von Nhan et al. (2017) befürworteten, kooperativen Sicherheitspartnerschaften eignen. Wo lässt sich dann also eine (neue) Grenze zwischen unerwünschtem Vigilantismus und befürworteter Vigilanz ziehen? Hier wäre es unabdingbar auch die Sichtweisen und Erfahrungen der offiziellen Strafverfolgungsbehörden zu erfassen, um tragfähige Konzepte zu erarbeiten.

In der bestehenden Literatur scheint man sich einig, dass digilantes Handeln privater Akteure – insbesondere in seiner Ausprägung als „crowdsourced policing" – in Zukunft noch weiter zunehmen wird (vgl. Schneider und Trottier 2012; Nhan et al. 2016; Powell et al. 2018). *„Online communities of ‚digilantes' are here to stay",* resümieren Nhan et al. (2016, S. 358). Ein Fazit, welches die Relevanz weiterführender Forschung und die Dringlichkeit der aufgeworfenen Fragen unterstreicht.

Literatur

Abrahams, R. (1998). *Vigilant citizens. Vigilantism and the state*. Cambridge: Polity Press.

Ahmad, A. (2. März 2015). A note on call-out culture. *Briarpatch Magazine*. https://briarpatchmagazine.com/articles/view/a-note-on-call-out-culture. Zugegriffen: 5. März 2019.

Altheide, D. (2004). The control narrative of the internet. *Symbolic Interaction, 27*(2), 223–245.

ARD. (21. November 2018). "Tatort: Treibjagd." Fernsehfilm. https://www.daserste.de/unterhaltung/krimi/tatort/sendung/treibjagd-100.html. Zugegriffen: 18. Febr. 2019.

Arfsten. K.-S. (2010). *The Minuteman Civil Defense Corps: Border Vigilantism, Immigration Control and Security on the US-Mexican Border*. Hamburger Studien zur Kriminologie und Kriminalpolitik (Bd. 48). Berlin: LIT.

Arfsten, K.-S. (2012). Every Man is Entitled to Defend His Castle… – Vigilantismus während der London "riots". *Kriminologisches Journal, 44*(2), 101–117.

Arfsten, K.-S. (2018). *Under watchful eyes: Public vigilance in the post-9/11 United States*. Unveröffentlichte Dissertation. Freiburg, i.B.: Albert-Ludwigs-Universität Freiburg.

Arvanitidis, T. (2016). Publication bans in a facebook age: How internet vigilantes have challenged the youth criminal justice act's ‚secrecy laws' following the 2011 vancouver stanley cup riot. *CGJSC/RCESSC, 5*(1), 18–32.

Baraniuk, C. (2. Mai 2014). The amateur detectives tackling murders and kidnaps. *BBC*. http://www.bbc.com/future/story/20140501-meet-the-bedroom-detectives. Zugegriffen: 11. Jan. 2019.

Baur, A., Burkhardt, A., & Kinzig, J. (2011). Am Pranger: Kriminalprävention durch Information? Über die Zulässigkeit und kriminalpolitische Wirksamkeit eines Präventivprangers für gefährliche Straftäter. *JuristenZeitung, 66*(3), 131–139.

Beigang, T., & Langer, S. (29. Januar 2018). Hass Kommentare: Aufrufe zur Selbstjustiz auf Facebook sind strafbar. Nordkurier. https://www.nordkurier.de/digital/aufrufe-zur-selbstjustiz-auf-facebook-sind-strafbar-2931100701.html. Zugegriffen: 20. Jan. 2020.

Booth, R. (25. Oktober 2013). Vigilante paedophile hunters ruining lives with internet stings. *The Guardian*. https://www.theguardian.com/uk-news/2013/oct/25/vigilante-paedophile-hunters-online-police. Zugegriffen: 12. Dez. 2018.

Bosker, B. (27. Dezember 2013). Why we should all fear the righteous online mob. *Huffington Post*. https://www.huffingtonpost.com/2013/12/27/justin-sacco-online-vigilantism_n_4505452.html. Zugegriffen: 12. Jan. 2019.

Braithwaite, J. (1989). *Crime, shame and reintegration*. Cambridge: Cambridge University Press.

Braithwaite, J. (1993). Shame and modernity. *The British Journal of Criminology, 33*(1), 1–18.

Braithwaite, J. (2000). Shame and criminal justice. *Canadian Journal of Criminology, 42*(3), 281–298.

Brodowski, D., & Freiling F. C. (2011). Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft. *Schriftenreihe Forschungsforum Öffentliche Sicherheit* Nr. 4. Berlin: Freie Universität Berlin.

Brückweh, K. (2006). Mordlust: Serienmorde, Gewalt, und Emotionen im 20. Jahrhundert. Frankfurt/New York: Campus Verlag.

Byrne, D. N. (2013). Digilantes and the frontier of radical justice online. *Radical History Review, 117,* 70–82.

Campbell, E. (2015). Policing Paedophilia: Assembling bodies, spaces and things. *Crime Media Culture, 12*(3), 345–365.

Chang, L. Y. C., & Poon, R. (2017). Internet vigilantism: Attitudes and experiences of university students toward cyber crowdsourcing in Hong Kong. *International Journal of Offender Therapy and Comparative Criminology, 61*(16), 1912–1932.

Cheung, A. (2014). Revisiting privacy and dignity: Online shaming in the global e-village. *Laws, 3,* 301–326.

Christie, N. (1977). Conflicts as property. *The British Journal of Criminology, 17*(1), 1–15.

Christie, N. (1986). The ideal victim. In E. A. Fattah (Hrsg.), *From crime policy to victim policy* (S. 17–30). London: Palgrave Macmillan.

Clune, B. (28. November 2013). Digital vigilantism: Think before putting pictures of ‚Wrongdoing' online. *The Guardian*.

Conan, N. (27. November 2007). Cyber vigilantes: Do-it-yourself justice online. *National Public Radio (NPR)*. https://www.npr.org/templates/transcript/transcript.php?storyId=16659289&t=1551199603156. Zugegriffen: 21. Febr. 2019.

Condry, R. (2010). Secondary victims and secondary victimization. In S. G. Shoham, P. Knepper, & M. Kett (Hrsg.), *International Handbook of Victimology* (S. 219–249). Boca Raton: CRC Press/Taylor & Francis Group.

Dennis, K. (2008). Keeping a close watch – The rise of self-surveillance and the threat of digital exposure. *The Sociological Review, 56*(3), 347–357.

Dewey, C. (10. März 2015). Crowdsourcing may have solved a 20-year-old cold case. *The Washington Post*. https://www.washingtonpost.com/lifestyle/style/how-the-internet-may-have-solved-a-20-year-old-cold-case/2015/03/10/02a4a326-acb1-11e4-9c91-e9d2f9fde644_story.html?utm_term=.6093effee8e4. Zugegriffen: 21. März 2019.

DIE WELT. (11. September 2014). Tierquälervideo: Unbeteiligte online als "Katzenkiller" geoutet. Online Ausgabe. https://www.welt.de/vermischtes/article132155332/Unbeteiligte-online-als-Katzenkiller-geoutet.html. Zugegriffen: 21. Febr. 2019.

Dittmeyer, M. (2013). Persönlichkeitsrechtsverletzungen durch Äußerungen im Internet. Typische Fallgruppen. *DuD – Datenschutz und Datensicherheit 12,* 780–786.

Dorfer, T., & J. Schulz. (19. April 2013). Sunil Tripathi und der Boston-Anschlag: Hauptverdächtiger für wenige Stunden. *Süddeutsche Zeitung*. https://www.sueddeutsche.de/panorama/sunil-tripathi-und-der-boston-anschlag-hauptverdaechtiger-fuer-wenige-stunden-1.1653521. Zugegriffen: 21. Nov. 2018.

DPA. (24. April 2012). Facebook-Posting: Anwälte werfen Ariane Friedrich unrechtmäßiges Verhalten vor. *Die Zeit Online*. https://www.zeit.de/digital/internet/2012-04/ariane-friedrich-facebook-pranger. Zugegriffen: 5. März 2019.

Drutschmann, D. (22. August 2014). Aufruf zur Selbstjustiz: Am Online-Pranger. *Der Tagesspiegel*. https://www.tagesspiegel.de/themen/digitalisierung-ki/aufruf-zur-selbstjustiz-am-online-pranger/10370720.html. Zugegriffen: 8. Jan. 2019.

Duggan, M. (11. Juli 2017). Online Harassment 2017. *Pew Research Center*. http://www.pewinternet.org/2017/07/11/online-harassment-2017/. Zugegriffen: 21. Febr. 2019.

Dumsday, T. (2009). On cheering Charles Bronson: The ethics of vigilantism. *The Southern Journal of Philosophy XLVII,* 49–67.

Dunsby, R. M., & Howes, L. M. (2019). The NEW adventures of the digital vigilante! Facebook user's views on online naming and shaming. *Australian & New Zealand Journal of Criminology, 52*(1), 1–19.

e Silva, K. K. (2018). Vigilantism and cooperative criminal justice: Is there a place for cybersecurity vigilantes in cybercrime fighting? *International Review of Law, Computers & Technology, 32*(1), 21–36.

Elias, N. (1997). *Über den Prozess der Zivilisation*. Berlin: Suhrkamp.

Ellrich, F. (14. April 2018). Selbstjustiz: Magdeburger sucht Täter in Eigenregie. *Volksstimme.de*. https://www.volksstimme.de/lokal/magdeburg/selbstjustiz-magdeburger-sucht-taeter-in-eigenregie. Zugegriffen: 21. Febr. 2019.

Evans, J. (2003). Vigilance and vigilantes: Thinking psychoanalytically about anti-paedophile action. *Theoretical Criminology, 7*(2), 163–189.

Fileborn, B. (2014). Online activism and street harassment: Digital justice or shouting into the ether? *Griffith Journal of Law & Human Dignity, 2*(1), 32–51. (Special Issue: Women & Violence).

FORSA. (2018). Ergebnisbericht: Wahrnehmung von Hasskommentaren im Internet. Düsseldorf: Landesanstalt für Medien NRW. https://www.medienanstalt-nrw.de/fileadmin/user_upload/lfm-nrw/Foerderung/Forschung/Dateien_Forschung/forsaHate_Speech_2018_Ergebnisbericht_LFM_NRW.PDF. Zugegriffen: 12. März 2019.

Franck, G. (2019). The economy of attention. *Journal of Sociology, 55*(1), 8–19.

Fuchs, E., Kelley M. B., & Lubin G. (12. April 2013). Social media makes teen rape more traumatic than ever. *Business Insider*. https://www.businessinsider.com/the-impact-of-social-media-on-rape-2013-4?IR=T. Zugegriffen: 21. März 2019.

Goffman, E. (1963). *Stigma: Notes on the management of spoiled identity*. New York: Simon & Schuster.

Gottschalk, K. (1. September 2014). Videospiel-Debatte: Wer Sexismus anprangert, wird mit Vergewaltigung bedroht. *Der Spiegel Online*. http://www.spiegel.de/netzwelt/netzpolitik/anita-sarkeesian-feministische-videospielkritik-und-morddrohungen-a-988906.html. Zugegriffen: 1. März 2019.

Graff, B. (23. April 2012). Digitaler Gegenschlag, maximale Verletzung. *Süddeutsche Zeitung*. https://www.sueddeutsche.de/panorama/ariane-friedrich-outet-verfasser-obszoener-mail-digitaler-gegenschlag-maximale-verletzung-1.1339657. Zugegriffen: 5. März 2019.

Grigoriadis, V. (9. August 2007). ‚To Catch a Predator': The new American witch hunt. *Rolling Stone*. https://www.rollingstone.com/tv/tv-news/to-catch-a-predator-the-new-american-witch-hunt-75418/. Zugegriffen: 5. März 2019.

Gruber, A. (10. Oktober 2018). Ein Jahr #MeToo: „Für Frauen wird es online schnell besonders ekelhaft". SPIEGEL Online. http://www.spiegel.de/netzwelt/web/metoo-debatte-ingrid-brodnig-ueber-frauenhass-im-netz-a-1231787.html. Zugegriffen: 12. März 2019.

Haas, N. (2010). *Public support for vigilantism*. Leiden: Leiden University Press.

Hai-Jew, S. (2014). *Vengeance culture online: A qualitative meta-analysis and position paper. Human rights and the impact of ICT in the public sphere: Participation, democracy, and political autonomy* (S. 64–93). Hershey, PA: IGI Global.

Harvard Law Review Association. (2003). Shame, stigma, and crime: Evaluating the efficacy of shaming sanctions in criminal law. *Harvard Law Review, 116*(7), 2186–2207.

Heitmeyer, W., & Hagan, J. (2002). Gewalt – Zu den Schwierigkeiten einer systematischen internationalen Bestandsaufnahme. In W. Heitmeyer & J. Hagan (Hrsg.), *Internationales Handbuch der Gewaltforschung* (S. 15–25). Wiesbaden: Springer VS.

Hess, A. (6. Mai 2010). De-Friendly fire: American University student makes facebook rape accusation. *Washington City Paper*. https://www.washingtoncitypaper.com/columns/the-sexist/blog/13118920/de-friendly-fire-american-university-student-makes-facebook-rape-accusation. Zugegriffen: 2. März 2019.

Hilgers, M. (2012). *Scham: Gesichter eines Affekts*. Göttingen: Vandenhoeck & Ruprecht.

Hill, C. (2017). How digital communities cope: Cyber-vigilantism following the Boston marathon bombings. The Yale Review of International Studies. http://yris.yira.org/essays/2039. Zugegriffen: 15. März 2019.

Hitzler, R. (1993). Bürger machen mobil: Über die neue soziale Sicherheits-Bewegung. *Forschungsjournal Neue Soziale Bewegungen, 6*(3–4), 16–27.

Hombach, S. (15. Januar 2019). Doxing: Die Erzählung vom jungen weißen Hacker. *Die Zeit Online*.

Huey, L., Nhan, J. & Broll, R. (2012). ‚Uppity civilians' and ‚cyber-vigilantes': The role of the general public in policing cyber-crime. *Criminology & Criminal Justice 13*(1), 81–97.

Hungermann, J. (22. April 2012). Ariane Friedrich prangert obszönen Verehrer an. *Die Welt*. https://www.welt.de/sport/olympia/article106213398/Ariane-Friedrich-prangert-obszoenen-Verehrer-an.html. Zugegriffen: 13. Febr. 2019.

Innes, M. (2004). Signal crimes and signal disorders: Notes on deviance as communicative action. *The British Journal of Sociology, 55*(3), 335–355.

Ipsos-Mori. (2017). Poll: Online abuse or harassment against women. https://drive.google.com/file/d/1-gxSWRJsEl-CCO4HGs4uqV6NNoYe_nP2/view. Zugegriffen: 12. März 2019.

Jane, E. (2017). Feminist Digilante responses to slut-shaming on facebook. *Social Media+Society 3*(2), 1–10.

Jason, Z. (28. April 2015). Game of Fear. *Boston Magazine*. https://www.bostonmagazine.com/news/2015/04/28/gamergate/2/. Zugegriffen: 14. Jan. 2019.

Johnston, L. (1996). What is vigilantism? *British Journal of Criminology, 36*(2), 220–236.
Juliano, S. (2012). Superheroes, bandits, and cyber-nerds: Exploring the history and contemporary development of the vigilante. *Journal of International Commercial Law and Technology, 7*(1), 44–64.
Jüttner, J. (23 April 2012). Ariane Friedrichs Selbstjustiz: Der Spießrutenlauf. *SPIEGEL Online*. http://www.spiegel.de/panorama/leute/ariane-friedrich-wehrt-sich-gegen-belaestigung-bei-facebook-a-829286.html. Zugegriffen: 13 Febr. 2018.
Kaiser, G. (2002). Medienkriminalität: Spiegel der Wirklichkeit oder Instrument der Kriminalpolitik? *Zeitschrift für Rechtspolitik, 35*(1), 30–34.
Karstedt, S. (1996). Recht und Scham. *Neue Kriminalpolitik, 8*(4), 22–25.
Kaser, R. (29. September 2017). The consequences of online vigilantism. *The Next Web*. https://thenextweb.com/socialmedia/2017/09/29/consequences-online-vigilantism/. Zugegriffen: 23. Febr. 2019.
Kaspar, K. (2017). Hassreden im Internet – Ein besonderes Phänomen computervermittelter Kommunikation? In K. Kaspar, L. Gräßer & A. Riffi (Hrsg.), *Online Hate Speech: Perspektiven auf eine neue Form des Hasses* (S. 63–85). Schriftenreihe zur digitalen Gesellschaft NRW, Bd. 4. Düsseldorf: Kopaed.
Katyal, N. K. (1997). Deterrence's difficulty. *Michigan Law Review, 95*(8), 2385–2476.
Katyal, N. K. (2001). Criminal law in cyberspace. *University of Pennsylvania Law Review, 149*(4), 1003–1114.
Keller, J. (2015). Can Digital Vigilantism Make the Internet Safer for Women? Pacific Standard Magazine. https://psmag.com/environment/how-one-jock-helped-bring-internet-vigilantism-to-the-public-eye.
Kepplinger, H. M. (2016). Rationalität und Ethik – Zur Verantwortung von Journalisten für die Berichterstattung über schwere Gewalttaten. In F. J. Robertz & R. Kahr (Hrsg.), *Die mediale Inszenierung von Amok und Terrorismus* (S. 173–183). Wiesbaden: Springer VS.
Kohm, S. A. (2009). Naming, shaming and criminal justice: Mass-mediated humiliation as entertainment and punishment. *Crime Media Culture, 5*(2), 188–205.
Kotecha, K. C., & Walker, J. L. (1976). Police Vigilantes. *Society 13*(3), 48–52.
Kowalewski, D. (2002). Vigilantismus. In W. Heitmeyer & J. Hagan (Hrsg.), *Internationales Handbuch der Gewaltforschung* (S. 426–440). Wiesbaden: Springer VS.
Krempl, S. (10. Juli 2017). G20-Krawalle: Linke und Polizei beklagen „Online-Hetzjagd" wegen privater Internet-Fahndung. *Heise Online*. http://www.heise.de/-3768185. Zugegriffen: 13. Febr. 2019.
Kunczik, M. (2016). Die Verdopplung des Leides – Sekundäre Viktimisierung durch Berichterstattung. In F. J. Robertz & R. Kahr (Hrsg.), *Die mediale Inszenierung von Amok und Terrorismus* (S. 151–169). Wiesbaden: Springer VS.
Kunczik, M., & Bleh, W. (1995). *Kriminalitätsopfer in der Zeitungsberichterstattung. Folgen der Berichterstattung aus der Perspektive der Opfer*. Mainz: Weißer Ring.
Kushner, D. (8. September 2014). The masked avenger. How anonymous incited online vigilantism. *The New Yorker*. https://www.newyorker.com/magazine/2014/09/08/masked-avengers. Zugegriffen: 23. Febr. 2019.
Kushner, D. (27. November 2013). Anonymous vs. Steubenville. *Rolling Stone Magazine*. https://www.rollingstone.com/culture/culture-news/anonymous-vs-steubenville-57875/. Zugegriffen: 12. März 2019.

Lally, N. (2017). Crowdsourced surveillance and networked data. Special Issue on Securing with Algorithms. *Security Dialogue 48*(1), 63–77.

Landesanstalt für Medien NRW. (13. April 2018). Mehr als 130 Anzeigen binnen 70 Tagen. „Verfolgen statt nur Löschen" zieht erste Bilanz. Pressemitteilung. https://www.medienanstalt-nrw.de/service/pressemitteilungen/pressemitteilungen-2018/2018/april/verfolgen-statt-nur-loeschen-zieht-erste-bilanz.html. Zugegriffen: 12. März 2019.

Lee, T. G. (22. Juni 2015). The real story of Sunil Tripathi, the Boston bomber who wasn't. *NBC News*. https://www.nbcnews.com/news/asian-america/wrongly-accused-boston-bombing-sunil-tripathys-story-now-being-told-n373141. Zugegriffen: 23. Febr. 2019.

Leonard, J., & Morin M. (17. Januar 2002). Stalking the web predator: A Colorado Homemaker has won praise – And arrests – For her efforts against kiddie porn. But critics of such online crusaders call it a form of vigilantism. *Los Angeles Times*.

Levy, A. (5. August 2013). Trial by twitter. *The New Yorker*. https://www.newyorker.com/magazine/2013/08/05/trial-by-twitter. Zugegriffen: 3. März 2019.

Li, S. (17. September 2014). Social media sleuths help track down hate crime suspects. *The Atlantic*. https://www.theatlantic.com/national/archive/2014/09/social-media-sleuths-help-track-down-hate-crime-suspects/380364/. Zugegriffen: 21. März 2019.

Lichtenberg, A. (25. April 2012). Selbstjustiz im Internet. *Deutsche Welle*. https://www.dw.com/de/selbstjustiz-im-internet/a-15907740. Zugegriffen: 12. März 2019.

Linkins, J. (19. April 2013). Reddit moderator apologizes to Sunil Tripathi's family. *Huffington Post*. https://www.huffingtonpost.com/2013/04/19/reddit-sunil-tripathi-apologize_n_3117051.html?guccounter=1&guce_referrer_us=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_cs=bprsCUfDxU9v6H2W7bTUfw. Zugegriffen: 3. Jan. 2019.

Lobo, S. (11. Februar 2019). Umgang mit Gewalttaten: Ja zur privaten Social-Media-Notwehr! *SPIEGEL Online Debatten-Podcast*. https://soundcloud.com/user-728223693/umgang-mit-gewalttaten-ja-zur-privaten-social-media-notwehr. Zugegriffen: 18. Febr. 2019.

Lynskey, D. (21. Februar 2017). The rise and fall of Milo Yiannopoulos – How a shallow actor played the bad guy for money. *The Guardian*. https://www.theguardian.com/world/2017/feb/21/milo-yiannopoulos-rise-and-fall-shallow-actor-bad-guy-hate-speech. Zugegriffen: 12. März 2019.

Maercker, A., & Mehr, A. (2006). What if victims read a newspaper report about their victimization? A study on the relationship to ptsd symptoms in crime victims. *European Psychologist, 11,* 137–142.

Maiaroto, T. (26. November 2013). The average life span of viral web content. *Social Media Today*. https://www.socialmediatoday.com/content/average-life-span-viral-web-content. Zugegriffen: 21. Febr. 2019.

Mallén, A. (2016). Stirring up virtual punishment: A case of citizen journalism, authenticity and shaming. *Journal of Scandinavian Studies in Criminology and Crime Prevention, 17*(1), 3–18.

Malone, N. (24. Juli 2017). Zoë and the Trolls. *New York Magazine*. http://nymag.com/intelligencer/2017/07/zoe-quinn-surviving-gamergate.html. Zugegriffen: 5. März 2019.

Martin, R. (2007). Digilante justice: Citizenship in cyberspace. *The New Atlantis, 16,* 124–127.

Marx, G. T., & Archer, D. (1976). Community Police Patrols and Vigilantism. In H. J. Rosenbaum & P. C. Sederberg (Hrsg.), *Vigilante Politics* (S. 129–157). University of Pennsylvania Press.

Massaro, T. (1991). Shame, culture, and American criminal law. *Michigan Law Review, 89*(7), 1880–1944.

McCarthy, N. (23. Oktober 2014). Online harassment: Who's most at risk? *Forbes*. https://www.forbes.com/sites/niallmccarthy/2014/10/23/online-harassment-whos-most-at-risk-infographic/#5813cb2d58d9. Zugegriffen: 12. Febr. 2019.

McDonald, D. (2014). The politics of hate crime: Neoliberal vigilance, vigilantism and the question of Paedophilia. *International Journal for Crime, Justice and Social Democracy, 3*(1), 68–80.

McLure, H. (2000). The wild, wild web: The mythic American West and the electronic frontier. *The Western Historical Quarterly, 31*(4), 457–476.

Meloy, M. L., & Miller, S. L. (2010). *The Victimization of Women: Law, Policies, and Politics*. New York: Oxford University Press.

Menzel, S. (28. Juli 2016). Polizei warnt vor Selbstjustiz im Internet: Facebook-Fahndung hat Folgen. *Neue Westfälische Zeitung*. https://www.nw.de/lokal/kreis_guetersloh/guetersloh/20870208_Polizei-Guetersloh-warnt-vor-Selbstjustiz.html. Zugegriffen: 13 Febr. 2019.

Milivojevic, S., & McGovern, A. (2014). The death of Jill Meagher: Crime and punishment on social media. *International Journal for Crime, Justice and Social Democracy, 3*(3), 22–39.

Molloy, M. (25. Juni 2018). Online shaming: The dangerous rise of the internet Pitchfork Mob. *The Telegraph*. https://www.telegraph.co.uk/news/2018/06/25/online-shaming-dangerous-rise-internet-pitchfork-mob/. Zugegriffen: 24. Febr. 2019.

Moncada, E. (2017). Varieties of vigilantism: Conceptual discord, meaning and strategies. *Global Crime, 18*(4), 403–423.

Moore, C. (21. September 2016). Send in the clown: Internet supervillain milo doesn't care that you hate him. *Out Magazine*. https://www.out.com/out-exclusives/2016/9/21/send-clown-internet-supervillain-milo-doesnt-care-you-hate-him. Zugegriffen: 12. März 2019.

Moore, M., Nakano, T., Enomoto, A., & Suda, T. (2012). Anonymity and roles associated with aggressive posts in an online forum. *Computers in Human Behavior, 28*(3), 861–867.

Morozov, E. (2. Juli 2009). Mobile vigilantism or geek justice? *Foreign Policy*. https://foreignpolicy.com/2009/07/02/mobile-vigilantism-or-geek-justice/. Zugegriffen: 21. März 2019.

Murphy, T. (26. April 2013). The internet is actually surprisingly good at fighting crime. *Mother Jones*. https://www.motherjones.com/politics/2013/04/reddit-internet-solving-fighting-crime/. Zugegriffen: 21. März 2019.

Myles, D., & Trottier D. (2017). Leveraging visibility, gaining capital? Social media use in the fight against child abusers: The case of Judge Beauce. *Social Media+Society 3*(1), 1–12.

Nhan, J., Huey, L., & Broll, R. (2017). Digilantism: An analysis of crowdsourcing and the Boston marathon bombing. *British Journal of Criminology, 57,* 341–361.

Noble, W. (2017). Cyber-vigilantism – How the cyber mob behaves. In T. Owen, W. Noble, & F. C. Speed (Hrsg.), *New perspectives on cybercrime* (S. 45–61). London: Palgrave Macmillan. (Palgrave Studies in Cybercrime and Cybersecurity).

SPIEGEL Online. (17. Oktober 2018). Sigi Maurer: Initiative gegen Hass im Netz sammelt 100.000 Euro. http://www.spiegel.de/panorama/sigi-maurer-initiative-gegen-hass-im-netz-sammelt-100-000-euro-a-1233711.html. Zugegriffen: 24. März 2019.

Otto, N. (2002). *Kriminalitätsberichterstattung und ihre Auswirkungen auf die Opfer und ihr soziales Umfeld. Wie beurteilen Kriminalitätsopfer die Berichterstattung über ihren eigenen Fall?* Unveröffentlichte Dissertation. Mainz: Johannes-Gutenberg-Universität.

Paul, A. T. (2005). Die Rache und das Rätsel der Gabe. *Leviathan, 33,* 240–256.

Peelo, M. (2006). Framing homicide narratives in newspapers: Mediated witness and the construction of virtual victimhood. *Crime Media Culture, 2*(2), 159–175.

Penny, L. (1. Mai 2013). Die netten Jungs von nebenan. *EMMA*. https://www.emma.de/artikel/steubenville-die-netten-jungs-von-nebenan-266288. Zugegriffen: 15. Jan. 2019.

Perraudin, F. (24. April 2017). Paedophile hunters jeopardising police work, says senior officer. *The Guardian*. https://www.theguardian.com/society/2017/apr/24/paedophile-hunters-jeopardising-police-work-child-protection. Zugegriffen: 24. Febr. 2019.

Petersen, M. (21. November 2014a). Gewaltvideo aus Tübingen: Appelle nach Prügelattacke auf Schülerin. *Stuttgarter Zeitung*. https://www.stuttgarter-zeitung.de/inhalt.gewaltvideo-aus-tuebingen-appelle-nach-pruegelattacke-auf-schuelerin.332ebe2a-aa95-46e2-aec9-bb254edd06c6.html. Zugegriffen: 15. Jan. 2019.

Petersen, M. (21. November 2014b). Gewaltvideo aus Tübingen: Die Reaktionen der Jugendlichen im Netz. *Stuttgarter Zeitung*. https://www.stuttgarter-zeitung.de/inhalt.gewaltvideo-aus-tuebingen-appelle-nach-pruegelattacke-auf-schuelerin-page1.332ebe2a-aa95-46e2-aec9-bb254edd06c6.html. Zugegriffen: 15. Jan. 2019.

Phillips, B. (2017). Inequality and the emergence of vigilante organizations: The case of Mexican Autodefensas. *Comparative Political Studies, 50*(10), 1358–1389.

Powell, A. (2015). Seeking rape justice: Formal and informal responses to sexual violence through technosocial counter-publics. *Theoretical Criminology, 19*(4), 571–588.

Powell, A., & Henry N. (2017). *Sexual violence in a digital age*. Palgrave Studies in Cybercrime and Cybersecurity. London: Palgrave Macmillan.

Powell, A., Overington, C., & Hamilton, G. (2018). Following #JillMeagher: Collective meaning-making in response to crime events via social media. *Crime Media Culture, 14*(3), 1–20.

Pratten, D., & Sen, A. (2008). *Global vigilantes*. New York: Columbia University Press.

Presser, L., & Sandberg, S. (2014). Narrative criminology for these times. *British Society of Criminology Newsletter, 75,* 7–10.

Quent, M. (2016a). *Bürgerwehren – Hilfssheriffs oder inszenierte Provokation?* Berlin: Amadeu Antonio Stiftung.

Quent, M. (2016b). Selbstjustiz im Namen des Volkes: Vigilantistischer Terrorismus. *Aus Politik und Zeitgeschichte* (APuZ). Bundeszentrale für Politische Bildung. https://www.bpb.de/apuz/228868/vigilantistischer-terrorismus?p=all. Zugegriffen: 8. März 2019.

Robertz, F., & Kahr, R. (2016). Am Anfang war das Wort – Ein kommunikationswissenschaftlicher Blick auf Berichterstattung als Anlass zur Eskalation von Gewalt. In F. Robertz & R. Kahr (Hrsg.), *Die mediale Inszenierung von Amok und Terrorismus* (S. 13–27). Wiesbaden: VS Verlag.

Robertz, F., Oksanen A., & Räsänen P. (2016). *Viktimisierung junger Menschen im Internet. Leitfaden für Pädagogen und Psychologen.* Wiesbaden: Springer.

Ronson, J. (2015a). *So you've been publicly shamed*. New York: Riverhead Books.

Ronson, J. (12. Februar 2015b). How one stupid tweet blew up Justine Sacco's life. *The New York Times*. https://www.nytimes.com/2015/02/15/magazine/how-one-stupid-tweet-ruined-justine-saccos-life.html. Zugegriffen: 20. Febr. 2019.

Rose, M., & Fox, R. (2014). Public engagement with the criminal justice system in the age of social media. *Oñati Socio-Legal Series, 4*(4), 771–798.

Rüdiger, T.-G. (2017). Der digitale Raum – Ein polizeifreier Verkehrsraum? Der Rechtsstaat zwischen Präsenz, Selbstjustiz und Legalitätsprinzip. In B. Frevel & M. Wendekamm (Hrsg.), *Sicherheitsproduktion zwischen Staat, Markt und Zivilgesellschaft* (S. 213–239). Wiesbaden: VS Verlag.

Rüdiger, T.-G., & Bayerl, S. (2018). *Digitale Polizeiarbeit: Herausforderungen und Chancen*. Wiesbaden: Springer VS.

Ryan, E. G. (6. Februar 2015). How to make an accused rapist look good. *Jezebel*. https://jezebel.com/how-to-make-an-accused-rapist-look-good-1682583526. Zugegriffen: 3. März 2019.

Saliger, F. (2013). Aushöhlung der Unschuldsvermutung durch gezielte Öffentlichkeit? *Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft, 96*(3), 173–187.

Sallavaci, O. (2018). Crime and social media: Legal responses to offensive online communications and abuse. In H. Jajankhani (Hrsg.), *Cyber Criminology, Advanced Sciences and Technologies for Security Applications* (S. 3–23). Cham: Springer Nature Switzerland AG.

Salter, M. (2017). *Crime, justice and social media*. London: Routledge.

Schaschek, S. (12. August 2014). Brutale Drohungen im Internet: Hetze gegen Genderforscherinnen. *Tagesspiegel*. https://www.tagesspiegel.de/wissen/brutale-drohungen-im-internet-hetze-gegen-genderforscherinnen/10318416.html. Zugegriffen: 13. März 2019.

Schmidt-Lux, T. (2013). Vigilantismus als politische Gewalt. Eine Typologie. *BEHEMOTH*: *A Journal on Civilization* 6(1), 98–117.

Schmidt-Lux, T. (2017). *Gerechte Strafe: Legitimationskonflikte um vigilante Gewalt*. Weinheim: Beltz Juventa.

Schmidt-Lux, T. (2018). Anspruch und Glauben. Vigilantismus als Herausforderung staatlicher Legitimität. In P. Stekeler-Weithofer & B. Zabel (Hrsg.), *Philosophie der Republik* (S. 142–155). Tübingen: Mohr Siebeck.

Schmoll, T. (26. April 2013). Tripathi, zu Unrecht verdächtigt, ist tot. *Stern*. https://www.stern.de/politik/ausland/nach-dem-terroranschlag-von-boston-tripathi–zu-unrecht-verdaechtigt–ist-tot-3210370.html. Zugegriffen: 24. Febr. 2019.

Schneider, C. J., & Trottier, D. (2012). The 2011 vancouver riot and the role of facebook in crowd-sourced policing. *BC Studies, 175,* 57–72.

Shaw, E. (16. September 2014). Philly hate suspects tracked down by anonymous twitter hero. *Gawker*. https://gawker.com/philly-hate-crime-suspects-tracked-down-by-anonymous-tw-1635661609. Zugegriffen: 5. März 2019.

Shontell, A. (27. Juli 2013). What it's like when reddit wrongly accuses your loved one of murder. *Business Insider*. https://www.businessinsider.com/reddit-falsely-accuses-sunil-tripathi-of-boston-bombing-2013-7?IR=T. Zugegriffen: 24. Febr. 2019.

Shotland, L. (1976). Spontaneous Vigilantes. *Society 13*(3), 30–32.

Silke, A. (2001). Dealing with vigilantism: Issues and lessons for the police. *The Police Journal, 74,* 120–133.

Skoric, M. M., Chua, J. P. E., Liew, M. A., Wong, K. H., & Yeo, P. J. (2010). Online Shaming in the Asia context: Community empowerment of civic vigilantism? *Surveillance & Society, 8*(2), 181–199.

Smallridge, J., Wagner, P., & Crowl, J. N. (2016). Understanding cyber-vigilantism: A conceptual framework. *Journal of Theoretical & Philosophical Criminology, 8*(1), 57–70.

Smith, D. (30. April 2006). Mobile vigilantes snap sex pests in action. *The Guardian*. https://www.theguardian.com/technology/2006/apr/30/news.theobserver. Zugegriffen: 6. März 2019.

Snyder, P., Doerfler P., Kanich C., & McCoy, D. (1.–3. November 2017). Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxing. *IMC Conference*. London.

Stalder, F. (2017). *Kultur der Digitalität*. Berlin: Suhrkamp.

Stegbauer, C. (2001). *Grenzen virtueller Gemeinschaften*. Wiesbaden: Westdeutscher Verlag.

Stengel, E. (2. Juli 2018). Selbstjustiz: Nach Pädophilie-Beitrag: Medienanstalt geht gegen RTL vor. *Augsburger Allgemeine Zeitung*. https://www.augsburger-allgemeine.de/panorama/Nach-Paedophilie-Beitrag-Medienanstalt-geht-gegen-RTL-vor-id51536441.html. Zugegriffen: 23. Dez. 2018.

Stratton, G., Powell, A., & Cameron, R. (2016). Crime and justice in digital society: Towards a ‚digital criminology'? *International Journal for Crime, Justice, and Social Democracy, 6*(2), 17–33.

Straziuso, J. (7. März 2004). TV stations draw fire for sex stings: Reports set up with assistance of vigilante group. *The Arizona Republic*.

BITKOM Studie. (2017). Cybercrime: Jeder zweite Internetnutzer wurde Opfer. https://www.bitkom.org/Presse/Presseinformation/Cybercrime-Jeder-zweite-Internetnutzer-wurde-Opfer.html. Zugegriffen: 23. März 2019.

Suler, J. (2004). The online disinhibition effect. *Cyberpsychology & Behavior, 7*(3), 321–326.

Tankebe, J. (2009). Self-Help, policing, and procedural justice: Ghanaian vigilantism and the rule of law. *Law & Society Review, 43*(2), 245–269.

Thissen, T. (30. Mai 2012). Lynchmob in Emden: „Lasst uns das Schwein tothauen. *DIE WELT*. https://www.welt.de/vermischtes/article106394394/Lasst-uns-das-Schwein-tothauen.html. Zugegriffen: 18. Febr. 2019.

Tiku, N., & Newton C. (4. Februar 2015). Twitter CEO: ‚We Suck at Dealing with Abuse.' *The Verge*. https://www.theverge.com/2015/2/4/7982099/twitter-ceo-sent-memo-taking-personal-responsibility-for-the. Zugegriffen: 23. Febr. 2019.

Tripp, T. M., Bies, R. J., & Aquino, K. (2007). A vigilante model of justice: Revenge, reconciliation, forgiveness, and avoidance. *Social Justice Research, 20*(1), 10–34.

Trottier, D. (2017). Digital vigilantism as weaponization of visibility. *Philosophy and Technology, 30,* 55–72.

Tyler, T. (2006). Why People Obey the Law. Princeton: Princeton University Press.

Van Dijk, J. (2013). *The culture of connectivity: A critical history of social media*. Oxford: Oxford University Press.

Voskamp, F., & D.-K. Kipker. (2013). Virtueller Pranger Internet: „Shitstorm" und „Cybermobbing" als Bühne für die Meinungsfreiheit? – Providerpflichten nach der BGH-Rechtsprechung. *DuD – Datenschutz und Datensicherheit 12,* 787–790.

Wall, D., & Williams, M. (2007). Policing Diversity in the digital age: Maintaining order in virtual communities. *Criminology & Criminal Justice, 7*(4), 391–415.

Warren, I. (2009). *Vigilantism, the Press and Signal Crimes 2006–2007. Australian and New Zealand Critical Criminology Conference* (S. 275–284). Melbourne: Monash University.

Wehmhoener, K. A. (2010). Social norm or social harm: An exploratory study of internet vigilantism. Master's Thesis. Greenlee School of Journalism and Communication, Iowa State University. https://lib.dr.iastate.edu/etd/11572/.

Wergins, C. (6. August 2017). Deutscher Student sieht sich als Opfer von Rufmord. *Die Welt*. https://www.welt.de/vermischtes/article167413440/Deutscher-Student-sieht-sich-als-Opfer-von-Rufmord.html. Zugegriffen: 5. März 2019.

Wettlaufer, J. (2015). The shame game. *RSA Journal, 161*(5564), 36–39.

Wiedemann, C. (2014). Between swarm, network, and multitude: Anonymous and the infrastructures of the common. *Distinktion: Scandinavian Journal of Social Theory 15*(3), 309–326.

Winter, M. (2003). Metamorphosen des staatlichen Gewaltapparates: Über die Entwicklung von Polizei und Militär in Deutschland. *Leviathan, 31*(4), 519–555.

Yar, M. (2012). Crime, media and the will-to-representation: Reconsidering relationships in the new media age. *Crime, Media, Culture 8*(3), 245–260.

Yardley, E., Lynes, A. G. T., Wilson, D., & Kelly, E. (2018). What's the deal with ‚Websleuthing'? News media representations of amateur detectives in networked spaces. *Crime Media Culture, 14*(1), 81–109.

Young, C. (3. Februar 2015). Columbia Student: I Didn't Rape Her. Daily Beast. https://www.thedailybeast.com/columbia-student-i-didnt-rape-her. Zugegriffen: 20. Jan. 2020.

Zabel, B. (2011). "Öffentliche Pranger" und reformierter Strafprozess: Aktuelle Tendenzen der Medialisierung vor und während des Ermittlungsverfahrens. *Goltdammer's Archiv, 158,* 347–364.

Zadrozny, B. (2. Januar 2019). He Lures alleged child predators and shames them on facebook. Now one of his targets is dead. *NBC News*. https://www.nbcnews.com/news/us-news/he-lures-alleged-child-predators-shames-them-facebook-now-one-n953856. Zugegriffen: 23. Febr. 2019.

Zedner, L. (2006). Policing before and after the police: Historical antecedents of contemporary crime control. *The British Journal of Criminology, 46*(1), 78–96.

Die Zeit. (24. Januar 2013). Ariane Friedrich: „Ich bin hier das Opfer, nicht der". Online Ausgabe. https://www.zeit.de/digital/internet/2013-01/ariane-friedrich-stalking-facebook?. Zugegriffen: 13 Febr. 2019.

Süddeutsche Zeitung. (18. März 2013). Steubenville-Prozess: Football-Spieler wegen Vergewaltigung verurteilt. https://www.sueddeutsche.de/panorama/steubenville-prozess-football-spieler-wegen-vergewaltigung-verurteilt-1.1627051. Zugegriffen: 4. März 2019.

Zetter, K. (21. November 2007). Cyberbullying suicide stokes the internet fury machine. *Wired*. https://www.wired.com/2007/11/cyberbullying-suicide-stokes-the-internet-fury-machine/. Zugegriffen: 12. Jan. 2019.

Digitale Rechtsdurchsetzung

Ist der Rechtsstaat automatisierbar?

Claudia Otto

Vorwort

„Wir müssen bei der Durchsetzung des Rechts besser werden – schnell, konsequent, sichtbar“, sagte der amtierende Bundestagspräsident Wolfgang Schäuble am 11. September 2018 im Bundestag (Welt 2018). *„Wir brauchen keine Revolution, sondern einen starken und toleranten Rechtsstaat“,* betonte Schäuble weiter (Welt 2018).

Seine Aussage ist nicht auf den Kontext des aktuell im Fokus stehenden, besorgniserregenden Rumorens am rechten Rand beschränkbar; der Rechtsstaat schwächelt und bummelt in vielen Bereichen. Dementsprechend fordert Bundesministerin der Justiz und für Verbraucherschutz sowie Chefin des sog. „Effizienzministeriums“ Dr. Katarina Barley einen Pakt für den Rechtsstaat und sein Verständnis als Daueraufgabe (Dokumente, Bundestag BT-Drs. 193400). Daneben verspricht die Bewegung um sog. „Legal Tech“ mehr Effizienz der Rechtsdienstleistung durch Automatisierung: Den Menschen soll ohne Rechtsanwälte und sogar ohne Gerichte schneller, besser und günstiger – gar kostenlos – zu ihrem Recht verholfen werden. Juristen und Nichtjuristen diskutieren darüber hinaus u. a. über sich angeblich selbstvollziehende kluge Verträge („Smart Contracts“).

Die Erwartungen an den Gesetzgeber, das „Effizienzministerium“ und zeitgleich den „Knight Rider des 21. Jahrhunderts“, den Algorithmus, sind groß. Die technologischen Entwicklungen einerseits und die sie anwendenden Gedanken andererseits sind allerdings zu weit voraus, um sie als Legislative und Exekutive demnächst einholen zu können. Schnelligkeit ist also nicht zu erwarten. Hat der starke und tolerante Rechtsstaat unter diesen Umständen also zu tolerieren,

C. Otto (✉)
Frankfurt, Deutschland
E-Mail: claudia.otto@rechtinnovativ.online

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

T.-G. Rüdiger und P. S. Bayerl (Hrsg.), *Cyberkriminologie,*
https://doi.org/10.1007/978-3-658-28507-4_23

dass die Durchsetzung von Recht und Gesetz vorverlagert und in die „Hände“ von Privaten und gar Algorithmen gelegt wird? Kann auch darin die geforderte Konsequenz des Rechtsstaates liegen? Oder bedeutet diese Entwicklung sogar die Aufweichung der Gewaltenteilung und damit des Rechtsstaates selbst?

Der Beitrag widmet sich den Fragen:

1. Was die Digitalisierung für das geradezu hölzerne Rechtssystem bedeutet;
2. Wo der Bedarf an staatsunabhängiger, technologiegestützter Rechtsdurchsetzung aktuell besonders groß ist,
   a. was dies für die Vertragsfreiheit bedeutet,
   b. welche Chancen und
   c. welche Gefahren sich hieraus ergeben;
3. Welche Handlungsimplikationen sich hieraus für Legislative, Exekutive und Judikative ergeben.

1 Was bedeutet die Digitalisierung für das geradezu hölzerne Rechtssystem?

„Hölzernes Rechtssystem“ klingt beinahe frevelhaft. Doch kann dieser Begriff tatsächlich als eine Beschreibung für einen weit verbreiteten physischen Noch-Zustand der Arbeitsplätze in der Justiz verstanden werden. Veraltetes Inventar, veraltete Arbeitsmittel, veraltete Kommunikationsweise: Eine identische elektronische Akte für telefonische Auskünfte, wenn die Papierakte gerade nicht zur Hand ist? In der Regel Fehlanzeige: Die Digitalisierung erscheint nirgends so weit entfernt wie von der Justiz.

Doch auch in seiner Reaktion auf die verschiedenen Ersuche der Bürger um Recht erweist sich der Rechtsstaat, insbesondere die deutsche Justiz, als hölzern und überfordert. Die Berichte über eine überlastete deutsche Justiz häufen sich (beispielhaft „Justiz in Not: Deutschlands Richter am Limit“, MDR 2019). Während die Verfahren immer mehr werden, fehlt es am notwendigen Personal, um diese zu bearbeiten und einer zeitnahen Entscheidung zuzuführen. Die Digitalisierung kann dem kaputtgesparten (Pröbel, Vorsitzender Richter der Jugendstrafkammer, Landgericht Erfurt in „Justiz in Not: Deutschlands Richter am Limit“, MDR 2019) Rechtsstaat helfen. Neue Technologien erlauben ein effizienteres Miteinanderarbeiten, nicht nur in einer Geschäftsstelle, sondern auch mit den Verfahrensbeteiligten. Allein eine vollständige, mit der ggf. noch vorhandenen Papierakte identische elektronische Akte, in die Geschäftsstellenmitarbeiter und Richter gleichzeitig hineinschauen können, erspart viel Transportzeit und -aufwand sowie unnötige Kommunikation mit den Verfahrensbeteiligten, etwa durch

Wegfall der Erkundigungsanrufe oder schriftlichen Mitteilungen der Aktenabwesenheit.

Eine Umstellung der Arbeitsweise dauert. Monate, sogar Jahre. Nicht ohne Grund sieht das Gesetz zur Einführung der elektronischen Akte in der Justiz und zur Förderung des elektronischen Rechtsverkehrs vom 5. Juli 2017 in Artikel 11 zur Änderung der Zivilprozessordnung (ZPO) und § 298a ZPO vor, in einem neuen Absatz 1a, Satz 1, zu regeln, dass die Gerichtsakten ab dem 1. Januar 2026 (!) elektronisch geführt werden. Für die Familien-, Arbeits- und Sozialgerichte, Verwaltungs- und Finanzgerichte sind entsprechende Vorschriften vorgesehen. Nur in der Strafprozessordnung bleibt die elektronische Aktenführung bis zum 31. Dezember 2025 fakultativ, vorbehaltlich abweichender Bestimmungen durch die Bundesregierung und Landesregierungen: § 32 Abs. 1 S. 1 StPO lautet auf *„Die Akten können elektronisch geführt werden“*.

Wenn bereits die Umstellung auf die elektronische Akte noch mindestens sechs Jahre dauern kann, kann man sich vorstellen, wie viel Zeit die Digitalisierung anderer Prozesse voraussichtlich in Anspruch nehmen wird. Die erwähnte Überbelastung von Gerichten und Behörden führt zwangsläufig zu weniger Zeit für einen einzelnen Rechtsfall: Ab- und Verkürzungen zulasten der Akzeptanz der Rechtssuchenden und sogar des Rechts selbst sind die Folge. Diese Probleme kann die elektronische Akte allein nicht lösen. Auch ist zu berücksichtigen, dass staatliche Digitalisierungsbemühungen erheblich unter Minder- und Schlechtleistung von beauftragten Dienstleistern leiden und ausgebremst werden können. Die Erfolgs- und Risikofaktoren sind vielfältig. Der Wille des Gesetzgeberkopfes ist stark, doch das Muskelfleisch ist schwach, wie der Fall des besonderen elektronischen Anwaltspostfach (kurz: beA) gezeigt hat (beispielhaft: Böck 2019).

Das Bedürfnis der Bürger nach zeitnaher Durchsetzung ihrer Rechte kann jedoch nicht Jahre warten. Strafe verliert mit der Zeit an Bedeutung. Zeit bedeutet in die Länge gezogene Qualen für Geschädigte. Die Nichtverfolgung von Straftaten wegen überlasteten Strafverfolgungsbehörden vermittelt zusätzlich den Eindruck von Bedeutungslosigkeit der Taten und Opfer. Überlastete Richter sind Menschen und vor Fehlern nicht gefeit. Hastig geschlossene Prozessvergleiche zugunsten von Zeitgewinn bedeuten Verlust im Sinne eines schnellen Endes mit Schrecken. Mit dem spürbaren Sand im rechtsstaatlichen Getriebe wird aus dem Rechtssicherheits- und Rechtsfriedensversprechen der grundgesetzlich vorgesehenen Rechtsweggarantie (Art. 19 Abs. 4 GG) eine gefühlte Garantie des Rechts- und Bedeutungsverlusts.

Daher wird in der juristischen und nichtjuristischen Gesellschaft nach anderen Lösungen der Rechtsdurchsetzung gesucht: Runter vom Holzweg und schwimmen mit (oder gegen) dem Strom.

2 Wo der Bedarf an staatsunabhängiger, technologiegestützter Rechtsdurchsetzung aktuell besonders groß ist

Staatsunabhängige Rechtsdurchsetzung schränkt den hier zu diskutierenden Themenbereich erheblich ein: So liegt das sog. Strafmonopol beim Staat, nicht beim Verletzten. Die Verfolgung und Ahndung von Straftaten ist allein Recht und Pflicht des Staates. Auch das Verwaltungsrecht, das Sozial- und Steuerrecht regeln schwerpunktmäßig die Rechte und Pflichten zwischen Bürger und Staat: zu- und untereinander, in der Regel in einem Über-/Unterordnungsverhältnis. Aus dieser Beziehung kann sich der Bürger nicht ohne entsprechende Rechteeinräumung von Staatsseite her herauslösen und Staatsunabhängigkeit herstellen. Staatsunabhängige, technologiegestützte Rechtsdurchsetzung kann daher nur dort in Betracht kommen, wo die Rechte und Pflichten natürlicher und juristischer Personen im Wesentlichen frei untereinander und im Vorhinein bestimmt werden können; nämlich im Rahmen des zivilrechtlichen Vertrags.

2.1 Vertragsfreiheit

Die Vertragsfreiheit ist eine tragende Säule unserer freiheitlichen Gesellschaft und nach der Rechtsprechung des Bundesverfassungsgerichts Ausfluss des Grundrechts der allgemeinen Handlungsfreiheit (Art. 2 Abs. 1 GG, BVerfGE 8, 274, Rn 212 ff.). Das Bürgerliche Gesetzbuch (BGB) ist ein sie konkretisierendes und näher ausgestaltendes Gesetz. Die Automatisierung von vertraglichen Regelungen fällt ebenso hierunter; sie darf die Vertragsfreiheit allerdings nicht einseitig zulasten des Vertragspartners oder mehrerer anderer Vertragsparteien einschränken. Insbesondere sind sog. Allgemeine Geschäftsbedingungen nicht papierabhängig (vgl. § 305 Abs. 1 S. 2 BGB: *„Gleichgültig ist, […] welche Form der Vertrag hat“*).

2.1.1 Pacta sunt servanda: Verträge sind einzuhalten

Der Gedanke ist schnell erfassbar: Wo die Vertragsparteien gemeinsam über die Konditionen ihres Zusammenwirkens frei bestimmen können, können sie ebenso gemeinsam über die Konditionen des weiteren Miteinanders oder der Trennung im Falle eines Konfliktes entscheiden. Ein gerichtlicher Vergleich zur Beendigung eines Rechtsstreits ist nichts anderes als ein (neuer) Vertrag; und die wohl beliebteste Form der schnellen und arbeitsarmen Rechtsstreitbeendigung unter Richtern in Zeiten überlasteter Gerichte.

Der Nachteil des Prozessvergleichs ist, er kostet Gerichts- und Anwaltsgebühren. Der Vorteil des gerichtlichen Vergleichs ist, er stellt einen tauglichen Vollstreckungstitel dar (§ 794 Abs. 1 Nr. 1 ZPO). Liegen sämtliche Vollstreckungsvoraussetzungen vor, kann hieraus die Zwangsvollstreckung betrieben werden: Diese Voraussetzungen sind der Vollstreckungsantrag, der Vollstreckungstitel (hier der Prozessvergleich), die Vollstreckungsklausel (der amtliche Vermerk der Vollstreckbarkeit auf dem gerichtlichen Vergleichsdokument) und die Zustellung des Vollstreckungstitels.

Der Nachteil wiederum: Auch die Zwangsvollstreckung erfolgt nicht kostenlos.

Warum also sollen die Parteien solche Konfliktlösungen nicht zeitlich früher und kostensparend regeln; gegebenenfalls sogar zum Zeitpunkt des ursprünglichen Vertragsschlusses, aus dem der Konflikt sich erst ergeben hat. In Kombination mit einer technischen „Vollstreckungslösung“. Verträge sind schließlich einzuhalten.

2.1.2 Das Problem der mangelnden Vorhersehbarkeit des Lebens

Der Mensch kann die Zukunft allerdings nicht vorhersehen. Wer Verträge abschließt, vertraut sich in einem Mindestmaß; sonst würde man keinen Vertrag eingehen. Wo konfliktträchtige Umstände erwartungsgemäß hinzutreten können, bestimmen die Parteien vorausschauend Konfliktlösungsregelungen unter Berücksichtigung ihrer beider Interessen. Wo die Vertragsparteien im Verlaufe des Lebens mit Unwägbarkeiten und Unsicherheiten rechnen müssen, verwenden sie regelmäßig abstrakt formulierte, situationsangemessen näher zu bestimmende Vertragsbestimmungen, um eine Vielzahl möglicher Konfliktfälle zu Befriedungszwecken erfassen zu können. Hierdurch wird einander eine angemessene Kontrolle über die Vertragsbeziehung eingeräumt und Vertrauen ineinander geschaffen.

Technologie-basierte vorausschauende Lösungen können diese Unvorhersehbarkeit und damit Vielgestaltigkeit des Lebens sowie die Vielfältigkeit der Auslegung einer abstrakten Formulierung nach dem Willen der Vertragsparteien (§§ 133, 157 BGB) nicht abdecken. Dabei ist es völlig gleich, welche Technologie verwandt wird. Ob etwa rein regelbasierte Entscheidungsfindung durch einen simplen Algorithmus oder komplexes Machine Learning, das v. a. auf eingespeisten und statistisch bewerteten Daten basiert: entscheidungserheblich ist stets im Vorhinein ausgewähltes, i.e. veraltetes Vorwissen. Einen Konflikt wegen der fehlenden Vorhersehbarkeit nicht lösen zu können, schlimmstenfalls sogar zu verschlimmern infolge einer Fehlinterpretation des Computers aufgrund von Altwissen, frustriert und vertieft den Konflikt anstatt ihn zu lösen.

Bei der Auslegung einer Willenserklärung ist der wirkliche Wille zu erforschen und nicht an dem buchstäblichen Sinne des Ausdrucks zu haften (§ 133 BGB). Auch Verträge sind so auszulegen, wie Treu und Glauben mit Rücksicht auf die Verkehrssitte es erfordern (§ 157 BGB). Ein Computerprogramm, i.e. die in einer Programmiersprache geschriebene Arbeitsanweisung an einen Computer (Otto 2019), basiert ausschließlich auf dem durch die Programmiersprache vorbestimmten Wortsinne. Treu und Glauben sowie Verkehrssitte sind darüber hinaus unbestimmte, ebenfalls einzelfallbezogen auszulegende Rechtsbegriffe, die sich noch dazu im steten Wandel mit der Gesellschaft befinden, die ein strikt nach Anweisung arbeitendes Computerprogramm nicht abschließend beurteilen kann.

Die Digitalisierung und (Teil-)Automatisierung von Verträgen beschränkt sich aus diesen Gründen im Wesentlichen auf die vorhersehbaren, einfach gestalteten Fälle. Hier stellt sich vor allem die Frage der Wirtschaftlichkeit: Die Herstellung solcher „Vertragsprogramme“ ist aufwendig und kostenintensiv. Ein händisch niedergeschriebener Vertragstext ist demgegenüber erheblich leichter erstellt, bildungsunabhängig und kostengünstiger als ein aufwendig gestaltetes Vertragsprogramm, das einem Computerspiel gleicht und ständiger (Sicherheits-)Updates bedarf. Der Schwerpunkt – und wirkliche Nutzen – liegt daher vor allem in der effizienteren Gestaltung der Vertragsverwaltung.

Wird nicht zuletzt das Vertrauen der Vertragsparteien in- und zueinander durch einen Vertragsbruch gestört oder gar zerstört – auch dieser Umstand ist regelmäßig nicht vorhersehbar – wird eine Konfliktlösung unter Einbindung einer neutralen Stelle erforderlich sein.

2.1.3 Gesetzlich geregelte Konfliktlösung versus regelbasierte Konfliktlösung

Das Beispiel der potenzialreichen Online-Streitbeilegung für Fälle des Streits nach einem Online-Kauf (vgl. die Plattform für Online-Streitbeilegung (OS) bereitgestellt von der Europäischen Kommission) steht für die tatsächliche Möglichkeit der schnellen und kostengünstigen, weil Algorithmen-gestützten Konfliktlösung, insbesondere im grenzüberschreitenden Bereich, wo zusätzlich die Rechtswahl Streitpotential birgt.

Auch die komplexeren Prozessordnungen (u. a. Straf-, Zivil-, Verwaltungsprozessordnungen) sind nichts anderes als vorbestimmte Regeln für den Ablauf des Konfliktlösungsprozesses. Dabei ist die Komplexität und auch Abstraktheit, die wiederum sehr viel mit der Unvorhersehbarkeit des Lebens zu tun hat, der

wohl merklichste Unterschied zu einer Onlinemediation für Kaufvertragsstreitigkeiten: Die Prozessordnungen müssen für sämtliche denkbaren und nicht vorhersehbaren Fälle ihres jeweiligen Rechtsgebiets funktionieren.

Ein Konflikt, der – erwartungsgemäß – im Rahmen einer Algorithmen-basierten Onlinemediation nicht oder für beide Vertragsparteien nicht zufriedenstellend gelöst werden kann, kann immer noch den Rechtsweg wählen, in dem ein menschlicher Richter den konkreten Fall prüft und entscheidet. Gleiches gilt für Angebote sog. „Legal Techs"; Unternehmen, die mithilfe von (vermeintlich) Algorithmen-gestützten Online-Angeboten schnelles und günstiges Recht versprechen. Zum Gericht muss am Ende doch noch ein Rechtsanwalt, aus Fleisch und Blut, mit zwei Staatsexamina ausgestattet, gehen. Die hohe See wird hier nicht umschifft (vgl. „Vor Gericht und auf hoher See ist man in Gottes Hand"), sondern eigentlich nur das Kostenrisiko modifiziert.

3 Chancen der Automatisierung von vertraglichen Ansprüchen

Ein Anspruch ist das Recht, von einem anderen ein Tun oder Unterlassen verlangen zu können (§ 194 Abs. 1 BGB). Im Unterschied zu einem komplexen Gebilde wie dem Vertrag kann also dieser grundsätzlich auch anhand vorbestimmter algorithmischer Regeln festgelegt und damit automatisiert werden. Je komplexer die Bedingungen des Anspruchs allerdings, desto weniger ist er automatisierbar, oder schlicht wirtschaftlich unsinnig. So ist es insbesondere wichtig, einen „Stopp-Knopf" vorzusehen, der im Falle des Eintretens unvorhersehbarer Probleme die Entstehung eines Schadens und damit Konfliktes verhindert sowie Anpassungsgespräche veranlasst, wie sie normalerweise üblich sind.

Sog. „Smart Contracts" etwa, „auf einer Blockchain laufende" Computerprogramme, sollen ihrem Zweck nach nicht zu stoppen sein. Würden unter ihrer Nutzung Ansprüche und Verträge automatisiert, wird zwangsläufig Konflikt provoziert und nicht vermieden. Kluge Automatisierung lässt dort, wo das unvorhersehbare Leben hinzutritt, Denkpausen zu. Dann sind Chancen der Digitalisierung im Rahmen der Gesetze nutzbar und digitale Lösungen sogar nützlich. Wer jedoch einen vermeintlichen Anspruch dahin gehend erschafft, dass er ein Recht, einen anderen zu einem Tun oder Unterlassen zu zwingen, darstellen soll, der handelt rechtswidrig.

3.1 Gefahren, die sich hieraus ergeben

Problematisch wird es also dort, wo Automatisierung einseitige und für den anderen nicht erkennbare Vorteile verschaffen soll, insbesondere durch Verlagerung des Klage- und Kostenvorschussrisikos auf den schwächeren Vertragspartner, etwa den Verbraucher. Wenn ein Unternehmer etwa nach wirksam ausgeübtem Widerrufsrecht (§ 355 BGB) unter Nutzung eines sog. Smart Contracts weiterhin Zahlungen realisiert, weil dieser nicht zu stoppen ist und der Ersteller den Verbraucher hierüber nicht aufgeklärt hat bei Vertragsschluss, kann die rechtliche Wertung sogar bis hin zur strafrechtlich relevanten Benachteiligung des Verbrauchers reichen. Doch so weit muss mancher gar nicht erst gehen, um ein Vermögen mit kleinen Geldbeträgen aus (teil-)automatisierten Geschäften zu machen:

Im Falle von Massengeschäften mit relativ kleinen Beträgen von bis zu 500 EUR besteht ein großes Missbrauchsrisiko: Hier stehen Kostenrisiko und Zeitaufwand der gerichtlichen Geltendmachung regelmäßig in keinem Verhältnis zum Geldbetrag. Lediglich beispielhaft belaufen sich die Kosten eines Anwalts zur außergerichtlichen Geltendmachung von 100,00 EUR auf regelmäßig 83,54 EUR inklusive Umsatzsteuer. Im Falle des Unterliegens vor Gericht belaufen sich die Kosten auf insgesamt 385,55 EUR, davon sind 105 EUR Gerichtsgebühren; ein Kostenrisiko von 386 %, nebst den verlorenen 100 EUR. Das trägt so gut wie kein vernünftiger Mensch (sog. rationale Apathie). Und damit rechnen Anbieter. Auch mit der Nichtverfolgung oder Einstellung durch die überlastete Staatsanwaltschaft nach Strafanzeige.

In den Bereichen hoher, gar existenziell bedeutsamer Geldsummen ist zu erwarten, dass nur wenige Entscheidungen automatisiert werden bzw. wenig Automatisiertes zur Entscheidungsfindung genutzt wird; zu sehr stehen die Risiken außer Verhältnis zu den Chancen. Dort ist es vor allem für die „Investoren“ sinnvoller, auf gegebenenfalls teure Rechtsanwälte zu setzen, die im Schadensfall wegen Beratungsfehlern mit ihrer Berufshaftpflichtversicherung in Regress genommen werden können. „Handgemachte“ Qualität wird sich schon zum Zwecke der Schadloshaltung halten. Ganz ähnlich dem Maßanzug gegenüber dem maschinell hergestellten Anzug „von der Stange“, bei dem das Wegwerfen und Neukaufen die günstigere Konfliktlösungsstrategie ist.

4 Welche Handlungsimplikationen ergeben sich hieraus für Legislative, Exekutive und Judikative

Wie kann den genannten Gefahren beigekommen werden?

4.1 Gesetzgeber: Verbraucher stärken im Niedrigstreitwertsegment

Die aktuelle Rechtslage ist unbefriedigend, schaut man auf die Kostenrisiken bei kleinen Beträgen wie etwa den genannten 100,00 EUR, bei denen selbst der Gerichtskostenvorschuss 105,00 EUR beträgt. Der Grund für die gesetzliche Kostenstruktur ist die Entlastung der Gerichte – ein Argument, das in der heutigen Zeit der Digitalisierung und Onlinemediation nicht mehr trägt. Die Konfliktlösung sollte hier mehr und mehr für andere Lösungen geöffnet werden und nicht nur auf den Online-Kauf beschränkt werden. Eine belassene Belastung der wirtschaftlich Schwächsten ist nicht im Sinne des sonst gelebten hohen Verbraucherschutzes. Allerdings ist auch die Senkung von Gerichtskosten im Niedrigstreitwertsegment nicht zielführend, da die Gerichte hierdurch endgültig überlastet würden.

Lösungsansätze bieten die sog. Legal-Tech-Anbieter, die sich in Deutschland häufig als Inkassodienstleister nach dem Rechtsdienstleistungsgesetz (RDG) betätigen. Sie bieten, in sehr eng umrissenen und häufig gleichartig auftretenden Rechtsfällen, eine (kleine) Chance auf eine mögliche Rückerstattung des beanspruchten Geldbetrags, ohne dass der Verbraucher mit Kosten in Vorleistung gehen muss. Die Dienstleister behalten dabei in der Regel vom erfolgreich zurückgeforderten Geld einen hohen Prozentanteil als Honorar ein. Wenn es überhaupt zum Erfolg kommt: Denn ein wesentlicher und wichtiger Kritikpunkt ist hier, dass Beratungsfehler vom Anbieter bewusst einkalkuliert werden können und vom Rechtssuchenden hingenommen werden müssen. Dafür muss dieser im Falle des Unterliegens aber nichts bezahlen.

Rechtsdienstleistung durch andere als Rechtsanwälte darf jedoch grundsätzlich nicht mehr Risiko bei weniger Risikoabsicherung unterliegen: Den Rechtsanwalt treffen erhebliche Prüf- und Schutzpflichten zugunsten seines Mandanten. Für den Fall eines – noch immer menschlichen – Fehlers hat dieser zudem eine Berufs- und Vermögensschadenshaftpflichtversicherung vorzuhalten. Das Problem ist und bleibt jedoch: das übernommene Risiko kostet von Gesetzes wegen Geld. Die Risikoabsicherung wirkt sich allerdings nur sehr selten zugunsten

des Mandanten aus: mit dem fehlerunabhängigen Unterliegen und oben beschriebenen hohen Kostenrisiko ist stets zu rechnen. Auch dann ist der Rechtsanwalt zu vergüten. Damit ist im Falle der Beauftragung eines Rechtsanwalts gerade keine bessere, weil keine spürbare Risikoabsicherung gegeben.

Die Vereinbarkeit der verschiedenen, sich im Konflikt befindlichen Interessen (Verbraucher, Rechtsanwälte, „Rechtsdienstleister“) wird derzeit hitzig diskutiert. Die Rechtsanwaltschaft fühlt sich eines Teils ihres Geschäfts geradezu beraubt. Sinnvoll erscheint, die Lösung in der Verbraucheraufklärung und Vertragsfreiheit zu suchen. Der Verbraucher, der Kleinstbeträge bewusst mit hohem Unterliegens- aber fremdem Kostenrisiko zumindest versuchen möchte einzutreiben, sollte diese Möglichkeit nutzen können, bevor er gänzlich auf seinen Anspruch verzichtet. Die Aberkennung eines Wahlrechts zwischen „Legal Tech“ und Rechtsanwalt steht nicht im Einklang mit Art. 2 Abs. 1 GG, der allgemeinen Handlungsfreiheit. Sie schafft auch nicht mehr Geschäft für Letzteren, der zudem sein Fehler- und Haftungsrisiko durch den Einsatz von Technologie zwecks Massenbearbeitung von Kleinstforderungen geradezu exponentiell erhöht. Woher soll der Rechtsanwalt auch seine technische Expertise hernehmen?

Vertragsfreiheit sollte für den Verbraucher heißen: Wenn er sehenden Auges ein korrekt dargestelltes Risiko eingehen möchte und dies dem anwaltlichen Angebot vorzieht, dann soll er diese Freiheit auch haben.

4.2 Behörden: Mehr (Fach-)Personal

Neben der Digitalisierung des behördeneigenen Serviceangebots und der eigenen Prozesse müssen insbesondere die Aufsichts-, Datenschutz-, Strafverfolgungs- und Kartellbehörden mit mehr (Fach-)Personal ausgestattet werden. Die Digitalisierung bringt zahlreiche Risiken des Missbrauchs ihrer Möglichkeiten mit sich. Diesen kann in Unterbesetzung und fehlenden Kenntnissen nichts entgegengehalten werden.

4.3 Gerichte: E-Akte einführen, Prozesse verschlanken, Fortbildung

„Wir müssen bei der Durchsetzung des Rechts besser werden – schnell, konsequent, sichtbar“, sagte der amtierende Bundestagspräsident Wolfgang Schäuble am 11. September 2018 im Bundestag (Welt 2018). Diese Worte sind vor allem

für die deutschen Gerichte von Relevanz. Sie bleiben, neben den Rechtsanwälten, der wichtigste Weg des Einzelnen zum Recht – auch wenn Recht nicht immer dem subjektiven Gerechtigkeitsempfinden entsprechen mag.

Die schwierige Hauptaufgabe der Gerichte ist es, während der täglichen Arbeit diese auf digital umzustellen, ohne die bereits bestehende Überbelastung zu einem nicht mehr abbaubaren Aktenberg aufzutürmen. Sinnvoll erscheint hier vor allem eine Analyse von Ineffizienzen, deren Beseitigung mehr Zeit verschaffen kann.

Auch Richter und Staatsanwälte, die hoffentlich in Zukunft mehr personelle Unterstützung erhalten, brauchen Fortbildung, vor allem in Zeiten der Digitalisierung. Nur ist eine richterliche bzw. staatsanwaltschaftliche Fortbildungspflicht bislang nicht gesetzlich geregelt wie die der Rechtsanwälte (vgl. Kurzinformation des Bundestags zur Fortbildungspflicht in juristischen Berufen vom 25. Juli 2018). Dennoch, so ist es erkennbar, bemüht sich v. a. die Richterschaft aus eigener Motivation, neue Technologien und ihre Reibungspunkte sowie Intersektionen mit dem Recht besser zu durchdringen.

5 Schlusswort: Ist der Rechtsstaat automatisierbar?

Die Antwort lautet: Nein. Es ist schon schwer, einen Vertrag oder auch nur Anspruch rechtskonform zu automatisieren. Geschweige denn, ein über ein stark begrenztes Anwendungsgebiet hinausgehendes Konfliktlösungs-Tool zu schaffen. Zu vielfältig sind die Möglichkeiten, die sich aus der Vertragsfreiheit ergeben und zu vielschichtig das Leben in seiner Unvorhersehbarkeit, der mit rückwärtsgerichteten Lösungsansätzen der heutigen Technologien nicht beizukommen ist.

Entscheidend ist, die Digitalisierung als Vorteil zu begreifen, die Aufgaben der Justiz insbesondere durch schlankere Prozesse besser, das heißt vor allem menschen- und bestmöglich erfüllbar zu machen, Justiz und Verwaltung zu diesem Zwecke personell besser auszustatten und die Fortbildung zu fördern.

„Wir brauchen keine Revolution, sondern einen starken und toleranten Rechtsstaat“, betonte der amtierende Bundestagspräsident Schäuble (Welt 2018). Richtig. Revolution enthält immer eine gewisse Gewaltkomponente. Digitalisierung mit dem Brecheisen ist jedoch keine Lösung; sondern ein bedachtes, vernünftiges Voranschreiten im steten Austausch miteinander. Auch zwischen Staat und Bürger.

Literatur

Barley, K. (2018). Dokumente, Bundestag, BT-Drs. 193400. https://www.bundestag.de/dokumente/textarchiv/2018/kw37-de-justiz/566360. Zugegriffen: 23. Mai 2019.

Böck, H. (2019). Anwaltspostfach wird neu ausgeschrieben, Golem. https://www.golem.de/news/bea-anwaltspostfach-wird-neu-ausgeschrieben-1904-140392.html. Zugegriffen: 23. Mai 2019.

Bundesverfassungsgericht, BVerfGE 8, 274, Rn 212 ff.; BVerfGE 95, 267, Rn 142 ff. (stRspr.: „ständige Rechtsprechung“).

Justiz in Not: Deutschlands Richter am Limit. MDR vom 16. Januar 2019, in der ARD Mediathek bis 16. Januar 2020. https://www.mdr.de/tv/programm/sendung820940.html. Zugegriffen: 23. Mai 2019.

Otto, C. (2019). Schriftliche Stellungnahme der geladenen Sachverständigen Rechtsanwältin Claudia Otto im Rahmen der Öffentlichen Anhörung zu dem Antrag der Fraktion der FDP „Zukunftsfähige Rahmenbedingungen für die Distributed-Ledger-Technologie im Finanzmarkt schaffen“ (BT-Drucksache 19/4217) im Finanzausschuss des Deutschen Bundestages am 11. März 2019. https://www.bundestag.de/resource/blob/627774/a702b4a61c8b64e6fc9ac8176f473167/11—RAin-Claudia-Otto–COT-Legal-data.pdf. Zugegriffen: 23. Mai 2019.

Welt. (2018). Wir müssen bei Durchsetzung des Rechts besser werden. 12. September 2018. https://www.welt.de/print/welt_kompakt/print_politik/article181501770/Wir-muessen-bei-Durchsetzung-des-Rechts-besser-werden.html. Zugegriffen: 23. Mai 2019.

Weiterführende Literatur (Auswahl)

Barth, U. Legal Tech: Mietright gewinnt mit Höcker gegen Berliner Rechtsanwaltskammer. Juve, 17. Januar 2019, https://www.juve.de/nachrichten/verfahren/2019/01/legal-tech-mietright-gewinnt-mit-hoecker-gegen-berliner-rechtsanwaltskammer. Zugegriffen: 23. Mai 2019.

DAV, Deutscher Anwaltsverein, „Kein zusätzlicher Regulierungsbedarf für Legal-Tech-Angebote im RDG“, Statement von Rechtsanwalt Prof. Dr. Wolfgang Ewer, 26. April 2019. https://anwaltverein.de/de/newsroom/dav-kein-zusaetzlicher-regulierungsbedarf-fuer-legal-tech-angebote-rdg. Zugegriffen: 25. Mai 2019.

FAZ. Justiz an der Belastungsgrenze, 2. Januar 2019, https://www.faz.net/aktuell/gesellschaft/justiz-an-der-belastungsgrenze-die-ueberlastung-der-gerichte-15968366.html. Zugegriffen: 25. Mai 2019.

Otto, C. (2017). Welcome to the Matrix – Die schöne neue Welt der Smart Contracts, Recht innovativ, Ri 2017, S. 24 ff.

Otto, C. (2017). Bei Risiken und Nebenwirkungen lesen Sie das Gesetz oder fragen Sie den Hacker Ihres Vertrauens: vom Irrsinn mit den „Smart Contracts“ am Beispiel einer Predictive Policy, Ri 2017, S. 36 ff.

Otto, C. (2017). Guide to the Future -Der Prototyp eines automatisierten Wohnungsmietvertrags, Ri 2017, S. 46 ff.

Otto, C. (2017). Was ist eigentlich Legal Tech…?, Ri 2017, S. 84 ff.

Otto, C. (2017). Bermudadreieck Ethereum – wo Recht derzeit baden geht: Grenzen der Nutzung von Smart Contracts, Ri 2017, S. 86 ff.

Otto, C. (2017). Die Maske des blauen Todes – Gefahren anwaltlicher Tätigkeit via Facebook Messenger Chatbot, Ri 2017, S. 104 ff.

Hause Online Redaktion. (2019). Gesetzesentwurf zu Legal Tech, Erfolgshonorare bald auch für Anwälte? Haufe News, 16. Mai 2019. Zugegriffen: 25. Mai 2019.

Kummert, T. Die deutsche Justiz steht kurz vor dem Kollaps, WirtschaftsWoche, 28. Mai 2018. https://www.wiwo.de/politik/deutschland/ueberlastete-gerichte-die-deutsche-justiz-steht-kurz-vor-dem-kollaps/22603272.html. Zugegriffen: 25. Mai 2019.

Lorenz P. (2019). Sammelklagen, Erfolgshonorare, Prozessfinanzierung: Dürfen die das?, Streitgespräch vom 8. März 2019 in Legal Tribune Online. https://www.lto.de/recht/juristen/b/myright-weniger-miete-legal-tech-berufsrecht-anwaelte-erfolgshonorar-prozessfinanzierung-rdg/. Zugegriffen: 25. Mai 2019.

Müller, R. (2019). Wo Anwalt draufsteht, muss auch Anwalt drin sein. FAZ vom 15. Mai 2019. https://www.faz.net/aktuell/politik/inland/deutscher-anwaltstag-ueber-legal-tech-und-arbeit-eines-anwalts-16187518.html. Zugegriffen: 25. Mai 2019.

Narewski, N. (2019). FDP-Fraktion will Legal Tech im RDG freigeben. Anwaltsblatt, 25. April 2019. https://anwaltsblatt.anwaltverein.de/de/anwaeltinnen-und-anwaelte/berufsrecht/fdp-fraktion-will-legal-tech-im-rdg-freigeben. Zugegriffen: 25. Mai 2019.

rbb 24. (2019). Brandenburger Gerichte sind überlastet – und die Taten verjähren, 9. April 2019. https://www.rbb24.de/politik/beitrag/2019/04/brandenburg-straftaten-verjaehren-wegen-ueberlasteter-gerichte.html. Zugegriffen: 25. Mai 2019.

Remmertz, F. (2018). Legal Tech auf dem Prüfstand des RDG – Notwendig oder überflüssig? LR 2018, S. 163 ff. https://legal-revolution.com/images/pdf/Legal-Tech-auf-dem-Prfstand-des-RDG.pdf. Zugegriffen: 25. Mai 2019.

Remmertz, F. (2019). Rechtsdienstleistungen durch Legal-Tech-Anbieter. Anwaltsblatt, April 2019, S. 138 f. Auszug abrufbar unter https://www.remmertz.legal/pdf/Beitrag-Berliner-Anwaltsblatt-Heft-4-2019.pdf. Zugegriffen: 25. Mai 2019.

Richterbund: Hilfe für überlastete Gerichte lässt auf sich warten, beck-aktuell, Nachrichten, 22. Oktober 2018. https://rsw.beck.de/aktuell/meldung/richterbund-hilfe-fuer-ueberlastete-gerichte-laesst-auf-sich-warten. Zugegriffen: 25. Mai 2019.

Wendt, K. (2018). Erfordert eine Revolution der Technologie eine Revolution des Rechts? Künstliche Intelligenz, Robotik und Recht – Tagungsbericht, Ri 2018, S. 64 ff.

Zeit Online. Vier von fünf Bürgern beklagen überlastete Gerichte, 13. Januar 2019. https://www.zeit.de/news/2019-01/13/vier-von-fuenf-buergern-beklagen-ueberlastete-gerichte-190113-99-542044. Zugegriffen: 25. Mai 2019.

Alter Wein in Neuen Medien?

Polizeiliche Kommunikationspraxis in Social Media und Herausforderungen moderner Kriminalprävention

Daniel Wagner, Lara vom Feld und Thomas Görgen

1 Kriminalprävention in der digitalen Öffentlichkeit

Kommunikationsinhalte polizeilicher Kriminalprävention werden in Deutschland neben dem direkten Kontakt von polizeilichen Beschäftigten mit Bürgerinnen und Bürgern nach wie vor großteils über klassische Kommunikationsmedien wie Flyer, Broschüren, Plakate oder über Kooperationen mit Zeitungen und Fernsehen gestreut. Schon länger ist die Polizei mit entsprechenden Inhalten allerdings auch auf eigenen (statischen) Internetauftritten und seit wenigen Jahren in dialogischen, interaktiven Onlinemedien (Social Media) vertreten.

Die inhaltliche und formale Gestaltung kriminalpräventiver Themen, die polizeilichen Kommunikationsmodi zu ihrer Vermittlung und Verbreitung – und letztlich die Wirksamkeit kriminalpräventiver Kommunikation – waren schon vor

D. Wagner (✉) · L. vom Feld · T. Görgen
Deutsche Hochschule der Polizei, Münster, Deutschland

T. Görgen
E-Mail: thomas.goergen@dhpol.de

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

T.-G. Rüdiger und P. S. Bayerl (Hrsg.), *Cyberkriminologie,*
https://doi.org/10.1007/978-3-658-28507-4_24

der „Digitalen Revolution“ wenig erforscht.[1] Dies ist umso bemerkenswerter, da die Kriminalprävention nicht nur eine wichtige Aufgabe der Polizei darstellt (vgl. Mayer 2016), sondern sich eben auch in diesem Kontext (und nicht nur in Konflikt- oder Krisensituationen) Polizei und Öffentlichkeit begegnen und sich auch hierdurch ihr Verhältnis definiert und weiterentwickelt.

Dabei verdeutlicht gerade der anhaltende rapide und tief greifende Umbruch in der Kommunikationswirklichkeit, wie er in den letzten Jahrzehnten mit Begriffen vom Web 1.0 bis (mindestens) Web 4.0 beschrieben und in Anlehnung an Habermas (1962) teils als neuer, nunmehr digitaler bis algorithmischer Strukturwandel der Öffentlichkeit gesehen wird[2], dass eine systematische Auseinandersetzung mit aktuellen Dynamiken in der kommunikativ vermittelten Beziehung zwischen Polizei und Öffentlichkeit erforderlich ist (vgl. auch Rüdiger und Bayerl 2018). Dass dieses Verhältnis und auch die Rolle von Bürgerinnen und Bürgern als an der Sicherheitsproduktion Beteiligte fortlaufend ausgehandelt werden und dabei gerade auch Neue Medien eine Rolle spielen, zeigen nicht zuletzt auch internationale Forschungsprojekte jüngeren Datums wie Unity (vgl. Bayerl et al. 2015), Media4sec (vgl. MEDIA4SEC 2016) und Inspec2t (vgl. Leventakis et al. 2017), die (Online) Community Policing oder auch „Do-It-Yourself Policing“ in den Blick nehmen. Systematisch gewonnene Erkenntnisse zur polizeilichen Nutzung von Social Media für kriminalpräventiv ausgerichtete Kommunikation sind bisher allerdings die Ausnahme. Der Fokus liegt eher auf der oft allgemein gehaltenen Beschreibung der Bedeutung und Funktionalität von Social Media als Instrument der Kommunikation und Beziehungspflege mit der Öffentlichkeit. Kriminalpräventiv orientierte Kommunikation stellt dabei – soweit überhaupt angeschnitten – eine meist nicht näher betrachtete Teilfunktion dar.

Im vorliegenden Beitrag werden ausgewählte Ergebnisse einer Studie, die im Rahmen des BMBF-geförderten Verbundprojekts PräDiSiKo[3] an der Deutschen Hochschule der Polizei (DHPol) durchgeführt wurde, vorgestellt und diskutiert. Einen Schwerpunkt der Forschungsaktivitäten stellte die Bestandsaufnahme und

[1]Zur Wirksamkeitsmessung in der Kriminalprävention siehe etwa Sherman (1998); Walsh et al. (2018); Welsh und Farrington (2007).

[2]Vgl. etwa Hagen et al. (2017); für einen Überblick und eine kritische Perspektive zu entsprechenden Diagnosen siehe auch Schrape (2015).

[3]„Präventive digitale Sicherheitskommunikation – ein innovativer Ansatz für Kriminalprävention in sozialen Online-Medien“ (Laufzeit: November 2016 bis Oktober 2019); http://www.praedisiko.polizei-beratung.de.

Analyse der auf den offiziellen Social Media Accounts deutscher Polizeibehörden praktizierten Ansätze kriminalpräventiver Kommunikation dar. Dazu wurden neben einer Auswertung bestehender Forschungsliteratur zur Thematik zum einen entsprechende Kommunikationsinhalte auf polizeilichen Accounts erhoben und ausgewertet, zum anderen mündliche (leitfadengestützte Experteninterviews) und schriftliche (Selbstausfüller-Fragebogen) Befragungen polizeilicher Beschäftigter durchgeführt.

Befragt wurden Praktikerinnen und Praktiker aus den Bereichen Kriminalprävention (KP) und Presse- und Öffentlichkeitsarbeit (PÖA), sowohl solche in lokalen Polizeibehörden als auch solche in strategischen oder koordinierenden Positionen, etwa auf Landesebene.

Der für den Bereich PÖA entwickelte Interviewleitfaden öffnet mit allgemeinen Fragen zur Nutzung von Social Media in der Polizeibehörde, also wie sich die Nutzung dieser Kanäle und die Kommunikation mit der Öffentlichkeit über Social Media in der Praxis gestalten, um dann überzuleiten auf kriminalpräventive Inhalte und damit verbundene Erfahrungen der Befragten *(„Welche Rolle spielen kriminalpräventive Inhalte bei Ihrer Kommunikation über Social Media?“).* Der für den Bereich KP genutzte Leitfaden korrespondiert inhaltlich weitgehend mit dem Kriminalpräventions-Abschnitt des PÖA-Leitfadens. Da die meisten Befragten im KP-Bereich bisher allerdings kaum direkt mit Social Media als Teil ihrer Arbeit Erfahrungen sammeln konnten, mussten diese Interviews flexibler gehandhabt werden; das bedeutet konkret: ebenfalls teilstrukturiert, aber insgesamt offener, was Fragenformulierungen und -reihenfolge, sowie insgesamt die Gesprächsführung anbelangt. Dafür wurden zentrale Leitfragen, insbesondere zu Beginn des Gesprächs, offener und stärker erzählgenerierend formuliert, um zu einer Reflexion über die jüngere Entwicklung polizeilicher KP anzuregen *(„Bitte beschreiben Sie, wie sich die Arbeit der polizeilichen Kriminalprävention in den letzten Jahren entwickelt hat.“).* Es wurden 25 Interviews mit insgesamt 42 Gesprächspartnern durchgeführt: 16 Gespräche mit insgesamt 32 Beschäftigten in deutschen Polizeibehörden (in fünf Bundesländern), sowie neun Gespräche mit insgesamt zehn Beschäftigten in Polizeibehörden im europäischen Ausland (in fünf Ländern). Da hier speziell die Situation in Deutschland beschrieben und diskutiert werden soll, konzentriert sich der vorliegende Beitrag auf die Interviews, die in deutschen Polizeibehörden durchgeführt wurden (mit jeweils 16 Vertretern aus dem Bereich KP und aus dem Bereich PÖA).

Auch bei der deutschlandweiten schriftlichen Befragung war es erforderlich, zwei Instrumente zu erstellen, jeweils eines für Beschäftigte in den Bereichen PÖA und KP. Das Instrument für den Bereich PÖA ist etwas umfangreicher als für den Bereich KP und umfasst zusätzlich zu den in beiden Bögen enthaltenen

(identischen) Fragenbatterien zu kriminalpräventiven Inhalten Items zu den in der jeweiligen Behörde unterhaltenen Social Media Accounts und ihrer Nutzung. Aus den Bereichen KP und PÖA war jeweils ein Rücklauf von 70 Fragebögen zu verzeichnen, sodass 140 Bögen (aus 14 Bundesländern und vom Bund) in die Auswertung der schriftlichen Befragung einfließen konnten.

2 Polizeiliche Social Media Accounts

Die von deutschen Polizeibehörden am häufigsten für die externe Kommunikation genutzten Social Media Plattformen sind Twitter und Facebook.[4] So ließen sich im Mai 2018 127 offizielle Facebook- und 148 Twitteraccounts deutscher Polizeibehörden identifizieren (Abb. 1). Dabei organisieren sich die Bundesländer unterschiedlich. Während entsprechende Accounts in den meisten Flächenländern auf Ebene von Polizeipräsidien oder Kreispolizeibehörden (je nach Bundesland sind andere Strukturen und Bezeichnungen üblich) betrieben werden, unterhalten die Stadtstaaten sowie einige Flächenländer nur einzelne bzw. zentralisierte Accounts für das Bundesland. In der Regel orientiert sich die Verortung der Accounts bzw. die Zuständigkeit für deren Betreuung an der ohnehin gegebenen Struktur, was bedeutet, dass die jeweiligen Abteilungen für Presse- und/oder Öffentlichkeitsarbeit damit befasst sind. Diese sind üblicherweise als Stabsstellen direkt und eng an die Behördenleitung gebunden.

In den erfassten Accounts sind auch funktionsspezifische Accounts, etwa für Einsätze (ausschließlich Twitter) oder Karriere bzw. Nachwuchsgewinnung (meist Facebook) enthalten. Am einschlägigsten für die Kommunikation kriminalpräventiver Inhalte sind die anlassunabhängig und zur gesamten Bandbreite polizeilich relevanter (und mitunter auch polizeilich nicht relevanter) Themen kommunizierenden Accounts der Länderpolizeien auf Ebene der örtlichen Behörden.

Einen Überblick über die Reichweite der identifizierten Accounts gibt Tab. 1. Im Mai 2018 verzeichneten die Facebookaccounts deutscher Polizeibehörden in der Summe 2.691.189 Abonnenten und die Twitteraccounts 2.575.615 Follower; dies ist freilich nicht die Summe der „unique user“, da Personen, die mehrere Accounts abonniert haben, mehrfach gezählt werden. Außerdem finden sich unter

[4]Andere Plattformen (vorwiegend Instagram und YouTube) werden in deutlich geringerem Umfang genutzt.

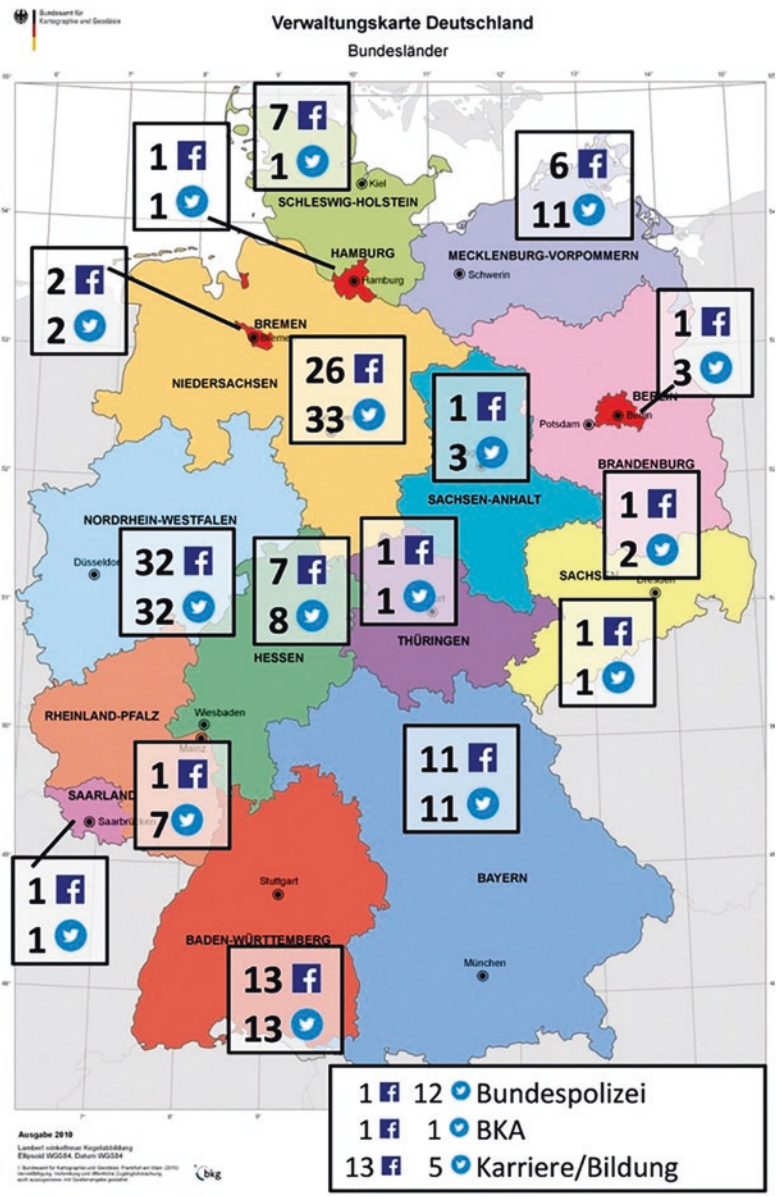


Abb. 1 Polizeiliche Facebook- und Twitteraccounts. (Eigene Erhebung, Mai 2018; hinterlegte Deutschlandkarte © Bundesamt für Kartographie und Geodäsie)

Tab. 1 Reichweite polizeilicher Accounts im Mai 2018. (Eigene Erhebung)

	Minimum	Unteres Quartil	Median	Oberes Quartil	Maximum	Summe
Facebook Seitenabonnenten (n = 126 Accounts)	27	4283	10.721	22.215	253.194	2.691.189
Twitter Follower (n = 141 Accounts)	7	1327	3087	8585	459.000	2.575.615

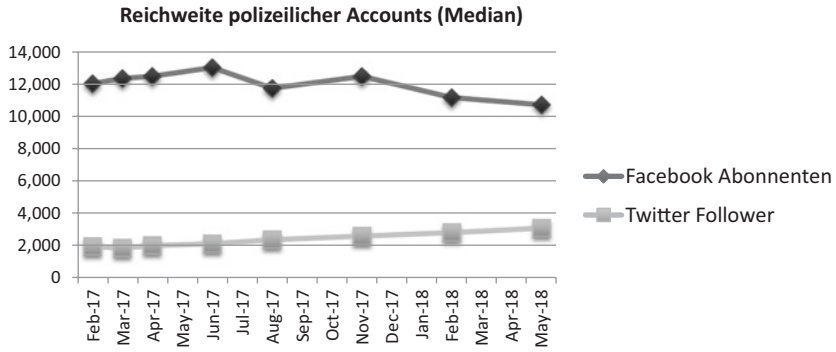


Abb. 2 Reichweite polizeilicher Accounts im Zeitverlauf. (Eigene Erhebung, Feb. 2017-Mai 2018)

den Abonnenten und Followern nicht nur Privatpersonen, sondern auch andere polizeiliche Accounts sowie weitere Institutionen. Gerade Twitter gehört längst zum Standardwerkzeug von Journalistinnen und Journalisten bzw. von Massenmedien, welche polizeiliche Accounts zumindest in der für sie relevanten Region beobachten.

Während die Summen der Facebookabonnenten und Twitterfollower zum Erhebungszeitpunkt Mai 2018 fast identisch waren, zeigt die Betrachtung des Medians (Abb. 2) einen auch im Zeitverlauf durchgehend sehr deutlichen Unterschied in der mittleren direkten Reichweite der Accounts beider Plattformen[5].

[5]Bei Abb. 2 ist zudem zu beachten, dass zu jedem Erhebungszeitpunkt in der Zwischenzeit neu eingerichtete Accounts miteinbezogen wurden, die natürlich erst einmal ohne große Reichweite starten und den Median tendenziell senken.

Dies hängt mit einer stärkeren Streuung bei Twitter zusammen, die sich darin ausdrückt, dass viele polizeiliche Twitteraccounts nur sehr wenige Follower haben und so den Median senken, während einige wenige Accounts als extreme Ausreißer nach oben prägend für die Summe sind. Eine ähnliche Tendenz, verbunden mit einer ebenfalls stark rechtsschiefen Verteilung, gilt zwar auch für die Abonnenten polizeilicher Facebookaccounts, ist dort allerdings etwas weniger ausgeprägt. Alleine die Summe der Follower der drei größten Twitteraccounts (München, Berlin und Berlin Einsatz) macht fast die Hälfte (48 %) der addierten Reichweite aus.

3 Allgemeine Kommunikationspraxis

3.1 Dimensionen und Ziele polizeilicher Onlinekommunikation

Anhand der Interviews mit den Beschäftigten im Bereich PÖA lassen sich drei zentrale Dimensionen polizeilicher Onlinekommunikation und mit diesen korrespondierende Funktionen bzw. Ziele identifizieren (Abb. 3). Zum einen bildet sich der polizeiliche Auftrag im engeren Sinn ab, in Form der Maßgabe, dass Kommunikationsakte sich dadurch begründen (sollen oder sogar müssen),

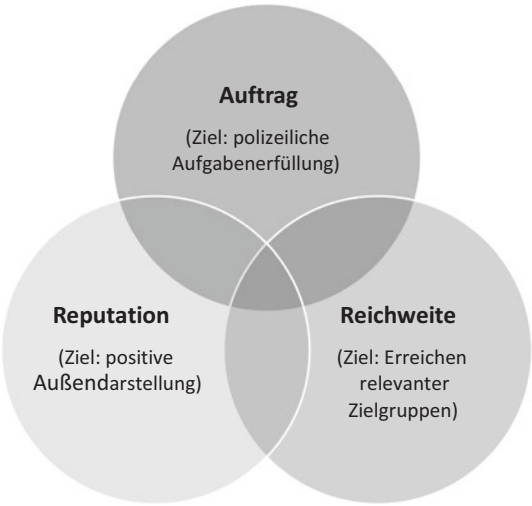


Abb. 3 Hauptdimensionen und Ziele polizeilicher Onlinekommunikation

dass sie einen Beitrag zur polizeilichen Aufgabenerfüllung leisten. Hier sind insbesondere die beiden polizeilichen Hauptfunktionen Strafverfolgung (korrespondierende Inhalte wären z. B. Fahndungsaufrufe) und Gefahrenabwehr (hierzu kann man zumindest „im weiteren Sinne“ auch kriminalpräventive Beiträge zählen, siehe dazu Klotter und Mayer 2018, S. 113) relevant. Eine weitere Dimension lässt sich als Reputation zusammenfassen und korrespondiert mit dem Ziel, die Polizei als Institution, sowie polizeiliches Handeln und teils auch polizeiliche Perspektiven positiv darzustellen; in diesem Zusammenhang ist auch oft von Image[6], Ruf, Ansehen, Respekt und Vertrauen die Rede. Und als dritte Dimension ist schließlich Reichweite zu nennen, was mit dem Erreichen relevanter Zielgruppen (in der Regel: die Menschen im Zuständigkeitsbereich der eigenen Behörde) oder auch einer möglichst breiten Öffentlichkeit korrespondiert (die Befragten beziehen sich, z. B. mit Verweisen auf eine gewünschte „virale Verbreitung“, nicht selten auf eine Verbreitung über die eigene geographische Zuständigkeit hinaus).

Eine Bezugnahme auf diese drei Dimensionen und ihre Verknüpfung lässt sich bei den meisten Befragten im Bereich PÖA feststellen. Eine auf Langfristigkeit angelegte, zielorientierte, effektive und sinnvoll umgesetzte polizeiliche Kommunikationsstrategie wird als Zusammenspiel dieser drei Ebenen geschildert. Es sind allerdings Unterschiede dahin gehend festzustellen, wie die einzelnen Dimensionen jeweils gewichtet werden und wie sie miteinander in Relation stehen bzw. stehen sollen.

Insbesondere die direkt mit der Betreuung der Accounts befassten Befragten nehmen deutlich Bezug auf die Wichtigkeit einer großen Reichweite, was in diesem Fall mit der Anzahl an Followern oder Abonnenten bzw. Fans verbunden wird. Die hervorgehobene Relevanz der Reichweite wird darüber begründet, dass so gewährleistet sei, etwa in Krisensituationen (im Polizeijargon: „besondere Lagen“) möglichst schnell möglichst viele Personen zu erreichen, sowohl direkt auf den polizeilichen Accounts als auch vermittelt über journalistische Akteure, die die Beiträge aufgreifen und weiterverbreiten. Voraussetzung für die Akzeptanz dieser Inhalte und etwaiger Verhaltensempfehlungen ist wiederum eine positive Reputation der Institution Polizei und damit verbunden, aber darüber noch hinausgehend, eine Wahrnehmung ihrer Informationstätigkeit in Social Media als authentisch und vertrauenswürdig. Über diese Argumentation

[6]Zur Herausforderung einer systematischen Unterscheidung der Begriffe Reputation und Image siehe stellvertretend Eisenegger (2015).

werden Kommunikationsinhalte und auch -stile legitimiert, die auf den Dimensionen Reichweiten- und/oder Reputationssteigerung verortet werden können und somit zwar nicht unmittelbar zur polizeilichen Aufgabenerfüllung beitragen, aber mittelbar einen Beitrag dazu leisten, indem sie eine förderliche Grundlage darstellen. Auch die Pflege einer positiven Reputation wird nicht nur als in sich selbst erstrebenswert angesehen, sondern als Teil einer potenziell reichweitengenerierenden Strategie.

Mit dieser indirekten Legitimation einher geht eine teils instrumentelle Perspektive auf Kommunikationsinhalte, die schwerpunktmäßig als reichweitengenerierend gepostet werden oder um durchgehende Kommunikation auf den genutzten Kanälen zu gewährleisten; letztgenanntes sei eine Grundlage für den Erhalt des Interesses auf Seiten von Öffentlichkeit und Medien und idealerweise auch geeignet zur Steigerung von Abonnentenzahlen. Dabei wird klar, dass die Befragten sich teils sehr intensiv damit auseinandersetzen, wie man eine gute Balance zwischen polizeilichen Aufgaben und Reichweitenerhöhung findet. Die Wichtigkeit von Reichweite wird dabei auch betont, aber Beiträge, die durch ihren Inhalt oder Stil vorwiegend aufmerksamkeitssteigernd wirken sollen, werden eher kritisch gesehen, nicht zuletzt, weil sich diese eventuell sogar negativ auf die Reputation einer professionellen, sachlichen, vertrauenswürdigen Behörde auswirken könnten.

> „Wir haben eigentlich das Prinzip: Wir können auch witzig sein oder was Kurioses machen. Aber es muss immer irgendwie eine Botschaft dahinterstecken. […] Ich sage mal bei so einer Aktion der Mehrwert ist natürlich, dass die Accounts bekannter werden. Dass Leute möglicherweise hier in der Region da nicht wussten, dass wir da so aktiv sind, vielleicht das nutzen. Oder sie wussten: Wir haben die Accounts, aber wir können auch nicht nur öde oder dröge Sprüche da bringen, sondern ein bisschen mehr. Dass die vielleicht Interesse bekommen, uns zu folgen. Aber sowas bringen wir sehr selten. Eher so der ‚seriöse Auftritt', sage ich mal, in Anführungszeichen. Und versuchen aber immer mehr vielleicht so eine pointierte Meldung oder sowas, vielleicht mehr Aufmerksamkeit zu erregen auf den einzelnen Post. Ich glaube, bis jetzt kam das insgesamt gut an." (Exp_PÖA[7])

[7]Zitate aus den Befragungen sind wie folgt gekennzeichnet: Exp_PÖA bzw. Exp_KP markieren mündliche Aussagen, die in den Experteninterviews von Befragten aus den Bereichen PÖA bzw. KP getroffen wurden, SB_PÖA bzw. SB_KP markieren freitextliche Antworten, die im Rahmen der schriftlichen Befragung von Beschäftigten in den Bereichen PÖA bzw. KP gegeben wurden.

„Aber es ist schon so, dass wir dort uns erst mal als Allererstes als Polizei sehen. So und Polizei, wofür steht Polizei? Wofür bekommt Polizei nach der neuesten Umfrage 88 Prozent des Vertrauens in der Bevölkerung? Insbesondere deshalb, weil wir […] sachlich seriös sind, weil wir als integer wahrgenommen werden, weil wir […] tatsächlich auch dieses Unparteiische auch darstellen. Und weil wir eben nicht jeden Klamauk mitmachen. […] So und dann gibt es natürlich den Spagat zu dem, was in der Community erfolgreich ist. […] Und je erfolgreicher man ist, desto öfter wird man wahrgenommen. Und dadurch schaffe ich dann wiederum mehr Reichweite. […] Und wir wollen uns schon sehr auf das, was Polizei ausmacht, konzentrieren, das natürlich auch mal witzig verpacken. […] Aber wichtig wäre uns halt immer, es nicht zu übertreiben.“ (Exp_PÖA)

3.2 Kommunikationsstil – zwischen Aufmerksamkeitsgewinnung und Sachlichkeit

Die soeben bereits angeschnittene Herausforderung, einen Kommunikationsstil zu entwickeln und zu pflegen, der zugleich der Institution Polizei, den Erwartungen der Öffentlichkeit an die Polizei und den Funktionslogiken von Social Media angemessen ist, wird breit diskutiert und soll nun näher beleuchtet werden.

Die für die polizeiliche Kommunikation Verantwortlichen haben die Erfahrung gemacht, dass in Social Media gerade aus Behördensicht potenziell heikle Stilmerkmale Aufmerksamkeit erwecken und dazu geeignet sind, die Adressaten (Privatpersonen wie auch journalistische Akteure) dazu anzuregen, mit dem Inhalt zu interagieren und so zu seiner breiten Streuung beizutragen. Als aufmerksamkeitsfördernd gelten etwa Emotionalisierung, Personalisierung, Humor/Ironie, Zuspitzung, und eine geeignete Visualisierung v. a. mittels überraschender, origineller, interessanter oder auch exklusiver Bilder (z. B. von einem Polizeieinsatz). Dienstfahrzeuge, Tiere (z. B. Polizeihunde) und ungewöhnliche Einblicke in bzw. Perspektiven auf die Polizeiarbeit werden ebenfalls genannt.

„Emotionale oder polizeinahe Themen verbreiten sich wesentlich besser als Präventionsbeiträge.“ (SB_PÖA)

„Seichte Beiträge mit Bildern (Kinder/Hunde) sind deutlich beliebter als sachliche Informationen (Sperrung aufgrund Unfall). Mehr als doppelt so viele ‚likes‘ im Schnitt.“ (SB_PÖA)

„Immer nur die gleichen Inhalte zu bringen, wird vielleicht auf Dauer für die Facebook-Leute dann auch ein bisschen langweilig. Und von daher ist es dann auch immer unsere Aufgabe zu gucken: Wie kann man ein Thema noch einmal

> interessanter machen? Indem man vielleicht mal einen Ansprechpartner zur Verfügung stellt.“ (Exp_PÖA)

> „Spektakuläre Bilder oder Geschichten. Ein Blick hinter die Kulissen unserer Arbeit.“ (SB_PÖA)

Es wird mehrfach thematisiert, dass Aufmerksamkeitsgewinnung nicht um jeden Preis geschehen dürfe. Die Befragten betonen weit überwiegend die Wichtigkeit der Wahrung der für die Polizei wichtigen Werte (eigentlich sogar: zentralen Identitätsmerkmale) Seriosität, Neutralität, Sachlichkeit und Glaubwürdigkeit.

> „Es bleibt in dem Themenfeld eine schwierige Balance zwischen (a) Reaktion auf Bürgeranliegen und eigener Vermittlung von Inhalten, (b) schneller Reaktion und dem Anspruch auf Seriosität, (c) Emotionalität zur Erreichung der Zielgruppen und Neutralität (die zu Recht von der Polizei erwartet wird).“ (SB_KP)

> „Aber wichtig ist für uns im Grunde auch, dass diese Seriosität auch rüberkommt […]. Auch die Seriosität und Glaubwürdigkeit spielen eine große Rolle. […] Es gibt sicherlich mal ein Thema, wo man sagt, da kann man auch mal humorvoll mit umgehen, da kann man auch mal etwas Witziges machen. Aber grundsätzlich in der Regel sind das sehr oft dann ernstere Themen, die man dann auch transportieren will, weil Präventionstipps, wo dann im Grunde auch tatsächlich dann ältere Leute zum Beispiel zu Opfern geworden sind oder werden könnten, da bietet es sich […] nicht an, da witzig zu sein oder so etwas.“ (Exp_PÖA)

Ein lockerer Ton in Social Media, etwa in Form einer leichten Abkehr von der üblichen Behördensprache, wird von manchen Befragten als positiv, und von der Mehrzahl der Befragten zumindest als kaum problematisch hinsichtlich der Vereinbarkeit mit Seriosität und Sachlichkeit angesehen, jedenfalls solange der Ton dem Inhalt der Beiträge angemessen ist.

> „Und in den Formulierungen dann der Meldungen, da gucken wir schon, dass das mit einer ansprechenden, lockeren Sprache formuliert ist, nicht zu formell, nicht zu behördlich, weil das würde nämlich die User beim Lesen abschrecken. Also wenn es der Sachverhalt und das Thema auch ermöglicht, machen wir das ein bisschen lustiger und lockerer. […] Da kriegen wir auch mal ein positives Feedback. Aber wir unterscheiden natürlich auch klar. Es gibt viele Themenbereiche, wo wir ganz sachlich, objektiv berichten, und bei manchen, da können wir ein bisschen in Richtung Humor gehen, aber nicht zu sehr.“ (Exp_PÖA)

Dies entspreche den Erwartungen der Adressaten an den Kommunikationsstil in Social Media. Allzu „kumpelhaft“ soll die Ansprache allerdings nicht sein, um

Distanz und Autorität zu wahren. Das „Sie“ ist die Norm, wenn auch nicht ohne Ausnahme.

> „Also siezen müssen wir, ist ja auch angebracht. Die Kollegen auf der Straße möchten ja auch nicht so direkt geduzt werden. Da gab es […] einen […] Erlass vom Innenministerium, der das […] festgeschrieben hat.“ (Exp_PÖA)

> „Ich denke, wenn wir anfangen, die Leute dann zu duzen, können wir sie nicht mehr siezen. Weil das ist dann vorbei. Aber man kann natürlich von Fall zu Fall, wenn wir das denn wollen, auch mit den Leuten anders noch umgehen, indem man die Antworten da, ja, ein bisschen salopper vielleicht formuliert.“ (Exp_PÖA)

Humor in seinen verschiedenen Ausformungen, etwa in Form von Ironie, Satire, Spott etc., kann hohe Verbreitungsraten fördern, da er den Aufmerksamkeitsregeln des Internets sehr gut entspricht. Entsprechende Inhalte werden zudem als ungewöhnlich für eine Institution wie die Polizei wahrgenommen und entsprechend häufig auch von Privatpersonen, Bloggern und journalistischen Akteuren aufgegriffen. Sie können positiv aufgenommen werden, was tendenziell eher in Onlineartikeln mit niedriger journalistischer Qualität und den internettypischen Listen stattfindet (stellvertretend „#wiesnwache: Die lustigsten Tweets der Polizei München vom Oktoberfest“ 2018), aber auch Gegenstand kritischer Auseinandersetzung sein (stellvertretend Fanta 2018). Was mitunter als bürgernah eingeordnet wird, ist angesichts der Autoritätsposition der Polizei heikel, insbesondere, wenn Humor zulasten Dritter geht, die quasi von der Obrigkeit verhöhnt werden (vgl. dazu vertiefend Wagner und Görgen 2018, S. 66 ff.). Entsprechend kritisch äußern sich auch manche polizeiliche Beschäftigte, die darin eine Gefahr für das Ansehen bzw. die Reputation der Polizei sehen.

> „Prinzipiell ist es vorstellbar für uns, das auch auf einem witzigen Niveau zu machen. […] trotzdem sollten wir uns als Behörde nicht lächerlich machen über die Leute. Ein gewisser Witz ist okay. Aber, wenn dahin geht dahingeht, dass man sagt, die Behörde macht sich jetzt von oben herab lächerlich eigentlich, über das polizeiliche Gegenüber. Dann ist, denke ich, für uns alle hier eine Grenze überschritten. Wo wir sagen, auf den Zug wollen wir nicht mit aufspringen. Auch wenn das andere Verbände doch in der Vergangenheit so gemacht haben, aber heute inzwischen selber sagen: ‚Okay, da sind wir vielleicht hier und da in unserem jugendlichen Leichtsinn ein bisschen über das Ziel hinausgeschossen.‘“ (Exp_PÖA)

Als unproblematisch und allgemein empfehlenswert, um bei den Adressaten Interesse hervorzurufen, wird die Nutzung oder bewusste Herstellung eines zeitlichen und lokalen Bezugs angesehen, also das Berichten über oder Anknüpfen

an aktuelle Ereignisse (z. B. Straftaten) in der Region. Dies werde von der Kernzielgruppe, also den Menschen in der eigenen geographischen Zuständigkeit, als relevant und anknüpfungsfähig wahrgenommen, was auch als potenziell förderlich für die Anschlusskommunikation und weitere Verbreitung von Botschaften, gerade auch mit präventivem Gehalt, gesehen wird. Dies wird insbesondere auch im Hinblick auf kriminalpräventive Kommunikationsinhalte empfohlen.

> „Lokale Inhalte sprechen die Zielgruppe an, Berichte über aktuelle lokale Geschehnisse bzw. kriminalpräventive Botschaften basierend auf solchen lokalen Ereignissen ziehen die Aufmerksamkeit an.“ (SB_KP)

> „Wenn man dann sagt: ‚Hier, das war an der so und so Straße, das war eine 87-jährige Frau aus [Stadtteil von A-Stadt]‘. Da ist die Betroffenheit der Menschen in [A-Stadt] halt ganz anders, als wenn das LKA offiziell warnt: ‚Das ist die Masche der Betrüger.‘ [Dann sagen die Adressaten:] ‚Ja gut, ist halt irgendwo in [B-Stadt] passiert, betrifft mich nicht.‘ Aber wenn es in der Nachbarschaft war, dann werden die Leute schon hellhörig.“ (Exp_PÖA)

> „Ein schönes Beispiel für Tagesgeschäft und dann verbunden mit einer Präventionsbotschaft waren diese falschen Polizeibeamten. Und da haben wir festgestellt, dass es dadurch, dass es tagesaktuell war, es auch einen echten Geschädigten gab, dass dann zu dem Zeitpunkt mehr Leute dafür sich interessieren als wenn man einfach anlasslos einen Präventionsbeitrag bringt. […] Wenn man dann draufsetzt mit der Präventionsbotschaft, erreicht man die Leute dann eigentlich ganz gut.“ (Exp_PÖA)

3.3 Grenzen der Planbarkeit und Standardisierung

Der Entwicklung von längerfristigen Kommunikationsstrategien und von Standards und Handreichungen (etwa in Form von Dienstanweisungen) für die Nutzung von Social Media sind Grenzen gesetzt. Ein nicht beeinflussbarer und schwer durchschaubarer Faktor ist etwa die algorithmische Aufmerksamkeitssteuerung auf den Plattformen. Gerade der Facebookalgorithmus wird als wechselhaft und undurchsichtig beschrieben; was auf den Timelines der Nutzer angezeigt wird, sei zudem sehr individuell von deren Nutzungsverhalten abhängig. Dem Algorithmus erfahrungsgemäß oder mutmaßlich „gefällige“ Strategien werden unter den polizeilichen Kommunikationsfachleuten ausgetauscht, aber auch externe Anregungen werden aufgegriffen. Dabei wird zwischen verschiedenen Medien differenziert, insbesondere eben zwischen Twitter, welches als das schnellere, zuverlässigere bzw. berechenbarere Medium wahrgenommen und entsprechend für die Streuung dringender, wichtiger Informationen bevorzugt

wird, und Facebook, welches ausführlichere Inhalte erlaubt, aber eben etwas enigmatisch und launenhaft erscheint.

> „Also bei Facebook kann ich, wenn ich Pech habe, durch den Algorithmus so fallen, dass ich eine aktuelle Nachricht erst einen Tag später irgendwo in meiner Timeline habe, bei Twitter eben in der Tendenz eher nicht." (Exp_PÖA)

> „Letzten Endes können wir ja gegen diese Algorithmen […] nichts machen, müssen damit leben. Und deswegen haben wir ja auch zum Beispiel Twitter. Wenn wir jetzt akute Einsatzlagen haben, wo wir über die aktuelle Lage aufklären möchten oder auch Warnungen herausgeben müssen, würden wir bei Facebook nur schreiben: ‚Zum aktuell laufenden Einsatz in Stadt XY halten wir Sie über Twitter auf dem Laufenden.' Weil […] Facebook halt auch zeitversetzt einzelne Beiträge anzeigt. Deswegen: Twitter ist in dem Fall viel besser." (Exp_PÖA)

> „Wir orientieren uns hier an Marketingstrategien aus der freien Wirtschaft und an den von Facebook vorgegebenen Algorithmen, um eine möglichst hohe Reichweite zu erhalten. Beispielhaft: Wir arbeiten mit Videos, da diese mehr organische Reichweite[8] erzielen und wir unsere Inhalte für die User zeitgemäßer an den Mann / die Frau bringen." (SB_PÖA)

Auch einer längerfristigen Planung sind Grenzen gesetzt, da die Polizei mehr als andere Organisationen auf unvorhersehbare Ereignisse reagieren muss und Kommunikationsanlässe nur bedingt beeinflussen oder selektieren kann. Trotzdem entwickeln und benutzen einige Behörden mehr oder weniger ausgearbeitete (z. B. wöchentliche oder monatliche) Redaktionspläne, achten auf geeignete Kommunikationsanlässe wie etwa bestimmte Thementage im Jahr oder planen teils auch serielle Publikationen, d. h. die intervallhafte Veröffentlichung zusammengehöriger Beiträge. Auch sind mitunter Bemühungen festzustellen, jedenfalls im Alltagsbetrieb eine einigermaßen gleichbleibende tägliche Menge an Beiträgen zu veröffentlichen und irritierende Abfolgen zu vermeiden, also etwa das Posten eines eher unbeschwerten Inhalts direkt nach einer sehr ernsten Nachricht.

> „Wir haben diesen Kalender, wo eigentlich jeden Tag irgendein anderer [Aktionstag] ist. Wo wir dann wirklich sukzessive, wenn es uns gerade in den Redaktionsplan passt [Anlässe nutzen]. […] Bei fünf Postings die Woche […] sind so viele

[8] Als organische Reichweite wird in der Regel die ohne Nutzung kostenpflichtiger Funktionen mögliche Verbreitung bezeichnet (in Abgrenzung zu bezahlter Reichweite).

> Tage dabei, wo die Tageslage nichts Spektakuläres hergibt und wir doch irgendwo einen Post den Usern im Endeffekt geben wollen.“ (Exp_PÖA)

> „Wir hätten gerne so einen [Redaktionsplan]. Also wir haben auch eine Redaktionssitzung, die mal stattfindet, mal nicht. Und eigentlich planen wir so einen Monat vor. Wir schauen auch, was gibt es für besondere Tage. Ich sage jetzt, weiß ich nicht, internationaler Tag Gewalt gegen Frauen […] und solche Tage nehmen wir dann zum Anlass, um uns irgendwelche Facebook-Inhalte dazu zu überlegen, die dann aber immer einen polizeilichen Bezug haben sollen. (Exp_PÖA)

Neben rechtlichen[9] und organisatorischen Rahmenbedingungen sind die zur Betreuung der betriebenen Accounts nötigen bzw. verfügbaren personellen wie sachlichen Ressourcen ein wesentlicher Faktor. Dazu gehören die technische Ausstattung (z. B. Kameras, Bildbearbeitungs- und Videoschnittsoftware) und insbesondere das verfügbare Personal und dessen Qualifikation. Während größere Dienststellen teils Social Media Teams unterhalten, können gerade kleinere Dienststellen, umso mehr bei besonderen Lagen, an Grenzen stoßen, nicht nur was die bloße Personaldecke anbelangt, sondern auch den praktischen Erfahrungsschatz, auf dem aufbauend Kommunikation geführt wird.

> „Es gibt einige […] Polizeibehörden, die noch kein Facebook haben oder beziehungsweise kurz davor stehen, das jetzt einzuführen. Das hat natürlich dann auch Fragen der Kapazität, der Personalfrage, der Ressourcen, die da zur Verfügung stehen, und auch der Erfahrung, die man mitbringt.“ (Exp_PÖA)

> „Um den Bereich professionell auszubauen ist eine personelle Stärkung des Bereiches förderlich. Mitunter sind die Organisationsstrukturen in der Polizei hinderlich für eine einheitliche Umsetzung von Standards.“ (SB_PÖA)

Dabei spielt auch eine Rolle, dass die Ausbildung für den Umgang mit Social Media in der Regel „on-the-job“ erfolgt, mitunter unterstützt durch erfahrene Kolleginnen und Kolleginnen aus Dienststellen, die bereits länger entsprechende Kanäle unterhalten.

> „Es ist zu einem hohen Grad learning by doing, muss ich Ihnen ganz ehrlich sagen. […] Wir können auf die Erfahrungen der anderen [Polizeibehörden] zurückgreifen,

[9] Auf rechtliche Fragen wie etwa Datenschutz und der Umgang mit problematischen bis hin zu strafrechtlich relevanten Kommentaren soll hier nicht näher eingegangen werden. Siehe dazu etwa Krischok (2018) oder auch Polizei Berlin (2013, insb. S. 12–14).

> auf die Hospitationen. […] Sich überall gewisse Informationen herauszuziehen und zu sagen, wir gehen dann unseren eigenen Weg aus den Informationen, die wir uns halt irgendwo herauspicken. Aber ja, ein festgeschriebenes Ding gibt es da nicht. Und es ist Vieles ganz neu.“ (Exp_PÖA)

Geeignetes Personal für die Social Media Arbeit wurde mehreren Befragten zufolge über Interessenabfragen unter Polizeibeamtinnen und -beamten im jeweiligen Bundesland oder den Dienststellen rekrutiert (nur relativ selten wurden bisher Seiteneinsteiger mit einschlägiger Qualifikation eingebunden oder eingestellt, dies scheint aber zuzunehmen). Auch Aufgaben wie Fotografieren, Filmen, Bildbearbeitung und Videoschnitt werden gewöhnlich von entsprechend versierten Beschäftigten wahrgenommen. Selbst die Nutzung von privater Ausstattung kommt vor.

> „Ja, ich verwende meine private Fotokameraausrüstung und jetzt neuerdings eine dienstliche Kamera. Das sind die Ressourcen. […] ‚Bring your own device.‘ (Lachen) Also, wir nutzen unsere privaten Sachen auch für den Dienst, allerdings man kann schon sehen anhand davon, dass wir auch mal so eine teure Kamera bekommen haben, dass also schon die Prioritäten auch zu unseren Gunsten gesetzt werden.“ (Exp_PÖA)

4 Kriminalpräventive Kommunikation

Der überwiegende Teil der polizeilichen Accounts auf Ebene der Länderpolizeien wird für ein breites Themenspektrum genutzt, welches auch Kriminalprävention umfasst. Ausnahmen sind insbesondere die in der Regel schon anhand des Accountnamens identifizierbaren, inhaltlich spezieller gefassten Accounts (etwa für Fahndung, Nachwuchsgewinnung oder Einsatzbegleitung). Auch Accounts polizeilicher Bildungseinrichtungen, der Bundespolizei sowie des BKA waren als weniger einschlägig einzuordnen. Accounts mit einem reinen oder überwiegend (kriminal-)präventiven Fokus sind bisher die Ausnahme.

Während Twitter als das schnellere und für Krisenlagen und einsatzbegleitende Kommunikation relevantere Medium angesehen wird, gilt Facebook bei den Befragten als die geeignetere Plattform für anlassunabhängige Kommunikation und die Vermittlung auch längerer kriminalpräventiv ausgerichteter Beiträge. Diese umfassen im Kern Informationen über Kriminalitätsrisiken und Möglichkeiten des Selbstschutzes bzw. der Vermeidung solcher Risiken, aber auch Hinweise auf Informations- und Kontaktmöglichkeiten.

4.1 Definition und Typisierung kriminalpräventiver Inhalte

Die inhaltliche bzw. thematische Bandbreite, die im Rahmen polizeilicher Kriminalprävention abgedeckt wird, ist groß. Sie beinhaltet nicht nur Aktivitäten, die als Kriminalprävention im engeren Sinn verstanden werden können, also einen deliktischen Bezug aufweisen und sich mit der Prävention konkreter Straftaten beschäftigten. Zum Tätigkeitsbereich der Fachabteilungen für Kriminalprävention innerhalb der deutschen Polizeien werden darüber hinaus auch Anstrengungen in Bereichen gezählt, die nicht unbedingt als deliktisch oder prädeliktisch angesehen werden (müssen), z. B. die Bereiche Alkohol-/Substanzkonsum, Mobbing, Radikalisierung, Intoleranz, Zivilcourage und Verkehrssicherheit.

Bereits bei der Auswertung des Forschungsstandes wie auch den ersten informellen Gesprächen wurde deutlich, dass es sehr unterschiedliche Ansichten gibt, was einen kriminalpräventiven Beitrag ausmacht und es insofern an klaren Definitionen und Operationalisierungen mangelt. Ein wichtiger Schritt der Untersuchung bestand entsprechend darin, Kriterien zu entwickeln, die die Erhebung und Kategorisierung von digitalen Inhalten mit kriminalpräventiver Dimension erlauben. Eine intensive Exploration lieferte einen Eindruck der Bandbreite der Inhaltstypen auf polizeilichen Accounts und insbesondere von Beiträgen, die eine mehr oder weniger deutliche kriminalpräventive Dimension aufweisen. Ein entsprechender Gehalt kann sehr subtil bzw. latent oder sogar nur außertextlich vorhanden sein, was paradoxerweise auch bei Beiträgen zu beobachten war, die eigentlich ganz offenbar aus kriminalpräventiver Intention gepostet wurden, etwa verdeutlicht durch ein entsprechendes Kampagnenlogo. Auf Basis dieser Exploration wurden eine Arbeitsdefinition und Kategorisierungskriterien für kriminalpräventive Beiträge entwickelt, welche dann anhand eines Datenkorpus von letztlich über 1.300 auf polizeilichen Facebookaccounts[10] erhobenen Beiträgen in einem iterativen Prozess verfeinert wurden. Tab. 2 zeigt, welche Kriterien ein Beitrag aufweisen musste, um im Rahmen der Analyse als kriminalpräventiv relevant eingestuft zu werden.

[10]Wie oben bereits erwähnt wird Facebook als die derzeit für entsprechende Inhalte relevanteste bzw. am intensivsten genutzte Plattform angesehen.

Tab. 2 Einschlusskriterien für Beiträge mit kriminalpräventivem Gehalt

Inhalt des Beitrags muss *mindestens einem* der untenstehenden Themenfelder zugeordnet werden können		Inhalt des Beitrags muss *mindestens eines* der untenstehenden Kriterien erfüllen
• Kriminalprävention im eigentlichen Sinne (mit deliktischem Bezug) • Weitere Tätigkeitsgebiete der polizeilichen Kriminalprävention, die nicht notwendigerweise (prä-)deliktisch sein müssen; konkret: Alkohol-/Substanzkonsum, Mobbing, Radikalisierung, Intoleranz, Zivilcourage[a]	+	• Über eine Einzelfallschilderung hinausgehende Explikation von Gefahren, Risiken oder Schutzmöglichkeiten • Bezug zu oder Hinweis auf eine Kampagne oder Veranstaltung, die Aufklärung über Gefahren, Risiken oder Schutzmöglichkeiten beinhaltet • Auskünfte bezüglich der (aktuellen und lokalen) Kriminalitätsentwicklung (allgemein oder deliktspezifisch)

[a]Der Bereich der Verkehrsunfallprävention wurde aus der Definition ausgeschlossen, es sei denn, entsprechende Beiträge wiesen einen deliktischen Bezug auf (z. B. illegale Autorennen, Trunkenheit im Verkehr)

Für die weitere Typisierung wurden die Beiträge hinsichtlich ihres kriminalpräventiven Inhalts betrachtet. Dabei spielte zum einen eine Rolle, wie stark die kriminalpräventive Komponente im Fokus des Beitrags steht (nachfolgend als „Gehalt“ bezeichnet), zum anderen, ob der Beitrag selbst relevante Informationen enthält, die dazu geeignet sein können, zur Kriminalprävention beizutragen, indem sie den Adressaten Informationen über Kriminalitätsrisiken und/oder Möglichkeiten, sich vor Kriminalitätsrisiken zu schützen, vermitteln (nachfolgend als „Position“ bezeichnet). Daraus ergeben sich hinsichtlich des Gehalts drei Kategorien kriminalpräventiver Beiträge (zentral, parallel/peripher und latent), von denen sich zwei wiederum in zwei Unterkategorien hinsichtlich der Position der relevanten Information unterteilen lassen (unmittelbar im Beitrag enthalten oder nur als externer Verweis vorhanden). Bei Beiträgen mit unmittelbar enthaltener Information (Unterkategorie a) sind sicherheitsrelevante Hinweise im Post selbst enthalten, bei solchen mit externem Verweis (Unterkategorie b) wird auf eine Informationsquelle verwiesen, welcher kriminalpräventive Hinweise entnommen werden können/sollen (sowohl Links zu entsprechenden Webseiten oder einer laufenden Kampagne als auch etwa Hinweise auf kriminalpräventive Veranstaltungen, Infostände, Sprechstunden, Beratungsstellen und ähnliches). Das Raster ist in Tab. 3 abgebildet.

Tab. 3 Typisierung kriminalpräventiver Beiträge

Kat.	KP-Gehalt	Definition	Unterkategorien
1.	Zentral	Kriminalpräventiver Inhalt ist einziger oder überwiegender Fokus des Posts	1a) Beschreibung von Gefahren, Risiken oder Schutzmöglichkeiten unmittelbar im Beitrag enthalten 1b) Beschreibung von Gefahren, Risiken oder Schutzmöglichkeiten nur als externer Verweis vorhanden
2.	Parallel oder peripher	Kriminalpräventiver Inhalt ist mit anderem Inhalt kombiniert, entweder in gleichberechtigter Form oder als Anhängsel desselben	2a) Beschreibung von Gefahren, Risiken oder Schutzmöglichkeiten unmittelbar im Beitrag enthalten 2b) Beschreibung von Gefahren, Risiken oder Schutzmöglichkeiten nur als externer Verweis vorhanden
3.	Latent	Kriminalpräventive Dimension ist nur angedeutet (z. B. Information über Kriminalitätsentwicklung) oder wird behauptet, aber weder eine Beschreibung von Gefahren, Risiken oder Schutzmöglichkeiten noch ein Verweis auf entsprechende Informationen an anderer Stelle ist vorhanden	–
4.	Keiner	Kein KP-Gehalt entsprechend Einschlusskriterien (siehe auch Tab. 2)	–

4.2 Anteil und Zusammensetzung

Im Rahmen der Untersuchung war die Rolle kriminalpräventiver Inhalte auf polizeilichen Accounts sowohl im Rahmen der alltäglichen Onlinekommunikation als auch im Rahmen intensiverer Kampagnen zu spezifischen Kriminalitätsthemen von Interesse. Im Untersuchungszeitraum ließen sich vor allem in Nordrhein-Westfalen landesweite kriminalpräventive Kampagnen identifizieren, die etwa in Form von jeweils einer Aktionswoche zum Thema Taschendiebstahl („Augen auf und Tasche zu“, 10. Juli 2017 bis 16. Juli 2017) und zum

Wohnungseinbruchsdiebstahl („Riegel vor! Sicher ist sicherer“, 09. Oktober 2017 bis 15. Oktober 2017) durchgeführt wurden. Auf den Accounts der teilnehmenden nordrhein-westfälischen Polizeibehörden wurden in den beiden Aktionswochen sämtliche (also nicht nur die kriminalpräventiven) Beiträge erhoben; dies schloss auch geteilte Beiträge ein, also solche, die von der jeweiligen Behörde nicht selbst erstellt worden waren. Um eine vergleichende Analyse mit dem Regelbetrieb durchführen zu können, wurden zudem auf den gleichen Accounts für zwei weitere (nicht direkt anschließende, aber zeitlich nahe liegende) Wochen, in denen keine kriminalpräventiven Kampagnen verortet waren (07. August 2017 bis 13. August 2017 und 04. September 2017 bis 10. September 2017), ebenfalls alle veröffentlichten Beiträge erhoben. In den vier Untersuchungswochen wurden insgesamt 1321 Posts auf 26 Accounts erhoben, kategorisiert und analysiert.

Der Anteil kriminalpräventiver Inhalte am Gesamtaufkommen variiert stark zwischen den Behörden, sowohl in den „Aktionswochen“ (Zeitraum mit laufender Kampagne), wo eine Spanne von 26 % bis 91 % festzustellen ist, als auch in den „Kontrollwochen“ (Zeitraum ohne laufende Kampagne), wo die Spanne 4 % bis 60 % beträgt. Im Durchschnitt über alle 26 Behörden ist für die Aktionswochen ein Anteil kriminalpräventiver Beiträge von insgesamt 46 % festzustellen, in den Kontrollwochen lediglich von 20 %. Dies ist in Abb. 4 dargestellt,

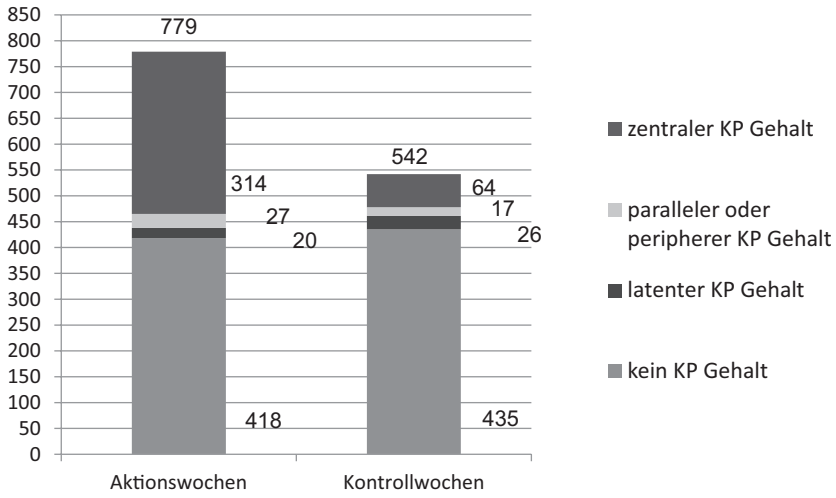


Abb. 4 Zusammensetzung der in den Aktions- und Kontrollwochen veröffentlichten Beiträge

wo die Beiträge mit kriminalpräventiver Dimension zusätzlich entsprechend ihres kriminalpräventiven Gehalts (zentral, parallel/peripher, latent) unterschieden werden. Dabei ist auch zu erkennen, dass die im Rahmen der Aktionswoche veröffentlichten Beiträge (die in der Regel der Kategorie „zentraler KP Gehalt“ zuzuordnen waren) offenbar als temporäre Zugabe quasi auf das reguläre Aufkommen aufgesetzt wurden.

Im Rahmen der Analyse der beiden Aktionswochen wurde zusätzlich zu den Beiträgen die Anzahl der Nutzerinteraktionen für die insgesamt 779 Beiträge erfasst und ausgewertet. Als Nutzerinteraktionen ist die Gesamtheit der Kommentare, Reaktionen („Gefällt mir“, „Love“, „Haha“, „Wow“, „Traurig“, „Wütend“) sowie der „Geteilt-“Angaben definiert. In Tab. 4 ist dargestellt, dass Beiträge mit kriminalpräventivem Inhalt deutlich weniger Nutzerinteraktionen hervorrufen als solche ohne einen erkennbaren kriminalpräventiven Bezug. Die ohnehin wenigen vorhandenen Kommentare beschränken sich zudem meist auf kurze Zustimmungsbekundungen, welche auf wenig Auseinandersetzung mit der Thematik hindeuten.

Von einer verhältnismäßig geringen Attraktivität kriminalpräventiver Beiträge wurde auch in den Experteninterviews und Hintergrundgesprächen mit Praktikerinnen und Praktikern berichtet. Innerhalb der drei Typen kriminalpräventiver Inhalte sind hinsichtlich der Nutzerinteraktionen Beiträge des ersten Typs (zentraler KP-Gehalt) am schwächsten positioniert. Beiträge des zweiten Typs (paralleler/peripherer KP-Gehalt) indessen scheinen auf die Nutzer weitaus attraktiver zu

Tab. 4 Nutzerinteraktionen bei Beiträgen im Zeitraum der Aktionswochen

	Anzahl Beiträge	Nutzerinteraktionen (Median)	Nutzerinteraktionen (arithmetisches Mittel)
Gesamte Beiträge im Zeitraum der Aktionswochen	779	21	63
Davon Beiträge ohne kriminalpräventiven Gehalt	418	41	94
Davon Beiträge mit kriminalpräventivem Gehalt	361	11	27
Davon mit zentralem KP-Gehalt (Typ 1)	314	10	22
Davon mit parallelem/peripherem KP-Gehalt (Typ 2)	27	27	75
Davon mit latentem KP-Gehalt (Typ 3)	20	15,5	40

wirken. Je deutlicher ein Beitrag als mit kriminalpräventiver Intention erstellt zu identifizieren ist, desto geringere Reaktionszahlen scheint er hervorzurufen.

„reine Präventions-Posts, die sind bei uns als Rohrkrepierer verschrien.“ (Exp_PÖA).

Bei Beiträgen des zweiten Typs sind die kriminalpräventiven Bezüge/Botschaften in aller Regel an aktuelle Einzelfallschilderungen oder deliktische Häufungen mit zumeist lokalem Bezug geknüpft. Dies korrespondiert mit der durchgehend von den Praktikerinnen und Praktikern geschilderten Wahrnehmung, dass der lokale und zeitliche Bezug für den Großteil der Abonnenten/Follower und damit tendenziell auch insgesamt für die Aufmerksamkeit, die einem Beitrag zukommt, von zentraler Relevanz ist. Typ drei (latenter KP-Gehalt) indessen weist im Mittel nur unwesentlich mehr Nutzerinteraktionen als Typ eins auf, obwohl auch hier zumeist aktuelle und lokale Bezüge bestehen.

4.3 Thematischer Fokus und Gestaltung

Bei der qualitativen inhaltlichen Analyse der Beiträge mit kriminalpräventiver Dimension zeigen sich Kontinuitäten in der (kriminalpräventiven) Kommunikation. Der aktuelle polizeiliche Nutzungsmodus von Social Media für den Zweck Kriminalprävention ist ähnlich wie bei den klassischen Medien (z. B. Broschüren und Flugblätter) fast vollständig als universelle Prävention zu charakterisieren. Hierbei wird die Öffentlichkeit als Ganzes angesprochen und zwar in der Regel als Gefährdete, sprich potenzielle Geschädigte von Straftaten; eine selektive oder indizierte Ansprache besonders gefährdeter oder potenziell delinquenter Personen/Gruppen ist die Ausnahme.

Auffällig ist zudem eine deutliche inhaltliche Selektivität bei kriminalpräventiven Beiträgen auf den behördlichen Accounts. Die Posts sind nicht nur in den entsprechenden Aktionswochen, sondern auch im Regelbetrieb weit überwiegend dem Bereich der Eigentums- und Vermögensdelikte zuzuordnen, behandeln Wohnungseinbruchsdiebstahl, Taschen- und Trickdiebstahl sowie Betrugsdelikte. Die Bandbreite kriminalpräventiver Inhalte, wie sie etwa im Medienangebot des Programms Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK[11]) zu finden ist, bildet sich dabei kaum ab. Überraschend

[11] https://www.polizei-beratung.de/medienangebot/

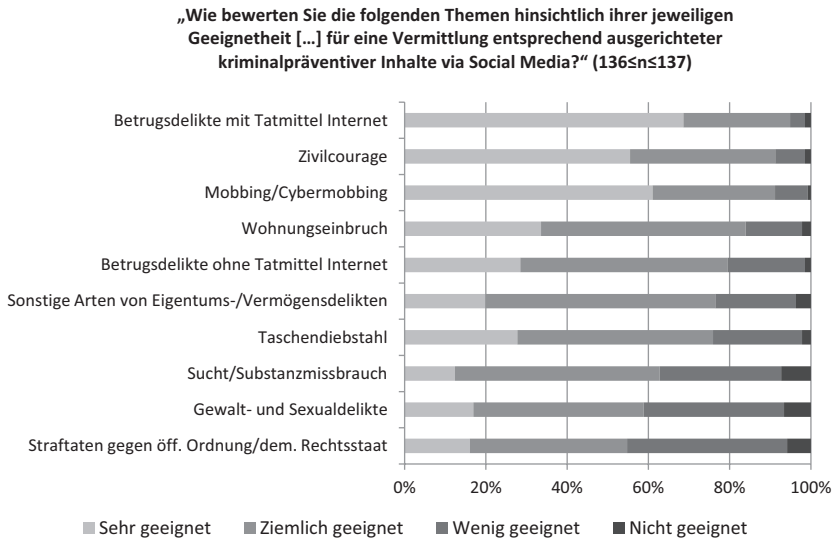


Abb. 5 Schriftliche Befragung PÖA und KP: Geeignetheit kriminalpräventiver Inhalte/Themen zur Behandlung in Social Media

ist, dass auch der eigentlich naheliegende Themenbereich der Internetsicherheit kaum präsent ist. Umso mehr, da auch die schriftlich befragten polizeilichen Beschäftigten in den Bereichen KP und PÖA (jeweils 70 Befragte) gerade Präventionsinhalte mit Bezug auf Internetbetrug als am besten geeignet[12] für die Behandlung in Social Media bewerteten (Abb. 5).

Hinsichtlich der Ausschöpfung der Möglichkeiten, die Social Media bieten, lässt sich feststellen, dass zwar mitunter das Potenzial genutzt wird, audiovisuelle Inhalte unkompliziert zu verbreiten, dass aber die Social Media kennzeichnende interaktive, dialogische Ebene zur Vermittlung präventiver Inhalte (bisher) wenig genutzt wird. Ausnahmen im Untersuchungszeitraum stellten etwa sogenannte Facebook-Sprechstunden, dar. Zwar tendiert das Modell „Sprechstunde“ oder auch „Expertenchat“ letztendlich zu einem unidirektionalen Informationsfluss vom Beratenden (Polizei) zum Beratenen

[12]Vorgegeben waren die in der Abbildung gezeigten zehn (für Deutschland) typischen Betätigungsfelder polizeilicher Kriminalprävention, sowie die Möglichkeit, weitere Themen zu nennen und zu bewerten.

(Bürgerin/Bürger), jedoch ist durchaus Diskussions- und Aushandlungspotenzial gegeben, wobei die Resonanz auf die Präventionssprechstunden allerdings oftmals gering ausfiel und nur wenige Fragen im Livechat gestellt wurden. Eine Besonderheit stellte dabei die unmittelbare Einbindung von örtlichen Kolleginnen oder Kollegen aus dem Bereich der Kriminalprävention dar, die ansonsten kaum eine Rolle bei der kriminalpräventiven Kommunikation auf den polizeilichen Accounts spielen. Wie eingangs angeschnitten wurde, liegt die „Hoheit" über fast alle polizeilichen Social Media Accounts der deutschen Polizeibehörden bei den eng an die Behördenleitungen gebundenen Abteilungen für Presse- und/oder Öffentlichkeitsarbeit.

Im Rahmen der Interviews mit polizeilichen Praktikerinnen und Praktikern der Presse- und Öffentlichkeitsarbeit und der Kriminalprävention zeigte sich, dass die beiden Abteilungen zwar durchaus – in unterschiedlicher Intensität – in Kontakt stehen, dass aber zum einen dieser Kontakt zumeist eher unregelmäßig und vor allem anlässlich von Ereignissen wie kriminalpräventiven Kampagnen, Großveranstaltungen oder deliktischen Häufungen (z. B. einer Einbruchsserie) stattfindet. Zum anderen haben die KP-Abteilungen in Bezug auf die polizeilichen Accounts gewöhnlich eher eine unterstützende Funktion, liefern also etwa Informationen zu, die von der PÖA eingestellt (und davor ggf. für Social Media aufbereitet) werden, oder nehmen an gemeinsamen Aktionen teil.

> „Also wir liefern ja nur. Das darf man ja nicht vergessen. So eine Facebook-Sprechstunde wird ja von PÖA im Grunde genommen organisiert. Wir stehen für die Fachfragen zur Verfügung." (Exp_KP)

Bezogen auf die Intensität der Zusammenarbeit im Allgemeinen gilt es sicherlich die organisatorische (verschiedene Abteilungen) sowie die räumliche Trennung (Abteilungen befinden sich häufig nicht im gleichen Gebäude) zu beachten. Mit Blick auf die konkrete Zusammenarbeit im Rahmen kriminalpräventiver Social Media Aktionen kann die Annahme formuliert werden, dass hier auch Generationenunterschiede eine Rolle spielen könnten, etwa was die grundsätzliche Affinität für Social Media betrifft. Dabei wird auf den höheren Altersdurchschnitt im Bereich KP im Vergleich zum Bereich PÖA angespielt.

> „dass Berufsanfänger im Bereich der Prävention arbeiten, ist […] eigentlich ausgeschlossen. […] Das ist bei sozialen Medien nicht der Fall. Diejenigen, die in sozialen Medien aktiv sind, sind auch häufig diejenigen, die […] jünger sind." (Exp_PÖA)

Während die interviewten Akteure der PÖA, für die Social Media alltägliche Arbeitswerkzeuge darstellen, durchweg grundsätzlich positive, auf die Chancen konzentrierte Einstellungen zur polizeilichen Social Media Nutzung aufwiesen, war bei den Vertreterinnen und Vertretern der KP eher Zurückhaltung festzustellen. Diese hatten allerdings zum größten Teil bislang keine konkreten Erfahrungen mit der beruflichen Nutzung von Social Media gemacht. Auch hier wurde dies nicht zuletzt als Generationenfrage gesehen.

> „ich bin kein Digital Native. Und das muss ich einfach so auch akzeptieren. Auch dass die heutige, auch nonverbale Kommunikation dem Wandel unterliegt, eine ganz andere Dynamik hat und dann müssen das eigentlich die machen, die tatsächlich dann auch die Digital Natives sind.“ (Exp_KP)

5 Fazit

Zusammenfassend lässt sich feststellen, dass kriminalpräventive Beiträge auf polizeilichen Accounts in der Regel universeller Prävention bzw. Generalprävention zuzuordnen sind und die Adressatinnen und Adressaten fast ausschließlich als potenzielle Geschädigte bzw. von recht allgemein gehaltenen Kriminalitätsgefahren Bedrohte adressiert werden. Nur selten werden konkrete Zielgruppen angesprochen, sondern eher die Bevölkerung als Ganzes. Versuche, direkter und zielgruppenspezifisch bestimmte Risikogruppen (mögliche Opfer, aber eben auch potenzielle Täter) anzusprechen, sind selten und bleiben meist relativ allgemein. Für eine gezieltere Ansprache dürften allerdings ohnehin andere Plattformen geeigneter sein als die eine breite Öffentlichkeit adressierenden allgemeinen Behördenaccounts auf Facebook und Twitter.

Kriminalpräventive Inhalte sind insgesamt gestalterisch relativ wenig ausdifferenziert und die Möglichkeiten digitaler Medien werden nur bedingt ausgeschöpft; dies betrifft sowohl die audiovisuellen Gestaltungsmöglichkeiten, als auch die interaktive oder auch nur dialogische Ebene. Die Beiträge weisen oft einen „do-it-yourself-Charakter“ auf (und bleiben damit mitunter hinter der gestalterischen Qualität von „offline“-Materialien zurück), was auch mit den begrenzten personellen und sachlichen Ressourcen verbunden sein dürfte, die dafür zur Verfügung stehen. Gegenüber anderen Inhalten stechen sie kaum heraus und scheinen wenig Beachtung zu erfahren. Im Vergleich zu anderen Inhalten weisen sie mit die niedrigsten Reaktions- und Interaktionszahlen auf, laden anscheinend also kaum und selten zum Teilen, Kommentieren, Liken oder sogar

zum Dialog bzw. einer tiefer gehenden gemeinsamen Auseinandersetzung mit den enthaltenen Botschaften ein. Auch von ihren Urhebern werden sie in der Regel als vergleichsweise unattraktiv charakterisiert.

Zudem ist eine geringe thematische Bandbreite festzustellen. Der Schwerpunkt liegt auf Eigentums- und Vermögensdelikten wie Wohnungseinbruchsdiebstahl, Taschen- und Trickdiebstahl und Betrug. Schwerere Delikte wie Gewalt- und Sexualdelikte, politisch motivierte Kriminalität und ähnliches sind kaum Thema kriminalpräventiver Beiträge auf polizeilichen Accounts; sie werden wenn überhaupt in Form konkreter Ereignisse kommuniziert, oft in Kombination mit Fahndungsaufrufen. Auch das Thema (Cyber-)Mobbing[13] ist wenig präsent, obwohl es angesichts der jungen Zielgruppe und der heute oft üblichen Involvierung digitaler Medien eigentlich naheliegt; das gleiche gilt für das Thema Zivilcourage, welches ebenfalls selten und wenn dann vorwiegend indirekt, das heißt in Form der positiven oder negativen Bewertung des Handelns konkreter Personen bei geschilderten, aktuellen Ereignissen angeschnitten wird.

In einigen Beiträgen sind Ansätze zu erkennen, die auch in der polizeilichen Kriminalprävention jenseits des Internets (also „in real life“) und in einschlägigen polizeilichen und wissenschaftlichen Veröffentlichungen beschrieben und empfohlen werden, nämlich die Einbeziehung von „Guardians“ (zum Begriff der capable guardians vgl. etwa Cohen und Felson 1979); diese sollen kriminalpräventive Informationen, die für vulnerable Menschen in ihrem Umfeld relevant sein könnten, an diese weitervermitteln oder die Informationen selbst in Handeln umsetzen, das geeignet ist, zum Schutz anderer Menschen beizutragen. Entsprechende Strategien lassen sich unter anderem in Informationen finden, die sich mit Delikten gegen ältere Menschen auseinandersetzen; so wurde im Untersuchungszeitraum etwa vor betrügerischen Anrufen angeblicher Polizeibeamter gewarnt und im Beitrag explizit dazu aufgerufen, auch ältere Angehörige zu informieren.

Ein zentrales Funktionsmerkmal von Social Media, nämlich die Möglichkeit zur Interaktion und zum Dialog, wird von vielen polizeilichen Befragten auf ihre reichweitengenerierende Teilfunktion reduziert, nämlich in Form des Teilens und Weiterverbreitens von polizeilichen Inhalten. Der bi- oder multilaterale Austausch der Polizeibehörden mit den Adressatinnen und Adressaten wird kaum in den Mittelpunkt gerückt. Mindestens implizit bestimmt nach wie vor ein recht

[13]Auch wenn die darunter gefassten Handlungen nicht zwangsläufig (Vorstufen von) Kriminalität darstellen, ist dies doch ein relevantes Handlungsfeld polizeilicher Kriminalprävention in Deutschland.

klassisches Sender-Empfänger-Modell die Vorstellungen und Ansprüche der polizeilichen Akteure. Dies spiegelt sich auch in den kriminalpräventiven Inhalten wider, die in der Regel nach dem Muster gestaltet sind, dass die Polizei als Spezialistin mit Expertenwissen die Öffentlichkeit über Kriminalitätsrisiken und ggf. Handlungsoptionen informiert. Eine Aushandlung über die Informationen und Ratschläge ist dabei fast nie und eine Anschlusskommunikation höchstens in rudimentärer Form vorgesehen. Hier sind auch wieder die personellen Ressourcen zu beachten, die eine Auseinandersetzung mit Kommentaren von Nutzern nur in begrenztem Maß zulassen. An dieser Stelle läge zudem eine häufigere und direktere Einbindung von Beschäftigten aus der Kriminalprävention nahe und böte Potenzial. Dass dies jedenfalls auf lokaler Ebene bisher nur selten geschieht, lässt sich neben offenkundigen Hindernissen wie räumlicher und organisatorischer Distanz und unterschiedlichen Funktionsbeschreibungen und Schwerpunktsetzungen auch auf organisationskulturelle Unterschiede zurückführen. Einer niedrigen Affinität bis hin zu einer ausgeprägten Skepsis gegenüber Social Media bei den Beschäftigten im Bereich KP steht eine höhere Innovationsaffinität (freilich auch vor dem Hintergrund eines hohen Anpassungsdrucks an sich wandelnde Kommunikationsgepflogenheiten) im Bereich PÖA gegenüber. Zudem sieht sich nicht nur die Prävention als „polizeiintern zumindest umstrittener bis wenig anerkannter Bereich“ (Howe 2017, S. 167) vor besondere Herausforderungen gestellt, wenn es darum geht, ihren Ansätzen Geltung zu verschaffen; auch die Social Media Nutzung ist, als neuer Aufgabenbereich, innerhalb der Institution nicht unumstritten. Internes „Lobbyieren“ (Howe 2017) ist entsprechend in beiden Bereichen wichtig und notwendig.

Literatur

Bayerl, P. S., van der Giessen, M., & Jacobs, G. (2015). Report on existing approaches and best/effective practices to community policing (11–15). https://www.unity-project.eu/wp-content/uploads/2015/12/D3.1-Report-on-Existing-Approaches-and-Best-Practices-to-CP.pdf. Zugegriffen: 2. März 2018.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608.

Eisenegger, M. (2015). Identität, Image und Reputation – Eine kommunikationssoziologische Begriffsarchitektur. In R. Fröhlich, P. Szyszka, & G. Bentele (Hrsg.), *Handbuch der Public Relations* (S. 431–460). Wiesbaden: Springer VS.

Fanta, A. (2018). Twitter und die Hauptstadtbullen: Darf die Polizei eigentlich Ironie? https://netzpolitik.org/2018/twitter-und-die-hauptstadtbullen-darf-die-polizei-eigentlich-ironie/. Zugegriffen: 24. März 2019.

Habermas, J. (1962). *Strukturwandel der Öffentlichkeit.* Frankfurt a. M.: Suhrkamp.

Hagen, L. M., Wieland, M., & In der Au, A.-M. (2017). Algorithmischer Strukturwandel der Öffentlichkeit. *Medien Journal, 2,* 127–143. https://ejournals.facultas.at/index.php/medienjournal/article/download/1476/1336/. Zugegriffen: 29. Sept. 2018.

Howe, C. (2017). Infrastruktur: Praktiken einer internen Lobbyarbeit. In T. Scheffer, C. Howe, E. Kiefer, D. Negnal, & Y. Porsché (Hrsg.), *Polizeilicher Kommunitarismus. Eine Praxisforschung urbaner Kriminalprävention* (S. 167–182). Frankfurt a. M.: Campus.

Klotter, G., & Mayer, A. (2018). Evidenzorientierte Qualitätssicherung in der Polizeiarbeit – Am Beispiel des Programms Polizeiliche Kriminalprävention der Länder und des Bundes. In M. Walsh, B. Pniewski, M. Kober, & A. Armborst (Hrsg.), *Evidenzorientierte Kriminalprävention in Deutschland: Ein Leitfaden für Politik und Praxis* (S. 113–128). Wiesbaden: Springer VS.

Krischok, H. (2018). Das Internet in der polizeilichen Gefahrenabwehr. In T.-G. Rüdiger & P. S. Bayerl (Hrsg.), *Digitale Polizeiarbeit: Herausforderungen und Chancen* (S. 237–257). Wiesbaden: VS Verlag.

Leventakis, G., Kokkinis, G., & Papalexandratos, G. (2017). Community policing case studies: Proposing a social media approach. In P. Bayerl, R. Karlović, B. Akhgar, & G. Markarian (Hrsg.), *Community policing – A European perspective* (S. 139–158). Cham: Springer.

Mayer, A. (2016). Strategische Überlegungen zur Rolle der polizeilichen Kriminalprävention: Voraussetzungen erfolgreicher polizeilicher Kriminalprävention. *Forum Kriminalprävention, 2,* 46–48.

MEDIA4SEC. (2016). Report on state of the art review. http://media4sec.eu/downloads/d1-1.pdf. Zugegriffen: 20. Febr. 2018.

Polizei Berlin. (2013). Abschlussbericht Projektgruppe Neue Medien. https://netzpolitik.org/wp-upload/Abschlussbericht_Projektgruppe_Neue_Medien.pdf. Zugegriffen: 2. März 2018.

Rüdiger, T.-G., & Bayerl, P. S. (2018). Digitale Polizeiarbeit: Von Herausforderungen zu Chancen. In T.-G. Rüdiger & P. S. Bayerl (Hrsg.), *Digitale Polizeiarbeit: Herausforderungen und Chancen* (S. 11–15). Wiesbaden: Springer VS.

Schrape, J.-F. (2015). Social Media, Massenmedien und Öffentlichkeit – Eine soziologische Einordnung. In K. Imhof, R. Blum, H. Bonfadelli, O. Jarren, & V. Wyss (Hrsg.), *Demokratisierung durch Social Media? Mediensymposium 2012* (S. 199–211). Wiesbaden: Springer VS.

Sherman, L. W. (1998). *Evidence-based policing*. Washington, DC: Police Foundation.

Wagner, D., & Görgen T. (2018). Polizeiliche Kriminalprävention via Social Media. In A. Dessecker & M. Rettenberger (Hrsg.), *Kriminologie und Praxis. Schriftenreihe der Kriminologischen Zentralstelle: Bd. 73. Medien – Kriminalität – Kriminalpolitik* (S. 53–82). Wiesbaden: Eigenverlag Kriminologische Zentralstelle e. V.

Walsh, M., Pniewski, B., Kober, M., & Armborst, A. (Hrsg.). (2018). *Evidenzorientierte Kriminalprävention in Deutschland: Ein Leitfaden für Politik und Praxis.* Wiesbaden: Springer VS.

Welsh, B. C., & Farrington, D. P. (2007). Evidence-based crime prevention. In B. C. Welsh & D. P. Farrington (Hrsg.), *Preventing crime* (S. 1–17). New York: Springer.

#wiesnwache: Die lustigsten Tweets der Polizei München vom Oktoberfest. (29.09.2018). Abgerufen von münchen.tv. https://www.muenchen.tv/wiesnwache-die-lustigsten-tweets-der-polizei-muenchen-vom-oktoberfest-286162/. Zugegriffen: 24. März 2019.

Vorhersage von Gruppendynamiken auf der Grundlage von Daten aus Sozialen Netzwerken

Michael Spranger und Dirk Labudde

1 Einführung und Motivation

Das Kommunikationsverhalten von Menschen hat sich in der letzten Dekade stark verändert. Es hat eine Verlagerung der Kommunikation in die virtuelle Welt stattgefunden, welche durch die entsprechenden Technologien unterstützt wird. Auf der einen Seite hat die Anzahl der Kommunikationen und der ausgetauschten Nachrichten deutlich zugenommen, auf der anderen Seite lässt sich ein Trend zu spezifischen Sub-Sprachen erkennen. Die Kommunikation in sozialen Medien zeichnet sich durch veränderte Schreibweisen und Wortwahl aus (Spranger et al. 2017a). Ein weiterer Trend neben der Zunahme von Cyberkriminalität im engeren und erweiterten Sinne ist auch, dass ein Teil der Kommunikation zur Planung, Vorbereitung und Durchführung einer Straftat im digitalen Raum erfolgt.

Die globale Vernetzung unserer modernen Informationsgesellschaft ermöglicht es einerseits zu jedem beliebigen Zeitpunkt und von nahezu jedem beliebigen Ort mit unseren Freunden, Bekannten und Geschäftspartnern in Kontakt zu treten; andererseits ermöglicht die Nutzung des Internets aber auch Cyberkriminellen neue Möglichkeiten potenzielle Opfer auszuspähen oder an diese heranzutreten oder sogar weltumspannende kriminelle Netzwerke zu erzeugen.

Straftaten verlagern sich ins Internet, neue Kriminalitätsphänomene entstehen. Der Effekt der Entstehung neuer Kriminalitätsphänomene hat eine Reihe von

M. Spranger (✉) · D. Labudde
Hochschule Mittweida, Mittweida, Deutschland
E-Mail: spranger@hs-mittweida.de

D. Labudde
E-Mail: labudde@hs-mittweida.de

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

T.-G. Rüdiger und P. S. Bayerl (Hrsg.), *Cyberkriminologie,*
https://doi.org/10.1007/978-3-658-28507-4_25

gesellschaftlichen und gesellschaftspolitischen Diskussionen in Gang gesetzt. Allein die Begriffe „Sicherheit“, „Terror“ und „Cyberattacke“ sind zu sogenannten Schlüsselwörtern geworden.

Aus vielen Studien wird klar, dass das Phänomen „Internetkriminalität“ oder „Cybercrime“ verschiedene Termini besitzt. Unter Cybercrime oder IuK-Kriminalität werden Straftaten verstanden, die unter Ausnutzung moderner Informations- und Kommunikationstechnik (IuK) begangen werden (Bundeskriminalamt 2018).

Nach Büchel und Hirsch (2014) zählen dazu klassische Fälle der Computerkriminalität, also Straftaten bei denen explizit in den Tatbestandsmerkmalen Elemente der EDV (Programme, Daten, technische Hilfsmittel) erwähnt werden, Fälle in denen moderne Informations- und Kommunikationstechnologie als Hilfsmittel zur Verabredung, Planung, Vorbereitung oder Durchführung einer Tat genutzt wurde oder Fälle in denen die Netzinfrastruktur selbst zum Ziel einer Straftat geworden ist (z. B. Bedrohung von Informationstechnik). Dies schließt alle Angriffe gegen die Integrität, Verfügbarkeit und Authentizität von elektronisch gespeicherten oder übermittelten Daten ein. Der weitläufige Charakter des Begriffs Cybercrime ist vor allem in den weitgefächerten Möglichkeiten der Einbeziehung des Internets in aktuelle Kriminalitätsphänomene und der hohen Dynamik in der Weiterentwicklung der Informations- und Kommunikationstechnik begründet.

Der Schutz des Einzelnen und der Gesellschaft vor Straftaten aus dem beschriebenen Deliktsfeld muss, im Angesicht steigender Deliktszahlen (Bundeskriminalamt 2019), eines der wichtigsten Ziele jedes Staates mit Zunahme der Digitalisierung sein. Die dezentrale Natur des Cybercrimephänomens macht die Definition und Abgrenzung eines Tatortes schwierig bis unmöglich. Vereinheitlichte Verfahrensweisen und eine harmonisierte Gesetzgebung über Ländergrenzen hinweg sind erforderlich, um die Ausbreitung krimineller Strukturen zu verhindern und die Kommunikation im Netz sicher zu machen. Hier setzt die 2001 vom Europarat ausgehandelte Cybercrime-Konvention an, welche 2009 in Deutschland in nationales Recht umgesetzt wurde (BFDI nennen).

Daneben muss natürlich auch das individuelle Recht auf informationelle Selbstbestimmung im digitalen Raum gewährleistet werden, das heißt prinzipiell kann jeder Bürger selbst entscheiden, ob und welche Informationen er an Dritte weitergeben möchte und gegebenenfalls unter welchen Bedingungen. Ausnahmen hiervon bedürfen grundsätzlich einer gesetzlichen Regelung und erfordern ein Überwiegen des Interesses Dritter oder der Allgemeinheit gegenüber dem Schutzinteresse des Betroffenen. In Deutschland regeln in diesem Zusammenhang insbesondere §§ 152, 163 StPO, die Rechte und damit verbundenen Pflichten von Behörden.

Die Bekämpfung von Cybercrime erfordert im hohen Maße die Analyse öffentlich zugänglicher Daten mit dem Ziel der Aufklärung von Straftaten sowie die Untersuchung spezieller Kriminalitätsphänomene, wie Serienstraftaten, organisierte Kriminalität oder Terrorismus um Muster und Trends zu erkennen, welche die Entwicklung effektiver Strategien zu deren Bekämpfung ermöglichen (s. a. Kap. „GIS und Geoinformatik bei der Polizei“). Derartige Untersuchungen sind in den USA seit längerem unter dem Begriff „Predictive Policing“ (dt. vorhersagende Polizeiarbeit) bekannt. Allgemein bezeichnet der Begriff die Analyse heterogener Datenquellen mit dem Ziel einer effektiveren Bekämpfung bzw. Verhinderung von Kriminalität in der Zukunft (Pearsall 2010).

In Deutschland beschäftigten sich erste Studien vor allem mit der Adaption und Weiterentwicklung geografischer Informationssysteme und raumbasierter Modelle zum Zweck der Bestimmung von Auftrittswahrscheinlichkeiten und Ausbreitungsmodellen von Straftaten (Rolfes 2017). Übertragen auf die virtuelle Welt und hier insbesondere den Bereich der sozialen Netzwerke ermöglicht die Analyse von Gruppendynamiken zum einen langfristige Aussagen über die Entwicklung von Gruppen mit einem gewissen Gefahrenpotenzial z. B. extremistische Gruppierungen in Sport und Politik, zum anderen die kurzfristige Vorhersage von damit verbundenen kritischen Ereignissen. Diese Informationen können von Sicherheits- und Strafverfolgungsbehörden zur strategischen Kräfteplanung genutzt werden.

Die Auswertung digitaler Daten im Netz bezieht sich vor allem auf die von den einzelnen Nutzern wissentlich oder unwissentlich hinterlassenen Spuren, welche auch als digitaler Fußabdruck der jeweiligen Person bezeichnet werden. Zu diesem gehören unter anderem Texte, Kurznachrichten, Bilder, Videos, Browserinhalte (Surfverhalten) und persönliche Informationen aus sozialen Netzwerken, einschließlich der damit verbundenen Metadaten, wie geografische Informationen (Labudde und Spranger 2017; s. Abb. 1).

Viele Straftaten aus dem Phänomenbereich Cybercrime nehmen ihren Anfang in der realen Welt (z. B. Ausspähen von Sicherheitslücken, Social Engineering) oder werden nach virtueller Planung in der realen Welt durchgeführt (z. B. Terroranschläge). Das hat zur Folge, dass virtuelle und reale Welt nicht voneinander getrennt betrachtet werden dürfen. Raumzeitliche und virtuelle Muster müssen stattdessen gemeinsam analysiert und bewertet werden und dienen wechselseitig als Wissensquelle. Im oben betrachteten Beispiel der Analyse von Gruppendynamiken in sozialen Netzwerken ermöglicht beispielsweise die zusätzliche Extraktion von zeitlichen und geographischen Merkmalen aus Social-Media-Texten (Posts und Kommentare) die Korrelation mit realen Ereignissen.

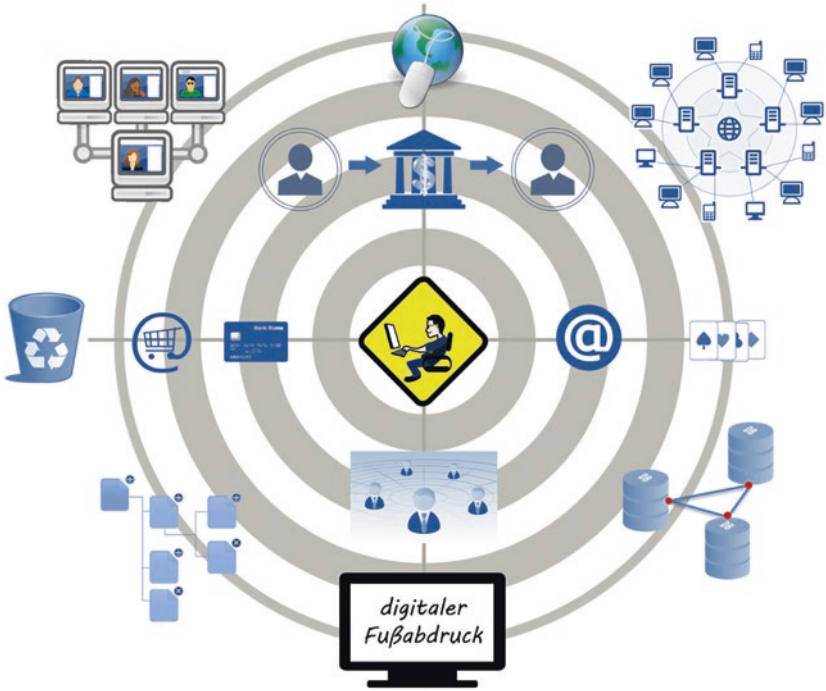


Abb. 1 Spuren eines Nutzers im Netz bestimmen seinen digitalen Fußabdruck (Labudde und Spranger 2017)

Die zukünftige Entwicklung des Predictive Policing ist eng verknüpft mit Fortschritten in den Bereichen des maschinellen Lernens und der künstlichen Intelligenz (Rolfes 2017). Nach einer kurzen Diskussion der Besonderheiten der Kommunikation von virtuellen Gruppen im nächsten Abschnitt sollen daher dem Leser in Abschn. 3 die Möglichkeiten einer Analyse dieser Kommunikation mithilfe moderner Textminingmethoden vorgestellt werden. In Abschn. 4 werden anschließend aktuelle Anwendungsfälle für Predictive Policing aufgezeigt, welche im darauffolgenden Abschnitt mit Informationen aus der Kommunikation virtueller Gruppen verknüpft werden.

2 Kommunikation in virtuellen Gruppen

Als Arbeitsdefinition einer Gruppe schlagen Proshansky und Seidenberg vor:

> „Zwei oder mehr Individuen, die kollektiv wie folgt charakterisiert werden können: Sie haben gemeinsame Normen, Überzeugungen und Werte und sie unterhalten implizit oder explizit definierte Beziehungen zueinander, sodass das Verhalten eines jeden Folgen für den anderen hat. Diese Merkmale (Eigenschaften) entstehen aus der Interaktion der Individuen und haben für sie Konsequenzen, wobei die Individuen hinsichtlich irgendeines spezifizierten Gruppenziels ähnlich motiviert sind.“ (Proshansky und Seidenberg 1965; zitiert nach Dorsch et al. 1994, S. 300)

Die Soziologie unterscheidet zwischen Primär- und Sekundärgruppen, formellen und informellen, sowie zwischen Klein- und Großgruppen. Primärgruppen umfassen Gebilde wie Familie, Freundschaftskreise etc. – dem gegenüber stehen organisationale oder willkürlich gebildete Sekundärgruppen (Dorsch et al. 1994; Cooley 1909). Formelle Gruppen sind vor allem organisational in festen Rollen organisiert und dienen sachlich-instrumentellen Zielen, d. h. sie unterliegen selbstauferlegten Normen und Satzungen (z. B. Arbeitsgruppen). Informelle (willkürliche) Gruppen bilden sich spontan auf der Basis persönlicher Beziehungen, haben jedoch in vielerlei Hinsicht ähnliche Eigenschaften wie formelle (Face-to-Face-Beziehung, Wir-Gefühl, Affektivität) (Döring 2003).

Zur Beschreibung der Gruppendynamik wird zwischen den Dimensionen Zugehörigkeit sowie Macht und Intimität unterschieden (Amann 2003; König und Schattenhofer 2011, S. 34 f.).

2.1 Bedürfnis nach Zugehörigkeit

In der Literatur wird davon ausgegangen, dass das Bedürfnis nach Zugehörigkeit aus der Evolution resultiert. Es umfasst die angeborene Motivation des Menschen nach stabilen, positiven Bindungen. Empirische Befunde weisen darauf hin, dass diese Tendenz unabhängig von Situation und Kultur ist. Es wird beispielsweise argumentiert, dass Menschen die starke, enge Beziehungen zu anderen aufbauen, höhere Überlebenschancen in der Evolutionsgeschichte hatten, waren diese doch in hohem Maße, z. B. bei der Beschaffung von Nahrung voneinander abhängig. Utilitaristische Theorien gehen von sozialen Austauschprozessen aus. Dazu zählen nicht nur materielle Güter, sondern auch psychologische wie Liebe (Baumeister und Leary 1995). So konnten Coan et al. (2006) zeigen, dass allein

die Hand einer anderen Person zu halten, einen positiven Einfluss auf belastende Ereignisse hat. Sie zeigten, warum Bindungen einen starken positiven Einfluss auf das Erleben von kritischen Situationen haben. Ein herausragender Befund war, dass es zu einer Reduktion der Aktivierung des Hypothalamus kam. Damit trägt körperlicher Kontakt dazu bei Stress zu verringern und die psychische und physische Gesundheit zu fördern.

2.2 Bedürfnis nach Macht

Zum Erreichen gemeinsamer Ziele brauchen Gruppen eine Machtstruktur, welche durch Hierarchien oder Normen geschaffen werden kann (König 2012). Besonders in formellen Gruppen der Arbeitswelt sind Hierarchien klar aufgeschlüsselt und Normen festgelegt. Auf die Besonderheiten und Andersverteilung dieser Strukturen wird detaillierter bei informellen Gruppen eingegangen.

Normen entstehen infolge von Interaktion, also wechselseitiger Einflussnahme, bilden sich gemeinsame Verhaltensrichtlinien heraus. Was ist erlaubt, welche Meinungen werden akzeptiert und welche Ziele werden verfolgt? Die Verteilung solcher normativen Erwartungen bezieht sich dabei entweder auf alle Gruppenmitglieder oder auf einzelne Positionen innerhalb der Gruppenhierarchie. Normen sind abhängig von der Gruppenstruktur, gemeinsamen Zielen und von äußeren sozialen Einflüssen. Die Gruppe überwacht, welche Privilegien und Sanktionen beim Einhalten oder Verstoß verteilt werden (Schneider 1975). March (1954) unterteilt Normen in drei Idealtypen und stellt Zusammenhänge zwischen Anerkennung und Verhalten bei drei Normtypen her. Der erste Typus *Norm als unerreichbares Ideal* führt zu einem anhaltenden Anstieg der Zustimmung durch die Gruppe, je mehr sich der Einzelne dieser Vorstellung annähert. *Norm als erreichbares Ideal* führt zu gleichbleibender Zustimmung der Gruppe, sobald das Ideal durch das Individuum erfüllt wird. Der letzte Typ *Norm als Präferenzwert* führt nach Erreichen des Gruppenziels zu einer Abnahme der Gruppenzustimmung, zu finden zum Beispiel bei der Bestimmung des Arbeitstempos in einer Gruppe.

2.3 Bedürfnis nach Intimität

Dieses Bedürfnis ist wachstumsorientiert. Wichtigste Dimensionen sind Reziprozität, emotionale Beziehungen und Liebe. Diese ist zu unterscheiden von dem Bedürfnis nach Nähe, welches durch Angst und Unsicherheit ausgelöst wird. Personen mit einer hohen Ausprägung schließen sich eher Gruppen an

und schließen Freundschaften, als Personen mit einem niedrigen Bedürfnis nach Intimität (Hess 2018). Im Sinne des Gruppenkontexts versteht sich Intimität eher als Nähe der Gruppenmitglieder zueinander, denn enge Freundschaften oder Liebesbeziehungen beruhen auf Exklusivität. So kann es auch zur Untergruppenbildung innerhalb der Gruppen kommen. Dieses Phänomen steigt mit der Anzahl der Gruppenmitglieder an. In digitalen Medien kommt die Anonymität als zusätzliches Merkmal für gruppendynamische Prozesse dazu.

2.4 Informelle Gruppen

Der informellen Gruppe kommt forschungsgeschichtlich eine besondere Bedeutung zu. Mayo (1945) führte in den Jahren 1927–1932 in den Hawthorne-Werken von General Electrics Studien zur Effizienzsteigerung durch. Es wurde mit Beleuchtung, Temperatur, aber auch Arbeitszeiten und Pausen experimentiert. Heraus kam jedoch, dass individuelle Arbeitsleistung und Verbundenheit zum Betrieb vor allem auf die Zusammensetzung der Arbeitsgruppe und den informellen Gruppen zurückgehen. Es lässt sich sagen, je strenger formale Gruppen, desto wichtiger sind die informellen Gruppen. Beide Formen sind jedoch nicht immer streng voneinander separierbar. Beispielsweise sind beide parallel in der Arbeitswelt zu finden, wo sie bedeutsam zum Wechselspiel von Bedürfnis des Individuums und erbrachter Leistung beitragen.

Unterschiede zwischen formellen und informellen Gruppen finden sich insbesondere in deren Eigenschaften. Neidhardt (1999) definiert informelle Gruppen als direkte und dauerhafte Beziehung zwischen beruhendem Interaktions- und Kommunikationsnetz. Das bedeutet es wird anders als in formellen Gruppen und Organisationen auf eine formelle Zugehörigkeit oder Mitgliederorganisation oder Rollendifferenzierung verzichtet. Dieses fordert ein hohes Maß an Sicherheit und Verbundenheit, damit die Gruppe auch außerhalb der Zeiten des direkten Kontakts aufrecht erhalten bleibt. Damit verbunden ist ein hohes Maß an Reziprozität, das heißt Mitglieder müssen dem sozialen Austausch gerecht werden, z. B. durch regelmäßige Treffen oder Kommunikation (Harring et al. 2010). Ein weiteres Merkmal solcher Gruppen ist die begrenzte Größe und relative Dauerhaftigkeit. Anders als in formellen Gruppen sind Hierarchien keine starren Gebilde. In solchen Gruppen bilden sich starke und stabile Hierarchien nur dann aus, wenn es einen hohen Druck zu Handlungen und Entscheidungen gegenüber gegnerischen Gruppen gibt (Neidhardt 1999).

Da es in der Regel keine sanktionierbaren Verpflichtungen gibt, geht informellen Gruppen ein Vertrauensvorschuss voraus. Das bedeutet, die ausbleibende

Verletzung der eigenen Erwartungen an den sozialen Interaktionspartner muss abgesichert sein. Insbesondere darf die offene Kommunikation nicht verletzt werden. Im Vergleich zu formellen Gruppen sind Themen nicht spezifiziert. Es können aber Themen, die einem exklusiven Bereich vorenthalten sind, ausgenommen werden, wie intime Gespräche in Liebesbeziehungen. Grundsätzlich darf über alles geredet werden, was damit eine starke Abgrenzung zu formellen Gruppen wie Arbeitsteams darstellt (Harring et al. 2010). Auch die Kommunikation ist deutlich zu unterscheiden. So darf grundsätzlich jedem Mitglied ein Anliegen vorgebracht werden, wohingegen in formellen Gruppen meist Hierarchien oder festgelegte Normen dem entgegenstehen. Abgrenzungen der Mitglieder entstehen entsprechend der gegenseitigen Interessen, der eigenen Entscheidung der einzelnen Mitglieder, wer mit wem und in welchem Maße Zeit verbringt und im Austausch steht (Harring et al. 2010).

Bohnsack et al. (1995) konnten zeigen, dass Kommunikation nicht primär sach-, zweck- oder produktionsorientiert ist, sondern durch gemeinsam Erlebtes und die Übereinstimmung des Erlebten geprägt ist. Das bedeutet die Kohärenz einer solchen Gruppe beruht auf gefühlter Ähnlichkeit und der Passung eigener Ziele und Werte mit denen der Gruppe, sowie Sympathie und Emotion. Bohnsack et al. (1995) bezeichnen solche Verbindungen als „konjunktiven Erfahrungsraum“, der es ermöglicht einen Abgleich zwischen dem selbst erlebten und den Erfahrungen anderer herzustellen. Damit weisen sie darauf hin, dass sozial geteilte Perspektiven nicht nur Folge ähnlicher Erfahrungen sind, sondern aus Gruppenprozessen heraus entstanden sind.

2.5 Reale und virtuelle informelle Gruppen

Der Begriff der virtuellen Gruppe wurde von Howard Rheingold (1993) geprägt und leitet sich vom Begriff „Virtual Communities“ ab. Allgemein lässt sich eine solche Gruppe als Zusammenschluss von Personen begreifen, die sich nie physisch begegnet sind. Rheingold (1993) versteht virtuelle Gruppen als soziale Zusammenschlüsse von Personen im Netz, die über einen längeren Zeitraum emotional geprägte öffentliche Diskussionen führen, welches ein persönliches Beziehungsgeflecht im virtuellen Raum hervorbringen.

Auch bei dieser nichtphysischen Form lässt sich formell und informell trennen. Beispielsweise gibt es Themenforen oder virtuelle Arbeitsteams in denen Kommunikationsinhalte festgeschrieben und Abweichungen davon sanktioniert werden. Virtuelle Gruppen sind ebenso abhängig von regelmäßiger Kommunikation wie reale. Erst mit wiederholter Kommunikation entsteht das Gefühl

der Zugehörigkeit mit der Gemeinschaft. Die oben beschriebenen Eigenschaften informeller Gruppen lassen sich leicht auf die der virtuellen informellen Gruppen übertragen, allerdings mit Einschränkungen und mehr Lockerung. Gemeinsamkeiten liegen besonders in der Unbestimmtheit der Themen sowie der Kommunikationspraxis.

Bedeutsam sind sicherlich die Größe der Gruppe und der soziale Kontakt untereinander. Allein die Reichweite sozialer Medien und deren Verbreitung lässt ein viel größeres Netz der Gruppenmitglieder zu. Reale informelle Gruppen sind von einer relativen Dauerhaftigkeit geprägt. In virtuellen Gruppen können Zugehörigkeiten schneller wechseln, weil diese mit weniger persönlichen Verlusten verbunden sind, denn die Anonymität hinter den Bildschirmen gewährleistet Intransparenz der eigenen Person. Im Kontrast zu realen Gruppen steht die durch Internetdienste dargebotene Offenheit und Öffentlichkeit, wohingegen reale Gruppenbildung eher auf emotionaler und persönlicher Kommunikation beruht. Hierarchiebildung ist fast ausgeschlossen, denn allein die sichere Zuordnung von realen Personen zu deren virtueller Identität ist kaum möglich (Thiedeke 2003).

Gruppen sind von verschiedenen äußeren Bedingungen abhängig. Dazu zählen besonders Besitzverhältnisse, finanzielle und inhaltliche Ziele, formale Aufgaben- und Verantwortungsverteilung. Ebenso zählen auch kulturelle Einflüsse zu diesen Bedingungen. Zu den inneren Bedingungen zählen insbesondere eigene bewusste und unbewusste Gefühle, Bedürfnisse und Wertvorstellungen, sowie Verhaltensweisen der anderen Mitglieder. Es ist wesentlicher Bestandteil einer Gruppenformation, die eigenen Bedürfnisse in Kohärenz mit denen der Gruppe zu bringen, um ein stabiles Wir-Gefühl zu erzeugen.

Gruppen in sozialen Netzwerken unterliegen den gleichen Bedingungen wie eine Gruppe im realen Raum. Auch eine virtuelle Gruppe besitzt wohldefinierte Dimensionen, um die Bewältigung einer gemeinsamen Aufgabe zu garantieren. Die Abb. 2 stellt die erforderlichen Dimensionen dar.

Im Vergleich zu Gruppen in der realen Welt ist die Machtverteilung in virtuellen Gruppen eher gleichverteilt. Dies führt zu einer größeren Dynamik und einer geschätzten „höheren Ehrlichkeit“, welche durch die Anonymität verstärkt wird. Die tabellarische Gegenüberstellung von Vor- und Nachteilen der Kommunikation in realen und virtuellen Gruppen zeigt eine starke Sachorientierung bei geringem sozialem Einfluss (siehe Tab. 1).

Der transportierte Inhalt in virtuellen Gruppen kann analog zu realen Gruppen in folgende Schwerpunkte unterteilt werden: Information (eigentliche Nachricht), Emotionen, Meinungen und Standpunkte. Mit Werkzeugen des modernen Text Mining ist es möglich diese Kommunikation zu analysieren.

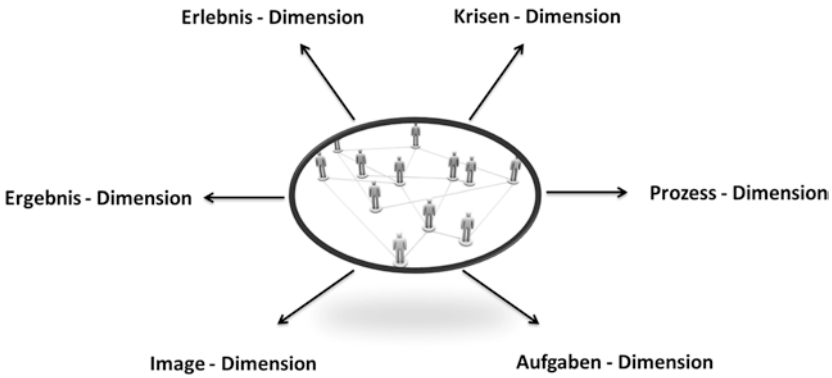


Abb. 2 Dimensionen einer virtuellen Gruppe. (Nach Haug 2016, S. 14)

Tab. 1 Vergleich Gruppenkommunikation reale und virtuelle Welt. (Nach Sulzbacher 2003)

Vorteile Gruppen-kommunikation in der realen Welt	Keine Unterschiede	Vorteile Gruppen-kommunikation in der virtuellen Welt
Besseres Verständnis von Inhalten	Effektivität der Gruppe	Wenig soziale Einwirkungen
Gruppenentscheidungen können leichter erzielt werden	Situationsbezogenes Wissen	Gleichmäßige Verteilung von Kommunikation
Starker Wissenszuwachs, trotz geringer Sachorientierung		Starke Sachorientierung

3 Text Mining – Monitoring der Kommunikation

Der folgende Abschnitt ist Teil der Dissertationsschrift des Autors (Spranger 2019). Der größte Teil der beschriebenen textuellen Daten im Ermittlungsverfahren liegt mittlerweile digital vor, auch wenn sie am Ende teilweise in Papierform überführt werden. In vielen Wirtschafts- und Industriebereichen haben sich Textminingtechnologien als Werkzeug der automatisierten Gewinnung von Informationen aus Text bewährt. Die digitale Kommunikation in virtuellen Gruppen ist mit den modernen Werkzeugen des Text-Mining analysierbar, auch wenn die Texte, welche aus dem Umfeld der Forensik stammen eine besondere

Herausforderung darstellen. Das Kommunikationsverhalten (als Teil des digitalen Fußabdruckes) eines Nutzers bzw. einer Gruppe von Nutzern kann mit modernen Methoden des Text Mining analysiert werden:

> „Mit dem Terminus Text Mining [Hervorhebung der Verfasser] werden computergestützte Verfahren für die semantische Analyse von Texten bezeichnet, welche die automatische bzw. semi-automatische Strukturierung von Texten, insbesondere sehr großen Mengen von Texten, unterstützen.“ (Heyer et al. 2008)

Aufgaben des Text Mining sind unter anderem:

- Identifikation von Termini
- Berechnung semantischer Relationen
- Ähnlichkeiten zwischen Begriffen bestimmen
- Ähnlichkeiten zwischen Dokumenten bestimmen
- Finden von Definitionen, Erläuterungen und Referenzen

Die in der Definition vorgestellte eher pragmatische Definition zeigt, dass Text Mining die Basis für Anwendungen bilden kann, welche als technische Anwendung i. S. d. geschilderten Problematiken Ermittler in ihrer täglichen Arbeit unterstützt. Der entscheidende Durchbruch für den gezielten Einsatz im Bereich polizeilicher Ermittlungen fehlt allerdings bislang und ist dem Fehlen geeigneter Konzepte für die extrem heterogenen Bereiche polizeilicher Ermittlungen und den damit verbundenen heterogenen Texten, welche zudem besondere Charakteristiken aufweisen, zuzurechnen. Hinzu kommt, dass bisherige Lösungsansätze nur Insellösungen für einzelne Untersuchungsproblematiken darstellen, die weder den Kontext der zugehörigen Ermittlungen berücksichtigen, noch die gewonnenen Daten aus unterschiedlichsten Quellen in geeigneter Weise zusammenführen, um einen ganzheitlichen Blick auf die gewonnenen Informationen zu erlauben.

3.1 Forensisches Text Mining

Forensisches Text Mining bezeichnet das interdisziplinäre Feld, welches sich Methoden aus Informationsrückgewinnung, Verarbeitung natürlicher Sprache, Statistik, maschinellen Lernverfahren, Mustererkennung, Datenbanktechnologien, Netzwerkforschung, wissensbasierten Systemen, künstlicher Intelligenz, High-Performance-Computing und Datenvisualisierung nutzbar macht, um

große Mengen von Texten zu strukturieren, mit dem Ziel Muster und Trends zu erkennen, welche die Entwicklung und Vorhersage von Straftaten ermöglichen (Predictive Policing) sowie inkriminierte Texte zu finden und daraus Informationen zu extrahieren, welche zur vollständigen Aufklärung aller Tatumstände einer Straftat beitragen.

Die Analyse digitaler forensischer Texte ist regelmäßig eine Aufgabe in vielen Bereichen kriminalistischer Ermittlungen. Als digitale forensische Texte werden in diesem Zusammenhang alle Texte bezeichnet, welche auf digitalen Speichermedien sichergestellt wurden, weil sie entweder selbst inkriminiert oder anderweitig geeignet sind, eine begangene strafbare Handlung, i. S. d. materiellen Strafrechts – auch teilweise – zu rekonstruieren oder zu beweisen und somit Gegenstand kriminalistischer Ermittlungen mit dem Ziel der Beweissicherung geworden sind. Untersuchungen dieser Art sind ein Teilgebiet der forensischen Informatik und immer abhängig von der vorher durchzuführenden physikalischen Datensicherung.

Im Bereich der organisierten Kriminalität ist in Zeiten von Smartphones und globaler Vernetzung die Verabredung und Anbahnung krimineller Handlungen, selbst über Ländergrenzen hinweg, durch die Verwendung von Kurzmitteilungsdiensten, Messengern und sozialen Netzwerken so einfach geworden wie nie zuvor. Die Nutzung jedes dieser Medien hinterlässt jedoch unweigerlich Spuren, welche – analysiert und ausgewertet – aufschlussreiche Details liefern können und mit deren Hilfe beispielsweise Tathergänge rekonstruiert werden können. Nicht zuletzt erlaubt die Analyse der textbasierten Inhalte öffentlich zugänglicher sozialer Netzwerke, Hinweise auf mögliche Tatverdächtige, Opfer oder Zeugen von Straftaten zu gewinnen oder sogar deren geplante Ausführung ganz oder teilweise zu verhindern.

Kriminalität, die aus dynamischen Gruppen heraus bei Großereignissen entsteht, organisierte und vor allem politisch motivierte Kriminalität stellen regelmäßig eine solche Störung des Gleichgewichtszustandes dar. Informationen, die durch das Beobachten der Aktivitäten derartiger Gruppierungen im Internet und insbesondere in den sozialen Netzwerken gewonnen werden, können dazu verwendet werden, die Wahrscheinlichkeit eines Auftretens derartiger Ereignisse im Sinne vorausschauender Polizeiarbeit (engl.: Predictive Policing) zu bestimmen.

Die Heterogenität der untersuchten digitalen Daten und der schnelle Wechsel von Kommunikationsformen erschweren die Automatisierung dieser Prozesse. Aktuell in Deutschland verfügbare und durch Ermittlungsorgane genutzte

Software, wie beispielsweise X-Ways Forensics[1], Forensic Toolkit (FTK)[2], XRY Office[3] oder Cellebrite UFED Physical Analyzer[4], bilden insbesondere den semantischen Aspekt des Analyseprozesses nur ungenügend und nicht abgestimmt auf die Besonderheiten inkriminierter Texte ab. Sie fokussieren vor allem Aspekte der Sicherung und Wiederherstellung von Daten sowie das schlagwort- oder musterbasierte Suchen in großen Datenbeständen. Versuche, semantische Komponenten basierend auf Erkenntnissen aus dem Bereich des Text Mining zu integrieren, scheitern regelmäßig im Praxistest bei der Konfrontation mit Daten aus laufenden Ermittlungsverfahren.

Im Allgemeinen sind die folgenden abstrakten Aufgaben durch eine computergestützte Lösung zu realisieren:

- Erkennung und Klassifizierung von Texten mit einer fallbasierten kriminalistischen Relevanz
- Erkennung von Entitäten und Relationen als Basis zur Aufdeckung von Täter-Opfer-Netzwerken
- Entdeckung geplanter Aktivitäten
- semantische Erschließung fragmentierter Texte
- Erkennung versteckter Semantik

Forensische Texte sind wie bereits angedeutet beweiserhebliche textuelle Daten, die im Zuge des Beweissicherungsverfahrens durch Beamte der Polizeien der Länder sichergestellt oder beschlagnahmt worden sind. Diese Daten verfügen oft über folgende Eigenschaften:

- das Datenmaterial ist von erheblicher Heterogenität bezüglich seiner Struktur und Domäne
- wichtige Informationen können in nicht textbasierten Daten stecken (z. B. Fotokopien von Rechnungen)
- es gibt völlig irrelevante Texte, welche durch ihre Quantität relevante Informationen verdecken können (Vordrucke, Formulare, Templates, …)

[1] http://www.x-ways.net/forensics/index-d.html

[2] http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk

[3] https://www.msab.com/products/office/

[4] http://www.cellebrite.com/de/Mobile-Forensics/Applications/ufed-physical-analyzer

- Informationen können absichtlich verschleiert worden sein, um sie vor Entdeckung zu schützen
- Texte können von starken syntaktischen Schwächen geprägt sein
- Texte können durch Löschen/Rekonstruktion stark fragmentiert sein

Die aufgeführten Spezifika unterscheiden den untersuchten Textkorpus von anderen üblicherweise in der Forschung verwendeten und evaluierten textuellen Daten. Ferner ergab eine Umfrage, welche durch die Autoren unter Kriminalisten kooperierender Ermittlungsbehörden durchgeführt wurde, dass das Auffinden und Separieren relevanter Dokumente der aufwendigste und schwierigste Teil der Auswertung ist (Spranger und Labudde 2014).

Kurznachrichten (Kurzmitteilungsdienste, Messenger und soziale Netzwerke) sind eine besondere Herausforderung im Rahmen der forensischen Textanalyse. Die Gründe hierfür liegen vor allem in der Kombination der grundlegenden Charakteristik forensischer Texte und einer hohen Informationsdichte, die sich zum einen aus der Beschränkung der zur Verfügung stehenden Anzahl von Zeichen, andererseits aus der Art ihrer Verwendung ableitet. Insbesondere werden Kurznachrichten meist als eine Art „Nebenbei-Nachricht“ versendet, weshalb ihr Kontext für Außenstehende vielfach im Dunkeln bleibt. Da das Kommunikationsverhalten vor allem durch die Art der Verwendung des entsprechenden Mediums geprägt ist, hat ein Wechsel der Plattform bei ähnlicher Nutzung nur einen relativ geringen Einfluss auf das Schreibverhalten der Benutzer. Deshalb können die Ergebnisse prinzipiell auf andere Formen der schriftlichen Kommunikation übertragen werden. Voraussetzung für die Analyse inkriminierter Kurznachrichten ist die Kenntnis der strukturellen und inhaltlichen Besonderheiten dieser Art der Kommunikation (s. Abschn. 2; s. a. Kap. „Warum automatische Verfahren bei der Detektion von Hate Speech nur die halbe Miete sind“).

Das durch die Autoren entwickelte forensische Analysewerkzeug für Kurznachrichten MoNA (Mobile Network Analyzer) bildet einen Prozess für die Analyse der Kommunikation wie folgend ab (s. Abb. 3):

- Physikalische Datensicherung und Export als Excel-Workbook oder XML-Datei
- Einlesen der exportierten Datei in MoNA
- Zusammenfassung einzelner Nachrichten zu zusammenhängenden Gesprächen
- Bewertung jedes Gesprächs hinsichtlich der Fallrelevanz
- Visualisierung des Kontaktnetzwerkes unter Markierung von Kontakten, die verfahrensrelevante Nachrichten ausgetauscht haben

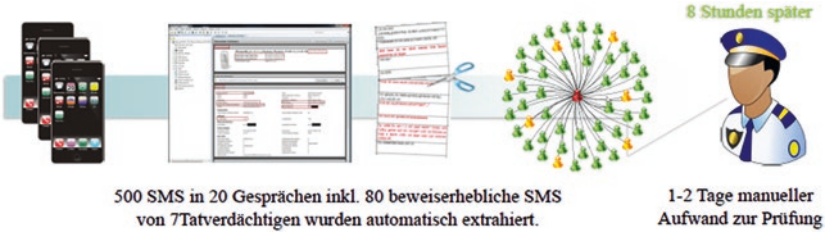


Abb. 3 Analyseprozess forensischer Kurznachrichten mit MoNA (Labudde und Spranger 2017)

- Lesen und Bewerten des reduzierten Suchraums (der Nachrichteninhalte der markierten Gespräche einzelner Kontakte in Abhängigkeit ihrer Relevanz)

Dem Algorithmus wohnt eine Detektion zusammenhängender Konversationen inne. Es werden aus den einzelnen Kurznachrichten über ein statistisches Verfahren sogenannte Gesprächs-Cluster gebildet. Nach Bestimmung der Gesprächs-Cluster, besteht der nächste Schritt darin, herauszufinden, welche dieser Konversationen deliktbezogen relevante Nachrichten hinsichtlich des Untersuchungsauftrages beinhalten (Abb. 4).

Mit dem implementierten Prototyp konnte der Arbeitsaufwand für das Finden verfahrensrelevanter Nachrichten im Ermittlungsprozess auf schätzungsweise 15 % der ursprünglich benötigten Zeit gesenkt werden. In einer Langzeitstudie mit verschiedenen Ermittlungsverfahren sollte dieser tatsächliche Nutzen weiter evaluiert werden.

Neben der Analyse von Kommunikationen einzelner Nutzer bzw. als sogenannte Gruppen-Chats (z. B. WhatsApp) spielt die Analyse von Gruppen (virtuellen Gruppen) in sozialen Netzwerken eine entscheidende Rolle. Die Analyse sozialer Netzwerke aus sicherheitsstrategischer Sicht verfolgt vor allem zwei Ziele. Zum einen sollen potenzielle Gefahren erkannt und in ihrem Umfang und der Lokalisierung abgeschätzt werden. Zum anderen ist für die langfristige Planung von Sicherheitskräften vor allem die Entwicklungsrichtung einer Gruppierung, hinsichtlich ihres Größenwachstums, ihrer Ausrichtung oder Radikalisierung sowie der Zunahme ihrer Gewaltbereitschaft, von Interesse (siehe Abschnitt „Predictive Policing“).

Für die Analyse wurde bereits mit einer prototypischen Implementierung von beschriebenen Frameworks begonnen. Der durch die Autoren entwickelte Social Network Analyzer (SoNA) bildet aktuell, bezogen auf Soziale Netzwerke, die folgenden Features ab:

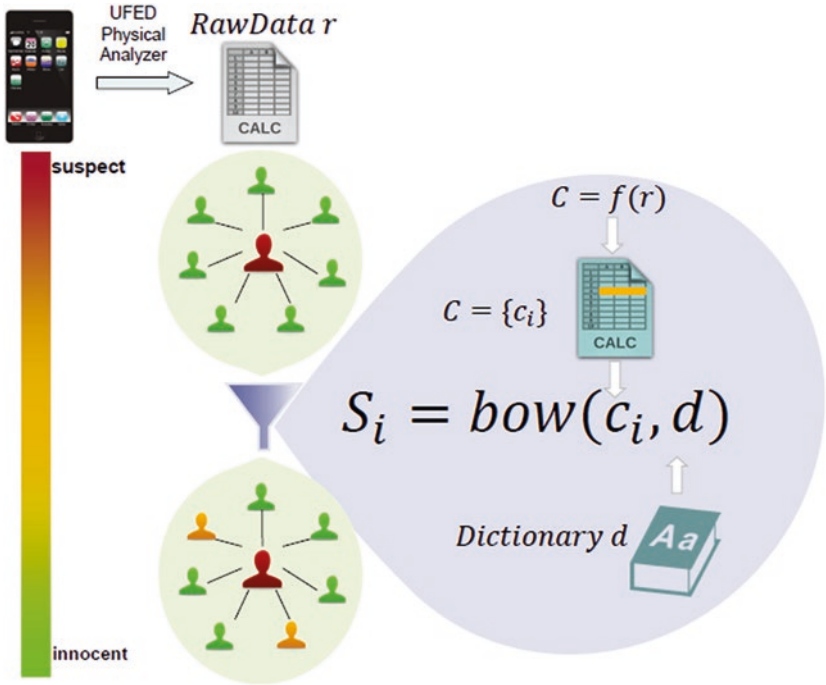


Abb. 4 Prozess der Kurznachrichtenanalyse. Aus den Rohdaten r, werden alle Nachrichten zu Konversationen C (Gesprächs-Cluster) zusammengefasst. Diesen können dann, mithilfe eines Bag-of-Words-Modells und einer auf Ermittlererfahrung beruhenden Wissensbasis, Signifikanzwerte zugeordnet werden. Diese bilden die Grundlage für die Einfärbung fallrelevanter Kontakte im aus r extrahierten Kontaktnetzwerk (Labudde und Spranger 2017)

- musterbasierte Volltextsuche
- zeitbasierte Visualisierung von Personennetzwerken
- zeitbasierte Visualisierung der Kommunikation auf Basis latenter Topics
- wissensbasierte Gefahrenbewertung

Die derzeitige Implementierung und grafische Oberfläche ist in Abb. 5 dargestellt.

Damit ist es möglich Daten von sozialen Netzwerken – aktuell Facebook und Twitter – zu beziehen, zu analysieren und als 2D-Graph darzustellen. Verschiedene Filteroptionen erlauben die Reduktion der Ergebnisse auf die fall-

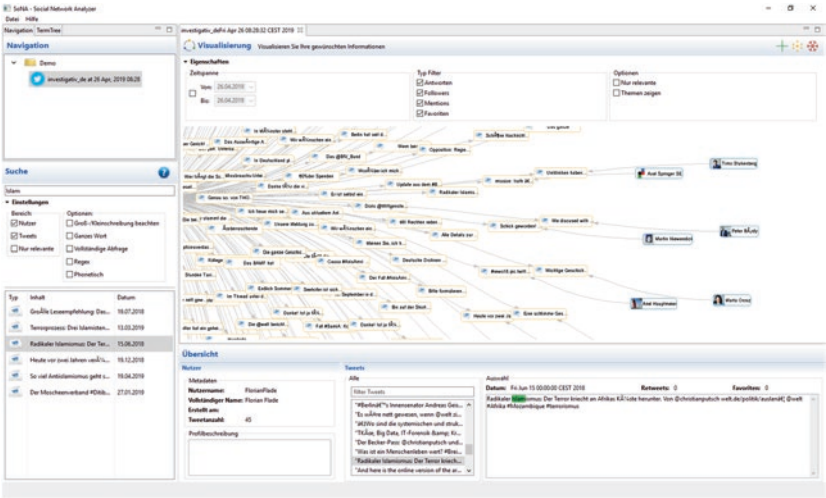


Abb. 5 Die graphische Nutzerschnittstelle des entwickelten Prototyps eines Social Network Analyzers (SoNA) zur wissensbasierten Analyse sozialer Netzwerke als Werkzeug der präventiven Ermittlungsarbeit

relevanten Informationen in Abhängigkeit der Bedürfnisse des zuständigen Ermittlers. Dabei können Daten von spezifischen Teilen des Netzwerks über zu bestimmende Zeiträume oder eine festzulegende Menge abgerufen werden, bevor sie im Model Repository abgelegt werden. Die so erzeugten Modelle können dann annotiert und zielführend analysiert werden. Aufgrund aktueller datenschutzrechtlicher Bestimmungen ist der Abruf von Informationen nichtöffentlicher Profile nicht möglich. Für die Bewertung des Gruppenverhaltens ist eine Analyse von nichtöffentlichen Profilen nicht erforderlich.

4 Predictive Policing

Die nachfolgenden Ausführungen entstammen, sofern nicht anders gekennzeichnet, einem Aufsatz eines der Autoren (Labudde 2018). Wie bereits eingangs erwähnt, bedeutet Predictive Policing „vorausschauende Polizeiarbeit“ und zielt auf die Verwendung mathematischer Modelle zur Vorhersage und Abschätzung von Kriminalitätsrisiken, -mustern und -trends ab, um durch Ergreifung operativer Maßnahmen, wie das Erhöhen der polizeilichen Präsenz in einem bestimmten

Gebiet, geeignet auf diese zu reagieren (Labudde). Aktuell werden in Deutschland durch die Strafverfolgungsbehörden der unterschiedlichen Länder verschiedene Systeme getestet. So versuchen einige Länder beispielsweise mit dem PreCrime Observation System (Precobs) mittels geeigneter Vorhersagen Wohnungseinbrüche zu effektiver zu bekämpfen bzw. verhindern. Voraussetzung für derartige Prognosen ist das Vorliegen historischer Daten in Form von Ergebnissen langjähriger Beobachtungen für ein bestimmtes Gebiet (Grünwald 2017).

Neben diesen technischen Beschränkungen unterliegt jede aktuell in diesem Zusammenhang verfügbare Technik und die damit verbundene Technologie weiteren Grenzen vor allem gesellschaftspolitischer Natur. In der wissenschaftlichen Literatur wird bereits seit längerem kontrovers über die Potenziale und Grenzen des Einsatzes von Predictive Policing in den USA und anderen englischsprachigen Ländern diskutiert (vgl. u. a. Perry et al. 2013, S. 115; Hunt et al. 2014, S. 7 f.; Nix 2015, S. 275 f.; Benbouzid 2015, S. 53 f.; Aradau und Blanke 2016; Polansky und Fradella 2016, S. 40 f.; Ferguson 2012, S. 261 f.; Ferguson 2017). Fachgebiete wie Politik-, Rechts- und Polizeiwissenschaften, Kriminologie, (Kriminal-) Soziologie oder auch Geographie liefern Beiträge zu diesem Diskurs. In der Bundesrepublik ist demgegenüber die wissenschaftliche Debatte noch recht übersichtlich (vgl. Gluba 2014, 2016; Hedelt 2016, S. 166 f.; Merz 2016; Belina 2009). Dabei gehen erste Ansätze bereits auf das 18. Jahrhundert zurück (Abb. 6).

In Gitternetzen, welche sich über eine Region erstrecken, wurde die Anzahl der Verbrechen eingezeichnet. In der heutigen Zeit werden computergestützte Ansätze verwendet. Ziel dieser Werkzeuge ist die Kennzeichnung von sogenannten Hotspots, d. h. Gebiete mit einer erhöhten Kriminalitätsrate. Erst in der letzten Dekade kamen Wahrscheinlichkeitsmodelle bzw. Ausbreitungsmodelle, analog zu Ansätzen aus der Epidemiologie, hinzu. Die Epidemiologie (von griech. epidḗmios „im ganzen Volk, über das ganze Volk verbreitet“ und lógos „Lehre“; Pfeifer 2005) ist eine *„Wissenschaft von der Entstehung, Verbreitung, Bekämpfung und den sozialen Folgen von Epidemien, zeittypischen Massenerkrankungen und Zivilisationsschäden“* (Duden 2019). Das epidemiologische Verhalten der meisten Infektionskrankheiten kann mittels mathematischer Modellierungen nicht nur untersucht, sondern auch prognostiziert werden. Solche mathematischen Ansätze und Modelle wurden auf das Gebiet des „Predictive Policing“ in urbanen Räumen übertragen.

In der Verbrechenssoziologie wird seit den 1970er Jahren von der „Repeat Victimisation“ (Grove und Farrell 2012) gesprochen, die sich Vorhersagesoftware zunutze macht (Farrell und Sousa 2010). Gemeint ist die Annahme, dass

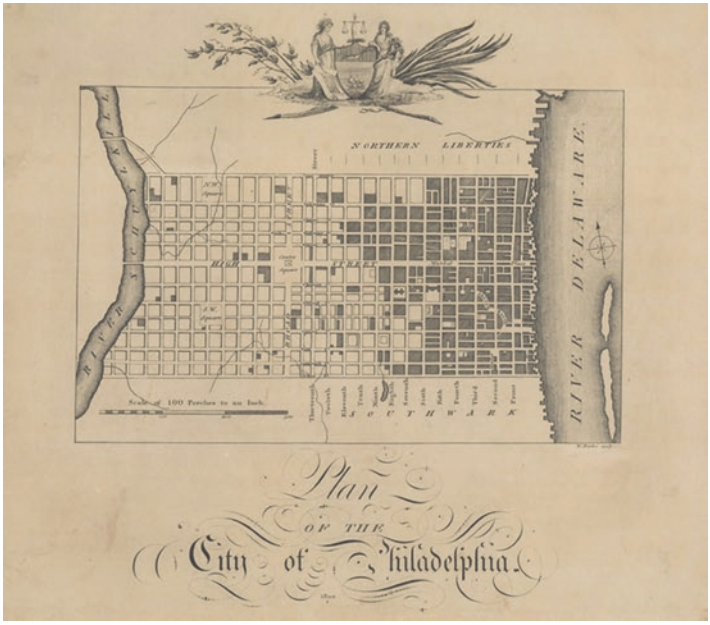


Abb. 6 Erste Ansätze der Kriminalstatistik. Städte wurden in Quadranten eingeteilt und die Anzahl der Verbrechen visualisiert (Foster 2004)

Orte oder Personen mehrfach aufgesucht („viktimisiert“) werden. Ergänzt wird diese Hypothese durch die Near-Repeat-Hypothese, welche die Erhöhung der Auftretenswahrscheinlichkeit von Straftaten vor allem in die Gebiete verlegt, in denen vorher ähnliche Straftaten verübt wurden (Townsley et al. 2003). Solche „Re-Viktimisierungen“ finden üblicherweise sehr bald nach den vorherigen Ereignissen statt (meist bis 48 h danach) (Johnson 2008a). Dieser Zusammenhang lässt sich in einen Algorithmus überführen und anwenden. Der besonders häufig geführte Nachweis der Near-Repeat-Hypothese für Wohnungseinbrüche (Gluba 2014) erklärt möglicherweise die Fokussierung deutscher Strafverfolgungsbehörden auf den Test des Einsatzes prädiktiver Softwarelösungen für diesen Deliktsbereich. Allerdings wurde die Hypothese in den USA auch in Zusammenhang mit Feuergefechten (Wells et al. 2011), KFZ-Diebstahl oder Raub (Youstin et al. 2011) gebracht. An dieser Stelle sei jedoch auf die unterschiedliche Datenlage in den USA und Deutschland in Bezug auf Kriminalitätsraten in den unter-

schiedlichen Deliktsbereichen hingewiesen, welche eine direkte Überführung auf Deutschland verhindert bzw. nur bedingt möglich macht.

Eine weitere theoretische Grundlage ist die *Routine Activity Theorie* (Cohen und Felson 1979), die regelmäßige Tätigkeiten untersucht und einbezieht. Zu diesen Routineaktivitäten gehört u. a. das Ausgehen am Wochenende, der Besuch von Großveranstaltungen oder das Pendeln zur Arbeit. Computergestützte Ansätze machen sich dies zunutze, indem Daten von Großveranstaltungen oder Verkehrsdaten eingebunden werden (Gluba 2014).

In einer ähnlichen Herangehensweise wird ein *Lifestyle Approach* (Hindelang et al. 1978) zur Zuschreibung eines Opferrisikos in Abhängigkeit bestimmter Einflussfaktoren des Lebensstils wie Alter, Geschlecht, Einkommen, Familienstand oder Bildung angenommen. So kann etwa berücksichtigt werden, in welchen Gegenden Menschen mit hohem Einkommen oder wenig Bildung leben, was dann Rückschlüsse auf bevorstehende Straftaten erlauben kann (Schurink 1992; Gluba 2014).

Insbesondere im urbanen Raum könnte durch Predictive Policing eine ökonomische Effizienzsteigerung der Polizeiarbeit erfolgen. Durch die stetig wachsende Datengrundlage in Folge moderner Technologien, könnte diese Technik in den nächsten Jahren immer bedeutsamer werden. Dabei werden die Methoden zur Vorhersage bereits in anderen Branchen eingesetzt, so zum Beispiel in der Marktforschung. Beispielsweise können Verbindungen zwischen dem Kauf gewisser Artikel und bevorstehenden Wetterereignissen gezogen werden. Die amerikanische Supermarktkette Wal-Mart stellte dabei fest, dass Kunden vor angekündigten schlechten Wetterereignissen gehäuft Wasserflaschen, Klebeband und Erdbeerkuchen kaufen. Die Verbindung der ersten beiden Artikel zu schlechten Wetterereignissen ist offensichtlich, die des Erdbeerkuchens jedoch nicht. Dennoch kann mit Hilfe von statistischen Analysen eine derartige Verbindung aufgedeckt werden. In gleicher Art und Weise können Verbindungen zwischen kriminalistisch relevanten Ereignissen durch die Techniken des Predictive Policing abgeleitet werden. Durch die Untersuchung und Auswertung vergangener Ereignisse in lokaler Umgebung können zukünftige Verbrechen mit einer gewissen Konfidenz vorhergesagt werden (Beck und McCue 2009; Gluba 2014).

Vor allem durch das Aufkommen der Massendaten und neuartiger Auswertemethoden im Bereich Big Data hat Predictive Policing an Diskussionspotenzial in den letzten Jahren gewonnen. Eine im Jahr 2008 veröffentlichte Studie bedient sich der Analyse wiederkehrender lokaler Muster, um das Auftreten von Schießereien in Philadelphia, USA vorherzusagen (Ratcliffe und Rengert 2008). Durch die Anwendung räumlich-zeitlicher Clusteringmethoden konnte gezeigt werden, dass das Auftreten einer erneuten Schießerei innerhalb von zwei Wochen

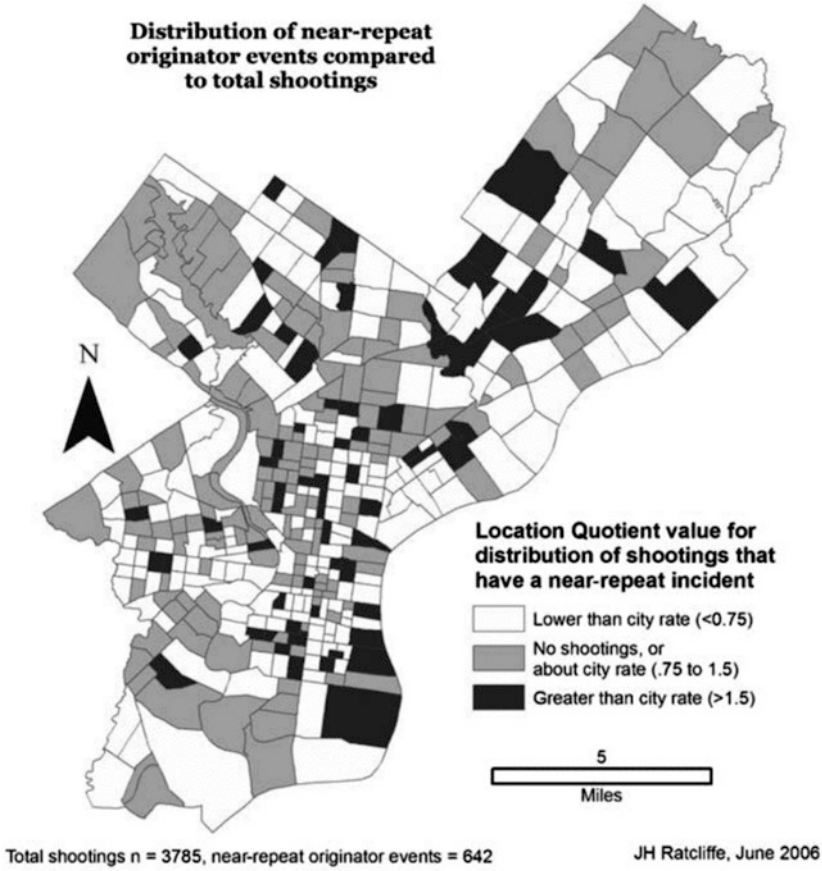


Abb. 7 Die Vorhersage des Auftretens von Schießereien im räumlich-zeitlichen Umfeld von Philadelphia, USA (Ratcliffe und Rengert 2008)

und maximal einen Bezirk entfernt um 33 % erhöht ist (Abb. 7). Auch wenn der Deliktbereich Schießereien in Deutschland kein Massendelikt ist, soll dieses Beispiel die Kombination von verschiedenen Auswertemethoden hervorheben.

Vor allem in Bezug auf die Wiederholung von Straftaten kann Predictive Policing einen wertvollen Beitrag leisten. Eine Untersuchung aus dem Jahr 2012 analysierte das Auftreten von Einbruchserien. Hierbei wurde gezeigt, dass zwischen Beginn und Ende der Serie selten mehr als sieben Tage liegen (Haberman und

Ratcliffe 2012). Auch der organisatorische Umfang der präventiven Bekämpfung derartiger Delikte kann durch den Einsatz von Predictive Policing besser abgeschätzt werden. Dies erweist sich jedoch als besonders anspruchsvoll, wenn wie im Beispiel von kurz andauernden Einbruchserien schnelles Eingreifen und Flexibilität in der Organisationsstruktur notwendig sind. Hier sei auch noch mal auf die Unterschiede zwischen USA und Deutschland hingewiesen.

Generell sind die Aussichten des Vorhersagens von sogenannten Kriminalitäts-Hot-Spots vielversprechend. Insbesondere das Verwenden von aufgezeichneten Daten zur Bildung einer Hot-Spot-Karte führt zu erfolgreichen Vorhersagen von Kriminalitätsschwerpunkten (Bowers et al. 2004).

Die Anwendung auf urbane Systeme ist Gegenstand aktueller Forschung (Groff 2007). Dies beruht häufig auf der Annahme, dass Straftaten sich räumlich als auch zeitlich zuordnen lassen. Dennoch existieren zwei Grundannahmen. Zum einen besagt die sogenannte Boost-Theorie, dass durch einen Einbruch betroffene Häuser zukünftig noch weitere Straftäter anziehen, die die guten Gelegenheiten weiter ausnutzen wollen (z. B. nach dem ersten Einbruch ersetzte oder zurückgelassene Gegenstände). Konträr dazu besagt die Flagged-Theorie, dass mehrere Einbrüche das Risiko für die Straftäter erhöhen: die attraktiven Ziele sind bereits polizeibekannt oder markiert (flagged) (Johnson 2008b).

Auch die Vorhersage des am wahrscheinlich nächsten räumlichen Ballungszentrums (Clusters) einer Verbrechensserie ist ein wichtiger Indikator, der für die Analyse herangezogen werden sollte. Auch wenn die konkrete Lokalisierung zukünftiger Cluster schwierig erscheint, zeigen sich gewisse Muster, die ein „Gleiten“ in nahe Stadtgebiete widerspiegeln (Johnson und Bowers 2004). Die Integration taggenauer Informationen in die Vorhersage von Kriminalitäts-Hot-Spots erhöht die Chancen engere Zeitfenster angeben zu können, in denen ein Verbrechen wahrscheinlich stattfinden wird. Damit können vorhandene Ressourcen und Polizeikräfte effizienter und intelligenter verteilt werden (Tompson und Townsley 2010). Bereits existierende Studien haben gezeigt, dass die Vorhersage von Verbrechensschauplätzen an Genauigkeit gewinnt, sobald größere Datengrundlagen betrachtet werden. Am Beispiel von Seattle, USA, wurden Daten von 14 Jahren einbezogen, um den generellen Trend und die Verschiebung von Kriminalitäts-Hot-Spots zu untersuchen (Weisburd und Lum 2005).

Wie bereits erwähnt lässt sich die Analyse und damit verbunden die Vorhersage von räumlichen und zeitlichen Kriminalitätsmustern wesentlich verbessern, indem zusätzliche Informationen, welche beispielsweise mit Hilfe von Textminingtechnologien aus sozialen Medien gewonnen wurden, lernenden Systemen als externes Wissen zur Verfügung gestellt werden (Rolfes 2017).

5 Predictive Policing im Zeitalter der Sozialen Medien

Im Zeitalter sozialer Medien hinterlässt jeder Nutzer, bewusst oder unbewusst, eine Menge persönlicher Daten in Form von Text, Bild, Audio etc., die auch als sein digitaler Fußabdruck bezeichnet werden (vgl. Abschn. 1). Die Heterogenität und schiere Menge dieser Daten stellen in Ermittlungsverfahren, wenn es darum geht fallrelevante Informationen zu extrahieren, eine große Herausforderung dar. Auf der anderen Seite stellt dieses häufig mit dem Begriff „Big Data“[5] gleichgesetzte Phänomen einen Datenpool für Methoden des maschinellen Lernens und der künstlichen Intelligenz bereit und ermöglicht so die Entwicklung und Anwendung von Vorhersagealgorithmen (Predictive Policing) (Labudde und Spranger 2017).

So kann beispielsweise das Kommunikationsverhalten als Teil des digitalen Fußabdruckes eines Nutzers bzw. einer Gruppe von Nutzern mit modernen Methoden des Text Mining analysiert werden. Gerade Meinungen und Standpunkte Einzelner oder Untergruppen sind im Kontext der Betrachtung gruppendynamischer Prozesse, dem damit verbundenen Wachstum (Bedeutung) und der gesellschaftspolitischen Ausrichtung der virtuellen Gruppe im Rahmen des Predictive Policing von prominenter Bedeutung.

Hier können beispielsweise mithilfe der Sentimentanalyse (Opinion Mining) Informationen zu Meinungen, Gefühlen, Bewertungen, Einschätzungen, Einstellungen und Emotionen gegenüber unterschiedlichen Entitäten, in diesem Kontext, insbesondere Personen, Organisationen, Religionsgruppen und Minderheiten, untersucht werden (Liu 2012). In einen zeitlichen Kontext gebracht, können so Trends analysiert und in Verbindung mit der Extraktion weiterer Informationen (Orte, Zeiten, Ereignisse mit potenziell gefährdendem Charakter) vorhergesagt werden. Ansätze für derartige Verfahren wurden durch die Autoren in Spranger et al. (2015, 2017a, b) vorgestellt.

Abb. 8 zeigt den grundsätzlichen Aufbau des durch die Autoren vorgestellten Systems eines Analysewerkzeugs für soziale Netzwerke welches Entscheidern von Strafverfolgungsbehörden Vorhersagen über lang- und kurzfristige Gruppendynamiken liefert. Zentrales Element ist hier eine durch Experten entwickelte Wissensbasis mit semantischen Informationen zu abstrakten

[5]Big Data umfasst üblicherweise neben den hier genannten Dimensionen Menge und Heterogenität weitere, wie die Geschwindigkeit der Änderung der Daten, deren Unsicherheit oder Verkehrswert.

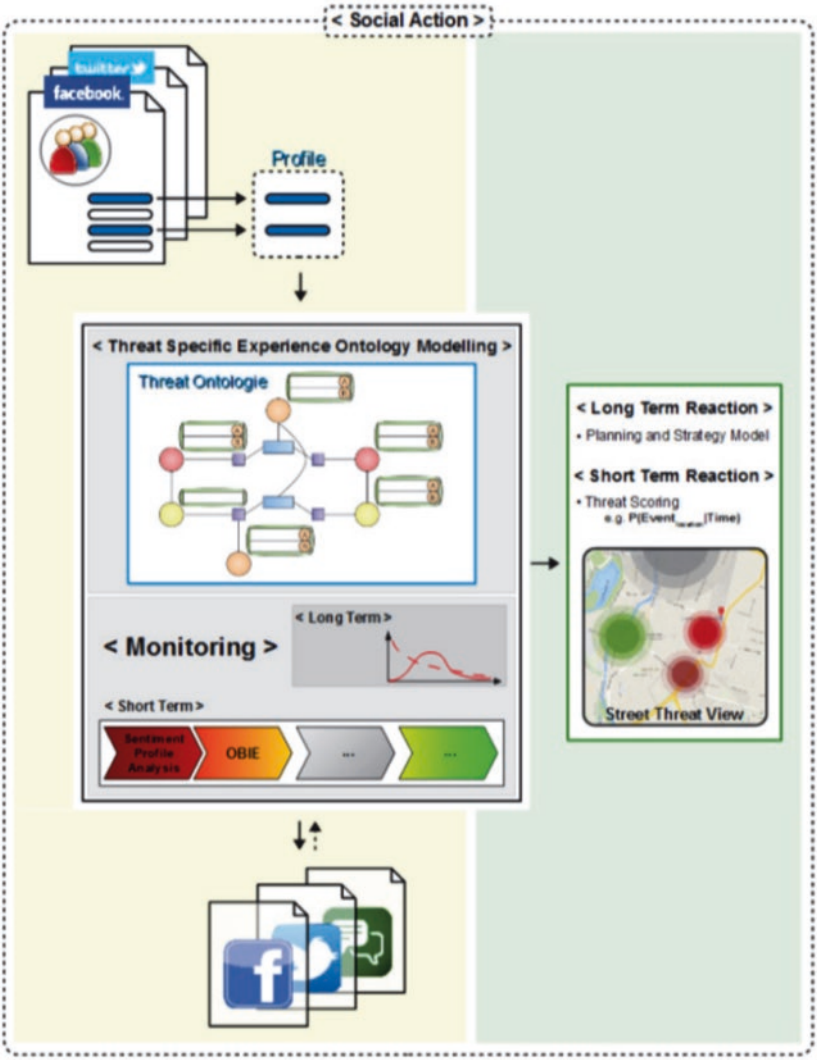


Abb. 8 Schematische Darstellung eines Frameworks zur Analyse sozialer Netzwerke im Sinne eines Predictive Policing (Spranger et al. 2015)

Bedrohungsszenarien/Gefahrenlagen. Aus Gruppen, deren Mitglieder an einer Diskussion teilnehmen, die inhaltliche Überschneidungen mit derartigen Bedrohungsszenarien aufweist und von denen zumindest einige Nutzer ein Profil besitzen, welches sie einem legal definierten Kreis von Gefährdern zuordnet, werden digitale Daten analysiert und Informationen zur konkreten Bedrohung extrahiert. Verschiedene Scoring-Funktionen ermöglichen die Identifizierung von Bedrohungs-Hot-Spots oder können für die Ableitung langfristiger Entwicklungen von Gruppen und Cliquen genutzt werden. Mithilfe der Wissensbasis werden die extrahierten Informationen strukturiert und mit den Ergebnissen der Sentimentanalyse verknüpft. Eine Automatisierung dieser Prozesskette erfordert im Einzelnen die Implementierung der folgenden Arbeitsschritte:

- Erstellung einer bedrohungsbezogenen semantischen Wissensbasis
- Extraktion von Kommunikationsinhalten (Posts/Kommentare) und Metadaten
- Detektion der Themenschwerpunkte und Abgleich mit der Wissensbasis
- Bewertung des Sentiments und Verknüpfung mit extrahiertem Wissen
- Detektion von kurzfristig geplanten Aktionen und deren raumzeitliche Verortung
- Simulation der langfristigen Entwicklung von Gruppen und Hotspots

Mit SoNA (Social Network Analyzer) stellten die Autoren den Prototyp einer computergestützten Analyse von Gruppen in sozialen Netzwerken vor (Spranger et al. 2017a). Die Software ermöglicht die Analyse offener Facebookgruppen, Twitter- und Telegramnetzwerke. Bei der stichprobenhaften Auswertung unterschiedlicher Netzwerke konnten retrospektiv Zusammenhänge zwischen dem Anwachsen an negativen Kommentaren und Posts und realen Ereignissen beobachtet werden (siehe Abb. 9), welche es nahe legen, dass eine Vorhersage potenziell gefährdender Ereignisse auf Basis historischer Daten tatsächlich möglich ist.

Dabei wurden ausschließlich negative Posts und Kommentare einer offenen Facebookgruppe über einen Zeitraum von 22 Tagen berücksichtigt. Man erkennt deutlich ein Anwachsen der negativen Stimmung bis ein lokales Maximum erreicht wird. Nach einer kurzen Plateauphase auf hohem Niveau kommt es zum drastischen Einbruch der Kommunikation. Dieser Einbruch lässt sich, unter Berücksichtigung des Kommunikationsinhalts, mit einem realen Ereignis (Krawalle, Zerstörungen, Randale, Schlägereien) in einen Zusammenhang bringen. Dabei diente die Plateauphase der Ereignisplanung und der plötzliche Kommunikationszusammenbruch korrelierte mit der Stimmungsentladung in der realen Welt. Das Ergebnis zeigt, dass die beschriebenen Verfahren Hinweise auf

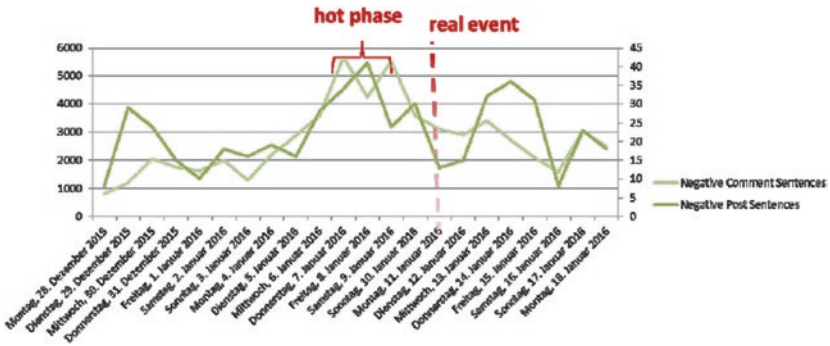


Abb. 9 Ergebnisse einer Sentiment-Analyse einer offenen Facebook-Gruppe mit extremistischen Tendenzen

die Planung von Straftaten im Sinne eines Predictive Policing liefern können, welche im virtuellen Raum geplant ihre Verwirklichung in der realen Welt finden.

6 Ausblick und Diskussion

In diesem Beitrag wurden Möglichkeiten der Analyse von Kommunikation und Dynamik virtueller Gruppen als Grundlage der Verbesserung der raumzeitlichen Vorhersage von Ereignissen als Werkzeug der vorausschauenden Polizeiarbeit diskutiert.

Techniken und Technologien des Predictive Policing versuchen mithilfe der Informationen aus sozialen Netzwerken und digitalen Daten von Nutzern, die Wahrscheinlichkeit des räumlichen Auftretens von Kriminalität zu bestimmen oder mithilfe mathematischer und statistischer Methoden zu modellieren. Ein Verständnis des Verhaltens und der zeitlichen Veränderung der Dynamiken in virtuellen Gruppen mit hohem Gefährdungspotenzial kann wertvolle Hinweise auf zukünftige Straftaten liefern und in Kombination mit datenbasierten Erkenntnissen bezüglich Repeat Victimization und der Routine Activity Theorie könnte die Bestimmung von Auftrittswahrscheinlichkeiten von Straftaten signifikant verbessert werden.

Ein nicht zu unterschätzendes Risiko stellt zum gegenwärtigen Zeitpunkt die Qualität der erhobenen Daten dar. Die wissenschaftliche Arbeit sollte von Kriterien wie Vollständigkeit, Korrektheit, Verlässlichkeit, Genauigkeit und Aktualität

der verarbeiteten Daten und Informationen auch bei großen Datenmengen geleitet sein. Ist dies nicht der Fall besteht die Gefahr von fehlerhaften Daten und Scheinkorrelationen, was zu fehlender Signifikanz von Wahrscheinlichkeitsaussagen, Fehlinterpretationen und damit falschen Vorhersagen führen würde. Der Einsatz von Werkzeugen des Predictive Policing erfordert deshalb auch immer eine kritische Auseinandersetzung mit der verwendeten Methodik/Technologie und den zugrunde liegenden Daten. Voraussetzung für eine solche Reflexion ist jedoch ein methodisch-technisches Grundverständnis des mit der Auswertung betrauten Nutzers, über welches üblicherweise nur Fachexperten mit abgeschlossenen naturwissenschaftlich-technischem Hochschulstudium verfügen (Rolfes 2017).

Literatur

Amann, A. (2003). Vergemeinschaftungsmuster: Zugehörigkeit und Individualisierung im gruppendynamischen Raum. *Gruppenpsychotherapie und Gruppendynamik, 39,* 201–219.

Aradau, C., & Blanke, T. (2016). Politics of prediction. *European Journal of Social Theory, 20*(3), 373–391. https://doi.org/10.1177/1368431016667623.

Baumeister, R. F., & Leary, M. R. (1995). The need to belong: Desire for interpersonal attachments as a fundamental human motivation. *Psychological Bulletin, 117*(3), 497–529. https://doi.org/10.1037/0033-2909.117.3.497.

Beck, C., & McCue, C. (2009). Predictive policing: What can we learn from Wal-Mart and Amazon about fighting crime in a recession? *Police Chief, 76*(11), 18.

Belina, B. (2009). Kriminalitätskartierung – Produkt und Mittel neoliberalen Regierens, oder: Wenn falsche Abstraktionen durch die Macht der Karte praktisch wahr gemacht werden. *Geographische Zeitschrift, 97*(4), 192–212.

Benbouzid, B. (2015). From situational crime prevention to predictive policing. *Champ pénal, 12*. https://doi.org/10.4000/champpenal.9066.

Bohnsack, R., Loos, P., Schäffer, B., Städtler, K., & Wild, B. (1995). *Die Suche nach Gemeinsamkeit und die Gewalt der Gruppe: Hooligans, Musikgruppen und andere Jugendcliquen*. Wiesbaden: VS Verlag.

Bowers, K. J., Johnson, S. D., & Pease, K. (2004). Prospective hot-spotting: The future of crime mapping? *British Journal of Criminology, 44*(5), 641–658. https://doi.org/10.1093/bjc/azh036.

Büchel, M., & Hirsch, P. (2014). *Internetkriminalität: Phänomene – Ermittlungshilfen – Prävention*. Heidelberg: Kriminalistik Verl. Verl.-Gruppe Hüthig Jehle Rehm.

Bundeskriminalamt. (2018). Bundeslagebild Cybercrime 2017. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2017.html?nn=28110. Zugegriffen: 01. Oktober 2017.

Bundeskriminalamt. (2019). Polizeilich erfasste Fälle von Cyberkriminalität im engeren Sinne* in Deutschland von 2004 bis 2017. https://de.statista.com/statistik/daten/studie/295265/umfrage/polizeilich-erfasste-faelle-von-cyberkriminalitaet-im-engeren-sinne-in-deutschland/. Zugegriffen: 28. Mai 2019.

Coan, J. A., Schaefer, H. S., & Davidson, R. J. (2006). Lending a hand: Social regulation of the neural response to threat. *Psychological Science, 17*(12), 1032–1039. https://doi.org/10.1111/j.1467-9280.2006.01832.x.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588. https://doi.org/10.2307/2094589.

Cooley, C. H. (1909). *Social organization: A study of the larger mind*. New York: Scribner.

Döring, N. (2003). *Sozialpsychologie des Internet: Die Bedeutung des Internet für Kommunikationsprozesse, Identitäten, soziale Beziehungen und Gruppen* (2. Aufl.). Göttingen: Hogrefe.

Dorsch, F., Häcker, H., Stapf, K. H., & Becker-Carus, C. (Hrsg.). (1994). *Dorsch psychologisches Wörterbuch: 15000 Stichwörter, 800 Testnachweise* (12. Aufl.). Bern: Huber.

Duden. (2019). Epidemiologie. https://www.duden.de/node/41034/revision/41063. Zugegriffen: 5. Juni 2019.

Farrell, G., & Sousa, W. (2010). Repeat victimization and hot spots: The overlap and its implications for crime control and problem-oriented policing. In G. Farrell & K. Pease (Hrsg.), *Repeat victimization* (S. 221–240). Boulder: Lynne Reiner.

Ferguson, A. G. (2012). Predictive policing and reasonable suspicion. *Emory Law Journal, 62*(2), 259–325.

Ferguson, A. G. (2017). Policing predictive policing. *Washington University Law Review, 94*(5), 1109–1189.

Foster, A. K. (2004). *Moral visions and material ambitions: Philadelphia struggles to define the republic, 1776–1836*. Lanham: Lexington.

Gluba, A. (2014). Predictive Policing – eine Bestandsaufnahme; Historie, theoretische Grundlagen, Anwendungsgebiete und Wirkung. Landeskriminalamt Niedersachsen. https://netzpolitik.org/wp-upload/LKA_NRW_Predictive_Policing.pdf. Zugegriffen: 01. Oktober 2017.

Gluba, A. (2016). Mehr offene Fragen als Antworten: Was für eine Bewertung des Nutzens von Predictive Policing noch zu klären ist. *Die Polizei, 2,* 53–57.

Groff, E. R. (2007). ‚Situating' simulation to model human spatio-temporal interactions: Simulation to model human spatio-temporal interactions: An example using crime events. *Transactions in GIS, 11*(4), 507–530. https://doi.org/10.1111/j.1467-9671.2007.01058.x.

Grove, L., & Farrell, G. (2012). Once Bitten, twice shy: Repeat victimization and its prevention. In B. Welsh & D. P. Farrington (Hrsg.), *The Oxford handbook of crime prevention* (S. 404–422). New York: Oxford-Univ.-Pr.

Grünwald, C. (2017). „Predictive Policing" – ein erfolgversprechender Ansatz zur Verbrechensbekämpfung? https://www.datenschutz-notizen.de/predictive-policing-ein-erfolgversprechender-ansatz-zur-verbrechensbekaempfung-0817538/. Zugegriffen: 28. Mai 2019.

Haberman, C. P., & Ratcliffe, J. H. (2012). The predictive policing challenges of near repeat armed street robberies. *Policing: A Journal of Policy and Practice, 6*(2), 151–166. https://doi.org/10.1093/police/pas012.

Harring, M., Böhm-Kasper, O., Rohlfs, C., & Palentien, C. (2010). Peers als Bildungs- und Sozialisationsinstanzen – eine Einführung in die Thematik. In M. Harring, O. Böhm-Kasper, C. Rohlfs, & C. Palentien (Hrsg.), *Freundschaften, Cliquen und Jugendkulturen* (S. 9–19). Wiesbaden: VS Verlag.

Haug, C. V. (2016). *Erfolgreich im Team: Praxisnahe Anregungen für effizientes Teamcoaching und Projektarbeit* (5. Aufl.). München: dtv.

Hedelt, P. (2016). Big Data Crime Prevention – ein wissenschaftlich fundiertes Verfahren? *Die Polizei, 6,* 166–170.

Hess, U. (2018). *Allgemeine Psychologie II – Motivation und Emotion*. Stuttgart: Kohlhammer.

Heyer, G., Quasthoff, U., & Wittig, T. (2008). *Text mining: Wissensrohstoff Text: Konzepte, Algorithmen, Ergebnisse.* Herdecke: W3L-Verlag.

Hindelang, M. J., Gottfredson, M., & Garofalo, J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization*. Cambridge: Ballinger Publishing Company.

Hunt, P., Saunders, J. M., & Hollywood, J. S. (2014). *Evaluation of the Shreveport predictive policing experiment*. Santa Monica: RAND Corporation.

Johnson, S. (2008a). The near-repeat burglary phenomenon. In L. Tompson & S. Chainey (Hrsg.), *Crime mapping case studies: Practice and research* (S. 123–132). Chichester: Wiley.

Johnson, S. D. (2008b). Repeat burglary victimisation: A tale of two theories. *Journal of Experimental Criminology, 4*(3), 215–240. https://doi.org/10.1007/s11292-008-9055-3.

Johnson, S. D., & Bowers, K. J. (2004). Stability of space-time clusters of burglary. *British Journal of Criminology, 44*(1), 55–65.

König, O. (2012). Gruppendynamische Grundlagen. In Hrsg Gruppenpsychotherapie (Hrsg.), *Bernhard Strauß und Dankwart Mattke* (S. 21–36). Berlin: Springer.

König, O., & Schattenhofer, K. (2011). *Einführung in die Gruppendynamik* (5. Aufl.). Heidelberg: Carl-Auer.

Labudde, D. (2018). Sicherheit ist die Abwesenheit von Kriminalität – eine Hypothese: P(Sicherheit) = 1 – P(Kriminalität). In P. Winzer & J. Beyerer (Hrsg.), *Beiträge zu einer Systemtheorie Sicherheit (acatech DISKUSSION)* (S. 145–149). München: Herbert Utz Verlag.

Labudde, D., & Spranger, M. (Hrsg.). (2017). *Forensik in der digitalen Welt: Moderne Methoden der forensischen Fallarbeit in der digitalen und digitalisierten realen Welt*. Berlin: Springer Spektrum.

Liu, B. (2012). *Sentiment analysis and opinion mining*. San Rafael: Morgan & Claypool Publishers.

March, J. G. (1954). Group norms and the active minority. *American Sociological Review, 19*(6), 733–741. https://doi.org/10.2307/2087920.

Mayo, E. (1945). *The social problems of an industrial civilization*. Andover: Andover Press.

Merz, C. (2016). Predictive Policing; Polizeiliche Strafverfolgung in Zeiten von Big Data. http://www.abida.de/sites/default/files/Dossier_Predictive_Policing.pdf. Zugegriffen: 5 Juni 2019.

Neidhardt, F. (1999). Innere Prozesse und Außenweltbedingungen sozialer Gruppen. In B. Schäfers (Hrsg.), *Einführung in die Gruppensoziologie: Geschichte, Theorien, Analysen* (3. Aufl., S. 135–156). Wiesbaden: Quelle & Meyer.

Nix, J. (2015). Predictive policing. In R. G. Dunham & G. P. Alpert (Hrsg.) *Critical issues in policing: Contemporary readings* (S. 275–288). Long Grove: Waveland Press, Inc.

Pearsall, B. (2010). Predictive policing: The future of law enforcement? *National Institute of Justice Journal, 266,* 16–19.

Perry, W. L., McInnis, B., Price, C. C., Smith, S., & Hollywood, J. S. (2013). *Predictive policing: The role of crime forecasting in law enforcement operations*. Santa Monica: RAND.

Pfeifer, W. (2005). *Etymologisches Wörterbuch des Deutschen* (8. Aufl.). München: Deutscher Taschenbuch Verlag.

Polansky, J., & Fradella, H. (2016). Does ‚Precrime' mesh with the ideals of U.S. Justice? Implications for the future of predictive policing. *Cardozo Public Law, Policy and Ethics Journal, 15,* 253.

Proshansky, H., & Seidenberg, B. (Hrsg.). (1965). *Basic studies in social psychology.* New York: Holt, Rinehart and Winston.

Ratcliffe, J. H., & Rengert, G. F. (2008). Near-repeat patterns in Philadelphia shootings. *Security Journal, 21*(1–2), 58–76. https://doi.org/10.1057/palgrave.sj.8350068.

Rheingold, H. (1993). *The virtual community: Homesteading on the electronic frontier*. Reading: Addison-Wesley Publishing Company.

Rolfes, M. (2017). Predictive Policing: Beobachtungen und Reflexionen zur Einführung und Etablierung einer vorhersagenden Polizeiarbeit. In P. Jordan, F. Pietruska, & J. Siemer (Hrsg.), *Geoinformation & Visualisierung: Pionier und Wegbereiter eines neuen Verständnisses von Kartographie und Geoinformatik: Festschrift anlässlich der Emeritierung von Herrn Prof. Dr. Hartmut Asche im März 2017*. Potsdam: Universitätsverlag.

Schneider, H.-D. (1975). *Kleingruppenforschung*. Wiesbaden: Vieweg + Teubner.

Schurink, W. J. (1992). *Victimization: Nature and trends*. Pretoria: Human Sciences Research Council.

Spranger, M. (2019). *Text Mining als Werkzeug im repressiven und präventiven Ermittlungsprozess*. Dissertation, Technische Universität Dresden, Dresden.

Spranger, M., & Labudde, D. (2014). Towards establishing an expert system for forensic text analysis. *International Journal On Advances in Intelligent Systems, 7*(1, 2), 247–256.

Spranger, M., Heinke, F., Grunert, S., & Labudde, D. (2015). Towards predictive policing: Knowledge-based monitoring of social networks. In C. Ernst & A. Schmidt (Hrsg.), *IMMM 2015: The fifth international conference on advances in information mining and management: Datasets 2015, the international symposium on challenges for designing and using datasets: June 21–26, 2015, Brussels, Belgium* (S. 39–40). Wilmington: IARIA.

Spranger, M., Siewerts, H., Hampl, J., Heinke, F., & Labudde, D. (2017a). SoNA: A knowledge-based social network analysis framework for predictive policing. *International Journal On Advances in Intelligent Systems, 10*(3, 4), 147–156.

Spranger, M., Becker, S., Heinke, F., Siewerts, H., & Labudde, D. (2017b). The infiltration game: Artificial immune system for the exploitation of crime relevant information in social networks. In D. Labudde & J. L. Mauri (Hrsg.), *IMMM 2017: The seventh international conference on advances in information mining and management: Datasets 2017, the international symposium on challenges for designing and using datasets: June 25–29, 2017, Venice, Italy*, (S. 24–27). Wilmington: IARIA.

Sulzbacher, M. (2003). *Virtuelle Teams: Eine Möglichkeit, komplexe Aufgaben über Raum, Zeit und Organisationsgrenzen hinweg effektiv zu meistern?* Marburg: Tectum-Verlag.

Thiedeke, U. (2003). *Virtuelle Gruppen: Charakteristika und Problemdimensionen* (2. Aufl.). Wiesbaden: VS Verlag.

Tompson, L., & Townsley, M. (2010). (Looking) back to the future: Using space—time patterns to better predict the location of street crime. *International Journal of Police Science & Management, 12*(1), 23–40. https://doi.org/10.1350/ijps.2010.12.1.148.

Townsley, M., Homel, R., & Chaseling, J. (2003). Infectious burglaries: A test of the near repeat hypothesis. *The British Journal of Criminology, 43*(3), 615–633.

Weisburd, D., & Lum, C. (2005). The diffusion of computerized crime mapping in policing: Linking research and practice. *Police Practice and Research, 6*(5), 419–434. https://doi.org/10.1080/15614260500433004.

Wells, W., Ling, W., & Ye, X. (2011). Patterns of near-repeat gun assaults in Houston. *Journal of Research in Crime and Delinquency, 49*(2), 186–212. https://doi.org/10.1177/0022427810397946.

Youstin, T. J., Nobles, M. R., Ward, J. T., & Cook, C. L. (2011). Assessing the generalizability of the near repeat phenomenon. *Criminal Justice and Behavior, 38*(10), 1042–1063. https://doi.org/10.1177/0093854811417551.

GIS und Geoinformatik bei der Polizei

Chancen und Potenziale für Ermittlungen

Roman Povalej und Dirk Volkmann

1 Geografisches Informationssystem (GIS)

Mit einem GIS können raumbezogene Informationen mit Geopositionen verknüpft und schließlich systematisiert, organisiert, analysiert und präsentiert werden (Bill 2016, S. 8). GIS-Anwendungen werden unter anderem erfolgreich im Gesundheits- und Katastrophenmanagement, der Kriminologie und der Umweltforschung sowie zunehmend an Bedeutung im polizeilichen Einsatz- und Ermittlungsmanagement gewinnend (Bill 2016, S. 69 f.). Da im Grunde alle mobilen Digitalgeräte mit einem GPS[1]-Empfänger ausgestattet sind, gehört die Positionsbestimmung mittels Satellitenpositionierungssystemen quasi zur Standardfunktionalität (Bill 2016, S. 69 f.). Notwendige Korrekturen der GPS-Daten erfolgen in Deutschland mittlerweile in Echtzeit, ohne dass eine eigene Referenzstation abgerufen wird. So stellt z. B. der Satellitenpositionierungsdienst SAPOS der deutschen Landvermessung, die ein flächendeckendes Netz

[1]Global Positioning System (GPS) ist eines von mehreren satellitengestützten Messsystemen, die unter dem übergeordneten Begriff des Globalen Navigationssatellitensystem (GNSS) gefasst werden (Bill 2016, S. 69).

R. Povalej (✉)
Polizeiakademie Niedersachsen, Hann. Münden, Deutschland
E-Mail: roman.povalej@polizei.niedersachsen.de

D. Volkmann
Polizeiakademie Niedersachsen, Nienburg, Deutschland
E-Mail: dirk.volkmann@polizei.niedersachsen.de

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

T.-G. Rüdiger und P. S. Bayerl (Hrsg.), *Cyberkriminologie,*
https://doi.org/10.1007/978-3-658-28507-4_26

bestehend aus über 270 Referenzstationen haben, Korrekturdaten für GPS bereit (Bill 2016, S. 72).

Ein wesentliches Unterscheidungsmerkmal von Geodaten zu anderen Daten bzw. Informationen stellt ihr Raum- und Zeitbezug dar (Booch et al. 2006, S. 25 f.). Die räumliche (spitale) Dimension eines Objekts lässt sich in einen direkten Raumbezug (eindeutige Bestimmung der Position durch Koordinaten in einem Referenzkoordinatensystem, s. ISO 19111), als primäre Metrik bezeichnet, und in einen indirekten Raumbezug (Festlegung durch geografische Identifikatoren wie Adressen, s. ISO 19112), als sekundäre Metrik bezeichnet, einteilen (Bill 2016, S. 163, 174, 192; World Meteorological Organisation 2005).

Hingegen bezieht sich die zeitliche (temporale) Dimension meist nur auf eine Konstante Zeit, die ordinalskalar (relativ zueinander) oder intervallskalar (absolut) gemessen werden kann (Bill 2016, S. 197; World Meteorological Organisation 2005). Der Zeitbezug gewinnt immer mehr an Bedeutung und der Bedarf in der Geoinformatik nimmt stetig zu, insbesondere bei der Analyse von Veränderungen zwischen Alt- und Neudaten und bei der Generierung von Sensor- und Messnetzwerken (Bill 2016, S. 193).

Die grundlegende Voraussetzung für die Arbeit mit einem GIS stellt die direkte oder indirekte Generierung von Geodaten dar. Hierfür werden bei den Polizeien Gerätschaften wie Digitalisierbretter, Scanner, Bildsensoren, Vermessungs- und Dokumentationsgeräte für die Bewältigung spezifischer Aufgaben, wie zur Tatort- oder Unfallaufnahme oder bei größeren Schadensereignissen, bei denen entsprechende Geodaten erhoben werden, eingesetzt.

2 Möglichkeiten von GIS-Produkten

Mit GIS-Produkten ist die Zusammenstellung georeferenzierter Informationen unabhängig von ihrer Datengröße umsetzbar (Intergraph 2008, S. 1–17 f.). Entsprechend lassen sich Daten und daraus resultierende, auch themenbezogene Karten in 3D-Modelle umsetzen, sodass sich durch Mapping räumliche Muster als Entscheidungsoptionen darstellen lassen, die die Basis für einen effizienteren und effektiveren Analyse- und Lösungsansatz bilden können (Geosystems o. D.). Der Abgleich der Spurenlage am aktuellen Tatort ist mit anderen Ereignisorten hinsichtlich eines Modus Operandi reproduzierbar, sodass diese frühzeitige Selektion der Informationen mit gleichgelagerten Ereignissen die Grundlage für die weiterführenden Ermittlungen eröffnen kann. Beispielsweise ist der Echtzeitabgleich von biologischen oder technischen Formspuren als Ein- oder Abdruck umsetzbar (Geosystems o. D.).

Die 3D-Modellierung basiert auf den 2D-Betriebsdaten der topografischen Grundkarte mit der primären und sekundären Metrik, wodurch schematische oder realistische Szenerien mit einer 360°-Ansicht dargestellt werden können (ESRI 2019c). Mit dem Abschluss des TanDEM-X-Projektes steht erstmals ein globales Höhenmodell der Erde frei zur Verfügung, basierend auf einer stereoskopischen Zwillings-Satellitenvermessung der Erdoberfläche (Deutsches Zentrum für Luft- und Raumfahrt 2018). Spezielle Anwendungen lassen die detaillierte Zerlegung von Gebäuden hinsichtlich ihrer Außen- und Innenstrukturen zu, sodass z. B. Fassaden, Wände, Türen und mechanische Systeme angezeigt oder ausgeblendet werden können (Powell et al. 2018). Somit lassen sich gefährdete Objekte, wie Bank- und Geldinstitute oder Schulen, aus der 3D-Ansicht in einer 360°-Grad-Ansicht durch Zerlegung in die einzelnen Ebenen etagen- bzw. raumweise und ihre Raumaufteilungen inklusive der Inneneinrichtungen visualisiert darstellen (Powell et al. 2018).

Des Weiteren können gespeicherte 3D-georeferenzierte Tat- bzw. Unfallorte auf der Karte abgebildet werden. Sofern neben der Punktwolke auch eine Layer-Bearbeitung mit einem CAD-Tool erfolgt sein sollte, ist auch die Zerlegung der Layer hinsichtlich der Objekte in Ebenen möglich, die die Ermittlungsarbeit frühzeitig auf die tatrelevanten Spuren fokussiert möglich macht, sodass die permanente, visuelle Reproduzierbarkeit des Ereignisortes mit Realbezug die kriminalistische Fallanalyse immens vereinfachen kann.

Gängige GIS-Produkte wie ArcGIS bieten auch Sichtbarkeitsanalysen an (Nayak 2019a). Das ist ein Instrument zur Bestimmung der Metriken zweier Objekte, z. B. Gebäude, Begrünung und Freiflächen (Nayak 2019a). So kann jede Ansicht eines Raumes entsprechend quantifiziert in einem Rasterformat abgebildet werden (Nayak 2019a). Neben einzelnen Zimmern kann auch eine Sichtfensteranalyse vorgenommen werden, sodass das Sichtfeld von einem festen Aussichtspunkt zu dem betreffenden Objekt nachvollziehbar wird (Nayak 2019b). Grundsätzlich können bei der Sichtbarkeits-Projektion Dächer, Wände und Fenster für das Modell deaktiviert werden, um sich bei einem mehrstöckigen Gebäude eine etagenorientierte Darstellung erschließen zu können (Nayak 2019b). Die Modellierung erfolgt über die 3D-Kartendarstellung als Szene. Diese Analyse erlaubt auch eine tageszeit- bzw. -lichtabhängige Betrachtung (Nayak 2019b). Neben der Sichtbarkeitsanalyse besteht bei einer Vielzahl von GIS-Produkten die Möglichkeit der Bedrohungsanalyse, die bei der Planung von entsprechenden Szenarien (Geiselnahme, Terror, Umweltkatastrophe etc.) zur Ermittlung und Ausweisung von Sicherheitszonen mit Angabe der erforderlichen Entfernungen herangezogen werden kann (Powell et al. 2018). Die Analysemethoden sind insbesondere für den polizeilichen Einsatz von Spezialkräften von Interesse, weil sie eine effiziente und effektive Einsatzplanung ermöglichen.

Zudem lassen sich Luftkorridore für Multicopter- oder Drohneneinsätze über Rasteranalysen berechnen, um optimale Flugrouten vorzuplanen und im laufenden Betrieb unter Berücksichtigung von z. B. Freileitungen, weitere Hindernisse aus der Luft, Orte potenzieller menschlicher Interaktionen wie Schulen, kleine Flugzonen wie an Krankenhäusern und Flughäfen sowie Bereich starken Windes zu verarbeiten (Cappelli 2019).

Auch höhendifferenzierte Schrägansichten von Objekten (aufgenommen aus der Luft) können zusammengefügt und in entsprechenden Karten visualisiert werden, sodass sich einzigartige Perspektiven auf Fronten und Seiten von Gebäuden und Orten am Boden eröffnen, die z. B. zur polizeilichen präventiven oder repressiven Aufklärung eingesetzt werden können (ESRI 2019a). Die Luftbilder sind in Echtzeit einlesbar – beim G20-Gipfel 2017 entsprechend umgesetzt.

Auch die Umwandlung und Extraktion georeferenzierter Bilder in 3D-Karten ist mit Mapillary problemlos umsetzbar, sodass Straßenfotos, aufgenommen mit Mobiltelefonen oder Consumer-Kameras, in kürzester Zeit zusammengefügt, rekonstruiert und letztlich auf dem GIS-Produkt hochgeladen werden können (ESRI 2019a). Die von Google Street View verbreiteten Bilder auf Straßenebene sind eine weitere Form von Geodaten, die mit dem GIS-System auswertbar sind (ESRI 2019a).

Weiterhin erlauben gängige GIS-Produkte die Georeferenzierung aus visuellen Darstellungen von Informationen in Form von Panoramabildern oder von Light Detection and Ranging-(LIDAR)[2]-Daten, Laserabstands- und Geschwindigkeitsmessung (ESRI 2019a).

Auch ein Monitoring ist mit GIS-Produkten realisierbar (ESRI 2019b), sodass z. B. die Manipulation von vernetzten Einsatzfahrzeugen durch eine Cyber-Attacke zeitnah eine Warnmeldung generiert und entsprechende Maßnahmen zur Abwehr ergriffen oder die Suche nach vermissten insbesondere älteren, häufig dementen Personen, die im Rahmen der Hausnotrufdienstleistung zunehmend mit GPS-Trackern ausgestattet werden, im Ereignisfall in Echtzeit geortet werden können (ESRI 2019b). Auch das zunehmende Umweltmonitoring durch kommunale Träger, d. h. die Übersendung der relevanten Informationen in Echtzeit von der Überwachungs- an die Exekutivbehörde, führt mit einem solchen Instrument zu einer effektiveren und effizienteren polizeilichen Einsatzplanung hinsichtlich Vorbereitung und Umsetzung bei gleichzeitiger Erfolgskontrolle (ESRI 2019b).

[2]LIDAR bezeichnet eine Methode zur optischen Abstands- und Geschwindigkeitsmessung bzw. Fernmessung atmosphärischer Parameter (Könneker und Müller 1998).

3 Erhebung raumbezogener Daten bei der Polizei

Neben optoelektronischen Scannern, die ein Objekt punkt- und zeilenweise abtasten und in digitale Informationen wandeln (Baldenhofer o. D.), gewinnen mittlerweile auch biometrische Scanner weiter an Bedeutung (Bundesamt für Sicherheit in der Informationstechnik o. D., S. 1). Diese digitale Technik kommt zum Einsatz, wenn die Papillarleisten eines Fingers, Venenmuster der Handinnen-, Handrücken- oder Fingervenen mittels Infrarot-Kamera oder Finger- und Handabdrücke mittels Livescan-Printing (daktyloskopische ED-Behandlung) gescannt werden, um die zweifelsfreie Identifikation von Personen aus persönlichen, kommerziellen (unternehmerischen), Notfall- oder kriminellen Aspekten zu ermöglichen (Fingerprinting 2019).

Die 3D-Vermessungs- und Dokumentationsverfahren werden bei den Polizeien für die Tatort- und Unfallaufnahme eingesetzt und gehen dabei weit über eine schlichte Tatortaufnahme hinaus. Die generierten virtuellen Orte sind jederzeit verfügbar, virtuell betretbar und bieten viele Möglichkeiten für weiterführende Ermittlungen. Die für die 3D-Effekte eingesetzten Gerätschaften, wie Spiegelreflex-, Stereo-, Panoramabild-, Infrarotkamera, terrestrische oder handgeführte Laserscanner, Kombinationsgeräte aus Laserscannern und Kameratypen, sind vielfältig und werden anhand der Anwendungsgebiete eingeteilt. Während kamerabasierte Systemausstattungen mit photogrammetrischen, d. h. stereoskopischen Messverfahren oder Panoramamessverfahren arbeiten, basieren bei 3D-Lasercannern die Verfahren auf dem Prinzip der Impuls-Laufzeit-Messung, Phasendifferenzmessung und Triangulationsmessung (Bill 2016, S. 68).

Neben statischen Verfahrensweisen (Rotationsbewegung um 360° in horizontaler Richtung bei unterschiedlichen Öffnungswinkeln) gewinnen immer mehr dynamische Verfahren (wie Airborne Laserscanning mit unbemannten oder bemannten Fluggerät oder kinematisches terrestrisches Laserscanning mit Kfz oder Eisenbahn) an Bedeutung (abf diagnostics 2015; Qitterer o. D.; Tsuchiya 2007, S. 1498), um künftig auch großräumige linienhafte Strukturen erfassen zu können (Fritsch 2014, S. 4 f.).

In Abhängigkeit vom Delikt, dem Spurenaufkommen, des öffentlichen Interesses und der Zugänglichkeit des Tatortes werden verstärkt Laserscanner-Kombinationsgeräte eingesetzt, die mit einem 3D-Laserscanner und einem integrierten oder adaptiven digitalen Kamerasystem ausgestattet sind, um mittels Bildverarbeitungsalgorithmen eine 3D-Punktwolke koloriert für die

Erstellung eines Orthofotos[3/4] zu generieren bzw. das projizierte CAD-Modell texturiert abzubilden (Tsuchiya 2007, S. 1498).

Mittlerweile hält auch im Bereich der ED-Behandlung die Fertigung der personenbezogenen Bildaufnahmen mittels 3D-Kombinationsverfahren bestehend aus Laserscanner und Kamerasystem Einzug, sodass die 3D-Projektion im alltäglichen Arbeitsprozess immer mehr verwendet wird.

4 Stand bei der Polizei Niedersachsen[5]

Digitale Luftbildaufnahmen von einem Umwelttatort wurden mit einem Kamerasystem der Fa. GoPro von einem Hexacopter[6] gefertigt und versuchsweise in einer Analysestelle ohne Georeferenzierung stereoskopisch ausgewertet, d. h. der generierte 3D-Effekt eröffnete die volumetrische Berechnung des Umweltschadens, z. B. Abraumhalde (Agioft 2019). Stereoskopische Auswertungen von Unfall- bzw. Tatorten sind seit einigen Jahren mit einer Spiegelreflexkamera, hochauflösend und kalibriert ohne Geodatenerhebung, realisiert worden. Mit den erzeugten Bilddaten wurden präzise Entfernungsmessungen und detaillierte 2D- bzw. 3D-Dokumentation komplexer Objekte ermöglicht und mit dem Auswertesystem PHIDIAS (Fa. Bentley Systems) weiterbearbeitet (Schwermann und Effkemann o. D.).

Aktuell befindet sich ein Kamerasystem in der Pilotierungsphase (piXplorer 500, Fa. Clauss Rodeon), das grundsätzlich 406 Einzelbilder bei einer 360° Rotation automatisch verrechnet und an einem Peripheriegerät mittels herstellerspezifischer Software (R2S Forensic, Fa. abf diagnostics GmbH) ein Panoramabild erzeugt (abf diagnostics 2017, S. 6). Seit einiger Zeit setzt die Polizei Niedersachsen für die Tatort- und Unfallaufnahme auch ein 3D-Laserscanner-Kombinationssystem vom Typ Z&F IMAGER 5010C (Fa. Zoller &

[3]Ein Orthofoto ist eine verzerrungsfreie, maßstabsgetreue Abbildung der Erdoberfläche, die durch photogrammetrische Verfahren aus Luft- oder Satellitenbildern abgeleitet werden (Bartelme 2005, S. 134 f.; Bill 2016, S. 104).

[4]Gescannte oder direkt digital referenzierte Bilder werden mittels digitaler Auswertegeräte bzw. -systeme zur Beseitigung von projektiven Verzerrungen eingesetzt und zur Erzeugung eines Orthofotos verwendet (Bill 2016, S. 104).

[5]Die GIS-Sachstandsanalyse bezieht sich hier weitestgehend auf das Bundesland Niedersachen, da die Autoren Angehörige der Polizeiakademie Niedersachsen sind.

[6]Hexacopter – unbemanntes Fluggerät (Multicopter) mit sechs Antriebsaggregaten (Rotoren).

Fröhlich) ein, ausgestattet mit einer integrierten Kamera mit HDR-Technologie im Rotor (Zoller & Fröhlich 2018). Dieses Gerät besitzt in der horizontalen Richtung ein Sichtfeld von ca. 360° und in der vertikalen Richtung von etwa 320° (Zöller & Fröhlich 2018). Mit diesem Gerät können Farb- mit hochaufgelösten Laserscandaten kombiniert werden. Die direkte Georeferenzierung ist aufgrund herstellerspezifischer Besonderheiten derzeit nicht umsetzbar.

Bei der Suche in fließenden oder stehenden Gewässern nach vermissten Personen oder Gegenständen wird häufig ein Sonar-Gerät an einem schwimmenden Träger oder Fahrzeug als sogenannter Fisch über einen Arm montiert eingesetzt und im Gewässer unterhalb der Wasserlinie fortbewegt wird. Die gewonnenen Daten werden georeferenziert abgebildet, sodass eine primäre Fundortbestimmung über Geo-Daten möglich ist. Zudem sind Fahrzeuge neuerer Bauart sowie die Funkgeräte mit GPS-Sendern ausgestattet, sodass Geo-Position im Einsatzfall von der Leitstelle abgerufen werden kann. Die Ausweisung der Geo-Koordinaten erfolgt systembedingt in der GPS-Projektion; allerdings werden diese Informationen in Abhängigkeit von der Schwere des Deliktes für die Vorgangsbearbeitung generiert, z. B. bei Tötungsdelikten oder Delikten gegen die sexuelle Selbstbestimmung.

4.1 Vorgangsbearbeitungssystem (VBS) – NIVADIS

Seit 2004 wird bei der Polizei Niedersachsen für die Vorgangsbearbeitung das Niedersächsische Vorgangsbearbeitungs-, Analyse-, Dokumentations- und Informations-System (NIVADIS) verwendet (Niedersächsische Landesregierung 2012, S. 2). Die Erfassung sekundär metrischer Informationen (Adressencode: Postleitzahl, Ort, Straßenname, etc.) im VBS erfolgt über Kataloghilfen. Der Koordinatenbezug der Geodaten sieht optional eine Selektion zwischen GPS- (Grad, Minuten, Sekunden) und universalen transverbalen Mercator (UTM[7])-Koordinaten[8] (Hier: Rechts- und Hochwert) vor, wobei die UTM-Werte mit realem Koordinatenreferenzbezug ausgewiesen werden.

[7]Die universelle transversale Mercatorprojektion basiert auf einem Ellipsoiden, dem eine transversale Zylinderprojektion zugrunde liegt (Kappas 2001, S. 19 ff.).

[8]Universal Transversale Mercator (UTM) – Koordinatenprojektion basiert auf dem Modell eines Erdellipsoids n. Hayford (transversale Zylinderprojektion) mit einer Streifenbreite von 6° und einer längentreuen Schnittkurvenabbildung (Bartelme, 2005, S. 218). Die Zählung der Streifen beginnt beim Mittelmeridian 177° westlicher Breite (Bill 2016, S. 186).

Die Georeferenzierung wird im VBS bei strafrechtlichen Sachverhalten mit dem Anlegen des Grundvorganges und der damit verbundenen Eingabe der postalischen Daten als Pflichtfelder automatisch vorgenommen. Sofern der Adressencode eindeutig definiert ist, werden die Geodaten auf die Hausnummer referenziert entsprechend angegeben. Sollte allerdings kein exakt normierter Adressencode (Wald-, Feld- oder Wiesengrundstück bzw. Gewässer) vorhanden sein, weist das VBS einen Geodatenbezug aus, der im Einzelfall vom tatsächlichen Referenzpunkt auch sehr stark abweichen kann. Darüber hinaus besteht bei nicht strafrechtlichen Sachverhaltsbezügen keine direkte Georeferenzierung der Daten, sodass diese manuell vorgenommen werden müsste.

Unterschiede zeigen sich auch in der Abbildung der Koordinatenbezüge beider Vorgangsarten. Liegt eine Straftat vor, werden UTM-Koordinaten mit Nachkommastellen generiert, wohingegen bei einem nicht strafrechtlich relevanten Ereignis die UTM-Koordinaten ohne Kommastellen generiert werden. Somit weichen diese beiden Koordinatenbezüge für ein identisches Objekt voneinander ab. Wenn die Adressatencodes nicht exakt definiert sind, ergeben sich z. B. unterschiedliche UTM-Werte in den Katalogfeldern Gewässer und Tatort.

Die Visualisierung der georeferenzierten Daten erfolgt im VBS unabhängig von der Maßstabswahl über eine thematisch-kartographische Projektion mit der Prämisse auf der Ausweisung der sekundären metrischen Daten unter Abbildung des realen Gebäudebestands. Die primären metrischen Daten werden in Abhängigkeit vom Ereignis entsprechend optional zugewiesen. Eine 3D-Projektion der Geodaten ist im VBS NIVADIS nicht möglich.

4.2 Fallbearbeitungssystem (FBS) – SAFIR

Neben NIVADIS nutzt die Polizei Niedersachsen seit 2009 als Fallbearbeitungssystem (FBS) die Software zur Analyse, Fallbearbeitung, Informationsverarbeitung und Recherche, kurz SAFIR, basierend auf einem Softwareprodukt (RSCase) der Fa. Rola, das die Bearbeitung von Umfangsverfahren bzw. Verfahren mit umfangreichen Datenaufkommen mit Bezug zu komplexen Kriminalitätsphänomenen, wie Wirtschaftskriminalität, organisierte oder politisch motivierte Kriminalität (Niedersächsische Landesregierung 2012, S. 2) unterstützt. Das FBS gewährleistet einen standardisierten Daten-Import und -Export, sodass komplexe Dateigrößen und Datei-Formate in digitaler audiovisueller, visualisierter oder animierter Projektion, z. B. Luftbilder, Audio- CAD-Dateien, problemlos transferiert und fallspezifisch analysiert werden können.

Die Georeferenzierung der Informationen erfolgt im FBS SAFIR mit integrierten grafischen Softwarepaketen, wie Analyst's Notebook, um Erkenntnisse und Zusammenhänge visualisiert darstellen zu können. Allerdings basiert die Generierung der Geoinformationen auf dem VBS-Datenbestand, sodass auch in der FBS die sekundäre Metrik in der Verwaltung der relationalen Datenbank favorisiert wird. Unter Verwendung dieser Analysetools kann ein Bezug zur primären Metrik (Geo-Koordinaten) hergestellt werden, der eine 2D- bzw. 2,5D-Präsentation ermöglicht. Eine automatische Zuweisung der primären Geodaten erfolgt mit der Dateneingabe nicht. Für diese Generierung ist eine Geodatenabfrage erforderlich. Bei dieser Abfrage kann zwischen einer GPS-basierten Dezimalgrad- (Grad, Minuten, Sekunden) und einer UTM-Koordinatenprojektion gewählt werden. Anzumerken bleibt, dass sich systemalgorithmische i. S. v. benutzerunabhängige Auswahlkriterien in der Praxis progressiv bewähren.

Die Visualisierung der georeferenzierten Daten erfolgt auch im FBS unabhängig vom Maßstab als generalisierte, thematisch-kartographische Projektion mit der Prämisse auf der Ausweisung der Flächennutzung unter Angabe sekundärer metrischer Daten, z. B. von Straßennamen und Hausnummern, wobei der reale Gebäudebestand nicht oder nur marginal generiert abgebildet wird. Eine 3D-Projektion der Geodaten ist in der aktuellen Version des FBS nicht möglich. Allerdings sind Bilddaten als 3D-Projektion mit dem FBS bearbeitbar. Der Raumbezug lässt sich hierbei einzig auf der thematisch-kartografische Grundkarte beziehen und bedingt visualisieren.

4.3 Leitstellensysteme – T-System

Die kooperativen Regionalleitstellen (KRL) stellen einen Verbund des Landes Niedersachsen (Polizei) mit kommunalen Trägern (Landkreise) dar (Hameln-Pyrmont o. D.) die die Dienststellen der Polizei, der Rettungswachen und Feuerwehren sowie diverser Hilfsorganisationen (DRK, DLRG, THW, etc.) hinsichtlich der Aufgaben- und Einsatzlagenbewältigung koordinieren (Wittmund 2018). Die Leitstellen in Niedersachsen sind aktuell nicht mit einem einheitlichen Leitstellensystem ausgestattet, welches in Zukunft ändern wird.

Topografische Karten werden sowohl vom Map-Server als auch vom ArcGIS-Server des Landkreises genutzt. Der Austausch der hinterlegten Layer-Informationen kann nicht problemlos realisiert werden, da die Erweiterung mit Layern nur eingeschränkt möglich ist. Die visualisierte Kartendarstellung ist nur in einer 2D-Projektion möglich, sodass ein räumlicher Ebenenschnitt in die

Häuserfluchten und Bauwerke nicht umsetzbar erscheint. Zudem besteht keine Möglichkeit eines direkten Datenaustauschs bzw. einer direkten Datenabfrage von Informationen in Echtzeit vom VBS bzw. FBS mit den leitstellenspezifischen Produkten. So können aktuelle Tatortspuren nicht in Echtzeit mit bereits vorhandenen Spuren abgeglichen werden und in Konsequenz Zusammenhänge nicht in Echtzeit erkannt werden.

Weder eine in die thematischen Karten implizierte Videoeinspielung noch eine Videoanalyse in Echtzeit ist produktintegriert möglich, sodass diese Sequenzen overlayed oder auf einem separaten Bildschirm eingespielt werden müssen. Die Softwareprodukte auf den Leitstellen sind für sich genommen sehr effektiv und effizient, bei der Kompatibilität zwischen den Systemen aber besteht noch Handlungsbedarf. Hier würden sich ganzheitliche GIS-basierte Produktlösungen anbieten, die einen Datentransfer automatisieren und Interoperabilitäten aufweisen.

4.4 Predictive Policing

Predictive Policing (PP) wurde in vielen Bundesländern umgesetzt, unter anderem in Bayern und Baden-Württemberg mit PreCobs, in Niedersachsen mit PreMap und in Nordhein-Westfalen Skala. Mittels PreMap soll präventiv aktuell die Zahl der Tageswohnungseinbrüche zukünftig aber auch Brandstiftungsdelikte oder Kfz-Delikte reduziert werden. Der Near-Repeat-Algorithmus berücksichtigt neben den kriminalwissenschaftlichen Daten auch Angaben über Wetterprognose, Bebauung, Verkehrsanbindung und sozioökonomische und demografische Strukturen (Heidorn 2018). Die Berücksichtigung einer selektiven Komponente, z. B. hinsichtlich eines täterspezifischen Modus operandi[9], könnte die Prognose optimieren.

4.5 Scanner- und Kamerabildauswertung

Die eingesetzten Vermessungs- und Dokumentationsverfahren erfassen aktuell die Geo-Daten nicht implizit, sodass in der Vorgangsbearbeitung die primär metrischen Bezüge indirekt über sekundäre Metrik erhoben werden müssen. Die

[9]Modus Operandi bezeichnet die typische Vorgehensweise eines Täters an einem Tatort (Burghard et al. 1984, S. 148).

Auswertung der mit dem Scanner-Kamerasystem generierten Daten erfolgt mit einer herstellerspezifischen Software (ZF LaserControl). Die gewonnenen Informationen (Einzelscans) werden auf einem Speicher abgelegt und automatisch zu einer Punktwolke zusammengeführt. Die Software ermöglicht die Verknüpfung der Scan- mit den Bildpunkten der Kamera, sodass die Punktwolke über die Farbdarstellung schneller verortet und zu einem farbigen Orthofoto verarbeitet werden kann. Störfelder bzw. verpixelte Sichtfelder können bereits in diesem Stadium bereinigt werden. Gleichzeitig generiert die Software die Positionierung des Scanners und stellt die Aufstellstandorte visualisiert in einer Draufsichtprojektion dar. Problematisch gestalten sich spiegelnde Oberflächen (Spiegelungen, Fenster, Lacke) an Objekten. Eine stereoskopische Auswertung basierend allein auf den gewonnenen Bildinformationen ist aktuell nicht realisierbar.

Grundsätzlich können Teile von Gebäuden oder Gegenständen (PKW, Bus etc.) entfernt werden, indem die entsprechenden Pixel nicht generiert werden. Somit wird der Blickwinkel in das Objekt freigegeben. Letztlich werden so zwei Orthobilder, zum einen unter Berücksichtigung sämtlicher und zum anderen das mit den bereinigten Punktdaten generiert. Allerdings ist eine Bearbeitung des Orthobildes mit einer 3D-Software nicht vorgesehen, sodass die Zerlegung von Gebäuden und Gegenstände in Einzelbestandteile nicht möglich ist.

Die Auswertung der mit Kamerasystem piXplorer 500 (Fa. Clauss Rodeon) erstellten Daten erfolgt mit der Software R2S Forensic (Fa. abf diagnostics GmbH), die neben der Erstellung eines sphärischen Panoramabildes auch direkte Bildvergleiche von dokumentierten Spuren und Beweismitteln vornehmen kann, z. B. daktyloskopische Spuren bzw. Tatwerkzeuge als Spurenträger unter Einbindung entsprechender Dokumente (abf diagnostics 2017, S. 6 ff.).

Die Beschaffung eines Handscanners ist in Planung, aber noch nicht umgesetzt. Sofern stereoskopische Bild- bzw. 3D-Scaninformationen vorliegen, ist eine Visualisierung in einem VRL grundsätzlich möglich und in einigen Fällen bereits praktiziert worden.

5 Auslesen von Peripheriegeräten

Das Auslesen von Mobilfunk-Geräten (Smartphone, Tablet, PDA etc.) ist heute essenzieller Bestandteil der Ermittlungstätigkeit polizeilicher Behörden. Dabei werden Produkte wie Cellebrite, Elcomsoft, MSAB, Oxygen Forensic, X-Ways, Access Data, Magnet Forensics eingesetzt.

Beim Auslesen der stationären und mobilen Geräte sollte neben den sekundären auch das Augenmerk auf den primär metrischen Daten[10] liegen. Die Geoinformationen können in visualisierter Form, direkt oder indirekt, vorliegen oder bei permanentem Betrieb der Geräte im Online-Modus (stetige Empfangsbereitschaft) automatisch durch die Satellitensignale über die interne GPS-Antenne die Geopositionen generiert werden. Hierbei können Informationen in visualisierter Form i. d. R. mit einem Geo-Standort in Verbindung gebracht werden. Derartige Informationen sollten direkt georeferenziert werden, sodass den Bildinformationen ein georeferenzierter Standort zugewiesen und die entsprechenden Koordinaten in einem GIS-Produkt abgegriffen werden können, z. B. Mapility-Tools, die die Geo-Daten aus den Fotos und Bildern auslesen (Hesseling 2015).

Digitale Bilder bzw. Fotografien beinhalten oft sogenannte Metadaten. Insbesondere Exif-Daten (Exchangeable Image File Format) werden nahezu von jedem Kamera- und Smartphone-Hersteller unterstützt und beinhalten neben Datum und Uhrzeit auch Geo-Informationen und Kamerawinkel, die sofern mit GPS-Empfänger herstellerseitig ausgestattet, automatisch generiert und an jedem weiteren Client nachträglich eingefügt (Hesseling 2015). Auch XMP-Daten (Extensible Metadata Platform) enthalten meist Exif-Informationen, sodass auch hier die Georeferenzierung automatisch erstellt wird (Hesseling 2015). Mit diversen Online-Tools, z. B. Jeffrey's Exif Viewer, Picasa oder Darktable, lassen sich die Basisbild-Informationen auslesen, die unter dem Attribut Location zum einen den Koordinatenbezug in Grad-Dezimal bzw. Längen- und Breitengrad und zum anderen die Lokalisation bezüglich der Koordinaten sowie dem Attribut Datum, die neben diesem auch die Uhrzeit ausweisen (Hesseling 2015). Diese Auswertetools sind insbesondere bei anonymen visualisierten Anzeigen von besonderem Interesse, um beispielsweise den Tatort lokalisieren und die handelnden Akteure ggf. durch eine Bilddatenanalyse identifizieren zu können.

Die Online-Präsenz mobiler Geräte führt zur permanenten Erstellung bzw. Erzeugung geobasierter Informationen, die in der letzten Konsequenz abgerufen werden können. Diese Geo-Daten sind mit einer Standortabfrage bzw. Geolokalisierung über eine spezielle Software abrufbar, die auch als App verfügbar ist, z. B. Geoloc (2019).

Erwähnt sei noch, dass mit dem Zugang zum World Wide Web (WWW) automatisch eine IP-Adresse zugewiesen wird, sodass der Anschlussinhaber

[10]Siehe hierzu Ausführungen in Abschnitten „Geografisches Informationssystem (GIS)“ und „Möglichkeiten von GIS-Produkten“.

des Zugangs ins Netz beim Provider registriert wird. Die Daten des Anschlussinhabers zu der entsprechenden IP-Adresse sind über den Provider abrufbar. Anhand der IP-Adresse lassen sich nicht nur sekundär metrische (Uhrzeit, Datum etc.), sondern auch primär metrische (Standort, Position) Informationen auslesen.

Anonymisierte IP-Adressen (Proxys, VPNs oder andere Anonymisierer) können ggf. mit einer speziellen Software (GeoIP, Fa. MaxMind) identifiziert und ggf. der georeferenzierte Standort angezeigt werden (MaxMind o. D.). Die Datenbankrecherche über ein Tool, das die Whois-Server durchsucht, führt über die IP-Adresse zu diversen Attributen u. a. dem Standort (Stadt, Adresse) und die zugehörigen GPS-Koordinaten, die auf der Geobasis-Webseite über Eingabe der Koordinaten visualisiert abgebildet werden können (Kratzenberg 2015). Sofern anonymisierte Adressen nicht ausgelesen werden können, besteht noch die Option über spezielle Tools (IPNetInfo) mit Whois-Server-Suche (Arin, Ripe, APNIC, LACNIC oder AfriNIC) mindestens auf den Provider und ggf. auf die IP-Adresse mit den Verbindungswegen schließen zu können (Papenfuß o. D.).

6 Auslesen von Fahrzeugdaten

Das Kfz von heute stellt ein mobiles Rechenzentrum dar, ausgestattet mit unzähligen Prozessoren. Die Abgasreinigungsanlage wird computergestützt über die sogenannte On-Board-Diagnose-(OBD-)-2-Schnittstelle gesteuert (Zotow und Urbanki 2013). Mit dem Betriebssystem Windows kann über die OBD-2-Schnittstelle auf die im Fahrzeug verbauten Steuergeräte zugegriffen werden, und es besteht die Möglichkeit, über eine Remote-Freigabe auf die Geräte mittels Fernsteuerung durch VNC, Team-viewer oder RDP zuzugreifen (Fluhr 2019). Auch rein elektrisch angetriebene Kfz besitzen eine solche Schnittstelle, hier als EOBD bezeichnet, sodass die motor- und fahrtspezifischen Daten auslesbar sind (Outils OBD Facile 2017).

Diese Option der Datengenerierung ist insbesondere bei Neufahrzeugen von immenser Bedeutung, da zu Navigationszwecken auch ein entsprechendes GPS eingebaut wurde, wobei Ungenauigkeiten in der Bestimmung der realen Position sich in der Größenordnung von wenigen Zentimetern in Anlehnung an die Sicherheitsnorm ISO 26262 (Funktionale Sicherheit für Straßenfahrzeuge) befinden (Fluhr 2019). Bei auftretenden Störungen, z. B. kurzfristige Signalunterbrechung, kommen interne Sensoren zum Einsatz, die aufgrund von spezifischen Algorithmen die Navigation fortführen, analog unbemannter Fluggeräte (Fluhr 2019). Das Auslesen der Fahrzeugdaten aus vernetzten Fahrzeugen (Baujahr 2004 und jünger) mittels Adapter und Diagnosesoftware sich unproblematisch gestaltet.

Bei vorhandenen Navigationssystemanbindungen lassen sich auch die Geopositionen des Fahrzeuges auslesen. Zukünftig wird eine vernetzte Flottenstruktur von E-Fahrzeugen per Satellitensystem (Galileo) überwacht und entsprechend gesteuert mit dem Ziel, Verkehrsunfälle und Verkehrskollapse, insbesondere in den Ballungszentren, zu vermeiden.

In der gewerblichen Binnenschifffahrt werden zur Erforschung der Unfallursache im Rahmen der Schiffsunfallaufnahme die Geodaten aus dem elektronischen Navigationsinformationssystem (Inland ECDIS) erhoben und ausgewertet, z. B. richtungsweisender Kurs und Geschwindigkeit, Positionsbestimmung sowie Manöver des letzten Augenblicks (Schulze o. D.). Wobei die Bestimmung der Position des Fahrzeuges meist ohne Erhebung der georeferenzierten Daten in die Ermittlungen einbezogen werden.

Die MarineTraffic-Webplattform[11] ist ein Online-Service, die die georeferenzierten Schiffspositionsdaten und Bewegungen von See- und Binnenschiffen als Live-Abbildung auf einer Karte ausweist (Lekkas et al. 2006). Darüber hinaus werden weitere schiffsspezifische Daten (Schiffsname, Flaggenstaat, MMSI-Nummer, Art des Schiffes, Schiffslänge usw.) angegeben. Dabei nutzt die Webplattform MarineTraffic das Automatic Identification System (AIS), ein UKW-basiertes System, bei dem ein AIS-Transponder als Bordgerät fungiert, ausgestattet mit einem Positionsempfänger (GPS-Empfänger) und einem Datenfunkgerät, und den Austausch der Navigations- und Schiffsdaten realisiert (Bureau Telematica Binnenvaart o. D., S. 2). Auch für Echtzeit-Positionsbestimmungen von Flugzeugen existieren webbasierten Plattformen (wie Flightradar24 oder Flightradar.live), die neben den Geo-Daten auch spezifische Flug-Informationen, z. B. Flugnummer, generieren (Felder o. D.). Da das autonome Führen bei Flugzeugen und Schiffen durch einen Autopiloten zum Ausrüstungsstandard gehört, ist die Auswertung der georeferenzierten Daten aus den Aufzeichnungsgeräten der Bordsysteme ein wesentlicher Bestandteil der Ermittlungsarbeit der Polizei.

[11]MarineTraffic ist eine offener Webplattform-Service der die Positionen und Bewegungen sowie spezifische Daten von Schiffen verwaltet und visualisiert als Live-Karte darstellt (Ellerbrock 2014, S. 18 ff.). Die für MarineTraffic erforderlichen Daten und Informationen werden mit sogenannten Automatic Identification System (AIS) – Automatisches Schiffsidentifizierungssystem – realisiert, wobei ein AIS-Transponder als Bordgerät fungiert, ausgestattet mit einem Positionsempfänger (GPS-Empfänger) und einem Datenfunkgerät (Bureau Telematica Binnenvaart o. D., S. 2).

Im Rahmen der Schwerlastüberwachung stehen neben dem Auslesen des digitalen Kontrollgerätes mit den darin enthaltenen fahrzeug- und fahrerspezifischen Daten auch noch weitere Daten zur Verfügung, die nicht nur vor Ort, sondern auch in den Speditions- oder Logistikunternehmen verfügbar sind. Die Kommunikation zwischen dem Unternehmen und seiner Fahrzeugflotte wird über Online-Plattform sichergestellt. Hierfür werden verschiedene zusätzliche Telematik-Geräte inklusive der erforderlichen Fahrzeugortungsgeräte in den Fahrzeugen verbaut, z. B. Webfleet, Fa. TomTom, oder VDO FleetVisor mit TruckLinc und DriverLinc System, Fa. Continental Automotive GmbH (Continental Automotive GmbH 2019; Webfleet Solutions B.V. 2018). Die auf einem Server ohne oder mit einem Cloud-Anbieter bereitgestellte Software sowie Daten sind über das Internet zugänglich, sodass die Peripheriegeräte (Clients, PC's, Tablets, PDA's, Smartphones) von verschiedenen Orten auf diese Informationen zugreifen und ggf. be- bzw. verarbeiten (Continental Automotive GmbH 2019; Kuhfuß 2015). Die Positionsbestimmung wird auch hier in Echtzeit durch GPS-Ortung der Fahrzeuge ermöglicht (Continental Automotive GmbH 2019; Webfleet Solutions B.V. 2018). Das System zeichnet letztlich geobasiert die Reiserouten und -daten auf, abrufbar über den Server für die Fahrzeugflotte. Darüber hinaus ermöglicht die Nachrüstung von GPS-Loggern bei LKW-Aufliegern oder -wechselbrücken eine erhöhte Absicherung gegen Diebstahl – TrailerLINC, Fa. Continental Automotive GmbH (Dobos 2017). Auch die Erstellung eines Bewegungsprofils erfolgt mit Geo-Daten. Die generierten Geo-Daten lassen sich abrufen und in Echtzeit visualisieren.

7 Auslesen von Verkehrssteuerungsdaten

Das Fahrzeug der Zukunft, ein sogenanntes modernes connected car, wird pro Stunde in etwa 25 GB an Daten erzeugen (Nickl und Weigl 2018 S. 15). Durch mehrere Assistenten soll zukünftig die Koordination zwischen Vehicle-to-Road (Ampel, Fußgängerüberweg etc.), Vehicle-to-Vehicle (Sensoren Fahrzeug-Fahrzeug) und Pedestrian (Fußgänger über Mobilgerät etc.) gewährleistet werden (Kawabata et al. 2015, S. 20 f.). Diese Vision ist in modernen innerstädtischen Verkehrssystemen für den öffentlichen Personennahverkehr in Form der Vehicle-to-Road-Steuerung über Sensoren und Aktoren bereits realisiert. Während in der Vergangenheit die Vorrangsteuerung über Kontaktschleifen, Bake-Funk-Systeme, Infrarotsysteme, induktive Meldeübertragung oder Oberleitungskontakte realisiert wurde, sehen aktuelle Lösungen WLAN-Steuerungen mittels Sensoren und Aktoren vor, d. h. die Objekte werden z. B. über die MAC-Adresse in der

Anlage registriert, die die Vorrang- und Verkehrssteuerung ermöglicht. Die Start-Zeit-Analyse sowie der Abgleich der Reise- und Wartezeit mit den georeferenzierten Informationen aus den Lichtsignalanlagen führen zu einem intelligenten urbanen Leitsystem. Die WLAN-Steuerung setzt den Online-Modus mobiler Geräte voraus, sodass die Vorrangsteuerung eine Annäherung erkennen kann und die Steuerungsschleife ausgelöst. Somit lassen sich Geodaten künftig auch über die Signal- und Steuerungssysteme der urbanen Verkehrsleitsysteme generieren.

8 GIS-basierte Produktlösung GeoFES

Das Geogestützte-Feuerwehrentscheidungshilfesystem (GeoFES) stellt ein Einsatzführungssystem für Behörden und Organisationen mit Sicherheitsaufgaben dar und unterstützt insbesondere Führungskräfte bei der Bewältigung von Standardeinsätzen sowie Groß- und Flächenschadenslagen, z. B. Flächenbrände, Naturereignisse (Eurocommand 2015). Dieses System integriert und exploitiert konsequent Geo-Informationen zur Lageerkundung auch im Vorfeld und insbesondere für räumliche Analyse, sodass Einsatzabschnittbildungen problemlos von Führungskräften vor Ort wie auch zentral vom Lagezentrum bei flexibler und primitiver Benutzung durch entsprechende Konfigurationsstrukturen arrangiert werden können (Eurocommand 2015). Die automatische Dokumentation, d. h. die Protokollierung aller Maßnahmen sowohl von Kräften vor Ort über mobile Peripheriegeräte als auch aus dem zentralen Führungszentrum, erfolgt in einem Einsatztagebuch als Berichtspflicht ad-hoc, sodass die gewonnenen Informationen referenziert in Handkarten, Schadenskonten, Lagebildern, Analysen bzw. Kräfteübersichten präsentiert werden können (Eurocommand 2015). Auf der Basis der Geo-Daten lassen sich in Echtzeit Ermittlungen von Gefahren-, Such-, Warn- und Evakuierungsbereichen analysieren und darauf stützend entsprechende Maßnahmen ableiten, die sich auf einer rollen- und aufgabenbasierten Zusammenarbeit, auch Behörden übergreifend, stützt (Eurocommand 2015).

9 Zusammenfassung und Ausblick

Raumbezogene Daten tangieren nahezu alle Bereiche der polizeilichen Sach- und Ermittlungsarbeit und sind somit von zentraler Bedeutung. Die Erhebung der Daten kann automatisch über den Adressencode und umgekehrt systemimmanent über mobile bzw. stationäre Geräte oder gar manuell im Nachhinein über eine geobasierte Grundkarte generiert werden.

Durch den Einsatz GIS-basierter 2D/3D-Technolgie wird die Tatortarbeit sowohl im Straftat- als auch Verkehrsdeliktsbereich immens stilisiert, sodass nicht zuletzt der objektive Tatbefund lückenlos dokumentiert, mittels Auswertesoftware visualisiert und durch einen Sachbearbeiter analysiert werden kann. Diese Auswertungsmethodik eröffnet völlig neue Perspektiven in der polizeilichen Tatortarbeit. Insbesondere durch Einbindung von Geo-Informationen lassen sich objektivere Vergleiche mit anderen Tatorten auch ad-hoc hinsichtlich eines gemeinsamen Modus Operandi ziehen. Gerade eine georeferenzierte Aufbereitung der statistischen Zahlen kann insbesondere dazu beitragen, Brennpunkte und Querverweise im Kontext Cybercrime deutlicher zu identifizieren.

GIS-Produktlösungen werden mittlerweile erfolgreich seit Jahren im Bereich des Krisen- und Sicherheitsmanagement zur Bewältigung größerer Schadensereignisse (Umweltkatastrophen, Terrorismus, etc.) eingesetzt. Somit bietet eine GIS-basierte Plattform eine Vielzahl an Synergien, um geobasierte Daten für Kartenprojizierung und Visualisierung, Bilddaten- und Fernerkundungsanalyse, 3D-Modellierung inklusive CAD-Modifizierung und deren permanente Reproduzierbarkeit auch in einem virtuellen mobilen oder stationären Raum, räumliche Analysen und Beziehungen inklusive Kriminalitätsprognose bzw. -prävention i. S. v. Predictive Policing auch in Echtzeit, Datenmanagement und insbesondere BigData-Administration auch App-basiert zu nutzen, sodass eine ressourceneffiziente und -effektive Entscheidungshilfe zur Bewältigung von Einsatzlagen darstellbar erscheint.

Die 3D-Tatort- und 3D-ED-Behandlung-Informationen können in einem virtuellen Raum als Tatrekonstruktion zusammengeführt werden. Hier können Tatvorgänge auf ihre Plausibilität hin überprüft werden und durch Simulationen kann die wahrscheinlichste Variante des Tathergangs bestimmt werden. So kann ein Sachverständige z. B. anhand der dokumentierten Verletzungen und Deformationen der beteiligten Fahrzeuge den wahrscheinlichsten Unfallhergang ermitteln. Zudem können die bewerteten Szenarien vor Gericht als 2D-Aufnahme oder besser als virtuelle 3D-Rekonstruktion vorgeführt werden. Somit hätten alle Beteiligten vor Gericht eine bessere Bewertungsbasis für ihre Einschätzungen. Auch Formspuren können mit entsprechenden Gerätschaften digital aufgenommen werden und können direkt in den virtuellen Szenarien eingespielt werden.

Weitere Tätigkeitsfelder eröffnen sich mit neuen Technologien wie dem Internet der Dinge und Cloud-Computing. Eine Vielzahl an Gerätschaften werden miteinander verbunden. Daten und Informationen, insbesondere Geo-Informationen, müssen entsprechend aufgenommen und verarbeitet werden. Es entsteht eine völlig neue Welt der Informationsverarbeitung. So können z. B. das

autonome Fahren und die damit einhergehende Verwendung digitalisierter Verkehrssteuerungssysteme im öffentlichen Verkehrsraum, aber auch der sogenannte Smarthome-Sektor, stärker forciert und unterstützt werden. Gerade deswegen bedeutet die Umsetzung der europäischen Vorschriften zum Austausch von Geo-Daten innerhalb der Institutionen und über Ländergrenzen hinaus, die strukturelle Vernetzung der Systeme insbesondere in ihrer Interoperabilität und Kompatibilität, sodass behördliche Institutionen flexible Verbundlösungen angehen könnten, die insbesondere sich auch in einer Geoportallösung mit einer GIS-Umgebung in Form eines GIS-Servers umsetzen lassen. Demnach könnte ein vernetzter Verbund im Sinne der INSPIRE-Richtlinie (Europäisches Parlament und Rat der Europäischen Union 2007) insbesondere der Institutionen und Behörden angedacht werden, der nicht zuletzt auch aus ökonomischen Beweggründen immense Vorteile mit sich bringen würde. Entscheidend bei der Entwicklung einer einheitlichen GIS-Infrastruktur ist die Berücksichtigung datenschutzrechtlicher, ökonomischer und struktureller Aspekte.

Literatur

abf diagnostics (2015). *piXplorer 500 Forensik – Tatortkopien auf „Knopf-druck“*. (abf d. GmbH, Hrsg.). Kranzberg, Bundesrepublik Deutschland. https://www.abfdiagnostics.com/de/produkte/pixplorer-500-forensik/index.html. Zugegriffen: 31. März 2019.

abf diagnostics (2017). *Tatortfotografie 2018 – Automatische, sphärische Fotografie; Automatisches „Stitching“*. (abf d. GmbH, Hrsg.). Kranzberg, Bundesrepublik Deutschland. (S. 3–11). https://www.abfdiagnostics.com/cms/upload/literatur/abf_diagnostics_Informationsbroschre_Tatortfotografie_2018.pdf. Zugegriffen: 31. März 2019.

Agisoft (2019). *Metashape – photogrammetrische Verarbeitung digitaler Bilder und Erzeugung von 3D-Geodaten.* (A. LLC., Hrsg.). St. Petersburg, Russland. https://www.agisoft.com/. Zugegriffen: 5. Apr. 2019.

Baldenhofer, K. G. (o. D.). *Lexikon der Fernerkundung: Optoelektronischer Scanner*. Friedrichshafen, Bundesrepublik Deutschland. http://www.fe-lexikon.info/lexikon-o.htm. Zugegriffen: 11. Juli 2019.

Bartelme, N. (2005). *Geoinformatik – Modelle, Strukturen, Funktionen* (4. Aufl.). Berlin: Springer.

Bill, R. (2016). *Grundlagen der Geoinformationssysteme* (6. Aufl.). Berlin: Wichmann.

Booch, G., Rumbaugh, J., & Jacobsen, I. (2006). *Das UML Benutzer-handbuch – Aktuell zur Version 2.0.* (I. d. GmbH, Hrsg., & G. T. GmbH, Übers.). München: Addison-Wesley.

Bundesamt für Sicherheit in der Informationstechnik (o. D.). *Fingerabdruckerkennung* (BSI, Hrsg.). Berlin, Bundesrepublik Deutschland. https://www.bsi.bund.

de/SharedDocs/Downloads/DE/BSI/Biometrie/Fingerabdruckerkennung_pdf.pdf?__blob=publicationFile. Zugegriffen: 28. März 2019.

Bureau Telematica Binnenvaart (o. D.). *Was ist ein AIS? Eine Einführung zu Inland AIS in der Binnenschifffahrt*. Eine Zusammenarbeit der Niederlande, Deutschlands und der Europäischen Union. https://www.wsv.de/wsa-toe/schifffahrt/Schifffahrtszeichen/Info-AIS.pdf. Zugegriffen: 3. Juli 2019.

Burghard, W., Herold, H., Hamacher, H. W., Schreiber, M., Stümper, A., & Vorbeck, A. (Hrsg.). (1984). *Kriminalistik Lexikon*. Heidelberg: Kriminalistik.

Cappelli, K. (2019). *Drohnenkorridore für Paketzustellung berechnen*. ESRI, ArcGIS Pro, (Hrsg.). Redland, USA. https://www.esri.com/arcgis-blog/products/arcgis-pro/analytics/calculate-drone-corridors-for-package-delivery/. Zugegriffen: 17. März 2019.

Continental Automotive. (2019). *Fleet Management Lösungen* (C. Automotive GmbH, Hrsg.). Hannover. https://www.continental-automotive.com/de-DE/Trucks-Buses/Interior-Cabin/Tachographs,-Telematics-Services/Fleet-Management-Solutions. Zugegriffen: 8. Apr. 2019.

Deutsches Zentrum für Luft- und Raumfahrt (04.10.2018). *Globales 3D-Höhenmodell der TanDEM-X-Mission frei verfügbar* (DLR, Hrsg.). Köln, Bundesrepublik Deutschland. https://www.dlr.de/dlr/desktopdefault.aspx/tabid-10080/150_read-30139/#/gallery/32238. Zugegriffen: 14. Apr. 2019.

Dobos, L. (24. April 2017). *Tracking: Vogelperspektive auf der Anhänger-flotte – Premiere für GPS-Sender von VDO* (H. V. GmbH, Hrsg.). München: Huss. https://logistik-heute.de/news/tracking-vogelperspektive-auf-die-anhaengerflotte-13655.html. Zugegriffen: 8. Apr. 2019.

Ellerbrock, B. (2014). *Auf Frachtschiffen unterwegs ‚Sag dem kleinen Abenteuer das Du kommst'*. Berlin: epubli GmbH.

ESRI. (2019a). *ArcGIS-Bildband. Die Natur der Fernerkundung. Informationen aus der Ferne gesammelt* (E. Inc., Hrsg.). Redland, USA. https://learn.arcgis.com/de/arcgis-imagery-book/chapter2/. Zugegriffen: 17. März 2019.

ESRI. (2019b). *ArcGIS. Geografische Daten verwalten* (E. Inc., Hrsg.). Redland, USA. http://desktop.arcgis.com/de/data-management/. Zugegriffen: 16. März 2019.

ESRI. (2019c). *ArcGIS. Solutions for local government* (3D-Grundkarten der Kommunalverwaltung). (E. Inc., Hrsg.) Redland, USA. http://solutions.arcgis.com/local-government/help/local-government-scenes/. Zugegriffen: 16. März 2019.

EUROCOMMAND. (2015). *Professionelles Werkzeug zur Einsatzführung* (E. GmbH, Hrsg.). Halstebek, Bundesrepublik Deutschland. https://www.eurocommand.com/komplettloesungen/professionelles-werkzeug-zur-einsatzfuehrung.php. Zugegriffen: 17. Apr. 2019.

Europäisches Parlament und Rat der Europäischen Union. (14. März 2007). *Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates vom 14. März 2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE)*. (R. d. EU ü. Amt für Veröffentlichungen der Europäischen Union, Hrsg.). Luxemburg. https://eur-lex.europa.eu/legal-cotent/DE/TXT/?uri=celex:32007L0002.

Felder, P. (o. D.). *flightradar.live*. Zürich, Schweiz. https://flightradar.live/?gclid=Cj0KCQjw4qvlBRDiARIsAHme6ouvLRaV8OxtV7pRgzCJkt1TfJMniXmvAe7MgU-Ej8m0qnFBMHk1-QGgaAlxcEALw_wcB. Zugegriffen: 8. Apr. 2019.

Fingerprinting. (2019). *Fingerabdruck-Identiikation (Fingerprint Identification)* (G. Übersetzer, Übers.). USA. http://www.fingerprinting.com/fingerprint-identification.php. Zugegriffen: 30. März 2019.

Fluhr, D. (2019). *Hexagon: GPS & GNSS. Autonomes Fahren & Co*. Berlin, Bundesrepublik Deutschland. https://www.autonomes-fahren.de/hexagon-gps-gnss/. Zugegriffen: 20. März 2019.

Fritsch, D. (2014). *Mobile Mapping – Eine Revolution im Vermessungs-wesen?* (U. Stuttgart, Hrsg.). Stuttgart, Bundesrepublik Deutschland. http://www.ifp.uni-stuttgart.de/publications/2014/2014-fritsch-MOBILE_MAPPING1.pdf. Zugegriffen: 31. März 2019.

Geoloc. (2019). *Geoloc – Finden Sie ein Handy, überall* (G. S.L.U, Hrsg.). Barcelona, Spanien. https://geoloc.mobi/de/#how-it-works. Zugegriffen: 8. Apr. 2019.

Geosystems. (o. D.). *GeoMedia – Features* (I. Corporation, Hrsg., & H. G. Partner, Redakteur). Germering, Bundesrepublik Deutschland. https://www.geosystems.de/produkte/geomediar/funktionen/. Zugegriffen: 14. Apr. 2019.

Hameln-Pyrmont, Landkreis. (o. D.). *KRL-Weserbergland – Der Ausblick* (L. Hameln-Pyrmont, Hrsg.). Hameln, Bundesrepublik Deutschland. http://www.krl-weserbergland.eu/der-ausblick/index.html. Zugegriffen: 23. Apr. 2019.

Heidorn, S. (21. September 2018). *Predictive Policing: So funktioniert die Verbrecherjagd mit Big Data!* (H. GmbH, Hrsg.). Jena, Bundesrepublik Deutschland. https://www.trendsderzukunft.de/predictive-policing-so-funktioniert-die-verbrecherjagd-mit-big-data/. Zugegriffen: 24. Apr. 2019.

Hesseling, C. (2015). *Ich sehe was, was du nicht siehst: Metadaten in Fotos* (iRights.info, Hrsg., V. Djordjevic, & H. Steinhau, Redak-teure). Berlin, Bundesrepublik Deutschland. https://irights.info/artikel/metadaten-fotos-anbringen-loeschen-bearbeiten/26353. Zugegriffen: 23. Apr. 2019.

Intergraph. (Januar 2008). *Arbeiten mit GeoMedia Professional* (Private Company, Intergraph Cooperation, Hrsg.). Huntsville, USA. Handbuch (S. 1–1158). http://www.umgis.de/fileadmin/dateiliste/downloads/externe/geomedia/geomedia_06/WorkingwithGeoMediaProfessional_300dpi.pdf. Zugegriffen: 14. Apr. 2019.

Kappas, M. (2001). *Geografische Informationssysteme. Das geografische Seminar*. Braunschweig: Westermann Schulbuchverlag.

Kawabata, A., Mouri, H., Murakami, T., Tanimichi, T., Shima, T., Uchiyama, & H., Yokoyama, A. (März 2015). *Interconnected cars that understand each other – Automatend driving development project*. In Hitachi technology 2015 – Moving forward with our social innovation buisness. (H. Kabashikigaisha, Hrsg.). Chiyoda, Japan. *Hitachi Review, 3*(64). http://www.hitachi.com/rev/pdf/2015/r2015_technology_all.pdf. Zugegriffen: 23. Apr. 2019.

Kermorvant, A. (Januar 2017). EOBD-Facile – OBD2 Software für Kfz-Diagnose unter Windows-PC/Macbook (Outils OBD Facile, Hrsg.). Plescop, Frankreich. https://www.klavkarr.de/software-eobd-facile-elm327.php. Zugegriffen: 27. März 2019.

Könneker, C., & Müller, A. (1998). *Lexikon der Physik. LIDAR*. Stuttgart, Bundesrepublik Deutschland & Spektrum Akademischer Verlag. https://www.spektrum.de/lexikon/physik/lidar/9033. Zugegriffen: 7. Juli 2019.

Kratzenberg, M. (8. Dezember 2015). *IP finden und Besitzer orten – So geht's!* (S. M. GmbH, Hrsg.). GIGA.de. Herausgeber: Ströer Media Brands GmbH. https://www.giga.de/software/sicherheit-utilities/sicherheit/ip-finden-besitzer-orten/. Zugegriffen: 8. Apr. 2019.

Kuhfuß, J.-O. (31. Mai 2015). *Was ist eine Cloud? – Einfach erklärt* (C. D. GmbH, Hrsg.). München, Bundesrepublik Deutschland & Hubert Burda Media. https://praxistipps.chip.de/was-ist-eine-cloud-einfach-erklaert_41255. Zugegriffen: 8. Apr. 2019.

Lekkas, D., et al. (2006). *Marine Traffic.* Mytilini, Griechenland. https://www.marinetraffic.com/en/ais/home/centerx:10.658/centery:52.419/zoom:18. Zugegriffen: 8. Apr. 2019.

MaxMind. (o. D.). *GeolP2 – Anonymuos IP-Datenbank. Erkennen Sie Proxys, VPNs und andere Anonymisierer* (MaxMind Company, Hrsg.). Waltham, USA. https://www.maxmind.com/en/solutions/geoip2-enterprise-product-suite/anonymous-ip-database. Zugegriffen: 8. Apr. 2019.

Nayak, N. (05. März 2019a). *Explorative Sichtbarkeitsanalyse aus Gebäuderäumen* (ESRI, ArcGIS Pro, Hrsg.). Redland, USA. https://www.esri.com/arcgis-blog/products/arcgis-pro/3d-gis/exploratory-visibility-analysis-from-building-rooms/. Zugegriffen: 17. März 2019.

Nayak, N. (5. März 2019b). *Sonnenlicht und Schatten* (ESRI, ArcGIS Pro, Hrsg.). Redland, USA. https://www.esri.com/arcgis-blog/products/arcgis-pro/3d-gis/sunlight-and-shadows/. 17. März 2019.

Niedersächsische Landesregierung. (27. März 2012). *Kleine Anfrage mit Antwort an den Niedersächsischen Landtag – Anfrage der Abge-ordneten PIA Beate Zimmermann (Linke, eingegangen am 02.02.2012 – Polizeiliche Daten im Verbund* (16/4650). (Nieder-sächsisches Ministerium für Inneres und Sport, Hrsg., & U. Schünemann, Redakteur). Hannover, Bundesrepublik Deutschland. Drucksache 16/4650. file:///C:/Users/Dirk/Downloads/16-2270%20(1).pdf. Zugegriffen: 13. März 2019.

Nickl, T., & Weigl, B. A. (2018). Bedrohungen durch Schwduling-basie-rende Angriffsszenarien im Automotive-Bereich. In O. T. Amberg-Weiden (Hrsg.), Bundesrepublik Deutschland. Frischmann Druck & Medien GmbH. Forschungsbericht 2018 (S. 3–188). https://www.oth-aw.de/files/oth-aw/Aktuelles/Veroeffentlichungen/Forschungsbericht/Forschungsbericht_2018_Internet.pdf. Zugegriffen: 23. März 2019.

Papenfuß, F. (o. D.). *IPNetInfo*. Hannover, Bundesrepublik Deutschland & Heise Media GmbH & Co. KG. https://www.heise.de/download/product/ipnetinfo-38542?hg=1&hgi=0&hgf=false. Zugegriffen. 25. März 2019.

Powell, J., Gup, A., & Sager, N. (13. December 2018). *Neue Funktionen in ArcGIS API 4.10 für JavaScript (Dezember 2018)* (ESRI, Hrsg.). Redland, USA. https://www.esri.com/arcgis-blog/products/js-api-arcgis/announcements/whats-new-in-arcgis-api-for-javascript-4-10-december-2018/. Zugegriffen: 17. März 2019.

Qitterer, B. (o. D.). *Aerofotografie – 360 Grad 3D Kamera* (AeroFotografie, Hrsg.). München, Bundesrepublik Deutschland. https://www.aerofotografie.de/360-grad-3d-kamera/. Zugegriffen: 5. Apr. 2019.

Schulze, B. (o. D.). *Marine Traffic Deutsch – Schiffsverfolgung mit dem Schiffsradar von Marine Traffic*. Welzow, Bundesrepublik Deutschland. https://schiffsradar.net/marine-traffic/#radar. Zugergriffen: 8. Apr. 2019.

Schwermann, R., & Effkemann, C. (o. D.). *Photogrammetrie/Laserscanning* (R.-W. T. Aachen, Hrsg.). Aachen, Bundesrepublik Deutschland. https://www.gia.rwth-aachen.de/node/254. Zugegriffen: 24. März 2019.

Tsuchiya, B. (Dezember 2007). *Laser-Scanning in der Architektur* (D. B. GmbH, Hrsg.). München, Bundesrepublik Deutschland & Beck. *Detail – Zeitschrift für Achitektur und Baudetail, 12*(2007), 1498–1499. http://www.illustrated-architecture.de/resources/1498_technik_Detail.pdf. Zugegriffen: 24. März 2019.

Webfleet Solutions B.V. (2018). *TomTom Webfleet – preisgekrönte Ortung. Orten Sie Ihre Fahrzeuge 24/7 in Echtzeit und sparen Sie bis zu 20% Kosten* (Webfleet Solutions B.V., Hrsg.). Amsterdam, Niederlande. https://www.webfleet.com/de_de/webfleet/lp/tomtomtelematics/tomtom-ortung/?&gclid=Cj0KCQiA9orxBRD0ARIsAK9JDx-Q8zTQLgYiNnqp9oTS_wzCOf593eCVdpi2I5XrJ6U8wQkgZtu6yuJAaAmuIEALw_wcB. Zugegriffen: 8. Apr. 2019.

Wittmund, Landkreis. (2018). *Kooperative Regionalleitstelle Ostfriesland (KRLO).* (L. Wittmund, Hrsg.). Wittmund, Bundesrepublik Deutschland. http://www.krlo.de/. Zugegriffen: 23. Apr. 2019.

World Meteorological Organisation – CBS Expert Team für WIS GISCs und DCPCs. (5. Oktober 2005). *ISO 191xx Reihe von Geoinformationsstandards*. Genf, Schweiz. https://webcache.googleusercontent.com/search?q=cache:on2Opj9yIMUJ, https://www.wmo.int/pages/prog/www/TEM/ET-WISC-I/ISO_191xx.doc+&cd=14&hl=de&ct=clnk&gl=de. Zugegriffen: 2. Apr. 2019.

Zotow, N., & Urbanki, A. (26. Juni 2013). *So lesen Sie den Computer von Autos aus*. München, Bundesrepublik Deutschland. München: PC Welt. https://www.pcwelt.de/ratgeber/Wie-in-der-Werkstatt-So-lesen-Sie-die-Schnittstelle-von-Autos-aus-6587706.html. Zugegriffen: 20. März 2019.

Zoller & Fröhlich. (2018). *Z+F IMAGER 5010C, 3D Laserscanner* (Z&F GmbH, Hrsg.). Wangen, Bundesrepublik Deutschland. https://www.zf-laser.com/Z-F-IMAGER-R-5010C.3d_laserscanner.0.html. Zugegriffen: 30. März 2019.

Warum automatische Verfahren bei der Detektion von Hate Speech nur die halbe Miete sind

Konstanze Marx

1 Hate Speech und ein breites Bedeutungsspektrum

Hate Speech ist ein Phänomen, das spätestens seitdem das Netzwerkdurchsetzungsgesetz verabschiedet worden ist, in den öffentlichen Diskurs gelangt ist. Im Rahmen dieses Gesetzes sind Betreiber Sozialer Netzwerke angehalten, ein transparentes Beschwerdemanagement in Bezug auf rechtswidrige Inhalte zu den folgenden Tatbeständen zu etablieren:

- § 86 StGB: Verbreiten von Propagandamitteln verfassungswidriger Organisationen
- § 86a StGB: Verwenden von Kennzeichen verfassungswidriger Organisationen
- § 89a StGB: Vorbereitung einer schweren staatsgefährdenden Gewalttat
- § 91 StGB: Anleitung zur Begehung einer schweren staatsgefährdenden Gewalttat
- § 100a StGB: Landesverräterische Fälschung
- § 111 StGB: Öffentliche Aufforderung zu Straftaten
- § 126 StGB: Störung des öffentlichen Friedens durch Androhung von Straftaten
- § 129–§ 129b StGB: Bildung krimineller Vereinigungen, Bildung terroristischer Vereinigungen, Kriminelle und terroristische Vereinigungen im Ausland
- § 130 StGB: Volksverhetzung

K. Marx (✉)
Universität Greifswald, Greifswald, Deutschland
E-Mail: Konstanze.Marx@uni-greifswald.de

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

T.-G. Rüdiger und P. S. Bayerl (Hrsg.), *Cyberkriminologie,*
https://doi.org/10.1007/978-3-658-28507-4_27

- § 131 StGB: Gewaltdarstellung
- § 140 StGB: Belohnung und Billigung von Straftaten
- § 160 StGB: Beschimpfung von Bekenntnissen, Religionsgesellschaften und Weltanschauungsvereinigungen
- § 184b StGB: Verbreitung, Erwerb und Besitz kinderpornographischer Schriften, in Verbindung mit
- § 184d Zugänglichmachen pornographischer Inhalte mittels Rundfunk oder Telemedien; Abruf kinder- und jugendpornographischer Inhalte mittels Telemedien
- § 185 StGB: Beleidigung
- § 186 StGB: Üble Nachrede
- § 187 StGB: Verleumdung
- § 201a StGB: Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen
- § 241 StGB: Bedrohung
- § 269 StGB: Fälschung beweiserheblicher Daten

Es handelt sich hier um eine lange Liste. Hate Speech jedoch taucht nicht explizit auf, was die Frage aufwirft, wo genau Hate Speech hier anzusiedeln ist. Hate Speech, so ist man sich im interdisziplinären Diskurs weitestgehend einig, ist der *„sprachliche[n] Ausdruck von Hass gegen Personen oder Gruppen […], insbesondere durch die Verwendung von Ausdrücken, die der Herabsetzung und Verunglimpfung von Bevölkerungsgruppen dienen“* (Meibauer 2013, S. 1). Wagt man aber einen Blick in die diskursive Verhandlung von Hate Speech z. B. auf Twitter, fallen recht unterschiedliche Auffassungen – man könnte auch *Ethnokategorien* sagen – von Hate Speech auf. Ich habe das in Marx (2017b, 2018) ausführlich diskutiert und stelle die Argumentation daher hier nur zusammenfassend dar.

So kann man im Prinzip von Paralleldiskursen sprechen, die grob zwei Perspektiven auf vergleichbares sprachliches Material erkennen lassen. Die Hate Speech-Etikettierung wird erstens als Instrument dafür begriffen, Meinungsäußerungen als Rechtsverstoß zu deklarieren. Die Vertreter*innen dieser ersten Perspektive kommen gleichzeitig als Produzent*innen des fraglichen sprachlichen Materials infrage und verteidigen damit ihre eigenen Äußerungen. Sie setzen Hate Speech mit dem Aussprechen unerwünschter Wahrheiten gleich, mit Widerspruch, Meinungsverschiedenheiten oder mit Kritik. Alle diese Interpretationen laufen in etwa in der Bedeutung „unerwünschte nicht öffentlichkeitstaugliche Gegenrede“ zusammen. Ein Beispiel dafür ist (1):

(1) Wann wird aus Kritik Hatespeech? Komischerweise immer genau dann, wenn ihr anderer Meinung seid:^) #againsthatespeech, (TW, 2016-11-17, K1, T1, L3)[1]

Dass Hate Speech keinesfalls als Kritik verharmlost werden kann, lässt sich klar daran festmachen, dass Kritik gänzlich ohne Verbalagressivitäten, Schuldzuweisungen, allgemeine Diskreditierungen oder Stereotypkodierungen auskommt. Eine neue Bedeutungskomponente wird markiert, wenn Hate Speech als NORMALFALL deklariert wird, wie in (2).

(2) Wer im Internet present ist und sich durch #Hatespeech angegriffen fühlt hat dort nichts zu suchen. (2017-05)

Dieser Tweet mag als Anspielung auf den raueren Umgangston im Netz (Feldweg et al. 1995, S. 143; Kleinke 2007, S. 311–336) zu verstehen sein, was gleichzeitig die Hate Speech-Problematik verharmlosen würde. Der vielzitierte „raue Umgangston“ jedoch weist Nuancen auf, die es zu differenzieren gilt. Dass das Konzept Hate Speech konsequent überstrapaziert wird, zeigt denn auch Beispiel (3) deutlich:

(3) War das von Lammert am Freitag nicht eigentlich auch #HateSpeech!? (TW, 2017-06)

Der Bundestagspräsident hatte gegenüber Erika Steinbach am 30. Juni 2017 klargestellt, dass Bundestagsabgeordnete Entscheidungen unabhängig von Freigaben durch Fraktionen und Parteien treffen und Gewissensentscheidungen einzig von der Instanz „jeweiliger Bundestagsabgeordneter“ abhängig seien, eine im Zusammenhang mit Hate Speech vollkommen unverdächtige Äußerung also.[2] Selbst der deutliche Verweis vom Rednerpult, an das Erika Steinbach noch einmal herantreten wollte, enthält keinerlei Despektierlichkeiten, sondern spiegelt nur die Einhaltung der Regeln, die für alle Redner*innen im Bundestag gelten. Exemplarisch dafür, dass im Diskurs eine große Unsicherheit darüber artikuliert wird, wie Hate Speech zu definieren sei, ist Beleg (4).

---

[1]Die Quellenangaben für die Beispiele setzen sich zusammen aus einem Kürzel für die jeweilige Soziale Netzwerk-Seite (*TW* steht für *Twitter*), dem Erscheinungsdatum und den Social Media-Funktionen für Kommentare *(K),* Retweets oder Teilen *(T)* und Like(s) *(L).*

[2]u. a. hier nachzuvollziehen: https://www.focus.de/politik/videos/abstimmung-ueber-ehe-fuer-alle-im-bundestag-als-erika-steinbach-mit-merkel-abrechnet-erteilt-ihr-norbert-lammert-eine-lektion_id_7301515.html.

(4) Lasst uns #Hatespeech sperren! Was ist das eigentlich? Wissen wir auch nicht so genau … aber es gehört gesperrt. (TW, 2017-05)

Das wird zum Anlass genommen, mit der Bedeutung zu spielen, sie polemisch in alle Richtungen auszuweiten, und damit das dahinterstehende Konzept ad absurdum zu führen. Wenn hier vorgetäuscht wird, dass jede noch so harmlose Äußerung, jede berechtigte Kritik, jeder nachweisbare Fakt und die Wahrnehmung eines demokratischen Grundrechts (seine Meinung frei zu äußern) mit Hate Speech gleichzusetzen sei, wirkt das auf die Diskriminierungsdebatte zurück, die als nicht zielführend, ja diffus markiert wird.

Zweitens ist die Hate Speech-Etikettierung mit der oben genannten interdisziplinären Definition kompatibel und knüpft an Volksverhetzung, Rassismus und/oder Diskriminierung an. Dabei wird Hate Speech als Form der Hetze klar von freier Meinungsäußerung unterschieden:

(5) #againsthatespeech? Aber dann darf ich ja nicht mehr als Meinung getarnte Volksverhetzung betreiben! Mimimi! (TW, 2016-11)

(6) Plumpe Hetze gegen Minderheiten, weil man was weis ich für Probleme hat, sind keine Meinung, sondern nur Hass #againsthatespeech (TW, 2016–11)

Die Vertreter*innen der zweiten Perspektive kommen als Adressat*innen für Hate Speech infrage oder als Regulierungsinstanzen. Tweets wie (5) und (6) bilden das andere Ende einer Skala, entlang derer verschiedene Auslegungen von Hate Speech anzusiedeln sind.

Mit Blick auf das im Diskurs zugewiesene vielgestaltige Deutungs- und Bedeutungsspektrum, kann man (vor)schnell zu dem Schluss gelangen, dass beinahe willkürlich ist, was unter Hate Speech zu verstehen ist. Zudem ist die Beobachtung wichtig, dass *Hate Speech* als Schlüsselbegriff sowohl in Kontexten auftauchen kann, die Hate Speech-Potenzial aufweisen als auch in Kontexten, die – ganz im Gegenteil – die Verwendung von Hate Speech kritisieren. Das alles erschwert oder besser: chaotisiert deren Identifikation. Diese wiederum ist aber eine wichtige Variable für die Umsetzung des Netzwerkdurchsetzungsgesetzes, in dessen Rahmen gefordert wird, die oben aufgelisteten sprachlich manifestierbaren Delikte zu enttarnen.

2 Eine Annäherung: Softwaregestützte Detektion

Angesichts der großen Menge an Daten, die derzeit sekündlich auf Sozialen-Netzwerk-Seiten entstehen, drängt sich die Überlegung geradezu auf, die Detektion von Hate Speech automatisiert anzugehen. An softwaregestützten Lösungen wird derzeit in einigen Forschergruppen gearbeitet, siehe etwa Paasch-Colberg et al. (2019) im Berliner BMBF-Verbundprojekt NOHATE[3], Jaki und de Smedt (2018), Hartung et al. (2017), Ferrara et al. (2016), Ashcroft et al. (2015), Kaati et al. (2015), Scanlon et al. (2014) oder Ting et al. (2013). Die Universität Colorado Boulder (USA) hat ein Tool entwickelt, mit dem Instagram gescannt werden kann und das Cybermobbing[4] zu 70 % entlarvt (Hosseinmardi et al. 2015).[5]

Das Modell von Hartung et al. (2017, S. 322) basiert auf lexikalischen und emotiven Mustern in bekannten deutschen rechtsextremen Profilen. Dazu werden Wort-Frequenzlisten (Bag of Words)[6] erstellt und Emotionen wie Wut, Ekel, Angst, Freude, Liebe, Traurigkeit, Scham, Überraschung und Vertrauen (vgl. Plutchiks 1980 „wheel of emotions“) markiert. Hierbei orientierten sich die Autor*innen an den Empfehlungen von Suttles und Ide (2013).[7] Darüber hinaus werden lexikographische Muster erfasst (z. B. *gegen* … <Substantiv> oder <Substantiv> … *statt* … <Substantiv>) sowie Merkmale der sozialen Identität,

[3]https://www.polsoz.fu-berlin.de/kommwiss/v/bmbf-nohate/project/index.html

[4]Cybermobbing und Hate Speech sind konzeptuell dahingehend zu unterscheiden, dass Cybermobbing sich oftmals an Personen innerhalb bereits existierender sozialer Kontexte richtet, während Hate Speech Personen aufgrund einer Zugehörigkeit zu einer Gruppe (Frauen, Geflüchtete, Homo- oder Transsexuelle) adressiert. Beide Phänomene sind jedoch dem großen Bereich Invektivität zuzurechnen und im Sinne des Netzwerkdurchsetzungsgesetzes relevant.

[5]https://www.colorado.edu/today/2018/06/11/squashing-cyberbullying-new-approach-fast-accurate

[6]Um Wörter in Algorithmen zu integrieren wird häufig der Bag-of-Words-Ansatz genutzt, in dessen Rahmen eine Sammlung aller relevanten Wörter erstellt wird. Relevant heißt im hier vorliegenden Fall, dass Wörter, die Twitterfunktionen bezeichnen, und sogenannte Stoppwörter (wie z. B. Artikel oder Pronomen) vor der Erstellung der Liste getilgt wurden.

[7]Suttles und Ide (2013) schlagen für die Klassifikation von Emotionen in Tweets binäre Klassifikatoren für vier Emotionspaare (Joy/Sadness; Anticipation/Surprise; Anger/Fear; Disgust/Trust) vor, weil Annotator*innen in den von ihnen durchgeführten Experimenten in einem großen Prozentsatz von Daten nicht nur eine, sondern mehrere Emotionen identifiziert haben.

die hier vor allem als kollektive Identität betrachtet wird (z. B. *unser[e|en|em|er|es]* … <Substantiv>). Im Ergebnis zeigt sich (dargestellt in Tab. 1) ein recht disparates Bild.

Insbesondere anhand der Ortsangaben (wobei die Variablen zur Differenzierung zwischen „local“ und „regional“ hier vernachlässigt werden), aber auch anhand von Wörtern wie *deutschland, durchgeführt* oder *spiegelonline* lässt sich vermuten, dass sie bei einer Suche nach Hate Speech vermutlich nicht zu einschlägigen Treffern führen.

Tab. 1 Die wichtigsten Merkmale aus einer globalen Liste von 100 Merkmalen, kategorisiert in Merkmalsklassen für die Kategorien N (für nicht-extremistisch) und R (rechtsextremistisch), entsprechend der Merkmalsgewichte im Modell bei Hartung et al. (2017, S. 324), hier inhaltlich übernommen

	Category N	Category R
Words	Heute, wir, beim, s, the, uhr, geht, für die, to, of, glückwunsch, Stellenangebot, feuerwehren, morgen, danke	d18, deutschland, #wehrdich, brd, deutsche, DTL, asylanten, Bürgerinitiative_wir, demonstration, asyl, herbstoffensive, asylbewerber, durchgeführt..!, volk, !..!
Network	Nabu, ldkth, awo, mikemohring, bodoramelow, mdr_th, cdu_franktion, naju, lmvth, der_AWO, lakoth16, DGB_Jugend, jef_de, dgb, bund_net	NPD, FN, suegida, identiäreaktion, weimarticker, sternde, spiegelonline, der_NPD, goldenerlöwe, npdde, Thüringer_NPD, agnordost, antifa, NPD-Landesverband, AB_ERFURT
Local	Erfurt, in_Erfurt	Hildburghausen, Jena, nordhausen, Saalfeld, Erfurt_), suhl, Webetgasse, Bauvereinstraße, Hußstraße, Gera_Zschochernstraße
Regional	Thüringen, thüringer, in_Thüringen, r2g, hochwasser, gebietsreform	Kyffhäuserkreis, wir_lieben, lieben_Thüringen
National/global	TTIP, #mitredeneu, Bund, ews2014	#merkelmussweg, genozid
Emotionality	– None –	EMO_TWEETS_PROP > 0.3, MOST_FREQ_EMOTION = Disgust

Jaki und de Smedt (2018, S. 3), die eine beachtliche Trefferquote ihres Systems von 84 % erzielen, haben ein 55.000 Tweets umfassendes Trainingskorpus[8] folgendermaßen zusammengestellt. Zunächst wurden manuell 112 subversive Twitter-Profile ermittelt. Als subversiv gelten Profile dann, wenn die Posts wiederholt rassistische Beleidigungen, Obszönitäten und gewalttätige Rhetorik enthielten und Indikatoren für eine rechtsextreme Ideologie aufwiesen, entweder direkt in der Profilbeschreibung oder indirekt (z. B. durch kodierte Sprache oder visuelle Metaphern). Die Profile wurden auf der Grundlage von abfälligen (auch: einschlägigen) Schlüsselwörtern ausfindig gemacht. Wenn dann ein Profil abfällig über Geflüchtete berichtete oder mindestens drei Tweets aufwies, die als beleidigend oder illegal kategorisiert werden konnten, wurde das Profil in den Datenpool integriert.

Interessant ist nun insbesondere dieser erste, der automatischen Bearbeitung vorgelagerte Schritt (bei Hartung et al. 2017 beträfe das die Erstauswahl der zu untersuchenden Profile), weil er so voraussetzungsreich ist.

Möchte man nämlich festlegen, was Hate Speech eigentlich ist, stößt man auf drei Problemfelder (siehe auch Marx 2019, S. 7), die im Folgenden ausdifferenziert werden sollen:

1. Äußerungen, die auf der sprachlichen Oberfläche keine Hate Speech-Merkmale aufweisen, können Hate Speech sein.
2. Äußerungen, die auf der sprachlichen Oberfläche Hate Speech-Merkmale aufweisen, müssen nicht Hate Speech sein.
3. Hate Speech tritt nicht notwendigerweise da auf, wo wir es vermuten.

3 Problemfelder bei der Identifikation von Hate Speech

3.1 Hate Speech ohne ostentative Hate Speech-Merkmale

Um die Schwierigkeiten in Problemfeld 1 zu illustrieren, möchte ich zwei Beispiele heranziehen:

(7) WIR SCHAFFEN DAS! („Face with Symbols on Mouth“-Emoji) (TW, @ Beatrxi_vStorch, 2018-04-07, K: 953, T: 137, L: 646)

[8]Ein 20.000 anonymisierte Tweets und 2000 Bilder umfassendes Subkorpus, das sogenannte POLLY-Korpus, ist für Studienzwecke öffentlich zugängig (De Smedt und Jaki 2018).

(8) Auf seine Zunge sind 200.000 Euro ausgelobt. Eine Praktik aus den Neunzigern in Russland. Ich würde an eure Sicherheit denken, anstatt plumpe Lügen zu verbreiten… sonst heißt es doch bald: je suis correctiv

Das erste Beispiel (Beleg 7) entstand im April 2018 unmittelbar nachdem bekannt geworden war, dass ein den letzten Ermittlungsständen zufolge psychisch kranker Mann sein Auto in eine Menschenmenge in der Münsteraner Innenstadt gesteuert hatte. Er wurde auf dem Twitter-Account der AfD-Politikerin Beatrix von Storch veröffentlicht. Auffällig sind nicht nur die Majuskeln, die in der Literatur mit hoher Lautstärke in Verbindung gebracht werden (siehe z. B. Loos 2011, S. 118), sondern auch das die Expressivität verstärkende Ausrufezeichen sowie ein „Face with Symbols on Mouth"-Emoji, das Fluchen oder einen plötzlichen Wutausbruch indiziert. Es handelt sich hier um die Wiederaufnahme eines Satzes, der zuerst in der Bundespressekonferenz am 31. August 2015 von Angela Merkel geäußert wurde und zwar als motivierendes Signal im Kontext der Flüchtlingspolitik.[9] Er wurde sowohl von Vertretern und Vertreterinnen der Willkommenskultur aufgegriffen als auch zynisch bedeutungsverkehrt von der rechtspopulistischen und rechtsextremen Bewegung mit der Nebenbotschaft, dass die Flüchtlingspolitik von Angela Merkel versagt.[10] An eben diese Komponente knüpft Frau von Storch hier an und dass sie richtig verstanden wird, lässt sich an den Kommentaren ablesen. Es gibt hier Personen, die die Einladung zur Hetze annehmen, wie in Beispiel (9):

(9) das wird der dicken deutschen Stasi Merkel grosse Freude bereiten Blut auf den Strassen zu sehen. Ich würde es mit ihrer hässliche Fratze aufwischen. (TW, 2018-07-04, K:0, RT:1, L:2, Antwort an @Beatrix_vStorch)

Es gibt Personen, die die Politikerin aufgrund ihrer Pietätlosigkeit kritisieren (10) und ihren Tweet klar als *Angst, Hass* und *Hetze* (11) kategorisieren.

(10) Ekelhafter Tweet! (TW, 2018-07-04, K:0, RT:0, L:3, Antwort an @Beatrix_vStorch)

(11) Angst/Hass/Hetze von Beruf. Du arme Wurst… Der Täter lebte etwa 100 Meter von meiner Tochter. Ich kotze nicht fremdenfeindlichen durch die Welt. Echt, geh Du zum Psychologen. (TW, 2018-07-04, K:0, RT:0, L:3, Antwort an @Beatrix_vStorch)

[9] https://www.bundesregierung.de/breg-de/aktuelles/pressekonferenzen/sommerpressekonferenz-von-bundeskanzlerin-merkel-848300

[10] Für einen mikrohistorischen Überblick zu den jeweiligen Äußerungssituationen: https://www.n-tv.de/politik/Wie-ein-Satz-zur-Provokation-wurde-article20600602.html.

Gleichgültig aber, welcher Gruppe von Personen, die Kommentator*innen hier angehören, sie dekodieren den Tweet der AfD-Politikerin problemlos als Hass, dabei ist die Phrase *Wir schaffen das* eigentlich (und insbesondere für automatische Detektionsverfahren) unverdächtig, enthält sie doch keinerlei vulgäres oder volksverhetzendes sprachliches Material. Die Identifikation dieses Kommentars als Hass erfolgt nämlich unter Zuhilfenahme komplexer Rezeptionsstrategien.

Beim Verstehen eines Textes ist selbstverständlich die wortwörtliche textuelle Information hochrelevant, sie ist aber nur eine Komponente bei der Erstellung einer mentalen Repräsentation (eines sogenannten *Textweltmodells,* dazu Schwarz 2008[3], S. 197–199), wenn Lesende die Bedeutung eines Textes erschließen wollen. So spielen bei der Erstellung des Textweltmodells auch der unmittelbare Kontext (der nicht sprachlich sein muss) und Weltwissen, das im Langzeitgedächtnis zur Verfügung steht, eine wichtige Rolle. Dass sich Weltwissen im Langzeitgedächtnis etabliert, kann Resultat diskursiver Prozesse sein. Leser*innen, die den Tweet des Accounts Beatrix_vStorch zur Kenntnis nehmen, lesen also nicht nur den Text, sondern berücksichtigen auch den Namen des Profils und das Wissen über die vermutlich dahinter agierende politische Person. Erkannt wird auch das Muster einer Amokfahrt, was dazu führt, Erfahrungen mit Amokfahrten in der Vergangenheit zu aktivieren und konkrete Terroranschläge z. B. in Nizza oder Berlin an das Ereignis in Münster anzubinden.[11] Dabei ist das konkrete Ereignis in Münster gar nicht Teil der textuellen Botschaft. Vielmehr wird anhand des Tweet-Zeitpunkts unmittelbar nach dem Ereignis eine Verknüpfung zwischen dem Inhalt des Tweets und dem Ereignis aufgebaut. Aktiviert wird auch, dass dem Satz *Wir schaffen das* nicht nur die Bedeutung der ‚Bewältigung einer Sache' inhärent ist, sondern dass diesem Satz im rechtspopulistischen Diskurs eine andere Deutung zugeschrieben wird, die sich in etwa so paraphrasieren lässt: „Wir schaffen das nicht/Wir scheitern/‚Das' bedeutet Kriminalität/Terror/Gewalt/Bedrohung" ö. ä. und als kritische bis hetzerische Referenz auf die Urheberin der Äußerung, die Bundeskanzlerin Angela Merkel, gilt.

Dieses (beim Lesen des Tweets) aktivierte Wissen trägt damit zu einer spezifischen Interpretation des Satzes bei: Der Personenreferent *wir* exkludiert die Rolle der Produzentin (hier Beatrix von Storch), d. h. dass deutlich wird, dass nicht @Beatrix_vStorch von einem *wir* spricht, sondern mit dem *wir* eine vage

[11]Informationen zur Amokfahrt in Münster: https://de.wikipedia.org/wiki/Amokfahrt_in_Münster, zum Anschlag in Nizza: https://de.wikipedia.org/wiki/Anschlag_in_Nizza und zum Anschlag in Berlin: https://de.wikipedia.org/wiki/Anschlag_auf_den_Berliner_Weihnachtsmarkt_an_der_Gedächtniskirche.

Menge inklusive der Bundeskanzlerin Merkel, die ja quasi zitiert wird und der Personen, die eine Willkommenskultur vertraten und vertreten, gemeint ist. Dieser Menge von Personen wird Verantwortung und damit auch Schuld (am Scheitern = nicht bewältigen) zugewiesen.

Als Sachverhaltsreferent (hier versprachlicht durch das ursprünglich komplex-anaphorisch[12] verwendete Demonstrativpronomen: *das*) gilt nicht mehr die erfolgreiche Integration von Flüchtlingen. Vielmehr wird die prinzipiell referenzielle Offenheit des Pronomens dafür genutzt, ein konkretes Ereignis zu referenzialisieren. Die ontologische Struktur dieses Ereignisses „Münster" wird dabei adaptiert, und auf bereits nach diesem Muster erfolgte Ereignisse übertragen. Münster wird also als Anschlag klassifiziert. Die verbale Verknüpfung *schaffen* – die ich hier mit *bewältigen* paraphrasieren möchte – wird damit negiert.

Es ist nun wichtig sich klarzumachen, dass es Menschen sind, die all diese Interpretationsprozesse ad hoc durchlaufen. Dabei ist noch völlig ungeklärt, wie genau die anderen semiotischen Ressourcen – in unserem Fall die spezifischen Bedeutungselemente des Emojis, aber auch die Typographie – Teil dieser Rekonstruktionsprozesse sind.

Ich komme nun zum zweiten Beispiel (Beleg 8), einer Nachricht, die an das journalistische Recherche-Team Correctiv ging.[13] Auch hier lassen sich an der sprachlichen Oberfläche keine auffälligen (im Sinne von diskriminierenden, rechtextremistischen, vulgären, obszönen oder beleidigenden) Wörter oder Wortverbindungen feststellen. Dennoch liegt hier eine perfide Drohung vor, die über komplexe Schlussfolgerungsprozesse (Inferenzen) rekonstruiert werden muss. So wird zunächst über zwei Feststellungen *Auf seine Zunge sind 200.000 ausgelobt* und *Eine Praktik aus den Neunzigern in Russland,* die nicht explizit miteinander verknüpft werden, ein Gewaltszenario skizziert, wobei eine „ausgelobte Geldsumme" die Assoziation mit einer offiziellen Fahndung mitaktiviert, ein Schema, das jedoch durch die Erwähnung der *Zunge* in Kombination mit einer *Praktik aus Russland* konterkariert wird. Dennoch kann hier der Versuch einer

[12]Komplex-Anaphern sind Wiederaufnahmeformen in Texten, die nicht auf einzelne Referenten Bezug nehmen, sondern auf ganze Sachverhalte. Mit *das* wird in der ursprünglichen Äußerung zum Beispiel auf die Aufgabe, die geflüchteten Menschen aufzunehmen und ihnen Hilfe zukommen zu lassen, referiert. *Das* bezeichnet hier nicht einfach einen sächlichen Gegenstand (siehe dazu Marx 2011).

[13]Diesen Beleg hat mir dankenswerterweise Hanna Gleiß von der zivilgesellschaftlichen Vernetzungsstelle gegen Hate Speech und für eine positive Debattenkultur im Internet DAS NETTZ zur Verfügung gestellt.

Legitimierung mitgelesen werden, weil die Person, die hier eigentlich bedroht wird, als Täter*in stilisiert wird. Es zeigt sich hier die typische Täter-Opfer-Umkehr (dazu u. a. Schwarz-Friesel und Reinharz 2013, S. 348), die in unterschiedlichen Kontexten (verbaler) Gewalt eingesetzt wird, um Gewalt als gerechtfertigt oder logische Konsequenz darzustellen. Es folgt eine persönlich formulierte Empfehlung *(ich würde),* die eine für Drohungen konstitutive Bedingung (in diesem Fall: keine *plumpe[n] Lügen [mehr] zu verbreiten*) transportiert. Damit geht die Unterstellung einher, Correctiv verbreite Lügen, was im darauf folgenden *sonst* noch einmal implizit als einzustellende Handlung subsumiert wird. Die Formel *Je suis x* ist eine typische Reaktion, mit der Nutzer*innen Sozialer Netzwerke ihre Solidarität mit den Opfern von Terroranschlägen bekunden und ihrer Trauer Ausdruck verleihen. Sie hat sich im Kontext des Anschlags auf die französische Satirezeitschrift Charlie Hebdo etabliert. Wird das *x* nun durch *Correctiv* ersetzt, wird damit impliziert, dass Correctiv einem Anschlag zum Opfer fallen wird.

Die Frage ist, wie derart komplexe, den unmittelbaren und mittelbaren Kontext und diskursives Wissen integrierende Prozesse in maschinelle Systeme implementiert werden können? An diesen Beispielen wird meines Erachtens sehr deutlich, wie wichtig das Wissen um diskursive Deutungsmodifikationen aber auch diskursive Traditionen ist, um Hate Speech zu identifizieren. In die Erstellung von Trainingskorpora für die automatische Detektion müssten also größere Einheiten als Wörter oder N-Gramme (üblicherweise Wortverbindungen bis zu drei Wörtern) einbezogen werden.

3.2 Hate Speech-Merkmale, aber keine Hate Speech

Nachdem oben aufgezeigt wurde, dass Hate Speech sich nicht notwendigerweise an der sprachlichen Oberfläche nachweisen lässt, möchte ich mich nun einem Beispiel zuwenden, dessen sprachliche Oberfläche salopp formuliert „Hate Speech verdächtig“ ist, dennoch liegt hier keine Hate Speech vor.

Es handelt sich hier um ein Exzerpt aus einem WhatsApp-Chat aus dem Korpus, das meinem Buch „Diskursphänomen Cybermobbing“ (Marx 2017a, S. 225) zugrunde liegt.

(12)

24	11:40:23	**B**	Du bist voll eklig du sau
			[Bilder werden hin und her geschickt]
25	11:44:13	**B**	Oh mann!

26	11:44:52	**B**	C du stricher!
27	11:44:53	**A**	Ist doch witzig
28			C hat verlassen
29	11:44:59	**A**	Noob
30	11:45:02	**A**	HURENSOHN
31	11:45:04	**A**	Spast ey
32	11:45:07	**A**	Leavt einfavh
33	11:45:08	**A**	Opfer
34 35	11:45:16 11.45:31	**A** **B**	Kackkind Kann seine Mitgliedschaft vergessen, NEUWAHLEN!

In diesem kurzen Ausschnitt ist nahezu das gesamte Repertoire an sprachlichen Ausdrücken, Realisierungsformen und Mustern zu finden, die als typisch für Cybermobbing gelten: Dehumanisierende Metaphern *(du sau),* pejorativ attribuierte Diminuierungen *(kackkind),* derbe Beschimpfungen *(Hurensohn)* in für die Emphase im interaktionsorientierten Schreiben typischen Majuskeln oder die Degradierung als *Opfer.* Hier liegt jedoch weder Hate Speech noch Cybermobbing vor, sondern sogenanntes *Bantering* (u. a. Labov 1972; Alexander et al. 2012) oder auch *Dissen* (dazu Deppermann und Schmidt 2001, S. 79 u. a.). Es zeigt sich in Verbal-Duellen, in denen sich die Beteiligten einer Peergroup spielerisch herabsetzen, um ihren Status innerhalb der Gruppe und über gruppeninterne Angemessenheitsnormen zu verhandeln. Im Beispiel wäre das etwa die Adressierung *du stricher!*. Typischerweise bewegen sich die Interagierenden dabei jenseits von Tabugrenzen (vgl. dazu Bahlo 2012; Schmidt 2004 u. a.), es geht aber nicht darum, Gewalt tatsächlich auszuüben. Gewalt hätte vermutlich die Gruppenspaltung zur Folge, Verbalduelle mit Banterfunktion hingegen stärken den Gruppenzusammenhalt. Sie sind kein spezifisches Phänomen unter Heranwachsenden, sondern sind auch unter Erwachsenen (z. B. in Großküchen, dazu Alexander et al. 2012 oder in Krankenhäusern, dazu Grainger 2004) gut dokumentiert.

Es ist deshalb auch wichtig, bei der Analyse die Beziehung der Interagierenden in den Blick zu nehmen, pragmatische und soziale Aspekte dürfen schlicht nicht ausgeblendet werden, vor allem dann, wenn Metaphern, wie *Das Wort als Waffe* oder *die Macht der Sprache* verwendet werden, die in vergleichbaren Fällen Schlobinski (2017) zufolge zu kurz greifen.

3.3 Wo müssen wir eigentlich nach Hate Speech suchen?

Ein drittes Problemfeld eröffnet sich nun mit Blick auf die Bedingung, Hate Speech sei einzig ein Problem der Sozialen Netzwerke, die im Netzwerkdurchsetzungsgesetz als gegeben vorausgesetzt wird, auf deren Grundlage aber auch automatisierte Detektionsinstrumente entwickelt werden.

Hate Speech ist – obgleich das Phänomen ubiquitär erscheint – nicht nur in Sozialen Netzwerken relevant und kann deshalb – selbst wenn die unter Abschn. 3.1 und 3.2 benannten Probleme gelöst sind – nicht umfassend erhoben und untersucht werden, wenn nicht Aktionen und Interaktionen in Onlinespielen aber auch Republikationen von Betroffenen in die Betrachtung integriert werden. Ich wende mich zunächst den Onlinespielen zu: So muss z. B. gefragt werden, wann und wie eigentlich Kinder mit diskriminierenden Äußerungen in Berührung kommen, die dann z. B. in Cybermobbingdaten wieder auftauchen (Marx 2013), obgleich der Erfahrungshorizont der Kinder im Grundschulalter normalerweise keine vergleichbaren Konzepte umfassen kann. Fündig wird man dann – wie sollte es anders sein – in Spielen mit Interaktionsfunktion, wie z. B. *Clash of Clans*. Das Nutzungsmindestalter beträgt 13 Jahre, wird aber oft deutlich unterschritten. Das merke ich immer dann, wenn ich mit vierten und fünften Klassen arbeite. Hier können die Kinder auf antisemitische Clannamen, wie *Judenhasser, Judenjäger, Judenklaue* stoßen, auf Gamernamen, wie *AdolpfH* oder *Himmler* (vgl. Rüdiger 2016), und sie können mit diskriminierender und dispektierlicher Sprache konfrontiert werden, z. B. *ich fick alle eure Mutter ihr seit hurensohne* usw. Selbst in Spielen, die ab 0 freigegeben sind, wie z. B. Moviestarplanet, finden sich Namen wie *adolf # fitler, Adolf # Hiter* oder *Adolf # Hilter,*[14] siehe auch Beispiel (13).

> (13) Was ist mit manchen Gamer_innen bloß los? Denen sollte @PlayStationDE jahrelang den Zugang sperren #WTF [plus Screenshot, der den Namen X_Adolf-Clitler_X in einer Spielumgebung zeigt] (TW, 2019-06-07, K:0, T:1. L:9)

Es ist nicht nur problematisch, dass Wörter mit volksverhetzendem und damit unter Umständen strafrechtlich relevantem Potenzial verwendet und

[14]Vgl. dazu einen Tweet vom Mitherausgeber dieses Bandes, Thomas Gabriel Rüdiger, vom 2. Juni 2019 (https://twitter.com/TGRuediger/status/1135274335248224257), der einen Screenshot enthält und in dem die Bedeutung von Interaktionsrisiken in Onlinegames hervorgehoben und für das Netzwerkdurchsetzungsgesetz relevant gesetzt wird.

entsprechende Konzepte in Spielumgebungen aufgerufen werden. Darüber hinaus muss auch der Zeitpunkt betrachtet werden, zu dem Kinder damit konfrontiert werden. Das ist oftmals dann der Fall, wenn Geschichte oder politische Weltkunde noch gar keine Unterrichtsfächer sind oder man bei weitem noch nicht zu diesen brisanten Themen vorgedrungen ist. Die Schüler*innen haben also gar keine Folie, vor der sie solche Äußerungen einordnen können. Diskriminierungen und verbale Gewalt gelangen so unter Umständen unreflektiert als Gamer*innen-Jargon in das sprachliche Repertoire von Kindern und Heranwachsenden und zwar gänzlich unbeachtet von automatisierten Detektionsverfahren, deren Suche auf Soziale Netzwerk-Seiten beschränkt wird.

Ein zweiter zu bedenkender Punkt in diesem Problemfeld ist, dass gerade Hassdaten oft nur deshalb zugänglich werden, weil sie re-publiziert werden, wie etwa in diesem Fall von dem Sprachwissenschaftler Anatol Stefanowitsch.

(14) Werde jetzt mein Buch verbrennen und mein Leben überdenken… (TW, @astefanowitsch, 2018-04-02, K:90, T:140, L: 1,2 Tsd.) [als Screenshot eingefügt:

From [geschwärzt]
Subject Ihr Buch „Eine Frage der Moral“
To [geschwärzt]
Guten Tag, Herr „Professor“ Stefanowitsch,

ich habe ihr Buch nicht gelesen, für Ihren als Pseudowissenschaft verbrämten Sprachfaschismus ist mir meine Zeit zu kostbar. Nichtsdestotrotz möchte ich Sie auffordern, uns endlich in Frieden zu lassen mit Ihren Vorschriften und Gängeleien.

Wie Nietzsche so treffend sagte: „Wenn der Faschismus wiederkehrt, wird er nicht sagen, ich bin der Faschismus. Er wird sagen, ich bin der Antifaschismus“ oder, wie man heute sagen würde, „ich bin die political correctness“.

Sie und Ihre Kollegen, oder sollte ich sagen, „Kollex*innen“, sind für mich nicht besser als die Nazis als die Sie jeden beschimpfen, der eine andere Meinung vertritt. Ich würde ja sagen, gehen Sie zurück nach Russland und nehmen Sie Ihr Buch gleich mit, aber dort will man Menschen wie Sie erst recht nicht haben.

Also bleiben Sie weiter unser Gast und genießen Sie die Vorteile der Meinungsfreiheit, die Sie nach Kräften abschaffen wollen.

Mit „freundlichen“ Grüßen
Dr. Helmut [geschwärzt]]

(15) On 2018-04-02 18:08:22 [geschwärzt] wrote:

Sehr geehrter Herr Dr. N[geschwärzt],
Vielen Dank für Ihre Einschätzung eines Buches, das Sie nicht gelesen haben. Sie ist für mich wertvoll, weil sie gänzlich unbeeinflusst vom Gegenstand der Kritik und damit viel objektiver ist als die Einschätzung tatsächlicher Leser*innen.

Auch Ihre Gastfreundschaft rührt mich sehr, denn in Russland ist es ja gerade um diese Jahreszeit sehr kalt und da müsste ich mein Buch, das Sie nicht gelesen haben, womöglich verwenden, um mir ein wärmendes Feuer aus den Strohmännern anzuzünden, die ich E-Mails wie der Ihren entnehmen würde.

Eine Frage noch aus kollegialem Interesse: In welchem Fach haben Sie promoviert? Das zu wissen würde mir helfen, Ihre wertvolle Kritik noch besser zu würdigen.

Mit freundlichen Grüßen
„Prof." Dr. Anatol Stefanowitsch

(16) Die Gefühle müssen raus, Helmut, lassen Sie sich bitte nichts anderes einreden. [als Screenshot eingefügt:

From [geschwärzt]
Subject Re: Nachfrage zu Ihrer Kritik
To [geschwärzt]

Du Ratte hältst dich wohl für sehr witzig, machst dir auf unsere Kosten einen Lenz, und glaubst, du kannst dich über uns lustig machen.

Falls es dich wirklich interessiert, ich besitze einen Ehrendoktor der Wirtschaftswissenschaften, also einer echten Wissenschaft, von der linke Untermenschen wie du nichts verstehen.]

Anatol Stefanowitsch wird in zwei persönlich an ihn gerichteten E-Mails diskreditiert *(Pseudowissenschaft, Sie sind für mich nicht besser als die Nazis),* diskriminiert (*gehen Sie zurück nach Russland)* und beleidigt *(Ratte, linker Untermensch).*[15]

Jemand, der*die Hate Speech untersucht, wüsste von dieser E-Mail nichts, wenn Stefanowitsch sie nicht selbst auf Twitter veröffentlicht hätte. Die Hoheit

[15]Der Schreiber nimmt für seine Hass-Nachrichten Stefanowitschs 2018 veröffentlichtes Buch *Eine Frage der Moral. Warum wir politisch korrekte Sprache brauchen* zum Anlass.

darüber, mit welcher Datenqualität dann weitergearbeitet werden kann, liegt aber dann bei den Personen, die re-publizieren.

Stefanowitsch etwa anonymisiert. Hasnain Kazim, ein anderer Autor, der Hasspost veröffentlicht, zum Beispiel im Buch „Post von Karlheinz" (hier werden „wütende Mails von richtigen Deutschen" zusammengestellt) hat nicht nur anonymisiert, sondern auch „behutsam in Rechtschreibung und Grammatik redigiert", was die Daten für einen linguistischen Zugang nahezu unbrauchbar macht.

Wichtig ist auch, dass re-publizierte Daten, die insgesamt eine nicht zu unterschätzende Quelle sind, nicht ohne Kontext veröffentlicht werden. Im Falle von Anatol Stefanowitsch sind das Kommentare, wie *werde jetzt mein Buch verbrennen und mein Leben überdenken…* in (14) oder *Die Gefühle müssen raus, Helmut, lassen Sie sich bitte nichts anderes einreden* in (16), denen Stefanowitsch den Angriff als kathartische emotionale Entlastung rahmen kann. Es wird damit eine typische Praktik zur Re-Behauptung von Diskurspositionen durch betroffene Personen illustriert. In diesem Zusammenhang ist auch zu sehen, dass Stefanowitsch die Betreffzeile (16) von *Ihr Buch „Eine Frage der Moral"* (siehe 14) geändert hat in *Nachfrage zu Ihrer Kritik* und mit diesem Reframing unqualifizierte Hetze ironisch diminuieren kann. Eine Fortsetzung dieser – ich nenne es einmal „Hass-Mail-Dokumentation" – findet sich zudem in einem weiteren Tweet, in dem Stefanowitsch mit dem Hinweis *Helmut, wir sind berühmt* einen Artikel der Leipziger Volkszeitung verlinkt, in dem der Verlauf wiederum partiell zitiert ist.

Darüber hinaus wird durch die Veröffentlichung der Nachrichten – im Übrigen auch der E-Mail-Antwort (15) – auf die erste E-Mail in (14) von Stefanowitsch sichtbar, wie schnell es im Kontext von Hate Speech zur Eskalation kommt. Bereits in der zweiten E-Mail fallen alle zumindest die Form wahrenden Elemente weg: Es fehlen Anrede- und Abschiedsfloskeln, der Adressat wird nicht mehr gesiezt, die Anredeformen nicht mehr groß geschrieben und der Stil ist vulgär.

Im Kontext von Hate Speech sind also nicht nur einzelne Nachrichten relevant, sondern auch Interaktionssequenzen, die entsprechend berücksichtigt werden müssen. Der kurze hier zitierte Verlauf zeigt deutlich, dass wir uns nicht einem statischen Phänomen gegenüber sehen, sondern dass sich Hate Speech in der Interaktion dynamisch entwickelt und unterschiedliche Formen annehmen kann. Somit müssten theoretisch auch Interaktionsverläufe erfasst werden, die auf Sozialen Netzwerk-Seiten nicht notwendigerweise konzentriert repräsentiert sind. Erschwerend für die automatische Detektion kommt hinzu, dass betroffene Personen unter ethischen Aspekten vollkommen zurecht Bildschirmfotos verwenden, um Hass und Hetze keine weitere Verbreitung zu ermöglichen.

4 Fazit

Ich habe an drei Problemfeldern aufgezeigt, dass die automatische Detektion von Hate Speech durch qualitative Analysen ergänzt werden muss. Hate Speech ist nicht immer an der sprachlichen Oberfläche erkennbar und muss durch komplexe Schlussfolgerungsprozesse rekonstruiert werden. Vermeintlich typische Hate Speech-Merkmale an der sprachlichen Oberfläche können mit Blick auf spezifische soziale Konstellationen als gruppenstabilisierend identifiziert werden und wären in automatischen Erhebungen falsche Positive. Hate Speech tritt zudem in Umgebungen auf, die bislang keine Berücksichtigung gefunden haben, wie z. B. Onlinespiele (s. a. Kap. „Hate Speech in der Computerspielkultur“). Hate Speech wird aber auch in nicht automatisch durchsuchbaren Formaten re-publiziert und bleibt dann selbst auf Plattformen verborgen, auf denen automatisierte Detektion recht gut zu funktionieren scheint.

Es zeigt sich gerade an solchen Fällen, dass es unerlässlich ist, als Forscher*in in den relevanten Umgebungen präsent zu sein. Spielumgebungen, in denen sich Kinder bewegen, können nicht als Verbreitungsräume für extremistisches Gedankengut identifiziert werden, plattforminhärente Regeln auf Instagram, Twitter, Facebook und Co. können nicht erkannt werden, wenn das Kommunikationsverhalten nicht auch online mitverfolgt wird und die Interaktionsroutinen nicht partizipativ ergründet werden. Softwaregestützte Verfahren sind vielversprechend und in jedem Fall zu unterstützen, insbesondere angesichts der Fülle von Daten, die sekündlich im Social Web produziert werden. Mit Blick auf den Sprachoberflächenfokus und die plattformenzentrierten Tools möchte ich jedoch den Mehrwert betonen, den solche Ansätze erfahren, wenn sie qualitativ, methodisch umfänglich ergänzt werden. Nur so kann das Phänomen Hate Speech umfassend erforscht werden, um Grundlagen für die Prävention bereitzustellen. Das integriert vergleichbare Methoden auch für die polizeiliche Ermittlung ebenso wie die Ausbildung in verschiedenen Kontexten. Hier bietet sich eine enge Zusammenarbeit zwischen der Linguistik, der Polizeiwissenschaft und der Kriminologie an.

Literatur

Alexander, M., Maclaren, A., O’Gorman, K., & Taheri, B. (2012). „He just didn’t seem to understand the banter“: Bullying or simply establishing social cohesion? *Tourism Management, 33*(5), 1245–1255.

Ashcroft, M., Fisher, A., Kaati, L., Omer, E., & Prucha, N. (2015). Detecting Jihadist messages on Twitter. *Proc. 5th European Intelligence and Security Informatics Conference* (S. 161–164). IEEE Computer Society.

Bahlo, N. (2012). Let's talk about sex – Vulgärer und sexualisierter Sprachgebrauch Jugendlicher als Thema im Projektunterricht. *Aptum. Zeitschrift für Sprachkritik und Sprachkultur, 8*(1), 48–60.

Deppermann, A., & Schmidt, A. (2001). Dissen: Eine interaktive Praktik zur Verhandlung von Charakter und Status in Peer-Groups männlicher Jugendlicher. *Osnabrücker Beiträge zur Sprachtheorie, Themenheft Sprech-Alter, 62,* 79–98.

De Smedt, T., & Jaki, S. (2018). The Polly corpus: Online political debate in Germany. *Proceedings of CMC and Social Media Corpora*, (S. 33–36).

Feldweg, H., Kiebinger, R., & Thielen, C. (1995). Zum Sprachgebrauch in deutschen Newsgruppen. *Osnabrücker Beiträge zur Sprachtheorie, Themenheft Neuen Medien, 505,* 143–154.

Ferrara, E., Wang, W.Q., Varol, O., Flammini, A., & Galstyan, A. (2016). Predicting online extremism, content adopters, and interaction reciprocity. arxiv. https://arxiv.org/abs/1605.00659. Zugegriffen: 15 Juni 2019.

Grainger, K. (2004). Verbal play on the hospital ward: solidarity or power? *Multilingua, 23,* 39–59.

Hartung, M., Klinger, R., Schmidtke, F., & Vogel, L. (2017). Identifying right-wing extremism in German Twitter profiles: A classification approach. In: F. Frasincar, A. Ittoo, L. Nguyen, & E. Métais (Hrsg.), *Lecture notes in computer science: Bd. 10260. Natural language processing and information systems (NLDB 2017)* (S. 320–325). Cham: Springer.

Hosseinmardi, H., Mattson, S. A., Rafiq R. I., Han R., Lv, Q., & Mishra, S. (2015). Detection of cyberbullying incidents on the Instagram social network. arXiv:1503.03909v1.

Jaki, S., & De Smedt, T. (2018). Right-wing German hate speech on Twitter: Analysis and automatic detection. (Unveröffentlichtes Manuskript). http://www.organisms.be/downloads/jaki2018.pdf. Zugegriffen: 15 Juni 2019.

Kaati, L., Omer, E., Prucha, N., & Shrestha, A. (2015): Detecting multipliers of jihadism on twitter. *IEEE Int. Conference on Data Mining Workshop (ICDMW).*

Kleinke, S. (2007). Sprachliche Strategien verbaler Ablehnung in öffentlichen Diskussionsforen im Internet. In S. Herrmann, S. Krämer, & H. Kuch (Hrsg.), *Verletzende Worte. Die Grammatik sprachlicher Missachtung* (S. 311–366). Bielefeld: Transcript.

Labov, W. (1972). Rules for ritual insults. In W. Labov (Hrsg.), *Language in the inner city. Studies in black English vernacular* (S. 297–353). Philadelphia: University of Pennsylvania Press.

Loos, E. M. (2011). *Digitale Gespräche in einer virtuellen Welt? Eine linguistische Analyse der kommunikativen Spezifika spanischer Freizeitchat-Kommunikation im Spannungsfeld von Mündlichkeit und Schriftlichkeit*. (Dissertation). Universität Heidelberg. https://archiv.ub.uni-heidelberg.de/volltextserver/13320/. Zugegriffen: 15 Juni 2019.

Marx, K. (2011). *Zur Verarbeitung von Komplex-Anaphern. Neurolinguistische Untersuchungen zur kognitiven Textverstehenstheorie*. Berlin: TU-Verlag.

Marx, K. (2013). Denn sie wissen nicht, was sie da reden? Diskriminierung im Cybermobbing-Diskurs als Impuls für eine sprachkritische Diskussion. *Aptum, 2,* 103–122.

Marx, K. (2017a). *Diskursphänomen Cybermobbing. Ein internetlinguistischer Zugang zu [digitaler] Gewalt*. Berlin: De Gruyter (= Diskursmuster/Discourse Patterns).

Marx, K. (2017b). Two sides of the coin: Hate speech as communicative pattern. *10plus1, 3,* 42–45. http://10plus1journal.com/wp-content/uploads/2017/09/10plus1_issue-3_brainstorming_marx_42-45.pdf. Zugegriffen: 15 Juni 2019.

Marx, K. (2018). Hate Speech – Ein Thema für die Linguistik. In M. Albers & I. Katsivelas (Hrsg.), *Recht & Netz* (S. 37–57). Baden-Baden: Nomos.

Marx, K. (2019). Verrohung und Online-Interaktion – eine enge Koalition? *BPJM AKTUELL, 2,* 4–9.

Meibauer, J. (Hg.) (2013). *Hassrede/Hate Speech. Interdisziplinäre Beiträge zu einer aktuellen Diskussion*. Gießener Elektronische Bibliothek 2013 (= Linguistische Untersuchungen). http://geb.uni-giessen.de/geb/volltexte/2013/9251/pdf/HassredeMeibauer_2013.pdf.

Paasch-Colberg, S., Strippel, C., van Aken, B., Emmer, M., Trebbe, J., Löser, A., Franko, K., Trömel, M., & Laugwitz, L. (2019). Deep-Learning-Algorithmus zur Identifizierung von Hate Speech. Vortrag auf der 64. Jahrestagung der Deutschen Gesellschaft für Publizistik- und Kommunikationswissenschaft (DGPuK) „Integration durch Kommunikation in digitalisierten Öffentlichkeiten“, 9.–12. Mai 2019, Münster.

Plutchik, R. (1980). *Emotion: Theory, research, and experience*. New York: Academic Press.

Rüdiger, T.-G. (2016). #NoHate. München & Hatespeech in Onlinegames. Wir müssen mal reden! https://www.linkedin.com/pulse/münchen-hatespeech-onlinegames-wir-müssen-mal-reden-rüdiger.

Scanlon, J. R., & Gerber, M. S. (2014). Automatic detection of cyber-recruitment by violent extremists. *Security Informatics, 3*(1), 5. https://doi.org/10.1186/s13388-014-0005-5.

Schlobinski, P. (2017). Grundzüge von Macht und Sprache. Networx 77. https://www.mediensprache.net/networx/networx-77.pdf. Zugegriffen: 15 Juni 2019.

Schmidt, A. (2004). *Doing peer-group. Die interaktive Konstitution jugendlicher Gruppenpraxis*. Frankfurt a. M.: Lang.

Schwarz-Friesel, M. (2008). *Einführung in die Kognitive Linguistik* (3. Aufl.). Tübingen: Francke.

Schwarz-Friesel, M., & Reinharz, J. (2013). *Die Sprache der Judenfeindschaft im 21. Jahrhundert*. Berlin: De Gruyter.

Suttles, J., & Ide, N. (2013). *Distant supervision for emotion classification with discrete binary values*. Berlin: Springer.

Ting, I. H., Chi, H. M., Wu, J. S., & Wang, S. L. (2013). *An approach for hate groups detection in facebook*. Netherlands: Springer.

Cyborgs bei der Polizei?

Soziotechnische Aspekte der Mensch-Maschine-Kollaboration

Viktoria Pawlowski

1 Einleitung

Innerhalb des digitalen Raums muss ich immer öfter beweisen, dass ich ein Mensch bin, um überhaupt bestimmte Funktionen und Dienste nutzen zu können. Konkreter, ich muss nachweisen, dass ich keine Maschine, kein Roboter bin, um an gewissen Internetdiensten partizipieren zu können (s. Abb. 1).

Ist die Digitalisierung unserer Lebenswelten so fortgeschritten, dass Menschen und Maschinen in solch einem Ausmaß ineinander verwoben sind, dass sie nicht mehr eindeutig voneinander zu unterscheiden sind? Und macht uns dieser Zustand alle zu Cyborgs, zu hybriden Wesen ohne klare Grenzziehung zwischen Mensch und Maschine? Welche Effekte resultieren aus solch einer scheinbaren Auflösung eindeutig wirkender Trennungen?

Solche Beobachtungen gesellschaftlicher Phänomene führten mich zu der Fragestellung, welche Auswirkungen eine fortschreitende Digitalisierung auf die alltägliche Praxis der Polizeikräfte haben könnte. Die Institution Polizei ist ein stark vernetztes und hierarchisch aufgebautes Netzwerk aus menschlichen und nicht-menschlichen Akteuren und das Kommunikationsmedium Funkgerät und

Überarbeitete und gekürzte Fassung meiner 2018 unter dem Titel „Cyborgs bei der Polizei? Soziotechnische Aspekte der Mensch-Maschine-Kollaboration, am Beispiel des Funkgerätes“ an der Universität Hamburg eingereichten Abschlussarbeit für den M.A. Internationale Kriminologie.

V. Pawlowski (✉)
Hamburg, Deutschland
E-Mail: viktoria.pawlowski@web.de

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

T.-G. Rüdiger und P. S. Bayerl (Hrsg.), *Cyberkriminologie,*
https://doi.org/10.1007/978-3-658-28507-4_28

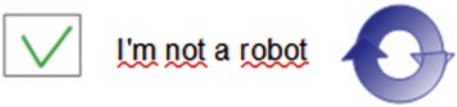


Abb. 1 Übliches Format einer online Kontrolle „I am not a robot“

-netz der Polizei wurden in den letzten Jahren in Europa von analog auf digital umgestellt, was einer erweiterten Digitalisierung dieser Lebenswelt entspricht. Die Sprache der Polizeikräfte wird nun in Form von Datenpaketen vermittelt, transformiert in Nullen und Einsen. Die Umstellung des Polizeifunknetzes von analog auf digital ist hierfür nur ein Beispiel, auch der vermehrte Einsatz von Kameras oder der alltägliche Umgang mit Smartphones und Computern bilden diese Realität ab.

Das Funkgerät wird im Polizeidienst besonders häufig sowie routiniert eingesetzt und alltäglich eng am Körper getragen, um damit kontinuierlich zu interagieren. Es entstehen besonders dichte Mensch-Maschine-Kollaborationen aus Polizist_in und Funkgerät, die unter dem Aspekt hybrider Wirkmechanismen untersucht werden sollen.

Dafür beginne ich mit der Präzisierung meines Forschungsgegenstands und der Fragestellung sowie einer Reflexion des relevanten Forschungsstands. Folgend definiere ich meine Ausgangsüberlegungen sowie forschungsleitende Annahmen und konkretisiere meine erkenntnistheoretische Perspektive. Zur Generierung auswertbarer Daten wurden narrative Interviews mit drei Hamburger Polizeikräften geführt[1]. Das Herzstück dieser Arbeit bildet der Auswertungs- und Diskussionsteil dieser gesammelten Informationen, in dem Beobachtungen und Phänomene zu einem weiterentwickelten Verständnis des Cyborg-Begriffs führen und zu der Erkenntnis, dass Handlungsträgerschaft in Kooperation mit digitalen Maschinen nicht nur eindeutig in menschlichen Akteuren eingeschrieben ist. Aus den Anforderungen nach Anpassung und aus der gesteigerten Vernetzung, resultieren neuartige Varianten von Norm und Abweichung sowie diverse Ein- und Ausschlussmechanismen. Verantwortung und Handlungsträgerschaft wird nicht ausschließlich in Menschen verortet, sondern auch an digitale Geräte abgegeben. Ich arbeite folgend spezifische Hoffnungen, Visionen und Enttäuschungen, die an eine Digitalisierung geknüpft sind, heraus und schließe mit einem Resümee und Ausblick.

Ich möchte mich nicht Charlie Chaplins nachstehender Prämisse einer deutlichen Unterscheidung zwischen Menschen und Maschinen anschließen, sondern

[1]Die Interviewten werden folgend als A., B. und N. betitelt.

betrachte diese als Akteure innerhalb eines Netzwerkes das ich Cyborg nenne, in dem sich diese oszillierend gegenseitig bedingen. Dennoch stimme ich den anmahnenden Worten seiner Abschlussrede aus dem Film „Der große Diktator“ zu.

> „Wir haben die Geschwindigkeit entwickelt, aber innerlich sind wir stehen geblieben. Wir lassen Maschinen für uns arbeiten und sie denken auch für uns. […] Wir sprechen zu viel und fühlen zu wenig. Aber zuerst kommt die Menschlichkeit und dann erst die Maschinen. […] Ihr seid viel zu schade für diese verwirrten Subjekte, diese Maschinenmenschen mit Maschinenköpfen und Maschinenherzen. Ihr seid keine Roboter, ihr seid keine Tiere, ihr seid Menschen!“ (Chaplin 1940)

2 Forschungsgegenstand und Fragestellung

Den zentralen Forschungsgegenstand bildet die Mensch-Maschine-Kollaboration am Beispiel von Polizeikräften in Hamburg und den von ihnen genutzten Funkgeräten, welche neben Bodycams, Computern usw. nur ein Beispiel für die gesteigerte Digitalisierung im Polizeialltag darstellen. Es wird untersucht, ob die alltägliche Nutzung von Kommunikationsapparaten zu einer hybriden Arbeitsweise führen und das Polizeipersonal als aus Cyborgs bestehend betrachtet werden kann. Ein Augenmerk liegt dabei darauf, ob die Polizeikräfte sich selbst und ihre Kollegen_innen direkt als Cyborgs bezeichnen oder nicht, respektive ob sich in ihren Aussagen Hinweise auf solch ein Selbstverständnis ermitteln lassen und wie mögliche Konsequenzen dieser engen Verbindung aus Mensch und digitalem Gerät reflektiert werden.

2.1 Begriffsbestimmung Cyborg

Cyborgs sind Hybridwesen aus biologischen Organismen und Maschinen, die nicht nur einen Teil der Fiktion, sondern auch der sozialen Wirklichkeit abbilden (Haraway 1995). Der Begriff Cyborg entstand 1960 und ist eine Zusammensetzung der Wörter cybernetic organism (Clynes und Kline 1960). Ursprünglich sollte mit diesem theoretischen Konzept antizipiert werden, wie Menschen ihren Körper im Kontext der Raumfahrt durch technische Ausstattung erweitern bzw. modifizieren können, um im Weltraum arbeiten und leben zu können (Clynes und Kline 1960). Seitdem wurde Cyborg als Begriff vielfältig erweitert und umgedeutet.

Naheliegende Assoziationen zum Cyborg stammen aus der Science-Fiction. In diesem Genre lassen sich unterschiedlichste Interpretationen der Mensch-Maschine-Mischwesen finden. Insbesondere wenn nach Cyborgs bei der Polizei gefragt wird, können Bilder aus dem Film RoboCop[2] imaginiert werden (A. [01:42:24])[3]. *„Part Man, Part Machine, All Cop. RoboCop: The Future Of Law Enforcemen“,* versprechen die Filmplakate. Ob hybride Wesen aus menschlichen oder männlichen Teilen und Maschinen tatsächlich die Zukunft der Strafverfolgung und Cyberkriminologie darstellen, wird im folgenden Diskussionsteil aufgegriffen. Zunächst möchte ich jedoch die Ideen von Cyborgs aus diesem narrativen Genre herauslösen und im Alltäglichen fixieren.

Mensch-Maschine-Kooperation findet sich seit längerem in der Medizin, z. B. in Form von Diagnosegeräten, Implantaten oder Prothesen, und es ist ein Wandel in der Präsentation und Wahrnehmung von stellvertretenden Gliedmaßen zu beobachten. Sowohl im Internet als auch in den Printmedien und im Fernsehen finden sich zur Schau gestellte Hightech-Prothesen in unterschiedlichsten, farbenfrohen und aufwendig gestalteten Designs. Je nach Anforderung werden neuartige Funktionen entwickelt, wie etwa zum Schwimmen oder Rennen.

Im Sport, in Filmen und auf Laufstegen werden Prothesen genutzt und gezeigt und keine Holzbeine oder Krücken mehr versteckt. Beim Super Bowl[4] am 5. Februar 2018 feierte z. B. ein Filmtrailer der Universal Pictures Premiere, der den „sexiest man alive“[5] Dwayne Johnson als Actionhelden zeigt, der eine Beinprothese trägt.

Im April 2018 verpflichteten die Seattle Seahawks, eine American Football Mannschaft der NFL, zudem Shaquem Griffin, den ersten *einhändigen* Sportler in der Historie der Profiliga, der seine Spiele mit Prothesen bestreitet (Süddeutsche Zeitung 2018).

Ich plädiere für eine ergänzte und fluide Begriffsdefinition, nicht nur auf die Nutzung reiner Ersatzteile limitiert oder starr eingegrenzt. Cyborgs zeigen sich auch in Interaktion mit Geräten, die nicht als Äquivalent für eine Fähigkeit

---

[2]Paul Verhoeven, 1987.

[3]Neben RoboCop bildet z. B. auch der als Manga, Anime und Realverfilmung bekannte „Ghost in the Shell“ von Masamune Shirow (1989), Mamoru Oshii (1995) und Rupert Sanders (2017) einen Cyborg als Staatsbeamtin ab; schien den befragten Probanden aber unbekannt und wurde innerhalb der Interviews nicht aufgegriffen.

[4]Der Super Bowl ist das jährliche Endspiel der National Football League (NFL) im American Football.

[5]Dwayne Johnson wurde 2016 vom People Magazin zum „sexiest man alive“ gewählt (Jordan 2016).

oder ein Körperteil dienen, sondern Sinneseindrücke und Leistungsfähigkeiten erweitern sowie neu schaffen können. Ich schließe mich Andy Clarks Theorien der Natural-Born Cyborgs an, der das Aufkommen der Armbanduhr als Entstehungsmoment des Cyborg-Zeitalters fixiert und dabei auf den Einfluss, durch die permanente Zeiterfassung und die Ausrichtung nach dieser, auf den Menschen verweist (Clark 2003). Smartphones versteht Clark als neuartige Sinnesorgane, die den Zugang zum Internet schaffen und das Erleben dessen ermöglichen (Clark 2003). Das Internet selbst erfasst Clark dabei als neue Sinndimension (Clark 2003). Aus der Perspektive der Kognitionswissenschaften heraus argumentiert Clark, dass Menschen durch Technologien erleben und fühlen, da das Interagieren mit nichtbiologischen Technologien dem menschlichen Verstand immanent sei (Clark 2003):

> „For what is special about human brains, and what best explains the distinctive features of human intelligence, is precisely their ability to enter into deep and complex relationships with nonbiological constructs, props, and aids.“ (Clark 2003, S. 5)

Das Maß, indem der Mensch Werkzeuge und technische Geräte nutzt, differenziert ihn signifikant von anderen Spezies, sodass der Mensch ontologisch ein Natural-Born Cyborg ist (Clark 2003). Polizeikräfte bilden hierbei keine Ausnahme. Als vermehrt vernetzte Personen innerhalb der hierarchisch strukturierten Institution Polizei interagieren sie selbst in Netzwerken aus menschlichen und nicht-menschlichen Akteuren. Dieser Zustand prädestiniert die Nutzung eines erweiterten Cyborg-Begriffs zur kriminologischen Untersuchung der Polizeikräfte, da vermutet wird, diese seien Auswirkungen einer gesteigerten Digitalisierung ausgesetzt.

Im Netzwerk der Cyborgs innerhalb Deutschlands tritt der „Cyborgs e. V. – Gesellschaft zur Förderung und kritischen Begleitung der Verschmelzung von Mensch und Technik“ als Lobbyist der Hybridwesen auf und setzt sich öffentlich für die Schaffung und Durchsetzung von eindeutig formulierten Cyborg-Rechten ein (Cyborgs e. V. 2014). In Clarks Kanon einstimmend, plädiert der Verein für die Abschaffung einer scharfen Trennung zwischen Mensch und Maschine:

> „Der Mensch gestaltet seine Umwelt und sich selbst, ist aber selbst Produkt der natürlichen Evolution. Eine Unterscheidung zwischen „künstlich“ und „natürlich“ ist daher sinnlos. Technologie ist Teil von uns, Produkt unserer Gedanken, Wünsche und Ziele. Sie ist nichts Externes sondern Ausprägung unserer gemeinsamen Kultur, Teil unserer Umwelt und Teil von uns selbst. Wir sind längst eine Cyborg-Gesellschaft, auch wenn die meisten Individuen sich nicht als Cyborgs fühlen.“ (Cyborgs e. V. 2014)

Ein Schlüsselwerk zum Forschungsgegenstand Cyborg bildet das „Manifest für Cyborgs“ von Donna Haraway, indem auch sie für die Überwindung obsoleter Dichotomien argumentiert, wie etwa der Unterscheidung in künstlich und natürlich (Haraway 1995). Steif verharrende Einteilungen, Grenzziehungen und Gegenüberstellungen von Mensch und Maschine sind inadäquat, um technik-assoziierte Phänomene sozialwissenschaftlich umfassend zu analysieren (Haraway 1995). Daher plädiere ich, dem theoretischen Konzept der Cyborg nach Haraway folgend, dafür:

> „die Cyborg als eine Fiktion anzusehen, an der sich die Beschaffenheit unserer heutigen gesellschaftlichen und körperlichen Realität ablesen läßt. Sie sollte aber auch als eine imaginäre Ressource betrachtet werden, die uns einträgliche Verbindungen eröffnen kann.“ (Haraway 1995, S. 34)

Haraways Konzept, formuliert aus einer feministischen Perspektive heraus und der damit einhergehenden Herrschaftskritik (Haraway 1995), bietet sich zudem im Zusammenhang mit der Untersuchung hierarchischer Strukturen der Polizei an, in denen die Cyborgs vermutet werden, was im folgenden Diskussionsteil wieder aufgegriffen wird. Ebenso wie die Frage danach, ob die befragten Polizisten sich selbst als Cyborgs verstehen und wahrnehmen.

Clark und Haraway folgend, nutze ich den Begriff Cyborg um die Wechselwirkungen der Kooperation aus Polizist_in und Funkgerät zu untersuchen. Das Funkgerät ist Teil des beruflichen Alltags der Beamten_innen und es gibt kaum ein zweites Gerät, das sie so oft und routiniert nutzen und stets eng am Körper tragen:[6]

> „A cyborg is a human being with an electronic device implanted in or permanently attached to their body for the purpose of enhancing their individual senses or abilities beyond the occasional use of tools.“ (Park 2014)

Das Funkgerät wird nicht gelegentlich oder vereinzelt durch die Polizeikräfte genutzt, vielmehr gehört es zum elementarsten elektronischen Gerät, das die individuellen Sinne der Nutzer_innen verbessert und erweitert (s. o.) und bietet sich entsprechend an, als zu untersuchendes technisches Element der Mensch-Maschine-Kollaboration, die ich hier Cyborg nenne. Wie der Hybride selbst stetig modifizierbar ist, soll die Definition nicht unveränderlich eingegrenzt, sondern als

[6] *„Funkgerät ist schon das Elementarste“* (N. [00:44:10]).

dynamisches Konzept verstanden werden und stellt selbst einen Untersuchungsgegenstand der folgenden Analyse dar.

2.2 Fragestellung

Wie schon angeklungen ist, richtet sich das primäre Forschungsinteresse auf die vermuteten Wechsel-/Wirkungen einer engen Kooperation aus Menschen und digitalen Apparaturen. Dies führt zu der leitenden Fragestellung: *Welche Auswirkungen hat eine fortschreitende Digitalisierung des Polizeialltags, unter Berücksichtigung eines gradualisierten Handlungsbegriffs und hybrider Konstellationen, auf die Arbeitsvorgänge der Mensch-Maschine-Kollaboration und welche Prognosen lassen sich daran ablesen?* Daran anknüpfende Fragen lauten:

- Wenn Menschen und Maschinen miteinander arbeiten, wer trifft dann wann, welche Entscheidungen (Bernstein und Raman 2015)? Wem oder welchem Gegenstand wird welche Verantwortung beigemessen? Von welchen Akteuren wird die Digitalisierung wie ausgehandelt?
- Wie werden die Auswirkungen der Digitalisierung von den Befragten selbst reflektiert und bewertet?
- Welche Mechanismen des Ein- und Ausschlusses wirken in der charakteristischen Netzstruktur der Polizeiarbeit im Zusammenhang mit der Nutzung digitaler Geräte und Räume?

Exkurs: Gradualisiertes Handeln
Kognition wird im Konzept des gradualisierten Handelns, als verteiltes Einwirken auf ein Netz aus menschlichen und nicht-menschlichen Akteuren begriffen (Rammert 2007). Artefakte wie das Funkgerät oder Smartphone bilden nicht bloß Instrumente und Werkzeuge, weiter sind sie in hybride Systeme aus Informationsverarbeitung integriert (Rammert 2007). Diese Ansätze der Technografie (Rammert und Schubert 2006) entsprechen den Vorannahmen eines hybriden Zusammenwirkens aus Menschen und Maschinen und widersprechen der „Annahme einer Ersetzbarkeit menschlicher Tätigkeit durch technische Geräte und der Übertragbarkeit menschlicher Kognition an maschinelle Informationsverarbeitung“ (Rammert 2007, S. 23). Produktives Kognitionshandeln generiert sich erst aus der einträglichen Verbindung aus Aktivitäten und einem routinierten Zusammenspiel mehrerer Instanzen (Rammert 2007). Dieses Konzept der Kognition und des verteilten, gradualisierten Handelns bilden zentrale Vorannahmen innerhalb des Forschungsprogramms der Technografie und werden herangezogen

zur Erfassung und Analyse soziotechnischer Kooperationen, die Rammert als „distributed agency“ fixiert, also den verteilten Handlungsweisen innerhalb hybrider Zusammenhänge (Rammert 2007).

Um den vermuteten Phänomenen auf die Spur kommen zu können, wurden die Befragten unter dem Aspekt des Natural-Born Cyborgs betrachtet (s. o.). Ich setze Grenzziehungen und Wechselwirkungen zwischen Menschen und Maschinen nicht voraus oder verneine diese, sondern mache eben jene zum Themenschwerpunkt (Rammert 2007). Dies stellt keine abgeschlossene Fragestellung dar, sondern wird fortlaufend theoriegeleitet und den Ergebnissen der Erhebungen entsprechend reflektiert. Die forschungsleitenden Fragen unterliegen theoretischen Vorannahmen, auf die folgend näher eingegangen wird.

3 Forschungsstand

Speziell für die Kriminologie sind Cyborgs soziale Phänomene, die erkenntnisreiche Forschungsergebnisse verheißen, da sie immanent in sich Grenzziehungen und Überschreitungen dieser vereinen und so neuartige Kriminalitätsformen, juristische Herausforderungen[7] und durch die Modifizierbarkeit des Menschen auch Verschiebungen in den Rahmungen von Norm und Abweichung schaffen. Sie bringen Irritationen in sozialwissenschaftliche Fragen nach gesellschaftlicher Reproduktion und sozialer Kontrolle und stellen hierarchische Beziehungen zwischen Menschen und Maschinen infrage (Brown 2006).

Spätestens seit dem Manifest für Cyborgs von Haraway (s. o.) erweckten die Hybridwesen das Interesse der Geistes- und Sozialwissenschaften. Der Kognitionswissenschaftler Clark trägt ein weiteres Schlüsselwerk dieser Thematik bei, da hier an seine Theorien des Natural-Born Cyborgs (Clark 2003) angeknüpft wird (s. o.). Aus der Perspektive der Anthropologie fordert Arturo Escobar eine fortlaufende, interdisziplinäre Eruierung der „Cyberculture“, in der der technologische Wandel essenziell auf die Gesellschaft einwirkt (Escobar 1994). Kriminologisch widmeten sich Wytske van der Wagen und Wolter Pieters dem Wandel von Cybercrime zu Cyborg Crime, mit den Methoden der Akteur-Netzwerk-Theorie (van der Wagen und Pieters 2015). Dieser wird allerdings oft unterstellt, ontologische Abgrenzungen zwischen menschlichen, natürlichen und

[7]Vgl. z. B.: *„Mit […] Schnittstellen ausgestattete Patienten erschien manchen Experten schon als Cyborgs. Damit würde unsere Rechtsprechung nicht mehr für sie gelten. Von diesen Patienten verursachten Unfälle dürften Haftungsfragen aufwerfen.“* (Clausen 2015).

technischen Handlungsträgern zu bestreiten, dabei sollen diese Grenzziehungen hier selbst ein Gegenstand der Forschung sein (Rammert 2007).

Dem fiktiven Charakter des RoboCops aus dem Film von 1987 und der Neuverfilmung von 2014, sowie der Cyborg-Staatsbeamtin aus „Ghost in the Shell" (s. o.) widmete sich z. B. der Kulturwissenschaftler Mark Friedrich Eichhorn, auch unter dem Aspekt der jeweiligen Arbeitssituation der Cyborgs als Staatsdiener_in (Eichhorn 2013). Jedoch liegt der Fokus Eichhorns Ausarbeitung auf der medialen Darstellung des Berufsalltags der Hybridwesen, nicht auf der Untersuchung aktueller, realer Phänomene, jenseits der Fiktion.

Aus der Perspektive der Politikwissenschaften greift Volker Eick den Begriff des RoboCops auf, im Zusammenhang mit am Polizeikörper getragenem Equipment (Eick 2017). **Eick** bezieht sich allerdings auf die sukzessive genutzten BodyCams, nicht auf das im Arbeitsalltag der Polizei omnipräsente Funkgerät. Eick stellt fest, dass Träger_innen des staatlichen Gewaltmonopols in den letzten ca. zehn Jahren immer mehr zu Träger_innen beträchtlicher Technologien wurden (Eick 2017). Anschließend an diese Feststellung, spielt nicht nur der Aspekt der Qualität der Polizeiausrüstung in der nachstehenden Analyse der geführten Interviews eine Rolle, sondern auch die Quantität der Geräte sowie die Platzierung dieser am Körper der Polizeikräfte wird als relevant erachtet und miteinbezogen.

Die Kriminologin Sheila Brown spricht von Technosozialität, in der die Wissensproduktion primär *über* Technologien, wie dem Digitalfunkgerät, vermittelt wird und *durch* diese Technologien entsteht (Brown 2006). Brown plädiert dafür, wie Rammert in seinem Programm der Technografie[8], Handlungsträgerschaft („agency") nicht exklusiv jeweils in den Menschen oder in der Technik zu verorten (Brown 2006; Rammert 2007). Deborah Lupton formuliert aus soziologischer Perspektive die forschungsleitende Frage danach, wie Menschen und Maschinen ineinander verwoben sind, korrelativ aufeinander einwirken und löst dabei konventionelle Trennlinien zwischen Menschlichem und Nichtmenschlichem auf (Lupton 2016). Luptons Frage soll in der folgenden Analyse anhand der Polizeikräfte und der Digitalfunkgeräte beantwortet werden und stellt damit eine Ergänzung und Fortführung bisheriger, wissenschaftlicher Forschung dar. Unsichtbare, aber auch deutlich erkennbare Grenzen und Verbindungen der hybriden Polizei-Cyborgs, einem Netzwerk aus Menschen, Funkgeräten und anderen Apparaturen, messe ich eine hohe Relevanz bei und vermute signifikante Wechselwirkungen.

[8]Auf Rammerts Forschungsprogramm der Technografie wird im folgenden Methodenteil detaillierter eingegangen.

Meine Untersuchung zum Konzept des Natural-Born Cyborg und den vermuteten Wirkmechanismen durch die Digitalisierung des Polizeialltags bildet eine Erweiterung des bisherigen Forschungsstands und folgt den Aufrufen, nach einem interdisziplinären Diskurs bezüglich der Mensch-Maschine-Kollaboration (Peters 2015).

4 Ausgangsüberlegungen und forschungsleitende Annahmen

Mein privates sowie berufliches Umfeld wurde ebenso in den letzten Jahrzehnten zunehmend von Technik durchdrungen, in Form des aufkommenden Internets, der Handys, der Erweiterung zum Smartphone u. Ä., wie bei jedem anderen. Dabei messe ich z. B. der Wahrnehmung und Reflexion einer gesteigerten Technisierung der verschiedenen Lebenswelten hohe Relevanz bei. Wie reflektiert die Allgemeinheit und das Individuum, verwoben in einem Geflecht aus digitaler Technik im Bereich der Kommunikation, Medizin, Unterhaltung, Informationsbeschaffung usw., diesen Wandel? Wie verändert sich der Umgang mit Privatsphäre und Datenschutz, der verschwimmenden Grenzziehung zwischen privat und öffentlich, real und virtuell, der Unterscheidung von Tatsachen und fake news? Muss sich der Mensch der Maschine angleichen damit die Leistungen gleichwertig bzw. gleichrangig anerkannt werden, um sich an der Technik messen zu können?

Eine gesteigerte Technologisierung scheint in der Allgemeinheit als modern gewertet zu werden. Aus der Perspektive der Politikwissenschaften heraus fasst Christopher Coenen dazu kritisch zusammen:

> „Problematisch ist […], Zukunftsvisionen zu propagieren und dabei reale gesellschaftliche Bedingungen zu ignorieren. Die körperliche Leistungsfähigkeit massiv zu verbessern, gar Mensch und Maschine zu verschmelzen, sind keine aus sich heraus legitimen Interessen. Sie sind nur im Rahmen übergeordneter gesellschaftlicher Ziele vernünftig. Und diese lassen sich nur demokratisch bestimmen.“ (Coenen 2015, S. 73)

Den Standards qualitativer Sozialforschung folgend, habe ich keine strikt fokussierten und abgeschlossenen Hypothesen aufgestellt, sondern in forschungsleitenden Annahmen erste Ansätze zum Forschungsgegenstand zusammengefasst. Obligatorisch habe ich aus der Auseinandersetzung mit vorhandenem Material zu den Themen Cyborgs und digitaler Polizeifunk heraus theoretische Vorannahmen und implizierte Interpretationen präzisiert (Przyborski und Wohrab-Sahr 2014):

- Der menschliche Körper der Polizeikräfte wird in Verbindung mit digitalen Geräten als hybrides Wesen, als Cyborg, konzipiert.
- Aus der hybriden Verbindung aus Mensch und Maschine entstehen wirkmächtige Phänomene, die potenziell sowohl als produktiv, als auch kontrollierend und manipulierend erfahren werden können.
- Die vermehrte Nutzung von und Interaktion mit digitalen Geräten wird allgemein hin als kontemporär und somit größtenteils als erforderlich und unumgänglich betrachtet. Eine kritische Reflexion der Technikfolgenabschätzung findet vermehrt in der Öffentlichkeit, Wissenschaft und Politik statt, im Vergleich zur Hinterfragung persönlicher, alltäglicher Handlungsweisen mit digitalen Medien.

4.1 Erkenntnistheoretische Perspektive

Medienwissenschaftler Gundolf S. Freyermuth postuliert, an das Konzept des Natural-Born Cyborg von Andy Clark anknüpfend: *„Wir sind nicht mehr, wer und was wir glauben zu sein: Menschen, wie es unsere Vorfahren waren. Wir sind längst Cyborgs“* (Freyermuth 2015). Vernetzte Geräte, welche die Cyborgisierung[9] antreiben, sind bspw. Kommunikationsmedien, etwa Smartphones oder Funkgeräte. Diese informationsübertragenden Trägersysteme

> „sind, wie der Begründer der Medienwissenschaft Marshall McLuhan […] erkannte, »extensions of man«, spezifische Erweiterungen dessen, was menschenmöglich ist. Sie steigern technisch unsere kreatürlichen Fähigkeiten, zu hören, zu sehen, zu handeln, zu begreifen. Damit verändern sie nicht nur die Wahrnehmung unserer Umwelt, sie ermöglichen auch neue Blicke auf uns selbst.“ (Freyermuth 2015, S. 57)

Anknüpfend an das soziologische Forschungsprogramm der Technografie, von Rammert und Schubert (2006), betrachte ich *Techniken* als von der Gesellschaft kreativ und artifiziell installierte Wirkzusammenhänge, die präzise und kontinuierlich gewünschte und erwartete Effekte produzieren (Rammert 2016). Es handelt sich nicht ausschließlich um ingenieurtechnisches Gebilde in Form

[9]Der Ausdruck „Cyborgisierung“ wird hier interimistisch genutzt, um das prozesshafte Charakteristikum eines fortschreitenden, digitalen Wandels zu fixieren, der sich auch auf den menschlichen Körper auswirkt und auf das Konzept des Cyborgs (s. o.) rekurriert, unabhängig davon, ob die Menschen sich selbst als Cyborgs wahrnehmen und definieren.

effizienter Werkzeuge und Maschinen (Rammert 2016). Vielmehr muss in der Forschung berücksichtigt werden, dass Techniken eine Dimension der sozialen Konstruktion der Mittel durch die Gesellschaft in sich bergen, Mittel mit denen Menschen in Kooperation arbeiten, leben und kommunizieren (Rammert 2016). „Techniken sind nicht nur technische Installationen aus physischer Materie, Energie und Information, sondern zugleich auch material vermittelte soziale Institutionen“ (Rammert 2016, S. 9).

Den verknüpften Strukturen von Funkgeräten ist immanent, dass sie schnell unübersichtlich wirken können, dass sich Grenzen und Verbindungen teilweise evident offenbaren, andere erst aufgedeckt werden müssen und einige wohl unsichtbar bleiben:

> „Für die Kollegen auf der Straße ändert sich eigentlich nicht all zu viel. Der hat nach wie vor noch ein Funkgerät. […] Der Bedienungsaufwand und die Möglichkeiten eines Digitalfunkgeräts sind aber ungleich größer. Das heißt, dass Ding ist an sich schon mal komplexer.“ (A. [00:12:13])

5 GPS–Ortung

Die Möglichkeiten zur Nutzung des satellitengestützten Global Positioning Systems (GPS) zur Ortung der Funkgeräte und ihrer Träger_innen wird von N. als Errungenschaft der Digitalisierung der Polizeiarbeit gewertet, auch wenn ihm die Bedenken und der Widerstand aus den eigenen Reihen gegen die kontinuierliche Option der Kontrolle, durch eine Erfassung der Position der Polizeikräfte, bekannt ist (N. [00:25:13]).

> „Das war bei den Alten [Funkgeräten] nicht so. Ähm, da hätte man extra ’nen GPS-Sender anbauen müssen. Die Funkgeräte, wenn die geklaut werden, das hatten wir auch vor ein, zwei Monaten in Hamburg, wurden welche aus dem Streifenwagen geklaut, Funkgeräte. Die kann man orten. Ähm, natürlich auch nur wenn sie angeschaltet sind, aber jetzt, ähm, ist da ein Marker drauf und sobald das Gerät wieder eingeschaltet wird, kann man sofort sehen, wo das Funkgerät ist. Und das gleiche gilt für den Streifenwagen. Wenn ich durch die Gegend fahr, ähm, sieht man, wo ich bin. Und diese, das war auch vor zwei, drei Jahren, da hat man dann gesagt, wir wollen’s auf jeden Fall machen. Da haben Manche gesagt, das geht nicht. Und unser Personalrat, die sind Sturm gelaufen.“ (N. [00:25:21])

N. erfasst im f*oucaultschen Sinne* das produktive Potenzial des Zusammenwirkens aus Wissen, Kontrolle und Macht, welches durch die Optionen der GPS-Ortung entsteht:

> „Die haben ne Klage vorbereitet. Und da hab ich immer wieder gesagt, ich seh so'n bisschen auch den Sicherheitsaspekt, ne. Was ist denn, wenn irgendwo 'n Amoklauf ist und ich bekomm, hör da nicht richtig zu und fahr, fahr da rein. Oder, solche ähnlichen Sachen. Oder irgendjemand braucht wirklich, tatsächlich Hilfe und der in der Einsatzleitzentrale sieht diesen Einsatzort, der hat irgendwo so'n großen Bildschirm und da sind ja ganz viele verschiedene Felder und da ist so'ne kleine Karte, ne. Und dann ist da, auch je nach dem welche Skalierung er hat, sieht er dann den Einsatzort, der ist dann so aufgepint. Und wenn Dein Auto direkt in der Nähe ist, ich sag mal so bis zu 500 Metern, dann sieht der das. Und wenn jetzt jemand sagt, z. B. Frau ruft im Park um Hilfe, und er zufällig sieht, dass da jemand in der Nähe fährt, dann gibt's doch nix besseres als zu sagen, ey Du! Bist da direkt um die Ecke, fahr da mal schnell hin. So und das, das sehen immer Viele nicht. Viele haben halt immer das Gefühl, sie werden kontrolliert. Aber ich, ich bin da ein bisschen, ähm. Ein größerer Feind ist Datenschutz in dem Bereich, ich mein, ich hab nicht viel zu verbergen, bei mir ist nicht viel zu holen. Ähm, es gibt auch immer Leute, die sagen, sie haben Angst dass dann der Chef immer guckt, wo bin ich denn unterwegs. Bin ich 'n guter Mitarbeiter, beurteilt halt. Das kann man in gewissen Bereichen auch nachvollziehen." (N. [00:25:21])

Auch wenn N. angibt, er habe nicht viel zu verbergen, bei ihm ist nicht viel zu holen (s. o.), wertet er Datenschutz innerhalb des geführten Interviews auch als einen bedeutsamen Aspekt und misst seiner Privatsphäre einen gewissen Wert bei, gerade wenn eine Vermischung von privaten und beruflichen Lebenswelten stattzufinden droht. N. zieht hier eine Verbindung zur Überwachung seiner Kommunikation, z. B. in schriftlicher Form per Mobiltelefon, nicht aber zur potenziell kontinuierlichen Ortung seines Standortes:

> „[I]ch empfinde es auch als gruselig, wenn ich ähm, jetzt, wenn irgendwann jemand auslesen könnte mit wem ich, ähm, Kontakt hatte und mit wem nicht und was für Kontakt. Das finde ich schon bisschen gruselig, weil, man muss sich ja nur mal überlegen was passiert wenn, was weiß ich, ein aufstrebender Politiker und dann heißt es, hier übrigens, Du hast, ähm, 'n Verhältnis gehabt mit, mit, ähm, Frau, Frau XY. So und dann wird, wird mir das schön Alles hingelegt und es heißt, hier Du willst wohl doch nicht mehr in die Politik gehen. Das find ich schon gruselig." (N. [00:22:39])

Der Interviewte N., der sich aktiv in einer Polizeigewerkschaft engagiert, bewertet den andauernden, öffentlichen Diskurs innerhalb Deutschlands und Europas zum Datenschutz gegenüber staatlicher Behörden und den diversen Variationen der Vorratsdatenspeicherung als extrem (s. u.). Die mögliche GPS-Ortung seiner Person, z. B. durch das Digitalfunkgerät, steht hinsichtlich seiner Befürchtungen bezüglich seiner Privatsphäre und einer möglichen Kontrolle nicht im Vordergrund. N. erfasst den Schutz der persönlichen Individualbereiche in einem Prozess gesellschaftlicher Aushandlung und plädiert für ein Mittelmaß, ohne dieses näher zu umreißen:

„Datenschutz ist schon echt extrem. Das ist immer das, diese Frage die wir uns als Polizisten immer stellen. Sind so, solche, gewisse Löschfristen auch gut, ne. Auf der anderen Seite profitiert man auch wieder davon. Und, ähm, das ist, ist so dieses, mh, Balance halt, ne. Irgendwie so da genau die Mitte zu finden. Das ist schwierig und ich glaube, ab, in vielen Bereichen ist Deutschland da auch Vorreiter, da den Balance halt zu finden. Äh, aber es ist ja auch so die Vorratsdatenspeicherung zum Beispiel.“ (N. [00:22:11])

6 Besteht die Polizei aus Cyborgs?

Der befragte Polizei-Cyborg N., der alltäglich mit dem Digitalfunkgerät kollaboriert, bezeichnet sich selbst nicht als solcher. Ich möchte mich nachstehend diesem Phänomen nähern und beginne damit, menschliche und nicht-menschliche Akteure in Relation zueinander zu setzen, innerhalb des Hamburger Polizeialltags.

Der Cyborg ist ein Netzwerk aus Mensch, Maschinen und anderen Gerätschaften, das sich selbst organisieren muss und indem alle Akteure oszillierend aufeinander einwirken und sich aneinander anpassen müssen. Welcher Akteur sich in welchem Maße welchen Bedingungen anpassen muss, ist nicht feststehend priorisiert. Der Cyborg ist eine fluide Struktur, der mit diversen Objekten möglichst produktiv interagieren soll.

Polizeibeamte_innen können alltäglich anfallenden, beruflichen Anforderungen nicht genügen, ohne eine sehr enge körperliche Verbindung mit nicht-menschlichen Akteuren einzugehen. Die Anzahl und Komplexität dieser Objekte scheint zu expandieren. Dies deutet eine fortschreitende Cyborgisierung der Polizeikräfte an, über das Konzept des Natural-Born Cyborg hinaus. Nicht jeder Natural-Born Cyborg muss derartige, langwierige Symbiosen mit teilweise sehr komplexen Apparaturen zur Ausübung der beruflichen Tätigkeiten eingehen.

Diese Gegenstände, wie der Computer oder das Funkgerät, werden innerhalb der hybriden Kollaboration vermenschlicht, bzw. haben vermenschlichende Begrifflichkeiten Einzug gehalten in den Sprachgebrauch der Polizeikräfte bezüglich des Funkgerätes:

„Sagen wir’s so, natürlich muss dieses Gerät, ähm, noch über Stromverfügung eingeschaltet sein. Und es muss, überhaupt ein, ein entsprechendes, äh, Signal liefern oder selber erst mal erlangen können, sprich GPS. Das muss, äh, gewährleistet sein. Wenn das der Fall ist, dann kann man dem Gerät schon mal aus der Ferne heraus sagen, dass es doch bitte seine Position mitteilen möge.“ (B. [00:22:50])

> „Also wenn ich jetzt hier meine, äh, iPhone-Such-App dann dort ein-, aktiviere, dann weiß ich auch wo mein Telefon sich gerade befindet, wenn ich das nicht in der Hand habe, oder in der Tasche. So was geht mit Digitalfunk natürlich auch, aber dazu muss überhaupt jemand erst einmal dieses Gerät entsprechend dazu überreden, das zu tun.“ (B. [00:23:19])

Der Interviewte B. artikuliert, dass das Digitalfunkgerät ansprechbar sei, es wird höflich gebeten sowie überredet und es soll damit erreicht werden, dass der digitale Akteur sich mitteilt.

Die Vermenschlichung der Maschine wurde von dem Befragten nicht in einen Zusammenhang mit einer Zunehmenden Verflechtung aus Mensch und Maschine artikuliert, keiner der drei Interviewten kam aus eigenem Antrieb auf das konkrete Thema Cyborg zu sprechen, sodass ich diese zum Abschluss der jeweiligen Interviews aus eigener Initiative heraus anführen und freie Assoziationen erfragen musste, um mich meinem Forschungsinteresse nähern zu können.

6.1 Assoziationen zum Begriff des Cyborgs

Auf den Ausdruck Cyborg angesprochen, antwortet N. ad hoc, er kenne den Begriff nicht, was er allerdings im selben Atemzug revidiert und einen Bezug zu Computerspielen herstellt, also zu virtuellen, digitalen sowie fiktiven Welten. Der Cyborg, den N. meinen theoretischen Vorannahmen nach verkörpert, verortet N. selbst nicht in der alltäglichen Lebenswelt, sondern innerhalb von Fiktion und Unterhaltung:

> „[K]ennst Du den Ausdruck Cyborg? Schon mal gehört?“ (V. [01:01:05])

> „Nee. Also Cyborg, also doch, das ist ja hier so’n, so’n, äh, ähm, na sag schon, im, im Computerspiel gibt’s doch Cyborgs, oder nicht?“ (N. [01:01:13])

Für N. sind Cyborgs „Maschinen“ (N. [01:01:26]), keine Symbiose aus diesen und Menschen. Sich selbst würde N. subjektiv nicht als Cyborg bezeichnen, er negiert dies vehement (N. [01:01:36]) im Gegensatz zu seinem Kollegen A. aus der IT-Abteilung, wie folgend aufgezeigt wird. N. empfindet kein Einwirken der Geräte auf seine Handlungsweisen und Verantwortungen:

> „Also am Ende, nimmt es mir ja niemand ab, das Denken, so, das. Ist immer, natürlich hab ich jetzt mein […] Smartphone wo ich auch mal nachgooglen kann,

irgend'n Paragrafen, ähm. Aber, nee, überhaupt nicht. Dafür, dafür ist die Polizei auch noch zu weit weg davon, glaub ich, ne." (N. [01:01:36])

„Also, am Ende, ähm, ist da kein Computer der überlegt, ob er, für mich, ob ich, ob ich schießen muss oder nicht. Oder, kein Kollege der sagt, irgendwie, läu- Du läufst jetzt hinterher, oder, oder nicht, so. Es ist, da ist man auf sich alleine gestellt, ne. Mit, vielleicht noch mit nem Kollegen zusammen, wo man sagt dann, ok, was machen wir jetzt? Ne. Das kann man ab und zu nochmal machen, man berät sich dann, so. Wie geh ich jetzt weiter vor, ne?" (N. [01:02:08])

„So, aber es ist jetzt irgendwie nicht so dass man, dass man sagt, dass der Computer einem groß irgendwas abnimmt. Das, das irgendwie nicht, nee." (N. [01:02:30])

Die Befragten A. und B. hatten sich offenbar vorbereitend mit dem Begriff des Cyborgs auseinandergesetzt und dieser führte zunächst zu Irritationen:

„'N Cyborg würd ich ja so verstehen, dass da, äh, ein Gerät eigenständig irgendwelche Dinge tut, die, ähm, ja, zwar beeinflusst werden können, aber grundsätzlich würde das Gerät das tun. Könnte vielleicht auch irgendetwas unterstützen, indem viele Sachen heute automatisiert ablaufen. Hier ist es so, dass alle Automatismen, die beim Funkgerät irgendwo ablaufen, müssen irgendwo initiiert werden." (B. [01:41:32])

B. verortet die Handlungsträgerschaft eindeutig in den Menschen und nennt keine hybride Verbindung, die sich wechselseitig beeinflusst, sondern erkennt deterministische Abläufe die initiiert werden und Automatismen auslösen. Es ist nicht eindeutig nachvollziehbar, warum B. direkt von der Benennung des Cyborgs auf ein selbstständiges Wirken von Maschinen schließt, statt auf eine hybride, verteilte Handlungsträgerschaft:

„Das heißt, das Gerät wird von sich aus nicht auf die Idee kommen, eine Textnachricht sich zu versenden. Das Einzige, was es wirklich tut, ist beim Notruf seine Position mir zu senden. Aber das auch nur, weil man's dem Gerät so gesagt hat. Das heißt, man hat es so programmiert, dass es das tut." (B. [01:42:00])

Der Befragte B. erlebt weder sich selbst noch seine Kollegen_innen als hybride Mischwesen aus Mensch und Maschine bzw. eindeutig nicht als Cyborgs:

„Es [die Benennung der Polizeikräfte als Cyborgs] passt nicht für Sie?" (V. [01:42:18])

„Nee, überhaupt nicht. Meiner Meinung nach gar nicht." (B. [01:42:20])

Der zweite Interviewpartner der IT-Abteilung äußert weiterführende und offener wirkende Assoziationen zum Thema Cyborg. „*Also ich hab da, äh, bei Cyborg fiel mir automatisch RoboCop ein*“ (A. [01:42:24]). A. wirkt zunächst unentschlossen und würde Polizeibeamte_innen in Anführungszeichen als Cyborgs bezeichnen.

Zuvor greift der Befragte A. selbstständig thematisch das Reflektieren der eigenen Handlungsweisen bezüglich der Digitalfunkgeräte auf und beschreibt eine fortschreitende, gesamtgesellschaftliche Cyborgisierung. Der Interviewte A. benennt Zweifel, an der Wahl des Mediums Funkgerät und impliziert eine erforderliche Anpassung durch den/die Polizeibeamten_in an die Maschine, da alternative Kommunikationsmedien wie das Smartphone „viel gegenwärtiger“ und somit „transparenter“ im Umgang wären (A. [00:15:10]):

> „Ist das eigentlich […] richtig so, was wir so veranstalten. Ist das Funkgerät, das richtige Medium, was wir da einsetzen? Oder, sollte man nicht gar ein Medium nehmen, was heute viel transparenter ist, nämlich zum Beispiel ein Smartphone. Also ein Smartphone zum Beispiel, das äh, das ist viel gegenwärtiger, viel, äh, offensichtlicher. Weil, unsere Kollegen draußen, auf der Straße […], haben, neben ihrem Funkgerät auch noch mindestens ihr privates Smartphone dabei. Und kommunizieren teilweise auch über ihr Smartphone. Über die Sicherheit, die das bietet, wollen wir gar nicht reden, aber, wir bieten hier auf der einen Seite eine sichere Infrastruktur an und auf der anderen Seite finden viele Sachen trotzdem, auf einer ganz anderen Gesprächsebene statt. Es wäre auch, äh, Blödsinn, dass im Endeffekt komplett auszublenden.“ (A. [00:15:10])

Der Interviewte A. wiederholt den Eindruck, dass sich Polizeikräfte den Anforderungen der Maschine anpassen müssen. Er impliziert einen Umgang miteinander, nicht das Bedienen und Steuern des einen Akteurs durch den anderen:

> „[S]o wird es ja teilweise gemacht, in den Formularen, dass, dass über das Formularwesen im Endeffekt dann auch ne Hilfestellung angeboten wird, ne. Das sollte aber möglichst schlicht und schlank erfolgen. Da steckt ne Fülle von Problemen dahinter. Standardisierung der Vordrucke, immer zur Verfügung stehen, der, der Leitungs-, äh, Wege. Die interne Verarbeitung muss IT-sicher sein. Also, wir haben ja einerseits eine IT-Schutz-Bedarfsvariante, einmal eine Datenschutz-Variante. Einmal ne technische Variante und einmal das, was tatsächlich passiert, wie wir mit den Daten umgehen. All das muss ja berücksichtigt werden. Und das alleine schon ist natürlich extrem komplex. Bei dieser ganzen Komplexität wird aber der Mensch ’n Stück weit immer vergessen und da eben halt so die Kurve zu kriegen, was ist am, am naheliegendsten. Also, wie kann man am besten miteinander, äh, so umgehen?“ (A. [01:11:25])

Der Befragte A. artikuliert Befürchtungen dahin gehend, dass durch eine steigende Cyborgisierung und vermehrte Komplexität der eingesetzten Geräte innerhalb des Polizeialltags, ein menschlicher Akteur seine Bedürfnisse und Handlungsweisen den Anforderungen der Maschinen unterordnen muss und dabei droht *„vergessen“* zu werden (s. o.).

A. macht deutlich, dass die Rolle der menschlichen Akteure innerhalb der Mensch-Maschine-Kollaboration von ihm reflektiert wird. Es wird deutlich, dass der Interviewte A. Aspekte, wie etwa Ergonomie, zugunsten der Polizeikräfte benennen kann, aber nicht fixiert werden kann, welcher Akteur sich letztendlich in welchem Maße an wen anpasst. Es werden Optionen genannt, wie etwa zur erleichterten Ansicht digitaler Bildschirme, aber nicht endgültig festgemacht, in welchem Rahmen die Polizeikräfte solche Entscheidungen eigenmächtig durchsetzen können:

> „Das geht hin bis dazu, dass ich mir, ähm, ich sag mal ne Oberfläche, ne Bildschirmoberfläche angucke und sage, ey, wie ist das jetzt eigentlich für mich am, am besten aufgeteilt. Da gibt es ja auch ganz unterschiedliche, ich sag mal, Sichtweisen. Ergonomisch, oder effizient, oder gefühlsmäßig, wie viel will ich sehen, ne? Äh, will ich da ein, ein, ein neuen. Wir haben ja teilweise diese, auf den Monitoren sehen Sie ja einmal die, die Desktop-Ansicht, das ist ne, ne komplexe Ansicht. Und dann haben Sie auch noch die, die einfachere.“ (A. [01:13:27])

> „App-Ansicht vielleicht, ne. Was möchte ich sehen?“ (A. [01:13:58])

> „Und das ist ne, finde ich, auch ne super spannende, äh, Fragestellung. Alles begleitet eigentlich durch dieses Thema Digitalisierung.“ (A. [01:14:01])

Auf eine mögliche Überforderung menschlicher Akteure durch die Notwendigkeit der Anpassung an digitale Akteure angesprochen, zieht der Befragte A. Verbindungen zum eh zeitweise belastenden Polizeialltag, wie etwa während des G20-Gipfels 2017 in Hamburg. Er beschreibt gesteigerte Anforderungen an die Handlungsweisen der Menschen, die aus einer fortgeführten Cyborgisierung resultieren:

> „Weil der Mensch auch überfordert sein könnte?“ (V. [01:14:09])

> „Ja, bestimmt. Bestimmt. Und das ist ja genau, das ist ja genau der Punkt. Ähm, diese Überforderung im Endeffekt zu vermeiden, weil die Kollegen und wir, draußen auf der Straße, haben, ähm, müssen ja auch noch ’n Einsatz irgendwo versuchen abzuwickeln. Wir müssen uns auch noch nicht mit dem Bürger auseinandersetzen, aber dafür sind wir ja eigentlich da. Und wenn dann noch, ein hoher technischer

> Aufwand dazu kommt, das auch noch zu begleiten und zu betreiben, an was soll ich denn noch alles denken?“ (A. [01:14:12])

Der Interviewte A. bestärkt das durchgeführte Forschungsvorhaben auch aus der Perspektive der Polizei heraus und spricht diesem Relevanz zu. A. empfindet subjektiv eine abnehmende Flexibilität in den Handlungsweisen der menschlichen Akteure durch eine gesteigerte Cyborgisierung:

> „Das muss man mal sicherlich mal diskutieren, das kann man auch philosophisch, soziologisch mit Sicherheit auch beleuchten. Natürlich findet so was statt. Ich kann mich ja immer entschuldigen dafür, weil ich irgendetwas nicht hatte. Ich hatte den Bohrer nicht, aber wieso krieg kein Loch in die Wand. Ne, also klar, weil ich den Bohrer nicht hatte, aber krieg ich nicht vielleicht auch anders ’n Loch in die Wand? So dieses, und da hab ich so manchmal das Gefühl, dass wir das genau verlernen.“ (A. [01:15:25])

Polizeikräfte sind nicht nur Netzwerke aus Menschen und Maschinen die im beruflichen Alltag miteinander kooperieren. Jede_r Polizeibeamte_in ist parallel auch in privaten Lebenswelten vermehrt ein selbstorganisierendes Konstrukt aus menschlichen und nicht-menschlichen Akteuren. „Alles begleitet eigentlich durch dieses Thema Digitalisierung“ (A. [01:14:01]).

7 Vor- und Nachteile einer allgemeinen Digitalisierung

Auf die Digitalisierung in privaten sowie beruflichen Lebenswelten angesprochen, und den damit einhergehenden Vor- und Nachteilen, artikuliert der Interviewte N. initial, dass er glaubt, „*der größte Teil ist’n riesengroßer Vorteil. Also das muss man wirklich sagen. So 90 Prozent ist’n großer Vorteil*“ (N. [00:56:07]). Folgend nimmt N. Bezug zu seinen Tätigkeiten im Bereich der Gewaltprävention an Schulen und nennt Cybermobbing als negativ konnotierten Aspekt der fortschreitenden Digitalisierung (N. [00:56:07]). Einen weiteren Nachteil sieht der Befragte N. darin, „dass Alle draußen, wenn irgendwo was ist, was filmen“ (N. [00:57:20]). N. bemängelt dabei nicht die Option der (audio-) visuellen Fixierung ausgeführter Handlungsweisen durch Polizeikräfte, sondern den Umstand, dass solche Aufnahmen immer nur einen Ausschnitt eines Ereignisses zeigen können und Zusammenhänge, Akteure und vorangegangene oder nachstehende Einwirkungen außer Acht gelassen werden können:

> „Da war Einer, der hatte 20 Frauen unsittlich berührt. So, das, hat kaum Einer mitbekommen. Dann haben wir den festgesetzt und dann hat er sich gewehrt, ähm, dann, umliegend, sozusagen, dieses, das Ganze zu brechen, hat der auch 'n paar bekommen. Wurde dann, ähm, irgendwann festgenommen. Und am Ende taucht dann ein Video auf, wie er ein paar von den Kollegen ins Gesicht bekommt." (N. [00:57:39])

N. markiert nicht die bloße Existenz solcher Filmaufnahmen und der damit einhergehenden selektiven Darstellung komplexer Einsatzsituationen als Nachteil. Vielmehr erkennt der Interviewte N. die Problematik darin, dass solche Ausschnitte im Internet digital über diverse Netzwerke verbreitet werden:

> „Nur dieser Ausschnitt. Und das ist immer das, diese Sachen womit wir zu kämpfen haben. Das ist dann am nächsten Tag bei YouTube, ne. Oder Kollegen werden von dieser 187, äh, Straßenbande, irgendwie, von, von Gzuz[10] und keine Ahnung was, werden sie ins Internet gestellt. Weil das coole Typen sind. Und dann hast Du welche, die irgendwie, die Polizisten sind Anfang 20, dann habe sie da noch Einen daneben, der auch Anfang 20 ist, die sitzen aufm Streifenwagen zusammen und dann lassen die sich da mehr oder weniger vorführen. Ganz schwierig, so. Und das sind so Sachen, damit, damit haben wir zu kämpfen, aber auf der anderen Seite, ist es 'n riesengroßer Vorteil. Wir haben so viele Erleichterungen dadurch." (N. [00:58:03])

Soziale Medien bilden Netzwerke ab, über die solche Filmausschnitte digital geteilt werden können. Die sogenannten *Sozialen* Medien bilden eigene Infrastrukturen aus diversen menschlichen und nicht-menschlichen Akteuren und reproduzieren somit materialisierte connectivity, also die Vernetzbarkeit bzw. Netzwerkfähigkeit. N. empfindet es als *„gruselig",* dass es Personen gibt, die *„ihr Handy zücken",* Unfallsituationen filmen und über digitale Netzwerke verbreiten (N. [01:19:01]):

> „[D]as wird natürlich mehr durch die zunehmende Digitalisierung, ganz klar. Ähm, aber es gab schon immer welche, die da hingeguckt haben. Jetzt hab ich halt die Möglichkeit da hinzugucken, es zu filmen und noch mit meinen, mit meinen Freunden zu teilen, ne. Das ist so der Unterschied, ne. Aber die Strafen, die werden, man fängt damit ja jetzt an, wenn, bekämpft das Problem, sozusagen, damit man das neu starten schafft, ne. Es gibt ja Sachen, die waren frü-,früher auch strafrechtlich nicht relevant, ne." (N. [01:19:16])

[10][„187 Strassenbande" und „Gzuz" sind Hamburger Musiker aus dem Hip-Hop-Genre].

Der Befragte N. erkennt in dieser connectivity Potenziale zur destruktiven Nutzung und benennt Phänomene der Anpassung der Rechtslage an neuartige Umstände (s. o.). N. spricht einer allgemeinen Digitalisierung aber wiederholt mehr Vor- als Nachteile zu (s. o.).

Im privaten Umfeld, bspw. während eines Urlaubs, empfindet N. die Optionen digitaler Kommunikationsmöglichkeiten teilweise als belastend und damit im Gegensatz zu Erholung stehend:

> „[I]ch find das manchmal ganz schön, einfach das Handy auch mal ’n paar Stunden weg zu legen. So. Es gibt so Tage, es gibt auch Tage, da nervt mich das, keine Frage. Im Urlaub, wenn ich irgendwie, ähm, ich war letztes Jahr sechs Wochen, bin ich durch Vietnam gereist. Und da war’s dann auch so, dass ich zwischendurch mal kein Netz hatte. So, ein oder zwei Tage. Und da war’s dann, als ich dann ins, ins, äh, nächste WLAN gekommen bin und dann geguckt hab, irgendwie, 300 Nachrichten, in irgendwelchen WhatsApp-Chats und so. Da fühlt man sich so’n bisschen abgeschlossen, so, ne. Von der We-, Außenwelt.“ (N. [00:58:45])

N. beschreibt das Ereignis, das 300 Kontaktaufnahmen an ihn gerichtet wurden, obwohl er nicht am Netzwerk Internet partizipieren konnte. Er fixiert den Moment des Gefühls, von der Außenwelt abgeschlossen zu sein, nicht in dem Zeitraum, indem er tatsächlich vom Netzwerk Internet ausgeschlossen war und keine Teilhabe an diesem hatte. Erst durch das Aufzeigen der 300 Möglichkeiten zur digitalen Kommunikation, von denen er davor keine Kenntnis hatte, lösen Assoziationen des abgeschlossen bzw. ausgegrenzt Seins von einer außenstehenden Welt aus (s. o.). Sobald N. sich mit der digitalen Sphäre verbunden hatte, nach einer ein bis zwei tägigen Abstinenz, wurden Emotionen im Zusammenhang mit Ausschlussmechanismen ausgelöst. Durch die Verknüpfung mit dem digitalen Netzwerk, empfindet N. sich abgetrennt statt eingebunden, was zunächst widersinnig anmutet.

Der Interviewte N. benennt konkret neue strafrechtlich relevante Tatbestände, die direkt aus einer Cyborgisierung der Lebenswelten resultieren. Er artikuliert, der Staat würde nicht angemessen zeitnah juristisch auf soziale Phänomene im Zusammenhang mit einer gesteigerten elektrischeren Nutzung, im Verlauf der Digitalisierung, reagieren:

> „Immer diese Frage, Diebstahl, ist, ähm, Entziehung elektrischer Energie ’n Diebstahl? So, damit hat man sich früher nie beschäftigt, bis dann irgendwie das aufkam, dass die alle Leute Strom geklaut haben. Da sagten die, ok, wir müssen ’n neuen Paragrafen schaffen, Entziehung elektrischer Energie. So, und das sind immer so Sachen, dann läuft der Staat immer hinterher und sagt, ok, ist ’n neues Phänomen, ne. So, das.“ (N. [01:19:46])

„Aber Du würdest sagen, das ist halt der Lauf der Dinge, war schon immer so?“ (V. [01:20:04])

„Ganz genau, das ist, war schon, man war schon immer interessiert.“ (N. [01:20:07])

„Das gehört ja zum normalen Menschen auch dazu.“ (N. [01:20:09])

„Aber es ist, verändert sich halt im Umgang damit. Und, dem muss man sich halt dann anpassen, ne.“ (N. [01:20:12])

Hier kristallisieren sich Formen verteilter, gradualisierter Handlungsweisen innerhalb hybrider Zusammenhänge heraus. Der Mensch muss reagieren, aktiv handeln, um sich damit den Auswirkungen der Digitalisierung anzupassen.

8 Das Individuum und die Digitalisierung

Der Befragte N. artikuliert weitere prekäre, soziale Phänomene, die aus der Cyborgisierung unterschiedlicher Lebenswelten resultieren, obwohl er die Effekte der Digitalisierung allgemein zu 90 % als vorteilhaft bewertet (N. [00:56:07]):

„Auf der anderen Seite muss man auch sagen, wenn im Internet Straftaten begangen werden, wir haben aktuell viel zu wenig Möglichkeiten um das zu ermitteln. Also, aktuell, in den letzten Tagen vor Weihnachten wird’s wieder mehr mit Internetbetrug, mit, ich hab mal ’n iPad hier und ein Macbook da bestellt. Das ist, eine riesen, also was da an die Wachen ran kommt an Leuten, was die Alles erleben. Und das ist ja nur, ähm, tatsächlich das Hellfeld und das Dunkelfeld kennen wir überhaupt nicht. Viele sagen ja auch, hier, hundert Euro, kein Bock, zeig ich nicht an. Das ist extrem. Und dann, wenn man das nicht rechtzeitig irgendwie beantragt, dass man da an die IP-Adressen ran kommt, dann sind die Daten weg.“ (N. [00:23:08])

Als Vorteil einer fortschreitenden Cyborgisierung markiert der Interviewte N., dass er sich geschützt fühlt durch hybride Strukturen aus digitalen und menschlichen Akteuren, obwohl diese auch als Überwachungs- und Kontrollmechanismen interpretiert werden können:

„[M]an möchte auch geschützt sein, es ist auch so ne Sache, auf unseren Streifenwagen haben wir auch Kameras, und die sind nach vorne, gehen nach vorne raus. Da ist Hamburg auch Vorreiter gewesen, wir waren die Ersten die das hatten. Bei Verkehrskontrollen, bei, ähm, Mitte der Neunziger wurde mein Kollege, der hat alleine jemanden kontrolliert und wurde von einem älteren, dementen Jäger

> erschossen, so. Und da hat man gesagt, ok, wir wollen auf jeden Fall, dass die Strafverfolgung mit aufgezeichneten Straßenverkehrsmitteln fahren, so. Und dann, ist halt so, wenn wir ein Fahrzeug anhalten, sagen wir, wir fahren mit dem Streifenwagen dahinter, dann geht die Kamera automatisch an. Ich mach stop Polizei und die filmt das Ganze.“ (N. [00:23:45])

Die Handlungsträgerschaft ist eindeutig aufgeteilt, N. „macht stop“ und die Maschine, in diesem Fall die Kamera, beginnt ihren Zweck zu erfüllen. Diese Kamera ist allerdings vom Streifenwagen aus nach Draußen ausgerichtet. N. spricht sich für weitere Kameras innerhalb der Streifenwagen aus, also für eine gesteigerte Interaktion von Menschen und Maschinen. Dieser Zustand würde für ihn subjektiv Ansprüche an die eigene Sicherheit erfüllen, innerhalb seines beruflichen Alltags, und geht mit der Weiterentwicklung digitaler Möglichkeiten einher, wie etwa Videoaufnahmen in High Definition:

> „[J]etzt ist grad die Debatte darum, diese Technik ist jetzt auch veral- so, veraltet, weil das schon von Anfang der Zweitausender ist und jetzt kein HD oder 4K-Technologien, da gibt es auch die Möglichkeit, nach innen zu filmen. So, und jetzt ist die große Debatte entbrannt. Darf man das? Sollte man das? Ähm, so und da bin ich jemand, ich sage, find ich, grundsätzlich sollen die das nicht sehen alles was ich getan hab, aber wenn sie merken, ich krieg den nicht zu fassen über Funk, ich krieg`s über Funk nicht, nicht über’s Telefon, dann würde ich es gut finden, wenn der Polizeifunk die Möglichkeit hätte so’n Notfall-Knopf zu drücken und zu sagen, jetzt guck ich da mal rein, weil da stimmt doch irgendwie was nicht.“ (N. [00:24:19])

Der Interviewte N. greift die Diskurse rund um eine optionale Videoüberwachung innerhalb der Streifenwagen auf und ignoriert dabei die Möglichkeiten zur Kontrolle durch potenziell geöffnete Mikrofone der Digitalfunkgeräte. Ein Erklärungsansatz hierfür könnte darin zu finden sein, dass Funkgeräte temporär betrachtet bereits viel länger zum Polizeialltag gehören, als die neuartigere, mobile Videotechnologie. Aber auch eine mangelnde Selbstreflexion im Umgang mit digitalen Akteuren und dem Dasein als Cyborg innerhalb hybrider Mensch-Maschine-Verbindungen könnten für diese Ausklammerung der Digitalfunkgeräte ursächlich sein. Hier bietet sich ein Anknüpfungspunkt für weitere Forschungsarbeiten an.

Der Befragte N. fixiert aber nicht nur Vorteile solch einer Kameraüberwachung innerhalb der Streifenwagen, also an seinem alltäglichen Arbeitsplatz. Ihm sind potenziell nachteilige Effekte solch einer Kontrollmöglichkeit bewusst, er spricht diese Sichtweisen allerdings ausschließlich anderen Akteuren als sich selbst zu:

„Aber da sagen auch Einige dann, ok, vielleicht bin ich auch grad bei McDonalds und hau mir da heimlich den Burger rein. Ähm, oder hab'n Verhältnis mit dem, dem Kollegen da drin, oder, oder, oder, da kam wieder diese ganze Bandbreite. Oder Einige sagen, ich möchte nicht, wenn ich einfach durch die Gegend fahr', kontrolliert werden." (N. [00:24:55])

Der Interviewte N. artikuliert den Eindruck, dass menschliche Akteure aktiv handeln müssen, um als Cyborgs produktiv und möglichst effizient arbeiten zu können. Sie müssen sich schulen lassen oder sich auf eigene Initiative fortbilden und mit der Digitalisierung vertraut machen:

„So, das ist, da 'n Wandel und auch durch die Digitalisierung, durch's Internet, ist das 'n riesen Bereich. Und das ist auch, etwas, dass wir als Polizei auch nicht immer Alle abdecken können. Ich würd sagen, ich bin einigermaßen fit, in Computern, aber es ist jetzt auch nicht, dass ich irgendwie Programmiersprachen kann oder irgendwie so, ähm, dafür haben wir gar nicht das, das, das Knowhow." (N. [01:14:25])

„Und da muss man die Leute für ausbilden." (N. [01:14:45])

N. benennt eigene Schwächen und Befürchtungen, die durch die Digitalisierung entstehen, da Handlungsweisen in der Interaktion aus Mensch und digitalem Gerät dokumentiert und zur Diskreditierung verwendet werden können:

„Ich weiß damals, in welcher Klasse war ich denn? 12., 11. oder 12. Klasse, da kamen irgendwie, auch irgendwie, dass Irgendeiner dem Andern Fotos von seiner Exfreundin rum geschickt hat und so. Aber da waren wir schon im Bereich 17, 18 Jahre. So, und das war damals schon der mega Skandal, ne. Und heute ist das bei den 14, 15jährigen, ist das gängige Praxis. So, dafür hat man ja hier Snapchat[11] erfunden. Dafür, dass die Bilder eigentlich verschwinden." (N. [01:16:53])

„Ich hab damals gesagt, ey, geil, so." (N. [01:17:28])

„Wenn, dann mach ich's über Snapchat, aber dann sagt irgendwann Einer, Du, jetzt kann man da Screenshots machen, so. Oh, verdammt." (N. [01:17:30])

[11][Snapchat ist ein digitaler Kommunikations-Dienst, bei dem sich versendete Nachrichten nach einer festgelegten Zeit selbst löschen sollen.].

Die Befragten A. und B. aus der IT-Abteilung der Polizei sehen auch eine Notwendigkeit in der Schulung der Kollegen bezüglich der fortschreitenden Digitalisierung des Polizeialltags. Erste Unsicherheiten seitens der menschlichen Akteure im Umgang mit den Digitalfunkgeräten, sollen durch die Kommunikation von Anwendungshinweisen relativiert worden sein:

> „Hat sich aber […] total relativiert. Weil mittlerweile weiß eigentlich fast jeder Kollege, Sprechen bedeutet ich muss erst, drücke drauf und warte dann dass ich meinen Piepton kriege. Dann kann ich sprechen.“ (A. [00:54:58])

Durch Abgabe eines Pieptons durch das Digitalfunkgerät erhält der menschliche Akteur die Berechtigung und technische Möglichkeit zur Handlungsweise, genauer zur Kommunikation. Die Handlungsträgerschaft ist innerhalb dieser hybriden Kooperation in unterschiedlicher Abstufung, je nach Betrachtungsweise, verteilt auf die menschlichen sowie nicht-menschlichen Akteure:

> „Grade so in Kommunikation, ja, sicherlich kann man den Kollegen beibringen ihr Smartphone virtuos zu nutzen. So dass man auch gut Einsatzkommunikation machen kann. Aber in Extremsituationen, da wo’s schnell gehen muss, da muss es auch einfach sein. Das heißt, ich nehm das Gerät, es ist vorher eingestellt, es ist eingeschaltet und die Sache ist erledigt.“ (B. [01:16:09]).

> „Ja. Und es muss funktionieren.“ (A. [01:16:31])

Menschen und Maschinen immer dichter miteinander zu verweben innerhalb routinierter Handlungsweisen, ist kein aus sich selbst heraus legitimiertes Interesse (Coenen 2015). „Sie sind nur im Rahmen übergeordneter gesellschaftlicher Ziele vernünftig. Und diese lassen sich nur demokratisch bestimmen“ (Coenen 2015, S. 73).

9 Ist modern gleichzusetzen mit digitalisiert?

Solche gesellschaftlichen Ziele werden innerhalb der Hamburger Polizei nicht direkt demokratisch ausgehandelt, bspw. innerhalb einer Wahl durch befragte Polizeikräfte bestimmt. Das Ziel einer modernen Polizei wird durch einen ernannten Vertreter, dem Hamburger Polizeipräsidenten, formuliert und initiiert (s. u.). N. bezieht sich in diesem Zusammenhang wiederholt auf die Vorteile, die er durch diese modernisierte Form der Polizeiarbeit sieht:

„Also aktuell, […] kümmert man sich glaub ich eher so, um andere Probleme ne. Es ist noch, insbesondere die Hamburger Polizei ist ja, ähm, mit unserem relativ neuen Polizeipräsidenten[12] noch, der ist jetzt auch schon zwei Jahre dabei, aber, der hat das Ziel, 'ne moderne Polizei daraus zu machen. Wir haben die Online-Wache, wo man Anzeigen erstatten kann, ähm. Dann geht man jetzt grade dazu über, zu sagen, ok, was können die Kollegen aufm Streifenwagen machen. Also, bisher ist es ja so, wenn ich draußen einen Verkehrsunfall aufnehmen, dann hast Du da Dein kleines Büchlein, da schreib ich alles mit meiner Sauklaue rein, fahr dann an die Wache und schreib es dann wieder in den Computer. Hab ich auch gesagt, ok, können wir das nicht irgendwie anders machen? Was, wo wir so seit Jahren von sprechen. Einfach nur zu sagen, ok, ähm, einfach ein iPad mit ner Maske, wo ich schon mal die ersten Sachen vorformulieren kann und ähm, schwierige Details, wie lange Texte, die mach ich dann drin, an der Wache, so wie bisher auch.“ (N. [00:17:28])

Der Befragte N. verortet den Zustand einer modernen Polizei in der Zukunft, nicht als gegenwärtig. Er artikuliert subjektiv sein Einverständnis und seine Zufriedenheit mit dem Vorgehen des Polizeipräsidenten, mit dessen Ziel diese gewünschte Modernität zu erreichen. Die Handlungsträgerschaft und Entscheidungsgewalt liegt bei einem wirkmächtigen Vertreter seiner Interessen, was sich nicht stereotyp auf alle anderen Polizeikräfte übertragen lässt. Auch hier bildet sich ein Ausgangspunkt weiterer wissenschaftlicher Untersuchungen an:

„[M]odernere Polizei heißt also, 'ne hochtechnologisiertere Polizei für den Polizeipräsidenten, oder?“ (V. [00:20:58])

„Joah, genau, joah. Also über, genau, also auch'n bisschen, um die Arbeit der Kollegen und Kolleginnen zu erleichtern. Zu sagen, ok wir, Doppel-Arbeiten, die schaffen wir 'n bisschen ab und, ähm, deswegen ist Herr Meyer genau der Richtige, der dafür'n bisschen auch'n Blick für hat. Das ist oft so bei Behörden, wenn man irgendwie nen Ausweis in Hamburg beantragt, dann darf ich jetzt mittlerweile übers Internet nen Termin machen. Dann krieg ich aber nen Termin in drei Monaten. Warum kann ich nicht den Ausweis beantragen, über das Internet?“ (N. [00:21:08])

10 Fazit

Es konnten im Verlauf des Forschungsprojekts drei zentrale Erkenntnisse herausgearbeitet werden, die sich eng aufeinander beziehen. In einem System aus menschlichen und nicht-menschlichen Akteuren müssen sich Polizeikräfte zurechtfinden und sich flexiblen Gegebenheiten anpassen um am Polizeidienst

[12][Ralf Martin Meyer (*1959), seit dem 29. April 2014 Polizeipräsident Hamburgs].

partizipieren zu können. Daraus resultieren neuartige Leistungsansprüche an die Menschen sowie an die Maschinen. Neue Normen entstehen und wer sich der Digitalisierung nicht anpasst, sich bspw. nicht schulen lässt, verhält sich abweichend und kann den Polizeidienst nicht ausüben. Technische Optionen der Überwachung und Kontrolle werden von den Interviewten in Zusammenhang mit der GPS-Ortung und den in Polizeiwagen mitgeführten Kameras gesetzt. Eine mögliche Dokumentation der polizeilichen Handlungsweisen durch offene Mikrofone der Funkgeräte wurde nicht in Erwägung gezogen. Die Reflexion der Mensch-Maschine-Kollaboration scheint selektiv zu verlaufen.

Zweitens ist herauszustellen, dass die Befragten sich selbst nicht als Cyborgs deuten oder bezeichnen würden, obwohl bspw. alle Kriterien des Natural-Born Cyborgs nach Clark erfüllt werden und ferner eine besonders enge Verbindung aus Mensch und Maschine innerhalb des Polizeidienstes aufgezeigt werden konnte. Polizeikräfte sind in einem besonderen Maße vernetzt in ihrem beruflichen Alltag und müssen mit digitalen Geräten interagieren, um überhaupt den Polizeidienst ausführen zu können. Im Zuge solch einer Digitalisierung droht der menschliche Akteur innerhalb des hybriden Netzwerks Cyborg vergessen zu werden (A. [01:11:25]).

Drittens konnte herausgearbeitet werden, dass eine fortschreitende Digitalisierung innerhalb der Hamburger Polizei als modern und damit positiv bewertet und angestrebt wird. Solch eine Konnotation und so ein Vorgehen legitimieren sich allerdings keineswegs aus sich selbst heraus, sondern sollten gesellschaftlich ausgehandelt werden (Coenen 2015). Eine Polizeigewerkschaft könnte hier korrektiv wirken. Der Befragte N., Vertreter einer Polizeigewerkschaft, reflektiert die Digitalisierung für sich ebenfalls als modern und positiv, trotz geweckter Hoffnungen, die in der Vergangenheit nicht erfüllt werden konnten, wie etwa bzgl. einer Bildübertragung innerhalb des Polizeifunknetzes. Auch Optionen der Überwachung und Kontrolle durch eine gesteigerte Vernetzung und Digitalisierung werden von den Befragten nicht als grundsätzlich negativ bewertet.

Abschließend bleibt festzuhalten, dass sich mit jeder Erkenntnis im Laufe dieses Forschungsprojekts weiterführende Fragen ergeben haben, die eigener Ausarbeitungen bedürften. Unter Verwendung der Grounded Theory und qualitativer Methoden der Sozialwissenschaften war dies allerdings ein vorweg anzunehmender Umstand. Der begrenzte Umfang solch einer Forschungsarbeit steht im Kontrast zum offenen Konzept des hybriden verzweigten Netzwerks Cyborg. Es bieten sich, durch die stete Weiterentwicklung der Digitalisierung diverser Lebenswelten und der nachgewiesenen Einflüsse auf menschliche sowie nicht-menschliche Akteure durch diese, zahlreiche Anknüpfungspunkte für fortführende Untersuchungen an.

Literatur

Bernstein, A., & Raman, A. (2015). Die große Abkopplung. *Harvard Business Manager, 37*(September), 32–41. (Erweiterte deutsche Ausgabe der Harvard Business Review, Harvard Business Publishing. Hamburg/Brighton).

Brown, S. (2006). The criminology of hybrids. Rethinking crime and law in technosocial networks. *Theoretical Criminology, 10*(2), 223–244.

Clark, A. (2003). *Natural-born cyborgs: Minds, technologies, and the future of human intelligence.* New York: Oxford University Press.

Clynes, M. E., & Kline, N. S. (1960). Cyborgs and space. *Astronautics, 13*, 26–27 und 74–76.

Coenen, C. (2015). Der alte Traum vom mechanischen Menschen. *Spektrum der Wissenschaft – Spezial. Physik, Mathematik, Technik, 2*(2015), 66–73. („Mensch, Maschine, Visionen – Wie Biologie und Technik verschmelzen").

Chaplin, C. (1940). Der große Diktator. Hier ein Auszug aus der Abschlussrede. Erstaufführung in deutscher Sprache im damaligen Westdeutschland 1958. https://www.youtube.com/watch?v=vi0tNhMyHtc. Zugegriffen: 24. Juni 2018.

Clausen, J. (2015). Rechtsfragen. Verschwimmende Grenzen zwischen Mensch und Technik. *Spektrum der Wissenschaft – Spezial. Physik, Mathematik, Technik, 2*(2015), 74–79. Spektrum der Wissenschaft Verlagsgesellschaft, Stuttgart.

Cyborgs e. V. (2014). *Manifest*. Berlin https://wiki.cyborgs.cc/wiki/Manifest. Zugegriffen: 12. März 2018.

Eichhorn, M. F. (2013). *Cyborgs*. Diplomarbeit, University of Vienna, Philologisch-Kulturwissenschaftliche Fakultät. Wien https://othes.univie.ac.at/27346/. Zugegriffen: 14. Juni 2018.

Eick, V. (2017). *Videos zum Hinfassen: BodyCams in den USA und der BRD*. In: Bürgerrechte & Polizei/CILIP (112). Berlin https://www.cilip.de/2017/03/22/videos-zum-hinfassen-bodycams-in-den-usa-und-der-brd/. Zugegriffen: 14. Juni 2018.

Escobar, A. (1994). Welcome to Cyberia: Notes on the anthropology of cyberculture. *Current Anthropology, 35*(3), 211–231.

Freyermuth, G. S. (2015). Übermenschenbilder. Visionen von Cyborgs künden von einer neuen Kultur menschlicher Selbstverbesserung. *Spektrum der Wissenschaft – Spezial. Physik, Mathematik, Technik, 2*(2015), 57–65. („Mensch, Maschine, Visionen – Wie Biologie und Technik verschmelzen").

Haraway, D. (1995). Ein Manifest für Cyborgs. Feminismus im Streit mit den Technowissenschaften. In C. Hammer (Hrsg.), *Die Neuerfindung der Natur. Primaten, Cyborgs und Frauen* (S. 33–72). Frankfurt a. M.: Campus.

Jordan, J. (2016). Dwayne ‚The Rock' Johnson is this year's sexiest man alive! In: people.com., Time Inc. New York. https://people.com/celebrity/sexiest-man-alive-2016-dwayne-johnson-the-rock/. Zugegriffen: 13. Juni 2018.

Lupton, D. (2016). Digital companion species and eating data: Implications for theorizing digital data-human assemblages. *Big Data & Society, 3*(1), 1–5.

Park, E. (2014). Ethical issues in cyborg technology: Diversity and inclusion. *Nano Ethics, 8*(3), 303–306.

Peters, S. (2015). *Die Technisierung des Menschlichen und die Humanisierung der Maschine* (S. 7–19). Halle: Mitteldeutscher (Saale).

Przyborski, A., & Wohlrab-Sahr, M. (2014). *Qualitative Sozialforschung. Ein Arbeitsbuch*. München: Oldenbourg.

Rammert, W., & Schubert, C. (Hrsg.). (2006). *Technografie. Zur Mikrosoziologie der Technik*. Frankfurt a. M.: Campus.

Rammert, W. (2007). *Technografie trifft Theorie. Forschungsperspektiven eine Soziologie der Technik*. Technical University Technology Studies Working Papers, TUTS-WP-1-2007, 1–35. Berlin.

Rammert, W. (2016). *Technik – Handeln – Wissen. Zu einer pragmatischen Technik- und Sozialtheorie*. Wiesbaden: VS Verlag.

Süddeutsche Zeitung (2018). *Shaquem Griffin wird erster einhändiger Profi der US-Football-Liga NFL*. München http://www.sueddeutsche.de/sport/handball-fuechse-berlin-holen-spektakulaer-acht-tore-auf-1.3962321. Zugegriffen: 17. Juni 2018.

van der Wagen, W., & Pieters, W. (2015). From cybercrime to cyborg crime. Botnets as hybrid criminal actor-networks. *British Journal of Criminology, 55*(3), 578–595.