SSOAR

Open Access Repository
www.ssoar.info

Bedrohung, Verwundbarkeit, Werte und Schaden: Cyberattacken und Cybersicherheit als Thema der Technikfolgenabschätzung

Weber, Karsten; Christen, Markus; Herrmann, Dominik

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Weber, K., Christen, M., & Herrmann, D. (2020). Bedrohung, Verwundbarkeit, Werte und Schaden: Cyberattacken und Cybersicherheit als Thema der Technikfolgenabschätzung. *TATuP - Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis / Journal for Technology Assessment in Theory and Practice*, *29*(1), 11-15. https://doi.org/10.14512/tatup.29.1.11

Nutzungsbedingungen:
Dieser Text wird unter einer CC BY Lizenz (Namensnennung) zur Verfügung gestellt. Nähere Auskünfte zu den CC-Lizenzen finden Sie hier:
https://creativecommons.org/licenses/by/4.0/deed.de

Terms of use:
This document is made available under a CC BY Licence (Attribution). For more Information see:
https://creativecommons.org/licenses/by/4.0

gesis
Leibniz-Institut
für Sozialwissenschaften

Mitglied der
Leibniz-Gemeinschaft

Diese Version ist zitierbar unter / This version is citable under:
https://nbn-resolving.org/urn:nbn:de:0168-ssoar-68918-9

Bedrohung, Verwundbarkeit, Werte und Schaden

Cyberattacken und Cybersicherheit als Thema der Technikfolgenabschätzung

Karsten Weber, *Institut für Sozialforschung und Technikfolgenabschätzung, Ostbayerische Technische Hochschule Regensburg, Galgenbergstraße 24, 93053 Regensburg (Karsten.Weber@oth-regensburg.de)* *https://orcid.org/0000-0001-8875-2386*
Markus Christen, *Digital Society Initiative, Universität Zürich (christen@ifi.uzh.ch)*
Dominik Herrmann, *Lehrstuhl Privatsphäre und Sicherheit in Informationssystemen, Fakultät Wirtschaftsinformatik und Angewandte Informatik, Otto-Friedrich-Universität Bamberg (dominik.herrmann@uni-bamberg.de)*

Die monetären Kosten, die jährlich weltweit durch Cyberattacken entstehen, wachsen stetig und bewegen sich in Dimensionen, die mit öffentlichen Haushalten ganzer Staaten verglichen werden können. Cyberattacken treffen Individuen, Unternehmen, öffentliche Einrichtungen, Behörden und Regierungen; sie treffen eine Infrastruktur, ohne die moderne Gesellschaften kaum mehr funktionieren. Doch die Gewährleistung von Cybersicherheit kann zu Zielkonflikten führen. Die Technologien zur Herstellung von Sicherheit und Resilienz dieser Infrastruktur sollten daher Gegenstand der Technikfolgenabschätzung sein.

Threat, vulnerability, values, and damage
Cyberattacks and cybersecurity as a subject of technology assessment

The annual monetary costs incurred worldwide by cyberattacks are growing steadily and are on a scale comparable to the budgets of entire countries. Cyberattacks affect individuals, businesses, public institutions, authorities, and governments; they affect an infrastructure without which modern societies can hardly function. But ensuring cybersecurity can lead to conflicts of interest. Technologies used to ensure the security and resilience of this infrastructure should therefore be a subject of technology assessment.

Keywords: *cybersecurity, cyberattacks, critical infrastructures, resilience*

This is an article distributed under the terms of the Creative Commons Attribution License CCBY 4.0 (https://creativecommons.org/licenses/by/4.0/)
https://doi.org/10.14512/tatup.29.1.11

Digitalisierung allerorts

Spätestens mit der weltweiten Verbreitung von Social Media und Smartphones, welche die Nutzung von Plattformen sowie des Internets allgemein zu jeder Zeit an jedem Ort ermöglichen, haben Informations- und Kommunikationstechnologien (IKT) fast alle gesellschaftlichen Lebensbereiche und Praktiken weithin sichtbar durchdrungen. Dies betrifft nicht nur alltägliche Lebensvollzüge wie Information, Konsum oder Bankgeschäfte einzelner Personen, auch die globale Verknüpfung wirtschaftlicher Prozesse – von Produktion über Logistik bis hin zum internationalen Finanzwesen – stützt sich heutzutage entscheidend auf IKT ab. Immer mehr, früher informell ablaufende wirtschaftliche und gesellschaftliche Prozesse werden in digitalen Systemen abgebildet und damit steuerbar. Dieser Prozess der Durchdringung wird seit einigen Jahren als Digitalisierung bezeichnet, doch es ist offenkundig, dass die damit benannten Veränderungen lange vor der Entstehung sozialer Medien und der mobilen Internetnutzung begonnen haben: Banken und Versicherungen, Fluggesellschaften und Logistikunternehmen haben bereits in den 1960er- und 1970er-Jahren, also vor mehr als einem halben Jahrhundert, damit begonnen, Geschäftsprozesse zu digitalisieren – nur nannte man dies noch nicht so. Handel, Industrie und Verkehr, aber auch die Gesundheitswirtschaft, die öffentlichen Verwaltungen, das Militär und die Sicherheitsbehörden sowie viele andere Sektoren der Wirtschaft und des öffentlichen Lebens nutzen schon lange IKT zur Verwaltung von Datenbeständen, die für die Funktion der entsprechenden Organisationen essentiell sind.

Vergleichsweise neu ist dagegen die massive Vernetzung all dieser IKT-Systeme. Zwar sind sehr große oder gar globale Computernetzwerke ebenfalls nichts wirklich Neues; man denke an das in den 1950er-Jahren entstehende vernetzte SAGE-Computersystem in den USA zur Steuerung der kontinentalen Flug-

abwehr (Redmond und Smith 2000) oder an die sowjetischen Pendants, die allerdings in westlicher wissenschaftlicher Literatur kaum behandelt werden (Gerovitch 2004). Im zivilen Bereich wären die großen Flugbuchungssysteme wie Sabre und Apollo zu nennen, die bereits in den 1960er- und 1970er-Jahren entstanden (Copeland et al. 1995). Doch diese Systeme nutzten Vernetzungstechnologien, die mit dem, was wir heute als Internet kennen, wenig bis nichts gemeinsam hatten. Ihre Zugänglichkeit war daher sehr eingeschränkt; in Hinblick auf Sicherheitserwägungen war dies vermutlich ein erheblicher Vorteil.

Unser heutiges Bild vernetzter Computer ist durch Ubiquität, allgemeine Zugänglichkeit, Mobilität und nicht zuletzt durch geringe Kosten der Vernetzung geprägt; auch wenn zunehmend der Energiebedarf der digitalen Transformation kritischer diskutiert wird (Jones 2018). Vielleicht aber noch mehr spielt eine Rolle, dass die meisten Menschen das Internet mit dem WWW und sozialen Medien gleichsetzen und deren Entertainmentfunktionen betonen. Damit gerät jedoch in den Hintergrund, dass diese Dienste längst zu einer Infrastruktur geworden sind, von deren korrekter Funktion ein erheblicher Teil der globalen Wertschöpfung abhängig ist.

Unabhängig davon, wie jemand auf vernetzte IKT schaut: Diese Technologie beeinflusst unsere Denkweise, unsere Interaktionen mit anderen Personen sowie mit Organisationen und Institutionen; sie verändert unsere Rollen als Bürgerinnen und Bürger, Arbeitnehmerinnen und Arbeitnehmer oder auch als Verbraucherinnen und Verbraucher. IKT als komplexe und vernetzte Basistechnologie des 21. Jahrhunderts macht unsere Welt zu einem wohlhabenderen, effizienteren und sehr interaktiven Ort – IKT kann die Kommunikation und Interaktion zwischen Menschen über Staats- und Kulturgrenzen hinweg erleichtern oder gar erst ermöglichen. Doch gleichzeitig machen Komplexität und hochgradige Vernetzung IKT anfällig für technisches Versagen sowie für kriminelle, terroristische oder gar kriegerische Attacken, sodass es mit zunehmender Komplexität und Vernetzung immer schwieriger wird, die Funktionsfähigkeit von Industrien oder Versorgungsinfrastrukturen aufrechtzuerhalten. Moderne Gesellschaften, deren Funktionsfähigkeit auf IKT beruht, sind daher – mit Ulrich Beck (1986) gesprochen – „gefährdete Gesellschaften“. Das ist der Ausgangspunkt des TATuP-Themas „Cybersicherheit“.

Je mehr Gesellschaften auf funktionierende IKT angewiesen sind, desto eher neigen sie dazu, Sicherheit über alle anderen Werte zu stellen.

Cyberspace, Cyberkriminalität, Cyberterror: Unsicherheit

Die durch Cyberattacken weltweit verursachten Kosten sind enorm: „Our current estimate is that cybercrime may now cost the world almost $ 600 billion, or 0.8 % of global GDP“ (CSIS 2018, S. 4). Andere Kennzahlen sind ebenso beindruckend wie erschreckend: „One major internet service provider (ISP) reports that it sees 80 billion malicious scans a day, the result of automated efforts by cybercriminals to identify vulnerable targets. Many researchers track the quantity of new malware released, with estimates ranging from 300,000 to a million viruses and other malicious software products created every day“ (CSIS 2018, S. 4). Aus gesellschaftlicher Sicht sind nicht nur die direkten Kosten (z. B. Reparaturkosten, betrugsbedingte Verluste), sondern auch indirekte Kosten (beispielsweise Kosten von Präventivmaßnahmen) und implizite Kosten (u. a. geringere Produktivitätssteigerungen durch geringeres Vertrauen in digitale Transaktionen) auf Verletzungen der Cybersicherheit zurückzuführen (Bauer und van Eeten 2009). Angesichts solcher Zahlen ist es wenig überraschend, wenn das Center for Strategic and International Studies schreibt: „Over the last 20 years, we have seen cybercrime become professionalized and sophisticated. Cybercrime is a business with flourishing markets offering a range of tools and services for the criminally inclined“ (CSIS 2018, S. 12). Wer weiß, wo man suchen muss, findet im Netz all die Werkzeuge, die notwendig sind, um selbst Cyberattacken zu verüben, ohne dass dabei ein besonderes Wissen notwendig wäre; man kauft sich einfach *Cybercrime-as-a-Service*.

Es kann somit kaum verwundern, dass aktuelle Cybersicherheitsdebatten geprägt sind von der Betonung immer größerer und vielfältiger werdender Bedrohungsformen, die von Cyberkriminalität und Cyberspionage bis hin zu Cyberterror und Cyberwar (Dunn Cavelty 2014) reichen. Cybersicherheit ist dadurch auch zu einer Angelegenheit staatlicher Akteure geworden; die Ausgaben für verteidigungsbezogene Aspekte von Cybersicherheit steigen (Brito und Watkins 2011; Boulanin 2013).

Schon dieser kurze Überblick weist auf die Gefahr hin, Diskurse über Cybersicherheit thematisch einzuengen: Je mehr Gesellschaften auf funktionierende IKT angewiesen sind, desto eher neigen sie dazu, Sicherheit über alle anderen Werte zu stellen, auf denen unsere Gesellschaften aufbauen. Infolgedessen werden Grenzen, die bisher unsere soziale, institutionelle, rechtliche und moralische Welt konstituiert haben, infrage gestellt, kompromittiert oder relativiert. Traditionelle Differenzierungen und Abgrenzungen getrennter sozialer Bereiche wie Familie und Freundschaft, Arbeit, Politik, Bildung, kommerzielle Aktivität und Produktion, Gesundheitswesen, Forschung usw., die jeweils durch kontextbezogene Normen und Regeln bestimmt sind, werden durch IKT bedroht. Betroffen sind beispielsweise Konzepte wie informierte Einwilligung, persönliche Daten oder Anonymität sowie die ihnen zugrundeliegenden Werte wie Autonomie, Fairness, Privatsphäre und Verantwortung. Diese Werte können durch eine übermäßige Betonung des Werts Sicherheit außer

Kraft gesetzt werden; insbesondere wenn Cyberbedrohungen als grundlegende Bedrohung der gegenwärtigen Lebensweise angesehen werden.

In Hinblick auf Privatsphäre, Datenschutz, Computer- und Cybersicherheit sollte allerdings nicht der Eindruck erweckt werden, dass die Debatte erst kürzlich begonnen hätte. Schon 1967 stellt Alan F. Westin in seinem häufig zitierten Buch *Privacy and Freedom* den Zusammenhang zwischen dem Schutz der Privatsphäre (als Schutz privater Daten) und Freiheit her; wenige Jahre später bringen Lance J. Hoffman (1973) und James Martin (1973) Sicherheit und Privatsphäre bei der Verarbeitung von Daten in Computersystemen zusammen. Sicherlich wäre es lohnenswert, die damaligen Diskurse zu rekonstruieren, um zu sehen, inwieweit daraus Lehren zu ziehen sind – vermutlich nicht in einem technischen Sinne, aber doch in politischer Hinsicht.

Wie viel Absicherung gegen Risiken von Cyberattacken – sei es krimineller, terroristischer oder kriegerischer Art – letztlich erforderlich ist, ist umstritten und muss gesellschaftlich stets neu ausgehandelt werden. Es kann gut sein, dass das Repertoire der vorhandenen Maßnahmen und Mechanismen bereits ausreicht, weil Gesellschaften es gewohnt sind, Risiken einzugehen und im Bedarfsfall zu handeln (Odlytzko 2019). Cybersicherheit herzustellen bedeutet nicht nur die Überwindung technischer Hindernisse, sondern benötigt gleichzeitig ein tieferes Verständnis für die Veränderungen, die sich aus der Digitalisierung des modernen Lebens ergeben. Es bedarf einer multiperspektivischen Sichtweise, an der Expertinnen und Experten aus verschiedenen wissenschaftlichen Disziplinen ebenso wie aus unterschiedlichen Professionen beteiligt sein müssen.

Die Beiträge dieser Ausgabe

Der erste Beitrag thematisiert das Problem, dass die Herstellung von Cybersicherheit ganz erhebliche langfristige Herausforderungen mit sich bringen kann. Tim Zander, Pascal Birnstill, Florian Kaiser, Marcus Wiens, Jürgen Beyerer und Frank Schultmann zeigen dies in ihrem Beitrag „IT-Sicherheit im Wettstreit um die erste autonome Fahrzeugflotte“. Zeit ist der Faktor, der Technikfolgenabschätzung so schwierig macht – je weiter in die Zukunft wir zu schauen versuchen, desto unschärfer wird unser Blick. Wenn aber heute Technik in den Verkehr (in diesem Fall im wortwörtlichen Sinne) gebracht wird, die in großer Zahl und langfristig genutzt wird und gleichzeitig auch erhebliche Schäden verursachen kann, dann wäre dem Vorsorgeprinzip zufolge ganz besondere Vorsicht geboten. Dies gilt ganz besonders für das von den Autoren gewählte Beispiel (teil-)autonomer Fahrzeuge mit einer Nutzungsdauer von 20 und mehr Jahren. Doch es gibt nur sehr wenige Einsatzgebiete, in denen es Erfahrung mit der kontinuierlichen Nutzung von IKT-Systemen über mehrere Jahrzehnte hinweg gibt; die oben bereits genannten Banken und Versicherungen haben ihre Computersysteme teilweise solange betrieben oder betreiben sie auch heute noch. Ein Vergleich mit einem großen technischen System wie dem Straßenverkehr würde aber vermutlich zeigen, dass sich die Erfahrungen der Banken und Versicherungen nur bedingt auf (teil-)autonome Fahrzeuge übertragen lassen. Eine Großrechenanlage (*mainframe*) als vergleichsweise geschlossenes System in einem hochkontrollierten Umfeld zu betreiben ist etwas anderes als die Funktionsweise eines aus Millionen Fahrzeugen und einer komplexen Infrastruktur bestehenden großen technischen Systems zu garantieren. Insbesondere, da letzteres unter beileibe nicht vollständig kontrollierten Bedingungen operiert und aus Geräten unterschiedlichster Hersteller besteht. Doch nicht nur die Komplexität unterscheidet sich; auch die Zahl der Stakeholder, deren Homo- bzw. Heterogenität und die Schadensarten unterscheiden sich.

Nachweisbarkeit von Cybersicherheit bedeutet, dass kein einziges Bauteil einer IKT-Infrastruktur Cyberattacken ermöglicht.

Der Beitrag „Building resilient cyber-physical power systems“ von Mariela Tapia, Pablo Thier und Stefan Gößling-Reisemann ist aus Perspektive der Technikfolgenabschätzung sowohl im Hinblick auf die Dimensionen der Zeit als auch des Risikos relevant. Die Stromversorgung gehört zu den kritischen Infrastrukturen, denn die Abhängigkeit der modernen Zivilisation von Elektrizität ist augenfällig. Stromausfälle sind nicht nur lästig, sondern können, wenn großflächig und langandauernd auftretend, Leben, Gesundheit und Eigentum vieler Menschen gefährden, Umweltzerstörung durch sekundäre technische Ausfälle bewirken, die Wirtschaft langfristig schädigen, kurzum: ein Land zum Stillstand bringen. Das Risiko ist also hoch, weil die Schadenshöhe enorm sein kann; das ist an sich nichts Neues. Doch da Stromversorgungssysteme (und andere kritische Infrastrukturen) heute ebenfalls informationstechnisch vernetzt sind, existieren neue Bedrohungen und Angriffsvektoren, die dazu beitragen können, dass nicht nur die Schadenshöhe groß ist, sondern auch die Eintrittswahrscheinlichkeit eines Schadens zunimmt. In solchen Fällen sollten (nicht nur) aus TA-Sicht die Alarmglocken schrillen, denn hier ist besondere Vorsorge notwendig. Insofern liefert der Beitrag Hinweise auf Verfahren, die in den TA-Methodenkoffer gut integriert werden können: Ana-

lysen der Vulnerabilität und Resilienz bedienen die Dimension des Risikos und der Zeit.

Kritische Infrastrukturen spielen in dem Beitrag „Siedlungswasserwirtschaft im Zeitalter der Digitalisierung“ von Martin Zimmermann, Engelbert Schramm und Björn Ebert ebenfalls eine zentrale Rolle; nun sind es aber nicht die Strom-, sondern die Wasserversorger, die in den Blick genommen werden. Im Alltag haben wir uns daran gewöhnt, die Verfügbarkeit von Wasser als etwas Selbstverständliches anzusehen und haben in der Regel vergessen, dass dahinter eine komplexe Infrastruktur steht, auch wenn diese in vielen Fällen regional eingegrenzt ist. Ebenso wie die Stromversorger sind die Wasserversorger zunehmend informationstechnisch vernetzt, sodass neue Angriffs- und Schadensszenarien möglich werden. Meist wäre der Ausfall der Wasserversorgung – sei sie nun durch eine Cyberattacke oder andere Faktoren verursacht – räumlich begrenzt. Allerdings bedeutet dies nicht notwendigerweise eine geringe Schadenshöhe, denn der Ausfall der Wasserversorgung in Großstädten wie Berlin würde möglicherweise Hunderttausende oder gar Millionen Menschen direkt betreffen. Indirekt wäre der Schaden vermutlich noch höher, da eine Attacke auf diese essentielle Versorgungsinfrastruktur psychologisch sehr wirksam wäre.

Diese drei Beiträge verdeutlichen: Es bedarf einer (cyber-)sicheren technischen Infrastruktur nicht nur für den Verkehr, für die Strom- und Wasserversorgung, sondern für alle Bereiche des Einsatzes vernetzter IKT. Entscheidend dabei ist, dass diese Sicherheit nachweisbar ist. Arnd Weber, Gernot Heiser, Dirk Kuhlmann, Martin Schallbruch, Anupam Chattopadhyay, Sylvain Guilley, Michael Kasper, Christoph Krauß, Philipp S. Krüger, Steffen Reith und Jean-Pierre Seifert zeigen in ihrem Beitrag „Sichere IT ohne Schwachstellen und Hintertüren“ auf, wie nachweisbare Sicherheit zu erreichen wäre. Die Größe des Autorenkollektivs deutet bereits an, dass es sich hierbei um keine triviale Aufgabe handelt. Denn letztlich bedeutet Nachweisbarkeit der Sicherheit, dass jedes Bauteil einer IKT-Infrastruktur nachweisbar sicher sein muss in dem Sinne einer (in der Praxis kaum erreichbaren) Zielvorgabe, dass es keine Cyberattacken ermöglicht. Dies gilt für die hochkomplexen Prozessoren und integrierten Schaltkreise, also die Hardware, ebenso wie für die Software, die auf den entsprechenden Geräten ausgeführt wird. Welche Brisanz dieses Thema besitzt, lässt sich an der öffentlich kontrovers diskutierten Frage erkennen, ob Geräte des chinesischen Herstellers Huawei beim Aufbau der nordamerikanischen und europäischen 5G-Netze genutzt werden dürfen, da befürchtet wird, dass die Geräte dieses Unternehmens Hintertüren enthalten, die beispielsweise chinesischen Geheimdiensten einen direkten und verdeckten Zugang zur weltweiten Kommunikation bieten. Hier geht es um Erwägungen individueller, unternehmerischer und staatlicher Sicherheit mit räumlich, zeitlich und risikobezogen weitreichenden Konsequenzen.

Fazit

In der Beschreibung der Beiträge des aktuellen TATuP-Themas war vor allem von Risiken und Schaden die Rede; das muss jedoch ergänzt werden um den Hinweis auf den Nutzen und die Chancen der Vernetzung. Auch beim Thema Cybersicherheit kommen Gesellschaften nicht umhin, eine vernünftige Abwägung von Kosten und Nutzen sowie Risiken und Chancen vorzunehmen.

Alle Beiträge des TATuP-Themas zeigen vor allem aber deutlich auf, dass das Nachdenken über Cybersicherheit ein Bestandteil der Technikfolgenabschätzung sein sollte. Moderne Technik hat heute immer IKT-Anteile; kaum mehr ein Gerät ist nicht vernetzbar. Man mag sich lustig darüber machen, dass Alltagsgegenstände wie Toaster, Küchenmaschinen oder Körperwaagen über WLAN verfügen. Bedenkt man jedoch, dass diese Geräte immer auch einen Zugriffspunkt zu einem WLAN-Netz darstellen, das wiederum den Zugang zum Rest des globalen Internets bieten kann, bekommen diese Alltagsgegenstände und deren Cybersicherheit eine neue Bedeutung. Consumer-Elektronik wird in der Regel nur Monate oder wenige Jahre mit Softwareupdates versorgt – danach werden Sicherheitslücken nicht mehr geschlossen. Diese Tatsache macht solche Geräte zu bevorzugten Angriffspunkten für Hacker, weil man in diesen Geräten beispielsweise unbemerkt Schadsoftware installieren kann, sodass etwa der Kühlschrank plötzlich Teil eines Botnetzes werden kann. Sollte man diese Geräte demnach entsorgen, weil sie ein (Cyber-)Sicherheitsrisiko darstellen? Fallen solche Systeme aus, kann dies eine Kaskade weiterer negativer Auswirkungen nach sich ziehen. Die Krisenfestigkeit ganzer Gesellschaften, das sollten die in den Beiträgen angesprochenen Themen deutlich aufzeigen, steht daher durch die ubiquitäre Nutzung hochkomplexer und vernetzter IKT infrage.

Beim Thema Cybersicherheit kommen Gesellschaften nicht umhin, eine vernünftige Abwägung von Kosten und Nutzen sowie Risiken und Chancen vorzunehmen.

In der Informatik kursiert Gerald Weinbergs – ein vor zwei Jahren verstorbener Computerwissenschaftler – zweites Gesetz: „If builders built buildings the way programmers wrote programs, then the first woodpecker that came along would destroy civilization.“ Sicherlich ist dieser Sinnspruch übertrieben, doch

auch in einer Übertreibung steckt meist ein Quäntchen Wahrheit. In den industrialisierten Staaten dieser Welt funktioniert kaum mehr etwas ohne IKT – das sollte nicht nur, aber auch jenen, die sich mit Technikfolgenabschätzung beschäftigen, zu denken geben.

Danksagung

Die Thema-Herausgeber möchten sich bei den Autorinnen und Autoren sowie den Gutachterinnen und Gutachtern für die gelungene Zusammenarbeit bedanken. Ganz besonderen Dank schulden wir Linda Kokott, die uns bei der Findung der Gutachterinnen und Gutachter unterstützt und bei der ersten Sichtung der eingegangenen Beiträge geholfen hat.

Literatur

Bauer, Johannes; van Eeten, Michel (2009): Cybersecurity. Stakeholder incentives, externalities, and policy options. In: Telecommunications Policy 33 (10–11), S. 706–719. DOI: 10.1016/j.telpol.2009.09.001.

Beck, Ulrich (1986): Risikogesellschaft. Auf dem Weg in eine andere Moderne. Frankfurt am Main: Suhrkamp.

Boulanin, Vincent (2013): Cybersecurity and the arms industry. In: SIPRI Yearbook 2013: Armaments, disarmament and international security, S. 218–226.

Brito, Jerry; Watkins, Tate (2011): Loving the cyber bomb? The dangers of threat inflation in cybersecurity policy. Mercatus Center, Georg Mason University, Working Paper No. 11–24. Online verfügbar unter https://www.mercatus.org/system/files/Loving-Cyber-Bomb-Brito-Watkins.pdf, zuletzt geprüft am 05. 02. 2020.

Copeland, Duncan; Mason, Richard; McKenney, James (1995): Sabre. The development of information-based competence and execution of information-based competition. In: IEEE Annals of the History of Computing 17 (3), S. 30–57. DOI: 10.1109/85.397059.

CSIS – Center for Strategic and International Studies (2018): Economic impact of cybercrime – no slowing down. Online verfügbar unter https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf, zuletzt geprüft am 05. 02. 2020.

Dunn Caveltry, Miriam (2014): Breaking the cyber-security dilemma. Aligning security needs and removing vulnerabilities. In: Science and Engineering Ethics 20 (3), S. 701–715. DOI: 10.1007/s11948-014-9551-y.

Gerovitch, Slava (2004): From newspeak to cyberspeak. A History of Soviet cybernetics. Cambridge, MA: MIT Press.

Hoffman, Lance (1973): Security and privacy in computer systems. Los Angeles, CA: Melville Publications.

Jones, Nicola (2018): How to stop data centres from gobbling up the world's electricity. Nature 561 (7722), S. 163–166. DOI: 10.1038/d41586-018-06610-y.

Martin, James (1973): Security, accuracy, and privacy in computer systems. Englewood Cliffs: Prentice-Hall.

Odlyzko, Andrew (2019): Cybersecurity is not very important. Working Paper. Online verfügbar unter http://www.dtc.umn.edu/~odlyzko/doc/cyberinsecurity.pdf, zuletzt geprüft am 05. 02. 2020.

Redmond, Kent; Smith, Thomas (2000): From Whirlwind to MITRE. The R & D story of the SAGE air defense computer. Cambridge, MA: MIT Press.

Westin, Alan (1967): Privacy and freedom. New York: Atheneum.

PROF. DR. PHIL. HABIL. KARSTEN WEBER
ist Ko-Leiter des Instituts für Sozialforschung und Technikfolgenabschätzung (IST) der OTH Regensburg und einer der drei Direktoren des Regensburg Center of Health Sciences and Technology (RCHST) sowie Honorarprofessor für Kultur und Technik an der BTU Cottbus-Senftenberg. Er beschäftigt sich derzeit mit individuellen und gesellschaftlichen Auswirkungen von IuK-Technologie sowie mit wertebasierter Gestaltung von Technik insbesondere im Gesundheitsbereich.

PD DR. HABIL. MARKUS CHRISTEN
ist seit 2016 Geschäftsführer der Digital Society Initiative und leitet eine Forschungsgruppe am Institut für Biomedizinische Ethik der Universität Zürich. Seine Forschungsgebiete sind Ethik von Informations- und Kommunikationssystemen, Neuroethik und Empirische Ethik.

PROF. DR. DOMINIK HERRMANN
hat den Lehrstuhl für Privatsphäre und Sicherheit in Informationssystemen an der Fakultät für Wirtschaftsinformatik und Angewandte Informatik der Otto-Friedrich-Universität Bamberg inne. Seine Forschungsthemen sind der Entwurf und die Bewertung nutzbarer und unaufdringlicher Technologien zur Verbesserung der Privatsphäre, der Schutz vor unerwünschter Verfolgung von Online- und Mobilnutzern sowie allgemein Sicherheits- und Datenschutzfragen.