TATuP

ZEITSCHRIFT FÜR TECHNIKFOLGENABSCHÄTZUNG IN THEORIE UND PRAXIS

JOURNAL FOR TECHNOLOGY ASSESSMENT IN THEORY AND PRACTICE

www.tatup.de peer reviewed & open access 29/1 (2020)

Thema Cybersicherheit. Bedrohung, Verwundbarkeit, Werte und Schaden

Forschung Möglichkeiten und Grenzen der Digitalisierung von Unterricht

Interview *Ernst Dieter Rossmann:* „Wissenschaft und politische Beratung“

TATuP – Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis ist die begutachtete Open-Access-Zeitschrift für das interdisziplinäre Feld der Technikfolgenabschätzung und angrenzende Forschungsgebiete. Die Zeitschrift richtet sich an eine inter- und transdisziplinäre Leserschaft.

TATuP – Journal for Technology Assessment in Theory and Practice is the peer reviewed open access journal for the interdisciplinary field of technology assessment and neighboring fields of research. It addresses an inter- and transdisciplinary readership.

IMPRESSUM / LEGAL NOTICE

HERAUSGEBER/EDITOR

Karlsruher Institut für Technologie (KIT)
Institut für Technikfolgenabschätzung
und Systemanalyse (ITAS)
Karlstraße 11
76133 Karlsruhe
Germany

VERLAG / PUBLISHING HOUSE

oekom verlag GmbH
Waltherstraße 29
80337 München
Germany

Institut für Technikfolgenabschätzung
und Systemanalyse (ITAS)
Karlstraße 11
76133 Karlsruhe
Germany
+49 (0)721 608 26014
redaktion@tatup.de

HINWEISE FÜR AUTORINNEN UND AUTOREN / INFORMATION FOR AUTHORS
www.tatup.de/index.php/tatup/Submit

ERSCHEINUNGSWEISE / PUBLICATION SCHEDULE
3× jährlich / 3× per year

BESTELLUNG / SUBSCRIPTION
www.tatup.de/index.php/tatup/subscriptionStatic

www.oekom.de/tatup/bezug
Verlegerdienst München GmbH
Aboservice oekom verlag
Gutenbergstraße 1
82205 Gilching
Germany
+49 (0)8105 388 563
+49 (0)8105 388 333
oekom-abo@verlegerdienst.de

TATuP ONLINE
www.tatup.de
Newsletter: www.oekom.de/newsletter

PAPIER / PAPER
Gedruckt auf Circle*offset* Premium White, 100 % FSC®-Recyclingpapier, zertifiziert mit dem Blauen Engel (RAL-UZ 14). /
Printed on Circle*offset* Premium White, 100 % FSC® recycled paper, certified with The Blue Angel (RAL-UZ 14).

DRUCK / PRINTING
Friedrich Pustet GmbH & Co. KG
93051 Regensburg
Germany
www.pustet-druck.de

ANZEIGEN / ADVERTISEMENTS
Mona Fricke
oekom verlag GmbH
+49 (0)89 54418417
anzeigen@oekom.de

VISUELLE KONZEPTION & GESTALTUNG / VISUAL CONCEPT & DESIGN
Kornelia Rumberg, www.rumbergdesign.de

GRAFIK & SATZ / GRAPHIC DESIGN & TYPESET
Tobias Wantzen, www.wantzen.com

ISSN
1619-7623 (Print), 2199-9201 (Online)

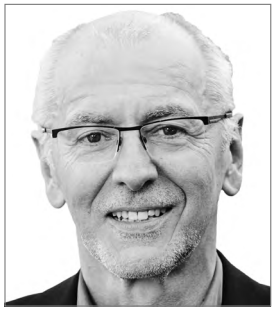
Erfüllungsort / Gerichtsstand: München, Deutschland
Place of fulfillment / Place of jurisdiction: Munich, Germany

RECYCLED Papier aus Recyclingmaterial FSC® C014889

Climate neutral Publisher ClimatePartner.com/53585-1805-1001

oekom kompensiert bereits seit 2008 seine unvermeidlichen CO_2-Emissionen. / Since 2008 oekom offsets its unavoidable CO_2 emissions.

Editorial



ARMIN GRUNWALD
Institut für Technikfolgenabschätzung und Systemanalyse (ITAS), Karlsruher Institut für Technologie (KIT)
(armin.grunwald@kit.edu)

ULRICH UFER
Institut für Technikfolgenabschätzung und Systemanalyse (ITAS), Karlsruher Institut für Technologie (KIT)
(ulrich.ufer@kit.edu)

Die Covid-19-Pandemie fordert weltweit viele tausend Tote, bringt Gesundheitssysteme an ihre Grenzen, reduziert das öffentliche Leben drastisch und dominiert die Medien. Auch Universitäten und Forschungseinrichtungen arbeiten unter großen Einschränkungen.

Unter den Bedingungen von Unsicherheit und steigenden Infektionszahlen heute, am 18. März, die aktuelle Situation aus Perspektive der Technikfolgenabschätzung (TA) zu kommentieren, ist an sich ein unsicheres Unterfangen. Angesichts der Beschleunigung der Ereignisse könnte am Drucktermin vieles schon überholt sein, vielleicht stellen die ‚gegenwärtigen Zukünfte' nur Momentaufnahmen dar.

Drei Beobachtungen der letzten Wochen möchten wir hier nennen, die über die eher trivialen, wenn auch real hoch relevanten, Dinge hinausgehen, z. B. dass mehr Vorsorge in der Verfügbarkeit von Mundschutzmasken angesagt sein muss.

Erstens: Das Coronavirus zeigt deutlich, wie die Fragilität moderner globaler Gesellschaften weitgehend von der Annahme verdrängt wurde, alles würde schon immer weiter so funktionieren. Obwohl die ‚Komprimierung von Zeit und Raum' seit Jahrzehnten den globalisierten Personen- und Warenverkehr charakterisiert, hatten dennoch auch viele Expertinnen und Experten noch vor wenigen Wochen nicht erkannt, dass ein Virus aus einer bisher weitgehend unbekannten chinesischen Provinz unser Leben auf den Kopf stellen könnte. Entsprechend wurde das Vorsorgeprinzip lange außer Acht gelassen, zu lange. Sich in Sicherheit wähnen, ist kein guter Ratgeber.

Zweitens: Ein Grundanliegen der TA ist es, auf signifikante systemische Risiken bei gleichzeitig als gering wahrgenommener individueller Gefährdung hinzuweisen, z. B. beim Thema Nachhaltigkeit. Aktuelle Einschränkungen individueller Freiheiten zur Entlastung des Gesundheitssystems zeigen die gesellschaftliche und politische Relevanz dieser Zusammenhänge überdeutlich.

Drittens: Ein Loblied auf die Digitalisierung! Interaktive digitale Formate für Information und Besprechungen mit schnellem Datenaustausch sind gegenwärtig essenziell. Aber wie steril, teils ineffektiv und irgendwie humorlos sind die digitalen Ersatzformate im ausschließlichen Gebrauch, wie reduziert ihre Erfahrungswelt, z. B. bei digitalen Gottesdiensten oder Familienfeiern. Ein Loblied auf die analoge Welt!

Für die TA, aber auch darüber hinaus, heißt dies: das Vorsorgeprinzip ernst zu nehmen und zu begreifen, dass Digitalisierung die analoge Welt bereichert, diese aber nicht ersetzen kann.

Armin Grunwald und *Ulrich Ufer*

http://dx.doi.org/10.14512/tatup.29.1.3

Inhalt

TATuP 1/2020

THEMA

Cybersicherheit

Cyberattacken bedrohen eine Infrastruktur, ohne die moderne Gesellschaften kaum funktionieren können. Doch die Gewährleistung von Cybersicherheit kann zu Zielkonflikten führen: Je mehr Gesellschaften auf funktionierende Informations- und Kommunikationstechnologie angewiesen sind, desto eher neigen sie dazu, Sicherheit über alle anderen Werte zu stellen.

10

FORSCHUNG

Möglichkeiten und Grenzen der Digitalisierung von Unterricht

Auch die Institution Schule steht vor den Herausforderungen der Digitalisierung. Der DigitalPakt Schule soll helfen, mehr digitale Medien zur Verfügung zu stellen. Doch bessere Lerntechniken führen nicht automatisch auch zu besserem Unterricht.

44

INTERVIEW

Wissenschaft und politische Beratung

Gesellschaftliche Transformationsprozesse stellen auch die Politik vor komplexe Herausforderungen. Ernst Dieter Rossmann (MdB) spricht im Interview über Ansprüche der Politik an die Technikfolgenabschätzung und ihre Rolle in der Demokratie.

52

Meldungen

POLITIK

Österreichisches Regierungsprogramm auf dem Prüfstand

Seit Januar 2020 gibt es in Österreich erstmals eine Bundesregierung aus ÖVP und Grünen. Bemerkenswert aus Sicht der Technikfolgenabschätzung: Im Programm wird „konkret über die Notwendigkeit evidenzbasierter Politik bei technologie- und innovationspolitischen Entscheidungen gesprochen“, so Michael Nentwich. Der Direktor des Wiener Instituts für Technikfolgen-Abschätzung (ITA) hat das Regierungsprogramm auf den Prüfstand gestellt. Er begrüßt den Willen der neuen Regierung, bei öffentlichen Digitalisierungsvorhaben, wie selbstfahrenden Fahrzeugen oder dem 5G-Netz, wissenschaftliche Erkenntnisse zu deren Technikfolgen zu berücksichtigen. Positiv sieht Nentwich auch, dass mit der TA verwandte Begriffe wie „Umweltfolgenabschätzung“ und „Wirkungsfolgenabschätzung“ wiederholt genannt werden. Zudem sei die Rede von ethischer Begleitung bei der Einführung von Technologien, die unsere Gesellschaft nachhaltig verändern. Auch „das wichtige Zukunftsthema ‚Künstliche Intelligenz‘ wurde von den Koalitionspartnern nicht nur als wirtschaftliche Chance begriffen“, stellt Nentwich fest. Vielmehr würden die Autorinnen und Autoren des Regierungsprogramms hier den großen gesellschaftlichen Diskussionsbedarf anerkennen.
www.oeaw.ac.at/ita

Enthält reichlich Technikfolgenabschätzung: das Regierungsprogramm der österreichischen Bundesregierung *(Foto: ita/Peissl)*

HISTORIE

Bundestag beschließt parlamentarische TA

Vor 30 Jahren entschied der Deutsche Bundestag darüber, eine parlamentarische Technikfolgenabschätzung einzurichten. Der historischen Entscheidung vom 16.

TA-Grafik *Technikfolgenabschätzung weltweit*

Globale Herausforderungen erfordern globales Denken. **27 Institutionen aus 22 Ländern und 5 Kontinenten** haben sich im vergangenen Jahr zum Netzwerk globalTA zusammengeschlossen, um sich über kulturelle und politische Grenzen hinweg auszutauschen und voneinander zu lernen.

Weitere Informationen:
globalta.technology-assessment.info

November 1989 waren 16 Jahre parlamentarischer Diskussion und zwei Enquete-Kommissionen vorangegangen, die in der lebhaften Debatte über das Für und Wider verschiedener TA-Modelle mündete. Die Mehrheit der Abgeordneten folgte schließlich dem Vorschlag der damaligen Regierungsparteien CDU/CSU und FDP, den Ausschuss für Forschung und Technologie zusätzlich mit der „Technikfolgen-Abschätzung" zu betrauen und eine externe Forschungseinrichtung mit der wissenschaftlichen Arbeit zu beauftragen. Neun Monate später unterzeichnete der Deutsche Bundestag schließlich am 29. August 1990 den ersten Vertrag mit dem Kernforschungszentrum Karlsruhe für eine dreijährige Pilotphase – die Geburtsstunde des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB). Das TAB wird seitdem durchgehend vom Institut für Technikfolgenabschätzung und Systemanalyse des Karlsruher Instituts für Technologie (KIT) betrieben. Das KIT ist die Nachfolgeorganisation des Kernforschungszentrums Karlsruhe. Seit September 2013 sind auch das IZT – Institut für Zukunftsstudien und Technologiebewertung und der VDI/VDE Innovation + Technik als Partner beteiligt.
www.tab-beim-bundestag.de/de/ueber-uns/geschichte.html

Fünf Fragen an: Denise Riedlinger

Wissenschaftskommunikatorin, Institut für Technikfolgen-Abschätzung der Österreichischen Akademie der Wissenschaften

Was bedeutet TA für Sie?
Es ist ein langes Wort für etwas, was uns alle betrifft! Ich persönlich bin durch TA „aufgewacht", sehe jetzt vieles anders. Ich wusste zum Beispiel lange nichts über Nanotechnologien oder darüber, wie Ältere oder Menschen mit Behinderungen von Innovationen betroffen sind.

Welche Forschungsfrage in diesem Feld finden Sie besonders spannend?
Sicherheit, Überwachung und Privatsphäre haben in Zeiten von KI und Gesichtserkennung hohe Relevanz. Wir haben ein Recht auf Privatsphäre, liefern uns aber gleichzeitig aus, indem wir über das Handy Daten an private Firmen übermitteln oder uns von „smarten" Lautsprechern abhören lassen.

Welcher Zukunftstechnologie sollten wir mehr Aufmerksamkeit schenken?
Die Blockchain wird unsere Gesellschaft verändern und globalen Handel auf eine neue Ebene heben. Das sollten wir uns bereits jetzt ansehen.

Gibt es einen Aspekt an TA, der besonders schwierig zu vermitteln ist?
Die Öffentlichkeit will Antworten, und sie hat ein Recht darauf. TA betrachtet viele Faktoren und befasst sich häufig mit schwer greifbaren Entwicklungen. Ein Tweet reicht da nicht immer aus, um zu vermitteln, dass und wie die Begleitung von Forschung und Innovation durch die TA der Gesellschaft nützt.

Warum ist gute (Wissenschafts-) Kommunikation zum Gelingen von TA nötig?
TA ist unabhängig. Wir liefern Wissen zu Dingen, über die oft noch nicht viel nach außen gedrungen ist. Eine gute Kommunikation ist wichtig, weil unsere Arbeit nicht nur für die Wissenschaft, sondern auch für die Gesellschaft und die Politik Bedeutung hat. Und weil wir verstanden werden wollen.

RANKING

Wuppertal Institut in Think-Tank-Spitzengruppe

Das „Global Go to Think Tank Ranking" hat das Wuppertal Institut erneut zu einem der wichtigsten Forschungs- und Beratungsinstitute weltweit gekürt. Der jährliche Report des Think Tanks and Civil Societies Program (TTCSP) der University of Pennsylvania untersucht den Stellenwert von Politikforschungsinstituten für Regierungen und die Zivilgesellschaft. Weltweit 1700 befragte Expertinnen und Experten aus Politik, Wissenschaft, Journalismus und Wirtschaft wählten das Wuppertal Institut auf Platz neun in der Kategorie Umweltpolitik. „Wir freuen uns sehr, dass die Stimme des Wuppertal Instituts auch international Gehör findet und damit die Arbeit und das hohe Engagement der Wissenschaftlerinnen und Wissenschaftler des Instituts honoriert werden", erklärte Manfred Fischedick, der wissenschaftliche Geschäftsführer des Wuppertal Instituts. Da viele der ökologischen Herausforderungen wie insbesondere der Klimaschutz nur auf globaler Ebene gelöst werden könnten, sei es für sein Institut von extrem hoher Bedeutung, wissenschaftliche Erkenntnisse so aufzubereiten, dass sie weltweit aufgegriffen werden können.
wupperinst.org

Aus dem openTA-Kalender

04.–06. 05. 2020, GRAZ
Critical Issues in Science, Technology and Society Studies
sts-conference.isds.tugraz.at/event/10/

07.–08. 05. 2020, TÜBINGEN
Social Robotics and the Good Life: The Normative Side of Forming Emotional Bonds with Robots
uni-tuebingen.de/einrichtungen/zentrale-einrichtungen/internationales-zentrum-fuer-ethik-in-den-wissenschaften/das-izew/

08.–10. 06. 2020, WIEN
Internationale Konferenz TA20 und NTA9: Digital, direkt, demokratisch? Technikfolgenabschätzung und die Zukunft der Demokratie
www.oeaw.ac.at/ita/veranstaltungen/aktuelle-veranstaltungen/ta20-nta9-konferenz/

17.–19. 06. 2020, LOGROÑO
ethicomp 2020: Paradigm Shifts in ICT Ethics: Societal Challenges in the Smart Society
www.unirioja.es/ethicomp/2020/

18.–21. 08. 2020, WIEN
Governance in an Era of Change – Making Sustainability Transitions. 11th International Sustainability Transition conference, WU Wien
ist2020.at

18.–21. 08. 2020, PRAG
Locating and Timing Matters: Significance and Agency of STS in Emerging Worlds, Chech Technical University
www.easst4s2020prague.org/venue/

WEITERE TERMINE UNTER
www.openta.net/kalender

MEDIEN

Quartier Zukunft startet Podcast

Angewandt forschen ohne Laborkittel oder Schutzbrille, mitten drin im wirklichen Leben. Wie das geht, zeigt seit dem Jahr 2012 das Reallaborprojekt „Quartier Zukunft – Labor Stadt“ im Karlsruher Stadtteil Oststadt. Gemeinsam mit Bürgerinnen und Bürgern, Stakeholdern, Politik und Stadtverwaltung wird dort an einer nachhaltigen Transformation des Quartiers gearbeitet. Um über ihre Forschung zu informieren und Ideen für nachhaltigeres Handeln zu liefern, haben die Wissenschaftlerinnen und Wissenschaftler nun den Podcast „Labor Zukunft – Forschung ohne Kittel“ ins Leben gerufen, für den sie mit dem Campus Radio Karlsruhe zusammenarbeiten. „Wir wollen Wissenschaft erleb- und hörbar machen und Denkanstöße für eine zukunftsfähigere Stadt geben“, erklärt Helena Trenks, die den Podcast des Quartier Zukunft redaktionell betreut. Seine Premiere feierte das Format im Januar 2020 im Campus Radio Karlsruhe. Neue Ausgaben mit Einblicken in die transformative Nachhaltigkeitsforschung gibt es künftig im Zwei-Monats-Rhythmus auf UKW 104,8 in Karlsruhe oder als Stream im Netz.
www.campusradio-karlsruhe.de

ENERGIEWENDE

„Storylines“ für das Energiesystem

Die Energiewende kann nur gelingen, wenn sie als gesamtgesellschaftliches Projekt organisiert wird. Doch wie genau das aussehen soll, wird selten klar formuliert. Das Kopernikus-Projekt ENSURE setzt hier an und zeigt vier mögliche Entwicklungspfade für das deutsche Energiesystem im Jahr 2030 auf. Entstanden sind die so genannten „Storylines“ in Stakeholder-Dialogen unter anderem mit Vertreterinnen und Vertretern aus Industrie, Gewerkschaften und Umweltschutz. Organisiert wurden die Veranstaltungen von der Deutschen Umwelthilfe und dem Öko-Institut gemeinsam mit dem Institut für Technikfolgenabschätzung und Systemanalyse (ITAS). „Zum ersten Mal hat eine vielfältige Gruppe von Vertreterinnen und Vertretern der Zivilgesellschaft über einen so langen Zeitraum zusammengearbeitet, um gemeinsam auszuformulieren, welche Pfade der Energiewende sie mitgehen würden“, erklärt Witold-Roger Poganietz vom ITAS. Ausführlich erläutert werden die Entwicklungspfade in der im Januar 2020 erschienenen Broschüre „Transformation des Energiesystems bis zum Jahr 2030“, die als PDF kostenlos zur Verfügung steht.
www.itas.kit.edu

STUDIE

Automatisiertes Fahren in der Schweiz

Notbremsen, Spur halten, Einparken – schon heute können Autos vieles besser als die Menschen am Steuer. Was, wenn Fahrzeuge vollständig autonom unterwegs sind? Potenziale und mögliche negative Folgen hat die Stiftung für Technologiefolgen-Abschätzung TA-SWISS für die Schweiz untersucht. Gesellschaft und Politik, so die Empfehlung der jetzt vorgelegten Studie, müssen diskutieren, wie weit der Staat in die künftige Mobilität eingreifen soll. Falls selbstfahrende Autos in Zukunft nur wenig reguliert werden, verspreche das einen hohen Grad an individueller Freiheit. Da Autos dann voraussichtlich auch häufig leer unterwegs sind, drohe aber ein weiter wachsendes Verkehrsaufkommen. Alternativ ließe sich mit Hilfe von selbstfahrenden Autos als Taxi- oder Busersatz in Städten der Verkehr und der Parkplatzbedarf reduzieren. Sollten gemeinsam genutzte Fahrzeuge auch auf dem Land bereitstehen, müsste die Verkehrsplanung voraussichtlich sogar von einer zentralen, staatlichen Stelle geleitet werden – was wiederum besondere Anforderungen an den Datenschutz stelle.
www.ta-swiss.ch

WISSENSTRANSFER

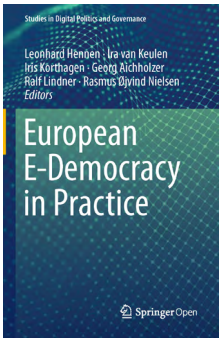
Bürgerwissenschaft zu Typ-1-Diabetes

Citizen Science bindet Bürgerinnen und Bürger unmittelbar in die Forschung mit ein. In der Regel beschränkt sich deren Rolle auf das Beobachten von Naturereignissen oder das Sammeln von Daten, etwa bei Vogelzählungen. Das Projekt TeQfor1 denkt Citizen Science einen Schritt weiter. Es stellt Menschen mit Typ-1-Diabetes, die selbstentwickelte Erweiterungen kommerzieller Systeme zur automatisierten Insulinabgabe nutzen, wissenschaftliche Methoden zur Verfügung. Diese versetzen sie in die Lage, die von ihnen eingesetzte Technologie nach eigenen Kriterien zu bewerten. „Bisher gibt es kaum Studien zur Wirksamkeit dieser automatisierten Erweiterungen. Die Lücke sollen in unserem Projekt die Bürgerinnen und Bürger schließen, die selbst mit Typ-1-Diabetes leben und diese Systeme nutzen“, erklärt die Projektleiterin Silvia Woll vom Institut für Technikfolgenabschätzung und Systemanalyse (ITAS). Durch ihren täglichen Umgang mit dem eigenen Diabetes hätten diese nicht nur eine besondere Expertise, sondern seien auch am besten in der Lage, Kriterien für Lebensqualität von Menschen mit Typ-1-Diabetes festzulegen. Erste Projektergebnisse werden im kommenden Jahr erwartet.
www.itas.kit.edu

PUBLIKATION

Mehr Mitsprache durch E-Partizipation

Digitale Technologien ermöglichen es Menschen, einfacher an politischen Entscheidungen und Willensbildungsprozessen teilzuhaben. Insbesondere auf EU-Ebene könnte das Konzept der E-Partizipation dabei helfen, bestehende Demokratiedefizite zu verringern. Wie das Potenzial digitaler Werkzeuge und Sozialer Medien auf europäischer Ebene ausgeschöpft werden kann, analysiert der neu erschienene Sammelband „European E-Democracy in Practice“. Anhand ausgewählter Projekte untersuchen die Autorinnen und Autoren die Funktionsweise von Instrumenten wie parlamentarischem Monitoring oder E-Voting. Darüber hinaus schlagen sie unter anderem eine einheitliche europäische Beteiligungsinfrastruktur vor, die Bürgerinnen und Bürgern Zugang zu sämtlichen Partizipationsangeboten der EU bietet. Das Open Access-Buch setzt den 2016 erschienenen Band „Electronic Democracy in Europe“ fort und basiert wie dieser auf Studien der European Technology Assessment Group (ETAG) im Auftrag des Europäischen Parlaments.



Hennen, Leonhard; van Keulen, Ira; Korthagen, Iris; Aichholzer, Georg; Lindner, Ralf; Nielsen, Rasmus Øjvind (2020) (Hg.):
European E-Democracy in Practice. Studies in Digital Politics and Governance. Cham: Springer International Publishing, 359 S., ISBN 9783030271831

Personalia

HELGE TORGERSEN hat sich zum Jahresende 2019 nach insgesamt 30 Jahren in der Technikfolgenabschätzung in den Ruhestand verabschiedet. Der promovierte Molekularbiologe war einer der ersten Mitarbeitenden der „Forschungsstelle für Technikbewertung“ in Wien und damit einer der ersten österreichischen TA-Experten überhaupt. Am 1994 aus der Forschungsstelle hervorgegangenen Institut für Technikfolgen-Abschätzung baute Helge Torgersen das Arbeitsfeld Biotechnologie auf. Darüber hinaus forschte er intensiv zum Verhältnis von Technikentwicklung und gesellschaftlicher Wahrnehmung und zuletzt zu theoretischen Fragen der Normativität in der TA.

[Bildquelle: ITA/Peissl]

MANFRED FISCHEDICK, bisheriger Vizepräsident des Wuppertal Instituts, ist seit Anfang 2020 wissenschaftlicher Geschäftsführer des Instituts. Die Aufgabe teilt er sich mit Uwe Schneidewind, der das Institut bisher alleine führte. Als Energie- und Klimaforscher leitete Fischedick über viele Jahre die Forschungsgruppe „Zukünftige Energie- und Mobilitätsstrukturen“. Er ist Professor an der Schumpeter School of Business and Economics der Bergischen Universität Wuppertal und Leitautor von Berichten des Weltklimarates (IPCC). Zudem berät Manfred Fischedick nationale und internationale Akteure in Politik und Wirtschaft bei der Umsetzung von komplexen Transformationsprozessen.

[Bildquelle: Wuppertal Institut]

ANDRÉ GAZSÓ ist erneut zum Vorsitzenden des Nano-Beratungsgremiums des österreichischen Gesundheitsministeriums ernannt worden. Die Leitung der Nanoinformationskommission (NIK) übernimmt der Philosoph und Biologe mit Spezialgebiet Risikoforschung bis 2023. Das vielfältig zusammengesetzte Gremium berät über Themen wie Verbrauchersicherheit, neue Materialien für Lebensmittelverpackungen und Sicherheit am Arbeitsplatz. Ziel sei es „Transparenz und Überparteilichkeit zu schaffen, wenn es um Nanosicherheit geht“, so Gazsó, der am Institut für Technikfolgen-Abschätzung in Wien forscht und dort seit 2007 für das Projekt NanoTrust verantwortlich ist.

[Bildquelle: ITA/Peissl]

THEMA

*Cyber*sicherheit

Bedrohung, Verwundbarkeit, Werte und Schaden

Cyberattacken bedrohen eine Infrastruktur, ohne die moderne Gesellschaften kaum funktionieren können. Doch die Gewährleistung von Cybersicherheit kann zu Zielkonflikten führen: Je mehr Gesellschaften auf funktionierende Informations- und Kommunikationstechnologie angewiesen sind, desto eher neigen sie dazu, Sicherheit über alle anderen Werte zu stellen. Ein TATuP-Thema herausgegeben von Karsten Weber, Markus Christen und Dominik Herrmann.

https://doi.org/10.14512/tatup.29.1.10

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*

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.

IT-Sicherheit im Wettstreit um die erste autonome Fahrzeugflotte

Ein Diffusionsmodell

Tim Zander, *Institut für Anthropomatik und Robotik, Lehrstuhl für Interaktive Echtzeitsysteme Karlsruher Institut für Technologie (KIT), c/o Technologiefabrik, Haid-und-Neu-Str. 7, 76131 Karlsruhe (tim.zander@kit.edu)*
Pascal Birnstill, *Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung (IOSB) (pascal.birnstill@iosb.fraunhofer.de)*
Florian Kaiser, *Institut für Industriebetriebslehre und Industrielle Produktion (IIP), Karlsruher Institut für Technologie (KIT) (florian-klaus.kaiser@kit.edu)*
Marcus Wiens, *Institut für Industriebetriebslehre und Industrielle Produktion (IIP), Karlsruher Institut für Technologie (KIT) (marcus.wiens@kit.edu)*
Jürgen Beyerer, *Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung (IOSB) (juergen.beyerer@iosb.fraunhofer.de)*
Frank Schultmann, *Institut für Industriebetriebslehre und Industrielle Produktion (IIP), Karlsruher Institut für Technologie (KIT) (frank.schultmann@kit.edu)*

In der Fahrzeugindustrie halten aktuell eine Reihe von Neuerungen Einzug. So sorgen neben dem Umstieg auf E-Mobilität hochtechnologische Assistenzsysteme in Fahrzeugen für einschneidende Veränderungen. Eine weitere mit diesen neuen Systemen einhergehende Neuerung ist, dass Autos nun wie Smartphones mit regelmäßigen Updates versorgt werden. Der Hersteller Tesla behauptet sogar, seine Autos in Zukunft per Softwareupdate zum vollautonomen Fahrzeug upgraden zu können. Diese Entwicklung kann zu einer nicht nachhaltigen und risikoreichen Entwicklung der IT-Security und der Umweltbilanz des Fahrzeugsektors führen.

IT security and competition in the automotive industry
A diffusion model

Today's automotive industry is changing rapidly. The slow movement toward electric mobility and highly technical assistant systems challenge old hierarchies. Another innovation associated with the latter is that cars now receive regular software updates, just like smartphones. Tesla even claims to be able to upgrade their cars to fully autonomous driving in the future. This could lead to an unsustainable and risky development of IT security and the environmental performance of the vehicle sector.

Keywords: *IT security; autonomous mobility; diffusion model*

https://doi.org/10.14512/tatup.29.1.16
Submitted: 23. 09. 2019. Peer reviewed. Accepted: 17. 12. 2019

Motivation

Durch den Einzug von Software mit regelmäßigen Updates in Fahrzeugen wird die IT-Security zunehmend relevant für Autobauer. Oftmals fehlt beim Anwender im Diskurs um die Bedeutung der IT-Security das Bewusstsein über die Möglichkeiten, welche Sicherheitslücken einem Angreifer bieten (Bordonali et al. 2017). Entsprechend vulnerabel sind viele modernen Automobile. Dabei sei, glaubt man Elon Musk, ein flottenweiter Hack eines der größten Risiken für die autonome Mobilität. Der Nachrichtendienst heise.de machte in einem Bericht auf die geringen Sicherheitsstandards in der Automobilindustrie aufmerksam, nachdem es einem Hacker gelungen war „weltweit den Verkehr beeinflussen" zu können (Scherschel 2019). Insbesondere die Motivation, eine Vorreiterposition in der autonomen Mobilität einzunehmen und so eine gute Marktposition zu erlangen, kann vor dem Hintergrund der kapitalintensiven Transformation in Richtung Elektromobilität eine weitere Gefahr für die IT-Sicherheit von Automobilen darstellen. Zusammengenommen kann die Verbindung aus Vernetzung, fehlender Erfahrung mit der neuen Technologie und hohem Wettbewerbsdruck potenziell zu hohen systemischen Risiken bzgl. der IT-Sicherheit führen.

Deep und Fleet Learning für autonomes Fahren

In modernen Fahrzeugen stehen sämtliche Fahrer- und Bedienbefehle wie Bremsen, Lenkung, Regelung der Antriebsleistung über ein elektronisches Nachrichtenprotokoll zur Verfügung. Damit sind alle Voraussetzungen erfüllt, um ein Fahrzeug

von einem Computerprogramm autonom steuern zu lassen. Die Frage, die sich nun stellt ist, welche Sensoren und welche Informationsfusion der Daten dieser Sensoren und welche daraus abgeleiteten Steuerbefehle für ein fahrerloses Fahrzeug nötig sind (Paden et al. 2016).

Ein modernes Auto besitzt eine Vielzahl von Sensoren. Als Beispiel dafür kann das seit 2011 vorgeschriebene Electronic Stability Control-System dienen, das durch gezieltes Verzögern einzelner Räder ein Ausbrechen des Wagens zu verhindern versucht. Dafür werden u. a. Sensoren für den Lenkwinkel, Drehrate, Radgeschwindkeits- sowie die Längs- und Gierachsenbeschleunigung benötigt. In einem Auto mit Autonomiestufe 2 (Perret et al. 2018; Gasser et al. 2012; Wood et al. 2019) wird zusätzlich eine Vielzahl von Sensoren für die Beobachtung der Strecke und der anderen Verkehrsteilnehmer benötigt (Gasser et al. 2012).

In der Folge gehen wir exemplarisch auf die Autonomisierungsbemühungen des elektrischen Fahrzeugherstellers Tesla ein. Die einzelnen Wettbewerber unterscheiden sich bezüglich ihres Vorgehens zwar in einigen Aspekten, diese unterschiedlichen Herangehensweisen sind jedoch für unsere Diskussion und für das weitere Verständnis der Thematik nicht weiter relevant. So hat Tesla seit 2016 für den „Autopilot" acht Kamera-, zwölf Sonar- und einen Radarsensor verbaut (Tesla 2019 b). Die eingehenden Daten dieser Sensoren müssen fusioniert werden, um den für das Fahrzeug relevanten Zustand der Umwelt zu schätzen. Diese Information über die aktuelle Situation und das entsprechende Ziel müssen dann in entsprechende Steuerbefehle umgesetzt werden.

Für die Verarbeitung von Bilddaten hat sich Deep-Learning als zielführend erwiesen. Bei diesen Verfahren werden künstliche neuronale Netze durch Lernbeispiele angepasst. Hierbei werden große Datenmengen analysiert, um Muster zu erkennen nach denen dann Entscheidungen getroffen werden können und nach denen das Verhalten ausgerichtet werden kann. Damit werden Maschinen befähigt, autonom ihr Verhalten zu optimieren. Mithilfe dieses Verfahrens können in neuen Bildern mit hoher Genauigkeit Objekte wie Tiere und Fußgänger erkannt werden. Passende Datensätze von Bildern zu erstellen und dann zu annotieren ist ein zeit- und kostenintensives Problem. Für den Betrieb eines autonomen Fahrzeugs ergeben sich weitere Herausforderungen bei der Sensorfusion. Unter anderem muss erkannt werden, welcher Teil der Fahrbahn wirklich frei befahrbar ist und ob etwaige bewegliche Hindernisse (wie andere Verkehrsteilnehmer) den geplanten Fahrweg versperren könnten.

Deshalb werden große Mengen an Trainingsbeispielen benötigt. Der Ansatz, auf welchen Tesla für dieses Problem zurückgreift, ist das sogenannte *Fleet Learning*. Hierbei trägt jedes Auto der Fahrzeugflotte zum Sammeln der Trainingsbeispiele bei. Als Beispiele dafür wurden am Tesla *Autonomy Investor Day* Trainingsdaten von der Flotte gesammelt und von Menschen annotiert, um richtig zu detektieren, ob Fahrräder an anderen Fahrzeugen befestigt sind oder als eigenständige Verkehrsteilnehmer am Verkehrsgeschehen teilnehmen (Tesla 2019 a). Ein weiteres Beispiel stellte die vollautomatische Generierung von Lerndaten dar, um Spurwechsel und Fahrverhalten anderer Fahrzeuge besser vorherzusagen.

Fleet Learning ermöglicht das Sammeln großer Mengen an Trainingsbeispielen für die Software autonomer Fahrzeuge.

Zusammenfassend kann Tesla durch Abfrage der sensorgenerierten Daten seiner Flotte und die Beobachtung der Tesla-Fahrer automatisiert Trainingsbeispiele sammeln und diese teilweise sogar automatisch annotieren (Eady 2019). Diese werden dann zur Verbesserung der Fahrzeugsoftware genutzt.

Obwohl es trotz dieser genannten Fortschritte zurzeit noch nicht klar ist, wann, bzw. ob überhaupt vollautonome Fahrzeuge existieren werden, sollte man sich darüber klarwerden, dass der Kauf eines vollautonomen Fahrzeugs viele Ähnlichkeiten mit dem Kauf von Softwarepaketen hat. So kostet zum Beispiel bei Tesla das gleiche Auto ohne die Autopilotfunktion 5.000 € weniger. Wie bei anderen Softwarelizenzen kann die kommerzielle Nutzung beschränkt werden. So enthält die Lizenz für den Autopiloten von Tesla eine Exklusivitätsklausel, die besagt, dass mit Autos im vollautonomen Modus nur im Tesla Robotaxi-Netzwerk Geld verdient werden kann (Tesla 2019 a).

IT-Sicherheit autonomer Fahrzeuge

Die Anbindung an das Internet zum Zwecke der Versorgung mit Updates, Verkehrs- und Mediendaten führt zu der Gefahr des Remotezugriffs durch unautorisierte Personen. So konnten Forscher 2014 demonstrieren, wie über das Mobilfunknetz ein Auto von der Ferne aus angegriffen wurde und unter anderem die Bremsen deaktiviert werden konnten (Miller und Valasek 2014). Es ist zu erwarten, dass elementare Funktionen wie Bremsen, Lenken und Beschleunigen evtl. sogar gewollt noch für längere Zeit über das Internet zur Verfügung stehen werden, da autonome Fahrzeuge vermutlich noch lange nicht auf alle Situationen selbstständig reagieren können (Wood et al. 2019). Ein menschlicher Operator müsste somit per Fernzugriff eingreifen, um z. B. ein

Wendemanöver zu vollführen, zu dem das Fahrzeug selbst nicht in der Lage ist.

Ein weiteres Problem ist ein starkes Wachstum der Softwaregröße und damit der Komplexität. So erhöhte sich die durchschnittliche Softwaregröße in Fahrzeugen von ca. 10 Mio. Codezeilen im Jahr 2010 auf ca. 150 Mio. Codezeilen im Jahr 2016. Als Konsequenz wurden in letzter Zeit vermehrt softwarebedingte Rückrufe von ausgelieferten Fahrzeugen durchgeführt. Die Sicherstellung hoher Softwarequalität nimmt insofern eine Schlüsselrolle ein, da sie maßgeblich die Sicherheit des Fahrzeugbetriebs bestimmt und für den breiten Gebrauch unerlässlich ist (Consumer Watchdog 2019). Eine weitere große Gefahr besteht für die Privatheit aller Verkehrsteilnehmer, da Fahrzeuge Kameras, andere Sensoren und entsprechende Hardware haben, mit denen eine Überwachung sowie Verarbeitung der Daten stattfinden kann. Von ihnen geht also mindestens die gleiche Gefahr für Persönlichkeitsrechte (u. a. Recht auf freie Entfaltung der Persönlichkeit sowie informationelle Selbstbestimmung) der Bürger aus wie von Überwachungskameras im öffentlichen Raum, die durch das Internet erreichbar sind. Darüber hinaus sind Datenschutzproblematiken bezüglich der Datenaggregation sowie der Analyse von Daten der gesamten Fahrzeugflotte zu nennen.

Ähnlich wie im Softwaremarkt ist auch eine Monopolisierung des Marktes für autonome Mobilität zu erwarten.

Auswirkungen auf den wirtschaftlichen Wettbewerb

Der dargestellte technologische Schock in der Automobilbranche durch autonomes Fahren verändert die Wettbewerbssituation erheblich. Hierbei ist die Verlagerung der Differenzierungsmerkmale und Veränderung der Wahrnehmung des Automobils von einer maßgeblich durch ihre Hardware bestimmten Maschine hin zu einer sich durch Software definierenden Maschine von großer Bedeutung (Teece 2018). So verschiebt sich durch autonomes Fahren der Fokus des Kunden vom Fahrerlebnis hin zur fahrzeuginternen Multimediaerfahrung (Aboagye et al. 2017). Dies hat zur Folge, dass sich die Regeln des Wettbewerbs grundlegend verändert und dadurch den Markt für neue Wettbewerber geöffnet haben. Dementsprechend drängen viele neue Wettbewerber auf den Automobilmarkt (Teece 2018). Hierbei ist nicht nur eine vertikale, sondern auch eine horizontale Integration vieler Unternehmen zu beobachten (Burkacky et al. 2018). Dies führt temporär zu einer Steigerung der Wettbewerbsintensität. Ermöglicht wird dies dadurch, dass die etablierten Unternehmen durch die veränderte Bedeutung der Software eines Automobils an Wettbewerbsfähigkeit sowie technologischem Vorsprung verloren haben und somit Markteintrittsbarrieren gesunken sind (Aboagye et al. 2017). Die Auswirkungen des technologischen Schocks verdeutlicht auch die Prognose einer Verringerung des Wertanteils traditioneller Technologien auf dem Automobilmarkt von 98 % im Jahr 2017 auf ca. 50 % im Jahr 2030 (Aboagye et al. 2017).

Die technologischen Rahmenbedingungen der Entwicklung des autonomen Fahrens bestimmen die neue Wettbewerbssituation. Hierbei nimmt die Erlangung eines technologischen Vorsprungs gegenüber den Konkurrenten bei der hohen Komplexität der Software, welche autonomes Fahren ermöglicht, eine entscheidende Rolle ein (Aboagye et al. 2017). Technologischer Vorsprung gegenüber den Wettbewerbern erhöht dabei die Wettbewerbsfähigkeit und damit die potenzielle Marktmacht sowie Marktdurchdringung eines Anbieters. Mit einer gesteigerten Marktdurchdringung verringern sich wiederum die Informationskosten (Charette 2009). Es sei dabei auf das *Fleet Learning* verwiesen, bei dem durch eine größere Marktausbreitung zusammen mit Netzwerkeffekten vereinfacht Trainingsdaten durch sich im Betrieb befindliche Fahrzeuge generiert werden können. Die geringeren Informationskosten gegenüber den Wettbewerbern mit schlechterer Marktposition ermöglichen es den Unternehmen nochmals, ihren technologischen Vorsprung weiter auszubauen (Bertoncello et al. 2016).

Die Entwicklung der Technologie des autonomen Fahrens führt dabei nicht nur zu einem technologischen Vorsprung, sondern verursacht auch hohe Fixkosten. Diese Fixkosten verteilen sich dabei auf alle Fahrzeuge, wodurch sich Skaleneffekte ergeben. Aufgrund der Skaleneffekte (Fixkostendegression) und Netzwerkeffekte (sinkende Informationskosten) steigt der Wert einer Flotte, wie bei Software-Produkten (Anderson 2008), überproportional zu der Zahl seiner Fahrzeuge. Dies wiederum impliziert Lock-In-Effekte, da mit steigender Größe des Netzwerks der Austritt aus dem Netzwerk für jeden Nutzer unattraktiver wird und durch die Exklusivitätsklausel in der Lizenz noch verstärkt wird. Aufgrund der hohen Entwicklungskosten für autonomes Fahren sowie der dargestellten Besonderheiten der Technologie erhöhen sich nun wieder die Markteintrittsbarrieren für neue Marktteilnehmer, welche die Marktposition bestehender Anbieter langfristig sichern. Ähnlich wie im Softwaremarkt (Anderson 2008) ist somit auch eine Monopolisierung des Marktes für autonome Mobilität zu erwarten.

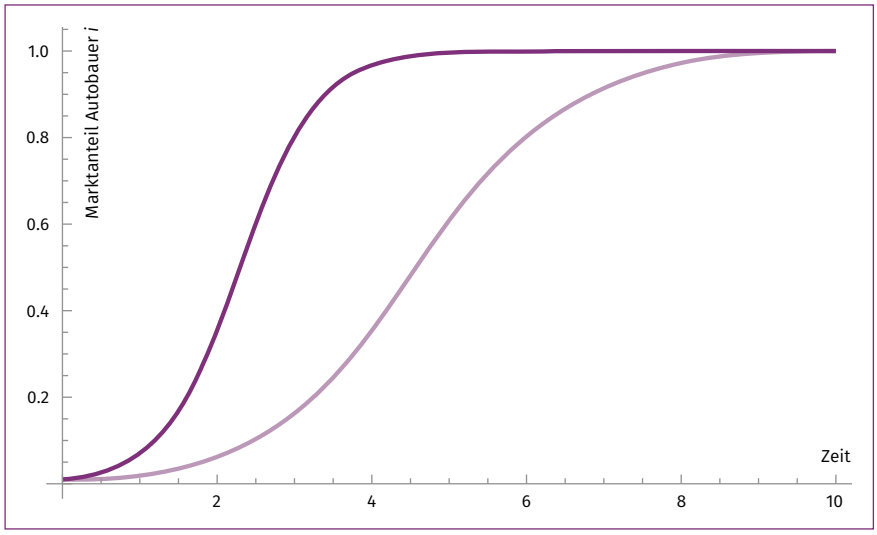


Abb. 1: Marktdurchdringung in Abhängigkeit von IT-Sicherheitsinvestitionen. *Quelle: Eigene Darstellung*

Diffusionsmodell für autonome Fahrzeuge

Um die Marktdurchdringung durch autonome Fahrzeuge und damit den Wettstreit um die erste autonome Fahrzeugflotte zu beschreiben, erscheint die Diffusionstheorie als besonders geeignet, da sie die Adoption neuer Technologien auf einem Markt und damit den Prozess der Marktdurchdringung beschreibt (Geroski 2000). Gemäß Rogers (2010) können die Nutzer neuer Technologien nach dem Grad ihrer Bereitschaft, diese zu nutzen, klassifiziert werden. Hierbei hängen Adoptionsentscheidungen von Informationen über den Nutzen dieser Technologie ab. Die Informationen können dabei aus direktem Erleben aber auch indirekt durch Erzählen erlangt werden. Unter der Annahme einer konstanten Penetrationsrate α kann der Marktanteil $f(t)$ bestimmt werden, der sich als sogenannte Sigmoidfunktion darstellen lässt.

$$f(t) = \frac{1}{1+\frac{1-f(t_0)}{f(t_0)} \cdot e^{-\alpha \cdot (t-t_0)}}$$

Dabei wird für den initialen Marktanteil $f(t_0)$ die Bedingung $f(t_0) > 0$ angenommen, das heißt, das Modell liefert eine Erklärung für die Diffusion autonomer Fahrzeuge nach bereits erfolgtem Markteintritt der Unternehmen. Die Penetrationsrate α beschreibt dabei die Geschwindigkeit der Marktdurchdringung beziehungsweise Diffusion autonomer Fahrzeuge. Sie stellt damit die wichtigste Komponente der Analyse des Wettstreits um die erste autonome Fahrzeugflotte dar.

Davies (1979) bestimmt hierbei als zentrale Determinante den pekuniären Nutzen der Technologie, d. h. die Höhe der Penetrationsrate wird maßgeblich durch den finanziellen Mehrwert durch die Adoption der neuen Technologie bestimmt. Hierbei gilt: je höher der Gewinn für den Nutzer, desto höher seine Priorität der Adoption der neuen Technologie und umso höher die Penetrationsrate. Somit stellt die Erhöhung des Gewinns für den Nutzer beziehungsweise die Vorteilhaftigkeit der neuen Technologie die Priorität für das Handeln der Unternehmen dar, wenn die Erlangung eines möglichst großen Marktanteils in möglichst kurzer Zeit das Ziel ist. Diese Ausrichtung unternehmerischen Handelns scheint in der dargestellten Wettbewerbssituation um die erste autonome Fahrzeugflotte plausibel zu sein.

Das Unternehmen muss also versuchen, autonome Fahrzeuge so günstig wie möglich auf den Markt zu bringen, um in der Phase des intensiven Wettbewerbs möglichst schnell eine ausreichend große Fahrzeugflotte (kritische Schwelle, ab der die Netzwerkeffekte und Skaleneffekte einsetzen) zu erreichen. Unter der Bedingung, dass das Unternehmen kurzfristig keinen Verlust macht, kann die kurzfristige Preisuntergrenze als Veräußerungspreis angenommen werden. Ein tieferer Preis würde das Unternehmen in finanzielle Schieflage bringen, während ein höherer Preis mit dem Unternehmensziel der schnellen Marktdurchdringung nicht konform wäre.

Die Penetrationsrate von Unternehmen i kann bei der Beschränkung der Bestimmung des Nutzens auf den monetären Mehrwert mit der Differenz aus Zahlungsbereitschaft und variablen Kosten gleichgesetzt werden.

$$\alpha_i = Z - k_{v,i}$$

Während im Allgemeinen Ansatz zur Bestimmung der Penetrationsrate ein Nutzenvergleich mit Konkurrenzprodukten erforderlich ist, genügt für den Monopolfall die hier vorgestellte einfache Version, die keine Interaktion mit Konkurrenten erfasst. Unter der Annahme einer konstanten Zahlungsbereitschaft der potenziellen Nutzer stellt sich die Marktdurchdringung in Abhängigkeit von k_v wie in Abb. 1 dar.

Im Hinblick auf die IT-Sicherheit kann es nun erstrebenswert erscheinen Kosten einzusparen, um mit einem geringeren Preis an den Markt zu gehen, insbesondere wenn man die IT-Sicherheit weder als Leistungsmerkmal noch als Begeisterungsmerkmal sieht (Kano et al. 1984). Dies kann am Beispiel der Verbindung von Infotainmentsystemen mit Controller Area Netzwerken erläutert werden, welche sicherheitsrelevante Fahrzeugsysteme steuern (Consumer Watchdog 2019). So stellt das Infotainmentsystem eine Leistungsanforderung und damit ein zentrales Differenzierungsmerkmal dar, während die IT-Sicherheit ein Basismerkmal darstellt. Um eine herausragende Leistung im Bereich des Infotainments zu erreichen, wird hierbei das Controller Area Network zulasten der Sicherheit mit dem Infotainmentsystem verbunden (Consumer Watchdog 2019). Dies hat den Vorteil, dass intelligente Lautstärkeregelungen in Abhängigkeit von

der Geschwindigkeit sowie der Motorgeräusche ermöglicht werden (Consumer Watchdog 2019). Darüber hinaus schränken Sicherheitsmaßnahmen die Funktionalität ein, welches den wahrgenommenen Nutzen bei den Kundinnen und Kunden und damit deren Zahlungsbereitschaft negativ beeinflusst. Es kann für die Firma also sinnvoll sein, in einem kurzfristigen Betrachtungshorizont auf Investitionen in Maßnahmen zur IT-Sicherheit zu verzichten, um eine gute Marktposition zu erreichen (Anderson 2008). Da Kundinnen und Kunden ein sicheres Automobil zunächst nicht von einem nicht sicheren unterscheiden können, kann es aufgrund dieser asymmetrischen Information sogar langfristig zum Marktversagen kommen (Akerlof 1970), wenn zeitversetzt die Sicherheitsdefizite bekannt werden und die Kunden dadurch schließlich verunsichert bzw. abgeschreckt werden. Hierbei unterstreicht das Beispiel der Firma Microsoft, bzw. deren Vorgehen zur Erlangung eines hohen Marktanteils, die angemerkte Ähnlichkeit der Softwarebranche zur Branche der autonomen Mobilität. So hatte Microsoft in den 1990er-Jahren das Motto „Ship it on Tuesday and get it right by version 3“ mit der bekanntermaßen schlechten IT-Sicherheit des Produkts in dieser Zeit. Um eine Monopolstellung zu erreichen war es also nicht nötig, ein von Anfang an sicheres Produkt zu entwerfen (Anderson 2008). Einsparungen bei den Ausgaben für IT-Sicherheit würden also zu einer schnelleren Durchdringung und Beherrschung des Marktes, jedoch langfristig zu steigenden Risiken führen.

Die Wartung von Software in autonomen Fahrzeugen muss langfristig sichergestellt werden.

Auswirkungen auf die IT-Sicherheit

Falls es möglich sein wird, ein vollautonomes Auto zu entwickeln, zur Marktreife zu führen und zeitnah eine entsprechende Marktposition zu erlangen (schnelles Szenario), wird die Bedeutung der IT-Sicherheit durch die große Verbreitung derselben Software an Bedeutung gewinnen. So steigert sich auch die Attraktivität eines Hacks durch die Möglichkeit, mehrere Fahrzeuge zu beeinflussen. Entsprechend wachsen die Anforderungen an die IT-Sicherheit der Fahrzeuge.

Falls sich autonomes Fahren in nächster Zeit nicht verwirklichen lassen sollte, bzw. eine schnelle Marktdurchdringung nicht erreicht werden kann (langsames Szenario) und sich die Investitionen in Techniken des autonomen Fahrens wie *Fleet Learning* als langfristig nicht rentabel erweisen, würden gegensätzliche Effekte eintreten (Porter 2019). So kann das investierte Kapital nicht mehr zurückgewonnen werden, was zur Abwicklung ganzer Unternehmen führen könnte oder diesen zumindest einen rigiden Sparkurs diktieren würde. In diesem Fall könnte es zum Problem werden, dass es dann keinen Verantwortlichen mehr gibt, der die Software warten kann oder will. Diese Gefahr wird durch die steigende Wettbewerbsintensivität in der Automobilbranche sowie durch das Eintreten vieler kleiner Unternehmen immer präsenter. Es wäre also dann unter Umständen unmöglich, etwaige Schwachstellen zu reparieren, da evtl. niemand mehr Zugriff auf den Quelltext der Software hat.

Mindestens würden jedoch Lebenszyklusprobleme auftreten, sollte sich herausstellen, dass die aktuelle Fahrzeuggeneration auch nicht mit Umrüstung für autonomes Fahren geeignet ist. So würde die Softwarewartung bei dieser veraltenden Flotte eine Externalität darstellen, da ökonomische Investitionen ohne zukünftigen Nutzen erforderlich wären. Dies kann damit erklärt werden, dass die Kosten für unterlassene Wartung nicht beim Automobilhersteller anfallen, sondern direkt beim Kunden. Dadurch finden diese Kosten in Marktpreisen keine Berücksichtigung. So wäre es denkbar, dass die Unternehmen den Softwaresupport für Altfahrzeuge einstellen oder den Betrieb derartiger Fahrzeuge künstlich verteuern (Wiens und Chamberlain 2018). Besonders plausibel werden diese Lebenszyklusprobleme, wenn man bedenkt, dass das Durchschnittsalter eines Autos in der Europäischen Union elf Jahre beträgt. So stellt sich die Frage, mit welchen Softwareentwicklungskonzepten man in 20 Jahren Updates für ein heutiges Fahrzeug zur Verfügung stellen kann (Anderson 2018).

Vorschläge zur Vermeidung

Um Bedrohungen durch softwaremäßig nicht mehr gewartete Altfahrzeuge zu vermeiden, wäre es denkbar, diese durch die einschneidende technische Maßnahme des *„Kill Switch“* hart vom Internet zu trennen (Consumer Watchdog 2019). Auch scheint die geforderte Trennung von Infotainment- und Kontrollsystemen in den Fahrzeugen im Hinblick auf die IT-Sicherheit begrüßenswert.

Als Mechanismus für die Erhöhung der IT-Sicherheit könnten Strafen für deren Vernachlässigung dienen. Natürlich stellen sich hier Fragen nach funktionierenden Strafverfahren und Durchsetzbarkeit, die noch überhaupt nicht geklärt sind. Der Vorschlag, sich an den Best Practices der Flugzeugindustrie zu orientieren und sich von allzu komplexer Software zu verabschieden, scheint im Sinne der Wartbarkeit und IT-Sicherheit wünschenswert (Consumer Watchdog 2019). Jedoch steht dies im Gegensatz zum Interesse der Autobauer, die neuesten Assistenzsysteme zu verbauen.

Da Softwarewartung wie gezeigt eine Externalität darstellt, könnten Anbieter zumindest im Falle wirtschaftlicher Schwie-

rigkeiten die Wartung einstellen, den Weiterbetrieb der Fahrzeuge verhindern, die Fähigkeit zur Wartung meistbietend verkaufen oder etwaige Gläubiger des Unternehmens könnten versuchen, durch die künstliche Verteuerung von Updates ihr Kapital zurückzuholen. Dies würde dazu führen, dass sich die Kosten für den Weiterbetrieb eines Fahrzeuges sehr erhöhen oder dieser schlicht unmöglich wird, sodass sich in der Folge die Lebensdauer eines Fahrzeugs verkürzt. Wenn man nun bedenkt, dass ungefähr die Hälfte des gesamten emittierten CO_2 eines Verbrennerfahrzeuges durch die Herstellung erzeugt wird – bei Elektrofahrzeugen ist der absolute Wert und der Anteil noch höher – so ist das vorzeitige Betriebsende eines Automobils aus IT-Sicherheitsproblemen bereits aus ökologischen Gründen untragbar (unter der Vorrausetzung, dass das Fahrzeug dann durch ein neues ersetzt wird). Eine Regulierung, die den Weiterbetrieb der Fahrzeuge über mindestens 20 Jahre sicherstellt, scheint insbesondere aufgrund der gesteigerten Lebenserwartung von Elektroautos wünschenswert. Dass das Interesse an IT-Sicherheit und am günstigen Weiterbetrieb von Altfahrzeugen geringer sein wird als bspw. von Flugzeugen, wird maßgeblich daran liegen, dass es sich bei den Betroffenen um eine deutlich weniger einflussreiche und zahlungskräftige Käufergruppe handelt (Anderson 2008). Da Fahrzeughersteller Gebrauchtwagenmärkte als Wachstumshindernis sehen (Bavier et al. 2019), liegt die Vermutung nahe, dass die mit Kontrolle über die in Fahrzeugen installierte Software einhergehende Macht irgendwann dazu genutzt wird, besonders in wirtschaftlich schwierigen Zeiten den Weiterbetrieb der Fahrzeuge zu erschweren, um damit künstlich Nachfrage zu erzeugen. Zumindest aber sollte nicht darauf gehofft werden, dass die Industrie selbst für eine nachhaltige Softwareentwicklung sorgt und so ein langfristiger Weiterbetrieb der Fahrzeuge mit sicherer Software möglich wird. Ein langfristiger Weiterbetrieb der Fahrzeuge würde einen Teil zur zukünftigen CO_2-Vermeidung beitragen. Aufgrund der bevorstehenden Klimakatastrophe sollten sich Wirtschaft, Wissenschaft und Politik zusammenzuschließen (Anderson 2001), um den IT-Sicherheit und sicheren Weiterbetrieb von Fahrzeugen über die geplante Obsoleszenz hinaus zu gewährleisten.

Literatur

Aboagye, Aaron; Baig, Aamer; Hensley, Russel; Kelly, Richard; Padhi, Asutosh; Shafi, Danish (2017): Facing digital disruption in mobility as a traditional auto player. Online verfügbar unter https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/Facing%20digital%20disruption%20in%20mobility%20as%20a%20traditional%20auto%20player/Facing-digital-disruption-in-mobility-as-a-traditional-auto-player.ashx, zuletzt geprüft am 17. 12. 2019.

Akerlof, Georg (1970): The market for „lemons". Quality uncertainty and the market mechanism. In: The Quarterly Journal of Economics, 84 (3), S. 488–500.

Anderson, Ross (2001): Why information security is hard. An economic perspective. Seventeenth Annual Computer Security Applications Conference, 10–14 December 2001. New Orleans: IEEE Computer Society. DOI: 10.1109/ACSAC.2001.991552.

Anderson, Ross (2008): Security engineering. A guide to building dependable distributed systems. New York: John Wiley & Sons.

Anderson, Ross (2018): Making security sustainable. In: Communications of the ACM, 61 (3), S. 24–26.

Bavier, Joe; Rumney, Emma; Miriri, Duncan (2019): Auto giants battle used car dealers for Africa's huge market. Online verfügbar unter https://www.reuters.com/article/us-africa-autos/auto-giants-battle-used-car-dealers-for-africas-huge-market-idUSKCN1RO0OJ, zuletzt geprüft am 19. 11. 2019.

Bertoncello, Michele et al. (2016): Monetizing car data new service business opportunities to create new customer benefit. Online verfügbar unter https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/Monetizing%20car%20data/Monetizing-car-data.ashx, zuletzt geprüft am 19. 11. 2019.

Bordonali, Corrada; Ferraresi, Simone; Richter Wolf (2017): Shifting gears in cyber security for connected cars. Online verfügbar unter https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/Shifting%20gears%20in%20cybersecurity%20for%20connected%20cars/Shifting-gears-in-cybersecurity-for-connected-cars.ashx, zuletzt geprüft am 19. 11. 2019.

Burkacky, Ondrej; Deichmann, Johannes; Doll, Georg; Knochenhauer, Christian (2018): Rethinking car software and electronics architecture. Online verfügbar unter https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/rethinking-car-software-and-electronics-architecture, zuletzt geprüft am 19. 11. 2019.

Charette, Robert (2009): This car runs on code. Online verfügbar unter https://spectrum.ieee.org/transportation/systems/this-car-runs-on-code, zuletzt geprüft am 19. 11. 2019.

Consumer Watchdog (2019): Kill switch. Why connected cars can be killing machines and how to turn them off. Online verfügbar unter https://www.consumerwatchdog.org/sites/default/files/2019-07/KILL%20SWITCH%20%207-29-19_0.pdf, zuletzt geprüft am 19. 11. 2019.

Davies, Stephen (1979): The diffusion of process innovations. Cambridge, U. K.: Cambridge University Press.

Eady, Trent (2019): Tesla's deep learning at scale. Using billions of miles to train neural networks. What Tesla can do that Waymo can't. Online verfügbar unter https://towardsdatascience.com/teslas-deep-learning-at-scale-7eed85b235d3, zuletzt geprüft am 19. 11. 2019.

Gasser, Tom et al. (2012): Rechtsfolgen zunehmender Fahrzeugautomatisierung. Gemeinsamer Schlussbericht der Projektgruppe. In: Berichte der Bundesanstalt für Straßenwesen. Fahrzeugtechnik Heft F83. Bremerhaven: Wirtschaftsverlag NW. Online verfügbar unter https://bast.opus.hbz-nrw.de/frontdoor/index/index/docId/541, zuletzt geprüft am 14. 01. 2020.

Geroski, Paul (2000): Models of technology diffusion. In: Research Policy 29 (4–5), S. 603–625.

Kano, Noriaki; Seraku, Nobuhiko; Takahashi, Fumio; Tsuji, Shin-Ichi (1984): Attractive quality and must-be quality. In: Journal of the Japanese Society for Quality Control 14 (2), S. 147–156.

Miller, Charlie; Valasek, Chris (2014): Adventures in automotive networks and control units. Online verfügbar unter https://ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf, zuletzt geprüft am 19. 11. 2019.

Paden, Brian; Cap, Michal; Yong, Sze Zheng; Yershov, Dmitry; Frazzoli, Emilio (2016): A survey of motion planning and control techniques for self-driving urban vehicles. In: IEEE Transactions on Intelligent Vehicles1 (1), S. 33–55.

Perret, Fabienne; Fischer, Remo; Frantz, Holger (2018): Automated driving as a challenge to cities and regions. In: TATuP – Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis 27 (2), S. 31–37. DOI: 10.14512/tatup.27.2.31.

Porter, Jon (2019): Elon Musk says free self-driving chip upgrade could come to older Teslas this year. Online verfügbar unter https://www.theverge.com/2019/7/8/20685873/tesla-fsd-chip-upgrade-2019-install-hw2-full-self-driving, zuletzt geprüft am 19. 11. 2019.

Rogers, Everett (2010): Diffusion of innovations. New York: The Free Press.

Scherschel, Fabian (2019): Hacker knackt Auto-GPS-Tracker. „Ich kann weltweit den Verkehr beeinflussen". Online verfügbar unter https://heise.de/-4408466, zuletzt geprüft am 19. 11. 2019.

Teece, David (2018): Tesla and the reshaping of the auto industry. In: Management and Organization Review 14 (3), S. 501–512.

Tesla (2019 a): Tesla Autonomy Investor Day. Online verfügbar unter https://ir.tesla.com/events/event-details/tesla-autonomy-investor-day, zuletzt geprüft am 19. 11. 2019.

Tesla (2019 b): Support Autopilot. Online verfügbar unter https://www.tesla.com/support/autopilot, zuletzt geprüft am 19. 11. 2019.

Wiens, Kyle; Chamberlain, Elizabeth (2018): John Deere just swindled farmers out of their right to repair. Online verfügbar unter https://www.wired.com/story/john-deere-farmers-right-to-repair, zuletzt geprüft am 19. 11. 2019.

Wood, Matthew et al. (2019): Safety first for automated driving. Online verfügbar unter https://www.daimler.com/documents/innovation/other/safety-first-for-automated-driving.pdf, zuletzt geprüft am 19. 11. 2019.

DR. TIM ZANDER

ist wissenschaftlicher Mitarbeiter des Lehrstuhls für Interaktive Echtzeitsysteme (IES) sowie des Kompetenzzentrums für angewandte Sicherheitstechnologie (KASTEL) und forscht im Bereich der Modellierung und Quantifizierung von IT-Security und Privacy.

DR.-ING. PASCAL BIRNSTILL

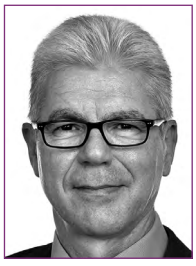
ist wissenschaftlicher Mitarbeiter am Fraunhofer IOSB und KASTEL. Seine Forschungsschwerpunkte liegen im technischen Datenschutz, der Datensouveränität und dem Trusted-Computing.

FLORIAN KAISER

ist wissenschaftlicher Mitarbeiter in der Forschungsgruppe Risikomanagement am Institut für Industriebetriebslehre und Industrielle Produktion (IIP) sowie KASTEL. Er forscht im Bereich des Cyberrisikomanagements und der Analyse sowie Modellierung von Wirtschaftssystemen.

DR. RER. POL. MARCUS WIENS

ist Leiter der Forschungsgruppe Risikomanagement am IIP sowie Mitarbeiter in KASTEL. Seine Forschungsschwerpunkte liegen im Bereich des ökonomischen Risikomanagements, der Analyse von System- und Verhaltensrisiken sowie der Akzeptanz- und Vertrauensforschung.



PROF. DR.-ING. JÜRGEN BEYERER

ist der Leiter des Fraunhofer IOSB sowie des IES Lehrstuhls sowie Mitarbeiter in KASTEL. Seine Forschungsschwerpunkte umfassen u. a. die Automatischen Sichtprüfung und Bildverarbeitung, die Mustererkennung und die semantische Umweltmodellierung.

PROF. DR. RER. POL. FRANK SCHULTMANN

ist Leiter des IIP, des Deutsch-Französischen Instituts für Umweltforschung sowie Inhaber des Lehrstuhls für Betriebswirtschaftslehre, insbesondere Produktionswirtschaft und Logistik und Mitarbeiter in KASTEL. Seine Forschungsschwerpunkte umfassen u. a. stoffstrombasiertes Produktionsmanagement, Konzeption und Optimierung industrieller Kreislauwirtschaftssysteme sowie die techno-ökonomische Bewertung nachhaltig orientierter Investitionen und Innovationen.

Building resilient cyber-physical power systems

An approach using vulnerability assessment and resilience management

Mariela Tapia, *Research Group Resilient Energy Systems, University of Bremen, Enrique-Schmidt-Str. 7, 28359 Bremen (mariela.tapia@uni-bremen.de)*
Pablo Thier, *Research Group Resilient Energy Systems, University of Bremen (thier@uni-bremen.de)*
Stefan Gößling-Reisemann, *Research Group Resilient Energy Systems, University of Bremen*

Power systems are undergoing a profound transformation towards cyber-physical systems. Disruptive changes due to energy system transition and the complexity of the interconnected systems expose the power system to new, unknown, and unpredictable risks. To identify the critical points, a vulnerability assessment was conducted, involving experts from the power as well as the information and communication technologies (ICT) sectors. Weaknesses were identified, e. g., the lack of policy enforcement, which are worsened by the unreadiness of the actors involved. Due to the complex dynamics of ICT, it is infeasible to keep a complete inventory of potential stressors to define appropriate preparation and prevention mechanisms. Therefore, we suggest applying a resilience management approach to increase the resilience of the system. It aims at better riding through failures rather than building higher walls. We conclude that building resilience in cyber-physical power systems is feasible and helps in preparing for the unexpected.

Die Gestaltung resilienter cyber-physischer Energiesysteme
Ein Ansatz basierend auf Vulnerabilitätsanalyse und Resilienzmanagement

Energiesysteme befinden sich in einem tiefgreifenden Wandel hin zu cyber-physischen Systemen. Disruptive Veränderungen, die von der Transformation des Energiesystems und der Komplexität der miteinander verbundenen Systeme herrühren, setzen das Stromnetz neuen, unbekannten Risiken aus. Mit einer Vulnerabilitätsanalyse unter Einbeziehung von Experten aus den Bereichen Energie und Informations- und Kommunikationstechnologien (IKT) wurden Schwachstellen identifiziert, z. B. Nachteile durch die fehlende Durchsetzung von Regulierungen, und eine mangelnde Anpassungsbereitschaft der beteiligten Akteure. Die komplexe IKT-Dynamik macht es unmöglich, potenzielle Stressoren vollständig zu erfassen, um geeignete Präventionsmechanismen zu definieren. Die vorgeschlagenen Resilienzmanagementmaßnahmen zielen darauf ab, Krisen besser zu bewältigen, anstatt auf höhere Barrieren zu setzen. Die Resilienz cyber-physikalischer Energiesysteme ist möglich.

https://doi.org/10.14512/tatup.29.1.23
Submitted: 23. 09. 2019. Peer reviewed. Accepted: 15. 01. 2020

Keywords: *cyber-physical power systems, resilience management, vulnerability assessment*

Introduction

Power systems are evolving through an extended convergence with information and communication technologies (ICT), leading to complex cyber-physical power systems (CPPS). This has brought opportunities to enhance the systems' performance and provide solutions to cope with the associated challenges of energy supply based on distributed and fluctuating renewable energies. However, cyber-attacks targeting power systems have been growing in number and sophistication in recent years. For instance, the attacks against the Ukrainian power grid in 2015 and 2016 that resulted in power outages (Dragos Inc. 2017). Another incident against a utility in the United States was reported on March 2019 (Sobzak 2019). Several risk and vulnerability assessments for power systems have been published in recent years (e. g. NIST 2014; Rossebo et al. 2017). In these studies, potential impacts and mitigation options were evaluated based on lists of potential threats and their likelihood of occurrence. We argue that due to the dynamic nature of ICT and its complex interdependency with the power infrastructure, we have to expect surprises. It will no longer be possible to identify a comprehensive inventory of potential threats, as is the case in classic risk management.

A reliable power supply is of great importance for almost all areas of life, therefore it is necessary to develop strategies that enable the power system to be prepared for expected and unexpected stressors. In other words, it is essential to apply a resilience management strategy. Many definitions of resilience exist in the scientific community (e. g. Jesse et al. 2019). For this study, we describe resilience as *a (socio-technical) system's ability to maintain its services under stress and in turbulent conditions* (Brand et al. 2017; Gleich et al. 2010). The advantage of using this definition is that it focusses on *the system services,* which must be outlined together with the stakeholders/us-

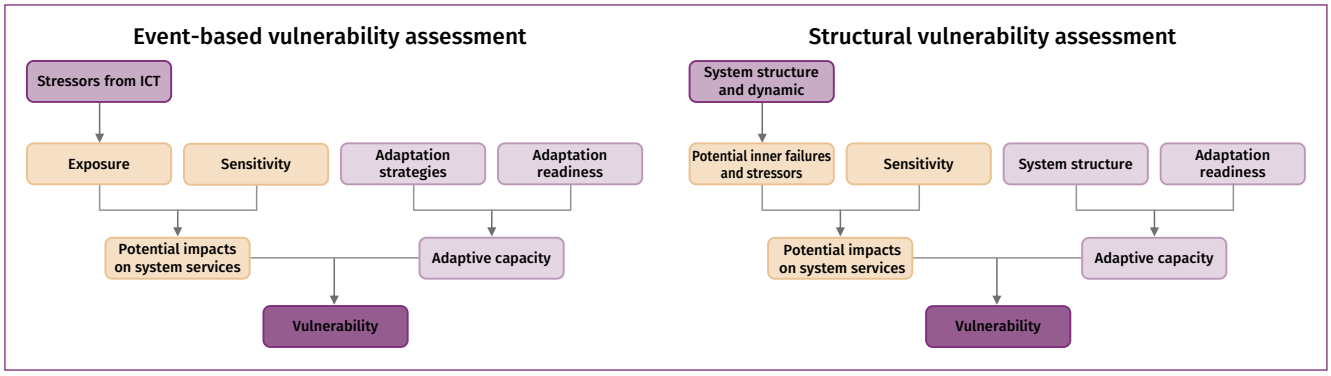


Fig. 1: Schematic representation of the VA methodology. **Left:** Event-based VA. **Right:** Structural VA.
Source: Authors' own compilation based on Gleich et al. (2010) and Gößling-Reisemann et al. (2013)

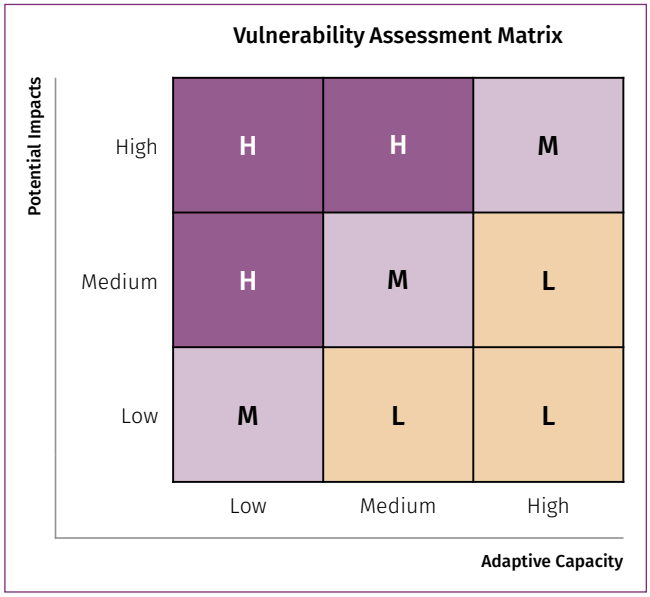


Fig. 2: Vulnerability assessment matrix that considers the level of potential impacts on system services and adaptive capacity. (**H**: High, **M**: Medium, **L**: Low).
Source: Authors' own compilation based on Gleich et al. (2010) and Gößling-Reisemann et al. (2013)

ers. In this way, changes and evolutions of the system are possible, which are core aspects of transitions. The focus lies on the complex nature of interconnectedness and interdependency, and the capability of the system to maintain its *services*.

This article presents the results of an empirical and interdisciplinary base study that involved actors from energy and ICT sectors through interviews and workshops, to get better insights into the vulnerabilities of CPPS. The study consists of two parts. First, a vulnerability assessment (VA) was performed to identify critical points coming from the ICT infrastructure. Second, a resilience strategy was developed by using a resilience management approach to identify how CPPS can be better prepared for any stressor.

Methodology

Vulnerability Assessment Approach

The event-based and structural VA methods (Fig. 1) carried out in Gleich et al. (2010) and Gößling-Reisemann et al. (2013) were used as reference for this study.

The potential impacts were evaluated based on their effect on the *system services,* which were defined in this case according to parameters for both the electric and ICT infrastructures. Regarding the electric infrastructure, the quantity criteria are determined by the system's ability to supply the connected load. The quality criteria are defined by direct technical parameters, such as power quality or reliability indices, and by indirect parameters, such as socio-economic and socioecological impacts. Regarding the ICT infrastructure, the approach considers the effect on the security requirements, i. e. confidentiality, integrity, availability and non-repudiation of data in transit or at rest (e. g. control commands, firmware, software, etc.).

The study focused on the German and European power system covering the complete electrical energy conversion chain and was limited to evaluate stressors from the ICT infrastructure. The component layer of the Smart Grid Architecture Model[1] was used as a reference architecture model. Two workshops and 19 semi-structured interviews were conducted with experts from the sectors: energy, industrial automation, ICT, and public bodies in the period between June 2016 to March 2017. The expert statements were evaluated by means of a comprehensive qualitative content analysis methodology based on Mayring (2014).

Combining the experts' opinions, relevant literature, and our own judgement, the potential impacts were qualitatively rated as high, medium or low according to the effects of stressors and structural weaknesses on the quality and quantity criteria of the system services. In order to determine the adaptive capacity, inputs from experts and literature were considered regarding existing or foreseen adaptation mechanisms and the readiness of the concerned actors to implement them. They were also qualita-

1 http://smartgridstandardsmap.com/

tively rated as high, medium or low. Consequently, the vulnerability level was the result of combining potential impacts and adaptive capacity according to the matrix showed in Fig. 2. A more detailed description on the VA methodology can be found in Tapia et al. (in press)

Resilience Management Approach

Resilient CPPS should have a diverse set of capabilities such as resistance/robustness, adaptation, innovation and improvisation to overcome known and unknown stressors. They help the systems to maintain their *system services* (see definition above). In this study, the resilience management approach described in Acatech et al. (2017) and Goessling-Reisemann and Thier (2019) was used as reference. It comprises a four-phase approach: (1) Prepare and prevent, (2) Implement robust and precautionary design, (3) Manage and recover from crises, and (4) Learn for the future. The suggested measures for each step were developed based on the VA results, the resilience design principles/elements described in Brand et al. (2017) and Goessling-Reisemann and Thier (2019), the statements of the interviewed experts, and our own judgments (Fig. 3).

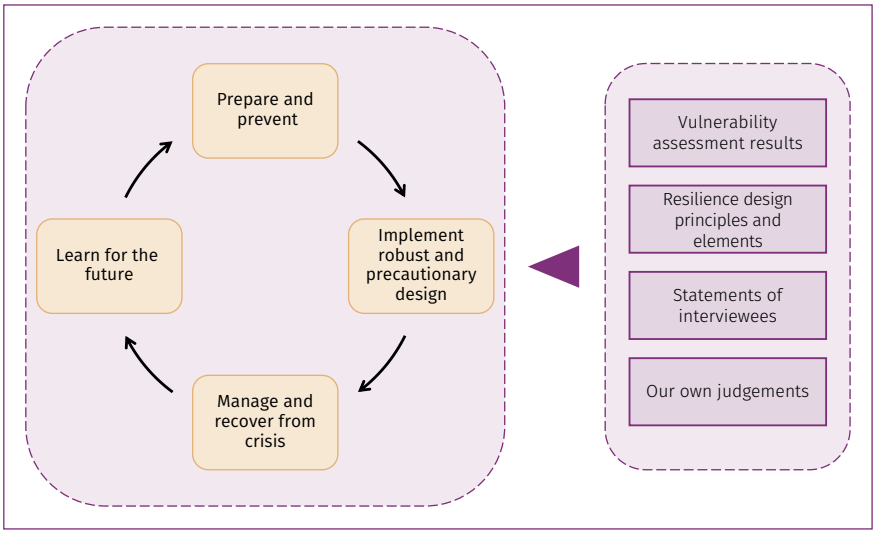


Fig. 3: Four phases of the resilient management approach scheme and the sources for determining the suggested measures for each phase. *Source: Authors' own compilation based on Acatech et al. (2017) and Goessling-Reisemann and Thier (2019)*

Vulnerability Assessment Results

The VA identified critical properties, structures and elements contributing to the vulnerability of the CPPS. Based on the qualitative content analysis results, the findings were sorted into the following four categories: (a) technology, (b) organizational security policies and procedures, (c) the human factor, and (d) regulations. Each category included subcategories and they were assessed individually using the VA methodology described above. All subcategories resulted in *high* vulnerability ratings following the combination of *medium to high* potential impacts with *medium or low* adaptive capacities (Tab. 1). The list of categories and subcategories is not intended to be comprehensive. However, it reflects the fact that the interviewees were queried about what the critical points are according to their opinion, which led to a list of high vulnerabilities. In the following section, the findings for each category will briefly be described.

Technology

The increased number of systems, endpoints and actors involved in the CPPS leads to a higher number of interconnections and communications. If these communications use unencrypted or

Category	Subcategory	Potential Impacts	Adaptive Capacity	Vulnerability
Technology	Insecure endpoints	M–H	M	**H**
	Insecure communications	M–H	M	**H**
Organizational security policies and procedures	Improper patch management	M–H	M	**H**
	Lack of interdisciplinary IT-OT knowledge	M–H	M	**H**
The human factor	Lack of security awareness in organizations	M–H	M	**H**
	Lack of security awareness among consumers	M–H	L	**H**
Regulations	Lack of effective implementation of standards and regulations	M–H	M	**H**
	Lack of coordinated effort to improve security	M–H	M	**H**

Tab. 1: Categories and subcategories that reflect critical properties, structures and elements of CPPS and the corresponding ratings of Potential Impacts, Adaptive Capacity and Vulnerability on the scale **L**: Low, **M**: Medium, **H**: High. *Source: Authors' own compilation based on Tapia et al. (in press)*

weakly encrypted network protocols, authentication keys and data payload are exposed (NIST 2014). Using Man-in-the-Middle attacks, threat agents will be able to listen, inject or manipulate messages between nodes. From one side, legacy communication protocols used in Industrial Control Systems (ICS) in the generation, transmission and distribution domains have evolved from proprietary point-to-point links and isolated from external networks to open and standard protocols. According to the experts, this represents a high security problem. The *'Crashoverride'* malware, which seems to have been used in the Ukraine blackout in 2016, is a good illustration of an advanced malware that leverages the weaknesses of certain ICS protocols (Dragos Inc. 2017).

From the other side, experts also stated that the more distributed and closer to the end-consumer the communication occurs, the more vulnerable it gets. The reason is that devices located at the customer premises (e. g. Internet-of-Things devices) are deployed with poor security features and furthermore, they are not regulated. In most of the cases, they do not have capabilities for secure key management, control access, or patch management. Security challenges and threats of smart home devices are discussed in Lee et al. (2014).

Organizational Security Policies and Procedures

Experts agreed that due to the increasing complexity and interdependencies between IT and Operation Technology (OT) infrastructures, the knowledge needed to address the new challenges has changed. In most of the cases, interdisciplinary knowledge is missing or limited, and therefore it is difficult to properly understand, design, implement and operate the complete complex system. Normally, OT assets are maintained by ICS operators and engineers rather than experienced IT professionals, which can result in common mistakes in maintenance, configuration, and lack of hardening (Bodungen et al. 2017). Moreover, typical IT systems security measures cannot be directly applied in ICS environments, because the process stability or availability could be affected. Therefore, specific and tailored security measures are needed.

As experts stated, ICS usually tend to be outdated, either because vendors do not provide security patches or because the particular system is time-critical. As a consequence, attackers are able to gain access to different system components by exploiting known security-gaps that have not yet been patched. Nevertheless, even if all patches and mitigations are kept up-to-date, attacks are becoming more sophisticated and adversaries use unknown zero-day exploits (McLaughlin et al. 2015), i. e. attacks based on previously unidentified and unpatched cyber-security gaps.

The Human Factor

The lack of effective security trainings and awareness programs in power sector organizations can lead to insufficiently trained or engaged personnel in cyber-security aspects (NIST 2014). Applying social engineering, threat agents are exploring new attack mechanisms targeting different levels in the organization. This is one of the fastest growing security problems according to the experts. In the Ukrainian blackout in 2015, attackers developed the *Blackenergy 3* tool malware and performed a phishing campaign targeting employees from the electricity distributor (Styzcynski and Beach-Westmoreland 2019).

Disgruntled employees, or ex-employees, who are not properly managed when leaving the company, may represent further potential threat actors. They could have detailed knowledge of the systems and access to critical data, allowing them to identify weak internal structures and methods to compromise the systems. Furthermore, critical information about the system configuration could be even publicly available through vendors' or asset owners' websites, employees' social media sites, or from other sources. Attackers can leverage this information for planning the attack.

Additionally, experts mentioned also that end users represent another vulnerable point because of their lack of awareness or understanding of the consequences of eventually low security of their smart devices. A more complex problem derives from end-users being prosumers, who may not have the expert-knowledge to implement and maintain appropriate security measures for Distributed Energy Resource (DER) systems (e. g. smart inverters).

Regulations

The lack of an effective implementation of security standards and regulations represents another critical point for CPPS. Experts considered that the absence of mandatory regulations to enforce power system operators to implement minimum required security standards, or vendors to provide the necessary security requirements in their products expose the system to possible cyber-attacks, for instance man-in-the-middle attacks on non-upgraded ICS systems running the IEC 60870-5 protocol (Maynard et al. 2014).

Different technical and organizational standards have been developed to address cyber-security requirements in smart grids (ENISA 2012; NIST 2014). Nevertheless, as experts stated, in most of the cases, these are only recommendations and the compliance to a minimum-security level is not enforced by regulations. Furthermore, the experts mentioned that there are no economic incentives for grid operators to invest in cyber-security enhancements. The decision to upgrade legacy ICS in order to implement the security measures could be delayed until the next planned lifecycle equipment replacement, not only because of the processes' criticality, but due to the additional associated costs. Another critical point, as experts remarked, is the missing effective coordination to improve security for the overall system.

The critical points discussed in this section are related to all categories mentioned above. The relationship is seen as lack of readiness of the involved actors to implement existing adaptation strategies. Thus, increasing the vulnerability level of each category itself.

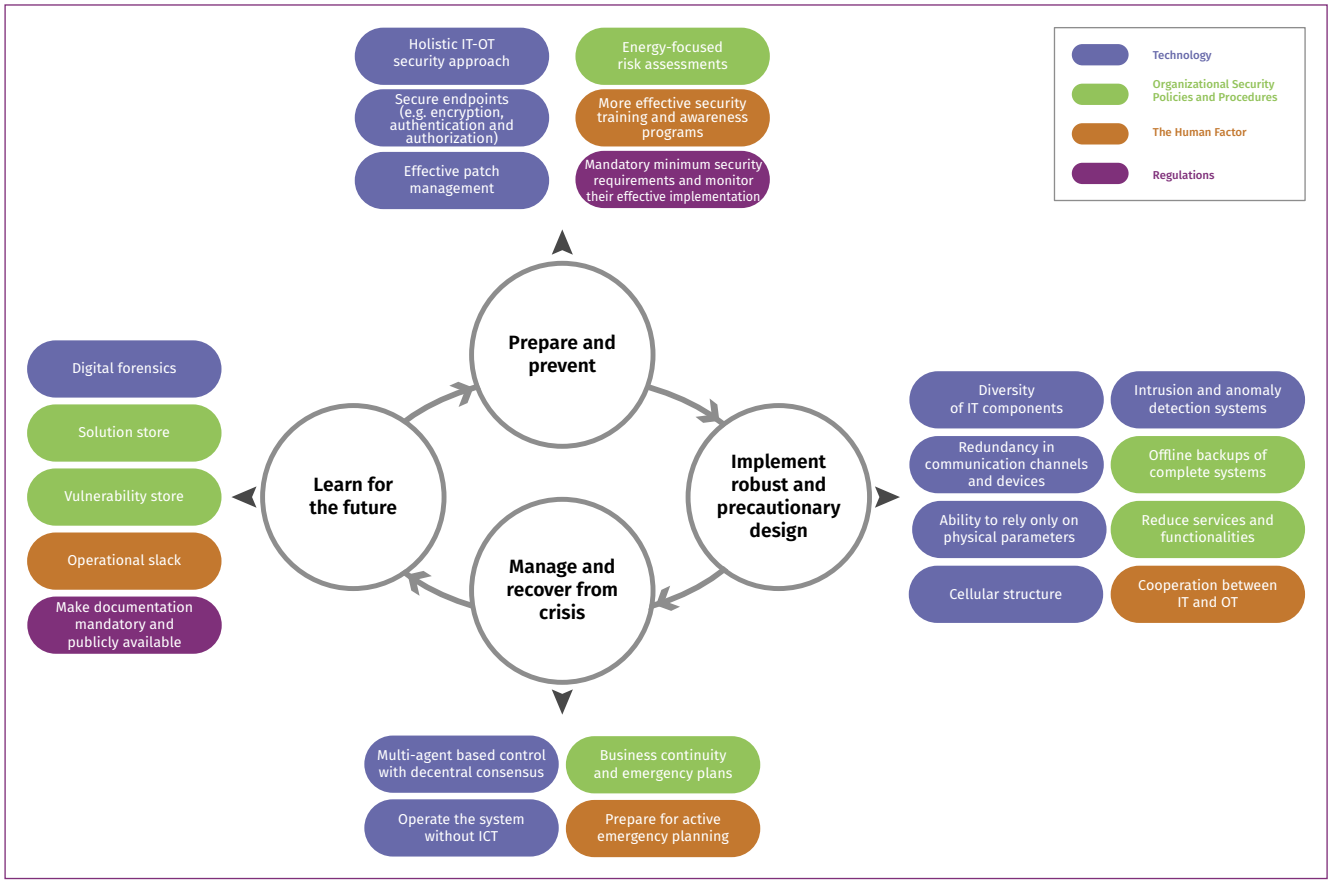


Fig. 4: Selection of resilience-enhancing measures and elements, sorted by the categories: Technology (blue), Organizational Security Policies and Procedures (green), the Human Factor (orange) and Regulations (grey), according to the Resilient Management approach phases.

Source: Authors' own compilation based on Tapia et al. (in press)

Resilience management strategy

The VA unveiled the critical vulnerable points. Security measures, if applied, have great potential to reduce some vulnerabilities. However, they focus mainly on trying to keep the malicious attackers outside of the system. Therefore, one of the biggest challenges is to find a way to broaden the horizon in handling known and unknown stressors by including recovering, adapting and learning mechanism after successful attacks, instead of only focusing on prevention and detection. This is the objective of the second part of the study. Our main concern is how to increase the resilience in CPPS. This requires the understanding that resilience is more than just eliminating identified vulnerabilities. The applied resilience management approach consists of four phases (Fig. 3).

During the **preparation and prevention** phase, weak points in the CPPS are identified and effective prevention measures must be derived. The focus here is on known stressors, thus a holistic security approach between IT-OT (IEC 2016), and energy-focused risk analysis and management strategies (Fischer et al. 2018) are needed. Experts also stressed the importance of scalable and regularly tested security measures at endpoints (e. g. encryption, authentication, authorization), intrusion detection systems, patch management, network segmentation, as well as more effective and engaging security trainings and awareness programs. Technology-wise, the implementation of additional measures for data storage and preserving of unused resources – operational slack – to better deal with surprises are helpful (Fischer and Lehnhoff 2018).

In order to enhance resilience, a **robust and precautionary system design should be implemented** from the beginning. This will empower the system to maintain its services even under stress or disturbances. The system should have a high diversity of IT components and redundancy in communication channels and devices (BNetzA 2019). Maintaining the ability to rely only on physical parameters for operation as well as hardware-based security are helpful. Furthermore, implementing a cellular structure in order to secure a minimum and stable power supply in case of a failing central ICT infrastructure appears beneficial (VDE 2015). Other suggestions supported by the experts are the implementation of real-time monitoring, intrusion and bad data detection schemes (Iturbe et al. 2016; McCarthy

et al. 2018), as well as periodic backups, and reducing services and functionalities in terms of data, ports, libraries, etc. (Fischer and Lehnhoff 2018).

A resilient power system is able to ride through failures in order to **manage and recover from crises.** While the stability and security in this phase could be enhanced by multi-agent based control with decentral consensus finding (Lehnhoff and Krause 2013), attention should also be paid to the ability to operate the system without ICT, i. e. manually, or to at least secure a *soft landing,* as experts stated. In addition, the provision of business continuity and emergency plans on a regional and local level, e. g. through *supplying islands* at least in and around public properties/buildings, and the preparation for active emergency planning and exercises based on realistic cyber-attacks have a high priority (Arghandeh et al. 2016).

Past and avoided disasters should be used in phase four **to learn for the future** in order to improve the adaptive capacity of the system. In this sense, digital forensic would allow to investigate incidents and near incidents in-depth and identify lessons. This should include the documentation of weaknesses that led to failures *(Vulnerability store)* (Gößling-Reisemann 2016). Furthermore, strengths that avoided crises in the past or enhanced recovery are equally worth identifying, as they form the basis for planning strategies and emergency scenarios *(Solution store)* (Gößling-Reisemann 2016). This documentation must be mandatory and publicly available.

Fig. 4 shows the summary of selected resilience-enhancing measures and elements for each phase of the resilience management approach. More details on the specific resilience management strategy described here can be found in Tapia et al. (in press).

Conclusions

In this study, critical properties, structures and elements contributing to the vulnerability of CPPS were identified. On one side, insecure communications or insecure end points, especially at the customer premises, resulted in a high vulnerability due to poor security features on the devices. On the other side, social engineering is a quickly growing security problem that enables threat agents to exploit one of the weaknesses present in every organization: the human factor. In spite of the existence of adaptation mechanisms that could minimize the impact, it was found that their implementation could be hindered by the lack of policy enforcement or the unreadiness of the involved actors to implement these measures. To address cybersecurity challenges, an integrated assessment considering physical, cyber and social perspectives is necessary. The aim is not only to try to keep attackers outside the system, but to design the system in a way that enables it to transform and adapt in order to cope with any kind of stressor. In other words, a resilience management strategy is needed that considers that resilience is more than just eliminating identified vulnerabilities. This article illustrated resilience enhancing measures assigned to the four phases of the resilience management cycle. One important measure is to establish an adequate cyber security regulation framework and monitor its effective implementation. Regarding the system architecture, a cellular structure and physical backup would build resilience in case of successful attacks. We conclude that introducing resilience principles/elements to the system and using a resilience management approach is a suitable way to prepare systems for the unexpected.

Acknowledgments

We acknowledge our beloved supervisor Prof. Dr. Stefan Gößling-Reisemann for his highly valuable insights and contributions during the research project Strom-Resilienz. We are very thankful to Prof. Dr. em. Arnim von Gleich for fruitful discussions and review of this manuscript, to Max Spengler for his support on the interview analysis, to Katja Hessenkämper, Katrina Stollmann and Cécile Pot d'or for proofreading.

Funding declaration

Project funded by the German Federal Ministry of Education and Research within the program Innovation and Technology Analysis, FKZ 16I1678.
http://www.stromresilienz.de

References

Acatech; Deutsche Akademie der Naturforscher Leopoldina e. V.; Akademienunion; Union der deutschen Akademien der Wissenschaften e. V. (2017): Das Energiesystem resilient gestalten. Maßnahmen für eine gesicherte Versorgung. Berlin: Acatech, Leopoldina, Akademienunion.

Arghandeh, Reza; Meier, Alexandra von; Mehrmanesh, Laura; Mili, Lamine (2016): On the definition of cyber-physical resilience in power systems. In: Renewable and Sustainable Energy Reviews 58, pp. 1060–1069.

BNetzA – Bundesnetzagentur (2019): Aktualisierung Sicherheitsanforderungen. Available online at https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/aktualisierung_sicherheitsanforderungen/aktualisierung_sicherheitsanforderungen-node.html, last accessed on 20. 12. 2019.

Bodungen, Clint; Singer, Bryan; Hilt, Stephen; Shbeeb, Aaron; Wilhoit, Kyle (2017): Hacking exposed industrial control systems. ICS and SCADA security secrets and solutions. New York: McGraw-Hill Education.

Brand, Urte et al. (2017): Resiliente Gestaltung des Energiesystems am Beispiel der Transformationsoptionen „EE-Methan-System" und „Regionale Selbstversorgung". Schlussbericht des vom BMBF geförderten Projektes RESYSTRA. Bremen: Universität Bremen. DOI: 10.2314/KXP:1667649884.

Dragos Inc. (2017): Crashoverride. Analyzing the threat to electric grid operations. Available online at https://dragos.com/blog/crashoverride/CrashOverride-01.pdf, last accessed on 21. 01. 2020.

ENISA – The European Network and Information Security Agency (2012): Smart grid security. Security related standards, guidelines and regulatory documents. Available online at https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids/smart-grids-and-smart-metering/smart-grid-security-related-standards-guidelines-and-regulatory-documents/view, last accessed on 21. 01. 2020.

Fischer, Lars; Lehnhoff, Sebastian (2018): IT-Security for functional resilience in energy systems. In: Matthias Ruth and Stefan Goessling-Reisemann (eds.):

Handbook on resilience of socio-technical systems. Croydon: Edward Elgar Publishing Limited, pp. 316–340.

Fischer, Lars; Uslar, Mathias; Morrill, Doug; Döring, Michael; Haesen, Edwin (2018): Study on the evaluation of risks of cyber-incidents and on costs of preventing cyber-incidents in the energy sector. Final Report. Available online at https://ec.europa.eu/energy/sites/ener/files/evaluation_of_risks_of_cyber-incidents_and_on_costs_of_preventing_cyber-incidents_in_the_energy_sector.pdf, last accessed on 21. 01. 2020.

Gleich, Arnim von; Gößling-Reisemann, Stefan; Stührmann, Sönke; Woizeschke, Peer; Lutz-Kunisch, Birgitt (2010): Resilienz als Leitkonzept. Vulnerabilität als analytische Kategorie. In: Klaus Fichter, Arnim von Gleich, Reinhard Pfriem and Bernd Siebenhüner (eds.): Theoretische Grundlagen für erfolgreiche Klimaanpassungsstrategien. Delmenhorst: Projektkonsortium ‚nordwest2050', pp. 13–49.

Goessling-Reisemann, Stefan; Thier, Pablo (2019): On the difference between risk management and resilience management for critical infrastructures. In: Matthias Ruth and Stefan Goessling-Reisemann (eds.): Handbook on resilience of socio-technical systems. Croydon: Edward Elgar Publishing Limited, pp. 117–135.

Gößling-Reisemann, Stefan (2016): Resilience. Preparing energy systems for the unexpected. In: Igor Link and Valentine Florin (eds.): IRGC Resource Guide on Resilience. Lausanne: EPFL International Risk Governance Center.

Gößling-Reisemann, Stefan; Wachsmuth, Jakob; Stührmann, Sönke; Gleich, Arnim von (2013): Climate change and structural vulnerability of a metropolitan energy system. The case of Bremen-Oldenburg in Northwest Germany. In: Journal of Industrial Ecology 17 (6), pp. 846–858.

IEC – International Electrotechnical Commission (2016): Power systems management and associated information exchange. Data and communications security. Part 12: Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems. 1.0. Geneva: IEC.

Iturbe, Mikel; Camacho, Jose; Garitano, Iñaki; Zurutuza, Urko; Uribeetxeberria, Roberto (2016): On the feasibility of distinguishing between process disturbances and intrusions in process control systems using multivariate statistical process control. In: Proceedings of the 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop, pp. 155–160.

Jesse, Bernhard-Johannes; Heinrichs, Heidi; Kuckshinrichs, Wilhelm (2019): Adapting the theory of resilience to energy systems. A review and outlook. In: Energy, Sustainability and Society 9 (1), p. 27. DOI: 10.1186/s13705-019-0210-7.

Lee, Changmin; Zappaterra, Luca; Choi, Kwanghee; Choi, Hyeong-Ah (2014): Securing smart home. Technologies, security challenges, and security requirements. Proceedings of the 2014 IEEE Conference on Communications and Network Security. San Francisco: IEEE, pp. 67–72. DOI: 10.1109/CNS.2014.6997467.

Lehnhoff, Sebastian; Krause, Olav (2013): Agentenbasierte Verteilnetzautomatisierung. In: Peter Göhner (ed.): Agentensysteme in der Automatisierungstechnik. Berlin: Xpert.press Springer-Verlag, pp. 207–223.

Maynard, Peter; Mclaughlin, Kieran; Haberler, Berthold (2014): Towards understanding man-in-the-middle attacks on IEC 60870-5-104 SCADA Networks. Proceedings of the 2nd International Symposium for ICS & SCADA Cyber Security Research, pp. 30–42. Swindon, U. K.: BCS Learning & Development.

Mayring, Philipp (2014): Qualitative content analysis. Theoretical foundation, basic procedures and software solution. Available online at https://nbn-resolving.org/urn:nbn:de:0168-ssoar-395173, last accessed on 21. 01. 2020.

McCarthy, James et al. (2018): Securing manufacturing industrial control systems. Behavioral anomaly detection. NISTIR 8219. Gaithersburg: National Institute of Standards and Technology. Available online at https://www.nccoe.nist.gov/sites/default/files/library/mf-ics-nistir-8219.pdf, last accessed on 21. 01. 2020.

McLaughlin, Kieran; Friedberg, Ivo; Kang, BooJoong; Maynard, Peter; Sezer, Sakir; McWilliams, Gavin (2015): Secure communications in smart grid. Networking and protocols. In: Smart Grid Security Book 2015, pp. 113–148.

NIST – National Institute of Standards and Technology Interagency (2014): Guidelines for smart grid cybersecurity. Vol. 1: Smart Grid cybersecurity strategy, architecture, and high-level requirements. Report 7628 Rev. 1. Gaithersburg: National Institute of Standards and Technology. DOI: 10.6028/NIST.IR.7628r1.

Rossebo, Judith; Wolthuis, Reinder; Fransen, Frank; Bjorkman, Gunnar; Medeiros, Nuno (2017): An enhanced risk-assessment methodology for smart grids. In: Computer 50 (4), pp. 62–71.

Sobczak, Blake (2019): Experts assess damage after first cyberattack on U. S. grid. Security. In: E & E News. Available online at https://www.eenews.net/stories/1060281821, last accessed on 21. 01. 2020.

Styzcynski, Jake; Beach-Westmoreland, Nate (2019): When the lights went out. A comprehensive review of the 2015 attacks on Ukrainian critical infrastructure. n. p.: Booze Allen Hamilton Inc. Available online at https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf, last accessed on 21. 01. 2020.

Tapia, Mariela; Thier, Pablo; Gößling-Reisemann, Stefan (in press): artec Paper No. 222: Vulnerability and resilience of cyber-physical power system. Results from an empirical-based study.

VDE – Verband der Elektrotechnik Elektronik und Informationstechnik (2015): Der Zellulare Ansatz. Grundlage einer erfolgreichen, regionenübergreifenden Energiewende. Frankfurt a. M.: VDE ETG.

MARIELA TAPIA

holds a M. Sc. in Renewable Energy. Since 2016, she is working as research associate in the research group *Resilient Energy Systems* at the University of Bremen. Her research focus is resilient transformation of power supply in developing countries.

PABLO THIER

has a background in experimental physics. Since 2015, he has been working in different projects at the University of Bremen in the research group *Resilient Energy Systems,* where he is developing a framework for making resilient decisions for energy systems.

PROF. DR. RER. NAT. STEFAN GÖßLING-REISEMANN (1968–2018)

was a theoretical physicist. He was the chair of the research group *Resilience Energy System* and the speaker of the *Advanced Energy Systems Institute* at the University of Bremen. His research aimed at solving the substantial problems of this planet. His last projects aimed at designing resilient and sustainable energy systems.

Sichere IT ohne Schwachstellen und Hintertüren

Arnd Weber, *Hexentalstr. 31, 79283 Bollschweil (arnd.weber@alumni.kit.edu)*
Gernot Heiser, *UNSW Sydney (gernot@unsw.edu.au)*
Dirk Kuhlmann, *Fraunhofer-Institut für System- und Innovationsforschung (dirk.kuhlmann@alumni.tu-berlin.de)*
Martin Schallbruch, *Digital Society Institute, European School of Management and Technology (ESMT) (martin.schallbruch@esmt.org)*
Anupam Chattopadhyay, *Nanyang Technical University (anupam@ntu.edu.sg)*
Sylvain Guilley, *Télécom ParisTech (sylvain.guilley@telecom-paristech.fr)*
Michael Kasper, *Fraunhofer Singapore (michael.kasper@fraunhofer.sg)*
Christoph Krauß, *Fraunhofer-Institut für sichere Informationstechnologie (christoph.krauss@sit.fraunhofer.de)*
Philipp S. Krüger, *Digital Hub Cybersecurity (philipp.krueger@alumni.digitalhub-cybersecurity.com)*
Steffen Reith, *Hochschule RheinMain (Steffen.Reith@hs-rm.de)*
Jean-Pierre Seifert, *Technische Universität Berlin (jpseifert@sect.tu-berlin.de)*

Unsere zunehmende Abhängigkeit von Informationstechnik erhöht kontinuierlich die Safety- und Security-Anforderungen bei deren Einsatz. Ein zentrales Problem hierbei sind Schwachstellen von Hard- und Software. Marktkräfte konnten diese Situation bislang nicht grundsätzlich beheben. Eine Gegenstrategie sollte deshalb folgende Optionen erwägen: (1) private und staatliche Förderung offener und sicherer IT-Produktion, (2) Verbesserung der souveränen Kontrolle bei der Produktion aller kritischen IT-Komponenten innerhalb eines Wirtschaftsraumes sowie (3) verbesserte und durchgesetzte Regulierung. Dieser Beitrag analysiert Vor- und Nachteile dieser Optionen. Es wird vorgeschlagen, die Sicherheit der Schlüsselkomponenten einer Lieferkette durch weltweit verteilte, offene und ggf. mathematisch bewiesene Komponenten zu gewährleisten. Der beschriebene Ansatz erlaubt die Nutzung existierender und neuer proprietärer Komponenten.

Secure IT without vulnerabilities and back doors

Increasing dependence on information technology calls for strengthening the requirements on their safety and security. Vulnerabilities that result from flaws in hardware and software are a core problem which market mechanisms have failed to eliminate. A strategy for resolving this issue should consider the following options: (1) private- and public-sector funding for open and secure production, (2) strengthening the sovereign control over the production of critical IT components within an economic zone, and (3) improving and enforcing regulation. This paper analyses the strengths and weaknesses of these options and proposes a globally distributed, secure supply chain based on open and mathematically proved components. The approach supports the integration of legacy and new proprietary components.

https://doi.org/10.14512/tatup.29.1.30
Submitted: 22. 09. 2019. Peer reviewed. Accepted: 08. 01. 2020

Keywords: *cybersecurity, sovereignty, open source, verification, supply chain risks*

Probleme

Die Abhängigkeit der Industriegesellschaft von Informationstechnik führt zu hohen Anforderungen an den sicheren Betrieb dieser Technik – sowohl im Sinne der funktionellen Verlässlichkeit *(Safety)* als auch der IT-Sicherheit im Sinne von Vertrauenswürdigkeit, Integrität, Verfügbarkeit (*confidentiality*, *integrity*, *availability*, CIA). Beide Anforderungen können, insbesondere in Kombination, durch derzeit produzierte IT-Systeme nur bedingt sichergestellt werden. Infolgedessen können Infrastrukturen ausfallen, Betriebsgeheimnisse entwendet, Autos ferngesteuert, Vermögensschäden verursacht und politische Institutionen ausgespäht werden (Weber et al. 2018 a, 2018 b).

Wesentliche Ursache für die Angriffsmöglichkeiten sind vielfältige Schwächen in Hard- und Software. Sie beginnen bei einfachen Fehlern in der Anwendungssoftware wie etwa dem *Heartbleed-Bug* innerhalb einer Komponente, die zur Verschlüsselung im World Wide Web genutzt wurde. Sie setzen sich fort in Angriffen wie durch die Erpressersoftware *WannaCry*, die den Geheimdiensten bekannte, aber nicht beseitigte Schwächen in Betriebssystemen ausnutzte. Neueren Datums sind Hardware-Trojaner (Becker et al. 2014), deren Existenz in elektronischen Halbleiterbauelementen, z. B. FPGA-Chips, und militärischen Radaranlagen in Syrien bereits behauptet wurde. Von zunehmender Bedeutung ist auch die Möglichkeit von Angriffen auf IT-Lieferketten (Huang 2019).

Eine substanzielle Verbesserung der Situation im Bereich IT-Sicherheit konnte in den letzten Jahren nicht erreicht werden, wie die Statistik der *Computer Vulnerabilities and Expo-*

sures zeigt (MITRE 2019). Spätestens seit den Snowden-Veröffentlichungen im Jahr 2013 muss davon ausgegangen werden, dass nationale Nachrichtendienste Schwachstellen gezielt herstellen oder ankaufen (Abb. 1). Offenkundig betrifft dies nicht nur die Dienste der USA: Auch Russland ist stark im *Cyberspace* aktiv, gleiches gilt für China. Offiziere der chinesischen Volksbefreiungsarmee haben bereits vor zwei Jahrzehnten die Herstellung „logischer Bomben" für Computernetzwerke vorgeschlagen (Liang und Wang 1999). Die aus strategischer Motivation geheim gehaltenen Hintertüren können unter Umständen von Kriminellen ausgenutzt werden, wie das Beispiel *WannaCry* belegt.

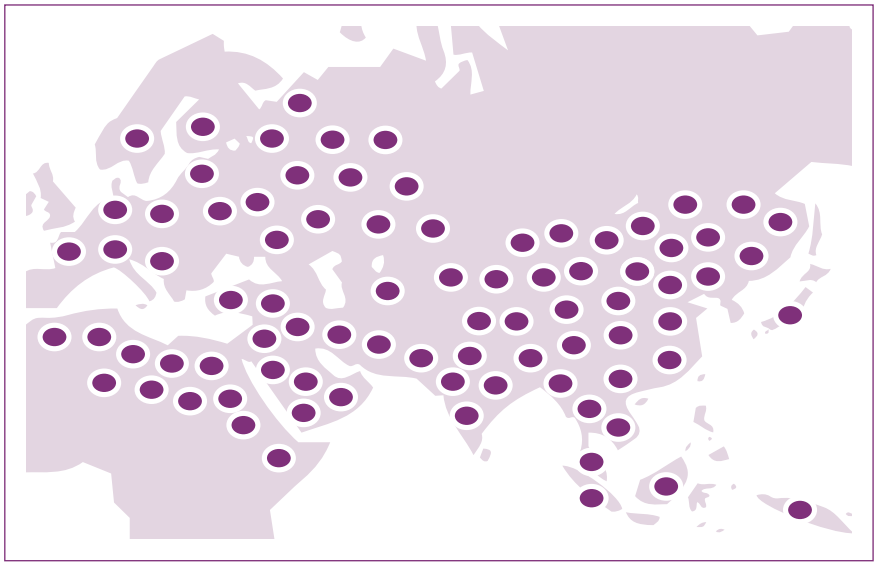


Abb. 1: Von der US-amerikanischen National Security Agency (NSA) kompromittierte Computer. Jeder Punkt repräsentiert > 500 Geräte. Der Whistleblower Edward Snowden veröffentlichte, dass z. B. Maschinen von HP, Dell und Cisco unterminiert und die Firmen Belgacom und Gemalto gehackt wurden.
Quelle: Angepasster Ausschnitt aus Snowden 2013

Nahezu täglich werden neue Schwachstellen entdeckt, die von Fehlern in der Programmierung bis zu ausnutzbaren Seiteneffekten spekulativer Programmausführung in der Hardware reichen (*Spectre* und *Meltdown*). Inzwischen muss selbst die Möglichkeit einer aktiven Einschleusung von Schwachstellen durch die verwendeten Entwicklungswerkzeuge in Erwägung gezogen werden. Die meisten Komponenten für Computer, einschließlich Softwaremodule und Chips, werden inzwischen in einer komplexen weltweiten Arbeitsteilung erstellt. Dabei sind viele Details der Implementierungen selbst für große industrielle Kunden intransparent. Dies gilt für integrierte komplexe Softwaremodule ebenso wie für einzelne Hardwarekomponenten. Daraus ergeben sich vielfältige Angriffsmöglichkeiten (Weber et al. 2018 a).

Zertifizierungen haben bislang lediglich begrenzte Aussagekraft für die IT-Sicherheit.

Angesichts der Abhängigkeit von digitalen Systemen und den Auseinandersetzungen im Cyberraum erscheint es unzureichend, das Risiko von schwerwiegenden Sicherheitsverletzungen ausschließlich mit Methoden des Risikomanagements und inkrementellen Updates anzugehen (Odlyzko 2019). In Ergänzung hierzu ist es erforderlich, einen grundlegenden Wandel in die Wege zu leiten, der informationstechnische Sicherheit mittels ökonomisch vertretbarer Verfahren fundamental verbessert und zwar unter Berücksichtigung der weltweit steigenden Konzentration von Kompetenzen und Wertschöpfung (Müller-Quade et al. 2017).

Entwicklungsoptionen

Die grundsätzliche Vermeidung von Schwachstellen in Hardware und Software wird im Allgemeinen als nahezu unlösbares Problem angesehen. So wird geltend gemacht, Soft- und Hardware seien zu kompliziert, verifizierte Lösungen teuer und unflexibel und hundertprozentige Sicherheit ohnehin nicht erreichbar. Obwohl aus empirischer und historischer Sicht einiges für diese Einschätzungen spricht, bleibt es Aufgabe der Forschung, die Prämissen dieser Argumente zu ermitteln, sie infrage zu stellen und nach realisierbaren Ansätzen zu suchen.

Herkömmliche Ansätze wie umfangreicheres Testen und *Patching* haben sich bisher als nicht ausreichend erwiesen (Weber et al. 2018 a). So helfen gegen mögliche Systemschwächen und durch finanzstarke Akteure gesponserte Angriffe graduelle Verbesserungen, wie Updates oder neue Systemschichten, bestenfalls graduell. Auch zusätzliche eingeführte Kontrollkomponenten bieten nur begrenzte Möglichkeiten, weil sie ihrerseits für Angriffe ausgenutzt oder umgangen werden können und zudem selbst mit unterminierten Werkzeugen entwickelt worden sein könnten.

Auf europäischer Ebene wird derzeit diskutiert, ob IT-Sicherheit durch Regulierung der Hard- und Software verbessert werden kann, etwa indem Zertifizierungen nach den *Common Criteria* oder dem *EU Cybersecurity Act* von 2019 vorgeschrieben werden. Derartige Zertifizierungen haben bislang lediglich begrenzte Aussagekraft, zumal bestehende Verfahren die Korrektheit der Implementierung meist nur mit Tests prüfen. Selbst wenn alle zertifizierten Software-Komponenten bewiesenermaßen sicher wären, besteht die Frage nach möglichen Hard-

ware-Schwächen fort, etwa wenn das Design oder der Produktionsprozess geändert wird. Überprüfungen werden z. B. dort kompliziert, wo Hardware-Hersteller Teile des Designs geheim halten, um Angriffe zu erschweren oder sie durch Prozessfestlegungen dazu verpflichtet sind. Hierdurch wird die Sicherheit tendenziell reduziert, da diese Komponenten nicht unabhängig nachprüfbar sind (Saltzer und Schroeder 1975; Eurosmart 2014). Ein Kunde kann ein solches Produkt nicht selbst beurteilen. Hinzu kommt, dass die Durchführung der anspruchsvolleren Zertifizierungsstufen sehr kostenintensiv ist.

Ehrgeiziger sind Versuche, die Kontrolle der IT Produktion auf nationaler Ebene sicherzustellen und kritische Systeme ausschließlich im Inland zu produzieren. So verfügt z. B. China über Durchgriffsmöglichkeiten, mit denen im Prinzip die gesamte Wertschöpfungskette kontrolliert werden kann. Vollständige Autonomie ist bei IT-Systemen allerdings schwer zu erreichen, sobald Hersteller für den Weltmarkt produzieren und Komponenten anderer Anbieter beziehen, deren Designfehler oder absichtlich eingefügte Hintertüren jedes IT-System beeinflussen können, in das sie verbaut sind.

Eine Herausforderung für die Forschung besteht darin, Verfahren zu entwickeln, die komplexere Systeme kostengünstig verifizieren können.

Option offene, verifizierte Lieferketten

Der im Folgenden vorgestellte Ansatz kombiniert offene Produktion, verifizierte Hard- und Software und sichere Lieferketten. Wir schlagen vor, offene Produktionsverfahren über die gesamte Lieferkette einzuführen, die Inputs und Werkzeuge ebenso wie die Produkte selbst umfasst. Hierzu ist zunächst die Schlüsselfrage zu beantworten: Wie können Schwächen und Hintertüren tatsächlich eliminiert werden? Danach ist zu fragen, wie der Ansatz zu finanzieren und mit der privatwirtschaftlichen Amortisation von Entwicklungsaufwänden für neue Produkte vereinbaren wäre.

Offenheit

Aus Sicherheitsperspektive haben offene Systeme einige grundsätzliche Vorteile gegenüber vertraulichen Systemen. So konstatiert das US Department of Defence im Rahmen einer Ausschreibung für Projekte zur Cybersicherheit: „Current commodity computer hardware and software are proprietary. A thorough security review cannot be performed on systems with undisclosed components." (SBIR 2018) Beispiele für offene Systeme sind das Betriebssystem Linux und das davon abgeleitete Android, die sich erfolgreich am Markt etabliert haben. Eine ähnliche Entwicklung könnte sich im Hardware-Bereich hinsichtlich des RISC-V Prozessor-Designs anbahnen. Diese offene Prozessorarchitektur, die an der Universität Berkeley unter Förderung durch die Defense Advanced Research Projects Agency (DARPA) und in Kooperation mit der Industrie entwickelt wurde, ermöglicht freie Inspektion und lizenzkostenfreie Weiterentwicklung.

Open source ist per se nicht mit Fehlerfreiheit gleichzusetzen. Dies belegt z. B. der bereits angesprochene *Heartbleed-Bug,* der auf einem jahrelang unentdeckten Implementierungsfehler beruhte. Hier sind Verbesserungen bei der Kontrolle von Spezifikationen und Designs etwa durch Intensivierung automatischer statischer und dynamischer Analyse von Programmen und Testen durch unabhängig arbeitende Gruppen denkbar (Kiss et al. 2015). Durch diesen Mehraufwand könnte die Sicherheit von Open-Source-Komponenten erheblich verbessert werden, doch intensiveres Testen allein kann nie ausschließen, dass unentdeckte Fehler verbleiben.

Formale Verifikation

Gegen unentdeckte Schwächen können offene Systeme Abhilfe schaffen, deren korrektes Funktionieren in Bezug auf Vertraulichkeit und Integrität der verarbeiteten Nutzerdaten mathematisch bewiesen ist („formal verifiziert"). Ein Vorreiter bei der praktischen Realisierung solcher Systeme ist *seL4,* ein Mitglied der L4-Familie von Betriebssystem-Mikrokernen (Klein et al. 2014, vgl. Abb. 2).

Ausgelöst vom Gleitkomma-Divisions-Fehler in Intel-Prozessoren im Jahr 1994 wird seit Jahrzehnten eine formale Verifikation von Teilen der CPU-Designs durchgeführt. Entsprechende Bestrebungen existieren zur Überprüfung kompletter RISC-V Prozessoren (Chlipala 2017). Die zugrundeliegenden formalen Spezifikationen und Beweise sind jedoch aufwändig und verlieren i. d. R. ihre Gültigkeit, sobald am verifizierten Objekt auch nur geringfügige Änderungen vorgenommen werden.

Eine Herausforderung für die Forschung besteht deshalb darin, Verfahren zu entwickeln, die komplexere Systeme kostengünstig verifizieren können. Die Schwierigkeiten für Korrektheitsbeweise komplexer Prozessoren steigen mit der Anzahl der Transistoren, Prozessorkerne, etc. jedoch stark an. Bislang ist unklar, ob man angesichts der wachsenden Integrationsdichte und Transistoranzahl der neuesten Prozessorgenerationen deren Design je zu vertretbaren Kosten beweisen können wird oder ob der Beweisaufwand durch grundsätzliche Änderungen des CPU- und Rechnerdesigns radikal gesenkt werden kann.

Abb. 2: Diese Entwicklungen zeigen beispielhaft, dass die neuen Ansätze in der Forschung, in Prototypen und in Produkten angewendet werden. *(V. l. n. r.:)* [1] Apples A11-Chip mit Secure Element, in dem der L4 Betriebssystemkern verwendet wird; [2] Unbemannter Boeing Hubschrauber kontrolliert durch das offene, bewiesene seL4; [3] Sicherheitsmodul mit dem offenen LEON-SPARC-v8-Prozessor; [4] Prototyp eines offenen Sicherheitsmoduls mit dem offenen VexRiscv Prozessor, mit einem Hardwarebeschleuniger für die ChaCha Stromverschlüsselung, ausschließlich mit offenen Entwurfswerkzeugen erstellt (auf einem FPGA-Chip laufend). *Quellen: [1] Wikipedia (2020); [2] Data61 (2020); [3] Sylvain Guilley, Secure-IC; [4] Steffen Reith*

Sicherung der Lieferkette

Die Lieferkette für IT kann an nahezu jedem Punkt erfolgreich angegriffen werden – Modifikation des Designs und Beeinflussung des Produktionsprozesses sind ebenso möglich wie die Subversion von Test- und Validierungsverfahren oder Austausch von Systemelementen während der Auslieferung. Es ist damit zu rechnen, dass die Sicherung einiger Komponenten, wie etwa Betriebssysteme oder Prozessoren, dazu führt, dass andere Komponenten angegriffen werden, z. B. Kommunikationschips oder verwendete Softwarewerkzeuge. Ein umfassender Ansatz hätte demzufolge möglichst große Teile dieser Kette zu sichern. Dort, wo auf geschlossene, nicht verifizierte Anwendungen, z. B. traditionelle Betriebssysteme, zurückgegriffen werden muss, sollten diese durch Mechanismen gekapselt werden, die sie vom vertrauenswürdigen Teil des Systems trennen.

Eine zentrale Herausforderung betrifft die Sicherung der Produktion der Halbleiter in den *Fabs* genannten Produktionsanlagen. Diese erfordern Milliardeninvestitionen und sind, neben den USA und Israel, auf wenige fernöstliche Länder konzentriert. Eine Strategie zur besseren Absicherung der Chip-Produktion kann sich unter anderem folgender Optionen bedienen:

- Lokale Fertigung durch als vertrauenswürdig betrachtete Betreiber und Mitarbeiter (*Trusted Fab*), eventuell auf eine Reihe kritischer Schritte am Schluss der Fertigung beschränkt (Sengupta et al. 2019).
- Kontrolle der Chips durch mathematische Verfahren, wie Verschlüsselung (Šišejković et al. 2019) oder zusätzliche Leiterbahnen (Seifert und Bayer 2015).
- Stichprobenartige Inspektion von Chips durch optische Prüfung. Aus praktischer Sicht funktioniert dies am besten bei einfachen Chips mit vergleichsweise großen Strukturen, deren Herstellung für Enthusiasten aus dem Open-Source-Umfeld machbar ist, wie durch das *Libre Silicon*-Projekt angestrebt (Libre Silicon 2020).

Die genannten Optionen müssen teils erst noch entwickelt und erprobt werden. Gleiches gilt für Ansätze zur Absicherung von Softwarewerkzeugen, die in der Herstellung von Hard- oder Software verwendet werden. Die drei zu untersuchenden Hauptoptionen sind hier:

- entweder ein offenes System von Werkzeugen zu schaffen und durch intensive Überprüfung die Gefahr von Schwachstellen oder Hintertüren zu minimieren
- oder den Output eines offenen Werkzeugs formal zu verifizieren
- oder den Output mit jenen proprietärer Werkzeuge auf funktionale Äquivalenz zu vergleichen.

Natürlich muss in allen Fällen die Integrität der Prüfumgebung sichergestellt werden, was evtl. nur langfristig geschehen kann. Der Vollständigkeit halber sei noch darauf hingewiesen, dass die Mathematik dabei helfen kann, die Authentizität von Chips sicherzustellen, z. B. durch Verwendung von *physically unclonable functions,* die physikalische Implementierungscharakteristika nutzen (Bruneau et al. 2019).

Kosten

Ein wichtiger Faktor für die Realisierung eines offenen Ansatzes ist die Finanzierbarkeit. Derzeit kommen die vorgeschlagenen formalen Verfahren aus Aufwandsgründen zumeist nicht in Betracht. Die Open-Source-Community beispielsweise setzt derzeit selten Instrumente zur formalen Spezifikation oder Verifikation ein. Einerseits wird dies als zu aufwändig angesehen, andererseits schränkt eine formal orientierte Vorgehensweise die Flexibilität bei der Weiterentwicklung erheblich ein. Es besteht also Forschungs- und Handlungsbedarf, um formale Beweise leichter und kostengünstiger durchführen zu können.

Die Stückkosten für formal verifizierte, offene Komponenten könnten verringert werden, wenn man höhere Losgrößen erreicht, die Entwicklungskosten global auf die Forschungsetats mehrerer Länder und Unternehmen verteilt, dem Beispiel der Kooperation von US-Firmen mit der DARPA folgend, und geringere Lizenzkosten als für proprietäre Tools einbezieht. Durch formal verifizierte Systeme entstehen zudem niedrigere Kosten für Sicherheitsmaßnahmen und für Schadensbehebung. Zudem könnten solche Komponenten wegen der hohen Qualität einen

Vorteil im Wettbewerb darstellen und regulatorischen Anforderungen leichter gerecht werden. Eine belastbare Schätzung der Kosten ist wegen der Vielzahl von Variablen derzeit schwer möglich.

Stand des Übergangs zu offenen, bewiesenen Systemen

Eine strategische Initiative für offene, formal bewiesene Komponenten und Systeme könnte auf einer Reihe von Vorarbeiten aufbauen, die seit längerem u. a. von der DARPA gefördert werden. Angesichts der wachsenden Abhängigkeit der US-amerikanischen IT-Wirtschaft von internationalen IT-Zulieferern folgerte die Agentur bereits 2017: „The Open-Source community needs to develop a complete infrastructure" (Salmon 2017, S. 9). Inzwischen hat auch die Industrie in den USA, Asien und Europa begonnen, sich intensiver mit dieser Thematik auseinanderzusetzen und bspw. hochleistungsfähige Multicore-CPUs auf RISC-V Basis zu entwickeln oder auf Softwareseite auf das verifizierte Mikrokernel-Betriebssystem seL4 zurückzugreifen (Sauter 2019; Hettinga 2019; hartpunkt.de 2018).

Durch diese Initiativen werden bereits heute öffentliche und private Gelder in Beweis-basierte, offene Architekturen investiert, die etwa im Bereich von Grafikkarten, Speichermedien oder eingebetteten Systemen zur Anwendung kommen sollen. Wie im Falle von Linux/Android in der Vergangenheit bereits beobachtbar, kann eine solche Entwicklung bewirken, dass sich der Einsatz derartiger Systeme von ihren ursprünglichen Einsatzfeldern (hochsichere Anwendungen, wie Luftfahrt, Verteidigung und IT-Sicherheitsmodule) auf andere Geräteklassen ausweitet.

Fazit zur globalen Implementierung offener Verifizierung

Im Sinne eines *constructive technology assessment* lassen sich Risiken für den deutschen, europäischen und letztlich globalen Raum nur dann substanziell verringern, wenn Mechanismen entwickelt werden, die die Anzahl von Schwachstellen, Fehlern und Hintertüren nachweislich reduzieren, idealerweise auf null: *Secure IT* statt *IT security*. Eine beträchtliche Zahl technischer Grundlagen für die Entwicklung offener, verifizierter Systeme ist bereits gelegt. Um diesen Ansatz jedoch systematisch auszubauen, bedarf es erheblicher Investitionsmittel. Nötig wären hier forschungs- und industriepolitische Programme zur Frage, wie komplette Wertschöpfungsketten von IT-Systemen offen und sicher gestaltet und verbreitet werden können. In den USA hat die DARPA hierzu einen Investitions- und Forschungsplan entwickelt (*Electronic Resurgence Initiative)*, der die lokale, sichere Produktion von IT-Komponenten zum Ziel hat. Dieser ist jedoch stark auf den militärischen Bereich fokussiert und bezieht US-Hersteller mit vertraulichen Produkten und Prozessen ein. Für den zivilen Bereich, gerade auch außerhalb der USA, sind folgende Programmelemente vonnöten:

1. Initiierung von Pilotprojekten und Prototypen, die die gesamte Wertschöpfungskette umfassen,
2. Weiterentwicklung und *Tooling* von Methoden der formalen Verifikation mit dem Ziel leichterer Anwendbarkeit sowie Ausweitung der Forschung zur formalen Analyse auf komplexere Systeme,
3. Techniken zur redundanten formalen Verifizierung durch geografisch verteilte, unabhängig arbeitende Teams, insbesondere zur Aufgabenverteilung und Zusammenführung der Ergebnisse,
4. Untersuchung von Techniken zur Zertifizierung, die nicht auf der Vertraulichkeit der Produktion und der Verifizierungstechniken beruhen,
5. Training einer ausreichenden Anzahl von fachlich qualifiziertem Personal sowie
6. Entwicklung und Erprobung von Methoden zur Kontrolle geografisch entfernter *Fabs* und weltweiter Lieferwege.

Parallel hierzu müssten Geschäftsmodelle mit dem Ziel erarbeitet werden, die anfänglichen Kosten möglichst global zu verteilen. Ähnlich der Förderung von RISC-V wäre hier eine Kostenteilung zwischen privaten und öffentlichen Trägern naheliegend. Preiswerte, verifizierte Werkzeuge und Komponenten könnten Innovationen in vielen Branchen erleichtern und für viele Länder die „Souveränität" im IT-Bereich stärken.

Ferner sollte untersucht werden, ob und wie eine derartige Zielstellung effizient durch politische oder durch regulatorische Maßnahmen flankiert werden sollte. Die Koordination des beschriebenen Vorhabens könnte dabei in Deutschland z. B. durch zwei in neuerer Zeit gegründete Regierungsinstitutionen gefördert werden: die Agentur für Innovation in der Cybersicherheit und die Agentur zur Förderung von Sprunginnovationen.

Das Ziel „Secure IT" statt „IT security" lässt sich nur erreichen, wenn die Anzahl von Schwachstellen, Fehlern und Hintertüren idealerweise auf null reduziert wird.

Der vorgeschlagene Ansatz hat die Absicherung der gesamten Produktions- und Lieferkette zum Ziel und erfordert deshalb abgestimmte Anstrengungen über eine Vielzahl von Arbeitsgebieten. Die Komplexität eines solchen Vorhabens dürfte jener der derzeitigen Pilot-Initiativen zur Etablierung europäischer *Cyber Competence Networks* nicht nachstehen. Deren Finanzierungsrahmen liegt zwischen 10 und 20 Millionen Euro und ein entsprechender Aufwand sollte auch für die Entwicklung eines technischen und organisatorischen Rahmens veranschlagt

werden. Echte Produktentwicklung für den zivilen Bereich würden allerdings deutlich höhere Aufwendungen erfordern (die DARPA hat hierfür derzeit für fünf Jahre ca. US-$ 1,5 Mrd. eingeplant). Die Umsetzung würde ein umfangreiches Public-Private-Partnership-Programm mit vielen Akteuren oder auch den Aufbau eines nationalen oder europäischen „Champions" unter Mobilisierung von Risikokapital erfordern, ggf. in Kooperation mit Akteuren aus anderen Ländern.

Aus politischer und ökonomischer Perspektive sollten parallele und alternative Entwicklungen auf globaler Ebene beobachtet und deren Ansätze und Risiken weiter analysiert werden. Hierzu gehören etwa Versuche, Lieferketten auf rein nationaler Ebene zu etablieren (USA, China, Indien) oder die Entwicklung und der Einsatz offener, aber bislang unbewiesener Hardware-Komponenten durch etablierte IT-Unternehmen.

Danksagung

Die Autoren danken G. Müller-Datz und A. Saffari für die Begutachtung sowie Vertretern US-amerikanischer und deutscher Unternehmen für Anregungen.

Literatur

Becker, Georg; Regazzoni, Francesco; Paar, Christof; Burleson, Wayne (2014): Stealthy dopant-level hardware Trojans. Extended version. In: Journal of Cryptographic Engineering 1 (4), S. 19–31.

Bruneau, Nicolas et al. (2019): Development of the unified security requirements of PUFs during the standardization process. In: Jean-Louis Lanet und Cristian Toma (Hg.): Innovative Security Solutions for Information Technology and Communications. Cham: Springer, S. 314–330.

Chlipala, Adam (2017): Coming soon. Machine-checked mathematical proofs in everyday software and hardware development. Chaos Communication Congress. Leipzig, Deutschland, 27.–30. 12. 2017. Online verfügbar unter https://events.ccc.de/congress/2017/Fahrplan/events/9105.html, zuletzt geprüft am 06. 11. 2019.

Data61 (2020): The HACMS project @ Data61. Online verfügbar unter https://ts.data61.csiro.au/projects/TS/SMACCM/, zuletzt geprüft am 08. 01. 2020.

Eurosmart – European Smart Card Association (2014): Security IC platform protection profile with augmentation packages. Version 1.0. Online verfügbar unter https://www.commoncriteriaportal.org/files/ppfiles/pp0084b_pdf.pdf, zuletzt geprüft am 06. 11. 2019.

hartpunkt.de (2018): Hensoldt kooperiert mit CSIROs Data61. Online verfügbar unter https://www.hartpunkt.de/hensoldt-kooperiert-mit-csiros-data61/, zuletzt geprüft am 08. 01. 2020

Hettinga, Wisse (2019): Sixteen core RISC-V processor Xuan Tie 910. Alibaba. In: EENewsEurope, 25. 07. 2019. Online verfügbar unter https://www.eenewseurope.com/news/sixteen-core-risc-v-processor-xuan-tie-910-alibaba, zuletzt geprüft am 06. 11. 2019.

Huang, Andrew (2019): Supply chain security. „If I were a Nation State". BlueHat IL 2019. Israel, Tel Aviv, 06.–07. 02. 2019. Online verfügbar unter https://www.youtube.com/watch?v=RqQhWitJ1As&list=UUp892CjX6wps88JivisRMtA&index=6&t=0s, zuletzt geprüft am 21. 01. 2020.

Kiss, Balázs; Kosmatov, Nikolai; Pariente, Dillon; Puccetti, Armand (2015): Combining static and dynamic analyses for vulnerability detection. Illustration on Heartbleed. In: Nir, Piterman (Hg.): Hardware and software. Verification and testing. Cham: Springer, S. 39–50.

Klein, Gerwin et al. (2014): Comprehensive formal verification of an OS microkernel. In: ACM Transactions on Computer Systems 32 (1), S. 2:1–2:70.

Liang, Qiao; Wang, Xiangsui (1999): Unrestricted warfare. Beijing: PLA Literature and Arts Publishing House. Online verfügbar unter https://www.oodaloop.com/documents/unrestricted.pdf, zuletzt geprüft am 06. 11. 2019.

Libre Silicon (2020): Libre Silicon. Free semiconductors for everyone. Online verfügbar unter https://libresilicon.com/, zuletzt geprüft am 08. 01. 2020.

MITRE (2019): CVE Details. Online verfügbar unter https://www.cvedetails.com/browse-by-date.php, zuletzt geprüft am 06. 11. 2019.

Müller-Quade, Jörn; Reussner, Ralf; Beyerer, Jürgen (2017): Karlsruher Thesen zur Digitalen Souveränität Europas. Online verfügbar unter https://www.fzi.de/fileadmin/user_upload/PDF/2017-10-30_KA-Thesen-Digitale-Souveraenitaet-Europas_Web.pdf, zuletzt geprüft am 21. 01. 2020.

Odlyzko, Andrew (2019): Cybersecurity is not very important. In: Ubiquity, Issue June, S. 1–23. DOI: 10.1145/3333611.

Salmon, Linton (2017): A perspective on the role of open-source IP in government electronic systems. 7th RISC-V Workshop. Milpitas, USA, 28.–30. 11. 2017. Online verfügbar unter https://content.riscv.org/wp-content/uploads/2017/12/Wed-1042-RISCV-Open-Source-LintonSalmon.pdf, zuletzt geprüft am 21. 01. 2020.

Saltzer, Jerome; Schroeder, Michael (1975): The protection of information in computer systems. In: Proceedings of the IEEE 63 (19), S. 1278–1308.

Sauter, Marc (2019): Wieso RISC-V sich durchsetzen wird. In: golem.de, 17. 10. 2019. Online verfügbar unter https://www.golem.de/news/offene-prozessor-isa-wieso-risc-v-sich-durchsetzen-wird-1910-141978.html, zuletzt geprüft am 21. 01. 2020

SBIR – The Small Business Innovation Research Program (2018): Open source high assurance system. Online verfügbar unter https://www.sbir.gov/sbirsearch/detail/1508741, zuletzt geprüft am 06. 11. 2019.

Seifert, Jean-Pierre; Bayer, Christoph (2015): Trojan-resilient circuits. In: Al-Sakib Pathan (Hg.): Securing cyber-physical systems. Boca Raton: CRC Press, S. 349–370.

Sengupta, Abhrajit; Nabeel, Mohammed; Knechtel, Johann; Sinanoglu, Ozgur (2019): A new paradigm in split manufacturing. Lock the FEOL, unlock at the BEOL. In: Proceedings der Design, Automation & Test in Europe Conference & Exhibition 2019.

Šišejković, Dominik; Merchant, Farhad; Leupers, Rainer; Ascheid, Gerd; Kegreiss, Sascha (2019): Control-lock. Securing processor cores against software-controlled hardware Trojans. In: Proceedings des ACM Great Lakes Symposium on VLSI, S. 27–32.

Snowden, Edward (2013): Worldwide SIGINT. Online verfügbar unter https://edwardsnowden.com/wp-content/uploads/2013/11/nsa1024.jpg, zuletzt geprüft am 21. 01. 2020.

Weber, Arnd; Reith, Steffen; Kasper, Michael; Kuhlmann, Dirk; Seifert, Jean-Pierre; Krauß, Christoph (2018 a): Sovereignty in information technology. Security, safety and fair market access by openness and control of the supply chain. Karlsruhe: KIT-ITAS. Online verfügbar unter http://www.itas.kit.edu/pub/v/2018/weua18a.pdf, zuletzt geprüft am 21. 01. 2020.

Weber, Arnd; Reith, Steffen; Kasper, Michael; Kuhlmann, Dirk; Seifert, Jean-Pierre; Krauß, Christoph (2018 b): Open source value chains for addressing security issues efficiently. In: Proceedings der IEEE International Conference on Software Quality, Reliability and Security Companion 2018, S. 599–606.

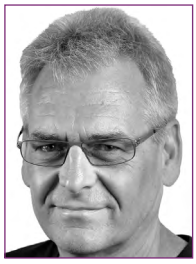
Wikipedia (2020): Apple A11 Bionic. Online verfügbar unter https://de.wikipedia.org/wiki/Apple_A11_Bionic, zuletzt geprüft am 21. 01. 2020.

PROF. DR.-ING. ANUPAM CHATTOPADHYAY

lehrt am SCSE, Nanyang Technical University, Singapur. An der RWTH Aachen arbeitete er an Chiparchitekturen, an EDA sowie an der Automatisierung der Spezifikation von Chips (RTL).

PROF. DR.-ING. SYLVAIN GUILLEY

ist CTO von Secure-IC, Frankreich, sowie Professor an Télécom-ParisTech, Mitarbeiter der École Normale Supérieure (ENS), Außerordentlicher Professor an der Chinesischen Akademie der Wissenschaften sowie Herausgeber von Standards wie ISO/IEC 20897 (Physically Unclonable Functions).



PROF. DR. GERNOT HEISER

ist leitender Forscher bei CSIRO's Data61 und Scientia Professor an UNSW Sydney (John Lions Chair of Operating Systems). Er war Gründer der Open Kernel Labs, deren L4 Kern u. a. in der Secure Enclave aller iOS-Geräte läuft. Er ist Chief Scientist (Software) bei HENSOLDT Cyber und Fellow der ACM, der IEEE und der australischen Akademie der Technischen Wissenschaften.

MICHAEL KASPER

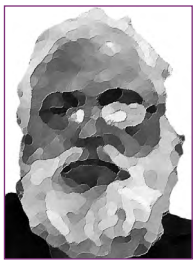
leitet die Arbeitsgruppe „Cyber- und Information Security" bei Fraunhofer Singapore und Mitbegründer von opentrust.ai in Singapur. Er ist assoziierter Senior Researcher beim Fraunhofer-Institut für Sichere Informationstechnologie (SIT).

PROF. DR. CHRISTOPH KRAUSS

leitet am Fraunhofer-Institut für Sichere Informationstechnologie (SIT), Darmstadt, die Abteilung Cyber-Physical Systems Security und ist verantwortlich für das Geschäftsfeld Automotive Security. Weiterhin ist er Professor für das Fachgebiet Netzwerksicherheit an der Hochschule Darmstadt.

PHILIPP S. KRÜGER

ist Managing Director von Accenture Security für Deutschland, Schweiz, Österreich und Russland. Er ist Mitbegründer der Digital Hub Cybersecurity, war Berater des Verteidigungsministeriums für Cyberspace und Innovation und ist Leiter der Agile Cyber Deterrence Group des Instituts für Sicherheitspolitik an der Universität Kiel.



DIRK KUHLMANN

ist Senior Researcher am Fraunhofer-Institut für System- und Innovationsforschung (ISI), Karlsruhe. Von 1995 bis 2017 arbeitete er für die Hewlett Packard Laboratories in Bristol in der Forschungsgruppe für IT-Sicherheit mit Schwerpunkt Open-Source-Software.

PROF. DR. STEFFEN REITH

ist Professor für Theoretische Informatik an der Hochschule RheinMain in Wiesbaden. Während seiner Tätigkeit bei Elektrobit Automotive hat er Produkte mit kryptografischen Funktionen für den Serieneinsatz in aktuellen Automobilen entwickelt.

MARTIN SCHALLBRUCH

ist stellvertretender Direktor des Digital Society Institute (DSI) und Senior Researcher an der European School of Management and Technology (ESMT) in Berlin. Gleichzeitig ist er Lehrbeauftragter am Karlsruher Institut für Technologie. Im Bundesinnenministerium war er zuletzt Leiter der Abteilung für Informationstechnik, Digitale Gesellschaft und Cybersicherheit.

PROF. DR. JEAN-PIERRE SEIFERT

ist Einstein Professor für das Fachgebiet „Security in Telecommunications" an der TU Berlin und den Telekom Innovation Laboratories. Er hat u. a. bei Infineon, Intel und Samsung geforscht.

DR. ARND WEBER

ist Volkswirt und Soziologe. Bis zu seiner Pensionierung war er Senior Researcher beim Institut für Technikfolgenabschätzung und Systemanalyse des KIT und hat die EU und die Bundesregierung beraten. Er hat u. a. an der Goethe-Universität Frankfurt und bei NTT Yokosuka geforscht.

Siedlungswasserwirtschaft im Zeitalter der Digitalisierung

Cybersicherheit als Achillesferse

Martin Zimmermann, *Institut für sozial-ökologische Forschung GmbH (ISOE), Hamburger Allee 45, 60486 Frankfurt am Main (zimmermann@isoe.de)*
Engelbert Schramm, *Institut für sozial-ökologische Forschung GmbH (ISOE) (schramm@isoe.de)*
Björn Ebert, *Institut für sozial-ökologische Forschung GmbH (ISOE) (ebert@isoe.de)*

Die Digitalisierung in der Siedlungswasserwirtschaft kann dazu beitragen, die Aufgaben, die sich für Wasserversorgung und Abwasserbeseitigung aufgrund des demografischen und klimatischen Wandels ergeben, besser anzugehen. Gleichzeitig können sich durch Cyberangriffe die Risiken für einen Ausfall dieser Kritischen Infrastrukturen vergrößern. Aspekte der Cybersicherheit werden im Wassersektor jedoch noch nicht hinreichend berücksichtigt. Entsprechende Regularien und Maßnahmen zielen alleine auf die Ausfallsicherheit der Infrastrukturen ab und vernachlässigen dabei die Versorgungssicherheit der Bevölkerung. Die Aufmerksamkeit der Politik auf große Wasserunternehmen und Versorgungsgebiete ignoriert Sicherheitslücken bei kleinen und mittleren Betrieben. Kooperationen zwischen mehreren Wasserunternehmen könnten ein geeignetes Mittel sein, diesbezüglich Synergieeffekte zu erzeugen.

Urban water management in the age of digitalization
Cybersecurity as an Achilles' heel

Digitalization in urban water management can help to better address the challenges for water supply and sanitation due to demographic and climate change. At the same time, cyberattacks can increase the risks for a failure of these critical infrastructures. However, aspects of cybersecurity are not yet sufficiently addressed in the water sector. Corresponding regulations and measures solely aim at the reliability of the infrastructures and neglect the security of supply for the population. Policy attention to large water utilities and supply areas ignores security gaps in small and medium-sized enterprises. Cooperations between several water utilities could be a suitable means of generating synergy effects in this respect.

https://doi.org/10.14512/tatup.29.1.37
Submitted: 26. 09. 2019. Peer reviewed. Accepted: 08. 01. 2020

Keywords: *critical infrastructure, cybersecurity, vulnerability, water infrastructure*

Einleitung

Zu den Funktionen der Siedlungswasserwirtschaft gehören neben dem Hochwasserschutz die öffentliche Trinkwasserversorgung sowie die Abwasserbeseitigung aus Siedlungen. Da deren grundlegende Wasserinfrastrukturen für gesellschaftliche und wirtschaftliche Prozesse unerlässlich sind (u. a. Wahrung der Versorgungssicherheit), können sie entsprechend der EU-Richtlinie 2008/114/EG als Kritische Infrastrukturen eingestuft werden, deren Schutz eine zentrale öffentliche Aufgabe darstellt.

In Deutschland werden 99 % der Bevölkerung über eine öffentliche Wasserversorgung mit Trinkwasser versorgt (Statistisches Bundesamt 2019 b): Insgesamt 4.400 Wasserversorgungsunternehmen befinden sich zumeist in unterschiedlichen Rechts- und Organisationsformen in kommunalem Eigentum. Nur 63 Unternehmen davon lieferten 2016 mehr als 10 Millionen m³ Wasser, davon einige auch ausschließlich als Lieferfirmen (z. B. die Bodenseewasserversorgung, die bis nach Tauber-Franken aktiv ist). Die meisten Unternehmen haben aber eigene Brunnen und operieren direkt in ihren Verteilgebieten, die viel kleiner sind und häufig an der Gemeindegrenze enden. Ähnlich ist die Situation auf der Ablaufseite, wo 97 % der Bevölkerung an die öffentliche Kanalisation mit 9.000 Kläranlagen angeschlossen sind (Statistisches Bundesamt 2019 a). Nur 276 Anlagen waren 2016 so groß, dass sie in mehreren Klärstufen mindestens 6 Millionen m³ Abwasser bearbeiteten, bevor ihr Ablauf in die Gewässer eingeleitet wurde. Beim Abwasser hängen Rechts- und Organisationsformen der Unternehmen sowohl mit der Kapazi-

tät der Kläranlage als auch der Größe und Siedlungsstruktur des Einzugsgebiets zusammen (Pointl et al. 2019).

Die Siedlungswasserwirtschaft steht derzeit vor einer Reihe von Herausforderungen, die sich u. a. aus dem demografischen Wandel und dem Klimawandel ergeben. Die Digitalisierung, beispielsweise in Form von flexibleren Mess-, Steuerungs- und Regelungssystemen (MSR), bietet dabei zum einen die Chance, durch intelligente Betriebsweisen auf außergewöhnliche Ereignisse (z. B. Extremwetterereignisse, kriminelle Gefahren, Stromausfälle) angemessener und schneller reagieren zu können. Zum anderen können Digitalisierungsprozesse durch die so erhöhte Komplexität der Infrastrukturen aber auch die Risiken für menschliches und technisches Versagen oder Sabotage (z. B. Hackerangriff, Terrorismus) vergrößern. Die Konsequenzen sind noch weitreichender, wenn die Abhängigkeiten der Wasserwirtschaft von der Energieversorgung oder Infrastrukturen der Informations- und Kommunikationstechnik (IKT) einbezogen werden. Momentan weist die deutsche Siedlungswasserwirtschaft im Vergleich zu anderen Branchen noch ein moderates Tempo bei der digitalen Transformation auf, u. a. aufgrund hoher Investitionskosten (z. B. Smart Grids und Smart Meters), fehlender Standards, fehlenden Fachpersonals oder Problemen bei Datenschutz und -sicherheit (Graumann 2017).

Digitalisierung innerhalb des Wasserversorgungssystems bringt hohe Anforderungen an IT-Sicherheits- und Datenschutzmaßnahmen für Erzeuger und Verbraucher mit sich.

Derzeit wird in Deutschland eine Novellierung des IT-Sicherheitsgesetzes geplant, mit dem die bestehenden Vorschriften dieses Gesetzes verschärft werden sollen. Im vorliegenden Artikel soll die Frage beantwortet werden, welche Gefährdungen sich für die Siedlungswasserwirtschaft unter Cybersicherheitsaspekten ergeben, ob die diesbezüglichen Regularien und Maßnahmen ausreichend sind und welche Schlussfolgerungen daraus gezogen werden müssen.

Gesetzliche Regelungen zur Cybersicherheit in der Siedlungswasserwirtschaft

Aus den USA wurden vor 2015 vereinzelt Cyberangriffe auf Wasserwerke bekannt. Nach Vorbild der USA (Clark et al. 2017) verabschiedete der Bundestag am 25. Juli 2015 ein Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme – das IT-Sicherheitsgesetz. Zentralakteur dabei wurde das 1991 gegründete Bundesamt für Sicherheit in der Informationstechnik (BSI); als zentrale Anlaufstelle für Betreiber Kritischer Infrastrukturen und Nationale Cybersicherheitsbehörde erhielt es zusätzliche Kompetenzen. Unternehmen, die große Kritische Wasserinfrastrukturen betreiben, wurden verpflichtet, eigene IT-Sicherheitsbeauftragte zu benennen, die die Cybersicherheit verantworten.

In der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz für die Sektoren Energie, Informationstechnik und Telekommunikation, Wasser, Ernährung (2016) und der ersten Verordnung zur Änderung der BSI-Kritisverordnung vom 21. Juni 2017 wurden Definitionen getroffen, die die Vorschriften der EU-Richtlinie 2008/114/EG umsetzten, die Einstufung von Anlagen als Kritische Infrastruktur festlegten und den betroffenen Unternehmen Kriterien (sog. „Schwellenwerte“) zur Bewertung ihrer Anlagen zur Verfügung stellten: Anlagen der Trinkwasserversorgung gehören bei mehr als 22 Mio. m³ jährlich verarbeiteter Wassermenge zur Schutzbedarfskategorie „hoch“. Sind 500.000 Einwohner an eine Anlage der Abwasserbeseitigung angeschlossen, so gehört diese in die entsprechende Schutzbedarfskategorie. Sie müssen branchenspezifische Mindeststandards erfüllen, insbesondere die Einführung eines Information Security Management Systems (ISMS), und relevante Vorfälle, die IT-Sicherheit betreffen, an das Bundesamt melden.

Der Schwerpunkt der Debatte hinsichtlich Cyberangriffen liegt in der Wasserwirtschaft derzeit auf den Operativen Technologien (OT) in den industriellen Netzen der Unternehmen, also der Prozessleit- und Automatisierungstechnik (Pointl et al. 2019; Lachance 2016). Die für administrative und organisatorische Aufgaben vorgesehenen Büro-Netze bzw. Informationstechnologien (IT) der Unternehmen werden nur insoweit berücksichtigt, als von ihnen auch Gefährdungen ausgehen können (Fluchs 2017).

Digitalisierung in der Siedlungswasserwirtschaft

In den vergangenen Jahren (2016–2019) haben sich Fachverbände der Wasserwirtschaft in Deutschland zunehmend mit der Frage der Digitalisierung wasserwirtschaftlicher Verfahrensprozesse und Systeme beschäftigt. Dabei wurden bisherige Praxisanwendung, Geschäfts- und gesellschaftliche Nutzen sowie potenzielle Chancen und Herausforderungen von Digitalisierung erörtert. In Anlehnung an „Industrie 4.0“ beschreiben in diesem Kontext Begriffe wie „Wasser 4.0“ (Schaffer et al. 2019) oder „Wasserwirtschaft 4.0“ (Pohl et al. 2017) Systeman-

sätze zur Transformation der Wasserwirtschaft hin zu vernetzten, automatisierten und zukunftsfähigen Systemen mit stärkerer Kundenorientierung und besserer Vernetzung innerhalb der Wertschöpfungskette. Dafür wird ein ganzheitlicher Ansatz aus intelligenten Versorgungsnetzen, sogenannten Smart Grids, gemeinsam mit *Internet of Things and Services* (IoT) zur Bereitstellung und Analyse von Daten sowie *Cyber-Physical-Systems* (CPS) für erforderlich gehalten (Schaffer et al. 2019, S. 6). CPS sind komplexe internetbasierte Datenkommunikationssysteme, die virtuelle und reale Wassersysteme vernetzen und damit Echtzeit-Monitoring sowie Vorhersagemodelle von Produktions-, Frühwarn- und Entscheidungsprozessen in Planung, Bau und Betrieb ermöglichen, was Risiken reduzieren und Kosten vermindern hilft (Schaffer et al. 2019, S. 6). Derartige Systeme sollen Ressourceneffizienz, Flexibilität und Wettbewerbsfähigkeit in der Wasserwirtschaft generieren, wobei der Verbraucherschutz im Vordergrund steht (Schaffer et al. 2019, S. 10; Pohl et al. 2017). Dabei werden eine qualitative Ressourcen- und Prozessoptimierung sowie die Chance auf ein verbessertes Daten- und Schnittstellenmanagement erwartet (Ammermüller und Fälsch 2017). Eine durch die Digitalisierung erbrachte Visualisierung kann ebenfalls zur Erhöhung des Systemverständnisses beitragen und Datenverfügbarkeit optimieren (Schaffer et al. 2019, S. 10). Trotz einer steigenden Bereitschaft zu digitalisieren, zeigt die deutsche Wasserwirtschaft bislang ein moderates Digitalisierungstempo. Sie erzielt einen weit unterdurchschnittlichen Wert ihres Umsatzes mit digitalisierten Produkten und 16 % der Betriebe verfügen über keinerlei digitalisierte Angebote (Graumann 2017).

Digitalisierung innerhalb des Wasserversorgungssystems bringt hohe Anforderungen an IT-Sicherheits- und Datenschutzmaßnahmen für Erzeuger und Verbraucher mit sich (Ammermüller und Fälsch 2017). Besonders CPS bergen durch die direkte Vernetzung virtueller und realer Wasserversorgungssysteme eine mögliche Angriffsstelle in der Cybersicherheit; dennoch setzt bspw. Siemens in Zukunftsprojekten der Abwasser-Steuertechnik auf Gesamtlösungen wie *Totally Integrated Automation* (TIA), bei der die gesamte Antriebs- und Steuerungstechnik von derselben Plattform gesteuert werden (Schaffer et al. 2019, S. 20). Eine Veränderung des Geschäftsmodells hin zu digitalisierten Systemen führt zu Herausforderungen im Personalwesen: Neue Qualifikationen erzeugen einen Mangel an internem Fachpersonal, deren Weiterbildung während des Geschäftsbetriebs zeitaufwändig ist. Der Einfluss branchenfremder qualifizierter Akteure („Disruptoren") hat wiederum Auswirkungen auf das etablierte Geschäftsmodell (Ammermüller und Fälsch 2017; Barjenbruch et al. 2016). Insgesamt erfordert die Digitalisierung einen hohen Investitionsbedarf und Zeitaufwand (Graumann 2017). Da Entscheidungen über Digitalisierungsprozesse meist zentral auf der strategischen Leitungsebene verortet sind, geschieht die Umsetzung in einem „Tone from the Top" (Schaffer et al. 2019, S. 10), was jedoch häufig den Bedürfnissen der einzelnen operativen Organisationseinheiten nicht entspricht. Beim Gesamtblick auf die Aspekte, die in der Siedlungswasserwirtschaft im Zusammenhang mit der Digitalisierung diskutiert werden, kann der Schluss gezogen werden, dass Probleme der Cybersicherheit vergleichsweise unterbelichtet bleiben.

Vulnerable Systembestandteile und Gefährdungen

Vulnerable Systembestandteile der Siedlungswasserwirtschaft

Zu den Operative-Technology-Systemen (OT-Systeme), also (geschlossene bzw. gekapselte Systeme), gehört die Mess-, Steuerungs- und Regelungstechnik (MSR) zur Überwachung und Steuerung technischer Prozesse mittels Computer-Systemen wie SCADA (Supervisory Control and Data Acquisition). In dieser Hinsicht unterscheiden sich die Bereiche der Wasserversorgung und Abwasserbeseitigung nicht grundsätzlich. OT-Systeme kommen hier z. B. zur Steuerung von Ventilen, Schiebern, Pumpen und Aufbereitungsprozessen sowie zur Regelung und Überwachung von Prozesswerten wie z. B. Druck und Durchfluss zum Einsatz. Manuelle Regulation ersetzend werden sie so zu einer entscheidenden Komponente der Wasserinfrastruktur. Dabei müssen die Systeme zur Echtzeitverarbeitung in der Lage sein und mit hoher Zuverlässigkeit und Verfügbarkeit arbeiten. OT-Systeme nutz(t)en im Unterschied zur IT daher oft andere, proprietäre Kommunikationsprotokolle und Standards. Außerdem trugen die Abgeschlossenheit von OT-Systemen und deren damit verbundene Unfähigkeit, PC-basierte Malware auszuführen, maßgeblich zu deren Sicherheit bei. Dadurch, dass die Erreichung funktionaler Ziele im Vordergrund stand, wurden OT-Komponenten oft ohne Berücksichtigung grundlegender IT-Sicherheitsanforderungen konzipiert und eingerichtet.

In jüngster Zeit werden jedoch auch IT-Standard-Netzwerkprotokolle in OT-Systemen eingesetzt, um die Kompatibilität zwischen OT und IT zu erhöhen. Zudem soll die Verknüpfung von IT, OT und Kommunikationsinfrastruktur den Betreibern von Wasserversorgungs- und Abwasserbeseitigungsanlagen die Fernsteuerung und Fernüberwachung ihrer Prozesse ermöglichen. Dies ist jedoch mutmaßlich mit einer Verringerung der Sicherheit von OT-Systemen und der damit gesteuerten und überwachten siedlungswasserwirtschaftlichen Infrastrukturen verbunden, siehe z. B. das Schadprogramm Stuxnet (Gaycken 2010). OT-Systemen kommt damit eine entscheidende Bedeutung für die Verwundbarkeit der Kritischen Infrastruktur Siedlungswasserwirtschaft zu. Informationstechnische Angriffe oder Manipulationsversuche werden mit hoher Wahrscheinlichkeit auf ebendiese Systeme ausgerichtet sein und können zu vorübergehenden Funktionsstörungen einzelner Komponenten bis hin zum Totalausfall der Wasserver- oder -entsorgung führen. Gezielte Attacken setzen jedoch ein hinreichendes Wissen über die Systeme voraus und sind mit einem vergleichsweise hohen Ressourcenaufwand (u. a. Zeit, Personen) verbunden, wobei sich durchaus die Frage stellt, ob der Zweck des Angriffs nicht auch mit anderen Mitteln zu erreichen ist (z. B. durch

unmittelbare Manipulation von Prozessen oder Beschädigung von Geräten).

Zu den vulnerablen Bestandteilen der Wasserversorgung gehören grob die Bereiche Wassergewinnung, Wasseraufbereitung und Wasserverteilung, zu denen der Abwasserbeseitigung die Bereiche Entwässerung, Abwasser- und Klärschlammbehandlung sowie Wasserausleitung (BSI 2014; Zimmermann und Schramm 2019). In allen Bereichen sind IKT-basierte Manipulationsversuche grundsätzlich möglich, wobei in Konsequenz unterschiedliche Schutzgüter (Gesellschaft, Natur) in verschiedenen räumlichen und zeitlichen Ausmaßen gefährdet sein können. Naheliegend wäre zunächst der Fall, dass die Rohwassergewinnung aus Grundwasser, Seen oder Talsperren (seltener direkt aus Fließgewässern) kompromittiert wird, was entsprechende Folgen für die Aufbereitung (z. B. Trockenfallen von Filtern) und Verteilung hätte. Denkbar wäre im umgekehrten Fall aber auch eine unkontrollierte Übernutzung von Grundwasser mit unerwünschten hydrogeologischen Konsequenzen (z. B. Salzwasserintrusionen aus anderen Grundwasserstockwerken). In Fällen, in denen die Ressourcenbasis über eine künstliche Grundwasseranreicherung gesteuert wird, können durch einen unerwünschten Eingriff u. U. Schadstoffe in das Grundwasser gelangen, wodurch sich auch die Gefahr der Erpressbarkeit ergeben kann.

In Bezug auf die Wasseraufbereitung im Wasserwerk sind prinzipiell sämtliche Aufbereitungsprozesse (z. B. Belüftung, Filtration, Enteisenung, Entmanganung, Desinfektion) durch Cyberattacken angreifbar, wodurch abhängig von der Wasserspeicherung die Versorgungssicherheit mengenmäßig oder qualitativ betroffen sein kann. Im Bereich der Wasserverteilung können abgesehen vom Ausfall von Pumpen zur Erhaltung des Versorgungsdrucks auch Smart Grids gestört werden, insbesondere mit Blick auf Aspekte der Netzsteuerung, des Demand Managements oder des Datenschutzes. Smart Grids sind derzeit in der Siedlungswasserwirtschaft noch nicht weit verbreitet. In Zukunft könnten IKT-bezogene Schwachstellen jedoch per Smart Metering bis in die einzelnen Haushalte hineinragen. Besonderheiten stellen soziotechnisch aufwändigere Systeme dar, wie etwa eine Fernwasserversorgung (z. B. Bodensee-Wasserversorgung) oder eine regionale Wasserbeschaffungsgesellschaft (z. B. Hessenwasser).

Darüber hinaus können die innerhäuslichen Versorgungsstrukturen von Wohn- und Bürotürmen durchaus ebenfalls als Teil der Kritischen Infrastruktur gesehen werden. Hier werden Betrieb und Wartung häufig an externe Facility-Management-Dienstleister übertragen, wodurch sich weitere Einfallstore hinsichtlich der Cybersicherheit ergeben. Innerhalb der öffentlichen Wasserversorgung sind daher auch gezielte Cyberattacken auf spezifische Branchen oder begrenzte Gebiete vorstellbar, wie z. B. das Frankfurter Bankenviertel oder Internetknoten und Rechenzentren, deren wasserbasierte Kühlung betroffen sein könnte. Im Gegensatz dazu verfügen große Produktionsstätten (z. B. der Chemie oder Automobilindustrie) oft über eine eigene Wasserversorgung und Abwasserbeseitigung, die gegenüber Cyber-Bedrohungen unterschiedlich gut gewappnet sind.

Das Risiko einer landesweiten Attacke auf die Siedlungswasserwirtschaft ist aufgrund deren Heterogenität und Kleinteiligkeit in Deutschland äußerst gering.

Unabhängig davon, ob öffentliche oder privatwirtschaftliche Wasserversorgungssysteme kompromittiert sind, ist zunächst ein räumlich begrenztes Einzugsgebiet eines Wasserversorgungsunternehmens oder sonstigen Betriebes betroffen. Eine gänzlich andere Bedrohungslage ergibt sich jedoch, wenn beispielsweise mehrere oder sämtliche Wasserwerke eines Landes einer Cyber-Attacke unterliegen. Das Risiko für ein derartiges Szenario kann für Deutschland aufgrund der Kleinteiligkeit und Heterogenität der Siedlungswasserwirtschaft als äußerst gering erachtet werden, ist aber in Ländern mit homogeneren oder zentralisierteren Strukturen grundsätzlich vorstellbar (z. B. Niederlande).

In Bezug auf die Abwasserbeseitigung sind Gefährdungen der Natur unter Cybersicherheitsaspekten als größer zu erachten als solche für die Gesellschaft, z. B. wenn Abwasser im Falle des Ausfalls der Reinigungsanlage unbehandelt in den Vorfluter abläuft. Wo, wie am Rhein, Trinkwasser aus Flusswasser gewonnen wird, kommt es durch das unbehandelt abfließende Abwasser zu Kaskadeneffekten. Aufgrund der gravitären Architektur der Schwemmkanalisation fließt Schmutzwasser ohne äußeren Energieeintrag zumindest bis zur nächsten Pumpstation oder gar bis zur Kläranlage. Die Pumpstation kann damit einen neuralgischen Punkt darstellen. Im schlimmsten Fall kommt es hier zu einem Rückstau des Schmutzwassers bis in die Wohnungen. In Gebieten mit Mischkanalisation gilt dies bei Niederschlag oder Starkregenereignissen auch für Abwasser. Dennoch wird auch in Österreich, wo die Abwasserbeseitigung rechtlich (wie in der EU) nicht als Kritische Infrastruktur gewertet wird, der Ausfallsicherheit von Abwassertransport und -behandlung eine so hohe Priorität beigemessen, dass eine gemeinsame Untersuchung der Cybersicherheit in beiden Bereichen und ein koordiniertes Vorgehen vorgeschlagen wird (Pointl et al. 2019).

Cyber-Gefährdungsszenarien für die Siedlungswasserwirtschaft

Im Kontext der Cybersicherheit in der Siedlungswasserwirtschaft können einerseits bewusst herbeigeführte Gefahren, etwa durch Kriminelle, Terroristen, aber auch Hacker oder Saboteure (Clark et al. 2017), sowie andererseits technisches und menschliches Versagen als Gefahrenkategorien unterschieden werden (Zimmermann und Schramm 2019). Letztere können das Einfallstor für intendierte Attacken darstellen, indem z. B. auf Nachlässigkeiten des Betriebspersonals spekuliert wird oder Fehler bewusst provoziert werden, u. a. ungenügende Zugriffskontrolle, Einschleppen von Schadsoftware oder veraltete Betriebssysteme (Pointl et al. 2019). Intendierte Cyber-Attacken können aus unterschiedlichen Motivationen heraus verübt werden. Klassische Sabotage und Terror wird von organisierten Hackern, sogenannten *Black Hats*, z. B. zum Zweck der Industriesabotage, der Erpressung oder aus ideologischen Gründen betrieben, wobei jeweils Staaten, Unternehmen oder die Öffentlichkeit das Ziel des Angriffs sein können. Dagegen können andere Hacker-Typen (*White Hats* oder *Grey Hats*) das Hacken aber auch als „sportliche Herausforderung" sehen ohne die Absicht, (größeren) Schaden herbeizuführen. Hier dient das Hacken u. a. zur Erlangung von Anerkennung in Hacker-Kreisen; es kann auch mit politischen oder anderen idealistischen Motiven verbunden sein. Schließlich ist aber auch eine interne Sabotage, z. B. verübt durch unzufriedene oder abgewiesene Mitarbeiter, denkbar (Clark et al. 2017). Völkerrechtlich problematisch ist die digitale Kriegsführung, da diese nicht nur auf die militärischen Kombattanten, sondern auch auf die Zivilbevölkerung zielt. Angriffe auf kritische Infrastrukturen finden zudem häufig auch ohne Kriegserklärung statt (Deutscher Bundestag 2015).

Bedingt durch die Abhängigkeit der vulnerablen siedlungswasserwirtschaftlichen Systembestandteile von der Stromversorgung, stellt deren Ausfall ein weiteres Gefährdungsszenario dar (Birkmann et al. 2010). Die Auswirkungen eines durch einen Cyberangriff bedingten Stromausfalls können zum Teil, aber nicht vollständig und nur vorübergehend, durch Notstromaggregate (z. B. zum Betreiben von Pumpen) abgefangen werden. Dieses Szenario wird in dem Roman „Blackout – Morgen ist es zu spät" von Marc Elsberg in einem dystopischen Narrativ illustriert (Koch 2016). Allerdings wird in der Imagination übersehen, dass es in Deutschland bezogen auf die Versorgung mit Trinkwasser in Ballungsgebieten eine Redundanz in einer infrastrukturell unabhängigen Notwasserversorgung gibt (Fischer et al. 2012; BBK 2016).

Regulierungsbedarf und Fazit

Die Praxis hat gezeigt, dass die deutschen Regelungen zur IT-Sicherheit durch eine ausschließliche Fokussierung auf Anlagen an der Wirklichkeit vorbeigehen: Es geht nicht um das reine (Optimierungs-)Geschehen in Wasseraufbereitungsanlagen, Verteilungsnetzen oder Leitzentralen, sondern um komplexe Wechselwirkungen. Mit dem Referentenentwurf für die Novellierung des IT-Sicherheitsgesetzes, dem sog. IT-Sicherheitsgesetz 2.0, verfolgt die Bundesregierung erstmals einen ganzheitlicheren Ansatz. Zudem sollen die für die Betreiber Kritischer Infrastrukturen bestehenden Meldepflichten und Verpflichtungen zur Einhaltung der Mindeststandards auf andere Branchen der Wirtschaft (z. B. die Abfallwirtschaft) ausgeweitet werden, soweit an ihnen besonderes öffentliches Interesse besteht.

„Um Cyber-Sicherheitsvorfällen insgesamt zu begegnen" (Meister und Biselli 2019), sollen nach dem Referentenentwurf aus dem Bundesinnenministerium jedoch nicht nur die Befugnisse der Strafverfolgungs- und Polizeibehörden, sondern auch die des Bundesamtes für Sicherheit in der Informationstechnik erheblich ausgeweitet werden. Da die Bedrohungen des Cyber-Raums unabhängig von den Grenzen der Bundesländer bestehen, sollen die Behörden der Länder durch das Bundesamt unterstützt werden. Ferner sind im Referentenentwurf Ermächtigungen vorgesehen, durch die das Bundesamt selbst fremde Geräte wie PCs oder Internet-Router aus der Ferne prüfen, in die Rolle von Verdächtigen schlüpfen und Internetverkehr manipulieren darf. Weiterhin will der Bund unsichere IT-Technik in den Unternehmen (ohne Ermächtigung und Zustimmung dieser) nachrüsten. Allerdings sind diese Durchgriffsregelungen aktuell höchst umstritten, weil sie Betreiberrechte und Datenschutz einschränken (Meister und Biselli 2019). Zudem wird das beabsichtigte Offenhalten und Nutzen von IT-Schwachstellen durch Sicherheitsbehörden auch innerhalb der Regierungskoalition als „geradezu kontraproduktiv für die IT-Sicherheit" bewertet (Esken 2019).

Mit dem Referentenentwurf für die Novellierung des IT-Sicherheitsgesetzes (IT-Sicherheitsgesetz 2.0) verfolgt die Bundesregierung erstmals einen ganzheitlichen Ansatz.

Nach dem Gesetzentwurf müssen Betreiber Kritischer Infrastrukturen künftig Systeme der Angriffserkennung betreiben. Ein *Intrusion Detection System*, wie es allerdings viele große Betreiber ohnehin bereits als selbstverständlichen Teil ihrer

IT-Sicherheit haben, um illegale Eindringlinge aufzuspüren, wird Pflicht. Zudem dürfen die Betreiber „Kernkomponenten" (also sicherheitsrelevante IT-Produkte, die zum Betrieb von Kritischen Infrastrukturen dienen und für diesen Zweck besonders entwickelt oder geändert wurden) nur noch von Herstellern beziehen, die vorher eine Erklärung über ihre Vertrauenswürdigkeit gegenüber dem Betreiber abgeben haben. Im Zusammenhang mit anderen Kritischen Infrastrukturen (z. B. Telekommunikation) wird aber angezweifelt (Meister und Biselli 2019), dass eine Erklärung über die Vertrauenswürdigkeit des Unternehmens ausreicht, wenn dieses im Ausland produziert und z. B. angenommen werden kann, dass vonseiten der dortigen Geheimdienste ein Zugriff bestehen könnte.

Cybersicherheit muss in Deutschland auch für kleinere und mittlere Unternehmen der Siedlungswasserwirtschaft gewährleistet sein.

Auch sind immer noch Software-Anwendungen von Regulierungen ausgenommen, die nicht nur im Rahmen von Kritischen Infrastrukturen verwendet werden, sondern für darüber hinaus gehende Zwecke entwickelt worden sind. Digitalisierungsbemühungen, bei denen Industrie-4.0-Anwendungen von der Stange gekauft werden, sind also nicht im Visier des staatlichen Versuchs, die Cybersicherheit für die Siedlungswasserwirtschaft zu verbessern.

Angesichts der von uns identifizierten Bedrohungsszenarien reichen die deutschen Regulierungsbemühungen keinesfalls aus. In der Debatte um das IT-Sicherheitsgesetz wird sich völlig falsch auf die großen Wasserunternehmen konzentriert. Aufgrund der größeren Sicherheitslücken, die bei den kleinen Unternehmen bestehen, könnte es jedoch für einen Angreifer auch interessant sein, z. B. viele kleine Wasserunternehmen im Speckgürtel einer Großstadt zu attackieren und dort die Wasserdienstleistungen zu unterbrechen.[1] Gerade in Deutschland sind die Betreiber der Wasserinfrastrukturen stark kommunal orientiert, sodass kleine und mittlere Unternehmen dominieren. Daher sollte das Schutzniveau der Kritischen Infrastrukturen keinesfalls von der Größe des Unternehmens abhängig sein. Wie die Sektor-Studie (BSI 2014) feststellt, ist gerade diese Größenordnung der Versorger aufgrund der Sicherheitsarchitektur besonders anfällig. Lösungen wird es auch für mittlere und kleine Unternehmen geben müssen, wenn nicht ein großer Teil der zu Versorgenden in Deutschland zum Spielball von Cyber-Angreifern gemacht werden soll.

Im Rahmen mehrerer Betreiberbefragungen haben Unternehmen der Siedlungswasserwirtschaft den Wunsch geäußert, externe Unterstützung für Cybersicherheit und den Schutz Kritischer Infrastrukturen einbeziehen zu können (Thim und Pöhls 2018; BSI 2014). Bei aller Vorläufigkeit ihrer Ergebnisse kommt die Sektor-Studie zu dem Ergebnis, dass es insbesondere kleinen und mittleren Wasserunternehmen schwer fällt, Kompetenzen zur IT-Sicherheit bei sich aufzubauen (BSI 2014). Jüngere Auswertungen haben dies bestätigt (Thim und Pöhls 2018). Allerdings könnten Kooperationen zwischen mehreren Unternehmen ein gutes Mittel sein, um hier zu Synergieeffekten zu kommen.

Doch nicht nur für die kleinen Wasserunternehmen bietet eine solche Zusammenarbeit trotz knapper Personaldecke die Möglichkeit, die Herausforderungen sowohl der Digitalisierung als auch der Cybersicherheit gut zu bewältigen. Das BMBF-Projekt „Dienstleistungen und Modelle für die gemeinsame Erbringung von Sicherheitsdienstleistungen", das eine Hochschule und ein Beratungsunternehmen mit dem Wasserunternehmen von Berlin und einem kleinen Zweckverband in Brandenburg durchgeführt hat, macht deutlich, dass auch für große Betreiber Vorteile in einer solchen Zusammenarbeit liegen können (Thim et al. 2012). Ein solcher Verbund könnte z. B. aus einem zentralen Kompetenzzentrum und mehreren regionalen Arbeitsgemeinschaften bestehen, in denen sich gebietsweise z. B. Wasserunternehmen zusammenschließen können, um bedarfsgerechte Schutzkonzepte zu erarbeiten und umzusetzen. Hierbei darf es nicht allein um die Ausfallsicherheit der Infrastrukturen gehen, sondern es muss ebenso auf die Versorgungssicherheit der Bevölkerung geachtet werden.

1 Kleine Wasserwerke können z. B. ein Wasseraufkommen von unter 100.000 m³ pro Jahr haben.

Literatur

Ammermüller, Britta; Fälsch, Marcel (2017): Digitale Wasserwirtschaft. Facts and Figures. Berlin: Verband kommunaler Unternehmen e. V.

Barjenbruch, Matthias et al. (2016): Forschungsbedarf in der Wasserwirtschaft. Water Innovation Circle. Bonn: DWA.

BBK – Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2016): Trinkwassernotversorgung. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

Birkmann, Jörn; Bach, Claudia; Guhl, Silvie; Witting, Maximilian; Welle, Torsten; Schmude, Miron (2010): State of the Art der Forschung zur Verwundbarkeit Kritischer Infrastrukturen am Beispiel Strom, Stromausfall. Berlin: Freie Universität Berlin.

BSI – Bundesamt für Sicherheit in der Informationstechnik (2014): KRITIS-Sektorstudie. Ernährung und Wasser. Öffentliche Version, Revisionsstand 16. März 2015. Bonn: Bundesamt für Sicherheit in der Informationstechnik.

Clark, Robert; Panguluri, Srinivas; Nelson, Trent; Wyman, Richard (2017): Protecting drinking water utilities from cyberthreats. In: Journal of American Water Works Association 109 (2), S. 50–58.

Deutscher Bundestag (2015): Anwendbarkeit des humanitären Völkerrechts auf Computernetzwerkoperationen und digitale Kriegsführung (Cyber Warfare). Ausarbeitung WD 2-3000-038/15. Berlin: Wissenschaftliche Dienste Deutscher Bundestag.

Esken, Saskia (2019): Zur Sache. Interview mit Saskia Esken. In: Gesellschaft für Informatik e. V. (Hg.): Jahresbericht 2018/19, S. 28. Online verfügbar unter https://gi.de/fileadmin/GI/Hauptseite/Service/Infomaterial/GI_Jahresbericht_19_Web.pdf, zuletzt geprüft am 21. 01. 2020.

Fischer, Peter; Rönnfeldt, Jens; Schindler, Norbert; Nees, Peter (2012): Trinkwassernotversorgung. Betrieb eines Bundes-Notbrunnens in Darmstadt. In: Bevölkerungsschutz (4), S. 23–25.

Fluchs, Sarah (2017): IT-Grundschutz-Pilotprofil bzw. IT-Grundschutz-Profil für die Wasserwirtschaft. Masterarbeit. Aachen: RWTH Aachen.

Gaycken, Sandro (2010): Stuxnet. Wer war's? Und wozu? In: DIE ZEIT, Nr. 48. Online verfügbar unter https://www.zeit.de/2010/48/Computerwurm-Stuxnet/komplettansicht, zuletzt geprüft am 25. 09. 2019.

Graumann, Sabine (2017): Energie- und Wasserversorger noch verhalten bei Digitalisierung. In: energie/wasser-praxis (4), S. 6–9.

Koch, Lars (2016): Heart of Darkness. Über das katastrophische Imaginäre des Blackouts. In: BEHEMOTH – A Journal on Civilisation 9 (1), S. 58–76.

Lachance, Lancen (2016): IT vs. OT für das Industrielle Internet. Zwei Seiten einer Medaille? In: GlobalSign Blog. Online verfügbar unter https://www.globalsign.com/de-de/blog/it-vs-ot-im-industriellen-internet/, zuletzt geprüft am 25. 09. 2019.

Meister, Andre; Biselli, Anna (2019): IT-Sicherheitsgesetz 2.0. Wir veröffentlichen den Entwurf, der das BSI zur Hackerbehörde machen soll. In: Netzpolitik.Org. Online verfügbar unter https://www.netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll, zuletzt geprüft am 25. 09. 2019.

Pohl, Christian; Spinnreker-Czichon, Dominic; Keilholz, Patrick (2017): Wasserwirtschaft 4.0. Voraussetzung für eine intelligente Vernetzung von Bestandssystemen. Bremen: DHI WASY.

Pointl, Michael; Winkelbauer, Andreas; Krampe, Jörg; Fuchs-Hanusch, Daniela (2019): Aspekte der IKT-Sicherheit in der österreichischen Siedlungswasserwirtschaft. In: Österreichische Wasser- und Abfallwirtschaft 71 (7–8), S. 374–384. DOI: 10.1007/s00506-019-0584-y.

Schaffer, Carsten; Vestner, Richard; Bufler, Ralf; Werner, Uwe; Ziemer, Christian (2019): Wasser 4.0. Berlin: German Water Partnership e. V. (GWP).

Statistisches Bundesamt (2019 a): Öffentliche Wasserversorgung und öffentliche Abwasserentsorgung. Öffentliche Abwasserbehandlung und -entsorgung. Fachserie 19, Reihe 2.1.2. Wiesbaden: Statistisches Bundesamt (Destatis).

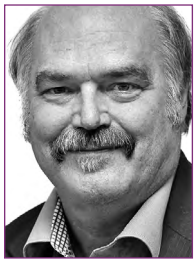
Statistisches Bundesamt (2019 b): Öffentliche Wasserversorgung und öffentliche Abwasserentsorgung. Öffentliche Wasserversorgung. Fachserie 19, Reihe 2.1.1. Wiesbaden: Statistisches Bundesamt (Destatis).

Thim, Christof; Pöhls, Uwe (2018): Stand der IT-Sicherheit in der Wasserversorgung. In: wwt wasserwirtschaft wassertechnik 2018 (1–2), S. 40–42.

Thim, Christof; Röchert-Voigt, Tanja; Proske, Niels; Heine, Moreen; Korte, Edgar (2012): Organisation des Schutzes der Kritischen Infrastruktur Wasserversorgung. Grundlagen und praktische Anwendung für Wasserversorger. Potsdam: Universität Potsdam.

Zimmermann, Martin; Schramm, Engelbert (2019): Digitalisierung als Herausforderung. Die Vulnerabilität Kritischer Infrastrukturen in der Siedlungswasserwirtschaft. In: Transforming Cities 2019 (4), S. 58–62.

DR.-ING. MARTIN ZIMMERMANN
ist wissenschaftlicher Mitarbeiter des ISOE und leitet seit Juli 2018 den Forschungsschwerpunkt Wasserinfrastruktur und Risikoanalysen. Er studierte Wirtschaftsingenieurwesen mit der technischen Fachrichtung Bauingenieurwesen an der TU Darmstadt und promovierte im DFG-Graduiertenkolleg „Topologie der Technik".



DR. ENGELBERT SCHRAMM
ist Mitbegründer des ISOE und war von 2014 bis Juli 2018 Mitglied der Institutsleitung. Er hat ein Studium der Biologie, Chemie und Erziehungswissenschaften an der Universität Frankfurt am Main absolviert. 1995 hat er zur Ideengeschichte des Kreislaufs an der TU Darmstadt promoviert.

BJÖRN EBERT
arbeitet als wissenschaftlicher Mitarbeiter des ISOE im Forschungsschwerpunkt Wasserinfrastruktur und Risikoanalysen. Er studierte Politikwissenschaft und Volkswirtschaftslehre in Frankfurt sowie an der Freien Universität Berlin und promoviert derzeit im Bereich der Technik- und Innovationssoziologie.

Chancen und Limitierungen der Digitalisierung von Unterricht

Eine Bewertung aus pädagogischer Perspektive

Johannes Gutbrod, *Institut für Berufspädagogik und Allgemeine Pädagogik, Zentrum für Lehrerbildung (ZLB), Karlsruher Institut für Technologie (KIT), Hertzstraße 16, 76187 Karlsruhe (Johannes.Gutbrod@kit.edu)*

Die Digitalisierung ist eine der großen Herausforderungen des 21. Jahrhunderts. Auch die Institution Schule ist hiervon betroffen. Der DigitalPakt Schule zwischen Bund und Ländern soll helfen, diese Aufgabe zu bewältigen, indem er digitale Medien zur Verfügung stellt. Das Problem liegt aus pädagogischer Sicht darin, dass im Unterricht zwischen der Lernmethode und der Lerntechnik durchaus unterschieden werden kann. Digitale Medien sind dem Bereich der Lerntechniken zuzuordnen. Lerntechniken sind für den Lernprozess zwar notwendige, aber keine hinreichenden Bedingungen.

Chances and limitations of digitalization of classes
An evaluation from a pedagogical perspective

Digitalization poses one of the most significant challenges of the 21st century, which also affects school as an institution. The so-called DigitalPakt Schule, an agreement between Germany's Federal Government and the States, is supposed to support this development by providing schools with digital media. In class, a distinction between learning methods and learning procedures is quite common. Digital media can be classified as learning procedures. This can lead to problems since learning procedures are necessary, but insufficient for a full learning process as such.

Keywords: *digitalization, school, lessons, digital media, criticism*

https://doi.org/10.14512/tatup.29.1.44
Submitted: 07.05.2019. Peer reviewed. Accepted: 04.12.2019

Einleitung

Das gesellschaftliche Leben wird zusehends digitaler. Die digitale Veränderung spielt „im Kontext von Industrie und Wirtschaft, Politik und Verwaltung, Medizin und Gesundheit, Wissenschaft und Fortschritt" längst eine überragende Rolle (Zierer 2017, S. 9). In einem Bereich der Gesellschaft scheint diese Entwicklung sich allerdings erst Bahn zu brechen: in der Schule. Obwohl diese Institution ausnahmslos alle Heranwachsenden auf das Leben vorbereiten soll, scheint sie noch nicht recht im digitalen Zeitalter angekommen zu sein. Nur wenige schulpflichtige Kinder in Deutschland beherrschen neben der Handschrift auch das Zehnfingersystem und noch weniger können nach Abschluss der Schule in einer gängigen Programmiersprache programmieren.

Um dieser Herausforderung zu begegnen, wollen Bund und Länder die Schulen bei der Digitalisierung von Bildungsprozessen unterstützen und stellen hierfür im sogenannten *DigitalPakt Schule* fünf Milliarden Euro bereit. Im Bereich der Digitalisierung haben nicht alle Schulen die gleichen Herausforderungen zu bestehen. „Mit dem DigitalPakt Schule wollen Bund und Länder für eine bessere Ausstattung der Schulen mit digitaler Technik sorgen" (BMBF 2019), um die „digitale Kompetenz" der Schulkinder zu fördern. Nur wer digital kompetent ist, kann „digitale Medien selbstbestimmt und verantwortungsvoll nutzen" (BMBF 2019). Um im Umgang mit ihnen geschult werden zu können, muss man digitale Medien wie Tablets und Whiteboards, aber auch Breitbandinternet auch zur Verfügung haben, wofür der Staat durch den DigitalPakt Schule sorgen möchte. In diesem Zusammenhang ist es wichtig zu erwähnen, dass die Idee des DigitalPakts Schule keineswegs neu ist. Bereits 1996 wurde der gemeinnützige Verein „Schulen ans Netz" gegründet, der es sich zur Aufgabe gemacht hatte, allen Schulen einen kostenfreien Internetzugang zur Verfügung zu stellen. Im Jahr 2012 wurde der Verein aufgelöst, da dieses vornehmliche Ziel laut Verein erreicht war.

Allerdings, so scheint es, liegt hier auch das Kernproblem. Denn allein mit der Bereitstellung von Geräten und digitaler Infrastruktur wie Tablets, Computern, VR-Brillen und Breitbandinternet für alle Schulen ist noch keine *Digitalisierung* bewältigt. Nach Meinung des Autors liegt die Herausforderung nicht im Bereich der Bereitstellung digitaler Infrastruktur, sondern vielmehr im Bereich der Haltung zur Digitalisierung, was so gewendet ein pädagogisches Problem darstellt und im Nachgang untersucht werden soll.

Pädagogische Unterscheidung

Der Unterricht ist das Kerngeschäft der Schule[1]. Unterricht lässt sich aus pädagogischer Sicht unter dreifachem Aspekt ausdifferenzieren: hinsichtlich seiner *didaktischen Dimension*, die thematisch-inhaltlich bestimmt ist (Was wird unterrichtet?); weiterhin hinsichtlich seiner *organisatorischen Dimension*, die bspw. die Zusammensetzung der Schulklassen und Räumlichkeiten umfasst (Unter welchen Rahmenbedingungen wird unterrichtet?). Letztlich kann eine *methodische Dimension* unterschieden werden, die die konkrete Unterrichtsgestaltung betrifft (Wie wird unterrichtet?) (Fend 2008; Rekus und Mikhail 2013).

Da Lehrpersonen durch Bildungs- und Lehrpläne vorgeschrieben wird, in welchem Schuljahr und Fach welche Lehrinhalte zu vermitteln sind (Didaktik), während zugleich die Klassenzusammensetzung, die betreuende Lehrperson, die Raumeinteilung sowie die Anordnung der Stundentafel von der Schulleitung festgesetzt werden (Organisation), haben Lehrpersonen einzig Einfluss auf die methodische Gestaltung des Unterrichts.

Die *methodische Dimension* ist hiernach sozusagen das pädagogische Herzstück des Unterrichts, „denn von der Art und Weise, wie die methodischen und unterrichtsmethodischen Gliederungsmomente in der Praxis gestaltet werden, hängt zuallererst ab, ob wir einen Unterricht ‚gut' nennen können" (Pöppel 1992, S. 54). Das lernmethodische Vorgehen wird in der Schule durch die Fächer bestimmt[2], da die jeweilige Methode in die Konstitution der Gegenstände unserer Erkenntnis eingeht bzw. weil die angewandte Lernmethode die Gegenstände als solche allererst bestimmt. Demgemäß haben Lehrpersonen keinen Einfluss auf die Lernmethode, sind jedoch bei der Führung des unterrichtsmethodischen Lernwegs unentbehrlich. Zum Beispiel führen sie die Erkenntnis im Deutschunterricht durch das Erklären unbekannter Worte oder durch eine Zeilennummerierung zur leichteren Orientierung im Text.

Damit ist eine subtile Unterscheidung des unterrichtlichen Methodenbegriffs angesprochen und eingeführt, die auch auf die Digitalisierung immense Auswirkungen hat. Aus pädagogischer Sicht ist streng zwischen der Lern*methode* und der Lern*technik* zu unterscheiden. Kurz gesagt: Mithilfe der Lern*methoden* wird Erkenntnis generiert, mithilfe der Lern*techniken* ist das nicht möglich. Einige Beispiele mögen dies illustrieren.

Im Mathematikunterricht soll eine Strecke unter Zuhilfenahme eines Zirkels und eines Lineals halbiert werden. Für die mathematische Operation sticht man mit dem Zirkel jeweils in die Endpunkte der Strecken ein und zeichnet je zwei Halbkreise so ein, dass sie sich einmal ober- und einmal unterhalb der Strecken schneiden. Anschließend richtet man das Lineal an den Schnittpunkten der Kreise aus, um die gegebene Strecke zu halbieren. In der Mathematik ist der richtige Umgang mit Lineal und Zirkel notwendig, aber nicht jedes im Umgang mit diesen Instrumenten geschulte Kind ist zugleich auch in der Lage, eine Strecke zu halbieren (Ladenthin 2018, S. 114). Die mathematische Operation – die Lern*methode* der Mathematik – führt zu mathematischer Erkenntnis. Die hierfür notwendige Lern*technik* – der Umgang mit Zirkel und Lineal – ist pädagogisch ausgedrückt *inhaltsleer*. Die technische Verwendung von Hilfsmitteln und Instrumenten impliziert noch nicht das Verständnis der mathematischen Operation. Schließlich kann jemand auch die Strecke halbieren, ohne das geringste mathematische Verständnis aufzubringen und ohne im buchstäblichen Sinne zu begreifen, was er hier tut. Wer lernt, lernt also immer *durch* eine Lernmethode – hier im Beispiel die geometrische Streckenhalbierung – und *mithilfe* von Lerntechniken – hier im Beispiel die Handhabung von Zirkel und Lineal. Man lernt allerdings niemals *ohne* Lernmethode, denn dann hätte das Lernen keinen Inhalt bzw. keinen Gegenstand mehr.

Lerntechniken sind trotz ihrer Inhaltsleere für das Lernen essentiell. Sie „*begleiten* nicht nur, sie *unterstützen*, ja *ermöglichen* erst die unterrichtsmethodische Führung des Lehrers und die methodische Arbeit des Schülers" (Pöppel 1992, S. 95). Ohne Lern*techniken* ist Lernen unmöglich, obschon ihre Funktion ausschließlich auxiliar ist. „Eine Technik auf der Schülerseite

Allein mit der Bereitstellung digitaler Medien und Infrastruktur wie Tablets, Computer, VR-Brillen und Breitbandinternet ist noch keine Digitalisierung bewältigt.

1 „Die im Folgenden aufgeführten Vorschläge" sind so zu verstehen, dass sie „weder den institutionellen Rahmen der Schule" sprengen, noch, dass es einer „Umstrukturierung des Schulwesens oder des Schulalltags" bedarf (Gutbrod 2018, S. 169).

2 Es besteht aus pädagogischer Sicht ein hierarchischer Unterschied zwischen der Lernmethode (Tenorth und Tippelt 2007, S. 739) und der Unterrichtsmethode (Kambartel und Welter 1980, S. 1326).

ist das, was im Augenblick unter dem Schlagwort „Lernen des Lernens“ gefasst wird: Darunter sind technische Verfahren aufgeführt, die das Lernen unterstützen, ohne schon Inhalte zu erzeugen“ (Ladenthin 2018, S. 114).

Ein weiteres Beispiel mag dies hervorheben: Im Geografieunterricht ist es freilich besser, wenn alle Lernenden über das eigene Tablet auf eine aktuelle Weltkarte aus dem Internet zurückgreifen können, statt auf einen veralteten Altas blicken zu müssen. Selbst hier treten die digitalen Medien ausschließlich als Lern*technik* auf, so gravierend ihr Einfluss auf das Unterrichtsgeschehen auch sein mag. Es ist letztlich unumgänglich, dass Schülerinnen und Schüler die Namen der Länder nennen können. Hierfür stellt die anschauliche und fraglos aktuelle Darbietungsweise dennoch lediglich eine Hilfe dar. Wer die Kontinente auf der Weltkugel nicht verorten kann, dem liefert auch die farbenprächtigste Darstellung kaum mehr als eine, im Kant'schen Sinne, „blinde Anschauung“.

Digitale Medien erfahren im schulischen Kontext eine Transformation vom Freizeit- zum Arbeitsgerät.

Digitale Medien bieten im Unterrichtsgeschehen nicht gekannte Anschauungen und Darbietungsweisen, die zu einem schnelleren Verständnis der Sache beitragen können, wobei hier kein Kausalzusammenhang besteht. Das beschwerliche und oftmals belastende Lernen wird Schülerinnen und Schülern durch digitale Medien nur vermeintlich abgenommen. Lernen bleibt eben Lernen (Zierer 2017, S. 51). Diese Aufgabe ist nicht delegierbar, weder an Mitmenschen noch an eine Maschine. Jeder Mensch kann nur selbst verstehen, einsehen und Sinn stiften – kurz: lernen. „Dabei bezieht sich Lernen nicht nur auf die geistige Entfaltung, auf die Erweiterung von Einsicht und Kenntnissen und auf die Prägung von Bedeutungsgehalten, sondern auch auf die Änderung des motorischen und sozialen Verhaltens“ (Böhm und Seichter 2018, S. 308). Spitzer formuliert in diesem Zusammenhang: „Lernen setzt eigenständige Geistesarbeit voraus: Je mehr und vor allem je tiefer man einen Sachverhalt geistig bearbeitet, desto besser wird er gelernt“ (Spitzer 2012, S. 95), mit anderen Worten: Lernen *ist* ausschließlich eigenständige Geistesarbeit. Der sogenannte „Nürnberger Trichter“ ist auch durch die Digitalisierung des Unterrichts nicht gefunden.

Technikfolgenabschätzung unter pädagogischer Perspektive

Bildungsauftrag der Schule

Ausgehend vom Bildungs- und Erziehungsauftrag der Schule als ihrer Hauptaufgabe sollen im Anschluss die Folgen der Digitalisierung genauer betrachtet werden. Die Digitalisierung des Unterrichts geht die Bildung wie die Erziehung der Schülerinnen und Schüler gleichermaßen an; beide sollen aber hier getrennt voneinander thematisiert werden.

Digitale Medien treten im Unterricht in fast allen Fächern ausschließlich als Lern*techniken* und nur in ganz besonderen Fällen als Lern*methoden* auf. Methode sind sie bspw. in der Informationstechnischen Grundbildung (ITG), im Informatik- oder im Medienkundeunterricht, da sie dort selbst zum Gegenstand bzw. Inhalt des Unterrichts gemacht werden. Sie erfahren dann eine Transformation von der Lern*technik* zur Lern*methode*. Der Lerninhalt ist die Bedienung und Handhabung des PCs, des Tablets und der verschiedenen Programme und Applikationen. Der Umgang mit digitalen Medien muss als *Methode* erlernt werden, sodass sie in allen anderen Fächern später als Lern*technik* eingesetzt werden kann. Es ist dann insofern beinahe gleichgültig, welche Textart die Schülerinnen und Schüler in ihrem Dokument formatieren und bearbeiten, da im Informatikunterricht das Formatieren erlernt werden soll. Der Inhalt einer Präsentation rückt daher in den Hintergrund, da es darum geht, wie man das Präsentationsprogramm bedient. Die Inhalte der Datensätze sind eher zweitrangig, da die Schülerinnen und Schüler die Programmierung einer Datenbank erlernen und nicht die Daten interpretieren sollen. Dieser Unterricht hat eine enorm wichtige Bedeutung für alle anderen Fächer, da sie oftmals auf die Erkenntnisse und (Lern-)Ergebnisse aus diesem Bereich aufbauen, woraus sich allerdings zwei Herausforderungen ergeben.

Das Verhältnis von Lern*technik* und Lern*methode* kehrt sich in allen anderen Fächern um. Wo sie in der ITG, im Informatik- oder im Medienkundeunterricht noch als Selbstzweck aufgetreten sind, können die digitalen Medien in allen anderen Fächern nur noch als Mittel zum Zweck angesehen werden. Aufgrund vielfältiger Aufgabenstellungen, wie bspw. dem Erstellen von Referaten und gesonderten fachlichen Lernleistungen, ist ein eigener PC bzw. Laptop respektive die Kenntnisse im Umgang mit derlei Medien für Schülerinnen und Schüler beinahe unabdingbar. Ein tragbares Endgerät wie bspw. ein Tablet ist für den drahtlosen Internetzugang beinahe ebenso notwendig.

Jedoch versteckt sich hier ein Fallstrick der Technisierung des Unterrichts. Selbst ein gut formatiertes und einheitliches Dokument, eine übersichtliche Datenbank oder eine anschauliche Präsentation sind nicht brauchbar, wenn der Inhalt als schlecht zu bewerten ist. Im Informatikunterricht mag es zuträglich sein, wenn die Dateien das richtige Format haben. In vielen anderen Fächern ist die Formatierung des Referats lediglich ein Mittel, um den Lerninhalt ansprechend darzustellen. Allein die gelungene Darstellung und Formatierung sind gewiss im Fach Geschichte noch nicht als Leistung zu bewerten, da sie

keine historisch relevanten Inhalte, sondern eben informationstechnologische Fertigkeiten darstellen.

Die zweite Herausforderung betrifft den Umgang mit der technischen Revolution im Klassenraum. Die Digitalisierung des Unterrichts birgt die Gefahr, dass sich die Unterrichtsinhalte bzw. die Unterrichtsgegenstände den Mitteln, und hier besonders den digitalen Medien, unterordnen, weil Lehrpersonen als fortschrittlich gelten, wenn sie digitale Medien einsetzen. Die Ziele des Unterrichts dürfen jedoch nie den Medien untergeordnet werden, da sie unter diesen Umständen nicht mehr korrekt dargestellt werden können. Gerade die unterschiedliche Betrachtungsweise der Welt begründet ja die Eigenständigkeit der Schulfächer und diese Eigenständigkeit ist bedroht, wenn sich in der Bewertung von Referaten, Hausarbeiten und Präsentationen der gekonnte Umgang mit der Technik in der Notengebung widerspiegelt, obschon der sachgerechte Inhalt bewertet werden sollte.

Erziehungsauftrag der Schule

Der Umgang mit digitalen Medien im Klassenraum birgt noch einen weiteren Fallstrick, der vor allem in Zusammenhang mit dem schulischen Erziehungsauftrag steht. Die Aktivität der Lernenden wird durch die Digitalisierung vor eine neue Herausforderung gestellt. Lernen – als die pädagogische Hauptaufgabe der Schule – ist häufig mit Mühe und Anstrengung verbunden. Wie schon Platon im Höhlengleichnis allegorisch andeutet, können Wissen bzw. Wissenserwerb sogar (kognitive) Qualen bereiten.

Dem Bereich schulischer Medienerziehung sollte daher weitaus mehr Beachtung geschenkt werden, als dies momentan der Fall ist. Die Digitalisierung der Schule ist vor allem auch eine medienerzieherische Aufgabe. „Die Medienerziehung hat, unterschiedlichen pädagogischen Leitbildern folgend, in den vergangenen Jahrzehnten eine Vielzahl von Konzepten hervorgebracht, wie Heranwachsende an den Umgang mit Medien herangeführt werden können (Schaumburg und Prasse 2019, S. 126). Medienerzieherische Konzepte umfassen, grob gesagt, fünf Aspekte: vor Medien bewahren; ungewollte Erfahrungen im Umgang mit Medien reparieren; über Medien aufklären; die eigene Mediennutzung reflektieren; sowie mit und durch Medien handeln bzw. partizipieren (Schaumburg und Prasse 2019, S. 126). Diese Aspekte zeigen deutlich, dass auch Kinder, die als *digital natives* bezeichnet werden, durchaus eine Erziehung im Bereich der Medien nötig haben. Die Nutzung eines Mediums ist nicht zwangsläufig mit dessen vernünftigem Gebrauch gleichzusetzen. In der Schule sollte daher vor allem darauf geachtet werden, alle Facetten der Medienerziehung zu berücksichtigen.

Die Verwendung eines Tablets in der Schule besteht eben nicht nur aus Wischen, Liken und Konsumieren, sondern aus Nachdenken, Übertragen und Anwenden. Das Tablet erfährt im schulischen bzw. unterrichtlichen Kontext eine Transformation vom Freizeit- zum Arbeitsgerät. Lernen bereitet dann eben nicht nur Spaß, sondern ist eine ernsthafte, streckenweise auch mühsame Angelegenheit. Aufmerksamkeitsheischende Applikationen zurückzustellen, erfordert ein hohes Maß an Selbstdisziplin.

Das beschwerliche und oftmals belastende Lernen wird Schülerinnen und Schülern durch digitale Medien nur vermeintlich abgenommen.

Diese Anstrengung soll durch die Digitalisierung abgemildert werden, da digitale Medien Erleichterung bei Lernprozessen versprechen. Komplizierte Sachverhalte sollen durch anschauliche digitale Darbietung schnell durchschaut, knifflige Aufgaben rascher gelöst und komplexe Gegebenheiten zügig begriffen werden.

In der Anwendung der digitalen Medien liegt auch ihre Krux. Sie hängt mit der herkömmlichen Benutzung und Attribuierung digitaler Medien durch die Schülerinnen und Schüler zusammen. Tablets, VR-Brillen, Smartphones und Computer werden von Kindern und Jugendlichen nicht als Arbeits-, sondern als Unterhaltungsgeräte betrachtet. Sie bieten überall und jederzeit Zugang zu sozialen Netzwerken im Internet, sie werden genutzt, um Fotos zu schießen und zu versenden sowie *Likes* zu verteilen. Diese herkömmliche Nutzung steht der Idee eines digitalisierten Unterrichts diametral entgegen, wenn hier die Geräte für Arbeit, Lernaufgaben und Anstrengung, dort für Entspannung, Erholung und Unterhaltung stehen.

Die Grenze zwischen Arbeit und Freizeit ist, gerade im Bereich digitaler Medien, ebenso wenig einfach zu ziehen und noch viel schwieriger einzuhalten, da die Freizeitbeschäftigung oft nur *eine App entfernt* ist[3]. Wenn sogar viele Erwachsene einen verantwortlichen Umgang mit digitalen Endgeräten vermissen lassen, kann die permanente Selbstdisziplinierung der Heranwachsenden nur schwer eingefordert werden. Spitzer hat auf diesen Umstand immer wieder hingewiesen (Spitzer 2012; 2018).

Technikfolgenabschätzung

Aus der Digitalisierung des Unterrichts ergeben sich weitere Herausforderungen für die Institution Schule. Denn aus ihrem Erziehungs- und Bildungsauftrag zu folgern, dass das Haupt-

3 Den Umstand der permanenten Ablenkung durch andere Apps macht sich die App *Forest* zunutze. Man pflanzt bei der Öffnung der App einen digitalen Sämling, der zum Baum heranreifen kann. Allerdings wächst der Baum nur, wenn man die App geöffnet lässt und keine anderen Apps während des Wachstums öffnet.

geschäft ein pädagogisches wäre, ist falsch. Die Schule ist ein Kampfplatz verschiedener Interessen. Bezüglich der Digitalisierung spielt die Ökonomie eine überragende Rolle.

Ökonomische Fragen drehen sich nicht allein um die ökologisch-ökonomische Dimension, ob man etwa in der digitalisierten Schule Papier sparen kann, da alle Akteure papierlos arbeiten, ob die Schulbücher digital vorliegen oder ob alle Daten in der schuleigenen *Cloud* gespeichert werden können und daher überall und jederzeit verfügbar sind.

Vielmehr sollte auch bedacht werden, dass ein technischer Generationenwechsel bei Hard- und Software hohe laufende Kosten verursacht, die so bisher im Bereich Schule nicht aufgetreten sind. Es ist sehr kostspielig, mittel- und langfristig quantitativ ausreichende und qualitativ geeignete digitale Endgeräte anzuschaffen, instand zu halten oder ersetzen zu müssen, ganz zu schweigen von den Randbedingungen der Digitalisierung des Unterrichts: Hierunter fällt bspw. die sachangemessene Ausbildung von professionellen Netzwerkbetreuenden, um ein Schulnetzwerk *am Laufen halten* zu können und zugleich zu berücksichtigen, dass sie aufgrund dieser zeitlichen Beanspruchung nicht mehr in vollem Umfang ihrer eigentlichen Aufgabe – dem Unterrichten – nachkommen.

Zugleich müssen alle digitalen Medien von der Schule auch verwaltet werden. Sie müssten alle inventarisiert, bei Bedarf Reparaturaufträge geschrieben und bspw. Tablets nach Beendigung der Schulzeit auch wieder von den Absolventinnen und Absolventen an die Schule zurückgegeben werden. Um die Endgeräte muss ein mit großem Aufwand betriebener Verwaltungsapparat entstehen.

Dies ließe sich vermeiden, würde man auf ein *BYOD*-System *(bring your own device)* umstellen, was allerdings erstens der Lernmittelfreiheit widersprechen, zweitens aus sozio-ökonomischer Sicht weiter Druck auf Heranwachsende ausüben würde, da diese eben nicht alle das neueste Endgerät besitzen, und drittens mit dem Datenschutz nur schwer vereinbar wäre. Dies tangiert auch die Frage nach dem Urheberrecht und dem Schutz der persönlichen Daten, worauf hier lediglich kurz hingewiesen werden soll. Das Thema Fortbildungen im Bereich der Digitalisierung für Lehrpersonen und die dazugehörigen Unterrichtskonzepte soll hier ebenfalls nur erwähnt werden.

Ökonomisches Denken spielt in der Institution Schule eine immer größere Rolle, obschon Benner (2015, S. 46) in seiner Praxeologie zu Recht darauf hingewiesen hat, dass sich die Praxen zwar beraten, aber nicht in den Bereich der anderen eindringen dürfen. Die Ökonomie strebt – auch im Bildungssektor – eine Gewinnmaximierung an: Aber im Bereich der Pädagogik geht es eben um Bildung und nicht um Gewinne. Dem Gewinnstreben der Konzerne kann nur Einhalt geboten werden, wenn die Zuschüsse, die der DigitalPakt Schule in Aussicht stellt, auch zielführend eingesetzt werden. Zu ebenjenem Schluss müssen auch die Erfinder des DigitalPakts gekommen sein, da einzelne Schulen ausschließlich dann Zuschüsse für ihre digitale Infrastruktur erhalten, wenn ein spezielles pädagogisches Konzept ausgearbeitet vorliegt (BMBF 2019). Gerade eine pädagogische Einbettung in den Schulalltag ist notwendig, damit der Einsatz der digitalen Medien die Hoffnung erfüllen kann, die man in sie setzt.

Gelungene Beispiele und Forschungsagenda

Schaumburg und Prasse (2019, S. 174) weisen den Digitalen Medien folgende Funktionen für das Unterrichten zu: „Motivieren, Präsentieren und Veranschaulichen, Aktivieren und Vertiefen, Differenzieren und Individualisieren, Kommunizieren und Kooperieren“. In Verbindung mit den Forschungsergebnissen des Schul- und Unterrichtsforschers John Hattie lassen sich einige Hinweise für den Einsatz digitaler Medien geben.

Hierunter fällt bspw. der oftmals vernachlässigte Bereich des bewussten Übens. Hattie stellt dies in seiner Studie *Visible Learning* klar heraus. „Auch wenn viele Lernende immer wieder glauben, alles sofort zu können: Es gehört zu den ältesten didaktischen Einsichten, dass Übung für Lernerfolg notwendig ist“ (zitiert in Zierer 2016, S. 68). *Bewusstes Üben* hat eine vergleichsweise hohe Effektstärke von 0,71[4] (ebd., S. 69). Allen Lernenden lassen sich durch ein Tablet individualisierte Übungsaufgaben für genau den Bereich zuweisen, in dem die Lehrpersonen Defizite erkannt haben. Den Einfluss der digitalen Medien sollte man an dieser Stelle allerdings nicht überschätzen: Es kommt immer auch auf das Niveau der Übungen an, dagegen kann man den Bereich des Problemlösens, des Synthetisierens und Bewertens von Aufgaben schwierig abbilden.

Digitale Medien können ebenso im Bereich der Evaluation eingesetzt werden. Hattie stellt „Feedback als Schüssel eines erfolgreichen Unterrichts“ (Hattie und Zierer 2018, S. 147) heraus. Es „gehört zu den am besten erforschten Methoden überhaupt und zieht einen der größten Einflüsse auf die Lernleistung nach sich: Allein 25 Meta-Analysen in den letzten 20 Jahren mit einer durchschnittlichen Effektstärke von 0,75 konnten in »Visible Learning« ausfindig gemacht werden“ (Hattie und Zierer 2018, S. 147). Feedback kann allerdings nur die Lehrperson geben, die zuvor evaluiert hat, was die Lernenden zu leisten im Stande sind und welche Hilfestellung sie noch benötigen. Für die Erhebung von Daten lassen sich Tablets mit speziellen Applikationen sinnvoll einsetzen.

4 „Das Ausweisen einer Effektstärke ist eine nützliche Methode, um Resultate über verschiedene Messzeitpunkte (wie standardisierte, von Lehrpersonen erstellte Tests, Schülerarbeiten) oder über Zeitpunkte oder zwischen Gruppen auf einer Skala miteinander zu vergleichen, die – unabhängig von den ursprünglichen Test-Scores – mehrere Vergleiche ermöglicht (z. B. x Punkte von 10 oder 100), und zwar über Inhalte und über Zeitpunkte hinweg. Diese unabhängige Skala ist eine der wichtigsten Vorzüge der Verwendung von Effektstärken, da sie relative Vergleiche über verschiedene beitragende Faktoren zur Schülerleistung ermöglicht“ (Hattie 2016, S. 3). Hattie bezeichnet eine Effektstärke größer als 0,4 als Umschlagpunkt. „Alle Einflüsse oberhalb des U-Punktes (d = 0,40) werden in der Zone „Erwünschte Effekte“ ausgewiesen, da dies diejenigen Einflüsse sind, welche die größte Auswirkung auf Lernleistungs-Outcomes der Schülerinnen und Schüler haben“ (Hattie 2013, S. 23).

Ebenso sollte sich die Schulforschung mit den Schattenseiten der Digitalisierung eingehend beschäftigen. Forschungsbedarf besteht im Bereich der Medienpädagogik, der als Oberbegriff u. a. die Subdisziplinen der Medien*didaktik* und der Medien*erziehung* subsummiert. Im Bereich der Medien*didaktik*, der Unterrichtsmodelle wie Fortbildungen umfasst, gibt es schon vielversprechende Ansätze (Schaumburg und Prasse 2019). Es ist weiterhin notwendig, dass Unterrichtsmodelle für die Nutzung digitaler Medien erstellt werden, auf die Lehrpersonen zurückgreifen können und es bedarf weiterer Fortbildungen. Der Medien*erziehung* kommt eine enorm wichtige Aufgabe zu. Hierunter fallen auch die Teilbereiche der Medien*nutzung* und der Medien*kritik*. Diesen Gebieten wird in Zukunft eine noch größere Bedeutung beigemessen werden müssen. Die Medien*nutzung* beschäftigt sich mit dem Konsumverhalten der Kinder und Jugendlichen und könnte in diesem Kontext disziplinübergreifend mit der Verhaltenspsychologie zusammenarbeiten. Es geht hierbei u. a. darum, die Bildschirmzeiten der Kinder und Jugendlichen im Blick zu behalten und ein erträgliches bzw. zumutbares Maß auszutarieren. Im Teilbereich der Medien*kritik* ist es wichtig, dass die Heranwachsenden lernen, sich von digitalen Medien so zu emanzipieren, dass sie keine pathologische *Smartphonesucht* entwickeln, wie Spitzer befürchtet.

In diesen Forschungsgebieten bietet sich der Erziehungswissenschaft in Kooperation mit zum Beispiel der Lernpsychologie und der Lehr-Lernforschung die Möglichkeit, disziplin- und fächerübergreifende Überlegungen zum Thema Technikfolgenabschätzung der Digitalisierung im Unterricht anzuregen.

Literatur

Benner, Dietrich (2015): Allgemeine Pädagogik. Eine systematisch-problemgeschichtliche Einführung in die Grundstruktur pädagogischen Denkens und Handelns. Weinheim: Beltz Juventa.

BMBF – Bundesministerium für Bildung und Forschung (2019): DigitalPakt Schule. Online verfügbar unter https://www.bmbf.de/de/wissenswertes-zum-digitalpakt-schule-6496.html, zuletzt geprüft am 22. 03. 2019.

Böhm, Winfried; Seichter, Sabine (2018): Wörterbuch der Pädagogik. Paderborn: Ferdinand Schöningh.

Fend, Helmut (2008): Theorie der Schule. Einführung in das Verstehen von Bildungssystemen. Wiesbaden: VS Verlag für Sozialwissenschaften.

Gutbrod, Johannes (2018): Schule und Gemeinschaft. Eine problemhistorische Rekonstruktion. Berlin: Peter Lang Verlag.

Hattie, John (2013): Lernen sichtbar machen. Überarbeitete deutschsprachige Ausgabe von „Visible Learning for Teachers" besorgt von Wolfgang Beywl und Klaus Zierer. Baltmannsweiler: Schneider Verlag Hohengehren.

Hattie, John (2016): Lernen sichtbar machen für Lehrpersonen. Überarbeitete deutschsprachige Ausgabe von »Visible Learning for Teachers« besorgt von Wolfgang Beywl und Klaus Zierer. Baltmannsweiler: Schneider Verlag Hohengehren.

Hattie, John; Zierer, Klaus (2018): Kenne deinen Einfluss! »Visible Learning« für die Unterrichtspraxis. Baltmannsweiler: Schneider Verlag Hohengehren.

Kambartel, Friedrich; Welter, Rüdiger (1980): Methode. In: Jörg Ritter und Karlfried Gründer (Hg.): Historisches Lexikon der Philosophie. Band 5. Stuttgart: Schwabe, S. 1304–1332.

Ladenthin, Volker (2018): Methoden des Pädagogikunterrichts. Münster: Waxmann.

Pöppel, Karl-Gerhard (1992): Unterrichten. Grundzüge und Gestaltungsformen des Lehrens und Lernens. Hildesheim: Georg Olms Verlag.

Rekus, Jürgen; Mikhail, Thomas (2013): Neues schulpädagogisches Wörterbuch. Weinheim: Beltz Juventa.

Schaumburg, Heike; Prasse, Doreen (2019): Medien und Schule. Theorie – Forschung – Praxis. Bad Heilbrunn: Julius Klinkhardt.

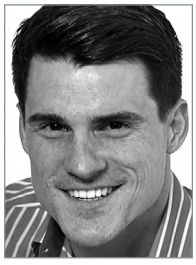
Spitzer, Manfred (2012): Digitale Demenz. Wie wir uns und unsere Kinder um den Verstand bringen. München: Droemer.

Spitzer, Mandfred (2018): Die Smartphone-Epidemie. Gefahren für Gesundheit, Bildung und Gesellschaft. Stuttgart: Klett-Cotta.

Tenorth, Heinz-Elmar; Tippelt, Rudolf (2007): Lexikon Pädagogik. Weinheim: Beltz.

Zierer, Klaus (2017): Lernen 4.0. Pädagogik vor Technik. Möglichkeiten und Grenzen einer Digitalisierung im Bildungsbereich. Baltmannsweiler: Schneider Verlag Hohengehren.

Zierer, Klaus (2016): Hattie für gestresste Lehrer. Kernbotschaften und Handlungsempfehlungen aus John Hatties »Visible Learning« und »Visible Learning for Teachers«. Baltmannsweiler: Schneider Verlag Hohengehren.



DR. JOHANNES GUTBROD

studierte Germanistik, Geografie, Sportwissenschaften und Pädagogik am Karlsruher Institut für Technologie (KIT). Derzeit arbeitet er als Lehrer sowie als wissenschaftlicher Mitarbeiter am KIT.

Vom Boulevard zum Umweltschutz

»Wenn ich es schaffe, dann schafft es jede(r)!«

Janine Steeger

Klimafreundlich reisen, abfallfrei einkaufen, bio essen, Energie sparen – wo soll ein normaler Mensch nur anfangen, wenn er nachhaltiger leben will? Vor dieser Herausforderung stand auch die RTL-Explosiv-Moderatorin Janine Steeger, als sie 2011 ihren Weg ins grüne Leben begann. Authentisch, ehrlich und mit viel Humor erzählt sie von den Hindernissen, Konflikten und wunderbaren Erlebnissen.

Janine Steeger

Going Green

Warum man nicht perfekt sein muss, um das Klima zu schützen

oekom verlag, München
176 Seiten, Klappenbroschur, 16 Euro
ISBN: 978-3-96238-176-9
Erscheinungstermin: 04.02.2020
Auch als E-Book erhältlich

oekom.de

DIE GUTEN SEITEN DER ZUKUNFT

oekom

DIE ZUKUNFT DES WIRTSCHAFTENS BEGINNT JETZT!

Die Zeitschrift Ökologisches Wirtschaften schließt die Lücke zwischen Theorie und Praxis einer nachhaltigen Gestaltung der Wirtschaft.

GÜNSTIGES PROBEABO

Zwei Ausgaben für nur 19,– Euro statt 37,50 Euro (inkl. Versand in Dtl.)

Bestellung an: abo@oekom.de

Herausgegeben von Institut und Vereinigung für ökologische Wirtschaftsforschung (IÖW und VÖW).

JETZT PROBEABO ANFORDERN!

Leseproben, Informationen zur Zeitschrift und Abobedingungen:

www.oekologisches-wirtschaften.de

oekom verlag

INTERVIEW

Wissenschaft und politische Beratung

Ein Gespräch mit E. D. Rossmann (MdB) über Komplexität, politische Entscheidungen und Technikfolgenabschätzung im Bundestag

Gesellschaftliche Transformationsprozesse stellen Wissenschaft und Politik gleichermaßen vor Herausforderungen. Damit ergeben sich neue und immer komplexere Anforderungen an die Technikfolgenabschätzung (TA) als wissenschaftliche und politikberatende Praxis. Ernst Dieter Rossmann, Vorsitzender des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung, spricht über veränderte Ansprüche an die TA, ihre Rolle in der Demokratie und die Praxis am Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB).

TATuP: *Welcher gesellschaftliche Transformationsprozess ist für Sie zentral und was ist nötig, um diesen Wandel voranzubringen?*

Ernst Dieter Rossmann: Um in das ganz große Fach zu greifen: Das Ziel des gesellschaftlichen Transformationsprozesses – der dann auch immer ein ökonomischer, kultureller und politischer Transformationsprozess sein muss – ist für mich, jetzt die Grundlagen dafür zu legen, das zum Ende dieses Jahrhunderts voraussichtlich 10 bis 11 Milliarden Menschen friedlich, frei und glücklich und im Einklang mit der Natur auf unserem Planeten leben können. Und wenn das unser Jahrhundertziel ist, ist auch der Weg dahin nicht ohne Bedeutung. Auch der Prozess ist ein Ziel. Denn er muss friedlich, demokratisch und gerecht erfolgen. Dafür müssen auch die kleinen Schritte auf dem Weg zum großen Ziel verstehbar dargestellt werden und gestaltet werden können. Dieser Prozess muss damit einen konkreten Zuwachs an Lebenssicherheit und Lebensqualität mit sich bringen.

Was erwarten politische Entscheidungsträger vonseiten der Wissenschaft?

An erster Stelle natürlich hervorragende Forschung – mit einem wirksamen Zuwachs an neuen Erkenntnissen, mit Relevanz schon von der Fragestellung her, unabhängig davon, ob es sich um fundamentale Grundlagenforschung oder um anwendungsorientierte Forschung handelt. Außerdem sollte eine Einordnung der Erkenntnisse in den bisherigen Wissensstand und in die weiteren Forschungsperspektiven vorgenommen werden, mit einer fächer- und disziplinenübergreifenden Orientierung und mit der Bereitschaft und Freude an der Vermittlung dieser Erkenntnisse im System der Forschung und der Wissenschaft selbst, aber genauso in den anderen Systemen wie z. B. der Wirtschaft, der Verwaltung, den Medien und den zivilgesellschaftliche Organisationen im Konkreten und der Öffentlichkeit im Allgemeinen. Und die Wissenschaft kann sehr viel in der Entwicklung von Konzepten zur Transformation in den verschiedensten Bereichen beitragen. Sie kann Entwicklungspfade und Alternativen aufzeigen und sich theoretisch wie praktisch bis hin zur sogenannten Dritten Dimension, also zur handlungsbezogenen Forschung und der Bürgerwissenschaft, selbst einbringen. Elfenbeinturm ist Geschichte und muss es bleiben.

Politische Entscheidungsträger erwarten von der Wissenschaft eine Art Dienstleistung als Aufklärung, als Erklärung und als Beratung. Die wissenschaftlichen Partner sollten für Dialogbereitschaft und Dialogfähigkeit stehen, als Stimme des Zweifels und der Orientierung, als Warnung und als Hoffnung. Und wir dürfen Neugierde und Offenheit gegenüber dem System demokratischer Politik erwarten, Selbstdistanz, Respekt und auch Empathie gegenüber den Entscheidungsträgern, d. h., den Volksvertretern und deren besonderer Legitimation durch die demokratische Wahl. Knapp gesagt: Es braucht wechselseitigen Respekt.

Gibt es da grundsätzliche System-Unterschiede zwischen Politik und Wissenschaft?

Politiker sind dazu beauftragt, sprich gewählt, ständig und immer wieder demokratisch neu Prioritäten zu setzen, Ressourcen zu verteilen, Regeln zu definieren, Gesetze zu machen. Und dies vor dem Hintergrund ihrer politischen Ziele und Werte und im Kontext von Parteien, Mehrheiten und Kompromissen. Im Spannungsfeld mit den vier Polen von Wahrheiten und Wahrhaftigkeit, von Werten und Interessen, bewegt sich die Wissenschaft vorrangig auf der Ebene von Wahrheiten und Wahrhaftigkeit. In der Politik kommt eine ganz starke Erweiterung um die Dimension der Werte und Interessen dazu. Die Begrenztheit von Ressourcen und Kapazitäten zwingt die Politik dabei ständig in die Entscheidung über Prioritäten und Posterioritäten und in die Bewertung von Aufwand und Ertrag, von realisierter Effizienz und wahrscheinlicher Perspektive. Politische Entscheidungen sind damit auch immer Risikoentscheidungen.

Was heißt das für die Dialogfähigkeit?

Wissenschaft und Forschung werden dieses aus ihrer Perspektive als Einschränkung und Kontrolle erleben können und müssen. Umso zwingender ist es, dass

https://doi.org/10.14512/tatup.29.1.52

sich beide Systeme argumentativ umfassend und kooperativ erklären. Umso wichtiger ist es, dass es einen ganz intensiven direkten oder indirekten Austausch von Wissenschaft und Politik gibt. Und umso wünschenswerter ist es schließlich, dass es auch einen personellen Austausch von Wissenschaft in Politik und umgekehrt gibt. Konkret: Der Deutsche Bundestag hat deutlich zu wenig ausgewiesene Wissenschaftler in seinen Reihen – von der personellen Repräsentanz des Systems Wissenschaft insgesamt, aber auch der Diversität der wissenschaftlichen Fach- und Management-Kompetenzen.

Geht es eher um Expertise bezüglich bestimmter Technikfelder oder auch um Expertise bezüglich der Gestaltung der eigentlichen Transformationsprozesse?

Die Expertise ist in allen wissenschaftlichen Feldern notwendig und wünschenswert, und nicht nur in den Technikfeldern, auch wenn diese natürlich wegen der technologischen Innovation und der daran anknüpfenden Technikfolgenabschätzung besonders im Fokus stehen. Vertreter aus dem Bereich der Lebenswissenschaften, der Sozialwissenschaft, der Kulturwissenschaft etc. sind hier unverzichtbar im Diskurs zur Technikfolgenabschätzung und deren Ableitungen mit Blick auf die Transformation. Nicht-technologieaffine Wissenschaften sind dabei aber genauso gefordert, angesichts gravierender nicht nur technologieinduzierter Umbrüche wie demografischen Veränderungen, Migration, Interreligiosität und Interkulturalität bzw. superkomplexer Herausforderungen wie dem Klimawandel.

Dass diese Umbrüche auch technologische Anforderungen hervorrufen, zeigt nur auf, wie die Komplexität der Probleme mit der Komplexität der Wissenschaft verbunden ist. Wir brauchen letztlich nicht nur eine Technikfolgenabschätzung, sondern genauso auch eine Technikbedarfsabschätzung. Damit sind wir dann auch mittendrin in der Frage nach der Transformation und deren Gestaltung. Technologien sind nicht zu trennen von den Implikationen ihrer Anwendung im Prozess hin zur gesellschaftlichen Transformation. Gesellschaftliche Probleme verlangen nach einem Prozess der Transformation in den Technologien und in ihrem wissenschaftlichen Vorfeld. Gute Technikfolgenabschätzung war schon immer Prozess-Gestaltungsexpertise und wird zukünftig noch mehr Technologie-Bedarfsexpertise einschließen.

Gute Technikfolgenabschätzung war schon immer Prozess-Gestaltungsexpertise und wird zukünftig noch mehr Technologie-Bedarfs-expertise einschließen.

Verschiebt sich da womöglich etwas? Etwa in Bezug auf die Aufgabenstellung und Arbeit der Technikfolgenabschätzung?

Diese Expertise hat in gewisser Weise schon immer zu einer guten Technikfolgenabschätzung dazu gehört, was die Handlungsoptionen und Pfadalternativen angeht. In Enquete-Kommissionen, die Institutionen der Technikfolgenabschätzung auf Zeit sind, arbeiten Wissenschaftler, Experten und politische Mandatsträger genauso zusammen wie beim Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB), dessen wissenschaftliche Berichte und Einschätzungen von den Abgeordneten abgenommen, eingeordnet und auch kommentiert werden.

Dr. Ernst Dieter Rossmann

ist Vorsitzender des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung. Seit 1998 ist er Mitglied der SPD-Fraktion im Deutschen Bundestag.

[Bildquelle: Susie Knoll]

Allerdings verläuft Prozessgestaltung in der Transformation ja in verschiedenen Phasen. Auf die Technikfolgenabschätzung im engeren Sinne folgen im Transformationsprozess eine Analyse des Technologieumfeldes und der Gestaltungsmöglichkeiten und eine Bündelung in Gestaltungspfaden und Optionen. Danach folgen eine Entscheidung über die Handlungsoptionen und schließlich eine Vermittlungs- und Umsetzungsphase. Ist am Anfang noch die Wissenschaft von besonderer Kompetenz, steht am Ende dieses idealtypischen Phasenmodells die Politik in der besonderen Verantwortung und Handlungsmächtigkeit. Allerdings ist dieses ja kein linearer Prozess, sondern es gibt hierin immer wieder Rückkopplungen und Evaluationen. Nun ist die Umsetzung in der Regel nicht nur ein rein politischer Prozess der Entscheidungen über Gesetze, Haushaltsressourcen und Institutionen etc., dazu gehören auch die ständige Kommunikation sowie Vermittlungs- und Vernetzungsaufgaben in alle anderen Bereiche in Gesellschaft, Wirtschaft, Kultur und Bildung. Dabei ist die Wissenschaft dann wieder zentral gefordert.

Wie verhalten sich Gestaltungsexpertise und demokratische Legitimität zu einander?

Einerseits gilt: Weil die Probleme der Zukunft, aber vor allen Dingen die Hand-

lungsoptionen in ihrer Komplexität mehr wissenschaftliche Expertise erfordern, kommt der Prozess-Gestaltungsexpertise eine zunehmende Bedeutung zu. Andererseits ist glasklar zu sagen: In der Umsetzungsexpertise und der Gestaltungsmacht ist die demokratisch legitimierte Politik in der Vorhand und sie muss es auch bleiben. Gefragt sind also weder ein Staat der weisen Männer à la Platon noch ein Staat der multikompetenten und allzeitdisponiblen Technokraten und Experten noch eine politische Autokratie mit diktatorischen Durchgriffsmöglichkeiten, sondern die gut beratenen, sorgfältig beratenden und voll verantwortlichen demokratischen Parlamente und ihre Regierungen. Diese haben den Auftrag und die Verantwortung zur Gestaltung dieser Prozesse. Sie müssen sich immer wieder der demokratischen Bewertung und Entscheidung über ihre Gestaltungsmacht durch das Volk stellen. Dies kann umständlich und widersprüchlich sein, so wie Demokratie auch langsam und aufwendig im Prozess sein kann, aber hoffentlich geleitet durch klare Werte und in der Auseinandersetzung mit bester Expertise und jedenfalls immer mit demokratischer Legitimation. Da dürfen die Volksvertreter sehr selbstbewusst sein und müssen es auch bleiben.

Demokratischen Parlamente und ihre Regierungen haben den Auftrag und die Verantwortung zur Gestaltung der Transformationsprozesse.

Wieviel Normativität steht der TA gut zu Gesicht, wieviel Neutralität?

Die Relativität von Wahrheit hat die Wissenschaft beschäftigt, solange es Wissenschaft gibt. Von Philosophen bis zu den Physikern, von Poppers Theorem der Falsifikation bis zur Unschärferelation von Heisenberg. Die zwingende Verbindung der Relativität von Wahrheit mit der Notwendigkeit von Wahrhaftigkeit im Auftreten und Handeln von Wissenschaft muss natürlich in die wissenschaftliche Dimension von Technikfolgenabschätzung hineinreichen und ist hierfür genauso existenziell wie in allen anderen Bereichen, in denen Wissenschaft gefordert ist. Nur bei den Folgen, die immer auf die Zukunft ausgelegt sind und die damit immer etwas potenziell Offenes in sich haben, geht es dann nicht nur um Wahrheiten und Wahrhaftigkeit, sondern eben primär auch um Werte und Interessen.

Gute Technikfolgenabschätzung ist an dieser Stelle hilfreich bei der Entwicklung von Handlungsoptionen, gibt es doch schon quasi axiomatisch Alternativen, und sei es die Alternative von Handeln und „Nicht-Handeln" – ganz im Sinne des einschlägigen Paradoxons des Philosophen und Kommunikationswissenschaftlers Paul Watzlawick, das Menschen nicht Nicht-Kommunizieren, also nicht Nicht-Handeln können. Gute Technikfolgenabschätzung macht dann die Voraussetzungen und Implikationen an Werten und damit verbundenen möglichen Interessen und Interessenkonflikten transparent – und damit diskutierbar und gegebenenfalls auch streitig entscheidbar.

Ist Neutralität schon gewahrt, wenn keine Eigeninteressen der TA-Akteure im Spiel sind, oder sollte es auch um „Wertneutralität" gehen?

Neutralität von Wissenschaft und Technikfolgenabschätzung beweist sich in dieser Transparenz, in der Entfaltung der möglichen Optionen und deren Priorisierung. Das gilt für die Transparenz von realen oder potenziellen Eigeninteressen, die damit kritisch einordbar werden, genauso wie für die Offenlegung von eigenen Werten und Haltungen, soweit sie von Relevanz für den Beratungs- und Begleitungsprozess der Technikfolgenabschätzung und der Transformation sind. Wer Werte mit Selbstdistanz verbinden kann, darf für sich besondere Professionalität und Glaubwürdigkeit in diesem Beratungsprozess geltend machen. Wer für sich auf Wertneutralität besteht, gerät in den Verdacht, über den Wertebezug von Handeln nicht gründlich genug reflektiert zu haben und mit „kalter" Technokratie eben schon wieder Neutralität zu den Problemen und ihren Lösungen zum Wert zu erheben. Entscheidend sind die Erklärung der eigenen Voraussetzungen und die Offenlegung und das Herausarbeiten von Implikationen an Werten und Interessen, sodass die Verantwortlichen im Prozess zu besseren eigenen Entscheidungen kommen können.

Welchen Transformationsprozessen ist die TA-/Wissenschafts-Szene selbst aktuell unterworfen? Welche Transformationsziele soll sie sich womöglich selbst setzen? Welche Rahmenbedingungen braucht sie dafür?

Ich muss und will mich auf drei Beobachtungen zu jenem Teil der TA-Szene beschränken, der im und für den Bundestag und damit an sehr exponierter Stelle arbeitet.

Erstens werden die Aufgabenstellungen, zu denen die Abgeordneten um Begutachtung und Beratung bitten, immer vielfältiger. Es geht um die ganze Breite der hochtechnologiegeleiteten Innovationen, Fragestellungen zu ökonomisch-ökologischen Transformationen genauso wie um soziale Transformationen. Die Leitung des TAB hat die komplexe Aufgabenstellung kürzlich mit den Leitbegriffen der Informationsfunktion, der Radarfunktion, der Orientierungsfunktion, der Dialogfunktion und der Vernetzungsfunktion umschrieben.

Zweitens werden dazu entsprechend auch die Umstände und die „Produkte" immer vielfältiger. So ist die politische Beratung zur Technikfolgenabschätzung im Deutschen Bundestag und ihre Be-

auftragung über die klassische Form der Erstellung eines umfangreichen Berichts mit Empfehlungen zu spezifischen Fragestellungen hinaus in ganz verschiedenen, weit gefächerten Berichten und zur Entwicklung von Optionen statt Empfehlungen erweitert worden. Hinzu kommen sehr kurze Problemaufrisse, im Sinne von Kurzprofilen, die die Abgeordneten bei ihrem Themenfindungsprozess unterstützen sollen und die gleichzeitig als Informationsquellen für deren alltägliche parlamentarische Arbeit genutzt werden können. Diese Kurzprofile sind eingebettet in das Gesamtkonzept eines Horizont-Scannings als Instrument zur Technologievorausschau und zur strategischen Früherkennung wissenschaftlich-technischer und sozioökonomischer Entwicklungen und Themen. Sie sollen einen Beitrag zur forschungs- und innovationspolitischen Orientierung und Meinungsbildung der zuständigen und interessierten Parlamentarier leisten: Schließlich hat sich das Aufgabenportfolio um den organisierten Dialog mit gesellschaftlichen Akteuren und öffentlichen Forschungsveranstaltungen im Deutschen Bundestag erweitert.

Drittens wird die Dimension der Wissenschaftskommunikation immer wichtiger, je mehr politische Entscheidungen sich auf Fragen der Ökologie, des Klimas, der Ressourcen, Werkstoffe und Materialen, der Genetik und der Bioökonomie beziehen. Hier muss sich Wissenschaft verständlich machen können gegenüber Politikern wie Medien, gegenüber der weiteren Öffentlichkeit wie den einzelnen Menschen. Das gilt erst recht für die Institutionen der Technikfolgenabschätzung und der Politikberatung in diesen Fragen. Mit deren besonderem Auftrag muss sich eine besondere Kompetenz in der Kommunikation verbinden. Die Akteure der Technikfolgenabschätzung können und müssen auch Wegbereiter zur guten Wissenschaftskommunikation sein. Sie müssen wissenschaftliche Wahrheiten in ihrer Relativität erklären und politische Implikationen und Optionen in ihren letztlich werte- und interessenbezogenen Implikationen darlegen können.

Was sehen Sie da als TA-Markenzeichen für die Zukunft?

Um diesen Ansprüchen gerecht zu werden, braucht es verlässliche Strukturen und Finanzen, Unabhängigkeit von Wirtschaftsunternehmen und anderen Interessenszusammenschlüssen, Selbstdistanz des Staates und Selbstbeschränkungen der Einrichtungen zur Technikfolgenabschätzung. Sie dürfen weder Unternehmen noch Think-tanks noch reine Forschungseinrichtungen sein wollen. Und sie sind es auch nicht. Sie haben andere Markenzeichen. Sie sind wissenschaftlich ausgewiesen und von Wissenschaft geprägt, unabhängig und auf Zeit beauftragt. Sie arbeiten an der Nahtstelle von Wissenschaft, Gesellschaft und Politik. Sie sind nicht die Macher von Erkenntnissen, Optionen und Prozessen, sondern deren ehrliche und kritische Makler. Das ist ihr Beitrag zu den notwendigen und wünschenswerten Transformationen, die vor uns liegen.

Wenn Voraussetzungen, Implikationen, Werte und Interessen von wissenschaftlicher Expertise offengelegt werden, kommt es zu besseren Entscheidungen in der Politik.

Das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) ist eine selbstständige wissenschaftliche Einrichtung, die den Deutschen Bundestag und seine Ausschüsse in Fragen des wissenschaftlich-technischen Wandels berät. Es wird seit 1990 vom Institut für Technikfolgenabschätzung und Systemanalyse (ITAS) des Karlsruher Instituts für Technologie (KIT) betrieben. Steuerungsgremium des TAB ist der Bundestagsausschuss für Bildung, Forschung und Technikfolgenabschätzung, dessen Vorsitzender Dr. Ernst Dieter Rossmann (SPD) ist. Seit 2013 kooperiert das ITAS/KIT bei der Betreibung des TAB mit dem IZT – Institut für Zukunftsstudien und Technologiebewertung gGmbH und der VDI/VDE Innovation + Technik GmbH.

Obwohl vom Bundestag als Auftraggeber finanziert, hat die wissenschaftliche Unabhängigkeit des TAB eine hohe und grundlegende Bedeutung. Alle Fraktionen müssen sich einstimmig auf ein Arbeitsprogramm für das TAB einigen und auch die Arbeitsergebnisse im Konsens abnehmen, bevor diese in die politische Debatte einfließen. Aktuelle Projekte und Publikationen des TAB finden sich unter http://www.tab-beim-bundestag.de.

BERICHT

Soziale Innovation in der digitalen Transformation

Daniel Krüger, *Sozialforschungsstelle, TU Dortmund, Evinger Platz 17, 44339 Dortmund (daniel2.krueger@tu-dortmund.de), https://orcid.org/0000-0002-3550-5629*
Rick Hölsgens, *Sozialforschungsstelle, TU Dortmund (henricus.hoelsgens@tu-dortmund.de), https://orcid.org/0000-0002-0408-4438*
Marthe Zirngiebl, *Sozialforschungsstelle, TU Dortmund (marthe.zirngiebl@tu-dortmund.de), https://orcid.org/0000-0001-7999-157X*

Der Diskurs um Digitalisierung und digitale Transformation zieht sich durch viele wissenschaftliche Disziplinen. Auch die internationale Forschungsgemeinde zu sozialer Innovation hat das Thema längst aufgegriffen, ist technologisch bedingter Wandel doch stark mit gesellschaftlichen Veränderungen verknüpft und wird zugleich aktiv durch die Gesellschaft gestaltet. Soziale Innovation wird definiert als „intentionale, zielgerichtete Neukonfiguration sozialer Praktiken in bestimmten Handlungsfeldern bzw. sozialen Kontexten, mit dem Ziel, Probleme oder Bedürfnisse besser zu lösen bzw. zu befriedigen, als dies auf der Grundlage etablierter Praktiken möglich ist“ (Howaldt und Schwarz 2010, S. 89). Sie lässt sich nicht nur in der Verbreitung und Anwendung von Technologien beobachten, zuweilen wird sie durch neue Technologien erst ermöglicht oder beantwortet gesellschaftliche Herausforderungen, die infolge technologischer Innovationen entstanden sind. Zu diesen Themen veranstalteten am 28. 10. und 29. 10. 2019 in Dortmund die European School of Social Innovation (ESSI) zusammen mit der TU Dortmund und der DASA Arbeitsweltausstellung die fünfte Global Research Conference „Social innovation and socio-digital transformation. Towards a comprehensive innovation policy“. Die Autor*innen dieses Berichts waren in Organisation und Durchführung involviert.

Obgleich die Veranstaltung einen Forschungsfokus hatte, konnte sie einen transdisziplinären Anspruch erfüllen und begrüßte neben zahlreichen Wissenschaftler*innen auch Vertreter*innen aus der Praxis. So diskutierten mehr als 200 internationale Expert*innen in drei übergreifenden Sessions und zwölf parallelen Workshops unterschiedliche Aspekte des Themas. Das Programm wurde dabei durch die Präsentation der zweiten Auflage des Atlas of Social Innovation (Howaldt et al. 2019) bereichert, der mit einer Sammlung von mehr als 40 Artikeln internationaler Expert*innen viele Themen der Konferenz behandelt.

Spannungsverhältnisse und neue Narrative

In der eröffnenden Keynote von Geoff Mulgan zeigte sich, dass das Verhältnis zwischen technologischer und sozialer Innovation nicht nur durch Potenziale geprägt ist. Konkret bemängelte er, dass Forschung zu sozialer Innovation mit gewinnorientierter Forschung konkurriere und soziale Themen einer höheren Priorisierung bedürften. Obwohl soziale Innovation inzwischen als eigenständige Innovationsform anerkannt werde, spiegele sich dies nicht in der Forschungsgeldverteilung wieder. So rief Mulgan zu mehr politischem Engagement auf, um die Rolle sozialer Innovation zu stärken. Das Verhältnis zwischen verschiedenen Innovationsformen stand auch im Fokus der umfassenden historischen Analyse von Benoît Godin. Er stellte fest, dass der Diskurs um Innovation seit den 1950er- und 1960er-Jahren durch das Aufkommen stärker differenzierter Innovationstypen geprägt sei. Im Kontext dieser semantischen Pluralisierung (zusammengefasst: „X-Innovationen“) konkurriere soziale Innovation daher mit anderen Innovationstypen (z. B.: ökologische Innovation). Godin benannte Pfade, wie sich soziale Innovation durchsetzen könne. Demnach müsse sie entweder den Mainstream aufgreifen und offener für wirtschaftliche Interessen werden oder völlig neuartige Ansätze verfolgen und etablieren.

Jürgen Howaldt plädierte für eine stärkere Rolle sozialer Innovation in Wissenschaft und Politik – und damit implizit auch für eine Rolle jenseits von X-Innovationen. Er betonte zugleich die Bedeutung veränderter Narrative und Theorien des Wandels, welche die Bedeutung veränderter Praktiken anerkennen müssten und schloss seinen Vortrag mit einer konkreten Forderung: Zu Beginn des 21. Jahrhunderts werde auf der Suche nach neuen sozialen Praktiken ein Pioniergeist benötigt, der auf diese Weise eine Sicherung der Zukunft möglich mache und allen Menschen ein reicheres und erfüllendes Leben ermögliche.

In seinem Vortrag zur Rolle von sozialer Innovation in Prozessen sozialer Transformation ging Lars Hulgård auf die theoretischen Wurzeln der wissenschaftlichen Diskussion um soziale Innovation ein. Er betonte die große Bedeutung sozialtheoretisch fundierter Konzepte sozialen Wandels und illustrierte deren Erklärungskraft am Beispiel von Max Webers protestantischer Ethik. Obgleich die Eignung des Praxisbegriffs für die Theorie sozialer Innovation durch Elizabeth Shove aus einer sozialtheoretischen Perspektive durchaus kritisch hinterfragt wurde, sind es letztlich Perspektiven auf soziale Prozesse, die ein tieferes Verständnis von Wandel zulassen, als es ein technozentrischer Blick erlauben würde.

Folgen von Innovationen und Lösungen

Mit seiner Forderung, soziale Innovation müsse „grün“ werden, betonte Philippe Martin, Mitglied des DG Research and Innovation der EU Kommission und Leiter der Social Innovation Task-

https://doi.org/10.14512/tatup.29.1.56

force, die Bedeutung sozialer Innovation für die Begegnung zentraler gesellschaftlicher Herausforderungen. Damit schlug er implizit auch einen Bogen zu den klima- und umweltrelevanten Folgen von Technik und verstand soziale Innovation als Ansatz, diesen zu begegnen.

Neben den Potenzialen sozialer Innovationen, um den Folgen technologischer Innovationen zu begegnen, wie beispielsweise dem Klimawandel, gilt es jedoch auch, die Risiken sozialer Innovationen selbst zu berücksichtigen. Genauso wie technologische Innovationen können auch diese nicht-intendierte Folgen haben. Während Johan Schot forderte, Innovationspolitik müsse die transformative Wirkung von Innovationen fördern, unterstrich Flor Avelino, dass soziale Innovationen mit transformativer Wirkung auch Risiken beinhalten könnten. Zwar suchten transformative soziale Innovationen bestehende problematische Strukturen zu transformieren, allerdings könnten sie diese im Gegenteil sogar reproduzieren, wenn sie im Zuge ihrer Verbreitung an diese angepasst würden.

Das 21. Jahrhundert erfordert neue soziale Praktiken, welche die Zukunft sichern und allen Menschen ein reicheres und erfüllendes Leben ermöglichen!

Wechselbeziehungen technologischer und sozialer Innovationen

Das Verhältnis zwischen sozialen Innovationen und technologischen Innovationen wurde nicht nur in Bezug auf Risiken und Spannungsverhältnisse beleuchtet. Vielmehr betonten zahlreiche Vortragende die Potenziale. So hob Johan Schot hervor, dass tiefgreifender Wandel (wie die digitale Transformation) einen Rahmen benötigten, den Technologien bieten könnten. Wenn Schot dies auch nicht explizit äußerte, lässt sich daraus doch schließen, dass digitalen Innovationen durchaus auch eine Rolle als Multiplikator sozialer Innovationen zukommen kann. In der Praxis zeigt sich dies Beispielsweise in der Verwendung von Internetplattformen.

Die Frage nach den gegenseitigen Potenzialen digitaler Innovationen und sozialer Innovationen wurde anhand konkreter Beispiele und Praxiserfahrungen in den Workshops näher beleuchtet. So diskutierten die Anwesenden die Frage, wie soziale Innovation in der Etablierung von Technologien die Akzeptanz erhöhen könnten. Dabei kristallisierten sich Co-Creation-Prozesse als vielversprechende Ansätze heraus, um Nutzer*innen in Feldern wie der Robotik oder der Pflege bereits frühzeitig einzubeziehen. Auch die Interdependenz zwischen sozialen Praktiken der Arbeit und Auswirkungen technologischer Entwicklungen wurde diskutiert.

Eine differenzierte Perspektive auf das Verhältnis von sozialen und digitalen Innovationen wurde ebenso in der Diskussion um die Rolle digitaler Innovation für Inklusion eingenommen. Die Etablierung digitaler Innovationen wurde hier in Bezug auf ihre nicht-intendierten Folgen für marginalisierte gesellschaftliche Gruppen betrachtet. Zugleich wurde die Frage beantwortet, wie dieselben Gruppen von der Digitalisierung profitieren könnten. Als Beispiel wurden hier offene Laboratorien benannt (z. B. MakerSpaces oder FabLabs), in denen Menschen mit Beeinträchtigungen ein pädagogisch begleiteter Zugang zu digitalen Technologien ermöglicht werde, welche die additive Fertigung individualisierter Hilfsmittel erlaubten.

Die Zukunft sozialer Innovation in der digitalen Transformation

Insgesamt konnte die Konferenz die Potenziale und Bedeutung sozialer Innovationen für die sozio-digitale und nachhaltige Transformation hervorheben und damit technikzentrierte Perspektiven ergänzen. Die Beiträge schärften den Blick auf das Verhältnis von Innovation und Wandel indem sie verdeutlichten, dass Digitalisierung von der Gesellschaft über die bloße Abschätzung von Technikfolgen hinaus aktiv gestaltet werden kann. Durch die Konferenz wurde zugleich deutlich, dass sich soziale Innovation als Forschungsfeld erst noch etablieren muss, um dieses Potenzial vollständig zu entfalten. Eine Reihe von Anknüpfungspunkten für praxisnahe und damit transdisziplinäre Forschung wurde in den beiden Tagen geschaffen. Zukünftige Veranstaltungen der zweijährigen Tagungsreihe unter der Schirmherrschaft der ESSI werden zeigen, wohin die Reise geht.

Literatur

Howaldt, Jürgen; Kaletka, Christoph; Schröder, Antonius; Zirngiebl, Marthe (Hg.) (2019): Atlas of social innovation. 2nd Volume: A World of New Practices. München: oekom verlag.

Howaldt, Jürgen; Schwarz, Michael (2010): Soziale Innovation. Konzepte, Forschungsfelder und -perspektiven. In: Jürgen Howaldt und Heike Jacobsen (Hg.): Soziale Innovation. Auf dem Weg zu einem postindustriellen Innovationsparadigma. Wiesbaden: VS Verlag für Sozialwissenschaften, S. 87–108.

Weitere Informationen

ESSI Conference 2019: www.essi-net.eu/?page_id=1229
Atlas of Social Innovation: www.socialinnovationatlas.net

BERICHT

(Un)Sicherheits-produktion im Cyberspace

Cybersecurity-Architekturen in Deutschland und der Schweiz

Jens Hälterlein, *Centre for Security and Society (CSS), Albert-Ludwigs-Universität Freiburg, Werthmannstr. 15, 79098 Freiburg (jens.haelterlein@css.uni-freiburg.de)*

Durch die zunehmende IT-Vernetzung von Unternehmen, staatlichen Einrichtungen und kritischen Infrastrukturen ist Cybersecurity seit den 1990er-Jahren zu einem sicherheitspolitischen Thema geworden. Sicherheitspolitik nimmt hierbei die Rolle einer institutionalisierten Technikfolgenabschätzung ein, die bemüht ist, Risiken, die durch Cybercrime und Cyberspionage für Staat, Wirtschaft und Bevölkerung entstehen, zu erkennen, zu bewerten und abzuwehren. Die staatlichen Architekturen und Institutionen der Cybersecurity und Cyberabwehr in Deutschland und der Schweiz standen im Zentrum der Veranstaltung „Cyber-Sicherheit. Architektur und institutionelle Kooperation in Deutschland und der Schweiz“, die vom Centre for Security and Society der Albert-Ludwigs-Universität Freiburg organisiert wurde und am 3. Juni 2019 in Berlin stattfand.

Ausgehend von der These, dass der Auf- und Ausbau institutioneller Vernetzungen und Kooperationen von staatlichen Agenturen einen oder vielleicht sogar den Kern der staatlichen Reaktion auf die neue Bedrohungslage darstellt, sollten im Rahmen von zwei Impulsvorträgen sowie einer Podiumsdiskussion die wesentlichen Unterschiede und Gemeinsamkeiten in den Herangehensweisen in beiden föderalen Staaten herausgearbeitet und die jeweiligen politisch-strategischen oder auch verfassungsrechtlichen Hintergründe thematisiert werden. Das von den Veranstaltern ausgegebene Ziel einer kritischen Reflexion zu den praktischen Grenzen und den strategischen Orientierungen der nationalen Strategien wurde von den Vortragenden und Diskutanten durchaus erfüllt. Wünschenswert wäre es allerdings gewesen, wenn auch der konstitutive Zusammenhang zwischen einer politischen Rhetorik des Cyberterrorismus und Cyberkriegs einerseits und des politisch beabsichtigten Aufbaus von Kapazitäten für eine aktive Cyberabwehr (das sogenannte Hackback) andererseits stärker thematisiert worden wäre. Auch die Frage, inwiefern der wachsende Markt für IT-Sicherheitslösungen aus der Erzeugung von Unsicherheit im Cyberraum profitiert und welche Schlüsse sich daraus ziehen lassen, wurde nicht gestellt.

Widersprüchliche Interessen in nationalen Cybersecurity-Strategien

In seiner Darstellung der staatlichen Cybersicherheitsarchitektur in Deutschland verwies Sven Herpig (Leiter Transatlantisches Cyber-Forum und Mitarbeiter der Stiftung Neue Verantwortung) zunächst auf eine zentrale Entwicklung: Zwar gelte weiterhin der Primat des Zivilen, d. h. defensive, zivile Organisationen waren und sind in Deutschland für die Cybersicherheit verantwortlich. Jedoch werde der militärische Bereich kontinuierlich aufgebaut und aktiver. Auch gäbe es bereits Diskussionen, ob das Militär – analog zum Katastrophenschutz – im Angriffsfall kritische Infrastrukturen verteidigen solle. Dies führe zu der kuriosen Entwicklung, dass das Innenministerium Maßnahmen zur Förderung der Cybersicherheit ankündigt (erstmals geschehen in der Cybersicherheitsstrategie der Bundesregierung von 2016), die zugleich die IT-Sicherheit einschränken. Dies sei beispielsweise der Fall, wenn es dem Verfassungsschutz technisch und rechtlich ermöglicht werden soll, IT-Sicherheitsbarrieren zu überwinden, um an bestimmte Daten zu kommen. Es ergebe sich daraus ein Interessengegensatz zwischen offensiven und defensiven Strategien der Cyberabwehr, der sich auch in unterschiedlichen Interessenlagen der zuständigen Behörden wiederspiegelt. Während das Bundesamt für Sicherheit in der Informationstechnik (BSI) generell daran interessiert ist, dass Sicherheitslücken in einer Software geschlossen werden, möchten die Strafverfolgungsbehörden und Nachrichtendienste diese Sicherheitslücken ggf. ausnutzen oder haben sogar den Wunsch, dass Sicherheitslücken gezielt in Informations- und Kommunikationstechnologien (IKT) eingebaut werden. Das zeige z. B. die aktuelle Diskussion um den neuen Mobilfunkstandard 5G. Solche Sicherheitslücken könnten natürlich wiederum für kriminelle Absichten ausgenutzt werden.

IT-Sicherheit als zentrales Problem

Die Unterscheidung von defensiver und offensiver Cyberabwehr sowie deren zuweilen widersprüchliche Effekte bildeten auch einen Schwerpunkt der Podiumsdiskussion. Bei der Analyse aktueller defensiver Strategien standen Probleme bei der Einschätzung der Bedrohungslage, das fehlende Vertrauen in die Arbeit der staatlichen Behörden, eine Meldepflicht von betroffenen Unternehmen sowie ausstehende gesetzliche Vorgaben für sicherheitskritische IT-Produkte im Zentrum.

Aus der Perspektive von André Duvillard (Delegierter des Sicherheitsverbundes Schweiz) sei es ein zentrales Problem für die nationale Cyberabwehr, dass es keine aussagekräftige Übersicht über Cyberdelikte gibt. Zwar wurde in der zweiten Cybersicher-

https://doi.org/10.14512/tatup.29.1.58

heits-Strategie der Schweiz von 2018 Cybersecurity als nationale Sicherheitsaufgabe definiert und ein Cyberradar zur Identifikation und Analyse von Bedrohungen eingerichtet. Es fehle jedoch an Vertrauen in die Arbeit der Behörden, sodass viele Firmen Vorfälle nicht melden würden. Sie fürchten um ihre Reputation, wenn Cyberangriffe in der Folge einer Meldung publik werden würden. In der Schweiz gibt es keine Meldepflicht und nur ein kleiner Teil der Cyberdelikte werde bei der Polizei zur Anzeige gebracht. Bei den kritischen Infrastrukturen funktioniere das Meldewesen gegenüber den Strafverfolgungsbehörden hingegen recht gut. Auf die Frage hin, ob die von professionellen Hackern durchgeführten Angriffe gar nicht bemerkt werden und gesetzliche Regelungen Anreize für Investitionen in die IT-Sicherheit ihrer Produkte erhielten. Rieger wies zudem darauf hin, dass die Software-Branche die einzige Branche sei, für die nach wie vor keine angemessenen Haftungsregeln und Gewährleistungsansprüche gelten. Der State of the Art in der Entwicklung von sicherer Software habe sich zwar in den letzten Jahren signifikant weiterentwickelt. Dadurch ließen sich nach seiner Schätzung vermutlich 80 % der Cyberangriffe abwehren. Dieser State of the Art komme aber nicht in der Breite zur Anwendung, weil die Unternehmen keine entsprechenden ökonomischen Anreize hätten. Das ausschlaggebende Kriterium bei der Produktentwicklung sei weiterhin *time-to-market*.

Die Dunkelziffer von Cyberangriffen, vor allem von nachrichtendienstlichen Cyberaktivitäten im Wirtschaftsspionagebereich, ist hoch.

bei Cybercrime mithin mit einem großen Dunkelfeld zu rechnen sei, betonte Frank Rieger (Sprecher des Chaos Computer Club), dass es zwar generell schwierig sei, über das Dunkelfeld Aussagen zu treffen, es aber dennoch anzunehmen sei, dass viele, vor allem nachrichtendienstliche Cyberaktivitäten im Wirtschaftsspionagebereich gar nicht sichtbar werden.

Sichtbar werden solche Aktivitäten häufig erst, wenn Probleme mit der Funktionalität eines betroffenen IT-Systems festgestellt werden oder wenn gestohlene Daten im Netz auftauchen. Eine Meldepflicht sei daher prinzipiell sinnvoll, da nur so überhaupt die Chance entstehe, einen Überblick über die Bedrohungslage zu bekommen. Wenn es aber darum gehe, die IT-Sicherheit zu erhöhen und Prävention von Cybercrime zu betreiben, sei das eigentliche Problem die Definition und Durchsetzung von branchenspezifischen Sicherheitsanforderungen. Es gäbe zwar Ansätze in diese Richtung. Dabei gehe es aber vor allem um Audit-Prozesse und weniger um konkrete technische Sicherheit. Auch gibt es durchaus Zertifizierungsprozesse für die IT-Sicherheit von Produkten, z. B. medizinischen Geräten. Diese Prozesse dauern aber zuweilen so lange, dass ein Gerät, das ursprünglich den Sicherheitsstandards entsprach, zum Zeitpunkt seiner erfolgten Zertifizierung nicht mehr sicher ist. Verkompliziert werde die Situation dadurch, dass ein Patch – also die Aktualisierung eines Computerprogramms oder seiner unterstützenden Daten – die Zertifizierung außer Kraft setzen würde. Die Dynamisierung des technischen Sicherheitsprozesses stecke insofern noch in den Kinderschuhen.

Manuel Bach (Leiter Nationales Cyber-Abwehrzentrum, BSI) fügte hinzu, dass sich die Bedrohungslage im Bereich Cybercrime durch das Internet der Dinge verändert habe, da dort viel „IT-Unsicherheit“ eingebaut sei. Einig waren sich die Diskutierenden weitestgehend darin, dass der Staat an diesem Punkt aktiv werden müsse, da die Hersteller nur durch entsprechende

Aktive Cyberabwehr nicht zielführend

Bei der anschließenden Bewertung der gegenwärtig diskutierten offensiven Maßnahmen und Strategien der Cyberabwehr standen Fragen der Effektivität und Angemessenheit im Vordergrund. Matthias Schulze (Mitarbeiter im Bereich Cyber-Sicherheitspolitik der Stiftung Wissenschaft und Politik) verwies zunächst auf die völkerrechtliche Problematik solcher Maßnahmen. Darüber hinaus stellte er deren Wirksamkeit infrage. Ob das Löschen von gestohlenen Daten oder das Zerstören der zum Angriff genutzten IT-Systeme eine präventive Wirkung habe, sei anzuzweifeln. Frank Rieger fügt hinzu, dass das Risiko von Kollateralschäden bei diesen Gegenangriffen mittlerweile immens sei, wenn etwa Cloud-Dienste betroffen sind. Auch gebe es ein generelles Attributionsproblem, da die Verursacher von Cyberangriffen nicht verlässlich identifizierbar sind.

Weitere Informationen

Konferenzprogramm und zusätzliche Informationen:
https://www.css.uni-freiburg.de/fileadmin/primary/Public/user_uploads/Aktuelles-News/CSS_Cyber-Sicherheit_-_Berlin_3._Juni2019.pdf

REPORT

Digitization – hopes and fears

Paul Grünke, *Institute for Philosophy, Karlsruhe Institute of Technology (KIT), Douglasstraße 24, 76133 Karlsruhe (paul.gruenke@kit.edu), https://orcid.org/0000-0002-3576-1921*
Aleksandra Kazakova, *Bauman Moscow State Technical University (kazakovaz@mail.ru), https://orcid.org/0000-0002-2952-8373*

The Budapest Workshop on Philosophy of Technology, hosted by the Budapest University of Technology and Economics on the 12th and 13th of December 2019, drew around 50 scholars from philosophy, history, sociology and Science and Technology Studies. Many of the talks approached the topic of Artificial Intelligence (AI) from socio-historical, epistemological or ethical perspective. Mark Coecklbergh gave the keynote speech and offered a comprehensive overview of ethical issues and policy directions concerning AI with a focus on Europe.

History and philosophy of technology

The philosophical legacy was revised with regard to current issues, for example by two reports discussing the "empirical turn" of the 1980s from different comparative perspectives.

Agostino Cera described the "empirical turn" as "transition from an over-distance to an overproximity". The new relativist and contextual approach to "technologies" (in the plural) confronted essentialism, determinism and dystopianism of the "classics", especially Heidegger. For Cera, this blurred the distinction between "problems" (requiring solutions) and "questions" (remaining open). "Engineerization of philosophy of technology" as problem-solving activity converged with scientific, technical or political expertise. Cera argued for leaving space for the genuinely philosophical "Grundfrage": the question of the historical or epochal phenomenon of technology as such.

For Darryl Cressman, the distinction between classical and empirical approaches is not relevant for critical philosophy. Marxist thought, he claimed, was always empirically oriented, recognizing the historical contingency of technology and disentangling reification of socio-economic interests in it. The "negative dialectics" reveals the inherent biases and reflects on alternatives, or "unrealized potential" of technology. This can be seen in the practices and imaginaries of users, which "contradict, or negate, the prescribed design and function". In our view, this focus on agency in production and use of technologies is in line with the objectives of participatory technology assessment (TA) and may become a conceptual resource for it.

Phil Mulins addressed the question of technological imaginaries of digitization, reconstructing Polanyi's participation in the mind-machine debate since the late 1940s. His concept of personal and tacit knowledge confronted both Cartesian dualism and reductionist theory of mind and underlay his scepticism about unlimited formalization, even though he acknowledged its indispensability for the complex modern societies. This makes Polanyi's post-critical philosophy relevant for the current debate on digitization, including questions of algorithmic bias and discrimination. Mulins formulated the task for TA nowadays: "Society needs both to set limits upon predictive analytics and to recognize better the potential of predictive analytics to promote the good society".

Epistemology

Two talks touched on epistemological questions concerning neural networks. Paul Grünke used the development of the neural network based chess engine AlphaZero to illustrate the different kinds of epistemic opacities, which are present in classical modeling and computer simulations compared to machine learning techniques. He claimed that the opacities in the traditional approaches are contingent, but machine learning introduced a fundamental kind of opacity. This model-opacity can make it impossible to trace the origin of specific results, because the underlying structure of the neural network cannot be understood.

Reto Gubelmann analyzed a claim made in the natural language processing community: the results of new translation systems using "neural machine translation" cannot be distinguished from those of professional human translators. They regard it as a clear step towards strong AI. Comparing this claim to Searle's classical Chinese Room thought experiment, Gubelmann showed that the techniques used (semantic representations via word embedding) are more advanced than classical statistical approaches and it could be argued that these systems do have some kind of linguistic understanding. Opacity of machine learning processes, however, limits our understanding of the machine's understanding.

Political science and media studies

A few talks focused on ideological implications of digitization. Jernej Kaluza explored fragmentation and polarization of the digital environment, manifesting itself both in collective and individual social action: from the rise of alt-right politics to mass shootings. He claimed that "digital hate" cannot be explained in psychological terms, but is a mutual reinforcement of individual choices and algorithms of personalization, creating the "endless You-loops", or a "static and narrowing version of oneself". Marginalization of hate speech, he argued, has the backfire effect of creating even more radicalized "rabbit holes".

https://doi.org/10.14512/tatup.29.1.60

Jacopo Bodini linked the subjective experience with the totality of digital culture. He claimed that hypothesis of the coming post-ideological era did not grasp recent metamorphosis of "ideology": from political or philosophical metanarrative to aestheticization of its own technological base. Its major feature is "transparency", which paradoxically conceals itself. Subjectively, it means ignoring the technological mediation of experience. The logic of "immediation" can be seen in the rise of populism and fake news, but also in the immersive way of digital life, shaping ("in-forming") individual perceptions and desires.

Ricardo Rohm investigated agency in opinion-making during the political crisis in Brazil, describing it as "architecture of misinformation". The interaction between "corporatocracy" and technocracy (IT-corporations and social platforms, advertisers and lobbies), he claimed, makes political marketing a real threat to representative democracy. The interplay of national and transnational actors reflects how through the globalization of politics civil society loses control at the national level. South American political systems are especially vulnerable, since their recent democratization evolves against the background of the digital revolution.

This discussion raises the further question for TA: what are the effective means of regulating the digital public sphere – both nationally and globally – for maintaining the argumentative and representative discourse?

Responsibility and decision-making

One of the salient topics during the whole conference was the question how to distribute accountability and responsibility of human actors, making decisions based on the suggestion of an automated expert system. A typical illustration: a doctor uses an expert system, which has a higher success rate of suggesting a treatment than the doctor him/herself. As a result, less time is allocated for decision making of the human, which discourages their disagreement with the expert systems, while in legal terms full responsibility and accountability are assigned to the doctor.

Chang-Yun Ku addressed this problem in a thought experiment of a conflict between a doctor's diagnosis and an AI recommendation: AI suggests a treatment and the doctor believes it is not necessary. Assuming that this fictional doctor would in this case be very likely to advocate the treatment, Ku pointed out a tension with Article 22 (1) of the General Data Protection Regulation, which requires that decisions, which will have significant impact on a person, should not be made solely by automated systems. Legally speaking, the decision is made by the doctor, but it can be argued whether he/she had enough autonomy in these circumstances.

Mark Coeckelbergh touched on similar problems, offering some insights into the ideas currently guiding European policy makers. Central to European policy is to ensure that humans make the decisions. Besides the philosophical problems of assigning responsibility to machines with their non-existent agency, he also referred to the "many hands problem", which makes it difficult to trace exactly who is responsible for the decision of a machine. In order for the human decision to be autonomous and at the same time, to include the recommendations by expert system, the human has to be able to understand its "reasoning". Efforts in the area of Explainable AI must be directed to enabling the decision maker, e. g. a doctor, to acquire enough information about the expert system to explain its result. Furthermore, the regulations on the use of AI technology must leave enough time for reflection on the results of the expert system. Otherwise, a decision will likely be replaced by a post-hoc rationalization.

How to distribute accountability and responsibility of human actors making decisions based on the suggestion of an automated expert system?

Many participants were critical of the idea that a human will always be legally responsible for decisions in these contexts. Going forward, there seem to be three different options: 1) accept the situation and act as described above; 2) find ways to distribute legal responsibility to the expert system; 3) reach a societal consensus that expert systems should not be used in some areas. The discussion did not result in a clear preference between these options.

The general leitmotif of this interdisciplinary workshop may be summarized as follows: what is human (knowledge, agency, responsibility) and what is not in the process of digitization. This theoretical question, however, is intertwined with a practical one (in a Kantian sense): what may we, a human society, hope to be? For achieving concrete results of TA, it seems that these questions need to be considered together.

BERICHT

Die Herrschaft der Algorithmen

Ulrich Smeddinck, *Institut für Technikfolgenabschätzung und Systemanalyse (ITAS), Karlsruher Institut für Technologie (KIT), Karlstr. 11, 76131 Karlsruhe (ulrich.smeddinck@kit.edu)*

„Die Geister, die ich rief …“ hatten die VeranstalterInnen zum Motto der Tagung „Die Herrschaft der Algorithmen“ des Karlsruher Forums für Kultur, Recht und Technik, des Kulturamt Karlsruhe und des Zentrums für Kunst und Medien (ZKM) am 17. 10. 2019 gewählt. Die Algorithmen übernehmen und der Mensch dankt ab. Der suggestive, dystopische Titel hatte offenbar den Nerv getroffen. Das Format war mit 300 Angemeldeten so gut besucht wie nie zuvor. Dabei wies bereits Prof. Christiane Riedel vom ZKM, Karlsruhe, in ihrer Begrüßung auf die lange Vorlaufzeit seit dem „Dartmouth Summer Research Project on Artificial Intelligence“ von 1955/56 hin. Schon da war die Erwartung groß, dass Maschinen Sprache benutzen, abstrahieren, Konzepte verfassen und lernen können. Immer wieder erkaltete das Interesse in „digitalen Wintern“. Jetzt ist die Aufmerksamkeit groß. Trotz aller Hoffnungen und Ängste gehe es letztlich darum, in den verschiedensten Einsatzbereichen in der digitalen Gesellschaft mit Maschinen Probleme zu lösen, die bisher nicht lösbar waren.

Wer regiert wen? Kernfragen an Recht, Wissenschaft und Wirtschaft

„Wie bilde ich Vertrauen in KI-Technologie?“ Mit der impliziten These dieses Vortragstitels, dass das Vertrauen fehle oder nicht ausreiche, setzte sich dann in einem ersten einführenden Vortrag Andrea Martin, Leiterin des privatwirtschaftlichen Watson IoT Center München und Mitglied der aktuellen Enquete-Kommission „Künstliche Intelligenz“ des Bundestages, auseinander. KI müsse lernen wie ein Kind, das in die Schule kommt. Es gehe um Sorge und Aufmerksamkeit anstelle von irrationaler Angst. Nur so ließen sich Voreingenommenheiten überwinden und Handlungsmöglichkeiten erschließen. Die digitalisierte Passkontrolle an Flughäfen oder die Brustkrebskontrolle, bei der die maschinelle Diagnose, in Kombination mit untersuchenden Ärzten, die optimale Erkennungsquote bringt – Systeme der Unterstützung –, seien eine „gute Sache“. In einem Einspiel-Filmchen stellte sie den menschenähnlichen Roboter Cimon vor, der auf der Raumstation ISS mit dem Astronauten Alexander Gerst Nettigkeiten austauscht. Demnächst gehe der große Bruder des Roboters hoch. Ihren derart rational geprägten Vortrag setzte sie dann mit einigen notwendigen Prinzipien fort: Der Mensch müsse unterstützt werden. Die Daten gehören dem Kunden. KI-Lösungen müssen transparent und erklärbar sein. Fairness sei nur über ausreichende und ausbalancierte Datenbestände erreichbar, sonst seien viele Bereiche wie das Rechtsystem, die Kreditvergabe oder das Personalwesen negativ betroffen. Sichere und verlässliche Lösungen entwickeln, Entwicklungen beobachten und evaluieren – über Leitfäden für die eigenen DesignerInnen und EntwicklerInnen hinausgehend engagiere sich ihr Unternehmen auch politisch, um den Diskurs zu führen. Welche Gremien, welche Menschen dürften entscheiden, was eine faire Lösung oder Regelung ist? Demokratisch legitimierte staatliche Stellen erwähnte sie nicht. Hier brauche es die interdisziplinäre Diskussion.

Wunschgemäß lieferten die nächsten beiden Referenten – mit aufklärerischen, Klischees entlarvenden und Erwartungen unterlaufenden Beiträgen:

Mit spontanen Vorbemerkungen reagierte zunächst der Technikphilosoph Prof. Armin Grunwald vom Institut für Technikfolgenabschätzung und Systemanalyse am Karlsruher Institut für Technologie. Zum einen: Wenn es eine Angst vor KI gäbe, dann sei es jedenfalls die falsche Angst – eine, die maßgeblich von der Science-Fiction-Vorstellungswelt geprägt sei. Aber KI sei kein schlafender King Kong, sondern von Menschen gemacht. Es gehe um Werte, Ideen, Geschäftsmodelle und Profit. „Manche machen KI, andere müssen sich anpassen.“ Wenn eine Furcht im Zusammenhang mit KI berechtigt sei, dann die vor großen Daten-Konzernen und ihren Geschäftsmodellen. Zum anderen: Wo bleibt der Mensch, wenn KI besser ist? Und: Ist das schlimm? Keinesfalls, so Grunwald. KI würde sonst nicht gebraucht, wenn sie nicht besser wäre. Es sei das Wesen der Technik, menschliche Schwächen auszugleichen. Am Beispiel des nützlichen Spatens machte er die Frage fest, warum KI demgegenüber Unterlegenheitsgefühle auslöse. Und fand die Erklärung in der Sprache: Der Mensch mache sich zum Opfer, wenn er Formulierungen wählt, in denen KI lernt, denkt und entscheidet: Worte, die KI vermenschlichen! Die Suggestion werde zum Fake, dem zu viele aufsitzen. „Der Roboter ist keiner von uns! Autonome Autos entscheiden nichts!“ Und: „Nehmen uns Roboter die Arbeit weg? Unsinn!“ Es seien die Menschen und Manager, die dahinterstehen. Die Vermenschlichung des Roboters lenke von den eigentlichen (wirtschaftlichen) Interessen ab.

Gerafft lauten seine Thesen und Punkte: 1. Technik-Nutzung sei mit Anpassung verbunden. Im Sinne einer Ko-Evolution verändere Technik die NutzerInnen. Die Verhaltenssteuerung durch Software sei erheblich größer als bei klassischer Technik. Software nehme den Rang einer Institution ein. 2. Weiß ich noch, was andere über mich wissen? Legitime Produktgestaltung werde irgendwann zum Problem, zur Grundrechtsgefährdung, wenn Persönlichkeitsprofile wirkmächtig werden („… was ich nicht bin, was ich nicht sein will …“). Digitalisierung berge das

https://doi.org/10.14512/tatup.29.1.62

Potenzial, die Bedingungen unserer Demokratie zu gefährden. 3. Grunwald fragt weiterhin: Zerstört Digitalisierung einen solidarischen Arbeitsmarkt? Wird authentisches Verhalten unmöglich, weil sich jeder beobachtet fühlt? Auf welcher Ebene ist zu regulieren? Wie ist die Kontrolle von Algorithmen möglich – verbunden mit dem Problem, dass ausschließlich Daten aus der Vergangenheit der Zukunft übergestülpt werden?

Der Rechtswissenschaftler Prof. Klaus Ferdinand Gärditz, Universität Bonn, kokettierte mit der Position des Außenstehenden/Juristen, der von den Inhalten keine Ahnung habe, um den Digitalisierungshype dann zum bloßen Komplexitätsproblem zu degradieren, das – wie andere Probleme auch – rechtsstaatlich zu bewältigen sei. Die Rechtsprechung habe etwa Verantwortlichkeiten sanktioniert, wenn es um Willenserklärungen in automatisierten Systemen oder missliebige Ergänzungsvorschläge für personalisierte Suchbegriffe geht (wenn z. B. ein Kläger sich gegen eine Verknüpfung mit dem Begriff Sektenführer wendet). Steuerrecht und Kartellrecht bieten Möglichkeiten, auch großen Internet-Konzernen beizukommen.

Die Vermenschlichung des Roboters lenkt von den eigentlichen (wirtschaftlichen) Interessen ab.

Im Weiteren überraschte Gärditz mit einem Plädoyer für das Imperfekte: Dem Ideal der Null-Fehler-Produktion mit KI stellte er das Bild der menschlichen Gesellschaft und der liberalen Rechtsordnung entgegen, die gut mit der Unvernunft des Menschen als Normalzustand lebe. Die Abwägung im Einzelfall, das Ausbalancieren von Interessen und rechtlicher Facetten sei rechtsstaatliches Ideal und tägliches Brot. Diese Aufgaben seien nicht determinierbar zu bewältigen. Deshalb seien Algorithmen nur von beschränktem Nutzen fürs Recht und selbstlernende Algorithmen gar nicht geeignet für staatliche Hoheitsträger. Demokratie lebe vom Voluntarismus. Kontingenz sei nicht programmierbar. Demokratie müsse nahbar sein. „Die freiheitliche Ordnung nimmt die Menschen wie sie sind. Sie braucht Orte des Zufälligen und der Dezentralität, das Recht, nicht rational zu sein und Fehler zu machen." Das alles verträgt sich schlecht mit der Digitalisierung. Deshalb dürften Algorithmen nur eine unterstützende Funktion haben, müsse in rechtlichen Verfahren die Subjektivität gem. Art. 1 Grundgesetz gewährleistet werden und wie in Art. 22 Abs. 1 Datenschutz-Grundverordnung ein Mindestmaß menschlicher Interaktion gewahrt bleiben. Die Schutzpflichten des Staates zwingen ihn zum Schutz vor Diskriminierungen und großen Monopolunternehmen. Die Verantwortung der Algorithmen-ErzeugerInnen sei zu regulieren. Der Minderheitenschutz müsse gegen den algorithmischen Mainstream aktiv mit Regelungen verteidigt werden. Der Ex-Territorialität der Internet-Konzerne mit Profitinteressen sei in der EU mit kartellrechtlichen Geldbußen zu begegnen, Machtasymmetrien mit Recht auszugleichen. Menschliche Interventionen seien unverzichtbar – ein Schutzraum in der Welt der Algorithmen.

Im Anschluss wurden zahlreiche weitere Vorträge zu den Themen-Komplexen „Wie intelligent sind Algorithmen?", „Vom Code zur Kunst – Die Kunst der Zukunft" und „Die Geister, die ich rief …" aus den verschiedensten Richtungen und Disziplinen geboten.

Resümee

Keine Frage: Es braucht ebenso niederschwellige wie kompetent besetzte Veranstaltungen wie diese, um Digitalisierung und Digitalisierungshype angemessen einordnen zu können. Das große Interesse unterstreicht, wie sehr das Thema die Gesellschaft umtreibt. Offenbar braucht es in diesem Frühling und Sommer der Digitalisierung aber auch Expertinnen und Experten, die die Euphorie und Erwartungen auf schnelle Erfolge bremsen, dem Diskurs etwas kühlende Luft zuführen und erklären, warum der Mensch den Robotern nicht unterlegen ist. Bereits der Karlsruher Oberbürgermeister Dr. Frank Mentrup hatte in seinem Grußwort festgestellt, dass die Neurowissenschaft noch nicht so weit ist, „alles einzulösen, was man sich von der Digitalisierung verspricht." Prof. Hannah Bast, Institut für Algorithmen und Datenstrukturen, Universität Freiburg, hatte in ihrem Referat zu „Transparenz und Fairness von KI und deren Überwachung" darauf verwiesen, dass KI schon viele Hoffnungen enttäuscht hat. Was es jetzt an Lösungen gäbe, sei schon 30, 40 Jahre alt; was darüber hinaus an KI-Lösungen erwartet werde, sei auch in zehn bis 20 Jahren nicht zu erwarten, weil keiner wisse, wie das alles zu realisieren sei. Unterdessen erzeugen Algorithmen längst im Alltag problematische Diskriminierungen (Orwat 2019). Vielleicht auch deshalb war die Tagung des Karlsruher Forums für Kultur, Recht und Technik/Kulturamt Karlsruhe und Zentrum für Kunst und Medien (ZKM) ein guter Ort auf dem langen Weg, um innezuhalten und um Euphorie, Gruseln und Expertenwissen miteinander zu konfrontieren und abzugleichen. Weitere Forschungsaktivitäten, aber auch der weitere Diskurs mit und in der Gesellschaft sind unerlässlich, um aus den angestoßenen, ja laufenden Entwicklungen das Beste zu machen.

Allen kritischen Einlassungen und ernüchternden Bemerkungen zum Trotz: Das beliebteste Foto-Motiv war der kleine menschenähnliche Roboter Pepper, dessen großer Bruder an diesem Tage leider nicht in Karlsruhe dabei sein konnte.

Weitere Informationen

Orwat, Carsten (2019): Diskriminierungsrisiken durch Verwendung von Algorithmen. Baden-Baden: Nomos.
Programm und Livestream zur Veranstaltung:
https://zkm.de/de/veranstaltung/2019/10/die-herrschaft-der-algorithmen.

REPORT

Technology assessment – thinking with values

Constanze Scherz, *Institute for Technology Assessment and Systems Analysis (ITAS), Karlsruhe Institute of Technology (KIT), Karlstraße 11, 76133 Karlsruhe (scherz@kit.edu), https://orcid.org/0000-0003-4488-439X*
Linda Nierling, *ITAS-KIT (linda.nierling@kit.edu), https://orcid.org/0000-0001-9129-550X*
Mahshid Sotoudeh, *Institute of Technology Assessment (ITA), Austrian Academy of Sciences (mahshid.sotoudeh@oeaw.ac.at)*
Lenka Hebakova, *Technology Centre ASCR, Strategic Studies Department (hebakova@tc.cz)*
Tomas Michalek, *Slovak Academy of Sciences (michalek@up.upsav.sk)*

The 4th European Technology Assessment Conference "Value-driven Technologies: Methods, Limits, and Prospects for Governing Innovations" was hosted by the Slovak Academy of Sciences in Bratislava. The Slovakian colleagues continued the tradition of the European TA Conferences: What luck! The Slovak Republic is one of the countries, which is in the process of establishing technology assessment (TA). Putting values at the core of the conference helped to fruitfully discuss current concepts, technical trends, and their specific relevance for technology assessment and related scientific activities in the field of knowledge-based policy-making in science, technology and innovation. Questioning the values for and behind TA served as an overall frame for keynotes, sessions and discussions.

Three keynotes by P. Sykora (University of Sts. Cyril, Trnava) on Health Technology Assessment, C. Müller-Birn (Freie Universität Berlin) on Artificial Intelligence and G. Meskens (Belgian Nuclear Research Centre & Ghent University) on Social Justice gave impulses and showed multiple perspectives and approaches on values in TA. With 184 participants from 29 countries, the conference was well attended, with many young scientists taking and interest in TA.

https://doi.org/10.14512/tatup.29.1.64

Role concepts in TA and Responsible Innovation

A. Grunwald (ITAS Karlsruhe) initiated and moderated together with R. von Schomberg (European Commission) the opening plenary session on role concepts accompanying conceptual discussions in TA and Responsible Research and Innovation (RRI). In particular, the tension between being a distant and neutral advisor, and an active and transformative actor shaping technology governance, was subject of an engaged plenary debate. In the session, previous discussions from both neighboring fields (TA and RRI) were recalled and scrutinized with respect to current challenges of TA. Presentations by H. Torgersen (ITA Vienna), Chr. Wittrock (Oslo Metropolitan University) and R. von Schomberg addressed issues of neutrality and independence of TA, drivers and influencing factors in RRI, and the role of TA and RRI in European innovation policy. Plenary discussion focused on specific role concepts of TA and RRI as well as their different institutional and political settings, thereby emphasizing the strong need for contextualization in this respect.

However, which developments can be considered really "new" for TA in terms of methods? The session "New Methods for TA" explored the potentials and challenges of quantitative computational content analysis. T. Sinozic (ITA) reported about the development and testing of a text mining methodology to extract policy recommendations from large amounts of evidence on European neighborhood policy. Taking the example of climate engineering, N. Matzner (University Klagenfurt) highlighted the capabilities of the programming language "R" to support the analysis of scientific networks. L. Capari and T. Udrea (ITA) demonstrated text-mining approaches, specifically word occurrence networks and topic modelling. In the concluding joint discussion, the presenters agreed on the potential of new digital methods to enrich the methodological portfolio of TA, when applied reflectively and in addition, rather than substitution, to other e. g. qualitative methods.

Limits and prospects for governing innovations

There is hardly any other field in TA where the limits and perspectives for innovations are as impressive as in assistive technologies (ATs). The session "Assessing similarities and gaps in ageing and disabilities: towards better assistive technologies" focused on specific dimensions of technologies for the elderly and people with disabilities. Seen from the perspective of TA, there are obstacles of fair and equal access to technological devices, e. g. due to costs, or the lack of a user-centered choice. Further, the role of health professionals was seen as a duality with possible relevance for further discussion within the TA context. This fruitful discussion was stimulated by presentations from L. Nierling and B. Krings (ITAS), M. Baumann and M. Maia (ITAS), E. Thorstensen (OsloMet), B. Schiffhauer and D. Schneider (Fachhochschule Bielefeld).

Another instructive example for the limits and prospects of governing processes are the impacts of digitalisation, artificial intelligence (AI) and big data on research. AI might challenge individual autonomy and skills of researchers as well as scien-

tific validity of AI-augmented research. Whether this change is disruptive or not with respect to established research cultures was discussed with panellists B. Humm (Darmstadt University), M. Nentwich (ITA), J. C. Schmidt (Darmstadt University) and S. Spiekermann (WU Vienna). The session chair S. Lingner (IQIB, Germany) summarized that AI should be regarded as a research tool. In this function, it can improve efficiency in science, open up new options and applications in research and might support the finding and formulation of new hypotheses and theories. AI's "black box" characteristic might challenge the established falsification mode of modern research. Therefore, it might tackle overall trust in AI-augmented research. This point might lead to a paradigm shift of late modern research from an explanatory to a predictive mode of research.

The governing implications of demographic change and its connections with the fourth industrial revolution was discussed: What is the role of the ageing and wealthy consumer? This was the topic covered by C. Seibt (University Kassel). U. Bechtold (ITA) identified a series of challenges in future work settings connected with both an ageing society and smart factories and questioned to what extent an organizational "top-down" view on these developments needs to be critically examined. K. Zimmermann and I. Hegny (Austrian Federal Ministry for Transport, Innovation and Technology) provided an overview on global technology trends for AT. They also presented lessons learned and their impact on the ministry's policy and funding interventions. M. Barland (NBT, Norway) outlined education policy and lifelong learning as one of the key governance areas at interface between ageing and technology to improve flexibility, personalization and the possibility of learning in simulated environments.

Another focus was on the governance of food waste reduction. T. Ratinger and L. Hebáková (Technology Centre of the Czech Academy of Sciences) presented strategies for food waste reduction in public catering. As globally one third of produced food is lost, food waste reduction requires information for consumers, responsibility of producers, and a new "social contract-agreement". B. Kebová (Zachraň Jídlo, SAVE FOOD) presented how NGOs deal with the issue of food waste and some solutions in the food value chain, including awareness building of consumers and using new technologies for food tracking that might reduce problems. M. Sotoudeh, S. Bettin, N. Gudowsky (ITA) presented the need for comprehensive solutions instead of fragmented policies and the need for critical evaluation of values behind visions on digitalization for food security from farm to grocery and landfill.

Value-driven technologies – how to give advice?

Values inscribed in new technologies are a relevant subject for TA. TA studies also reflect on the role of those deciding about and using new technologies (e. g. policy makers). The Dutch colleagues practiced a very innovative session format. First, the panelists M. Barland (NBT), Chr. Taylor (STEaPP), T. Jetzke (VDI/VDE), N. Tobler (TA Swiss), J. Loveridge (Harvard University) and M. Nentwich (ITA) discussed under the direction of I. van Keulen (Rathenau Institute) "How to serve Parliament as a TA institute?". The second part of the session was used for a so-called peer coaching. Anyone with a question on how to serve parliament could ask it to the panel via an app. These questions were projected onto the wall in real time; the method made the discussion very lively by continuously giving new impacts.

The increasing use of computer models and simulations to support policy formulation, implementation and evaluation point to the crucial role of TA in this area. P. Lopez (University of Vienna), A. Mager (ITA) and F. Fischer (TU Vienna), F. Eyert (Weizenbaum Institute for the Networked Society, Berlin) and

Values inscribed in new technologies are a relevant subject for TA.

D. Fuchs (ITA) showed how the recent predictive model of the Austrian employment service agency includes technical and societal biases that codify past inequalities. It was discussed what the consequences of this model are (emphasizing efficient labor market management while framing unemployment under neoliberal austerity policies at the same time) and how the diffusion of computational modelling has led to epistemic shifts.

The increasing use of AI is a key characteristic of digital transformation that is profoundly changing modern society. The aim of the session "Artificial Intelligence and the Future of Work and Education" was to discuss suitable policy responses that can help to prepare for the upcoming digital future. The presentations (M. Pazour and M. Fatun (Technology Centre of the Czech Academy of Sciences), C. Mader (Technology and Society Laboratory Empa, Zurich) and K. Braun (University of Stuttgart)) outlined the main issues related to the digital transformation from different angles, however, all of them ended up by pointing to the critical need for empowering society with new skills and competencies.

„Methods, Limits, and Prospects for Governing Innovations" were presented by G. Bianchi, M. Popper and T. Michalek (Slovak Academy of Sciences) on different attitudes to progressive gene therapies in Slovakia in the light of the ethical dimensions of human enhancement. A. Lang (IHS Vienna) presented experiences with governing genome editing and theories for dealing with 'wicked' problems. E. Haslinger-Baumann (University of Applied Science Vienna) emphasized the need for inclusion of clients and their family in quality assurance in 24h-caregiving at home by means of digital support. Co-Creation of Co-design plays a crucial role in expectations and concerns of the "Care Robot for Seniors" presented by P. D. Hos (University of Stuttgart) and "Technologies for older adults" presented by W. Rowan, S. McCarthy and C. Fitzgerald (University College Cork).

Education matters!

Questions how to communicate within and over TA run like a red thread through the conference. The discussions about value-driven technologies repeatedly showed that values could only serve as a point of reference for the evaluation of technologies if these are constantly renegotiated. The question arises how education and training can be developed to open up these reflective competences for students, but also technical professionals. "TA and Ethics for Value-driven Technologies: Educational Aspects" reflected on the perspectives of TA education as such and discussed formats how TA as a value-oriented approach can be integrated into technical education reflecting on the interactions over TA within diverse communities of scientists, technologists and engineers. The representatives of different national education systems (J. Kaźmierczak (Silesian University of Technology), E. Gavrilina and A. Kazakova (Bauman Moscow State Technical University), J. Sośnicka (Lodz University of Technology), R. Dürr (Karlsruhe Institute of Technology), E. Yadova (Moscow Business School) and K. Weber (OTH Regensburg)) touched upon methodological and organizational issues.

TA education needs to be self-reflective.

Further, they shared practical experiences, e. g. a dynamic balance between conceptual and practice-oriented teaching, discussed the advantages of teaching TA at different stages of education, including TA courses for educators themselves. The joint agreement was that a TA education needs to be self-reflective, explicating its contributions from different disciplines as well as its interdisciplinary approach. B. Gładysz (Warsaw University of Technology), J. Kaźmierczak, N. Malinovskaya and P. Malinovskii (National Research University) and A. Andreev (Moscow Power Engineering Institute) described needs to deal with social challenges and obstacles for interdisciplinary education. Requirements for teaching the teachers for value-driven technologies was discussed by M. Sotoudeh (ITA) to support future engineers to design technical innovations dealing with societal challenge.

Impacts of (new) technologies worldwide

„International TA perspectives" with cases from India, South Korea (M. Choi, Korea Institute of S & T Evaluation and Planning), Mexico, Jamaica and Germany showed that problem-orientation and interdisciplinary methodology of TA offer a promising frame to deal with cultural and ethical questions in relation to new and emerging technologies. The variety of presentations from "Science and technology for the people?" (A. Chakraborty, Chalmers University of Technology), "TA in forestry sector under climate change" (C. Scherz and S. Saha, ITAS), "Urban decentralized water, sanitation and hygiene interventions in technology assessment" (S. Ward, University of the West of England) or "Comparison of Ecosystem Services from Mixed and Monospecific Forests in Southwest Germany" (I. Almeida, Chr. Rösch and S. Saha, ITAS) demonstrated that a global dimension is needed in order to develop meaningful national comparisons, but also in order to approach the analysis of common future challenges on equal footing. The foundation of the globalTA network during the conference was an important step in this direction.

Under the perspective of organizational options, "Platform work" represents a global phenomenon with specific national strategies and impacts as it profoundly challenges traditional forms of organized labor and existing social welfare models. The session ranged from a case perspective of digital labor from Serbia by B. Andjelkovic (Public Policy Research Centre) over to a comparative perspective on recent developments of crowd work in Europe with a focus on Hungary by C. Makó and M. Illéssy (Hungarian Academy of Sciences) to an analysis of Austrian labor conflicts by P. Schörpf (FORBA) and B. Herr (University of Vienna).

What can be said at the end of such a packed conference? The TA-community is very lively. It was very inspiring to see that the community evolves in terms of content and that the debates are not only European but also international. The next TA conference will take place in Karlsruhe in 2021.

Acknowledgement

We thank numerous colleagues for their brief summaries of individual sessions: Anja Bauer, Ulrike Bechthold, Armin Grunwald, Alexandra Kazakova, Stephan Lingner, Maria Maia, Michal Pazour, Dirk Scheer and Ira van Keulen.

Further information

For members of the globalTA network see https://globalta.technology-assessment.info. Slides of the conference's presentations are available at https://bratislava2019.technology-assessment.info.

REZENSION

Prototyping Society

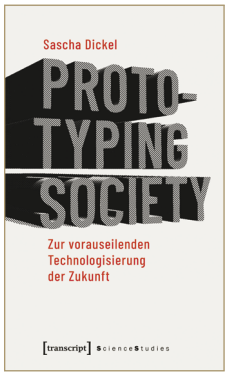
Maximilian Roßmann, *Institut für Technikfolgenabschätzung und Systemanalyse (ITAS), Karlsruher Institut für Technologie (KIT), Karlstr. 11, 76133 Karlsruhe (maximilian.rossmann@kit.edu),*
https://orcid.org/0000-0002-0499-030X)

„Wissen, beraten, gestalten" – so lauteten die Schlüsselbegriffe in der letzten TATuP-Ausgabe über den gesellschaftlichen Weg hin zu nachhaltigen Energiezukünften. Einen Affront hierzu bilden möglicherweise die zwei zentralen Thesen aus Sascha Dickels neuerschienenem Buch „Prototyping Society": Demnach werden erstens technische Zukünfte zunehmend durch die nicht-deliberative Praxis des Prototyping geformt, und zweitens reiche diese Gestaltungspraxis weit in die nicht-technische Welt hinein. Das als PDF-Dokument kostenfrei zugängliche Buch ist übersichtlich strukturiert in fünf Kapitel, die jeweils eine ethnografische Studie und die gesellschaftstheoretische Reflexion ihrer Besonderheit umfassen. Es adressiert ein weites Publikum, bietet Einblicke in Praktiken des Prototyping und regt an, antizipative Routinen in ihrer gesellschaftlichen Einbettung zu hinterfragen.

In fünf ethnografischen Stories führt der Autor in einen „Maker-Space" auf einen „Design-Thinking-Workshop", zu einer „Prototypenparty", auf einen „Hackathon" und zu einem „Beta-Test", und machen Bekanntschaft mit unterschiedlichen Charakteren. Die kurzen Geschichten sind reich an spannenden Beobachtungen, Interviews und Selbstversuchen. Unter anderem beobachtet der Autor Bestrebungen, etablierte Routinen und Machtverhältnisse in der Technikentwicklung zu überwinden, wenn Laien zusammen mit IT-lern eine App entwickeln oder am Prototyp Techniken bewerten. Wenn der Autor zum Beispiel beschreibt, wie in kurzer Zeit aus Pappkarton ein Objekt geformt wird, das ohne weitere Erklärungen einen futuristischen Robo-Krankentransport repräsentiert, zeigt dies die ungewöhnliche und für die Teilnehmenden inspirierende Qualität der Zusammenarbeit. Die beschreibenden Passagen ergänzen sich so zu einem vielseitigen Einblick in Szenen, Sprache und Praktiken gegenwärtiger Zukunftsgestalter, die dem hypothetischen Spekulieren das konkrete Ausprobieren von Ideen vorziehen. Sie bieten eine angenehm kurzweilige Abwechslung und viele Anknüpfungspunkte für theoretische Arbeit zu Technikzukünften.

Der Ansatz des Buches lässt sich verstehen als funktionale Analyse der empirischen Praxis und ihre theoretische Einbettung in aktuelle Gesellschaftsdiagnosen. Um über Prototypen zu sprechen, wird der Begriff nicht in Abgrenzung zu Modellen oder Laborgeräten bestimmt, sondern in der „objectual practice" des Prototyping: Prototypen sind Objekte die „in einer Praxis (1) etwas gegenwärtig verfügbar machen, das zukünftig realisiert werden soll. Sie (2) werden gebaut, um einen Entwurf zu testen. Und sie können (3) dazu dienen, gezeigt zu werden und potenzielle Entscheider zu überzeugen" (S. 32). Für weitere Differenzierung dieser Eingrenzung verweist Dickel auf nötige Folgestudien. Sein Interesse gilt hingegen der funktionsanalytischen Frage, auf welche gegenwärtigen Herausforderungen das Prototyping eine neue Antwort gibt.

Der Ausgangspunkt des Ansatzes geht einher mit der sozialwissenschaftlichen Kritik an Prognostik, Antizipation und Risikoanalyse: Uns ist klar, dass wir nicht wissen können, wie die Zukunft wird. In die Zukunft gerichtete Entscheidungen basieren deshalb auf anfechtbarem Nichtwissen. Für den Umgang mit diesem Problem der unsicheren Zukunft spielten sich deshalb in der Moderne Routinen ein – etwa im Sinne „planvoller wirtschaftlicher Investitionen, Regeln vorrausschauender politischer Staatskunst oder wissenschaftlicher Prognostik." (S. 35) Gegenwärtig forderten insbesondere die Dringlichkeit ökologischer Probleme, das Tempo von Wettbewerb und technischer Innovation sowie eine sich etablierende Kritik an Expertenwissen die eingangs zitierte Trias heraus. Eine gesellschaftliche Antwort auf diese Herausforderungen sei die hier untersuchte Praxis des Prototyping. Im Prototyping würden die Problemlösungen gegenwärtiger Zukünfte iterativ im Feedback mit der realweltlichen Anwendung entwickelt – ohne zuvor alle möglicherweise Betroffenen diskursiv zu beteiligen oder in einem deliberativen Diskurs Argumente abzuwägen. In Form des Prototyps sei die Zukunft keine „anfechtbare Argumentationskette" und „keine vage Vorstellung mehr, sondern etwas, *was mir begegnet*" (S. 37, Hervorhebung im Original). Diese Vergegenwärtigungs- und Evidenzierungspraxis beschränke sich, wie der Autor schreibt, nicht nur auf technische Fragen, sondern etabliere sich als Dispositiv zum Beispiel auch für Organisation und soziales Zusammenleben. Im Prototyping zeige sich somit das Versprechen einer neuen Routine für den Umgang mit Macht unter der Bedingung einer unsicheren Zukunft.



Dickel, Sascha (2019):
Prototyping Society. Zur vorauseilenden Technologisierung der Zukunft (1. Auflage). Science Studies.
Bielefeld: transcript Verlag. 174 Seiten, 27,99 € (Print), ISBN 9783837647365, PDF als Open-Access-Publikation unter: https://www.transcript-verlag.de/978-3-8376-4736-5

https://doi.org/10.14512/tatup.29.1.67

Dickels weitere Diskussion des Prototyping konzentriert sich vor allem auf die Einordnung in aktuelle Gesellschaftsdiagnosen, anstatt das Dispositiv weiter am empirischen Material praxeologisch als Antwort auf Probleme, bzw. auf einen „Notstand" (Foucault), einer zukunftsorientierten Gesellschaft herauszuarbeiten. Zwar reihen sich zugeschriebenen Hoffnungen des Prototyping ein in einen Kanon aus Ökonomisierung der Wissenschaft, Technisierung der Lebenswelt und der Kritik an linearen Innovationsmodellen, welche den Startpunkt technischer Entwicklung in den Disziplinen und Akademien der Wissenschaft verortet. Das Postulat einer Aufhebung und Neukonfiguration von Rollen- und Machtverhältnissen lässt sich jedoch in den empirischen Abschnitten nicht immer nachvollziehen. So legitimieren zum Beispiel die Design-Thinking-Coaches in einer der Fallstudien ihre Autorität durch akademische Titel und Kontakte nach Stanford, die prototypische App-Entwicklung von Laien zusammen mit zwei IT-lern erfolgt eben nicht auf Augenhöhe, und auch die Veranstalterin einer Prototypenparty verleiht offen ihrer Enttäuschung Ausdruck, dass für die Bewertung der materialisierten Zukünfte leider nur Laien, aber keine Investoren anwesend sind. Die empirischen Beboachtungen bestätigen die berechtigte Kritik am Postulat linearer Innovationsmodelle. Sie vermögen es aber nicht, ein Dispositiv zu plausibilisieren.

Das Buch stellt die funktionsanalytische Frage: Auf welche gegenwärtigen Herausforderungen gibt das Prototyping eine neue Antwort?

Für eine ausstehende Theoretisierung des Prototyping gibt die Fußnote auf S. 49 zu Kendall Waltons kunstphilosophischen „make-believe" Theorie einen interessanten Anstoß. Verstanden als Requisiten („props in a game of make-believe") umfasst die oben genannte Definition Prototypen und wissenschaftliche Modelle nämlich gleichermaßen. Diese doppelte Bedeutung von Prototyping als einerseits theoretisch-konzipierende, andererseits künstlerisch-darstellende Praxis könnte einen Raum für theoretisierende Reflexionen eröffnen, die sowohl das Erfahrbarmachen und Testen von Zukünften als auch ihre politische Verwendung zur Überzeugung von Investoren und Stakeholdern mit einbeziehen. Die Diagnose einer prototypisierenden Gesellschaft müsste dann jedoch gegenüber einer modellierenden, realexperimentellen oder ingenieurstechnisch geprägten Gesellschaft (*engineering society*) durch eine neue Distinktion verteidigt werden. Als Synthese zeigt sich im gesellschaftlichen Umgang mit der unsicheren Zukunft jedenfalls bereits jetzt eine neue Macht der Requisiten.

Das Buch besticht vor allem durch empirische Beobachtungen und neue Denkansätze. Um zu überzeugen, dass das Prototyping nicht nur alte Hoffnungen und bekannte Phänomene unter einem neuen Label zusammenfasst, sondern als neues Leitbild die Gestaltung von Zukünften maßgeblich verändert, müssen jetzt weitere Studien daran anschließen. Der Anspruch des Buchs ist also keine umfassende Theorie oder abschließende Analyse einer prototypsierienden Gesellschaft, sondern der Auftakt einer neuen Auseinandersetzung mit Materialität, Medialität und Sozialität antizipatorischer Praktiken. Die gründlichen Literaturbezüge machen die empirischen Beobachtungen höchst anschlussfähig, stellen Fragen und verbinden gegenwärtige Debatten, auch über das Prototyping hinaus: Wie kann es gelingen, allein durch ein Modell, die Imagination einer soziotechnischen Zukunft zu kommunizieren? Wer ist für das Resultat verantwortlich, wenn sich das diskursive Gestalten technokratisch in der Widerständigkeit iterativer Technikgestaltung naturalisiert? Ist der Prototyp ein „epistemisches Objekt" oder eher ein „potenzielles Produkt", dessen gegenwärtiger und künftiger Wert durch Zuschreibungen getragen wird? Findet sich im Design von Erfahrungen fiktiver Zukünfte möglicherweise eine Antwort auf die Fragen, warum „Techno-Fixes" heute die bevorzugte Problemlösung sind und Systemkritik sowie rationale Politikberatung häufig ins Leere laufen? Können und wollen wir von dem Ansatz gar lernen, nicht TA-Berichte zu schreiben, sondern in prototypischer Form überzeugende Erfahrungen von Technikfolgen und nachhaltigen Lebenskonzepten zu designen? Wer nun eine wohlbegründete Antwort erwartet, muss leider vertröstet werden, denn: „Prototyping als kritische Praxis muss selbst prototypisiert werden" (S. 156). Für Forschung und Technikfolgenabschätzung unter dem Motto „Living The Change" ist Sascha Dickels „Prototyping Society" deshalb das Buch der Stunde.

REZENSION

Süddeutsche „Umwelt-, Klima und Konsum-geschichte“

Marius Albiez, *Institut für Technikfolgenabschätzung und Systemanalyse (ITAS), Karlsruher Institut für Technologie (KIT), Karlstr. 11, 76133 Karlsruhe (m.albiez@kit.edu),* https://orcid.org/0000-0002-5421-4990

Die anthropogen verursachte Erwärmung der Atmosphäre und die damit einhergehenden klimatischen sowie ökologischen Auswirkungen betreffen in hohem Maße das Zusammenleben heutiger und zukünftiger Generationen. Die Art und Weise wie wir Energie nutzen oder Ressourcen verbrauchen sind wichtige Ansatzpunkte für den globalen Klimaschutz. So erregte die Internationale Energieagentur (IEA) Aufsehen, als sie im Vorfeld des World Energy Outlook 2019 explizit auf die steigenden Treibhausgas-Emissionen durch Geländewagen, kurz SUVs, hinwies. Gesellschaftliche Konsummuster, Klima und Umwelt bedingen einander, dennoch gibt es vergleichsweise wenige Arbeiten, welche die historischen Zusammenhänge dieses Wirkungsgefüges nachzeichnen. An dieser Stelle setzt der von Wolfgang Wüst und Gisela Drossbach herausgegebene Sammelband „Umwelt-, Klima- und Konsumgeschichte. Fallstudien zu Süddeutschland, Österreich und der Schweiz“ an. Die vorliegende Rezension gliedert sich in drei Teile: Zunächst stehen die Struktur des Buches und inhaltliche Schwerpunkte im Zentrum. Anschließend werden fachliche und methodologische Anknüpfungspunkte an das Feld der Technikfolgenabschätzung (TA) aufgezeigt. Der Beitrag schließt mit einer übergreifenden Bewertung durch den Autor.

Von Schwaben bis nach Oberösterreich

Das Buch startet mit einer Einführung, welche den Anlass, die räumlichen Bezüge sowie erste Schlüsselbegriffe, beispielsweise „Umwelt- und Konsumgeschichte“, vorstellt. Es folgt eine zweiteilige Zusammenfassung der Tagungen, auf denen das Werk basiert. Kernstück des Sammelbands sind vier Sektionen, die sich hinsichtlich ihrer räumlichen, beziehungsweise regionalen Zuordnung unterscheiden. Einige Fallstudien umfassen sehr lange Zeiträume und decken ganze Epochen ab, andere fokussieren vergleichsweise kurze Zeitspannen, beispielsweise mehrere Jahrzehnte eines Jahrhunderts. Mit Blick auf ihre TA-Relevanz werden in der Folge einzelne Beiträge diskutiert.

In der ersten Sektion finden sich vier Beiträge, die sich auf die Region Franken beziehen. Thomas Hagen beschäftigt sich in seinem Aufsatz mit der Historie des Biermonopols in der frühen Neuzeit und den damit einhergehenden Konflikten zwischen den Begünstigten, potenziellen Mitbewerbenden und Konsument*innen. Der Autor geht dabei nicht nur auf die beteiligten Akteure ein, sondern zeigt auch auf, welche klimatischen und konsumrelevanten Faktoren zu einer Steigerung der Biernachfrage beitrugen. Sabine Wüst analysiert das gewerbsmäßige Sammeln von Honig und Bienenvölkern, das sogenannte „Zeidelwesen“, aus umweltgeschichtlicher Perspektive. Insbesondere die Kirche und ihre hohe Nachfrage nach Wachs und Honig waren hier ein wesentlicher Konsumfaktor, aber auch die Nürnberger Lebkuchenindustrie.

Die zweite Sektion vereint sieben Beiträge, die in der Region Schwaben und Pfalz-Neuburg verortet sind. Die Themen sind dabei äußerst vielseitig. Die Spanne reicht von der Lebensmittelversorgung in mittelalterlichen Spitälern über die Entwicklung der Augsburger Trinkwasserversorgung bis hin zur Wahrnehmung von Naturräumen in der Stadt. Hier finden sich auch Einblicke in die jüngere Geschichte. So untersucht Nadja Hendriks Verständnisse und Umsetzungsstrategien des Leitbilds Nachhaltiger Entwicklung auf kommunaler Ebene von den 1970er-Jahren bis zu den Anfängen der Jahrtausendwende in der Gemeinde Buttenwiesen.

Sektion drei umfasst vier Beiträge, deren räumlicher Schwerpunkt auf ganz Bayern liegt. Wolfang Wüst setzt sich mit dem Leitbild Nachhaltiger Entwicklung vor allem zwischen dem 16. und 18. Jahrhundert sowie mit der Historie des Spargelanbaus in Bayern auseinander. In Martin Knolls Beitrag erfahren die Lesenden zudem, dass jagdkritische Haltungen und Schriften bis auf die frühe Neuzeit zurückgehen. In der vierten und letzten Sektion wird der räumliche Fokus auf Österreich, die Schweiz und Europa erweitert. Einen Schwerpunkt bilden Natur- sowie Wetterereignisse und deren Folgen. In der historischen Nachbe-

Wüst, Wolfgang; Drossbach, Gisela (Hg.) (2018):
Umwelt-, Klima- und Konsumgeschichte. Fallstudien zu Süddeutschland, Österreich und der Schweiz.
Berlin: Peter Lang GmbH.
94,95 Euro, ISBN 9783631777480

https://doi.org/10.14512/tatup.29.1.69

trachtung spielt dabei die Subjektivität von Beobachtenden eine wichtige Rolle. Thomas Wozniak wirft beispielsweise einen Blick auf Naturereignisse im Frühmittelalter und geht der Frage nach, inwiefern bei der Analyse religiöse Einflüsse berücksichtigt werden müssen.

Gesellschaft, Umwelt, Klima – und Technik

Mit Blick auf die TA-Relevanz der Beiträge finden sich an vielen Stellen des Buches Ausführungen zu technischen Entwicklungen und den damit einhergehenden historischen Folgen. Explizit wird dies in Gerhard Fritz' Analyse zu Auswirkungen von Naturereignissen auf wasserbetriebene Mühlanlagen deutlich, insbesondere zwischen dem 13. und 15. Jahrhundert. Wasserkraft diente als Hauptenergiequelle, sodass Hochwasser, Dürren und Eis die Kornproduktion erheblich beeinflussten. Neben diesen Überlegungen, geht der Autor auf weitere Folgen ein. Mühlen lagen für gewöhnlich nicht an natürlichen Wasserläufen, sodass Mühlkanäle errichtet werden mussten. Diese Kanäle waren nicht selten Gegenstand von Konflikten, sei es durch die Verteilung der Wasserressourcen oder durch gegenläufige Nutzungsinteressieren, verursacht z. B. durch Fischfang und Gerberei.

Neue Infrastrukturen zur Wasserversorgung transformierten Wasser von einem Naturgut hin zum Konsumprodukt.

Als weiteres Beispiel kann die Geschichte privater Wasseranschlüsse zwischen dem 16. und dem Beginn des 19. Jahrhunderts von Barbara Rajkay genannt werden. Sie macht deutlich, welchen Einfluss großangelegte Infrastrukturen auf die Stadtentwicklung Augsburgs hatten und inwiefern Fragen der Gerechtigkeit eine Rolle spielten, beispielsweise durch den Zugang zu Trinkwasser. Besonders eindrücklich zeichnet die Verfasserin die Transformation von Wasser als Naturgut hin zum Konsumprodukt nach. Des Weiteren untersucht Günter Dippold in seinem Beitrag zum Fischkonsum die Entwicklung der künstlich geschaffenen Teichwirtschaft und berücksichtigt damit einhergehende gesellschaftliche Debatten. Er verweist auch auf Aufzeichnungen des Privatiers Johann Schirmer gegen Ende des 19. Jahrhunderts zu Überfischung und Toxinen aus Fabriken. Handelt es sich bei Schirmers Arbeiten um eine frühe Form von „Citizen Science"?

Eine Herausforderung in der TA ist darüber hinaus die Verfügbarkeit von Daten, beziehungsweise der Umgang mit unsicheren Wissensbeständen. Die einzelnen Autor*innen beschreiten hier unterschiedliche Wege und Umwege, die auch interessante Impulse für die TA bieten können. So erstellt Christian Rohr Klassifikationskriterien für Hochwasser, indem er Aufzeichnungen für Reparaturkosten und Instandhaltung einer Brücke zwischen dem 15. und 16. Jahrhundert analysiert. Als weiteres Beispiel können Wolfgang Wüsts Analysen historischer Holz-, Forst- und Waldordnungen genannt werden, um den Ursprüngen des Nachhaltigkeitsprinzips in der Forstwirtschaft nachzuspüren. Zudem gibt Michaela Hermann Einblicke in die Arbeit der Archäologie und geht der Frage nach, inwieweit das historische Warenangebot Augsburgs durch Ausgrabungen alter Latrinen und Müllhalden rekonstruiert werden kann.

Fazit

Nach der Lektüre des Bandes fällt es dem Autor dieser Rezension schwer, jenseits des Verhältnisses von Umwelt, Klima und Konsum, eine allgemeingültige Fragestellung für das Buch herauszuarbeiten. Vielmehr vereint der Band ein breites Spektrum an Themen, die auf unterschiedlichen räumlichen Ebenen und über unterschiedliche historische Zeitspannen beleuchtet werden. Manche Beiträge beziehen sich in erster Linie auf einzelne Forschungsfelder, beispielsweise die Konsumgeschichte, andere greifen alle im Buchtitel genannten Felder auf. Aus TA-Perspektive wäre es durchaus interessant zu erfahren, welchen tiefergehenden Erkenntnisgewinn man sich gerade aus der Integration von umwelt-, klima- und konsumhistorischen Aspekten und dem Zusammenspiel der unterschiedlichen Aufsätze erhofft. Dies wird zwar Stellenweise aufgegriffen, hätte aber noch mehr zusammengeführt und ausgearbeitet werden können. Hier wäre neben der Einführung und den Zusammenfassungen zu Beginn ein weiteres übergreifendes Kapitel wünschenswert. Der Autor dieser Rezension hätte darüber hinaus gerne mehr zur Rolle des Leitbilds Nachhaltiger Entwicklung in der Umwelt- und Konsumgeschichte erfahren, allem voran auf welches Nachhaltigkeitsverständnis sich die Herausgebenden beziehen. Ungewöhnliche Begrifflichkeiten wie „Karma-Konsum" (S. 23) machen neugierig und hätten ebenfalls gegen Ende noch vertieft werden können. Zudem wären weitere übergreifende Erläuterungen zu den unterschiedlichen Verständnissen der Forschungsfelder hilfreich gewesen. Auch werden in den Aufsätzen immer wieder historische und argumentative Nebenexkurse unternommen, deren Motivation für den Autor nicht immer ersichtlich ist. Darüber hinaus möchte der Autor anregen, in einer weiteren Auflage zusätzliches (historisches) Kartenmaterial für Ortsunkundige aufzunehmen.

Ein großer Verdienst der Beteiligten ist sicherlich, dass sie den Versuch unternehmen, bisher wenig beachtete Forschungsfelder in der Geschichtswissenschaft aufzugreifen und zusammenzuführen. Die Beiträge sind auch für nicht-Historiker*innen verständlich verfasst, sodass das Werk zur wissenschaftlichen Arbeit, aber auch zum Schmökern und Entdecken genutzt werden kann. Zudem zeichnen sich die einzelnen Beiträge durch sorgfältige Recherche und Aufarbeitung aus. Besonders beeindruckt das Werk durch seine inhaltliche Breite, weshalb sich das Buch besonders gut für eine interdisziplinär denkende Leserschaft eignet.

PRAXIS

TA im österreichischen Regierungs-programm

Michael Nentwich, *Institut für Technikfolgen-Abschätzung (ITA), Österreichische Akademie der Wissenschaften, Apostelgasse 23, 1030 Wien (mnent@oeaw.ac.at),* https://orcid.org/0000-0003-2269-0076

Nach der mehrmonatigen Phase einer Expert*innen-Regierung, neuen Nationalratswahlen im September 2019 und den folgenden Koalitionsverhandlungen wurde Anfang 2020 eine Koalitionsregierung, erstmals bestehend aus der Österreichischen Volkspartei (ÖVP) und den Grünen, angelobt. Ergebnis der Koalitionsverhandlungen ist das nun vorliegende Regierungsprogramm 2020–2024.

Schon der Titel des Programms „Aus Verantwortung für Österreich" spricht von Verantwortung und lässt mit Blick auf Forschung und Innovation an *Responsible Research and Innovation* denken. In der Tat finden sich in diesem Übereinkommen bei genauerer Lektüre zahlreiche Hinweise auf die Notwendigkeit evidenzbasierter Politik, insbesondere von Technikfolgenabschätzung (TA) im Vorfeld technologie- und innovationspolitischer Entscheidungen. Im Zusammenhang mit der Digitalisierung nimmt sich die neue Bundesregierung die

> *„Durchführung hersteller- bzw. betreiberunabhängiger Technikfolgenabschätzungen bei wesentlichen öffentlichen Digitalisierungsvorhaben sowie verstärkte Durchführung von Technikfolgenabschätzungen bei risikogeneigten Regelungsmaterien (z. B. intelligente Transportsysteme, selbstfahrende Fahrzeuge, Assistenz- und Leitsysteme etc.)" (S. 324)*

vor. Konkret wird auch auf die Notwendigkeit der Berücksichtigung wissenschaftlicher Erkenntnisse aus der aktuell laufenden Studie des Instituts für Technikfolgen-Abschätzung (ITA) und des Austrian Institute of Technology (AIT) zu Gesundheitsrisiken der nächsten Mobilfunkgeneration 5G Bezug genommen (S. 317).

Darüber hinaus ist an zahlreichen Stellen von ethischer Begleitung der Einführung neuer Technologien die Rede, wie etwa des autonomen Fahrens (S. 136). Auch der Begriff der „Digitalisierungsethik" (S. 326) und die mit der TA verwandten Begriffe „Umweltfolgenabschätzung" (S. 157) und „Wirkungsfolgenabschätzung" (S. 104) sowie das „Vorsorgeprinzip" (S. 136) kommen vor. Konkrete TA-Themen, die auch schon von der TA-Community bearbeitet wurden/werden, sind etwa die Regulierung von Drohnen (S. 135), die Digitale Souveränität (S. 215) sowie Datenschutz und Privatsphäre, inklusive Datenschutz-by-Design (S. 320) und „datenschutz- und grundrechtsfreundliche Technikgestaltung" der Wirtschaft 4.0 (S. 323). Auch die häufig von der TA als Desiderat ins Spiel gebrachte Aufwertung der Datenschutzbehörde (S. 324) und deren Ausstattung mit ausreichenden Ressourcen (S. 27) finden sich im Programm.

Das wichtige Zukunftsthema „Künstliche Intelligenz" wurde von den Koalitionspartnern nicht nur als wirtschaftliche Chance begriffen, sondern auch der intensive Diskussionsbedarf in diesem Zusammenhang anerkannt (S. 325). Konkret wird ein Credo der TA als Leitlinie für die zukünftige Regierungsarbeit festgehalten:

> *„Ethische Reflexion hat ein immanenter Bestandteil der österreichischen KI-Politik und -Praxis zu sein (Human-Centered AI). KI-Entwicklung muss den Menschen und dessen Rechte im Blick haben, zum Beispiel hinsichtlich der Unterscheidbarkeit von Menschen und Maschine und des Schutzes von Konsumentinnen und Konsumenten." (S. 325)*

Schließlich ist aus Sicht der TA der sich durchziehende Fokus auf Umwelt- und Nachhaltigkeitskriterien zu begrüßen, etwa im Zusammenhang mit dem Ziel der „Green-IT" in der Bundesverwaltung (S. 320), bei der Entwicklung von Konsumprodukten (S. 39) sowie insbesondere in den Bereichen Mobilität (ab S. 120) und Energie (ab S. 102). Angesichts dieser Bekenntnisse und Vorhaben der neuen Regierung ist Optimismus angezeigt, dass Österreich den bewährten Pfad evidenzbasierter Politik in den kommenden Jahren zu einer mehrspurigen Straße ausbauen könnte.

Zum Nachlesen

Die neue Volkspartei und Die Grünen – Die Grüne Alternative (2020): Aus Verantwortung für Österreich. Regierungsprogramm 2020–2024. Online verfügbar unter dieneuevolkspartei.at/Download/Regierungsprogramm_2020.pdf bzw. gruene.at/themen/demokratie-verfassung/regierungsuebereinkommen-tuerkis-gruen/regierungsuebereinkommen.pdf.

TATuPDates

TATuP
Jg. 29, Bd. 2 erscheint
im Juli 2020 zum THEMA

„Amplified socio-technical problems in converging infrastructures“

Um den Ausstoß von Treibhausgasen dauerhaft zu reduzieren, sind nicht nur Anpassungen in einzelnen Sektoren wie Elektrizität, Transport oder Produktion erforderlich. Vielmehr müssen Sektoren intelligent miteinander gekoppelt werden, gerade weil ihre Integration sowie neues Nutzerverhalten Komplexität und Unsicherheit drastisch erhöht. Wie kann in diesem strukturellen Wandel das Funktionieren (kritischer) Infrastrukturen gewährleistet werden? Welche von technischen und sozialen Folgen entstehen aus der Sektorenkopplung? Gastherausgeber dieses TATuP-Themas sind Christian Büscher (KIT, Karlsruhe), Michael Ornetzeder (ITA, Wien), Bert Droste-Franke (IQIB gGmbH).

CALL FOR THEMA

Der Call für Einreichungen neuer TATuP-Themen ab Heft 2/2021 endete zum 31. Januar 2020. Die Redaktion dankt allen Einreicherinnen und Einreichern.

PUBLIZIEREN IN TATuP

Die TATuP-Webseite bietet Autorinnen und Autoren detaillierte Informationen über die Einreichung von Manuskripten und über die folgenden Redaktionsprozesse. TATuP ist frei zugänglich (open access), es werden keine „Author Processing Charges“ (APC) erhoben.
www.tatup.de/index.php/tatup/about/submissions

TATuP-ARCHIV

Die Integration von Archivbeständen in die digitale Plattform www.tatup.de ist abgeschlossen! Das TATuP-Archiv ist frei zugänglich *(open access)*, es bietet u. a. eine Schlagwortsuche in Metadaten und Volltexten aller Beiträge und wird somit auch zum historischen Archiv über Debatten und Diskurse in der Technikfolgenabschätzung. Auch Beiträge aus der Zeit vor dem Relaunch in Jg. 26 Heft 1–2 (2017) sind nun mit DOI zitierfähig.
www.tatup.de/index.php/tatup/issue/archive.

BEITRÄGE EINREICHEN UND ONLINE LESEN


www.tatup.de

AUF DEM LAUFENDEN BLEIBEN


www.oekom.de/newsletter

KOMMENTIEREN, TEILEN, LIKEN


www.facebook.com/TAjournal


www.twitter.com/TAjournal

Ein wunderschönes Erklärbuch zum Klimawandel

»Man ist nie zu klein dafür, einen Unterschied zu machen!«

Greta Thunberg

Ausgestattet mit liebevollen Illustrationen, bringt diese Erzählung Kindern ab 5 Jahren die Klimakrise nahe. Das Buch zeigt, dass es sich lohnt, sich zusammenzutun, und dass Klimaschutz sogar richtig Spaß machen kann!

Christina Hagn

Vom kleinen Eisbären, dem es zu warm geworden ist

oekom verlag, München
36 Seiten, Hardcover, vierfarbig, komplett illustriert, 14 Euro
ISBN: 978-3-96238-174-5
Erscheinungstermin: 04.02.2020
Auch als E-Book erhältlich

Hommage an den Eigensinn der Natur

»Ein guter Garten ist mehr als ein wohlfeiles Zurück zur Natur.«

Eva Rosenkranz

Für Eva Rosenkranz sind es die Widersprüche, die den Garten so faszinierend machen. Ihr Buch flaniert zwischen Sinnlichkeit und Gummistiefeln, Magie und Regenwurm, Zuversicht und Tragödien. Ein unterhaltsamer und lehrreicher Rundgang durch das Gartenjahr.

Eva Rosenkranz

Überall ist Garten

Zufluchtsort zwischen Lebenskunst und Überleben

oekom verlag, München
ca. 272 Seiten, Hardcover mit Leinenrücken, komplett vierfarbig mit Illustrationen, 25,– Euro
ISBN: 978-3-96238-107-3
Erscheinungstermin: 07.10.2019
Auch als E-Book erhältlich

natürlich oekom!

Mit dieser Zeitschrift halten Sie ein echtes Stück Nachhaltigkeit in den Händen. Durch Ihren Kauf unterstützen Sie eine Produktion mit hohen ökologischen Ansprüchen.

Wir...

- verwenden 100 % Recyclingpapier und mineralölfreie Druckfarben
- verzichten auf Plastikfolie
- kompensieren alle klimaschädigenden Emissionen
- drucken in Deutschland – und sorgen damit für kurze Transportwege

Weitere Informationen finden Sie unter www.natürlich-oekom.de und #natürlichoekom.

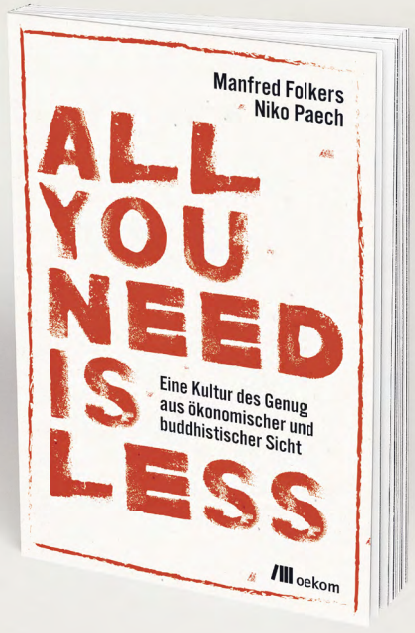
oekom

Glück durch Genügsamkeit

»Gegen die Klimakrise hilft nur eine Kultur des Genug.«

Niko Paech

Achtsamkeit und Nachhaltigkeit sind in aller Munde. Sie sind die zentralen Pfeiler der modernen Suffizienz-Bewegung, aber auch der Lehre des Buddha. Die Autoren loten aus, welche Potenziale diese Konzepte enthalten, um den Wachstumspfad zu verlassen und eine Kultur des Genug zu entwickeln.



Manfred Folkers, Niko Paech

All you need is less

Eine Kultur des Genug aus ökonomischer und buddhistischer Sicht

oekom verlag, München
256 Seiten, Klappenbroschur, 20 Euro
ISBN: 978-3-96238-058-8
Erscheinungstermin: 17.03.2020
Auch als E-Book erhältlich