ArGe ÖFG - Digitale Transformation: Safety, Security & Privacy

Edgar Weippl, Peter Parycek

Mai 2019

1 Zielsetzung

Die rasant fortschreitende Digitalisierung ergreift immer mehr wesentliche technische und administrative Infrastrukturen und dringt damit einerseits tief in wirtschaftliche und industrielle Prozesse und Abläufe, andererseits aber auch in den persönlichen Lebensbereich der Menschen ein. Die Digitalisierung wird eine Transformation der Gesellschaft nach sich ziehen und die individuelle Autonomie der Menschen vor neue Herausforderungen stellen. Damit sind neben den informationstechnischen Kernwissenschaften auch die Wirtschafts-, Sozial- und Rechtswissenschaften mit völlig neuen Themenfeldern konfrontiert.

Die Steuerung von Kommunikations-, Verkehrs- und Energieversorgungsnetzen mittels Software ist längst Realität geworden, ebenso die Abwicklung von Finanz- und Börsengeschäften. Die Automatisierung industrieller Fertigungsprozesse – Stichwort „Industrie 4.0“ – bedingt den massiven Einsatz von Software, die nicht nur den Fertigungsprozess selbst steuert, sondern auch die gesamte Liefer- und Wertschöpfungskette umfasst.

Unmittelbar betroffen sind alle Menschen beispielsweise von der umfassenden Digitalisierung des Gesundheits- und Krankenpflegebereichs. Hier geht es nicht nur um sensible persönliche Daten, sondern in zunehmendem Maße auch um die computergestützte Diagnoseerstellung und um die Steuerung von chirurgischen Eingriffen. Auch die Abwicklung privater Geschäfte im Internet („Online- Shopping“) erfordert die Speicherung und Übermittlung sensibler Daten. Ebenso werden viele behördenrelevante Vorgänge vermehrt digitalisiert – man denke nur an die Bürgerkarte und elektronisch unterstützte Wahlgänge. Weniger dramatisch, aber ähnlich „total“ wird in naher Zukunft die Anbindung von Haushaltsgeräten und Unterhaltungselektronik an das Internet sein – Stichwort „Internet of Things (IoT)“. Etwas weiter in der Zukunft, aber durchaus mittelfristig zu erwarten ist das autonome Fahren von Straßenfahrzeugen.

Die Konsequenz dieser Entwicklungen ist ein enormes Ansteigen des Datenverkehrs über feste Netze und über Funknetze. Damit sind aber auch die Gefahren des Auftretens von Fehlern, der Verwundbarkeit softwaregesteuerter Infrastruktur und der Verletzung

der Privatsphäre von Menschen gegeben. Die zugehörigen Schlagworte sind Safety, Security und Privacy.

Die zunehmende Vernetzung und die damit einhergehenden Risiken haben wesentliche Auswirkungen auf unsere Gesellschaft. Beispielsweise können kleine, geographisch verteilte Gruppen Krimineller durch zunehmende Spezialisierung effizienter arbeiten und mehr Schaden anrichten. Dieser Schaden beschränkt sich nicht mehr auf "digitale Systeme", sondern kann im Zeitalter von Cyber-Physical-Systems ganz unmittelbar zur Gefährdung von Gesundheit und Menschenleben führen. Es gilt *there is no safety without security.*

Ermittlungsbehörden fordern daher immer mehr Überwachungsmöglichkeiten; die gesammelten Daten gefährden allerdings die persönliche Freiheit, weil die vorhandenen Daten dann auch leicht für andere Bereiche weiterverwendet werden können. Privatsphäre und die geschützte Kommunikation sind Voraussetzungen für eine freie Presse, die wiederum ein wichtiger Bestandteil einer Demokratie ist. Security und im Besonderen Digital Forensics stehen oft scheinbar im Widerspruch zu Privacy und daher ist es wichtig, aufzuzeigen, wie Privacy geschützt werden kann ohne forensische Ermittlungen unmöglich zu machen.

Die ArGe „Cyber-Security" der ÖFG soll sich, wissenschaftlich möglichst breit angelegt, mit den angerissenen Themen beschäftigen und zu einer umfassenden Betrachtungsweise der mit der Digitalisierung verbundenen Probleme und Risiken gelangen und so zu ihrer Lösung beitragen.

Wesentliche Meilensteine auf diesem Weg sind

- Organisation eines Workshops zur Definition von „Public-Interest Technology" für Security in Österreich.
- Erstellung einer Übersichtskarte aller wesentlichen Security-Initiativen in Österreich. Im Gegensatz zur Kiras-Landkarte sollen Vereinigungen, Vereine und Hubs im Zentrum stehen. Weiters soll das Netzwerk an Kooperation und nicht die geographische Nähe deutlich gemacht werden.
- die Initiierung von kurzzeitigen bezahlten interdisziplinären Praktika. Falls zulässig, z.b. eine Co-Finanzierung der ARGE i.d. Höhe von z.b. 50%; (50% ARGE, 25% Entsender, 25% Empfänger)

2 Mehrwert

1. Die Arbeitsgemeinschaft wird *interdisziplinär* arbeiten und existierende — üblicherweise sehr fokussierte Forschungsprojekte — miteinander verbinden. Wesentlich ist hier die Betrachtung der Aspekte der Resilienz unserer Gesellschaft und wie in verschiedenen Gruppen, d.h. von kleinen lokalen Gruppen über Nationalstaaten zu Staatengemeinschaften, Entscheidungen getroffen werden und das Zusammenleben organisiert wird.

2. Digitalisierung ist notwendigerweise mit Globalisierung verbunden. Unternehmen und Menschen können weltweit kommunizieren und kooperieren; diese Chancen werden allerdings nicht nur für Positives genutzt: Kriminalität wird auch zunehmend spezialisiert und gerade in einer digitalisierten Welt sind schnelle, weltweit kooperierende AdHoc-Netzwerke Krimineller für nationalstaatlich agierende Ermittlungsbehörden eine Herausforderung. In der Arbeitgemeinschaft werden wir *Handlungsempfehlungen und mögliche Alternativen für regionale und nationalstaatliche Einflussmöglichkeiten* erstellen.

3 Forschungsbereiche

Exemplarisch greifen wir zwei Forschungsbereiche (Industrie 4.0 und Blockchain) heraus, die in der nationalen Forschung[1] sehr bedeutsam sind. Der Mehrwert, der durch die Arbeitsgemeinschaft entsteht, ist, dass zusätzlich zu der fachspezifischen Forschung die interdisziplinäre Vernetzung ermöglicht wird.

Je nach Interessen der TeilnehmerInnen, können diese Bereiche ergänzt, verändert oder auch ausgetauscht werden.

3.1 Industrie 4.0

Es gab wesentliche Veränderungen der Bedrohungslandschaft der Industriellen-Kontroll-Systeme (IKS) durch strategische Initiativen wie Industry 4.0 oder Smart Manufacturing. Daher ist ein systematischer Ansatz zur Bedrohungsmodellierung erforderlich, der auch neue Aspekte berücksichtigt, die sich aus der IT/OT-Konvergenz ergeben. Diese Änderung hat auch wesentliche Auswirkungen auf die Quantifizierung der Risiken, wie im folgenden Abschnitt erläutert.

3.1.1 Quantifizierung von Cyberrisiken industrieller Steuerungssysteme

Bei der Anwendung eines qualitativen Risikobewertungsansatzes werden die Risiken typischerweise in Risikoklassen (z.B. niedrig, mittel oder hoch) eingeteilt. Obwohl dieser Ansatz bequemer anzuwenden ist und weniger Aufwand durch Berechnungen/Schätzungen erfordert, sind selbst die groben Schätzungen typischerweise vage [BJB08]. Analysten benötigen jedoch numerische Schätzungen für Investitionsentscheidungen oder im Underwriting-Prozess, was die Quantifizierung von Risiken unerlässlich macht.

Je nach Perspektive (d.h. (Rück-)Versicherer oder Versicherter) ergeben sich unterschiedliche Probleme. Während Anbietern, Integratoren oder Betreibern das Gesamtbild der IKS-Bedrohungslandschaft sowie zuverlässige Datenquellen für Risikobewertungen fehlen können, müssen (Rück-)Versicherer das *nicht explizit versicherte Cyberrisiko* reduzieren, d.h. das Cyberrisiko, das *möglichst* implizit in Versicherungspolizzen aufgenommen wurde und wird [Pru17].

[1] Zu beiden Themen gibt es die COMET-Zentren CDP und ABC und zahlreiche Forschungsprojekte

In [CBB+16] identifizierten die Autoren, dass Risikobewertungsmethoden für IKS durch eine fragmentierte, zerfallene Betrachtung der Einzelschritte im Risikomanagementprozess gekennzeichnet sein können. Cherdantseva et al. [CBB+16] weisen insbesondere darauf hin, dass die Schaffung des Kontexts für den Risikomanagementprozess gemäß ISO 31000:2009 [ISO09] oft vernachlässigt wird, weil Risikoanalysten möglicherweise nicht in der Lage sind, die Komplexität von IKS auf überschaubare Niveaus zu reduzieren, ohne grundlegende Faktoren wie die Interdependenzen von Systemen auszulassen. Darüber hinaus stellen die Autoren von [CBB+16] fest, dass der Mangel an zuverlässigen Datenquellen, die den Schritt der Risikobewertung unterstützen würden (z.B. historische Daten zur Ableitung von Angriffswahrscheinlichkeiten), eine weitere Herausforderung darstellt.

Die Richtlinie VDI/VDE 2182 [VDI11] versucht, diesem Trend entgegenzuwirken. Wie in dieser Richtlinie festgelegt, sollten die Aktivitäten von Anbietern, Integratoren und Betreibern beim Schutz von IKS ganzheitlich betrachtet werden, da Maßnahmen aller drei Parteien die Sicherheit während des gesamten Lebenszyklus der Systeme beeinträchtigen können. Insbesondere das in der VDI/VDE 2182 [VDI11]Richtlinie vorgeschlagene Vorgehensmodell legt nahe, dass Anbieter, Integratoren und Betreiber zusammenarbeiten, indem sie Anforderungen und Dokumentationen zur Sicherheit von IKS austauschen. Da Wirtschaftsspionage im Rahmen der PSE jedoch ein großes Thema ist, ist die Umsetzung dieses Ansatzes schwierig. Das Fehlen angemessener Sicherheitsmechanismen zum Schutz des PSE-Prozesses verschärft dieses Problem weiter [WK17, KW18].

3.2 Gesellschaft

Public-Interest-Technology [Sch18] bezieht sich auf die Erforschung und Anwendung von Technologieexpertise zur Förderung des öffentlichen Interesses, der Generierung von öffentlichem Nutzen und der Förderung des öffentlichen Gutes. Bruce Schneier versucht in den USA, Wissenschaftler und Experten für diese Initiative zu begeistern und sich aktiv in die gesellschaftspolitische Diskussion einzubringen.

Durch die Komplexität der Digitalisierung sind den meisten politischen Entscheidungsträgern die damit verbundenen Risiken vermutlich nicht vollständig bekannt. Risiken, die von Datenbanken globaler Konzerne, die mit personenbezogenen Daten gefüllt sind, und von vernetzter Steuerung kritischer Infrastruktur ausgehen, können nur dann verstanden werden, wenn man zumindest über Grundwissen in Mathematik & Informatik, Naturwissenschaften und Ingenieurwissenschaften verfügt.

Shoshana Zuboff spricht von Überwachungskapitalismus [Zub19], in dem Menschen nicht mehr frei entscheiden können, ob ein Unternehmen ihre Daten verarbeiten darf oder nicht. Schattenprofile bei Facebook sind dafür ein anschauliches Beispiel[2]. Personalisierte Werbung wird offensichtlich auch zur Beeinflussung von Wahlen verwendet, wobei gezielte Wahlwerbung nicht das Ziel hat, Wähler von einem Kandidaten zu überzeugen, sondern Unterstützer der Gegenkandidaten zu Nicht-Wählern zu machen[3].

[2] Die Zeit. `https://www.zeit.de/digital/internet/2018-05/mark-zuckerberg-facebook-eu-parlament-anhoerung/seite-2`

[3] "We have three major voter suppression operations under way" (Bloomberg

Ein möglicher Gegenpol zur zentralisierten Digitalisierung, wie wir sie heute beobachten, sind möglicherweise Blockchains. Die zugrundeliegende Idee ist, dass sich Akteure in einem verteilten System ohne zentrale Vertrauensrollen auf eine einheitliche Sicht des aktuellen Zustands des Gesamtsystems einigen. Dennoch beobachten wir auch hier immer wieder eine Tendenz zur Zentralisierung [JZS+17]. Da eine Blockchain üblicherweise für alle Teilnehmer einsehbar ist, gibt es natürlich besondere Herausforderungen im Bezug auf Privacy. Vor allem, weil durch verschiedene Optimierungsmöglichkeiten wie Merged Mining auch noch zusätzliche Information aus 'verworfenen Blöcken' [SSJ+19] erhalten bleibt.

4 Forschungsfragen

1. Welche Auswirkungen hat Digitalisierung auf lokale gesellschaftliche Strukturen?
2. Wie funktionieren global verteilte, anonyme oder pseudonyme Systeme, deren Akteure nicht identifiziert und möglicherweise gar nicht identifizierbar sind? Welche Gesellschaftsformen funktionieren unter diesen Bedingungen stabil?
3. Ist Public-Interest-Technology[4] eine für Österreich erfolgversprechende Möglichkeit, um Safety, Security und Privacy in allen Lebensbereichen zu verankern?

5 Projektphasen

2019 – 2020 In den ersten beiden Jahres etablieren wir die Interdisziplinarität der Arbeitsgemeinschaft und widmen uns in drei Workshops vor allem dem Aspekt der fachlichen Verbreiterung.

Im Rahmen des ersten Workshops werden wir wir zwei wesentliche Punkte bearbeiten:

- Welche Wissenschaftsdiziplinen, die noch nicht ausreichend vertreten sind, können zu der Arbeitsgemeinschaft beitragen?
- Welche inhaltlichen Anpassungen des vorläufigen Arbeitsprogramms wünschen die Mitglieder?

Basierend auf den Ergebnissen des Workshops werden wir eine Reihe eingeladener Vorträge organisieren, die öffentlich frei zugänglich sein sollen. Die Vorträge sollen möglichst alle Wissenschaftsdisziplinen abdecken und das Thema aus der jeweiligen Forschungssicht diskutieren.

In zwei Folgeworkshops am Endes des ersten Jahres und im zweiten Jahr bereiten wir die Ideen und Ansätze der Vortragsreihe auf, um konkrete erste Schritte für Public-Interest-Technology in Österreich zu planen. In diesen Workshops werden auch die Er-

https://www.bloomberg.com/news/articles/2016-10-27/inside-the-trump-bunker-with-12-days-to-go);

[4] `https://public-interest-tech.com/`

gebnisse des von uns organisierten Dagstuhl-Seminars 20141 zum Thema Cyber-Risiko und -Versicherung einfließen[5].

2021 – 2022 In den Jahren 3 und 4 werden wir verstärkt auf wissenschaftlichen Konferenzen und in Journals publizieren, weil wir bis dahin Beiträge zu den Forschungsfragen erwarten. Außerdem planen wir, jährlich einen Workshop auf der ARES-Konferenz zu organisieren, der das Thema Public-Interest-Technology unterstützt. Die ARES-Konferenz ist insofern für das Thema gut geeignet, weil es eine technischwissenschaftliche Konferenz in Europa ist und Public-Interest-Technology darauf abzielt, technisch-wissenschaftliche Fachleute für das Thema zu gewinnen.

Die Ergebnisse der Arbeitsgemeinschaft können wir im Rahmen eines Workshops, co-located mit der IEEE Euro S&P Konferenz vorstellen, die voraussichtlich in Wien stattfinden wird. Die Rückmeldungen, die wir dort erhalten werden, werden uns helfen, das Arbeitsprogramm für die letzten drei Jahre genauer zu definieren.

2023 – 2025 In den Jahren 2023 bis 2025 werden wir unsere Umsetzung von Public-Interest-Technology in Österreich weiter verbessern und evaluieren, ob dieser Ansatz langfristig zu Verbesserungen führt. Die Forschungsergebnisse aller involvierten Disziplinen wollen wir in einem gemeinsamen Buch zusammenfassen. Der Vorteil eines Buchs liegt darin, dass wir dadurch wirklich Beiträge unterschiedlicher Wissenschaftsdisziplinen vereinen können, was bei fachlich fokussierten wissenschaftlichen Konferenzen schwierig ist.

Im Rahmen dieses Buchprojekts werden wir auch zusätzlch zu den geplanten Workshops ein Dagstuhl-Seminar beantragen, um die notwendigen Abstimmungen in einer gemeinsamen Woche intensiver Arbeit durchführen zu können.

6 Dissemination

1. *Dagstuhl* Seminare. Das Seminar 20141 zum Thema Cyber-Risiko und -Versicherung ist bereits genehmigt und kann als Grundlage dienen. Im Rahmen der Arbeitsgemeinschaft werden wir zumindest ein zweites Dagstuhl-Seminar beantragen, weil Dagstuhl mehrere Stärken hat. Erstens ist es international angesehen [Var11] und zweitens kommen daher internationale TeilnehmerInnen auf eigene Kosten zu dem Seminar, sodass die Ergebnisse in großem Rahmen diskutiert werden können und darauf aufbauend auch weitere Publikationen (Papers, Buch, Policy Briefs) entstehen können.

2. *ARES Workshops.* SBA Research organisiert seit vielen Jahren die ARES-Konferenz und sie ist eine solide, stetig wachsende Security-Konferenz in Europa. Im Rahmen der Konferenz finden auch ausgewählte Workshops statt, die ohne großen Zusatzaufwand organisiert werden können. Ein Workshop auf der ARES-Konferenz und die damit verbundene kurze Vorstellung des Workshops auf der Hauptkonferenz

[5] `https://www.dagstuhl.de/en/program/calendar/semhp/?semnr=20141`

(ca. 200 TeilnehmerInnen) erhöht die Sichtbarkeit der Arbeitsergebnisse der Arbeitsgemeinschaft.

3. Wir planen, ausgezeichnete wissenschaftliche Arbeiten, die im Rahmen der Workshops und Dagstuhl-Seminare entstehen, in einem *Special Issue eines Journals (z.B. Computers & Security)* zu veröffentlichen, bzw. durch die Bewerbung des CfP für das Special-Issue auch noch zusätzliche ForscherInnen für das Thema begeistern zu können.

4. *ÖFG Policy Briefs*[6] sind eine bereits etablierte Art, Informationen über Forschungsergebnisse für die österreichische Politik aufzubereiten. Wir werden zu ausgewählten Themen — auch im Rahmen geplanter Public-Interest-Technology-Aktivitäten — Policy Briefs veröffentlichen.

5. Am Ende der 7-Jahres-Periode sollen die Ergebnisse der Arbeitsgemeinschaft in einem *Buch* zusammengefasst werden. Das Buch wird entweder bei einem Verlag wie z.B. Springer veröffentlicht werden oder als Open-Access-Buch zur Verfügung gestellt werden.

7 Potentielle Mitarbeiter und Mitarbeiterinnen

1. Peter Puschner, TU Wien (Safety in Real-Time Systems)
2. Tanja Zseby, TU Wien (Security in Kommunikationsnetzen)
3. Matteo Maffei, TU Wien (Security and Privacy)
4. Stefan Schmid, Uni Wien (Sicherheit in Computernetzen)
5. Nikolaus Forgo, Uni Wien (IT-Recht)
6. Stefan Thurner, MedUni Wien (komplexe Systeme)
7. Iris Eisenberger, BoKu Wien (Innovations- und Technologierecht)
8. Stephan Kirste, Uni Salzburg (Rechts- und Sozialphilosophie)
9. Rainer Böhme, Uni Innsbruck (Information security & privacy, cybercrime research)
10. Ruth Breu, Uni Innsbruck (Security Engineering)
11. Stefan Mangard, TU Graz (Dependable IoT, Systems Security)
12. Peter Schartner, Uni Klagenfurt (IT Sicherheit, Cryptology)
13. René Mayrhofer, JKU Linz (Security Research) dzt. karenziert

[6] `https://oegfe.at/oegfe-policy-briefs/`

14. Michael Sonntag, JKU Linz (Smart-Home Security, Web Security ...)
15. Martina Mara, JKU Linz (Roboterpsychologie)
16. Michael Mayrhofer, JKU Linz
17. Stefan Perner, WU Wien
18. Martin Stierle, AIT (Security and Communication Technologies)
19. Robert Kolmhofer, FH Oberösterreich, Campus Hagenberg (IT Sicherheit)
20. Walter Hötzendorfer, Research Institute (Privacy)
21. Vertreter des BMI, Cyber Security Center (CSC) im BVT
22. Vertreter des BMLV, Kommando Führungsunterstützung und Cyber Defence

8 Budgetärer Rahmen

Jahr	Beschreibung	Kosten
2019–2020	3 Workshops inkl. Anreise und Übernachtung	15.000 EUR
2019–2020	Vortragsreihe mit ca. 8 Vorträgen	8.000 EUR
2020–2021	Workshops bei ARES	13.000 EUR
2020–2021	Veranstaltungen zu Public-Interest-Technology	8.000 EUR
2020–2021	Workshop bei IEEE Euro S&P	4.000 EUR
2023–2025	Vortragsreihe mit ca. 9 Vorträgen zum Buch	12.000 EUR
2023–2025	4–5 Workshops inkl. Anreise und Übernachtung	25.000 EUR
2019–2025	Co-Finanzierung interdisziplinärer Forschungspraktika	30.000 EUR
2019–2025	**Summe**	**105.000 EUR**

Literatur

[BJB08] Rok Bojanc and Borka Jerman-Blažič. An economic modelling approach to information security risk management. *International Journal of Information Management*, 28(5):413 – 422, 2008.

[CBB+16] Yulia Cherdantseva, Pete Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, and Kristan Stoddart. A review of cyber security risk assessment methods for scada systems. *Computers & Security*, 56:1 – 27, 2016.

[ISO09] ISO 31000:2009. Risk management – Principles and guidelines. Standard, International Organization for Standardization, Geneva, CH, November 2009.

[JZS+17] Aljosha Judmayer, Alexei Zamyatin, Nicholas Stifter, Artemios Voyiatzis, and Edgar Weippl. Merged mining: Curse or cure? In *International Workshop on Cryptocurrencies and Blockchain Technology (CBT'17) at ESORICS*, September 2017.

[KW18] Peter Kieseberg and Edgar Weippl. Security challenges in cyber-physical production systems. In Dietmar Winkler, Stefan Biffl, and Johannes Bergsmann, editors, *Software Quality: Methods and Tools for Better Software and Systems*, pages 3–16, Cham, 2018. Springer International Publishing.

[Pru17] Prudential Regulation Authority. Cyber insurance underwriting risk. Technical Report Supervisory Statement 4/17, Prudential Regulation Authority, July 2017.

[Sch18] B. Schneier. *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*. W. W. Norton, 2018.

[SSJ+19] Nicholas Stifter, Philipp Schindler, Aljosha Judmayer, Alexei Zamyatin, Andreas Kern, and Edgar Weippl. Echoes of the past: Recovering blockchain metrics from merged mining. In *Proceedings of Financial Cryptography*, 2019.

[Var11] Moshe Y. Vardi. Where have all the workshops gone? *Communications of the ACM (CACM)*, 54(1):5, 2011. http://doi.acm.org/10.1145/1866739.1866740.

[VDI11] VDI/VDE 2182. It-security for industrial automation - general model, 2011.

[WK17] E. Weippl and P. Kieseberg. Security in cyber-physical production systems: A roadmap to improving it-security in the production system lifecycle. In *2017 AEIT International Annual Conference*, pages 1–6, Sept 2017.

[Zub19] Shoshana Zuboff. *The Age of Surveillance Capitalism*. Profile Books, 2019.