Cyberkriminologie – Von digitaler Kriminalitätstransparenz bis zum Broken Web

Thomas-Gabriel Rüdiger

Zusammenfassung

Seit einigen Jahren formiert sich im deutschsprachigen Raum mit der Cyberkriminologie eine neue Subdisziplin der Kriminologie, die sich explizit der Betrachtung von digitalen Kriminalitätsdelikten und Normenüberschreitungen widmet. Diese Entwicklung erscheint naheliegend, denn die Betrachtung von digitalen Kriminalitätsformen muss auch die Besonderheiten eines faktisch globalen und grenzfreien digitalen Raums mit einbeziehen. In diesem Raum treffen die strafrechtlichen, aber auch moralischen Vorstellungen annähernd aller Gesellschaftsformen aufeinander und schaffen so einen gemeinsamen Kriminalitätsraum. Dieser ist geprägt von einer Art digitaler Kriminalitätstransparenz, die gleichzeitig in Ansätzen die „Präventivwirkung des Nichtwissens" durchbricht. Gleichzeitig zeigen diese Mechanismen, dass die formelle Kontrolle nicht mehr hinreichend in der Lage ist, diesen Raum auch zu regulieren. Erkenntnisse, die aus diesen Überlegungen gewonnen werden, können auch mittel- wie unmittelbar Auswirkungen auf die Ausrichtung einer digitalen Polizeiarbeit haben. Dieses Kapitel geht auf Konzepte der Cyberkriminologie ein und beschreibt ihre Wechselwirkung mit Formen digitaler Polizeipräsenz und -arbeit.

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

D. Wehe, H. Siller (Hrsg.), *Handbuch Polizeimanagement*,
https://doi.org/10.1007/978-3-658-34388-0_56

1 Die Etablierung der Cyberkriminologie

1.1 Ein globales Netz?

Wenn die New York Times über den Vorwurf eines einfachen Identitätsdiebstahls schreibt, muss an diesem vermutlich etwas Besonderes sein. Im August 2019 veröffentlichte sie einen Artikel, dass eine US-Astronautin während ihrer Dienstzeit auf der International Space Station (ISS) auf die Kontodaten ihrer von ihr getrennt lebenden Frau zugegriffen hatte (Baker 2019). Auch wenn das Verhalten zunächst als Identitätsdiebstahl eingestuft werden konnte, wurde die Astronautin nach einem Untersuchungsausschuss von den Vorwürfen freigesprochen (Rempfer 2020).

Der gesamte Sachverhalt konnte in dieser Form nur erfolgen, weil AstronautInnen auch auf der ISS Zugang zum irdischen digitalen Raum haben. Die Nasa verkündete bereits 2019, dass mit bis zu 600 MB pro Sekunde von der ISS aus gesurft werden könne (Garner 2019). Obwohl laut Auskunft der Nasa die AstronautInnen nur über Computer und nicht über Smartphones eine Internetverbindung zur Erde haben (Neumann 2019), eröffnet sich aber dadurch die Möglichkeit, letztlich weltweit mit Menschen zu interagieren, kommunizieren und zu spielen. Möglichkeiten, die auch aktiv genutzt werden, wenn beispielhaft der Astronaut Kimbrough im Juni 2021 direkt aus der ISS einen Twittergruß an Nürnberg versendet (Kimbrough 2021). Wenn man die Entwicklung weiterdenkt, wird auch die ISS nicht der entfernteste Ort sein, der vermutlich über eine Internetverbindung mit dem irdischen Netz verbunden sein wird. Ende 2020 gab die Nasa bekannt, dass Nokia mit dem Aufbau eines 4-G Mobilfunknetzes auf dem Mond beauftragt wurde (Banner 2020). Es ist vermutlich nur eine Frage der Zeit bis auch entsprechende Pläne für den Mars angegangen werden. Das Ergebnis wird ein allumfassendes Kommunikationsnetz darstellen. Aus einer solchen Kommunikation und Interaktion zwischen Menschen können aber auch immer Spannungen bis hin zu kriminellen Handlungen resultieren. Es bildet sich also dadurch nicht nur ein Kommunikationsnetz, es wird dadurch auch ein intrastellarer Kriminalitätsraum entstehen, in dem ein Mensch auf dem Mond genauso einen Normenbruch begehen kann wie jemand in Österreich oder Deutschland.

Bereits heute liegt der geschätzte Anteil der Weltbevölkerung, die das Internet nutzen, bei etwa 65 Prozent, was ca. 4 Milliarden Menschen entspricht (Statista 2019). Interessanterweise wird geschätzt, dass annähernd genauso viele Menschen Soziale Medien nutzen – also online-basierte Plattformen, die eine Kommunikation und Vernetzung zwischen den Nutzern ermöglichen (Bruhn und Hadwich 2015, S. 3) – (Statista 2021b). Die Bandbreite, was als ‚Soziale Medien' gezählt werden kann, ist entsprechend groß: von klassischen Messenger-Diensten wie WhatsApp und Telegram, über Soziale Netzwerke wie Facebook, Instagram oder TikTok bis zu Onlinegames wie Brawlstars und Fortnite. Alle ermöglichen Interaktion und Kommunikation zwischen ihren Nutzern. Auch in Deutschland gestaltet sich die Medien- und Internetnutzung vergleichbar. Insgesamt 94 Prozent der deutschen Bevölkerung ab 14 Jahren nutzten im Jahr 2020 das Internet zumindest gelegentlich. Das entspricht etwa 51 Millionen Deutschen (Beisch und Schäfer 2020, S. 463). In den

Altersstufen von 14–50 Jahren nutzte faktisch jeder in Deutschland das Internet (Beisch und Schäfer 2020, S. 464). Dabei sind auch hier vorrangig Soziale Medien beliebt. Dementsprechend nutzen 68 Prozent WhatsApp, 15 Prozent Instagram und 14 Prozent Facebook (Beisch und Schäfer 2020, S. 466). Mehr als die Hälfte der deutschen Internetnutzer – 56 Prozent – spielt zudem zumindest gelegentlich Computer- und Videospiele, wobei das Durchschnittsalter über 37 Jahren liegt (game e. V. 2021). Weltweit wird von etwa 3 Milliarden Gamern ausgegangen (Bankhurst 2020). In all diesen Programmen – solange sie einen Onlinemodus besitzen – kann prinzipiell die gesamte Weltbevölkerung aufeinander treffen und miteinander in Interaktion treten. Im Übrigen treffen hier auch annähernd alle Altersstufen aufeinander, was wiederum auch Kommunikationsrisiken gerade für junge Menschen eröffnet (vgl. u. a. Rettenberger und Leuschner 2020; Rüdiger 2020a). Gerade hier stellt sich die Frage, wie eigentlich in diesem Raum der Schutz auch von jungen Menschen und ein sicheres Miteinander gewährleistet werden kann. Denn hierzu braucht es ja gesichertes Wissen um die Mechanismen des Normenbruchs und der Normendurchsetzung in einem digitalen Kontext. Dabei standen gerade die Auswirkungen, die die Möglichkeit der Begehung von Normenbrüchen zwischen Menschen in einem nahezu grenz- und planetenfreien digitalen Raum haben, aber bisher bei kriminologischen Betrachtungen eher selten im Mittelpunkt, oder wie es Meier formuliert „die Veränderungen (haben) demgegenüber nicht – oder jedenfalls nicht in der Breite – zum Aufkommen neuer Forschungsfragen geführt, was bei einem Wandel, der wie die Digitalisierung sämtliche Bereiche der gesellschaftlichen Lebens durchzieht, überrascht“ (Meier 2016, S. 232). Genau hier setzt die Cyberkriminologie als Disziplin an.

1.2 Cyberkriminologie als neue Subdisziplin?

Bereits bei der Entstehung der Kriminologie, also der „Lehre vom Verbrechen“, als eigene Wissenschaft etwa ab dem 19. und 20. Jahrhundert zeichnete sich eine eher national orientierte Betrachtung des jeweiligen Untersuchungsfeldes ab. Damit ist nicht unbedingt nur der berühmte Anlage-Umwelt (nature-nurture) Streit gemeint, der sich bereits nach den Herkunftsländern der beteiligten Wissenschaftlern definierte, also italienische, französische und deutsche Schule (Neubacher 2017, S. 26). Vielmehr ist gemeint, dass das Untersuchungsfeld der Kriminologie, also normenabweichendes oder auch strafbares Verhalten, je nach Gesellschaft unterschiedlich definiert werden kann. Zwar kennen sicherlich die meisten Gesellschaftsformen auf der Welt Handlungen die Besitz oder die körperliche und sexuelle Integrität angreifen. Diese Deliktsformen werden teilweise auch als sog. „delicta mala per se“ erfasst, also Handlungsweisen, die in irgendeiner Form überall als ächtlich geahndet werden (Kunz und Singelnstein 2021, S. 31). Diese stehen den „delicta male mere prohibita“ gegenüber, also Handlungsweisen bei denen Gesellschaften sich selbst entscheiden, ob sie diese als strafbar ansehen oder gerade nicht. Welche Handlungen dann aber individuell genau erfasst werden, ist nicht so klar zu bestimmen. Ein „Diebstahl“ in Deutschland könnte eine völlig andere definitorische Bedeutung haben – im Sinne

der Tatbestandsmerkmale – als eventuell ein Diebstahl in Brasilien oder Japan. Auch wenn es ein Bestreben der Kriminologie ist, allgemeine Gesetzmäßigkeiten für Kriminalität bzw. einen Normenbruch zu definieren, so ist das bisher nicht gelungen. Dahinter steckt auch die Erkenntnis, dass diese Definition stets auch abhängig ist vom jeweiligen gesellschaftlichen Kontext (Rüdiger und Bayerl 2020b).

Dieses Konzept einer eher juristisch ausgeprägten Betrachtung von nach dem jeweiligen Verständnis strafbewährten Normenbrüchen, findet gegenwärtig jedoch seine Grenzen im Internet, d. h. in einem Raum, den sich Menschen weltweit teilen, während sie sich wiederum eigentlich in ihrem eigenen Land befinden. Denn dadurch wird „die analoge Nationalgemeinschaft zur digitalen Weltgemeinschaft“ (Bittner 2019), was bedeutet, dass in diesem global vernetzten Rahmen Kriminalität neu definiert und betrachtet werden müsste. Dabei erscheint es naheliegend, dass hier nicht zwangsläufig dieselben Erklärungsansätze funktionieren müssen wie bei der Betrachtung von Normenbrüchen, die in einem nicht digitalen und nicht weltumspannenden Kontext begangen werden. Dabei kann faktisch angenommen werden, dass analoge Delikte in einem eher nationalen Kontext und digitale Delikte in einem eher globalen Kontext stattfinden (Kigerl 2012, S. 470), das „Risiko der Opferwerdung also unabhängig vom Wohnort“ wäre (Dreißigacker et al. 2020, S. 323). Insgesamt erscheint es deshalb sinnvoll, bei den Erklärungsansätzen zur Entstehung von Normenbrüchen, etwaigen Täterprofilen und Fragen der Viktimologie auch die Besonderheiten dieses digitalen Raumes zu berücksichtigen und zu beschreiben.

Die kriminologische Betrachtung digitaler Deliktfelder steht allerdings noch weitestgehend am Anfang (Meier 2016, S. 232; Huber 2019, S. 25). Erst seit einigen Jahren nimmt sich eine Subdisziplin der Kriminologie diesen Gedankengängen an: die „Cyberkriminologie“ oder im englischsprachigen Raum „Cyber Criminology“ (vgl. u. a. Jahankhani 2018; Maras 2017; Meier 2016; Rüdiger und Bayerl 2020a). Bereits 2007 stellte Jaishankar mit der „Space Transition Theory“ die These auf, dass Menschen sich nach der Überschreitung der Schwelle vom analogen in den digitalen Raum anders verhalten würden und daher Kriminalität auch nicht gleich betrachtet werden könnte (Jaishankar 2007, S. 7 ff.). Mit diesem Ansatz stand er bereits frühzeitig dem Gedanken einer Art digitalen Dualismus gegenüber d. h., der Annahme, dass die digitale und die analoge Welt in einer Parallelität zueinander existieren bzw. sich gegenüberstehen und sich faktisch kaum gegenseitig beeinflussen würden. Er vertritt vielmehr die Annahme, dass kriminelles Verhalten im analogen Bereich auch in den digitalen Bereich importiert werden kann und umgekehrt. Bisherige kriminologische Ansätze seien seiner Ansicht nach aber nicht in der Lage die Begehung digitaler Delikte hinreichend zu erklären (Jaishankar 2007, S. 1 ff.). Entsprechend notwendig wäre eine Adaption oder Ausweitung der Disziplin Kriminologie in Richtung einer Cyberkriminologie.

Diese Adaption erfolgt allerdings nur sehr zaghaft. Gegenwärtig spielen bei den kriminologischen Überlegungen zu digitalen Delikten vor allem „rational choice“ Ansätze bzw. der durch Cohen und Felson ausgearbeiteten Grundsätze der „Routine Activity“ (Cohen und Felson 1979) eine Rolle als Erklärungsansätze (vgl. hierzu auch Bässmann 2015, S. 63; Kigerl 2012, S. 470). In jüngster Zeit scheint zudem ein

Fokus entsprechender theoretischer Ansätze auch vermehrt auf der Frage zu liegen, welche Auswirkungen das häufig von der Politik und Medien titulierte Bild eines rechtsfreien digitalen Raumes eigentlich auf die Hemmschwelle von Nutzern zur Begehung von Delikten haben kann (vgl. u. a. Rüdiger 2018; Steel et al. 2021)

Die Cyberkriminologie, die man als „Lehre von digitalen Normenbrüchen" definieren könnte, kann dabei gegenwärtig am ehesten als eine Art Subdisziplin der Kriminologie verstanden werden. Dabei kann sie auf bereits gemachte Erkenntnisse und Methoden der Kriminologie zurückgreifen und diese für die spezifischen Besonderheiten eines globalen digitalen Raums weiter- und fortentwickeln. Einige dieser Ansätze sollen im Folgenden eingeordnet werden.

2 Betrachtung „Ausgewählte kriminologische Besonderheiten im digitalen Kontext"

2.1 Die „Präventivwirkung des Nichtwissens" im Internet?

Popitz formulierte im Jahr 1968 seine berühmte Hypothese einer „Präventivwirkung des Nichtwissens" (Popitz 1968/2003). Aus der Hypothese können zwei grundlegende Annahmen abgeleitet werden. Das erste ist die Annahme, dass jeder Mensch im Laufe seines Lebens Normenbrüche begeht und auch mit diesen konfrontiert wird, dass also Kriminalität als solches nichts Besonderes ist, sondern normal und allgegenwärtig. Die zweite Annahme basiert darauf, dass zwar vermutlich jeder in seinem Leben Normenbrüche begeht, aber andere Menschen nicht vollumfänglich von diesen Normenbrüchen wissen. Kriminalität ist also nicht transparent, sondern findet weitestgehend im Dunkelfeld statt. Dabei beschreibt Popitz ein Gedankenkonstrukt, bei dem alle Menschen vollumfänglich wüssten, was jeder andere Mensch in seinem Leben schon für Normen gebrochen hätte. Zu Ende gedacht, würde deutlich, wie gering die Wahrscheinlichkeit wäre, dass diese Normenbrüche auch alle geahndet werden würden.

Übertragen auf Polizeiarbeit schließt sich an diese Überlegungen ein weiterer Gedankengang an. Die Sicherheitsbehörden, vermutlich nicht nur in Deutschland sondern weltweit, sind für die Bewältigung des Hellfelds mit personellen und finanziellen Ressourcen und den rechtlichen Befugnissen ausgestattet. Würde nun aber das Dunkelfeld transparent sein, würde die Gefahr einer Überlastung der Sicherheitsbehörden bestehen. Es müsste dann vermutlich selektiert werden, was noch verfolgt werden kann. Das wäre aber gerade in Deutschland mit dem absoluten Gültigkeitsanspruch des Legalitätsprinzips rechtlich nicht erlaubt.

Zum generellen Umfang des Dunkelfelds analoger Delikte und dessen Verhältnis zum Hellfeld schwanken die Angaben und eine Verallgemeinerung ist schwierig, da dies von Delikt zu Delikt unterschiedlich sein kann (Kunz und Singelnstein 2021, S. 279). Im Allgemeinen wird die Dunkelzifferrellation – also das Verhältnis zwischen Hell- und Dunkelfeld – auf etwa 1 zu 3 geschätzt (Schneider 2008, S. 558). Balschmiter et al. bestätigen diese Annahmen im Kern und erarbeiteten bspw. eine Dunkelzifferrellation bei Diebstahl von 1 zu 1, bei Betrug von 1 zu 5 und bei

Sachbeschädigung, Körperverletzungen und Raubdelikten von jeweils 1 zu 2 (Balschmiter et al. 2018, S. 53). Jedoch gibt es auch Extreme in der Dunkelfeld- und Hellfeldbetrachtung. So gibt es Delikte wie den Diebstahl eines Kraftfahrzeugs, bei dem Opfer eine Erstattung der Versicherung nur bei dem Vorliegen einer Anzeige erwarten können, sodass hier angenommen wird, das fast jeder Fall auch zur Anzeige gelangt (Neubacher 2017, S. 11). Andererseits gibt es aber auch Deliktsgruppen, und hier speziell wie Delikte mit digitalem Bezug, bei denen man von einem extrem großen Dunkelfeld ausgeht (Eisenberg und Kölbel 2017, S. 957 ff.).

Ziemlich unstrittig ist jedoch, dass in Deutschland beispielhaft vorsatzgetragene Tötungshandlungen extrem selten sind. So weist das polizeiliche Hellfeld in Form der Polizeilichen Kriminalstatistik (PKS) 2020 insgesamt „nur“ 245 vollendete Mord- und 369 vollendete Totschlagsdelikte, insgesamt also 614 vorsätzliche Tötungen, aus (BMI 2020b TS: 010000; 020010). Im Verhältnis zu der Gesamtzahl der in PKS registrierten Sachverhalte von 5.310.621 entspricht dies einem Anteil von 0,01 Prozent. Berücksichtigt man hierbei, dass für Tötungsdelikte in etwa eine Dunkelzifferrellation von 1 zu 1 angenommen wird (Wegener 2013, S. 93), würde es in Deutschland also in etwa insgesamt 1200 vollendete Tötungsdelikte im Jahr geben. Bei einer Bevölkerungszahl von 83.100.000 Menschen im Jahr 2021 (Statistisches Bundesamt 2021a), entspräche dies einer Häufigkeitsziffer von etwa 1,4 pro 100.000 Einwohner. Zum Vergleich, die Häufigkeitsziffer (HZ) bei Diebstahlsdelikten liegt in Bezug auf das polizeiliche Hellfeld bei 2023 und für alle polizeilich registrierten Sachverhalte zusammen bei 6386 (BMI 2020a). Auch müssen hierbei die klassischen Kritikpunkte an der PKS berücksichtigt werden. Neben den Fehlerindikatoren bei der Erhebung muss vor allem bedacht werden, dass es sich um durch die Polizei an die Staatsanwaltschaft abgegebene Ermittlungsverfahren handelt, die noch keinen Aussagewert über tatsächlich begangene Delikte haben müssen, sodass hier bereits aufgrund des sog. Trichtereffekts der PKS von einer niedrigeren HZ bei Hellfelddelikten ausgegangen werden kann (vgl. zum Trichtereffekt Schneider 2008, S. 553). Seit Jahren ist zudem ein stetiger Rückgang des polizeilichen Hellfeldes zu verzeichnen von 6.372.526 verzeichneten Delikten im Jahr 2016 auf mittlerweile 5.310.621 im Jahr 2020, was einem Rückgang von 16,66 Prozent entspricht. Als Gründe werden vor allem eine Verschiebung hin zu digitalen Delikten vermutet (Balschmiter et al. 2018; Rüdiger 2021). Gleichzeitig stieg laut dem Statistischen Bundesamt das Personal der Polizei auf 341.400 MitarbeiterInnen im Jahr 2020 an (Statistisches Bundesamt 2021b).

Wenn nun das Dunkelfeld tatsächlich in einer Art absoluten Transparenz aufgedeckt werden würde, könnte dies mehrere Effekte haben. Einerseits die bereits beschriebene Erkenntnis der Menschen, dass Normenbrüche als solches durch jeden begangen werden können. Andererseits auch die Erkenntnis, dass nur auf wenige Normenbrüche auch eine Ahndung erfolgt. Dieses Wissen könnte wiederum dazu führen, dass die eigene Bereitschaft, die Normen einzuhalten, sinken würde, da das Risiko einer Begehung als niedriger eingestuft wird. Experimentelle Überprüfungen der These der „Präventivwirkung des Nichtwissens“ von Diekmann et al. deuten auf eine Signifikanz der These hin (Diekmann et al. 2011). Demnach käme der „Dunkelziffer eine normstabilisierenden“ Bedeutung zu (Diekmann et al. 2011, S. 75).

Dies bedeutet, dass es im Interesse einer jeden Gesellschaftsform liegt, dass es keine absolute Verhaltenstransparenz gibt und gewisse Formen vor allem von „Alltagskriminalität", die also tatsächlich nicht selten stattfindet, auch unentdeckt bleibt.

Der digitale Normenbruch und Formen digitaler Kriminalität scheinen im Netz nun diese Konzepte auf den Kopf zu stellen. Denn Nutzer werden offenbar in einer solchen Masse mit Normenbrüchen konfrontiert, dass man von einer Normalisierung und Gewöhnung gar Habitualisierung an diese Delikte sprechen kann. Diese Form der digitalen Kriminalitätstransparenz scheint die beschriebene „Präventivwirkung des Nichtwissens" im Netz ansatzweise zu durchbrechen (Rüdiger 2021). Die Cyberkriminologie steht nun vor der Herausforderung zu beschreiben und zu analysieren welche Auswirkungen diese digitale Kriminalitätstransparenz haben kann.

2.2 Digitale Kriminalitätstransparenz oder von der Gewöhnung an digitale Normenbrüche

Die Frage, ob im Netz tatsächlich eine Form von digitaler Kriminalitätstransparenz herrscht, soll erneut an den Dunkelzifferrellationen entlang betrachtet werden, die bei klassischen analogen Delikten relativ gering sind und grob im einstelligen Bereich festgemacht werden können. Zunächst soll hierfür ebenfalls ein Rückgriff auf die PKS erfolgen. In Deutschland hat sich gegenwärtig eine zweigeteilte Einteilung von digitalen Delikten durchgesetzt: einmal Cybercrime im engeren Sinne – dies entspricht etwa Hackingdelikten – und Cybercrime im weiteren Sinne – also Delikte, bei denen in irgendeiner Form digitale Prozesse eine Rolle zur Tatausführung gespielt haben – sog. Tatmittel Internet (Clages und Gatzke 2020, Kap. II. ff.). Diese Aufteilung findet sich auch innerhalb der PKS wieder (Bundeskriminalamt 2020, S. 42). Demnach wurden 2020 insgesamt 108.474 Fälle von Cybercrime im engeren Sinne (Bundeskriminalamt 2020, S. 10) und 320.323 Fälle über das Tatmittel Internet – also im weiteren Sinne – erfasst (BMI 2020c). Diese Hellfeldzahlen, die sich auch noch auf Deliktgruppen beziehen und nicht auf einzelne Delikte, scheinen im Verhältnis zum Dunkelfeld wesentlich ungünstiger als bei analogen Delikten.

2.2.1 Cybercrime im engeren Sinne

Nach einer Studie des Branchenverbandes der Bitkom gaben im Jahr 2019 alleine 55 Prozent der befragten Internetnutzer ab 16 Jahren an, mit kriminellen Vorfällen im Internet Erfahrung gemacht zu haben (Bitkom 2020). Diese Zahlen scheinen der Höhe nach nicht unrealistisch. Nach einer Erhebung des Bundesamt für Sicherheit und Informationstechnik (BSI) in Kooperation mit der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) im Rahmen des Digitalbarometers 2020 gaben 25 Prozent der Befragten an, innerhalb der letzten 12 Monate Opfer von Cyberdelikten geworden zu sein. Hiervon gab wiederum fast jeder zweite an, Opfer von Betrug beim Onlineshopping gewesen zu sein (BSI und ProPK 2020, S. 4). Nach dem Norton Cyber Safety Insights Report 2021 waren im letzten Jahr 18,3 Millionen Deutsche Opfer von Formen von Cybercrime – vornehmlich Vermögens-

delikten. Insgesamt sollen zudem bereits 28,2 Millionen deutsche Internetnutzer mindestens einmal Opfer eines digitalen Delikts gewesen sein (Norton 2021, S. 9) – was dann auch entsprechend hohe Dunkelfeldzahlen nach sich ziehen würde. Bei Annahme, dass diese Zahlen soweit belastbar wären, würde dies bedeuten, dass es 18.300.000 Millionen Cybercrime Delikte im engeren Sinne in einem Jahr gegeben hat. Bei 108.474 Anzeigen im selben Zeitraum, würde dies einer dies einer Dunkelzifferrellation von etwa 1 zu 168 entsprechen.

2.2.2 Digitale Hasskommentare

Nicht nur eher klassisch anmutende Cyberdeliktsformen – wie Hacking oder Betrugshandlungen – weisen diese hohen Konfrontationsraten aus. Diese finden sich auch im Bereich von Sexual- oder Hassdelikten. Die Landesanstalt für Medien NRW (LFM NRW) erhebt regelmäßig die Konfrontation von Internetnutzern mit Formen von Hatespeech bzw. digitale Hasskriminalität. Insgesamt gaben knapp 76 Prozent der befragten Nutzer ab 14 Jahren an, bereits auf Hasskommentare im Netz gestoßen zu sein, bei den unter 25jährigen waren dies sogar 98 Prozent. Zu beachten ist aber, dass nicht jede Erfahrung in der Studie deckungsgleich mit strafbaren Handlungen sein muss (Landesanstalt für Medien NRW 2021, S. 1). Zum Vergleich lagen die in der PKS registrierten Fallsituationen zu Volksverhetzungen, die über das Tatmittel Internet begangen wurden, im Jahr 2020 bei lediglich 2173 (BMI 2020c, TS: 627000) und für alle Formen von Hasspostings einschließlich der Volksverhetzung bei 2607 (Bundeskriminalamt 2021b, S. 10). Insgesamt nutzten etwa 51 Millionen Deutsche ab 14 Jahren das Internet (Beisch und Schäfer 2020) wobei 76 Prozent mit Erfahrung mit Hasskommentaren knapp 38 Millionen Menschen entsprechen. Wenn davon nur 1 Prozent strafrechtlicher Natur wäre, würde es sich um etwa 380.000 Fälle handeln. Nicht unrealistisch, wenn man betrachtet, dass selbst das Bundesjustizministerium im Rahmen der Begründung zum Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität von etwa 250.000 Anzeigen wegen strafbaren Kommentaren im Jahr in Sozialen Medien ausgeht (Bundesministerium der Justiz und für Verbraucherschutz (BMJV) o. J., S. 26). In Bezug auf die Fallzahlen zu Hasspostings würde dies einer Dunkelzifferrellation von etwa 1 zu 145 entsprechen.

Diese hohe Konfrontationsraten scheinen mittlerweile auch Auswirkungen auf die Entwicklung einer Art von Vermeidungsverhalten zu haben. Nach der U25 Studie des ehemaligen Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI) befürchten 64 Prozent der 14–24jährigen im Netz beleidigt zu werden, was dazu führt, dass 38 Prozent ihre Meinung prophylaktisch nicht mehr äußern (Borchard et al. 2018, S. 67). In diesem Zusammenhang spricht die Studie sogar von einer Beleidigungskultur, denen die jungen Menschen im Netz ausgesetzt sind (Borchard et al. 2018, S. 53). Ähnliche Ergebnisse liegen auch durch die James Focus Studien aus der Schweiz vor. Demnach treffen 48 Prozent der Minderjährigen in der Schweiz mindestens mehrmals in der Woche auf Hasskommentare im Netz, 16 Prozent sogar täglich (Külling et al. 2021, S. 4).

2.2.3 Digitale Sexualdelikte und Cybergrooming

Ähnliche Fallzahlen lassen sich auch im Bereich der Sexualdelikte finden. Nach dem Mädchenreport 2020 berichten weltweit 58 Prozent der Frauen zwischen 15–25 Jahren von sexuellen Belästigungen, Beleidigungen oder auch Stalking (Plan International 2020, S. 17). Hierbei gaben 50 Prozent der betroffenen Frauen an, dass sie entsprechende Belästigungen häufiger in Sozialen Medien als auf der Straße erleben (Plan International 2020, S. 38). Auch Kinder und Jugendliche werden im Netz mit Sexualdelikten konfrontiert. Nach der SOS Kinderdorf Studie haben bereits 9 Prozent der 11–13jährigen Nacktfotos oder -videos erhalten (Kohout et al. 2018, S. 6). Diese Handlungsweisen können nach deutschem Recht als eine Form von Cybergrooming – also der onlinebasierten Anbahnung eines sexuellen Kindesmissbrauchs – gem. §§ 176 a Abs. 1 Nr. 3 und 176 b Abs. 1 StGB erfasst werden (Rüdiger 2020a).

Wichtig gerade bei diesem Phänomen ist es, dass die Strafbarkeit nicht von einer erlebten Viktimisierung des Kindes abhängig ist, sondern lediglich von der Tätermotivation. Insgesamt gaben 24 Prozent aller befragten 11–18jährigen Minderjährigen in Österreich an, bereits eine Form von sexualbasierter Onlinebelästigung erlebt zu haben (Kohout et al. 2018, S. 6). Die Speak Studie aus Deutschland erarbeitete 2017, das 32,7 Prozent der Mädchen und 8,7 Prozent der Jungen zwischen 14–16 Jahren von sexuellen Belästigungen im Internet berichteten (Maschke und Stecher 2017, S. 7). Die Partner 5 Studie erhob hingegen die entsprechende Belastung bei 16–18jährigen. Demnach gaben 46 Prozent der befragten Jugendlichen in dieser Altersgruppe an, sich bereits online belästigt gefühlt zu haben und 40 Prozent wurden ungewollt mit pornografischen Inhalten konfrontiert (Weller et al. 2021, S. 18). Insgesamt berichteten 59 Prozent von dem „Versuch der sexuellen Anbahnung“, weitere 18 Prozent berichteten zudem von Erpressungen durch Bilder und Videos (Weller et al. 2021, S. 24). Bereits im Jahr 2013 kam das LKA NRW im Rahmen des Lagebild Cybercrime zu der Erkenntnis, dass „für viele Kinder und Jugendliche die Annäherung mit sexuellen Motiven bereits selbstverständlicher Teil der Kommunikation im Internet (ist). Es ist von einem großen Dunkelfeld auszugehen“ (LKA NRW 2013, S. 21). Zur Einordnung der Zahlen: In Deutschland leben etwa 6 Millionen Kinder von 6–13 Jahren und 3 Millionen Jugendliche von 14–17 Jahren (Statista 2021a). Auch wenn jüngere Kinder noch seltener ins Internet gehen, kann nach der JIM Studie 2020 davon ausgegangen werden, dass annähernd alle Kinder ab 10–11 Jahren das Internet nutzen (Feierabend et al. 2021, S. 3). Basierend auf den Ergebnissen der dargestellten Studien, müsste es sich alleine bei Kindern und Jugendlichen dann um sechsstellige Konfrontationszahlen im Dunkelfeld handeln.

Das Hellfeld entspricht bei diesen Handlungen noch am ehesten dem bereits angesprochenen Cybergrooming. Dieses weist seit 2009 einen stetige Anstieg der Fallzahlen von 156 auf 2632 Fälle im Jahr 2020 auf (BMI 2020c, TS 131.400). Alleine der Anstieg der Fälle von 2019 mit 1754 Fälle auf 2632 Fälle im Jahr 2020 entsprach einem Zuwachs von 50 Prozent bei einer hohen Aufklärungsquote von 84,7 Prozent (BMI 2020c, TS 131.400). Bei einer niedrig angenommen konservativen Konfrontationsrate (siehe vorgehende Ausführungen) von etwa 100.000 Sachverhalte im Jahr, entspreche dies einer Dunkelzifferrellation von 1 zu 37, bei

einer ebenfalls nicht unbegründbaren Annahme von 500.000 Konfrontationen bereits von 1 zu 189. Dass auch diese Zahlen nicht völlig unrealistisch sind, zeigt erneut die Studie von Balschmiter et al. Diese ergab eine Dunkelzifferrellation bei Computerkriminalität im Allgemeinen von 1 zu 135 und im Zusammenhang mit dem unerwünschten Zusenden pornografischer Medien – was häufig auch als Phänomen „Dickpic" erfasst wird und auch bei Cybergrooming eine Rolle spielt – von 1 zu 404 (Balschmiter et al. 2018, S. 53).

2.2.4 Phisingmails als Sinnbild der Kriminalitätstransparenz

Zunächst kann also festgehalten werden, dass die Dunkelzifferrellation bei nahezu allen betrachten digitalen Delikten wesentlich höher liegt, als bei analogen Delikten. Das heißt, man kann hier tatsächlich von einer wesentlich häufigeren Konfrontationsrate und gleichzeitig einer geringen Anzeigebereitschaft ausgehen. Gleichzeitig ist damit die Wahrscheinlichkeit einer Konfrontation mit kriminellen Aktivitäten und damit deren Sichtbarkeit – Transparenz – im digitalen Raum offenbar wesentlich höher als aus dem physischen Raum bekannt ist.

Eine Situation, die vermutlich viele Menschen nachvollziehen können, ist, wenn sie dubiose Geschäftsvorschläge von unbekannten Freundschaftsanfragen in Sozialen Medien erhalten, oder schlicht wenn sie täglich in ihren Spamfilter schauen. Weltweit sollen täglich etwa 319 Milliarden Emails versendet werden, von denen im Dezember 2019 etwa 57 Prozent Spammails gewesen sein sollen. Dies würde pro Tag in etwa 180 Milliarden Spammails bedeuten (Krah 2021). In einem Jahr würden dies kaum fassbare Zahlen im Billionen Bereich ergeben. Nicht alle Spammails stellen natürlich auch strafbare Handlungen wie versuchte oder erfolgreiche Betrugs- oder Erpressungsdelikte dar. Am eindeutigsten können hier noch die sog. Phishingemails erfasst werden und solche die sog. Malware beinhalten. Es wird geschätzt, dass von diesen 180 Millarden täglichen Spammails etwa 4,7 Milliarden zu den strafbaren Phishingmails gezählt werden können (Avanan 2021).

Wenn man bedenkt, dass Deutschlands Anteil an der Weltbevölkerung in etwa 1 Prozent entspricht, wären dies wiederum 4,7 Millionen Phishingmails täglich. Selbst wenn hiervon wiederum nur ein Prozent der Emails tatsächlich die Schwelle zur Strafbarkeit nach deutschem Recht überschreiten würde, entspräche dies immer noch etwa 50.000 Delikte am Tag. Viele Betroffene werden dabei vermutlich die Phisingemails einfach ignorieren und gar nicht als Konfrontation mit Kriminalität erfassen. Huber geht davon aus, dass einige Betroffene nicht davon ausgehen, „dass der oder die Täter nicht gefasst werden können, also sehen sie auch keine Relevanz darin, die Vorfälle zur Anzeige zu bringen" (Huber 2019, S. 52). Kemme und Querbach sehen die Tendenz, dass Cyberdelikte als „weniger strafwürdig angesehen" werden, was sich auch in der Anzeigequote widerspiegeln würde (Kemme und Querbach 2020, S. 539).

Diese tägliche Konfrontation mit digitalen Delikten könnte Menschen im Gegenzug auch zeigen, wie gering offenbar die Angst der TäterInnen vor Strafverfolgung ist, was wiederum auch darstellt, dass das Risiko der TäterInnen tatsächlich gering

ist. Im Netz scheint also die „Präventivwirkung des Nichtwissens“ durchbrochen und Kriminalität wird für die Nutzer transparent. Das Ergebnis könnten fallende Hemmschwellen und eine Form von Gewöhnung im digitalen Raum bedeuten, die diesen Prozess weiter antreiben.

3 Formen formeller Kontrolle im digitalen Raum

Nach einer Betrachtung der Problematik der Normalität und Transparenz digitaler Delikte stellt sich auch die Frage, wie die formelle Kontrolle agiert, um diesen Mechanismen zu begegnen.

3.1 Funktion der digitalen Präsenz der Sicherheitsbehörden

Die Polizeiarbeit in Deutschland hat zwei primäre Funktionen: die Strafverfolgung und die Gefahrenabwehr. Die damit einhergehenden polizeilichen Initiativpunkte können einerseits von außen an die Polizei herangetragen werden, bspw. durch Hinweise an die Polizei durch Bürger, Strafanzeigen oder auch durch Mitteilungen anderer Behörden oder Institutionen. Andererseits können die Sicherheitsbehörden auch durch proaktive Handlungen selbst diese Initiativpunkte setzen. Nichts anderes sind die unterschiedlichen uniformierten Streifenformen der Polizei. Dabei ist es unwahrscheinlich, dass eine polizeiliche Streife tatsächlich auch proaktiv auf Straftaten trifft. So wird angenommen, dass zwischen 85–95 Prozent aller Anzeigen nicht auf die Strafverfolgungsbehörden zurückzuführen sind, sondern auf die Opfer selbst (Kunz und Singelnstein 2021, S. 307). Entsprechend gering muss die Rate der Anzeigen durch die Polizei selbst sein. Dies ist nachvollziehbar, denn eine Polizeistreife müsste ja zum Zeitpunkt der Tatausführung am konkreten Ausführungsort sein oder dort vorbeikommen. Bis auf Delikte wie Sachbeschädigungen – man denke hier z. B. an Graffitis oder die berühmten eingeschlagenen Fensterscheiben – die eine längerfristige Sichtbarkeit der strafbaren Handlung ermöglichen, sind kriminelle Handlungen auf der Straße aber eher flüchtiger Natur.

Während die Polizei Streife fährt oder läuft, kann sie also nicht erkennen wo innerhalb der letzten Tage Diebstähle, sexuelle Belästigungen oder auch Körperverletzungen begangen wurden, sofern diese nicht gemeldet wurden. Die Funktion der uniformierten Streifen scheint also weniger die proaktive Suche nach Straftaten zu sein. Vielmehr sind durch die Uniform Polizisten ansprechbar und erkennbar. Gleichzeitig besteht für jeden Teilnehmer am Straßenverkehr eine gewisse zufällige Wahrscheinlichkeit auf eine Streife zu treffen oder auch nicht, die letztlich eine generalpräventive Wirkung entfalten soll. Eine Untersuchung von Simpsons et al. in Kanada hat beispielsweise ergeben, dass bereits „Polizei Dummys“ – in der Studie wird der Begriff „Constable Scarecrow“ genutzt – eine präventive Wirkung auf die Einhaltung von Geschwindigkeitsbegrenzung haben können (Simpson et al. 2020).

Die wahrnehmbare Präsenz entfaltet also bereits eine präventive Wirkung. Man stelle sich im Gegenzug einen Straßenverkehr ohne zufällige und sichtbare Polizeistreifen vor.

So ähnlich ist aber gegenwärtig die Situation im digitalen Raum. Es gibt keine sichtbaren Polizeistreifen auf die ein Internetnutzer einfach zufällig im Netz stoßen könnte, so wie im Straßenverkehr auf eine Polizeistreife. Zwar gibt es sog. „anlassunabhängige Internetrecherchen", hier handelt es sich jedoch um reine Recherchemaßnahmen, bei denen die Polizei zwar gff. nach Straftaten sucht, dies aber nicht sichtbar für die Nutzer tut. Vor allem erfolgt auch keine für andere Nutzer sichtbare Sanktion, wie beispielsweise das Anhalten von jemandem, der zu schnell gefahren ist. Online entfällt also die präventive Wirkung einer uniformierten Streife. Nicht mal diese verdeckten Streifen werden jedoch offenbar bei allen Landespolizein betrieben (Wilke 2019). Eine wirklich sichtbare Form von Polizeistreifen digitale Polizeistreifen konnte in Deutschland nicht gefunden werden.

Auch in Situationen in denen Plätze, Viertel oder Ähnliches das Attribut der „Rechtsfreiheit" zugeschrieben wird, wird nicht selten die Erhöhung der uniformierten Präsenz der Polizei gefordert bzw. durchgeführt (Heitkamp 2020; Wurtzbacher 2008, S. 218). Dabei müssen die Sicherheitsbehörden dann auch damit rechnen, dass in einer solchen Situation durch mehr Polizeipräsenz die Kriminalstatistiken nicht sinken, sondern steigen. Dieser auch als Lüchow-Dannenberg-Syndrom bekannte Effekt (Schwind 2016, S. 59) beschreibt den Umstand, dass die Polizeipräsenz einerseits zu mehr Kontrollen durch die Polizei führt und andererseits für die Einwohner durch die direkte Ansprechbarkeit der PolizeibeamtInnen, die Hemmschwelle zur Meldung eines Normenbruchs geringer geworden ist. Im Ergebnis würden mehr Straftaten gemeldet und aufgedeckt und die Kriminalstatistiken steigen. Das muss dann beispielhaft eine Kriminalpolitik auch aushalten können. Der Umkehrschluss wäre, je weniger Polizeipräsenz existiert, umso niedriger sind die Kriminalstatistiken. Ein Umstand der durchaus auch kriminalpolitisch eingesetzt werden kann.

Wenn man diese Situation als Hypothese für den digitalen Raum formulieren würde, würde es heißen, dass digitale Polizeipräsenz, im Sinne einer zufälligen Wahrnehmbarkeit beim alltäglichen Surfen in Sozialen Medien, eine generalpräventive Wirkung entfalten könnte. Dies könnte die Hemmschwelle im Netz für den Normenbruch erhöhen und damit auch das sog. Brokenweb Phänomen, also das die Sichtbarkeit von Normenbrüchen und der fehlenden Sanktionierung das Gefühl der Rechtsfreiheit näher bringen und damit die Hemmschwelle zur Tatbegehung senken (vgl. dazu Rüdiger 2018, S. 259 ff.). Gleichzeitig würde die Bereitschaft zur Anzeige und damit das Hellfeld steigen und mittelbar das Dunkelfeld sinken.

Eine solche Durchbrechung der beschriebenen „Präventivwirkung des Nichtwissens" im digitalen Raum erfordert auf nationaler Ebene vor allem die sichtbare Erhöhung der Strafverfolgungswahrscheinlichkeit und das Signal an die Nutzer, dass der Rechtstaat aktiv sein Gewaltmonopol, soweit es möglich ist, auch im Netz wahrnehmen wird. Insbesonders die sichtbare und damit für den Nutzer wahrnehmbare Präsenz der Sicherheitsbehörden, und hier vor allem der Polizei, wäre hierbei ein kriminalpolitischer Ansatz.

3.2 Erscheinungsformen digitaler Präsenz der Polizei

Eine Studie der Bitkom kommt zu dem Ergebnis, dass knapp 90 Prozent der befragten Internetnutzer ab 16 Jahren eine höhere Präsenz der Polizei im digitalen Raum verlangen und ebenso viele fordern spezielle Polizeieinheiten die gegen Internetkriminalität vorgehen (Bitkom 2021). Mit welchen Erscheinungsformen ist die Polizei aber im digitalen Raum präsent?

Internet- und Onlinewachen Die gegenwärtige digitale Polizeipräsenz der deutschen Sicherheitsbehörden – im Sinne einer Wahrnehmbarkeit durch die Nutzer – ist dual gestaltet. Einerseits gibt es 16 Internet- oder auch Onlinewachen genannte Präsenzen der Landespolizein und eigene Internetseiten von allen relevanten Sicherheitsbehörden, wie dem BKA, der Bundespolizei oder auch dem Zoll (Bundeskriminalamt 2021a). Auf den Internetwachen können durch die Nutzer Hinweise und Anzeigen gegeben werden. Hier stellt sich auch die Frage, in wiefern es in einem globalen digitalen Raum sinnvoll ist, dass jedes Bundesland eine eigene Onlinewache betreibt und warum es nicht für Deutschland eine Art ‚Single Point of Contact' für Anzeigen gibt. Auch erscheint es zumindest fraglich, ob solche Wachen eigentlich von der Gestaltung her dafür geeignet sind, dass beispielhaft Kinder sich im Rahmen von Quarantäne-Situationen direkt und unkompliziert mit ihren Sorgen an die Polizei wenden können.

Die zweite Ebene digitaler Polizeipräsenz stellen die Social Media Accounts der Sicherheitsbehörden dar. Hier gibt es auch eine zwei- bis dreiteilige Aufsplittung (vgl. zur Struktur Bayerl und Rüdiger 2017, S. 919 ff.).

Institutionelle Polizeiaccounts Zunächst existieren die institutionellen Accounts. Das waren im Jahr 2020 insgesamt 368 Accounts von 216 Polizeibehörden oder deren Einrichtungen – z. B. Direktionen, Inspektionen und Hochschulen (Böber 2020). Knapp 44 Prozent – insgesamt 163 – der Accounts werden dabei auf Twitter, 38 Prozent auf Facebook – 142 – weitere 11 Prozent auf Instagram – 43 – betrieben. Die übrigen verteilen sich auf u. a. auf Youtube, Snapchat, TikTok oder auch LinkedIn. Polizeiliche Accounts im Bereich des Onlinegamings, trotz deren Relevanz gerade für jüngere Zielgruppen, sind nicht vorhanden (zur Kritik an dieser Situation Rüdiger 2020b). Auch wenn diese Zahlen recht hoch klingen, sind sie doch gemessen an der Personaldichte der deutschen Polizeibehörden von 341.400 MitarbeiterInnen und im internationalen Vergleich als sehr niedrig einzustufen. Alleine die niederländische Polizei hatte bereits 2018 insgesamt 3400 sog. „Wijkagenten" – also digitale Streifenpolizisten – in den Sozialen Medien im Einsatz mit alleine bei Twitter über 2200 Accounts (Vandeputte 2018) bei insgesamt 63.000 MitarbeiterInnen (Politie 2021). Umgerechnet würde dies in Deutschland etwa 10.000 Accounts entsprechen.

Personifizierte dienstliche Polizeiaccounts Seit einigen Jahren setzen manche Landespolizeien zudem – zumindest zaghaft – auf das Konzept des sog. „digital Community Policing", also Polizeiangehörige die mit ihren dienstlichen und individuellen Polizeiaccounts in Kommunikation mit den Nutzern treten, sog. „InstaCops" (Polizei Niedersachsen 2021; Rüdiger 2018, S. 285). Dies kann im aktiven Streifendienst erfolgen (vgl. z. B. Polizei Berlin Helena 2021) oder auch im Rahmen

von Imagemaßnahmen beispielhaft an den Polizeihochschulen (vgl. z. B. Annes Vlog 2021). Als Vorreiter dieses Konzepts in Deutschland kann die Polizei des Landes Niedersachsen angesehen werden, die mittlerweile bereits 22 entsprechende Instacops einsetzt (Polizei Niedersachsen 2021). Insgesamt dürfte sich die Anzahl aller offiziellen personalisierten Polizeiaccounts im mittleren zweistelligen Bereich bewegen.

Private Polizeiaccounts Neben diesen relativ wenig offiziellen Accounts, existiert eine unüberschaubare Anzahl an privaten Accounts von PolizeibeamtInnen, die sich aber gleichzeitig auch als PolizeibeamtInnen darstellen und auch Einblicke in ihren Arbeitsalltag liefern. Dass diese Accounts auch Fragestellungen sowohl für die PolizistInnen selbst als auch für die Polizeiinstitutionen mit sich bringen kann, erscheint naheliegend. So ist mit Adrienne Koleszár die wohl bekannteste (ehemalige) deutsche Polizistin mit einem solchen Account mit über 560.000 Tausend Abonnenten mittlerweile aus dem Polizeidienst ausgestiegen (adrienne_koleszar 2021). Im Rahmen eines Interviews spricht sie davon, das sich die Polizei schwer getan habe im Umgang mit ihr (RTL 2021). Dass die Sicherheitsbehörden offenbar tatsächlich mit Accounts ihrer BeamtInnen in Social Media hadern, ist naheliegend. Teilweise weisen diese Accounts – wie der von Koleszár – mehr Reichweite auf als offizielle institutionelle Polizeiaccounts, womit diesen auch eine größere Rolle bei der Außendarstellung und auch institutionellen Definition der Polizei zugesprochen werden kann. Gleichzeitig könnte aber auch gefragt werden, ob nicht die erhöhte Sichtbarkeit durch inoffizielle Polizeiaccounts auch irgendeine Form von generalpräventiver Wirkung entfalten könnte. Hier wären sicherlich spannende Forschungsfragen zu formulieren. Ein einheitliches Vorgehen der Polizein bei diesem Thema ist zudem nicht ersichtlich. Die Polizei des Landes Baden-Württemberg verbot bereits 2019 ihren PolizistInnen jegliches privates fotografieren oder videografieren, wobei explizit das danach gehende Veröffentlichen auf Social Media Accounts im Vordergrund stand (Wehaus 2019). Die Berliner Polizei hingegen hat extra Social Media Richtlinien für die eigenen BeamtInnen erstellt (Reuter 2020).

Die Sicherheitsbehörden sind also im Ergebnis nur gering mit eigenen Auftritten in den Sozialen Medien präsent und suchen noch eine Linie, um mit den privaten Accounts ihrer MitarbeiterInnen umzugehen.

3.3 Digitale „Kommunikationsfurcht“ bei den Sicherheitsbehörden?

Betrachtet man gegenwärtig offizielle Social Media Accounts der Polizei beispielhaft auf Twitter und Instagram fällt bei vielen sofort folgender Hinweis in der Profilbeschreibung auf „Keine Anzeigen, Kein 24/7 (Monitoring)“ (vgl. u. a. Polizei Berlin 2021; Polizei Saarland 2021; Polizei Thüringen 2021). Teilweise erfolgen noch Verweise auf Notrufnummern und Ähnliches. Dennoch erscheinen diese Hinweise vor dem Hintergrund des Legalitätsprinzips zunächst überraschend. Nach § 158 StPO ist eine Strafanzeige formlos mündlich oder schriftlich bei der Staatsanwaltschaft, den Amtsgerichten oder den Beamten und Behörden des Polizeidienst

möglich. Das Legalitätsprinzip nach §§ 152 Abs. 2 i. V. m. 163 Abs. 1 Satz 1 StPO bedeutet wiederum, dass die Staatsanwaltschaft und die Polizei verpflichtet sind, jedem verfolgbaren Anfangsverdacht einer Straftat auch nachzukommen. Die Staatsanwaltschaft hat dann Einstellungsmöglichkeiten, die Polizei jedoch nicht (Roggenkamp und König 2021, RN. 347 ff.).

Dieses Konzept war jedoch für eine Situation gedacht, in der Kriminalität nicht wie im Netz für die Polizei transparent ist und per Mausklicks selbst aufgerufen werden kann. Es war für einen Raum gedacht, in der die Polizei selbst auf relativ wenig Kriminalität aktiv stößt und dann aber die Anzeigen der Bürger ohne weitere Abwägung und Gewichtung aufzunehmen hat. Schon ohne den digitalen Kontext gibt es Kritik an diesem Prinzip, auch da andere Rechtsstaaten ihren Polizeien wesentlich mehr Freiräume in dieser Hinsicht lassen (Roggenkamp und König 2021, RN. 351 ff.). Dies könnte auch ein Grund für die im Verhältnis geringe Polizeipräsenz im Netz in Deutschland sein. Der Hintergrund dieser Hinweise wird vermutlich in einer Mischung aus verschiedenen Faktoren von Personalressourcen bis ggf. zur Angst einer „Überschwemmung" mit Anzeigen liegen. Das Problem scheint dabei offenbar auch zu sein, dass die schnelle Ansprechbarkeit in Sozialen Medien die Hürde für eine Anzeige oder die Mitteilung von Hinweisen niedrig hält, und die gesamte polizeiliche Verfahrensstruktur nicht darauf ausgerichtet ist. Ein Mitarbeiter des Social Media Teams der Münchener Polizei formulierte dies wie folgt: „[. . .] Außerdem hat die Ansprechbarkeit der Behörden zugenommen. Und auch das Meldeverhalten hat sich geändert. Es gibt sogar Gruppen, die organisiert nach möglichen Straftaten im Netz suchen und uns dann einen Schwung Links schicken" (Oswald 2020). Wie schwierig der Umgang mit dieser Situation und der Konfrontation mit der digitalen Kriminalitätstransparenz offenbar ist, wird dann durch das anschließende Zitat deutlich: „Wir sind ein digitaler Streifenwagen, der wir gar nicht sein wollen" (Oswald 2020). Auch wenn in diesem Zusammenhang die Frage naheliegt, wer denn außer der Polizei denn überhaupt eine digitalen Funkstreifenwagen darstellen kann, scheint die Diskrepanz, die daraus spricht, interessant. Die Nutzer scheinen offenbar die Polizeipräsenz im Netz wie im physischen Raum wahrzunehmen und fordern sogar eine Erhöhung der Polizeipräsenz und intensivere Maßnahmen gegen digitale Delikte (Bitkom 2021). Die Sicherheitsbehörden selbst scheinen hingegen eine gewisse Hemmschwelle zu haben, diese Funktionen auch wahrzunehmen, vermutlich auch weil sie zu recht eine Art Arbeitsunfähigkeit befürchten.

Sie wollen also offenbar eher ein passiver Teil des digitalen Raums sein, aber diesen nicht als echten polizeilichen Einsatzraum definieren. Denn das Lüchow-Dannenberg-Syndrom verdeutlicht, dass wenn mehr Polizeipräsenz im Netz vorhanden und auch ansprechbar wäre, die Kriminalstatistiken entsprechend steigen würden. Da die Polizei aber beim Legalitätsprinzip keine Ausnahmen kennt, würde sie mit der Aufhellung des Dunkelfelds auch mit der Kriminalität eines globalen digitalen Raums konfrontiert werden und müsste auch alles anzeigen. Dazu kommt, dass die Delikte relativ schnell durch Nutzer gesichert und angezeigt werden können. Die dargestellte Auseinandersetzung zu den Dunkelzifferrellationen zeigt aber mit welchen Fallzahlen hier gerechnet werden könnte. Auch kriminalpolitisch ist es

vermutlich attraktiver, sinkende Fallzahlen in der PKS zu verkünden als steigende, mit einer vermutlich dann sinkenden Aufklärungsquote.

Dies mag auch erklären, warum trotz einem Rückgang von knapp 16 Prozent – knapp 1 Millionen Delikte seit 2016 – in allen Fallzahlen der PKS bisher offenbar kein vergleichbar großer Ressourcentransfer ins Netz stattgefunden hat. Noch 2017 kam eine Erhebung zu dem Ergebnis, dass lediglich 1823 PolizistInnen in ganz Deutschland für digitale Themen zuständig waren, was unter 1 Prozent des damaligen Personalkörpers ist (Rüdiger 2019). Dabei steht Deutschland mit dieser Größenordnung nicht allein dar. In Österreich verkündete der Innenminister 2020, dass er aufgrund der Zunahme von digitalen Delikten beabsichtigt bei einem Personalkörper von insgesamt 23.000 Mitarbeiter die Zahl der sog. Cybercops von 300 – 1,3 Prozent – auf 600 – 2,6 Prozent – zu verdoppeln (BMI.AT 2020). Eine aktuellere Personalstärke in diesem Bereich konnte für Deutschland nicht mehr festgestellt werden. Es ist jedoch zu vermuten, dass die Personalstärke ähnlich wie in Österreich verstärkt wurde. Wenn man jedoch berücksichtigt, dass ein großer Teil der Lebenszeit der Menschen in den digitalen Raum verschoben wurde, stellt sich die Frage, ob diese bisherigen Bemühungen ausreichend sind. Eine Verlagerung der Ressourcen analog zum Rückgang der PKS, würde in Deutschland in etwa 30–45.000 MitarbeiterInnen in diesem Bereich entsprechen. Zum gegenwärtigen Zeitpunkt sind solchen Personalzahlen reine Utopie.

Eine Schlussfolgerung dieses geringen Personalansatzes könnte daher die beschriebene „Kommunikationsfurcht“ bei den Sicherheitsbehörden als eine Art Gegenmechanismus sein. Je weniger Kontakt mit den Nutzern und je weniger Präsenz, umso weniger potenzielle Anzeigen sind zu erwarten. In Bezug auf eine ähnliche Problemlage bei der IT-Struktur der Polizei, spricht ein Vertreter des Bundes der Kriminalbeamten (BdK) in einem Interview sogar davon, dass die „Strukturen verhindern oder vereiteln, dass wir (Anmerkung: Polizei Hamburg) Strafverfolgung betreiben“ (Mayer 2021).

Es führt aber noch zu einem weiteren Punkt. Im Netz könnte eine Situation eintreten oder schon eingetreten sein, in der zwar die Polizei zumindest rudimentär sichtbar präsent ist, aber diese geringe Präsenz keine generalpräventive Wirkung im Sinne des Broken Web Ansatzes (Rüdiger 2018) mehr entfalten kann; so ähnlich, als wenn zwar die Polizei an einer roten Ampel steht, aber nicht handelt, wenn jemand über die Ampel rübergeht und dies alle Umstehenden registrieren. Dies könnte Menschen zeigen, dass die formelle Kontrolle kein allzu großes Interesse an der Ahndung eines Normenbruchs hat, das Risiko des Normenbruchs also gering ist. Entsprechend sinkt die Hemmschwelle.

Anzeichen für so eine Situation finden sich durchaus. Die Polizei München veröffentlichte auf ihrer Facebook Seite am 30. Juli 2021 einen Zeugenaufruf zu einer Vergewaltigung einer 15jährigen Schülerin (Polizei München 2021b). Innerhalb der nächsten 24 Stunden hat die Polizei 525 Kommentare auf diesen Post erhalten. Darunter waren so viele von der Polizei als „Hassnachrichten“ eingestufte Kommentare, dass sie 405 Kommentare verbergen mussten (Abendzeitung München 2021). Im Ergebnis stellte die Polizei erstmalig in ihrer Geschichte die Kommentarfunktion ab und sprachen dabei explizit von „Hatespeech und Victim Bla-

ming“ (Polizei München 2021a). Im Nachgang einer Demonstration zur „Coronapolitik“ im August 2020 kam es der Berliner Polizei gegenüber zu einer ähnlichen Situation. Hier sollen alleine an einem Tag 30.000 Tickets durch das zugehörige Moderationsteam bearbeitet worden sein, statt normalerweise 3000. Hiervon soll ein signifikanter Anteil auch grenzüberschreitend gewesen sein. Als Beispiele entsprechender Kommentare werden genannt „Mörder“, „Faschisten“, „Verbrecher“, „Freund & Henker“. Eine Behördensprecherin wird damit zitiert: „der Hass ist plattformunabhängig, er erreicht uns massiv auf Twitter, aber ebenso auf Facebook und Instagram“ (Welt 2021). Vergleichbare Konstellationen waren bisher für die Polizei in Deutschland nicht recherchierbar und könnten auf eine veränderte Wahrnehmung der Polizeipräsenz im Netz hindeuten. Offenbar ist bei einigen der Nutzer der Eindruck entstanden, dass selbst das Risiko der Normenüberschreitungen bei Polizeiaccounts niedrig ist, sodass hier die Hemmschwelle entsprechend gesunken ist. Diese Situation könnte getragen werden durch das bereits beschriebene generelle Gefühl der Rechtsfreiheit im Netz.

4 Ist das Internet ein anomischer Raum?

Die Etablierung des digitalen Raumes hat ohne Zweifel das Potenzial, die vermutlich grundlegendsten gesellschaftsüberspannenden sozialen Transformationsprozesse des 21. Jahrhundert einzuleiten. Durch das Netz ist ein gesellschafts-, kultur- und rechtsüberspannender Kommunikations- und damit auch Kriminalitätsraum entstanden. Dieser Umwandelungsprozess führt zwangsläufig auch zu immensen Unsicherheiten und Regulierungsproblemen. Insofern ähnelt der digitale Raum gegenwärtig dem Konzept eines anomischen Raums nach Durkheim (Durkheim 2016), also einer Situation, in der die Regulierung bzw. Durchsetzung von Normen nicht mithalten kann mit den gesellschaftlichen Umbruchsprozessen, wodurch eine Art rechtsdurchsetzungsfreie Situation entsteht. Dabei verkennt Durkheim nicht, dass Normenbruch und damit auch Kriminalität die Realität jeder Gesellschaft ist, aber er geht davon aus, dass es ein zu viel und ein zu wenig geben kann. Er vergleicht es mit einer pathologischen Fieberkurve: zu wenig Temperatur (also zu wenig Normenbruch) ist ungesund und zu viel ebenfalls (Kreissl 2019, S. 246). In einem anomischen Raum ist der Normenbruch über eine Art Kipppunkt hinausgelangt. Menschen wird ersichtlich, dass Normen nicht mehr allgemeingültig geteilt werden und vor allem der Normenbruch nicht mit einer hinreichenden Wahrscheinlichkeit geahndet wird, die formelle Normenkontrolle also schlicht überfordert oder desinteressiert ist. Dies führt dann schlussendlich zu immer weiteren Normenbrüchen, einer Art anomischen Kreislauf. Es entsteht eine Situation, in der sich eine Gesellschaft neu strukturieren, wieder gemeingültige Normen finden und eine formelle Kontrolle schaffen muss, die in der Lage ist, diesen Normenbruch auch zu ahnden.

Wie dargelegt deuten Anzeichen daraufhin, dass im Netz ein solcher anomischer Kipppunkt offenbar nicht erst jetzt, sondern schon seit einiger Zeit eingetreten sein könnte, bezogen auf Deutschland. Kriminalität ist demnach in einer Form auch grenzüberschreitend für die Nutzer präsent, was für diese auf ein Versagen der

formellen Kontrolle hindeutet. Digitale Delikte bedeuten auch, dass Gesellschaften gleichzeitig mit TäterInnen auf der ganzen Welt konfrontiert werden. Dies stellt alle Formen formeller Kontrolle vor immense bis faktisch kaum lösbare Herausforderungen. Selbst in Deutschland besteht zwischen den einzelnen Polizeien der Länder und des Bundes die Gefahr, dass gleichzeitig an denselben Sachverhalten ermittelt wird. Der Vize-Landesvorsitzende des BDK Sachsen formuliert es in einem Interview zur Bekämpfung von digitaler Hasskriminalität wie folgt: „Diese Gefahr der Redundanzen ist aufgrund der Beschaffenheit des Internets als sehr hoch anzusehen. Der Kollege in Sachsen hat oftmals keine Kenntnis von den parallelen Ermittlungen in anderen Bundesländern. Hierdurch werden enorme polizeiliche Ressourcen gebunden.“ (Wilke 2019). Krischok (2018) arbeitete zudem heraus, dass auch im Bereichen der polizeilichen Gefahrenabwehr diese Probleme bestehen. Diese erfordern normalerweise die Feststellung der sog. örtlichen Zuständigkeit. Normalerweise ist dies eine reine Formalität; soll bedeuten, dass ein Polizist des Landes Bayern auch in Bayern tätig wird, aber wenn er in einem anderen Bundesland aktiv wird, es entsprechende Vereinbarungen geben muss. Der Kern ist, ein Polizist eines Bundeslandes hat nur in seinem Bundesland tätig zu werden und unterliegt auch nur dessen Polizeigesetz. Es gibt aber im digitalen Raum keine feststellbaren Landesgrenzen von Berlin oder dem Saarland. Aufgrund dieser kaum feststellbaren örtlichen Zuständigkeiten findet eine Verbrechensverhütung und Formen polizeilicher Gefahrenabwehr kaum statt (Krischok 2018).

Eine langfristige und strukturelle Lösung könnte in der Etablierung einer Art digitalen Weltstrafrechts liegen mit einer Institution, die den Normenbruch auch ahnden kann. Das würde bedeuten, das nicht jedes Land mit seinen Ressourcen einen gemeinsamen Raum versucht zu regulieren, sondern die Ressourcen gebündelt werden. Ein Zwischenschritt könnten hier entsprechende Initiativen im selben Sprachraum darstellen, beispielhaft zwischen den DACH-Ländern. Erst solche kriminalpolitischen und rechtlichen Prozesse scheinen überhaupt geeignet, das Gefühl der Rechtsfreiheit und niedrigen Strafverfolgungswahrscheinlichkeit, also dem Broken Web Phänomen, zurückzudrängen.

5 Schlussfolgerungen aus dem Blickwinkel der Cyberkriminologie

Die offenen Fragen und Überlegungen ließen sich vermutlich noch beliebig weiterführen. Es zeigt sich aber bereits, wie immens offenbar die bisherigen kriminologischen Forschungslücken, die u. a. solche Überlegungen auszulösen vermögen, tatsächlich sind. Wie können Konzepte uniformierter Polizei ins Netz transportiert werden? Welche Auswirkungen hat eine solche Polizeipräsenz überhaupt auf die Nutzer? Hat es eine präventive Wirkung, wenn ein deutscher Nutzer im Netz auf einen ausländischen Polizeiaccount stößt? Kann es gar eine negative Wirkung haben, wenn Nutzer im Netz auf Polizei stoßen, diese aber nicht auf Normenverstöße reagieren oder gar aus ganz anderen Ländern stammen? Welche Auswirkungen hat es, wenn Menschen im Netz mit Handlungen konfrontiert werden, die im eigenen

Land strafbar wären, aber nicht in dem Land, in dem der jeweilige Nutzer sitzt? Führt eine Enthemmung im Netz auch zu einer Enthemmung bei analogen Delikten? Sind Rechtsstaaten überhaupt noch in der Lage im Netz Regeln durchzusetzen, oder werden vielmehr IT-Firmen wie Meta und Co diese Funktion übernehmen? Und so weiter.

Auch wenn viele dieser Fragen noch nicht angegangen werden, wird die Beantwortung aber eine wichtige Rolle dabei spielen, wie wir den digitalen Raum als eine Art Weltgemeinschaft erleben werden und wie das Miteinander im Netz gestaltet werden soll. Es ist vermutlich auch für die Kriminologie eine der größten Herausforderungen ihrer noch jungen Geschichte, sich auf diese Fragen einzustellen. Dabei bietet der digitale Raum für die Kriminologie nicht nur Herausforderungen, er bietet ihr bisher auch kaum vorhandene methodische Chancen. Letztlich reicht ein digitales Endgerät und engagierte Wissenschafter und Wissenschaftlerinnen, um Kriminalitätsentwicklungen und Verhalten von Menschen auf der ganzen Welt im Netz beobachten zu können. Oder ein Forscher, der selbst die digitalen Medien im Sinne einer teilnehmenden Beobachtung nutzt, indem er sich in Communitys, Foren oder Games begibt, oder einfach in dem er Suchfunktionen in Sozialen Medien nutzt, um Kriminalität zu ergründen. Denn wann war es Kriminologen schon möglich so einfach vom Büro aus Experimente durchzuführen, sich mit einem Pseudonym in kriminalitätsaffinen Gruppen einzuschleusen oder Umfragen unter Betroffenen umzusetzen? Dies ist durch den digitalen Raum möglich geworden, auch wenn es sicherlich noch viel Zeit brauchen wird, um hier alle Möglichkeiten herauszuarbeiten.

Die Cyberkriminologie soll dabei helfen, diese Fragen strukturiert und mit einem angepassten Blickwinkel zu beantworten. Die Zukunft der digitalen Gesellschaft wird zeigen, dass auch hier empirisch begründbare kriminalpolitische Antworten auf Normenbruch und -kontrolle gefunden werden müssen.

Noch steht die Cyberkriminologie aber ganz am Anfang.

Literatur

Abendzeitung München (2021) Hetze und Hass zu Vergewaltigungsfall: Polizei muss Facebook-Kommentare sperren. In: Abendzeitung, 02.08.2021. https://www.abendzeitung-muenchen.de/muenchen/hetze-und-hass-zu-vergewaltigungsfall-polizei-muss-facebook-kommentare-sperren-art-746733. Zugegriffen am 11.09.2021

adrienne_koleszar (2021) Adrienne Koleszár. Instagram Account. https://www.instagram.com/adrienne_koleszar/. Zugegriffen am 11.09.2021

Annes Vlog (2021) Annes VLOG || PolizeiBB. Instagram Account. https://www.instagram.com/annes.vlog/. Zugegriffen am 11.09.2021

Avanan (2021) The history & future of phishing. https://www.avanan.com/resources/infographics/the-history-and-future-of-phishing. Zugegriffen am 11.09.2021

Baker M (2019) NASA Astronaut Anne McClain accused by spouse of crime in space. The New York Times, 23 August. https://www.nytimes.com/2019/08/23/us/astronaut-space-investigation.html. Zugegriffen am 03.08.2021

Balschmiter P, Roll H, Bornewasser M, Behnke L (2018) Erste Untersuchung zum Dunkelfeld der Kriminalität in Mecklenburg Vorpommern. Abschlussbericht 5:1–187

Bankhurst A (2020) Three billion people worldwide now play video games, new report shows – IGN. In: IGN, 15.08.2020. https://www.ign.com/articles/three-billion-people-worldwide-now-play-video-games-new-report-shows. Zugegriffen am 04.09.2021

Banner T (2020) Nasa beauftragt Nokia mit 4G-Netz für den Mond. In: Frankfurter Rundschau, 20.10.2020. https://www.fr.de/wissen/nasa-mond-nokia-4g-lte-mobilfunk-handynetz-artemis-raumfahrt-90075200.html. Zugegriffen am 04.08.2021

Bässmann J (2015) Täter im Bereich Cybercrime. Eine Literaturanalyse Teil. Bundeskriminalamt (Deutschland). Wiesbaden. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/Forschungsergebnisse/2015TaeterImBereichCybercrime.html?nn=27638. Zugegriffen am 11.09.2021

Bayerl PS, Rüdiger T-G (2017) Die polizeiliche Nutzung sozialer Medien in Deutschland: Die Polizei im digitalen Neuland. In: Stierle J, Wehe D, Siller H (Hrsg) Handbuch Polizeimanagement. Polizeipolitik – Polizeiwissenschaft – Polizeipraxis. Springer Gabler, Wiesbaden, S 919–943

Beisch N, Schäfer C (2020) Ergebnisse der ARD/ZDF-Onlinestudie 2020. Internetnutzung mit großer Dynamik: Medien, Kommunikation, Social Media. Media Perspektiven, Frankfurt am Main, S 462–481

Bitkom (2020) Mehr als jeder zweite Onliner Opfer von Cyberkriminalität. https://www.bitkom.org/Presse/Presseinformation/Mehr-als-jeder-zweite-Onliner-Opfer-von-Cyberkriminalitaet. Zugegriffen am 06.09.2021

Bitkom (2021) Internetnutzer fordern mehr Polizeipräsenz im digitalen Raum. https://bitkom.org/Presse/Presseinformation/Internetnutzer-fordern-mehr-Polizeipraesenz-im-digitalen-Raum. Zugegriffen am 09.09.2021

Bittner J (2019) Zur Sache, Deutschland! Was die zerstrittene Republik wieder eint! -eBook Edition Körber

BMI (2020a) Polizeiliche Kriminalstatistik. T01 – Häufigkeitszahl. https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2020/PKSTabellen/BundBelastungszahlen/bundBelastungszahlen.html?nn=145506. Zugegriffen am 10.09.2021

BMI (2020b) Polizeiliche Kriminalstatistik. T01 – Vollendete Fälle. https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2020/PKSTabellen/BundFalltabellen/bundfalltabellen.html?nn=145506. Zugegriffen am 10.09.2021

BMI (2020c) Polizeiliche Kriminalstatistik. T05 – Tatmittel Internet. https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2020/PKSTabellen/BundBelastungszahlen/bundBelastungszahlen.html?nn=145506. Zugegriffen am 10.09.2021

BMI.AT (2020) Nehammer: Verdoppelung der Cyber-Cops. Bundesministerium – Inneres (Österreich). https://bmi.gv.at/news.aspx?id=797375547A343246322B303D. Zuletzt aktualisiert am 10.09.2021, zugegriffen am 10.09.2021

Böber A (2020) Vernetzt bis in den letzten Winkel: So arbeitet die Polizei auf Social Media | MDR.DE. https://www.mdr.de/medien360g/medienwissen/polizei-auf-social-media-104.html. Zuletzt aktualisiert am 09.09.2021, zugegriffen am 09.09.2021

Borchard I, Jurczok F, Javakhishvili E, Repohl I (2018) DIVSI U25-Studie. Euphorie war gestern. https://www.divsi.de/publikationen/studien/divsi-u25-studie-euphorie-war-gestern/index.html. Zugegriffen am 07.09.2021

Bruhn M, Hadwich K (2015) Einsatz von Social Media für das Dienstleistungsmanagement. Springer Gabler (essentials), Wiesbaden

BSI, ProPK (2020) Digitalbarometer. Bürgerbefragung zur Cyber-Sicherheit. Zugegriffen am 06.09.2021

Bundeskriminalamt (2020) Bundeslagebild Cybercrime 2020. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2020.html;jsessionid=5EAE5A04F7EFFCBDBC83C1C380E6D7E0.live2291?nn=28110. Zugegriffen am 07.09.2021

Bundeskriminalamt (2021a) Onlinewachen der Landespolizeien. https://www.bka.de/DE/KontaktAufnehmen/Onlinewachen/onlinewachen_node.html. Zuletzt aktualisiert am 09.09.2021, zugegriffen am 09.09.2021

Bundeskriminalamt (2021b) Politisch motivierte Kriminalität im Jahr 2020 – Bundesweite Fallzahlen. Zugegriffen am 07.09.2021

Bundesministerium der Justiz und für Verbraucherschutz (BMJV) (o. J.) Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität, S 1–57. Zugegriffen am 10.09.2021

Clages H, Gatzke W (Hrsg) (2020) Cybercrime. VDP Verlag, Hilden

Cohen L, Felson M (1979) Social change and crime rate trends: a routine activity approach 44: 588–608. https://www.jstor.org/stable/2094589?seq=1#page_scan_tab_contents. Zugegriffen am 21.01.2018

Diekmann A, Przepiorka W, Rauhut H (2011) Die Präventivwirkung des Nichtwissens im Experiment. Z Soziol 40(1):74–84. Zugegriffen am 06.09.2021

Dreißigacker A, von Skarczinski B, Bergmann MC, Wollinger GR (2020) Cyberangriffe gegen private Internetnutzer*innen. In: Rüdiger T-G, Bayerl PS (Hrsg) Cyberkriminologie. Springer Fachmedien Wiesbaden, Wiesbaden, S 319–344

Durkheim É (2016) Kriminalität als normales Phänomen. In: Klimke D, Legnaro A (Hrsg) Kriminologische Grundlagentexte. Springer VS, Wiesbaden, S 25–31

Eisenberg U, Kölbel R (2017) Kriminologie, 7., völlig. neu bearb. Aufl. Mohr Siebeck, Tübingen

Feierabend S, Rathgeb T, Kheredmand H, Glöckler S (2021) JIM-Studie 2020. Jugend, Informatio Medien. https://www.mpfs.de/studien/jim-studie/2020/. Zugegriffen am 10.09.2021

game e. V. (2021) Rund 6 von 10 Deutschen spielen Games – game. https://www.game.de/marktdaten/rund-6-von-10-deutschen-spielen-games/. Zuletzt aktualisiert am 04.09.2021, zugegriffen am 04.09.2021

Garner R (2019) Space station's data rate increase supports future exploration. In: NASA, 19.08.2019. https://www.nasa.gov/feature/goddard/2019/data-rate-increase-on-the-international-space-station-supports-future-exploration. Zugegriffen am 04.08.2021

Heitkamp S (2020) Roland Wöller: Es wird keine rechtsfreien Räume geben. In: Sächsische Zeitung, 03.01.2020. https://www.saechsische.de/plus/innenminister-will-keine-rechtsfreien-raeume-dulden-5157312.html. Zugegriffen am 09.09.2021

Huber E (2019) Cybercrime. Eine Einführung. Springer VS (Lehrbuch), Wiesbaden/Heidelberg. http://swbplus.bsz-bw.de/bsz1666883158cov.htm. Zugegriffen am 10.09.2021

Jahankhani H (Hrsg) (2018) Cyber criminology. Springer International Publishing (Advanced Sciences and Technologies for Security Applications), Cham

Jaishankar K (2007) Establishing a theory of cyber crimes. Int J Cyber Criminol 1(2):7–9

Kemme S, Querbach M (2020) Strafbedürfnis und Kriminalitätsfurcht im Cyberspace. In: Rüdiger T-G, Bayerl PS (Hrsg) Cyberkriminologie. Springer Fachmedien Wiesbaden, Wiesbaden, S 507–545

Kigerl A (2012) Routine activity theory and the determinants of high cybercrime countries. Soc Sci Comput Rev 30(4):470–486. https://doi.org/10.1177/0894439311422689

Kimbrough S (2021) Tweet: Hallo Nürnberg, Deutschland! https://twitter.com/astro_kimbrough/status/1407822527485857797. Zugegriffen am 10.09.2021

Kohout R, Ikrath P, Modelhart A (2018) Sexuelle Belästigung und Gewalt im Internet in den Lebenswelten der 11- bis 18-Jährigen. https://www.sos-kinderdorf.at/getmedia/62adc879-ed91-4b3f-aa95-70b4371b6b86/Bericht_Sexuelle-Belastigung-und-Gewalt-im-Internet-in-den-Lebenswelten-der-11-bis-18-Jahrigen.pdf. Zugegriffen am 07.09.2021

Krah E (2021) Die E-Mail-Flut wächst. In: springerprofessional.de, 18.02.2021. https://www.springerprofessional.de/kommunikation/kommunikationstechnologie/die-e-mail-flut-waechst/18866136. Zugegriffen am 08.09.2021

Kreissl R (2019) Abweichendes Verhalten als gesellschaftstheoretische Kategorie – von Durkheim zu Garfinkel. jrp 27(4):244. https://doi.org/10.33196/jrp201904024401

Krischok H (2018) Das Internet in der polizeilichen Gefahrenabwehr. In: Rüdiger T-G, Bayerl PS (Hrsg) Digitale Polizeiarbeit. Herausforderungen und Chancen. Springer VS (Research), Wiesbaden, S 237–257

Külling C, Waller G, Suter L, Bernath J, Willemse I, Süss D (2021) JAMESfocus. Hassrede im Internet. https://www.zhaw.ch/de/psychologie/forschung/medienpsychologie/mediennutzung/james/jamesfocus/. Zugegriffen am 07.09.2021

Kunz K-L, Singelnstein T (2021) Kriminologie. Eine Grundlegung, 8. Aufl. Haupt Verlag, Bern. (UTB Recht, Soziologie, 1758)

Landesanstalt für Medien NRW (2021) Ergebnisbericht. forsa-Befragung zu: Hate Speech 2021. https://www.medienanstalt-nrw.de/themen/hass/forsa-befragung-zur-wahrnehmung-von-hassrede.html#c91404. Zugegriffen am 10.09.2021

LKA NRW (2013) Cybercrime in Nordrhein-Westfalen. Lagebild 2013. https://polizei.nrw/artikel/lagebild-cybercrime. Zugegriffen am 10.09.2021

Maras M-H (2017) Cybercriminology. Oxford University Press, New York

Maschke S, Stecher L (2017) Sexualisierte Gewalt in der Erfahrung Jugendlicher. Öffentlicher Kurzbericht, S 1–27

Mayer S (2021) Strukturelle Strafvereitelung im Amt. In: Wirtschaft, 28.07.2021. https://www.zdf.de/nachrichten/wirtschaft/wirtschaft-it-digitalisierung-polizei-100.html. Zugegriffen am 10.09.2021

Meier B-D (2016) Risikofaktoren der Onlinekriminalität. In: Neubacher F, Bögelein N (Hrsg) Krise – Kriminalität – Kriminologie, Bd 116. Forum Verlag Godesberg GmbH (Neue Kriminologische Schriftenreihe der Neuen Kriminologischen Gesellschaft e.V.), Mönchengladbach, S 231–245

Neubacher F (2017) Kriminologie, 3. Aufl. Nomos (Nomos-Lehrbuch), Baden-Baden

Neumann D (2019) ISS-Raumstation hat schnelleres Internet als die meisten von uns. In: futurezone.de, 27.08.2019. https://www.futurezone.de/digital-life/article226903257/Du-willst-schnelleres-Internet-Auf-der-ISS-Raumstation-surfst-du-mit-unfassbarer-Geschwindigkeit.html. Zugegriffen am 04.08.2021

Norton (2021) 2021 Norton cyber safety insights report global results. https://de.norton.com/nortonlifelock-cyber-safety-report. Zugegriffen am 06.09.2021

Oswald B (2020) Polizei muss immer häufiger gegen Hass im Netz ermitteln. In: BR24, 09.11.2020. https://www.br.de/nachrichten/netzwelt/polizei-muss-immer-haeufiger-gegen-hass-im-netz-ermitteln,RhFBrZx?UTM_Name=Web-Share&UTM_Source=Twitter&UTM_Medium=Link. Zugegriffen am 10.09.2021

Plan International (2020) Free to be Online? Girl's and young women's experiences of online harassment. https://www.plan.de/presse/pressemitteilungen/detail/welt-maedchenbericht-2020-digitale-gewalt-vertreibt-maedchen-und-junge-frauen-aus-den-sozialen-medien.html. Zugegriffen am 10.09.2021

Politie (2021) The Netherlands Police. https://www.politie.nl/en/common/home.html. Zuletzt aktualisiert am 09.09.2021, zugegriffen am 09.09.2021

Polizei Berlin (2021) @polizeiberlin. Twitter Account. https://www.instagram.com/adrienne_koleszar/. Zugegriffen am 10.09.2021

Polizei Berlin Helena (2021) polizeiberlin.helena. Instgram Account. https://www.instagram.com/polizeiberlin.helena/. Zugegriffen am 10.09.2021

Polizei München (2021a) Unser Ziel ist es, Euch auf Social Media mittels Warnhinweisen, Prävention und aktuellen Themen stets schnell zu informieren. (02.08.2021). https://de-de.facebook.com/polizeimuenchen/posts/2565717496907316?__tn__=-R. Zugegriffen am 10.09.2021

Polizei München (2021b) Zeugenaufruf nach Vergewaltigung (30. Juli 2021). https://de-de.facebook.com/polizeimuenchen/photos/a.552744488204637/2563152550497144/?type=3&theater. Zugegriffen am 10.09.2021

Polizei Niedersachsen (2021) Digitales Community Policing. https://www.polizei-nds.de/wir_ueber_uns/polni_socialmedia/digital.community.policing/digital-community-policing-112171.html. Zuletzt aktualisiert am 09.09.2021, zugegriffen am 09.09.2021

Polizei Saarland (2021) @PolizeiSaarland. Twitter Account. https://twitter.com/PolizeiSaarland. Zugegriffen am 10.09.2021
Polizei Thüringen (2021) @polizei_thuer. https://twitter.com/Polizei_Thuer. Zugegriffen am 10.09.2021
Popitz H (2003) Über die Präventivwirkung des Nichtwissens (1968). BWV BerlinerWiss.- Verl., Berlin, (Juristische Zeitgeschichte Kleine Reihe Klassische Texte, 8). Zugegriffen am 02.01.2018
Rempfer K (2020) Army astronaut accused of committing crime in space is cleared; ex-wife charged with making false statements. In: Army Times, 07.04.2020. https://www.armytimes.com/news/your-army/2020/04/07/army-astronaut-accused-of-committing-crime-in-space-is-cleared-ex-wife-charged-with-making-false-statements/. Zugegriffen am 03.08.2021
Rettenberger M, Leuschner F (2020) Cyberkriminalität im Kontext von Partnerschaft, Sexualität und Peerbeziehungen: Zur Cyberkriminologie des digitalen sozialen Nahraums. Forens Psychiatr Psychol Kriminol 14(3):242–250. https://doi.org/10.1007/s11757-020-00612-1
Reuter M (2020) Polizei und soziale Medien: Das dürfen Berliner Polizisten privat im Netz. https://netzpolitik.org/2020/polizei-und-soziale-medien-das-duerfen-berliner-polizisten-privat-im-netz/. Zuletzt aktualisiert am 10.09.2021, zugegriffen am 10.09.2021
Roggenkamp JD, König K (2021) Eingriffsrecht für Polizeibeamte in Niedersachsen, 3. akt. Aufl. Stuttgart: Deutscher Gemeindeverlag (Studienreihe öffentliche Verwaltung). http://www.kohlhammer.de/wms/instances/KOB/appDE/nav_product.php?product=978-3-555-02180-5. Zugegriffen am 10.09.2021
RTL (2021) Social Media-Knigge für Polizisten: „Insta-Cops! Denkt bitte darüber nach, was ihr postet!“. In: RTL Online, 02.06.2021. https://www.rtl.de/cms/social-media-knigge-fuer-polizisten-insta-cops-denkt-bitte-darueber-nach-was-ihr-postet-4770218.html. Zugegriffen am 10.09.2021
Rüdiger T-G (2018) Das Broken Web. Herausforderung für die Polizeipräsenz im digitalen Raum. In: Rüdiger T-G, Bayerl PS (Hrsg) Digitale Polizeiarbeit. Herausforderungen und Chancen. Springer VS (Research), Wiesbaden, S 259–299
Rüdiger T-G (2019) Polizei im digitalen Raum. In: Zeitschrift der Bundeszentrale für Politische Bildung (APUZ) 69. Jahrgang (23-23/2019), S 18–23
Rüdiger T-G (2020a) Die onlinebasierte Anbahnung des sexuellen Missbrauchs eines Kindes. Dissertation, Universität Potsdam
Rüdiger T-G (2020b) Polizei und Gaming – The next Level? Games und die Polizei – Das missverstandene Medium. In: Polizei Verkehr und Technik (PVT) (06/2020), S 26–29
Rüdiger T-G (2021) Digitale Kriminalitätstransparenz – Von der Durchbrechung der Präventivwirkung des Nichtwissens. Kriminalistik 2021(2):72–78
Rüdiger T-G, Bayerl PS (2020a) Cyberkriminologie. In: Rüdiger T-G, Bayerl PS (Hrsg) Cyberkriminologie. Springer Fachmedien Wiesbaden, Wiesbaden, S 3–12
Rüdiger T-G, Bayerl PS (Hrsg) (2020b) Cyberkriminologie. Springer Fachmedien Wiesbaden, Wiesbaden
Schneider H (2008) Grundzüge der gegenwärtigen Strafrechtspfelge und die Aufgabe der Kriminologie. In: Bock M, Göppinger H (Hrsg) Kriminologie, 6., vollst. neu bearb. u. erw. Aufl. Beck, München, S 541–567
Schwind H-D (2016) Kriminologie und Kriminalpolitik. Eine praxisorientierte Einführung mit Beispielen. Unter Mitarbeit von Jan-Volker Schwind. 23., neubearb. u. erw. Aufl. Kriminalistik, Heidelberg (Grundlagen die Schriftenreihe der „Kriminalistik“, 28)
Simpson R, McCutcheon M, Lal D (2020) Reducing speeding via inanimate police presence. Criminol Public Policy 19(3):997–1018. https://doi.org/10.1111/1745-9133.12513
Statista (2019) Statistiken zur Internetnutzung weltweit. In: Statista, 05.06.2019. https://de.statista.com/themen/42/internet/. Zugegriffen am 04.09.2021
Statista (2021a) Bevölkerung – Zahl der Einwohner in Deutschland nach relevanten Altersgruppen am 31. Dezember 2020. https://de.statista.com/statistik/daten/studie/1365/umfrage/bevoelkerung-deutschlands-nach-altersgruppen/. Zugegriffen am 10.09.2021

Statista (2021b) Social Media – Anzahl der aktiven Nutzer weltweit bis 2021 | Statista. https://de.statista.com/statistik/daten/studie/739881/umfrage/monatlich-aktive-social-media-nutzer-weltweit/. Zuletzt aktualisiert am 04.09.2021, zugegriffen am 04.09.2021

Statistisches Bundesamt (2021a) Bevölkerungsstand: Offizielle Einwohnerzahlen Deutschlands 2021. https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Bevoelkerung/Bevoelkerungsstand/_inhalt.html. Zuletzt aktualisiert am 27.08.2021, zugegriffen am 02.09.2021

Statistisches Bundesamt (2021b) Öffentlicher Dienst 2020: Personalzuwachs bei Kitas und Polizei hält an. https://www.destatis.de/DE/Presse/Pressemitteilungen/2021/06/PD21_289_741.html. Zuletzt aktualisiert am 22.06.2021, zugegriffen am 06.09.2021

Steel CMS, Newman E, O'Rourke S, Quayle E (2021) Lawless space theory for online child sexual exploitation material offending. George Mason University, University of Edingburgh, Fairfax

Vandeputte B (2018) In Nederland patrouilleert de wijkpolitie ook op het internet. In: VRT NWS: nieuws, 14.02.2018. https://www.vrt.be/vrtnws/nl/2018/02/14/digitale-wijkagent/. Zugegriffen am 09.09.2021

Wegener R (2013) Kriminologie. In: Madea B (Hrsg) Praxis Rechtsmedizin. Befunderhebung, Rekonstruktion, Begutachtung. Springer, Berlin/Heidelberg/s.l., S 88–94

Wehaus R (2019) Baden-Württemberg will keine „Instacops" – Grenzen für Selbstdarsteller bei der Polizei. In: Stuttgarter Nachrichten, 09.09.2019. https://www.stuttgarter-nachrichten.de/inhalt.land-macht-vorgaben-grenzen-fuer-selbstdarsteller-bei-der-polizei.689cde4f-f0ec-4d4e-81a3-993bbca040f4.html. Zugegriffen am 10.09.2021

Weller K, Bathke G-W, Kruber A, Voß H-J (2021) PARTNER 5 Jugendsexualität 2021. Sexuelle Bildung, sexuelle Grenzverletzungen und sexualisierte Gewalt. https://www.ifas-home.de/partner-5-jugenderhebung/. Zugegriffen am 10.09.2021

Welt (2021) „Querdenken"-Proteste: Berliner Polizei wird im Internet mit Hass überschüttet. In: WELT, 06.08.2021. https://www.welt.de/politik/deutschland/article232986265/Querdenken-Proteste-Berliner-Polizei-wird-im-Internet-mit-Hass-ueberschuettet.html. Zugegriffen am 11.09.2021

Wilke T (2019) „Klare Linie gegen Hasskommentare ziehen" | MDR.DE. https://www.mdr.de/nachrichten/sachsen/interview-stellv-landesvorsitzender-bdk-sachsen-schmorrte-hasskommentare-netzwerke-100.html. Zuletzt aktualisiert am 10.09.2021, zugegriffen am 10.09.2021

Wurtzbacher J (2008) Urbane Sicherheit und Partizipation. Stellenwert und Funktion bürgerschaftlicher Beteiligung an kommunaler Kriminalprävention. VS Verlag für Sozialwissenschaften/GWV Fachverlage GmbH Wiesbaden (Stadt, Raum und Gesellschaft), Wiesbaden. http://gbv.eblib.com/patron/FullRecord.aspx?p=752334. Zugegriffen am 10.09.2021

Dr. iur. Thomas-Gabriel Rüdiger Akademischer Oberrat, schloss 2003 an der Fachhochschule der Polizei des Landes Brandenburg sein Studium zum Diplom-Verwaltungswirt (FH) ab. An der Universität Hamburg studierte er nebenberuflich Kriminologie in einem Masterstudiengang und schloss diesen 2010 mit einer Arbeit zu Kriminalität im Zusammenhang mit Onlinegames ab. Seit 2012 war er als Kriminologe und Dozent am Institut für Polizeiwissenschaft der Hochschule der Polizei des Landes Brandenburg tätig. Im Jahr 2020 verteidigte er seine Dissertation zum Thema „Die onlinebasierte Anbahnung des sexuellen Missbrauchs eines Kindes – Eine kriminologische und juristische Auseinandersetzung mit dem Phänomen Cybergrooming" und promovierte zum Dr. iur. an der juristischen Fakultät der Universität Potsdam. Seit 2021 ist er Leiter des Instituts für Cyberkriminologie an der Hochschule der Polizei des Landes Brandenburg. Seine Forschungsschwerpunkte liegen neben der Cyberkriminologie, auf der digitalen Polizeiarbeit, digitalen Kinderschutz und Kriminalitätsformen im Zusammenhang mit Onlinegames. Neben der Veröffentlichung einer Vielzahl an Fachpublikationen ist er Mitherausgeber des Sammelbandes „Cyberkriminologie" und „Digitale Polizeiarbeit" und vertritt seine Themengebieten als ein viel gefragter Referent und Interviewpartner für unterschiedliche Medienformate sowie als Experte bei politischen Anhörungen.