

E..f..F..Kommunikation

Zeitschrift für Informatik und Gesellschaft

37. Jahrgang 2020

Einzelpreis: 7 EUR

1/2020 – März 2020

KÜNSTLICHE INTELLIGENZ

WuNDER^{als}LAND

FIFF 19
KON

22-24.11.19
UNIVERSITÄT
BREMEN



ISSN 0938-3476

• Im Bann der Netzwerke • Digitalisierung an Schulen • Weizenbaum-Studienpreis •

Inhalt

Ausgabe 1/2020

inhalt

- 03 Editorial
- Stefan HÜgel

Forum

- 04 Der Brief: Konservativ vs. „konservativ“
- Stefan HÜgel
- 06 Im Bann der Netzwerke
- Markus Reinisch
- 09 Digitalisierung an Schulen – so nicht!
- FlFF e. V. – Pressemitteilung
- 10 Bündnis fordert Verbot automatisierter Gesichtserkennung
- FlFF e. V. – Pressemitteilung
- 11 Gesetz zur Änderung des NetzDG und Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität
- Gemeinsamer Appell des FlFF und 11 Verbände

Schwerpunkt „Weizenbaum-Studienpreis 2019“

- 64 Weizenbaum-Studienpreis 2019 – Einleitung
- Stefan HÜgel
- 64 Thomas Gruber: Verquickung der mathematischen und informatischen Forschung an zivilen deutschen Hochschulen mit der modernen Kriegführung
- Laudatio für den 1. Preis von Stefan HÜgel
- 66 Mathematik, Informatik und Krieg
- Thomas Gruber
- 70 Alexandra Keiner: Legitimität von Algorithmen in politischen Verwaltungsorganisationen
- Laudatio für den 2. Preis von Richard Schöbel
- 71 Algorithmen im Asylprozess
- Alexandra E. Keiner
- 76 Philipp Imperatori: Verschlüsselungspolitik der USA
- Laudatio für den 2. Preis von Stefan HÜgel
- 77 Verschlüsselungspolitik der USA
- Philipp Imperatori, Thea Riebe und Christian Reuter

Rubriken

- 83 Impressum/Aktuelle Ankündigungen
- 84 SchlussFlFF

Titelbild: Caro von Totth nach einem Entwurf von Karin Vosseberg. Motiv der FlFFKon 2019

Schwerpunkt „#FlFFKon19“

- 14 Künstliche Intelligenz als Wunderland
Editorial zum Schwerpunkt
- Michael Ahlmann, Hans-Jörg Kreowski, Philip Love, Ralf E. Streibl, Karin Vosseberg, Margita Zallmann
- 16 Künstliche Intelligenz als Wunderland
- Stefan HÜgel
- 17 Die Empfehlungen der Datenethikkommission: Bedeutung für die Informatik
- Marit Hansen
- 21 Viel Lärm um Wenig
- Veronika Thiel
- 24 Geschlossene Gesellschaft
- Alexander von Gernler
- 26 Die Produktionsbedingungen Künstlicher Intelligenz
- Christoph Marischka und Dominik Wetzel
- 29 AG: Schöne neue Arbeitswelt 4.0?
- Birgit und Michael Ahlmann
- 31 AG: Gesundheitsdaten müssen aus den Fängen des Datenschutzes befreit werden
- Sylvia Johnigk
- 33 Eine Frage der Macht – Nachhaltigkeit und Digitalisierung
- Marie-Luise Abshagen und Nelly Grotefendt
- 36 Wird KI die Welt retten?
- Bernhard Stoevesandt und Martin Dörenkämper
- 39 AG: Demokratie und Überwachungskapitalismus
- Arkadi Schelling
- 40 AG: Nachhaltigkeitskultur in der Informatik
- Ulrike Erb, Oliver Radfelder und Karin Vosseberg
- 44 Technologiekritik als Herrschaftskritik
- Capulcu
- 47 EU weitet Meeresüberwachung mit Drohnen aus
- Matthias Monroy
- 48 Silicon Valley zieht in den Krieg
- Elke Schwarz
- 52 AG: „Ziviler Betrieb“
- Peter Ansorge
- 54 AG: Zivilklausel durchsetzen!
- Liam Hurwitz und Simon Rundé
- 56 Joseph Weizenbaum, Eliza und das Bild in der KI
- Detlef Borchers
- 59 Jahresrückblick 2018/19
- Stefan HÜgel und Rainer Rehak

FlFF e. V.

- 81 Protokoll der Mitgliederversammlung des FlFF

Editorial

Künstliche Intelligenz als Wunderland – vom 22.-24. November 2019 fand in Bremen unsere FlFF-Konferenz 2019 statt. Traditionell ist die darauf folgende Ausgabe der FlFF-Kommunikation der Konferenz und ihren Ergebnissen gewidmet.

Das Leitmotiv der Konferenz nimmt Bezug auf *Alice im Wunderland*, den Roman von Lewis Carroll, in dem die Protagonistin phantastische Abenteuer erlebt und skurrile Gestalten trifft. In unserer Einladung hieß es:

In der berühmten Erzählung Alice im Wunderland von Lewis Carroll begegnet die Protagonistin im Wunderland den merkwürdigsten Gestalten und erlebt kuriose Abenteuer. Ein neues Wunderland eröffnet sich heute durch Künstliche Intelligenz. Es ist von Robotern bevölkert, die Fußball spielen, tanzen, jonglieren, kochen, Dienstleistungen aller Art erbringen, Alte und Kranke pflegen und Orte erkunden, die für Menschen gefährlich oder unerreichbar sind. Es gibt dort selbstfahrende Autos und unbemannte Flugobjekte. Lernende neuronale Netze beeindrucken, weil sie fast alle Spiele gegen fast alle Spielerinnen und Spieler gewinnen. Man trifft allenthalben auf Systeme, die sehen, lesen, sprechen und lernen können. Und es wird gemunkelt, dass sich demnächst eine neue Spezies mit Superintelligenz dazu gesellen wird, die besser denken kann als alle Menschen zusammen.

Diese Ausgabe enthält die schriftlichen Fassungen der Beiträge zur Konferenz. Im Schwerpunkteditorial führen die OrganisatorInnen ausführlich in die Inhalte ein. Neben den Beiträgen der Referentinnen und Referenten enthält der Schwerpunkt auch einen Rückblick auf die Aktivitäten des vergangenen FlFF-Jahres.

Seit nunmehr zehn Jahren verleihen wir auf der FlFF-Konferenz den *Weizenbaum-Studienpreis* – früher *FlFF-Studienpreis* – für herausragende Abschlussarbeiten mit Bezug zu *Informatik und Gesellschaft*, so auch dieses Jahr. Die Laudationes und die Beiträge der Preisträgerin und der Preisträger sind ebenfalls in dieser Ausgabe enthalten.

Mit der *Aufmerksamkeitsökonomie und der subtilen Steuerung in sozialen Medien* setzt sich Markus Reinisch in seinem Beitrag auseinander: *Im Bann der Netzwerke*. Er formuliert darin fünf Ziele der schulischen Bildung zur Digitalisierung:

1. sich seiner „digitalen Identität“ bewusst zu werden,
2. die Fremdsteuerung nachzuvollziehen und
3. dabei das Subtile dieser Steuerung zu durchschauen. Schließlich sollten die Einsichten
4. zur Erkenntnis führen, dass Kommunikations-, Lern- und Identitätsbildungsprozesse zwischen realweltlichen und netzbasierten Welten, zwischen Nähe und Distanz, „zwischen Tiefe und Seichtheit, Profundität und Oberflächlichkeit, Wärme und Coolness, Herzlichkeit und Flüchtigkeit“ stattfinden.

5. In einem weiteren Schritt könnte es idealiter darum gehen, diese beiden Welten zueinander kritisch in Bezug setzen und daraus persönliche Konsequenzen für den Mediengebrauch ziehen zu können.

In einer Pressemitteilung zum *Digitalpakt* der Bundesregierung kritisieren wir eine Lizenz-Politik, die die Nutzung von Microsoft-Produkten bevorzugt, und fordern die datenschutzkonforme Verarbeitung der Daten von Schülerinnen und Schülern, die zu meist minderjährig sind. Warum wird hier nicht eine äquivalente Open-Source-Software-Lösung eingesetzt, so fragen wir. Damit könnten deutsche Schulen und Institutionen die Kontrolle über ihre Daten behalten, datenschutzkonforme Implementierungen leichter umsetzen und transparent die Datenschutzbestimmungen sicherstellen. Letzteres ist jedoch im Rahmen der verfügbaren und finanzierbaren Lösung mit Microsoft 365 kaum bis gar nicht zu garantieren.

Das Bundesinnen- und -heimatministerium hat einen Vorstoß unternommen, an 135 Bahnhöfen und 14 Flughäfen automatisierte Gesichtserkennung einzusetzen. Wir sehen darin eine Bedrohung der Freiheitsrechte und der Demokratie, konkret durch:

- Diskriminierung,
- Gefahr für die Demokratie,
- Missbrauchspotenzial,
- Falscherkennung,
- einfache Umgehung.

Gemeinsam mit weiteren zivilgesellschaftlichen Organisationen fordern wir deswegen ein Verbot. „Wir müssen uns jetzt diesen gefährlichen Plänen in den Weg stellen, bevor immer mehr öffentliche Räume mit biometrischen Erkennungssystemen bestückt werden, die zudem nicht einmal mehr Sicherheit bringen“, heißt es dazu in der Pressemitteilung, die wir aus diesem Anlass herausgegeben haben und die in dieser Ausgabe enthalten ist. Weitere Informationen zur Kampagne gibt es unter <https://www.gesichtserkennung-stoppen.de>.

In einem offenen Brief wandten wir uns gegen die vorliegenden Entwürfe für ein Gesetz zur Änderung des Netzwerkdurchsetzungsgesetzes und ein Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität:

Die ... Gesetzentwürfe ... sollen zwar erklärtermaßen dem Schutz der Meinungsfreiheit dienen, schaffen jedoch selbst eine enorme Gefahr für die bürgerlichen Freiheiten,

schreiben wir dazu in dem Brief an die Bundesministerin für Justiz und für Verbraucherschutz.

Wir wünschen unseren Leserinnen und Lesern eine interessante und anregende Lektüre – und viele neue Erkenntnisse und Einsichten.

Stefan Hügel
für die Redaktion



Konservativ vs. „konservativ“

Warum das nicht das Gleiche ist

Die weltweiten Krisen in Umwelt und Gesellschaft sind kein Zufall. Sie offenbaren, wie wir mit uns und dem Planeten umgehen, auf dem wir leben. Wenn wir diese Krisen meistern wollen, müssen wir uns die Regeln bewusst machen, nach denen wir unser Wirtschaftssystem aufgebaut haben. Erst wenn wir sie erkennen, können wir sie auch verändern – und unsere Freiheit zurückgewinnen.

Maja Göpel¹



Liebe Freundinnen und Freunde, liebe Mitglieder des FIFF,

gibt es einen Unterschied zwischen konservativ und „konservativ“?

Seit Beginn der Bundesrepublik werden wir überwiegend von „Konservativen“ regiert – so die verbreitete Einschätzung der politischen Ausrichtung vor allem der CDU und der CSU. Doch was bedeutet es eigentlich, konservativ zu sein? Die Lateinerin weiß: „Konservativ“ kommt von „conservare“ – das bedeutet soviel wie „bewahren“. Aber was ist es, das bewahrt werden soll? Gibt es also einen Unterschied zwischen konservativ und „konservativ“, wie der Titel suggeriert? Und was hat das mit dem Eingangszitat zu tun?

Eine existenzielle Frage der Menschheit ist heute die Klimakrise. 1980 wurden in Westdeutschland die *Grünen* gegründet. Sie engagierten sich gegen die Zerstörung der Umwelt und gegen die Vernichtung des menschlichen Lebens durch einen Atomkrieg. Sie wollten die Natur und die Menschheit bewahren – klassische Konservative also? Mitnichten. Sie galten – und gelten vielen bis heute – als „links“, also gerade nicht als konservativ.

Umweltschutz ist also nicht konservativ? Nun ja – gerade erklärte der als sehr „konservativ“ geltende Bundestagsabgeordnete Philipp Amthor: „Klimaschutz ist sogar eine superkonservative Sache!“² Es muss einen Unterschied geben zwischen alltäglichem konservativen Handeln und politischem Konservatismus – zwischen konservativ und „konservativ“. „Konservative“ PolitikerInnen wehren sich mit Händen und Füßen dagegen, das Pariser Klimaabkommen – das sie teilweise selbst mit unterzeichnet haben – durch effektive Maßnahmen in die Tat umzusetzen. Dies ist dagegen die wesentliche Forderung von *Fridays for Future* – sind sie die wahren Konservativen? Vielleicht müssen wir umgekehrt die Frage stellen: Ist die CDU wirklich konservativ?

Gehen wir einen Schritt weiter. Gelegentlich wird zwischen werte- und strukturkonservativ unterschieden. Aha. Ich selbst, beispielsweise, bin ein Anhänger der Werte des Grundgesetzes. Die Würde des Menschen, die freie Entfaltung der Persönlichkeit, das Recht auf Leben und körperliche Unversehrtheit, das Recht auf Asyl für politisch Verfolgte – das sind Werte, die ich bewahrt wissen möchte. Doch einige dieser Werte stehen unter permanentem Beschuss durch Menschen, die sich selbst als „Wertkonservative“ bezeichnen. Häufig musste in den letzten Jahren das Bundesverfassungsgericht einschreiten, um die Werte des Grundgesetzes gegen diese „Wertkonservativen“ zu schützen.³ Werte, von denen ich glaube, dass auch die meisten – wenn nicht alle – Mitglieder des FIFF sie vertreten. Demnach

wäre das FIFF ist ein zutiefst wertekonservativer Verband. Maja Göpel schreibt einige Seiten weiter:

„Wer Zukunft erfolgreich gestalten will, sollte also damit anfangen, von dem auszugehen, was tatsächlich der Fall ist, und nicht von dem, wie es früher einmal war.“⁴

Manche Menschen wünschen sich die früheren Verhältnisse zurück. Auch die CDU hat Mitglieder, die sich in besonderer Weise „wertkonservativ“ nennen: Die sogenannte *Werteunion*. Näher betrachtet scheint es sich dabei aber eher um so etwas wie eine „Arbeitsgemeinschaft AfD-Anhänger in der CDU“ zu handeln.⁵

Werte ist letztlich ein leerer Begriff, der von jedem so gefüllt wird, wie es gerade passt. Politische Parteien haben Werte, Gagnons haben Werte, die Mafia hat Werte, die Kirche hat Werte. Entscheidend ist, welche Werte es sind und wie glaubwürdig man sie vertritt.

Ein Beispiel: Politisch Konservative nennen gerne die *Familie*, wenn sie nach ihren Werten gefragt werden. Fragt man weiter, stellt sich gelegentlich heraus, dass dabei aber nicht alle Familien gemeint sind. Gleichgeschlechtliche Paare werden beispielsweise abgelehnt. Genauer müsste man also sagen: Der Wert dieser Konservativen ist die Familie, die auf einer heterosexuellen Beziehung zwischen Mann und Frau beruht.

Doch halt! In den letzten Jahren kamen einige Flüchtlingsfamilien zu uns, die vor den politischen Verhältnissen in ihrem Land fliehen mussten. Bei einigen dieser Familien gelang es nur dem Ehemann, Deutschland zu erreichen. Um den Wert *Familie* zu verteidigen, müsste selbstverständlich der schnelle Nachzug der anderen Familienmitglieder ermöglicht werden. Doch dagegen sperren sich manche „Konservative“. Also ist die Familie doch nicht ihr Wert, den sie vertreten? Was ist es dann? Ich wage kaum zu fragen: Sind die „Werte“, die diese Menschen vertreten, womöglich Rassismus und Homophobie?

Versuchen wir es mit einer anderen Art von „konservativ“: strukturkonservativ. Unsere Gesellschaft hat sich in den vergangenen Jahrhunderten Strukturen geschaffen, die uns ein komfortables Leben auf Kosten anderer sichern. Dazu gehören unser Wirtschaftssystem, die Einkommensverteilung, Grenzen und die Abgrenzung gegen Menschen, die *woanders* geboren wurden, Privilegien in Gesellschaft, in der Bildung, im Beruf. Ist es dies, was „Konservative“ bewahren wollen? Sind „Konservative“ eigentlich Strukturkonservative?

Ist das die Lösung? Die sich „konservativ“ nennen, auch „wertkonservativ“, sind in Wirklichkeit Strukturkonservative, die vor allem ihre Privilegien bewahren wollen. Wertkonservative, die zum Beispiel die Werte des Grundgesetzes wie Meinungs- und Pressefreiheit oder die Menschenwürde bewahren wollen, werden „Linke“ genannt. Scheinbar muss man solche Menschen entschieden bekämpfen, wie wir es gerade in Thüringen beobachten konnten. Das Schauspiel, das dort gerade von „konservativen“ Parteien aufgeführt wurde, war unerträglich.

Es gibt also viele Gründe, zwischen rechten und linken politischen Bewegungen und Einstellungen zu unterscheiden. Es kann nicht sein, die menschenfeindliche Ideologie der Rechten auch nur ansatzweise mit der Linken gleichzusetzen, wie es einige „Konservative“ immer wieder versuchen, auch zuletzt in Thüringen. Doch auch die politische Linke hat sich nicht immer mit Ruhm bekleckert, wenn es um den Erhalt der Natur ging.⁶ Wir müssen immer wieder erkennen, dass sozialer Fortschritt ohne ökologischen Fortschritt nicht möglich ist. Greta Thunberg sagte auf dem Weltwirtschaftsforum 2020 in Davos:

„... this is not about ‚right‘ or ‚left‘. We couldn't care less about your party politics. From a sustainability perspective, the right, the left as well as the center have all failed. No political ideology or economic structure has been able to tackle the climate and environmental emergency and create a cohesive and sustainable world.“⁷

Doch an einer Sache kommt man nicht vorbei: „Konservative“ Parteien sind außerordentlich erfolgreich. Die CDU/CSU, die (in Westdeutschland) in der Nachkriegszeit Nazi-Größen in höchste Staatsämter gehievt hat und heute teilweise offen über eine Zusammenarbeit mit einer Partei wie der AfD nachdenkt – und die gleichzeitig in der DDR als Blockpartei eng mit der SED zusammengearbeitet hat⁸, stellt heute im Bundestag und in einem Großteil der Landesparlamente die stärkste Fraktion. Auch Menschen, die objektive Nachteile durch ihre Politik in Kauf nehmen müssen, wählen sie wie selbstverständlich. Herbert Marcuse schrieb:

„Die Ergebnisse moderner Volksabstimmungen beweisen, dass die von der möglichen Wahrheit getrennten Menschen dazu gebracht werden können, gegen sich selbst zu stimmen.“⁹

Ist das das Erfolgsrezept „konservativer“ Parteien?

Mit Fliffigen Grüßen
Stefan Hügel

Anmerkungen

- 1 Maja Göpel (2020) *Unsere Welt neu denken. Eine Einladung*. Berlin: Ullstein, S. 22
- 2 <https://www.bento.de/politik/philipp-amthor-interview-ueber-greta-thunberg-instagram-und-konservativismus-a-984afe7a-c5eb-4ba9-9d25-1d4d2ec54b45>
- 3 Beispielsweise im Urteil des Ersten Senats des Bundesverfassungsgerichts vom 2. März 2010 (1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08) gegen die EU-Richtlinie 2006/24/EG zur anlasslosen Vorratsdatenspeicherung, https://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html
- 4 Maja Göpel (2020) a. a. O., S. 29
- 5 Skurril das Klima-Manifest 2020 des Konservativen Aufbruchs Bayern: Die Sonne steuert das Klima, nicht das CO₂. Kritisch dazu: Stefan Rahmstorf (2020) Das Klima-Manifest der WerteUnion, <https://www.spektrum.de/kolumne/das-klima-manifest-der-werteunion/1710322>
- 6 Vielleicht ein Grund, auch zwischen Linken und „Linken“ zu unterscheiden?
- 7 Greta Thunberg (2020) Rede auf dem Weltwirtschaftsforum 2020 in Davos, <https://www.youtube.com/watch?v=OGokqK7iBd4>
- 8 Funfact: Ist eigentlich schon einmal aufgefallen, dass die CDU die einzige DDR-Blockpartei der ‚Nationalen Front‘ war, die es nach der politischen Wende nicht einmal für nötig hielt, wenigstens ihren Namen zu ändern? Dazu die Studie von Bertram Triebel (2019) *Die Thüringer CDU in der SBZ/DDR - Blockpartei mit Eigeninteresse*. <https://www.kas.de/de/einzeltitel/-/content/die-thueringer-cdu-in-der-sbz-ddr>
- 9 Herbert Marcuse (1938) Zur Kritik des Hedonismus. in: *Zeitschrift für Sozialforschung*, Jahrgang VII/1938, S. 55-89, Zitat von S. 81



Das FlfF bittet um Eure Unterstützung

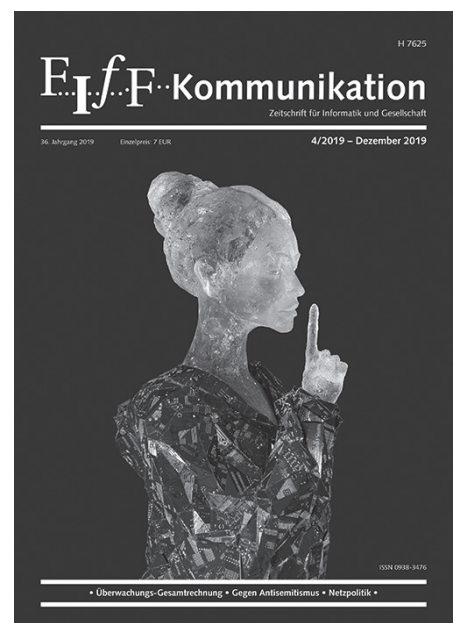
Viermal im Jahr geben wir die FlfF-Kommunikation heraus. Sie entsteht durch viel ehrenamtliche, unbezahlte Arbeit. Doch ihre Herstellung kostet auch Geld – Geld, das wir nur durch Eure Mitgliedsbeiträge und Spenden aufbringen können.

Auch unsere weitere politische Arbeit kostet Geld für Öffentlichkeitsarbeit, Aktionen und Organisation. Unsere jährlich stattfindende FlfF-Konferenz, der Weizenbaum-Preis, weitere Publikationen, Kommunikation im Web: Neben der tatkräftigen Mitwirkung engagierter Menschen sind wir bei unserer Arbeit auf finanzielle Unterstützung angewiesen.

Bitte unterstützt das FlfF mit einer Spende. So können wir die öffentliche Wahrnehmung für die Themen weiter verstärken, die Euch und uns wichtig sind.

Spendenkonto:

Bank für Sozialwirtschaft (BFS) Köln
IBAN: DE79 3702 0500 0001 3828 03
BIC: BFSWDE33XXX



Im Bann der Netzwerke

Aufmerksamkeitsökonomie und subtile Steuerung in den Sozialen Medien

In den letzten Jahren haben sich Social-Media-Forschung bzw. Social-Media-Monitoring zunehmend dafür interessiert, wie die Sozialen Medien genutzt werden. Dabei haben sie immer mehr über Nutzungsdauer, -arten, und -motive gerade der großen, einflussreichen sozialen Netzwerke herausgefunden. Vor allem aber mögliche Folgen einer Fremdsteuerung der Nutzerinnen und Nutzer – beispielsweise ein neues Verständnis von Gemeinschaft und Sozialität – wurden aus verschiedenen Perspektiven diskutiert und führten zu Zuschreibungen wie „Facebook-Gesellschaft“¹ oder „Generation Facebook“.² Lassen sich gesellschaftliche Veränderungen in den Sozialen Netzwerken tatsächlich verstärken? Inwieweit dirigieren die Plattformen Aufmerksamkeit systematisch und subtil, ausgerichtet an kybernetischen Prinzipien? Der erste Teil des Titels spielt an auf das viel beachtete Werk „Im Bann der Plattformen“ von Geert Lovink (2017), der zweite auf die FlFF-Konferenz von 2018, wo sich die Vorträge und Workshops aus verschiedenen Perspektiven mit „Gestaltungsfreiheiten und Machtmustern soziotechnischer Systeme“ beschäftigten. Insgesamt ergibt sich ein kritischer Blick auf maßgebliche Auswirkungen der viel genutzten Sozialen Medien an der Schnittstelle zwischen Soziologie und Informatik.

Subtile Aufforderungen zum Kommunizieren

Will man Überwachungslogiken und deren Konsequenzen in den Sozialen Medien aufzeigen, kann es hilfreich sein, zu den Anfängen der Sozialen Medien zurückzublicken: Da war das Web 2.0, anfangs als *Mitmachnetz* bezeichnet und ob der demokratischen Partizipationsmöglichkeiten von verschiedenen Seiten bejubelt. Selbstdarstellung, Inszenierung, Profilbildung und Vergleiche mit anderen waren mit hochgeladenen Daten und ein paar Klicks möglich. Zugleich machte die Kritik an den neoliberalen Geschäfts- und Profitstrategien rund um das Web 2.0 deutlich, dass es Konzernen wie Google um Datenabschöpfung in großem Stil ging. Im Mittelpunkt des Web 2.0 stand zunächst der *User-generated Content*: seine leichte, massenhafte Verbreitung und die Idee des *Prosumers* waren geeignet, Aufmerksamkeit zu generieren und Erlebnisse mitzuteilen. Technisch wurde das Web 2.0 zu den Sozialen Netzwerken weiterentwickelt. Den Möglichkeiten zur Selbstdarstellung und Vernetzung – im Web 2.0 wie in den Sozialen Medien heute – lagen bzw. liegen stets subtile Aufforderungen zum Kommunizieren zugrunde. Die Partizipation dabei „impliziert immer den gleichen Zwang zur ‚Anschließen‘; sie forciert mit der Ausrichtung der Netze zugleich die *Obligationen des Sichanschießens-müssens* [sic] und damit die Weise der Kommunikation, von der nicht abgewichen werden kann.“³ Voyeurismus und ständig auf Postings, Kommentare, Likes und Dislikes zu reagieren, halten einerseits den Fluss der Kommunikation am Laufen und verhindern andererseits – mit Blick auf die Nutzer – ein Gefühl des Ausgeschlossenenseins. Auf Seiten der Plattform-Betreiber hingegen geht es um eine Optimierung der Programmarchitektur, die sogleich wiederum auf die Benutzer zurückwirkt. So verfolgen Facebook und andere Plattformen eine kybernetisch orientierte, Stimmung beeinflussende „Optimierung der Kommunikationsströme, an die jeder sich nicht nur anschließen kann, sondern *muss*, ja *geradezu nicht anders kann als sich anzuschließen* und sich in ihre Netze zu verspinnen.“⁴ Die ursprünglich aus der Psychologie kommenden, viel diskutierten „Affordance“-Strategien im Social Web können aus mediensoziologischer Sicht verstanden werden als unmerklich *sanfte* Aufforderungen zum Kommunizieren – denn „gute Hirten führen *sanft*“, wie der Soziologe Ulrich Bröckling mit Blick auf Verhaltensführungs- und „Menschenregierungskünste“⁵ weitsichtig dargelegt hat.

Nudging und der Wert von Entscheidungen im Neoliberalen

Die auf Richard H. Thaler und Cass Sunstein zurückgehende Analyse der *Nudging*-Psychologie aus dem Jahre 2008 ist nur ein Beispiel für ausgefeilte subtile Verhaltenssteuerung mit oder ohne digitale Technologien. Die zu Steuernden sollen in eine gewünschte Richtung, zum erwünschten Verhalten geführt werden, aber eben *nicht* durch Zwang, argumentative Überzeugung, Überredung(skünste) oder auffälliges Drängen, sondern durch *sanftes* Anstupsen (Stupser = nudge) – in Form von algorithmengesteuerten Verlockungen, Anstoßen und Impulsen. Indem die *Entscheidungsarchitektur* und der *Handlungsrahmen* innerhalb der Kommunikations- und Entscheidungsprozesse entsprechend gesetzt oder modifiziert werden, soll die Wahrscheinlichkeit erhöht werden, dass sich Menschen verhalten wie erwartet.⁶ Analog zu *Big Data* ist hier oft auch von *Big Nudging* die Rede. Rainer Mühlhoff konkretisiert dies mit Blick auf die Schnittstelle soziotechnischer Systeme: „Nudges operieren dazu über das Design [...]: Das ist die räumliche grafische und interaktive Logik, in der Auswahloptionen präsentiert und aufbereitet werden.“⁷ Die Nutzer, die schließlich eine der Optionen wählen, sollen den (hohen) Wert ihrer eigenen Entscheidung mitbekommen, die ihnen erleichtert wurde. Hinter diesem *Wert* steckt jedoch vielmehr eine auf die binäre 0-1-Struktur zurückgehende, algorithmische „Entscheidungslogik“, wie Dieter Mersch hervorhebt: „Vernetzte Kommunikation ist in diesem Sinne entscheidungslogisch ‚gebündelte‘ bzw. ‚abgerichtete‘ Kommunikation“.⁸ Kritiker machen auf die enge Verschränkung des Stupsens mit Wettbewerbsstrukturen und somit auf die neoliberale Anschlussfähigkeit aufmerksam. Letztlich sind die smarten Geräte zum Self-Tracking und Körper-Monitoring Teil der Vergleichs- und Optimierungsprozesse in einer neoliberal zugerechneten Gesellschaft. Das Numerische der Geräte, Ist-, Soll- und Vergleichswerte können als kybernetische Nudging-Elemente verstanden werden: Die algorithmisch verstärkten Ambitionen, bestimmte Soll-Werte zu schaffen, sind Ansporn („Nutzer x hat bereits den Wert Y erreicht“), sich überzeugen (stupsen) zu lassen, um ebenfalls den Wert Y zu erreichen. Dabei stellen die Sozialen Netzwerke durch ihre Vernetzung und Reichweite die Plattformen dar, ohne die ein solcher Vergleich nicht möglich wäre. Permanent Daten über die Plattformen preiszugeben, heißt für die Nutzerinnen und Nutzer zugleich, sich selbst zu ver-

markten – nach vorgegebenen Regeln der neoliberalen Marktlogik. Um zu ihrem Wohl *gestupst* zu werden, d. h. auch, „um zu den begehrten sozialen Belohnungen vorgelassen zu werden, [wird] verlangt, daß Sie *sich selbst als Ware konzipieren*: als Produkte, die ‚aufmerksamkeitsstark‘ sind, die *Nachfrage* wecken und *Kunden* anziehen.“⁹ Die Sozialen Medien haben sich seit dem Web 2.0 auf diese Marktregeln nicht nur eingelassen, sondern sie so weit internalisiert und technisch implementiert, dass sie zu veritablen (Optimierungs-)Räumen für das neoliberale, sich selbst vergleichende und freiwillig unterordnende „unternehmerische Selbst“¹⁰ geworden sind. Zu Räumen, in denen *Wert* weniger als *wertvoll* für die Nutzer zu verstehen ist, sondern immer mehr im Sinne der Gewinnoptimierung von Datenkonzernen und letztlich als Anpassung.

Aufmerksamkeit bündeln im Assessment-Center

Eine Metapher, um diese Räume genauer zu beschreiben, buchstabierte die Journalistin und Soziologin Carolin Wiedemann im Anschluss an Bröckling aus: das *Assessment-Center* als Ort für die umfassende numerische Vergleichbarkeit mit anderen und damit auch als Ort der Selbstdarstellung, -optimierung und -disziplinierung. Während Bröckling 2007 das Leben „als permanentes Assessment Center“¹¹ unter den Bedingungen eines neoliberalen Marktes analysiert, geht Wiedemann konkret auf das Unternehmerische der Sozialen Netzwerke ein. Sie analysiert das Interface, die damit verbundenen Möglichkeiten, sich im Rahmen eines möglichst kreativen „Selfbrandings“ sichtbar und bewertbar zu machen und kommt zu dem Schluss: so „führt auch Facebook das Verhalten der UserInnen, es strukturiert deren Handeln, indem es sie dazu anleitet, sich auf eine ganz bestimmte Art und Weise zu verhalten, bestimmte Aspekte des Selbst und [...] bestimmte Dinge zu äußern.“¹² Voraussetzung dafür ist zum einen das Ansammeln von Daten der Nutzer und zum anderen ein Lenken von Aufmerksamkeit auf bestimmte Inhalte und Quellen. Relevanzen müssen gesetzt und Bewertungen getroffen werden: Informationen werden auf eine bestimmte, dem bisherigen Profil einer Person angepasste Art und Weise registriert, algorithmisch weiterverarbeitet und entsprechend adressiert. Aus der *Like-Economy* ist längst eine umfassende Aufmerksamkeitsökonomie geworden, die nicht nur für das Geschäftsmodell von Facebook, sondern auch für die kommerziellen Strategien anderer Social-Network-Plattformen charakteristisch ist. Was der Architekt, Software-Entwickler und Stadtplaner Georg Franck 1998 in seinem Buch „Ökonomie

der Aufmerksamkeit“ beschrieben hat, ist heute durch die Sozialen Medien mehr denn je eingelöst: die von ihm in puncto Einschaltquoten, Auflagenstärke, SMS und e-mail analysierte „neue Währung Aufmerksamkeit“ radikalisiert sich in der Digitalität und *Disruption* der Sozialen Medien zu einer neoliberalen, algorithmischen Bindung, Lenkung, Konzentration und letztlich zum Nutzbarmachen von Aufmerksamkeit. Die technischen Instrumente dafür: Big-Data-Techniken und Algorithmen.

Kybernetische Fremdbestimmung: Feedback als Endlosschleife

Der niederländische Medientheoretiker und Netzaktivist Geert Lovink bezieht sich in seinen Abhandlungen immer wieder auf die frühe Kybernetik, insbesondere den Zweig der Soziokybernetik. Er wirft auf dieser Folie einen kritischen Blick auf die allgegenwärtige Software(gläubigkeit), die nicht nur vernetzend *smart things* in vielen Lebensbereichen hervorbringt, sondern „deren Echtzeit-Feedback viele Nutzer abhängig macht.“¹³ So ist neben dem subtilen Anreiz-Setzen durch Nudging auch das Feedback als Steuerungsmittel rund um die Sozialen Medien zu sehen. Wichtig für die Plattform-Betreiber ist es dabei wie erwähnt, die Kommunikation aufrecht zu halten. Nur so bleiben der kybernetische Regelkreis in Betrieb und Feedback als Rückmeldung konkret greifbar, in Form der mess-, bewert- und vergleichbaren Äußerungen oder Reaktionen (*Likes/Dislikes, Retweets, Following, Sharing, etc.*), die sich als „Pandorageschenk der Sofortbelohnung“ lesen lassen für gepostete Informationen über sich selbst oder unter dem Unterhaltungsaspekt als „Kultur der Sofortbefriedigung“¹⁴. Beobachtet und beobachtet werden, handeln und Erwartungen haben, agieren und Reaktionen darauf bekommen, mit anderen Worten: Als relevant für das Design der Benutzeroberfläche wird das vorgeschlagen, was – algorithmisch errechnet – eine Reaktion provozieren wird. In der Interaktionslogik der Sozialen Medien gilt das kybernetische Prinzip: Die „computerbasierten Systemschleifen vermehren die Selbstbeobachtungspositionen und die Archivierungstechniken und ermöglichen, dass sich die UserInnen in allen Stadien ihrer biografischen Selbstdarstellung gegenseitig beobachten können.“¹⁵ Letztlich steckt hinter dem Reagieren auf ein Posting wiederum ein durch die Architektur der Software ermöglichter *Nudge*. Mit jedem Klick wird dieser Regelkreis aufrechterhalten und somit die Aufmerksamkeits- und Reputationsökonomie genährt. Mit dem Ist-Soll-Abgleich kommen zwei weitere kybernetische Faktoren in den Blick:



Markus Reinisch

Markus Reinisch ist Lehrer an einer bayerischen Mittelschule. Er schreibt neben literaturdidaktischen und gesellschaftspolitischen Beiträgen kritisch zu Themen der Digitalisierung für verschiedene Zeitschriften. Vor allem die Prozesse an der Schnittstelle zwischen Bildung und Digitalisierung nimmt er unter die Lupe. Zuletzt sind einige Aufsätze zu Big Data- und zur Algorithmenkritik erschienen.

Beobachtung und Anpassung. Es sind die Logiken der „Feedbackschleifen und Technologien des (Selbst-)Monitorings, die kontinuierliche Anpassungen an sich ebenfalls kontinuierlich wandelnde Zielmarken ermöglichen sollen“¹⁶. Was sich in den 60er- und 70er-Jahren zum Erreichen der gesetzten Ziele (*Soll-Wert* im Regelkreis, beispielsweise beim Thermostat) technisch aufwändig gestaltete, ist heute mittels Personalisierungs-Algorithmus problemlos umzusetzen. Der Algorithmus wirkt und der Nutzer Sozialer Medien gibt – meist unbemerkt – „sein Selbstbestimmungsrecht an eine Technologie ab, die ihm einzig noch die Freiheit gewährt, ständig mit sich selbst verbunden zu sein, insofern er sich einer *unreflektierten Selbstkontrolle* unterwirft, die mit einer *reflektierten Außensteuerung* korrespondiert.“¹⁷

Identitätsbildungsprozesse: „culture of real identity“

Man muss bei einer Analyse der Wirkungen Sozialer Medien nicht gleich von einer generellen „programmatische[n] Reduzierung von Gesellschafts- auf Netzwerkkonzepte“¹⁸ ausgehen, aber dennoch kritisch fragen, inwieweit die skizzierten Entwicklungen Subjektbildungsprozesse beeinflussen und Konzepte von Sozialität in Frage stellen. In der Tat gehört die vielfältige Kommunikation auf Sozialen Netzwerken längst zu den komplexen Prozessen der Identitätsbildung im Netz. Nicht nur jugendliche Akteure suchen in den Sozialen Medien nach passenden Darstellungs- wie Ausdrucksformen und stoßen bei Facebook etwa auf den Anspruch, innerhalb einer „culture of real identity“¹⁹ Freundschaften aufbauen und pflegen zu können. Muss eine solche Freund- bzw. Gemeinschaft, die sich oft nur in der gemeinsamen Praxis der Mediennutzung zusammengehörig fühlt, nicht oberflächlich und substanzlos bleiben? Es ist geradezu das Gegenteil selbstbestimmter, eigenverantwortlich-reflektierter Identitätsbildung, wenn der Mensch auf Social-Media-Sites „nicht nur als unbewusst beeinflussbar, sondern in seinem Verhalten auch noch als statistisch modellierbar“²⁰ verstanden wird. Die Fremdbestimmung bzw. subtile Steuerung zeigt sich auch, wenn *social browsing* das Suchen von Freunden im Realen ablöst, wenn Freundinnen und Freunde nur noch als Teil oder Steuerung eines umfassenden Feedback-Systems gesehen werden. Und wenn Techniken wie Nudging zur Anhäufung von Sozialkapital – analog zur neoliberalen *Humankapitalisierung* – eingesetzt werden und ihre Wirkung zeigen. Ferner ist es bedenklich und belegt den kybernetischen Regelungseifer, wenn Facebook seine Nutzer auf subtile und „clevere Weise dazu bringt, wesentliche Klassifizierungen selbst vorzunehmen, indem sie einander als *Freunde* identifizieren. Eine sublimale Verschiebung der Semantik von *Freund* oder *Freundschaft* durch mächtige soziale Plattformen – mit weit reichenden Folgen nicht nur für den Prozess der Identitätsbildung.

Vonnöten: Bildungsprozesse, die den Mediengebrauch reflektieren

So gilt es, die an der Schnittstelle zwischen Informatik und Soziologie aufgezeigten Entwicklungen der Fremdbestimmung und des paternalistischen *Anstupsens* bewusst zu machen,²¹ zum Beispiel im Rahmen von Lernprozessen in der Medien- und Informatikdidaktik. Nur so können Bildungsprozesse einen kri-

tischen Blick auf die Nutzung und Auswirkungen von Sozialen Medien ermöglichen und damit Anstöße – jenseits von Nudging-Strategien – geben, den eigenen Mediengebrauch zu reflektieren und die Möglichkeiten bzw. Arten der Steuerung zu verstehen. Zur Zielkategorie „Bildung in digitalen Welten“, die im Begriff ist, ältere medienpädagogische *Medienkompetenz*-Kategorien abzulösen, gehören schulartübergreifend wesentlich fünf Ziele:

1. sich seiner „digitalen Identität“ bewusst zu werden,
2. die Fremdsteuerung nachzuvollziehen und
3. dabei das Subtile dieser Steuerung zu durchschauen. Schließlich sollten die Einsichten
4. zur Erkenntnis führen, dass Kommunikations-, Lern- und Identitätsbildungsprozesse zwischen realweltlichen und netzbasierten Welten, zwischen Nähe und Distanz, „zwischen Tiefe und Seichtheit, Profundität und Oberflächlichkeit, Wärme und Coolness, Herzlichkeit und Flüchtigkeit“²² stattfinden.
5. In einem weiteren Schritt könnte es idealiter darum gehen, diese beiden Welten zueinander kritisch in Bezug setzen und daraus persönliche Konsequenzen zum Mediengebrauch ziehen zu können.

Das sind sicher ehrgeizige Ziele, doch wenn Nutzerinnen und Nutzer stattdessen auf die vorgegebenen Auswahloptionen der Sozialen Medien im Sinne einer behavioristischen Reiz-Reaktions-Struktur nur noch reagieren, dann sind sie von einem digital entmündigten (vgl. Mühlhoff), beliebig zu steuernden „Automatenmenschen“ (Eva Borst) in der Tat nicht weit entfernt.

Anmerkungen

- 1 Simanowski, Roberto: *Facebook-Gesellschaft*. Berlin 2016
- 2 Leister, Oliver/Röhle, Theo (Hg.): *Generation Facebook. Über das Leben im Social Net*. Bielefeld 2011
- 3 Mersch, Dieter: *Ordo ab chao – Order from Noise*. Zürich 2013, S. 49f., Hervorh. i. O.
- 4 Ebd., S. 81, Hervorheb. i. O.
- 5 Bröckling, Ulrich: *Gute Hirten führen sanft – Über Menschenregierungskünste*. Berlin 2017
- 6 Zu einer kurzen, kritischen Einführung in die Nudging-Theorie siehe z. B. Simanowski, Roberto: *Zauberformel Nudging – Die Marshmallowkultur oder das Pandorageschenk der Sofortbelohnung*. In: *Lette International* 125/2019, S. 27-31 und Bröckling, Ulrich: *Nudging: Gesteigerte Tauglichkeit, vertiefte Unterwerfung*. In: Ders. (vgl. Fußnote 5), S. 175-196
- 7 Mühlhoff, Rainer: *Digitale Entmündigung*. In: *FlFF-Kommunikation* 2/2019, S. 18-24, S. 19
- 8 Mersch (vgl. Fußnote 2), S. 65, Hervorh. i. O. Auch Simanowski (vgl. Fußnote 1) sieht eine „unentrinnbare Entscheidungslogik der Algorithmen“ (S.36) am Werk.
- 9 Bauman, Zygmunt/Lyon, David: *Daten, Drohnen, Disziplin. Ein Gespräch über flüchtige Überwachung*. Berlin 2014, S. 47
- 10 Bröckling, Ulrich: *Das unternehmerische Selbst. Soziologie einer Subjektivierungsform*. Frankfurt a. M. 2007

- 11 Ebd., S. 72
- 12 Wiedemann, Carolin: Facebook – das Assessment-Center der alltäglichen Lebensführung. In: Leistert/Röhle (vgl. Fußnote 2), S. 161-183, S. 163
- 13 Vgl. Lovink, Geert: Im Bann der Plattformen: Die nächste Runde der Netzkritik. Bielefeld 2017, S. 42
- 14 Simanowski (vgl. Fußnote 6), S. 27
- 15 Wiedemann (vgl. Fußnote 12), S. 176
- 16 Bröckling (vgl. Fußnote 6), S. 181
- 17 Borst, Eva: Der Automatenmensch. Zur Neutralisierung der Pädagogik im kybernetischen Kapitalismus. In: Bernhard, Armin u. a. (Hg.): Kritische Pädagogik. Eingriffe und Perspektiven, Heft 1 (2015), S. 39-62, S. 49f., Hervorh. i. O.
- 18 Nosthoff, Anna-Verena/Maschewski, Felix: "Democracy As Data"? Über Cambridge Analytica und die "moralische Phantasie". In: Blog

der Zeitschrift Merkur vom 06.02.2017, unter: <https://www.merkur-zeitschrift.de/2017/02/06/democracy-as-data-ueber-cambridge-analytica-und-die-moralische-phantasie/#more-5493> (Stand: 02.10.2019)

- 19 so der Facebook-Gründer, nachzulesen in der Zitate-Sammlung der Biografie von Mark Zuckerberg; zit. nach Simanowski (vgl. Fußnote 1), S. 22
- 20 Mühlhoff (vgl. Fußnote 7), S. 23
- 21 Zum Aspekt der Anpassung vgl. z. B. Eva Borst (vgl. Fußnote 17), S. 51: „Der Mensch wird zum informationsverarbeitenden Automaten, der gezwungen ist, sich seiner Umgebung anzupassen. Damit folgt er exakt den Regeln eines kybernetischen Systems. Er unterscheidet sich in nichts von einer selbstregulierten Maschine.“
- 22 Bauman/Lyon (vgl. Fußnote 9), S. 56



FlFF e. V. – Pressemitteilung

Digitalisierung an Schulen – so nicht!

FlFF kritisiert Digitalpakt mit Windows 10 und Office 365

29. November 2019 – Der Digitalpakt für Schulen wurde im Mai 2019 für ganz Deutschland – trotz seines Eingriffs in die Föderalisierung – im Rahmen der Strategie für Digitalisierung durch die Bundesregierung verabschiedet. Der Bund stellt hierfür über einen Zeitraum von fünf Jahren insgesamt fünf Milliarden Euro zur Verfügung, davon in dieser Legislaturperiode 3,5 Milliarden Euro.

Aufgrund des Charakters der Bundesmittel als Finanzhilfen bringen die kommunalen und privaten Schulträger bzw. Länder zusätzlich einen finanziellen Eigenanteil ein. Zusammengekommen stehen dann insgesamt mindestens 5,55 Milliarden Euro bereit. Rein rechnerisch bedeutet dies für jede der ca. 40.000 Schulen in Deutschland im Durchschnitt einen Betrag von 137.000 Euro oder umgerechnet auf die derzeit ca. 11 Millionen Schülerinnen und Schüler eine Summe von 500 Euro pro Schüler in dem Finanzierungszeitraum.

Den Verantwortlichen, somit Schulträgern oder Schulen, steht es zunächst frei, wofür konkret sie diese Gelder zur Modernisierung der IT-Infrastruktur einsetzen. Bereits im laufenden Schuljahr 2019/2020 sollen diese Gelder abgerufen werden, um z. B. Tablets zu kaufen. Zum funktionstüchtigen Einsatz solcher Tablets ist oftmals noch ein schulinternes WLAN zu implementieren. Mit diesen Anschaffungen und dem dauerhaften Betrieb solcher Elemente einer IT-Infrastruktur sind die Mittel pro Schüler verbraucht. Eine Hardware ohne Software ist untauglich. Als Software-Lösung sollen Verträge mit Microsoft geschlossen werden. Den meisten Schulträgern oder Schulen wird eine Lizenz von Office 365 Education unter A1 angeboten, das „Rundum-Wohlfühlpaket“, welches mit dem genehmigten Digitalpakt bzw. realisierbaren Kosten für Schulen noch betrieben werden könnte. Umfassendere Lizenzen, wie A3 oder gar A5, mit denen Verantwortliche Software-Dienste konfigurieren könnten, sind jedoch aus Kostengründen wohl kaum vermittelbar.

Das FlFF kritisiert diese Lizenz-Politik und fordert die datenschutzkonforme Verarbeitung der Daten von Schülerinnen und Schülern, die zumeist minderjährig sind. Warum wird hier nicht eine äquivalente Open-Source-Software-Lösung eingesetzt, wie sie z. B. von der Open Business Alliance [1] angeboten wird? Mit solchen Lösungen könnten deutsche Schulen und Institutionen

die Kontrolle über ihre Daten behalten, datenschutzkonforme Implementierungen leichter umsetzen und transparent die Datenschutzbestimmungen sicherstellen. Letzteres ist jedoch bei der im Rahmen der oben erwähnten Finanzierung verfügbaren Lösung mit Microsoft 365 unter A1 kaum bis gar nicht zu garantieren. Mindestens sind spezielle Regelungen in der Datenschutzgrundverordnung (DSGVO) anzuwenden, die aufbauend auf Artikel 5, 6 und 7 DSGVO in Artikel 8 DSGVO konkretisiert sind.

Das FlFF fordert Aufklärung, welche Interessen Microsoft verfolgt, denn die Deutsche Telekom AG hat die eigene deutsche Microsoft Cloud zum 31. August 2019 eingestellt. Das Treuhändermodell für Microsoft bei T-Systems ist damit ausgelaufen [2]. Microsoft wird ab 14. Januar 2020 für die Betriebssysteme auf den Servern 2008 und 2008 R2 den Support einstellen und die auf ihnen laufende Software statt dessen in ihre Cloud Azure migrieren, und damit auch alle Daten in Azure in den USA stellen [3]. Danach wird keine Kontrolle von Seiten deutscher Institutionen mehr möglich sein, und es besteht die Gefahr, dass Inhalts- und Verbindungsdaten ohne Wissen oder Genehmigung Betroffener auch an Schulen weiter gesammelt und per Gesetz an die NSA weitergegeben werden können. Solches hat Microsoft in anderen Zusammenhängen bereits getan [4].

Wie gefährlich die – schließlich lebenslang mögliche – Speicherung und Nutzung von Daten, Bildern, Medien- und App-Nutzung und alle Arten von Kommunikation für unsere Kinder ist, ist inzwischen hinlänglich bekannt geworden. Aber die Interessen und fundamentalen Rechte und Freiheiten von Kindern müssen vor allem auch an Schulen garantiert werden: Wenn ein hohes Risiko durch die Anwendung bzw. Umsetzung von Aufgaben im hoheitlichen Bereich durch IT-gestützte Prozesse in einer komplexen IT-Landschaft vorausgesetzt wird (die insbeson-

dere nicht als IT-Landschaft vor Ort beim Schulträger oder in der Schule betrieben wird), ist eine Datenschutz-Folgenabschätzung entsprechend Artikel 35 DSGVO durchzuführen. Mit einer solchen Datenschutz-Folgenabschätzung geht folglich einher, dass für Kinder bzw. Schulen technisch-organisatorische Maßnahmen höheren Anforderungen auch bzgl. der IT-Sicherheit genügen müssen. Vertraulichkeit und Integrität sind ebenso höher zu bewerten (Artikel 25 und Artikel 32 DSGVO). Zur Umsetzung im Besonderen auch dieser datenschutzrechtlichen Anforderungen muss verlangt werden, dass sichere Verschlüsselungen für Transport und Inhalt zu gewährleisten wären.

Das FIFV ruft dazu auf, Einspruch gegen die Regelungen des Digitalpakts einzulegen. Einsprüche gegen die derzeit bestehenden Verträge im Digitalpakt sind sachlich wie zeitlich höchst dringlich, da es Schulen jederzeit möglich ist, sich aus dem Digitalpakt zu bedienen und es bereits einzelne Schulen gibt, die dies

getan haben. Was passiert, wenn ein solcher Digitalpakt und damit verbundene Nutzung von Software für Hochschulen geschlossen würde? Ähnliche Implementierungen planen Länder ja in den öffentlichen Verwaltungen, Kommunen und Städten, die ggf. auf Microsoft-Enterprise-Lizenzen basieren sollen.

Referenzen

- [1] <https://osb-alliance.de>
- [2] <https://www.heise.de/newsticker/meldung/Auslaufmodell-Microsoft-Cloud-Deutschland-4152650.html>
- [3] <https://www.heise.de/ix/meldung/Microsoft-warnt-vor-Support-Ende-des-Server-2008-raet-zum-Cloud-Umzug-4586610.html>
- [4] <https://www.ft.com/content/7d3e0d6a-87a0-11e9-a028-86cea8523dc2>



FIFV e. V. – Pressemitteilung

Bündnis fordert Verbot automatisierter Gesichtserkennung Aktuelle Pläne des Innenministeriums müssen gestoppt werden

9. Januar 2020 – *Ein Bündnis aus zivilgesellschaftlichen Organisationen wendet sich gegen den Vorstoß des Innenministeriums, an 135 Bahnhöfen und 14 Flughäfen automatisierte Gesichtserkennung einsetzen zu wollen. Stattdessen fordert das Bündnis Gesichtserkennung stoppen ein Verbot dieser hochproblematischen Technologie in Deutschland. Auch wenn eine Verbesserung der Sicherheit etwa an Bahnhöfen grundsätzlich sinnvoll erscheint, ist automatisierte Gesichtserkennung als Mittel dafür nicht nur ungeeignet, sondern hat immense negative Folgen für Millionen Passanten und Reisende.*

Automatisierte Gesichtserkennung bedeutet eine permanente heimliche Personenüberwachung in öffentlichen Räumen wie Bahnhöfen oder Flughäfen. Die Körperdaten aller Vorbeiläufenden werden dabei erfasst und automatisiert mit Datenbanken abgeglichen, ohne dass die Betroffenen dies bemerken müssen. Damit greift die automatisierte Gesichtserkennung tief in die Rechte und Freiheiten von Menschen ein, wenn biometrische Körperdaten quasi im Vorbeigehen und anlasslos analysiert werden.

„Automatische Gesichtserkennung ist eine Hochrisikotechnologie“, erklärt Viktor Schlüter von der Organisation Digitale Freiheit: „Hohe Fälscherkennungsraten, die Diskriminierung von Frauen und People of Color und das enorme Missbrauchspotential stellen eine Gefahr für die Demokratie dar.“

„Dieses unnötige und invasive Biometriesystem ist nur ein weiterer Baustein, den maschinenlesbaren Menschen zu schaffen. Allein durch das zufällige Vorbeilaufen legen wir mit unseren Körperdaten eine digitale Spur, die uns alle auch wegen der Unzuverlässigkeit der eingesetzten Algorithmen in unseren Rechten und Freiheiten einschränkt“, sagt Dirk Engling, Sprecher des Chaos Computer Clubs.

„Die optische Vermessung von Gesichtern droht eine weitere Form der anlasslosen Überwachung zu werden, nur diesmal mit detaillierten Körperdaten“, fügt Rainer Rehak vom Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung hinzu. „Wir müssen uns jetzt diesen gefährlichen Plänen in den

Weg stellen, bevor immer mehr öffentliche Räume mit biometrischen Erkennungssystemen bestückt werden, die zudem nicht einmal mehr Sicherheit bringen.“

„Der Einsatz dieser Technologie zur Überwachung des öffentlichen Raumes schränkt auch politische Teilhabe ein: Wer fürchten muss, automatisch erfasst zu werden, wird im Zweifel eher nicht an einer Demonstration teilnehmen“, gibt Elisabeth Niekrenz von der Digitalen Gesellschaft zu bedenken.

Im Lichte stetig sinkender Kriminalitätsraten in Deutschland besteht nicht nur keinerlei Notwendigkeit für neue, teure und ineffiziente Überwachungsmaßnahmen zur anlasslosen Erfassung von Körperdaten von Reisenden, sondern ist es Zeit, ein Verbot dieser gesellschaftlich schädlichen Technologie in die Wege zu leiten. Ein Verbot automatisierter Gesichtserkennung in Deutschland hat bereits Vorbilder: Mehrere US-amerikanische Großstädte haben den Einsatz der Technologie durch staatliche Stellen im öffentlichen Raum aufgrund der damit verbundenen Gefahren verboten. Der Stadtrat von San Francisco etwa bezeichnete automatisierte Gesichtserkennung als „gefährliche Waffe“ sowie als inkompatibel mit einer gesunden Demokratie und verbot ihren Einsatz [0].

Dass die teure Technik überhaupt einsatzreif ist und den erhofften Zweck erfüllt, ist zudem zweifelhaft: In einem Gesichtserkennungstest von Innenministerium und Bundespolizei im Jahr 2018 in Berlin war die Fälscherkennungsrate so hoch, dass mehr als jede 200. Person fälschlicherweise erkannt wurde. Dies

würde allein am getesteten Berliner Bahnhof Südkreuz zu täglich 600 Fehlalarmen führen. Der Chaos Computer Club [1] und das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung [2] kritisierten die unwissenschaftliche Vorgehensweise und Auswertung der Tests sowie die deutlich geschönten Testergebnisse.

Das Bündnis *Gesichtserkennung stoppen* [3] besteht aus den zivilgesellschaftlichen Organisationen Digitale Freiheit, Chaos Computer Club, Digitale Gesellschaft, Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung sowie Digitalcourage.

Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung fordert die detaillierte Veröffentlichung der Ergebnisse der vergangenen und laufenden Biometrie-Tests an Bahnhöfen, um eine wissenschaftliche Bewertung der Ergeb-

nisse und eine öffentliche Diskussion über die Erkennungssysteme zu ermöglichen.

Referenzen

- [0] San Francisco Approves Ban On Government's Use Of Facial Recognition Technology, <https://www.npr.org/2019/05/14/723193785/san-francisco-considers-ban-on-governments-use-of-facial-recognition-technology>
- [1] Biometrische Videoüberwachung: Der Südkreuz-Versuch war kein Erfolg, <https://www.ccc.de/de/updates/2018/debakel-am-suedkreuz>
- [2] Verfälschte Studie zur Tauglichkeit grundrechtswidriger Techniken, <https://www.fiff.de/verfaelschte-studie-zur-tauglichkeit-grundrechtswidriger-techniken>
- [3] Webauftritt des Bündnisses, <https://www.gesichtserkennung-stoppen.de>



Gemeinsamer Appell vom 11. Februar 2020

Gesetz zur Änderung des Netzwerkdurchsetzungsgesetzes und Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität

Offener Brief zu den Referentenentwürfen

*Sehr geehrte Frau Bundesministerin Christine Lambrecht
(Bundesministerium der Justiz und für Verbraucherschutz),*

der Schutz von Grund- und Bürgerrechten ist eine essentielle Aufgabe demokratischer Rechtsstaaten. Dazu gehört, dass sich Menschen frei äußern können, ohne Angst vor Repressalien durch den Staat, aber auch ohne Angst haben zu müssen, von anderen Menschen aufgrund ihrer Äußerungen Bedrohungen oder Gewalt ausgesetzt zu sein. In einer Welt, die laut Freedom House seit 13 Jahren immer unfreier wird, kommt unserer Demokratie eine besondere Verantwortung zu, diese bürgerlichen Freiheiten zu schützen.

Die vom Bundesministerium der Justiz und für Verbraucherschutz (BMJV) in kurzem zeitlichen Abstand vorgelegten Gesetzesentwürfe für ein *Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität*, sowie ein *Gesetz zur Änderung des Netzwerkdurchsetzungsgesetzes* (NetzDG) tragen dieser Verantwortung jedoch nicht Rechnung. Sie sollen zwar erklärtermaßen dem Schutz der Meinungsfreiheit dienen, schaffen jedoch selbst eine enorme Gefahr für die bürgerlichen Freiheiten.

Wir, die Unterzeichnenden dieses Briefes, wollen heute jedoch nicht nur auf den Inhalt der Entwürfe eingehen, sondern müssen auch die offensichtlich fehlende Bereitschaft kritisieren, die vor einem Beschluss des Bundeskabinetts eigentlich gebotene fachliche und gesellschaftliche Debatte zur Wirksamkeit des NetzDG zu führen. Grundlage der Debatte hätte die Evaluierung des NetzDG sein können, die seit der Verabschiedung des Gesetzes angekündigt wurde. Mittlerweile ist bekannt, dass eine rechtswissenschaftliche Evaluierung des NetzDG stattfindet – die Ergebnisse liegen allerdings noch nicht vor und können so-

mit weder zum öffentlichen Fachdiskurs noch zu den veröffentlichten Referentenentwürfen beitragen.

Daher möchten wir Sie dringend dazu auffordern, die vorgelegten Entwürfe einer gründlichen Überarbeitung zu unterziehen, bevor das Kabinett hier das Gesetzgebungsverfahren initiiert. Dies ergibt sich vor folgendem Hintergrund:

1.

Beide Gesetzesentwürfe konstatieren „eine zunehmende Verrohung der Kommunikation“, ohne dafür auf empirische Belege verweisen zu können. Grundlage einer verantwortungsvollen Gesetzgebung in einem so grundrechtssensiblen Bereich wie der Medien- und Meinungsfreiheit sind jedoch belastbare Fakten, die in die komplexen Abwägungen, die solchen Gesetzgebungsverfahren zu Grunde liegen, mit einbezogen werden sollten. Hierzu hielten wir es für wichtig, dass vor der Verabschiedung weiterer restriktiver Regelungen in Kooperation mit den Plattformen Forschungsinstitutionen Zugänge zu Datenmaterial erhalten, das eine qualitative wie quantitative Überprüfung der Ausgangsthesen, wie auch der Wirksamkeit bereits bestehender Regelungen überhaupt ermöglichen. Notfalls wären die Betreiber der Plattformen hierzu zu verpflichten.

2.

Der Gesetzesentwurf für ein *Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität* verlagert die strafrechtliche Verfolgung von Äußerungen in sozialen Medien in solch er-

heblicher Weise vor, dass sie in einer für viele Menschen kaum noch vorhersehbaren Weise die Gefahr polizeilicher Ermittlungen und strafrechtlicher Verfolgung nach sich ziehen kann – obwohl es sich eben nicht stets um eindeutig rechtswidrige Äußerungen handelt, die den Rahmen des zulässigen „Meinungskampfes“ verlassen würden.

Zugleich schafft Ihr Gesetzentwurf eine Reihe problematischer Befugnisse, auf die Sie auch öffentlich schon mehrfach hingewiesen worden sind, auf die das BMJV leider bislang nur ungenügend reagiert hat:

Die Verpflichtung zur Herausgabe von Passwörtern ist gleich in mehrfacher Hinsicht problematisch. Passwörter liegen bei Providern üblicherweise in verschlüsselter Form vor. Dies ist essentielle Voraussetzung sicherer IT-Systeme. Es steht daher zu befürchten, dass staatliche Stellen Anreize setzen werden, Provider zum Vorhalten unverschlüsselter Passwörter anzuhalten, da die gewonnenen Informationen sonst für sie wertlos sind. Dies stünde jedoch datenschutzrechtlichen Vorgaben und IT-Sicherheitsanforderungen, wie unter anderem vom BSI gestützt, diametral entgegen. Zum anderen würde damit jegliche Nutzung digitaler Konten – vom sozialen Netzwerk bis zum Online-Banking – massiv unsicher. Der IT-Standort Deutschland wäre ein Schlaffenland für Hacker. Zudem sollte fraglich sein, inwiefern Beweise vor Gericht standhaft sein werden, wenn Ermittlungsbehörden sich mit Hilfe des erlangten Passworts in den Account eines Tatverdächtigen einloggen können.

Außerdem sind Journalistinnen und Journalisten von dieser weitreichenden Maßnahme nicht ausgenommen, was neben der Einschränkung der allgemeinen Bürgerrechte zu einer erheblichen Einschränkung des journalistischen Quellenschutzes führt. Medienschaffende können ihre Aufgabe als Informationsvermittler und Wächter der Demokratie nur erfüllen, wenn sie ihren Informanten gewährleisten können, dass ihr Name, die Umstände der Recherche und ihre Dokumente nicht preisgegeben werden.

Die Ausleitung von Teilnehmerinformationen in ein polizeiliches Zentralregister in Folge einer Meldung ist ebenfalls hoch riskant und mit den Grundsätzen der Medien- und Informationsfreiheit nicht zu vereinbaren. Es ist zu erwarten, dass jährlich die persönlichen Daten von hunderttausenden Bürgerinnen und Bürgern oftmals zu Unrecht bei Strafverfolgungsbehörden gespeichert werden. Solch eine Verdachtsdatenbank stellt einen Dammbruch in bisher nicht gekanntem Ausmaß dar, der dazu geeignet ist, die Grundsätze unseres Rechtsstaats und unserer liberalen Demokratie zu erodieren.

In Ihrem Gesetzentwurf zur Änderung des NetzDG finden sich weitere Vorhaben, die ihrem Ziel, Menschen die Räume zu schaffen, sich ohne Angst zu äußern, ausdrücklich widersprechen:

Wenn sowohl Opfer, als auch Täter von den sozialen Netzwerken „Gruppen“ zugeordnet werden sollen, um besser zu analysieren, wer bedroht wird und woher die Bedrohung kommt, dann schaffen wir Register etwa von „Juden“, „Homosexuellen“ oder „Transpersonen“. Dies sollte nicht nur aufgrund der Lehren der deutschen Geschichte eine rote Linie sein, sondern auch in Anbetracht der aktuellen Berichterstattung über den Missbrauch von polizeilichen Datenbanken durch Beschäftigte.

Ebenso weisen wir abermals darauf hin, dass es der Meinungsfreiheit nicht gut tut, wenn dazu aufgefordert oder auch nur ermuntert wird, künstliche Intelligenz zur Reglementierung von Sprache und Meinung einzusetzen. Der Illusion, dass Technologie heute auch nur ansatzweise in der Lage wäre, die feinen Nuancen von Sprache und Meinung erkennen und die Grenze zwischen zulässiger zugespitzter Sprache und strafbarer Schmähung bewerten zu können, darf sich der Gesetzgeber nicht hingeben.

3.

Schon bei dem ersten Entwurf des Netzwerkdurchsetzungsgesetzes haben die Unterzeichner vor drei Jahren mit der *Deklaration für Meinungsfreiheit* darauf hingewiesen, dass Rechtsprechung und Gesetzesvollzug nicht weiter privatisiert werden dürfen. Auch wenn die geplante Stärkung der Nutzer wie beispielsweise durch die Einführung eines Widerspruchsrechts zu begrüßen ist, bleibt die grundlegende Problematik bestehen – wird an anderer Stelle sogar weiter verschärft. Statt hier Verbesserungen vorzunehmen, wird das Problem mit Ihrem Vorschlag nunmehr aber verschärft. Staatliche Aufgaben dürfen unseres Erachtens in dieser Weise nicht an private Unternehmen, schon gar nicht an solche aus Drittländern, ausgelagert werden.

Sehr geehrte Frau Bundesministerin,

wir möchten Sie daher heute dazu auffordern:

Verzichten Sie auf die Einbringung solch hoch problematischer, die Informations- und Meinungsfreiheit im Internet gefährdender Regelungen.

Fördern Sie stattdessen die Erstellung empirischer Studien über „Hatespeech“ und das Nutzerverhalten in sozialen Medien. Unterstützen Sie bestehende zivilgesellschaftliche Initiativen dauerhaft finanziell bei ihrem Engagement gegen Antisemitismus und gruppenbezogene Menschenfeindlichkeit – online und offline. Statten Sie, gemeinsam mit den Bundesländern, Polizei und Justiz nicht nur personell und sachlich besser aus, sondern sorgen Sie für regelmäßige Fortbildungen und eine Digitalisierung dieser Behörden, die den Staat selbst in die Lage versetzt, Internetkriminalität effektiv und zeitnah zu bearbeiten und zu bekämpfen. Sorgen Sie für mehr Schwerpunktstaatsanwaltschaften und Kammern an den ordentlichen Gerichten, die sich auf Hatespeech und Internetkriminalität spezialisieren. Beispiele wie das ZAC in NRW oder das Cybercrime-Kompetenzzentrum in Hessen zeigen, dass der Staat auch ohne private „Hilfsheriffs“ gute Arbeit leisten kann. Schützen Sie Opfer von Bedrohungen konkret und nicht nur symbolisch und richten Sie hier bessere Beratungs- und Anlaufstellen ein.

Deutschland und seine freiheitliche Demokratie hat eine Vorbildfunktion in der Welt. Darauf können wir heute stolz sein und sollten die Freiheit der Meinungsäußerung gegen ihre Feinde auch im Internet verteidigen. Wir müssen es daher tunlichst vermeiden, Bürgerrechte mit Gesetzen zu bekämpfen, die ihnen selbst widersprechen. Illiberale Ideen kann man nicht mit illiberalen Gesetzen bekämpfen. Die dänische Organisation Justitia hat in der Studie *The Digital Berlin Wall: How Germany (Accidentally) Created a Prototype for Global Online Censorship*

jedoch bereits die erschreckenden Implikationen des bisherigen NetzDG aufgezeigt. Insbesondere Länder, die eben keine rechtsstaatlichen Demokratien sind oder gar autoritär regiert werden, berufen sich bei ihren freiheitsfeindlichen Regelungen auf das Vorbild Deutschlands.

Wir bitten Sie daher eindringlich: Berücksichtigen Sie die breite Kritik an Ihren Gesetzentwürfen und ziehen Sie diese für eine grundlegenden Überarbeitung zurück.

Mit freundlichen Grüßen

- *BdKom – Bundesverband der Kommunikatoren e. V.*
- *Bundesverband Digitale Wirtschaft (BVDW) e. V.*
- *cnetz – Verein für Netzpolitik e. V.*
- *D64 – Zentrum für Digitalen Fortschritt e. V.*
- *Digitale Gesellschaft e. V.*
- *DJV – Deutscher Journalisten-Verband e. V.*
- *eco – Verband der Internetwirtschaft e. V.*

- *FlfF – Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V.*
- *GI – Gesellschaft für Informatik e. V.*
- *ISOC.DE e. V. – Internet Society*
- *LOAD e. V. – Verein für liberale Netzpolitik*
- *Stiftung Datenschutz*
- *Wikimedia Deutschland e. V.*

Wissenschaft & Frieden 1/2020 „Atomwaffen – Schrecken ohne Ende“

Die Atombombenabwürfe auf Hiroshima und Nagasaki vor 75 Jahren markierten etwas bis dahin nie Dagewesenes. Anders als bei den Kämpfen und Massenbombardements des Zweiten Weltkriegs, die in Europa und Asien Millionen Menschenleben auslöschten, brachte hier jeweils eine einzelne Bombe den Massentod. Im Kalten Krieg bestand die Gefahr, dass Dutzende Länder Nukleararsenale erwerben und mit dem Einsatz drohen. Das wurde mit dem nuklearen Nichtverbreitungsvertrag verhindert, der vor 50 Jahren in Kraft trat. Der Schrecken durch Atomwaffen aber existiert weiter und nimmt ohne Abrüstungsverträge sogar wieder zu.

Außerhalb des Schwerpunkts erläutert *Michael T. Klare* die „Pompeo-Doktrin“ und wie die USA die Klimaveränderungen in der Arktis zu ihrem Vorteil nutzen wollen, und im Gastkommentar befasst sich *Michael Müller* mit Frieden in Bewegung.

„Nahost-Poker oder Mord als Politik“ ist das Thema der von Jürgen Nieth kommentierten Presseschau.

In W&F 1/2020 schreiben zu diesem Thema:

- *Regina Hagen*: Und wenn der Druckkessel platzt?
- *Franz Fujara*: Der Sündenfall – Atomrüstung, Wissenschaft und die Verantwortung des Einzelnen
- *Karl Hans Bläsius*: Atomkrieg – aus Versehen?
- *Jürgen Scheffran*: Atomwaffen, Umwelt und Klima – Grenzen des fossil-nuklearen Zeitalters
- *Susi Snyder*: Bombenbauer und Bombenbanker – Das Geschäft mit Atomwaffen
- *Regina Hagen*: Atomwaffen – eine Übersicht
- *Jens Heinrich*: Kernwaffen in Südasien – Arsenale, Doktrinen und Rüstungskontrolle
- *Gregory Kulacki*: Ein eigener Ansatz – Die Atomwaffendoktrin Chinas
- *Rebecca Johnson*: 50 Jahre NVV – Der nukleare Nichtverbreitungsvertrag, (k)eine Erfolgsgeschichte?
- *Ute Finckh-Krämer*: Mythos nukleare Abschreckung
- *Heinz-Günther Stobbe*: Das Ende der „Frist“ – Die atomare Abschreckung im Licht der römisch-katholischen Soziallehre
- *Moritz Kütt*: Wie werden Kernwaffen zerstört? Eine Abschätzung von Abrüstungsraten

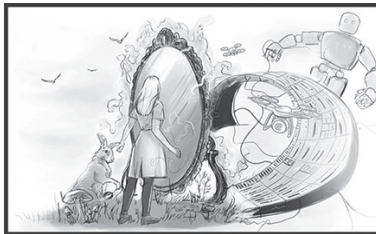


Wissenschaft & Frieden, 4/2019: „Ästhetik im Konflikt“.
9,00 € Inland, EU plus 3,00 € Porto (Bitte um Vorkasse: Sparkasse KölnBonn, DE86 3705 0198 0048 0007 72, SWIFT-BIC COLSDE33XXX)

W&F erscheint vierteljährlich. Jahresabo 35 €, ermäßigt 25 €, Ausland 45 €, ermäßigt 35 €, Förderabo 60 €. W&F erscheint auch in digitaler Form – als PDF und ePub. Das Abo kostet für Bezieher der Printausgabe zusätzlich 5 € jährlich – als elektronisches Abo ohne Printausgabe 20 € jährlich.

Bezug: W&F c/o BdWi-Service, Gisselberger Str. 7, 35037 Marburg, E-Mail: vertrieb@wissenschaft-und-frieden.de, www.wissenschaft-und-frieden.de

Wissenschaft und Frieden ist Trägerin des Göttinger Friedenspreises 2018



KÜNSTLICHE INTELLIGENZ WuNDER^{als}LAND

#FifKon19
Bremen, 22. – 24.11.19
2019.fiffkon.de

#FifKon19

Michael Ahlmann, Hans-Jörg Kreowski, Philip Love, Ralf E. Streibl, Karin Vosseberg, Margita Zallmann

Künstliche Intelligenz als Wunderland

Editorial zum Schwerpunkt

Die beiden Romane Alice im Wunderland und Alice hinter den Spiegeln von Lewis Carroll gehören zur Weltliteratur. Die Protagonistin erlebt phantastische Abenteuer und trifft skurrile Gestalten wie das weiße Kaninchen, den verrückten Hutmacher, die Grinsekatz, den Märzhasen und andere mehr. Viele Figuren sind an Schach und Kartenspielen angelehnt. Gewisse Ähnlichkeiten zur Künstlichen Intelligenz sind da doch kaum zu leugnen. Aufsehen erregt haben Spieleprogramme für Schach, Go, Poker und für viele andere Spiele, gegen die menschliche Gegnerinnen und Gegner auf verlorenem Posten stehen. Immer mehr Roboter in merkwürdiger Gestalt werden entwickelt, die teils erstaunliche Fähigkeiten besitzen, aber auch häufig bemerkenswert unbeholfen wirken.

Doch egal, ob mit oder ohne Wunderland-Metapher, es gibt seit einigen Jahren einen riesigen Hype um die Künstliche Intelligenz. Die unbestreitbaren wissenschaftlichen und technologischen Erfolge haben weltweit bei Politik und Wirtschaft hohe Erwartungen geweckt. In nahezu allen gesellschaftlichen Bereichen von Produktion, Dienstleistung, Transport und Verkehr über Verwaltung, Medizin, Bildung und Wissenschaft bis hin zum staatlichen Handeln einschließlich Polizei und Militär werden bahnbrechende Fortschritte prognostiziert. Auch das alltägliche Leben wird sich verändern. Es ist allerdings noch keineswegs gesichert, dass alle diese Blühträume reifen. Man darf davon ausgehen, dass die aktuellen Entwicklungen im Bereich der Künstlichen Intelligenz und der Robotik vielfältige Chancen eröffnen, aber auch erhebliche Risiken bergen wie die Vernichtung von Arbeitsplätzen, neue Formen der sozialen Überwachung und neue Arten perfider Waffensysteme.

Klar ist jedenfalls, dass einiges passieren wird. Denn es wird in den kommenden Jahren unglaublich viel Geld – umgerechnet Hunderte von Milliarden Euro – in die Entwicklung der Künstlichen Intelligenz (KI) gesteckt. Viele Länder der Welt haben KI-Strategien formuliert, um den Anschluss nicht zu verlieren, um die künftige Wertschöpfung zu garantieren, um führend zu sein oder zu bleiben, um in einem – möglicherweise nur eingebildeten – geostrategischen Rennen die Nase vorn zu haben. Interessanterweise wird dabei oft darauf verwiesen, dass nicht nur die Chancen zum Wohle der Menschen genutzt, sondern auch die Risiken vermieden und ethische Grundsätze eingehalten werden sollen. Ein typisches Beispiel ist die Strategie Künstliche Intelligenz der Bundesregierung (Stand: November 2018), die auf 47 Seiten einen detaillierten Rundumschlag macht, welche Bereiche wie von KI profitieren sollen. Die erklärten Ziele sind der Ausbau der „Wettbewerbsfähigkeit der deutschen Wirtschaft“ und ein „spürbarer gesellschaftlicher Fortschritt“. Das ist der Regierung nur vergleichsweise bescheidene 3 Milliarden Euro für sieben Jahre wert, während die Volksrepublik China im gleichen Zeitraum wohl 150 Milliarden ausgeben will und in den USA ohnehin jährlich mehr als der zehn- oder zwanzigfache Betrag investiert wird. Auch der Bundestag räumt dem Thema KI einen hohen Stellenwert ein. Er hat im Sommer 2018 eine Enquete-Kommission KI mit dem Zusatz „Gesellschaftliche Verantwort-



Die Eröffnungsveranstaltung fand im Übersee-Museum statt
Foto: Jürgen Howaldt, CC BY-SA 2.0 DE

tung und wirtschaftliche, soziale und ökologische Potenziale“ eingerichtet, um damit „eine der zentralen Debatten unserer Zeit“ aufzugreifen. Man kann nur wünschen, dass die Abgeordneten vernünftige Einsichten gewinnen.

Die Fiff-Konferenz 2019 bot den über 150 Teilnehmerinnen und Teilnehmern am Freitag und Samstag und über 100 am Sonntag die Möglichkeit, zu dieser Gemengelage in einem breiten Spektrum an Themen vieles über die gesellschaftlichen Auswirkungen der Entwicklung und des Einsatzes von Künstlicher Intelligenz und Robotik zu erfahren, sich damit auseinanderzusetzen und darüber zu diskutieren.

Der Schwerpunkt besteht aus den schriftlichen Fassungen der Vorträge auf der Fiff-Konferenz 2019 mit der Ausnahme von Rainer Rehaks Beitrag, der in der nächsten Fiff-Kommunikation nachgeholt wird, sowie Berichten aus den Arbeitsgruppen, bei denen nur die Arbeitsgruppe zum Drohnenkrieg fehlt. Die Artikel sind inhaltlich gruppiert, wobei die Zuordnung nicht immer ganz eindeutig möglich war:

- Ethische Aspekte mit den Artikeln von Marit Hansen, Veronika Thiel und Alexander von Gernler,

- Wirtschaft, Arbeit und Gesundheit mit dem Beitrag von Dominik Wetzel und Christoph Marischka und den Arbeitsgruppenberichten von Birgit und Michael Ahlmann sowie Sylvia Johnigk,
- Umwelt, Nachhaltigkeit und Klimawandel mit Beiträgen von Marie-Luise Abshagen und Nelly Grotefendt sowie von Bernhard Stoevesandt und Martin Dörenkämper und dem Arbeitsgruppenbericht von Ulrike Erb, Oliver Radfelder und Karin Vosseberg,
- Politik und Überwachung mit dem Artikel von Capulcu und dem Kurzbericht von Arkadi Schelling,
- Militär und zivile Gegenpositionen mit den Artikeln von Mathias Monroe und Elke Schwarz und den Arbeitsgruppenberichten von Peter Ansorge sowie Liam Hurwitz und Simon Rundé,

Den Schlusspunkt bildet der Artikel von Detlef Borchers, der ein interessantes Schlaglicht auf die Anfänge der KI wirft.

Auch wenn die meisten Beiträge eher die problematischen Seiten des KI-Hypes beleuchten, geht es keineswegs darum, KI in Gänze schlecht zu machen und mit Kassandrarufern das Unheil heraufzubeschwören. Andererseits ist aber eine kritische Auseinandersetzung dringend geboten, weil die allermeisten Veranstaltungen zu KI – sowohl die wissenschaftlichen als auch populären – den Stand der Dinge und die zu erwartenden Entwicklungen hochjubeln und euphorisch begrüßen. Das Programm des Wissenschaftsjahres 2019 zur KI belegt das eindrucksvoll. Die vielen Dutzenden Veranstaltungen haben fast alle das Für betont und zum Wider ist wenig bis gar nichts gesagt worden. In diesem Kanon war die FIF-Konferenz 2019 eine notwendige Gegenstimme.

Zu allen Vorträgen gibt es Videoaufzeichnungen, deren Nachbearbeitung bei Erscheinen dieser FIF-Kommunikation fertig sein sollte. Sie sind verlinkt auf der FIFKon2019-Webseite <https://2019.fifkon.de> und verfügbar als Mobile Lecture der Universität Bremen <https://mlecture.uni-bremen.de/ml/> im Wintersemester 2019/2020 sowie unter <https://media.ccc.de>.



„Gearbeitet“ wurde im MZH der Uni Bremen
Foto: Verograph, CC BY-SA 3.0

Danksagung

Das Organisationsteam der FIF-Konferenz 2019 bedankt sich ganz herzlich bei allen ungenannten Helferinnen und Helfern, ohne die eine solche Konferenz nicht stattfinden könnte.

Dank gilt auch allen Organisationen, die ideell und finanziell Unterstützung geleistet haben, so dass eine Konferenz mit vielen Höhepunkten machbar war – ohne Defizit. Dazu gehören die *Fakultät für Elektrotechnik und Informatik der Hochschule Bremen*, der *Studienbereich Informatik der Hochschule Bremerhaven* und aus der Universität Bremen die Informatik-Arbeitsgruppen *Softwaretechnik* (Prof. Dr. Rainer Koschke), *Graphtransformation* (Prof. Dr. Hans-Jörg Kreowski), *Theorie der Künstlichen Intelligenz* (Prof. Dr. Carsten Lutz), *Digital Media Lab* (Prof. Dr. Rainer Malaka), *Kombinatorische Optimierung und Logistik* (Prof. Dr. Nicole Megow) sowie *Computergraphik und Virtuelle Realität* (Prof. Dr. Gabriel Zachmann). Der Universität Bremen ist für die Bereitstellung der Räume zu danken, dem Fachbereich Mathematik/Informatik für die Bezahlung des Wachdienstes und der Medienstelle mit Alexander Hillmann, weil sie die technische Ausstattung für die Videoaufzeichnung und die Nachbearbeitung zur Verfügung gestellt hat. Als Nicht-regierungsorganisationen sind *AlgorithmWatch*, der *Arbeitskreis Software-Qualität und -Fortbildung e. V. (ASQF)*, die *Bremische Stiftung für Rüstungskonversion und Friedensforschung*, der *Chaos Computer Club e. V. (CCC)*, *Digitalcourage e. V.*, die *Gesellschaft für Informatik e. V. mit den Fachbereichen Informatik und Gesellschaft (FBIUG)* sowie *Künstliche Intelligenz (FBKI)*, die *Humanistische Union* und die *Informationsstelle Militarisierung e. V. (IMI)* zu nennen. Weitere Unterstützung kam vom *Deutschen Gewerkschaftsbund (DGB)*, vom *Landesverband Bremen der Gewerkschaft Erziehung und Wissenschaft (GEW)* – und der *IG Metall (IGM)* sowie von den Unternehmen *encoway*, *HEC*, *International Software Quality Institute (ISQI)*, *MeVis Medical Solutions AG* und *WPS – Workplace Solutions*.

Zu danken ist auch den Vortragenden und den Organisatorinnen und Organisatoren von Arbeitsgruppen, die mit ihren Beiträgen für ein breitgefächertes und anregendes Programm gesorgt haben. Als besonderes kulturelles Highlight der Konferenz muss auch hervorgehoben werden, dass das Theater der Versammlung die Einladung zu einer Aufführung ihrer experimentellen und interaktiven Klick-Performance *C COPY A, VERSCHLÜSSELT* angenommen hat. Außerdem hat das vielfach bewunderte Tagungsmotiv von Caro von Totth und Karin Vosseberg unsere Würdigung verdient.

Ein ganz besonderer Dank gilt den Teilnehmerinnen und Teilnehmern für ihr zahlreiches Erscheinen, für ihre vielen Diskussionsbeiträge und die gute Stimmung, für die sie gesorgt haben. Ohne sie wäre alle Mühe umsonst gewesen.

Zum Organisationsteam der FIF-Konferenz 2019 gehörten u. a. Birgit Ahlmann, Michael Ahlmann, Christiane Bodammer, Philipp Dittmann, Stefan Eirich, Johannes Feest, Hans-Jörg Kreowski, Aaron Lye, Philip Love, Klaus Lüttich, Arkadi Schelling, Ingrid Schlagheck, Andreas Spillner, Ralf E. Streibl, Karin Vosseberg und Margita Zallmann. Philipp Dittmann, Stefan Eirich, Alexander Hillmann Aaron Lye, Philip Love, Christian Pfaab, Aljoscha Windhorst und Margita Zallmann bildeten das Videoteam.

Aus unserer Sicht hat sich die Arbeit gelohnt.

FIfF-Konferenz 2019 – Künstliche Intelligenz als Wunderland

Begrüßung

Liebe Mitglieder des FIfF,
liebe Freundinnen und Freunde,
liebe Gäste,

es ist ein alter Menschheits Traum: Eine Maschine zu konstruieren, die uns Menschen möglichst nahe kommt, die uns das Denken abnimmt, die vielleicht eines Tages über uns hinauswächst und eine bessere Welt schafft: ein Wunderland. Heute verbinden wir diesen Traum mit der *Künstlichen Intelligenz*, die tatsächlich in begrenzten Anwendungsbereichen erstaunliche Leistungen zu erbringen vermag.

Doch jenseits von Bilderkennung und AlphaGo stellen sich Fragen an die Künstliche Intelligenz, zu deren Beantwortung diese Konferenz einen Beitrag leisten will:

Was kann Künstliche Intelligenz?

„Der Computer Nr. 3 sucht für mich den richtigen Boy. Und die Liebe ist garantiert für beide dabei.“ Für die Schlagersängerin France Gall war Ende der 1960er Jahre das Wunderland KI noch bescheiden. Was damals ein naiver Traum war, leisten heute Plattformen wie *Tinder*. Beim Schach und bei Go hat die Künstliche Intelligenz – oder besser: das Maschinelle Lernen – den Menschen schon lange hinter sich gelassen. Doch bei vielen anderen Fragen ist der Mensch der Maschine immer noch weit überlegen, und es ist sogar fraglich, ob eine der menschlichen Intelligenz analoge maschinelle Intelligenz – wie postuliert durch die *starke KI*-These – überhaupt möglich ist.

KI-Experte Wolfgang Wahlster übersetzt KI mit „Künftige Informatik“ – dies kann interpretiert werden als eine Menge von Methoden, die bereits heute und künftig in der Informatik eingesetzt werden, und die sich (teilweise) von den bisher angewendeten unterscheiden – nicht mehr, nicht weniger. Wie wir aus der Informatik wissen, sind die theoretischen Grenzen der Berechenbarkeit auch durch Künstliche Intelligenz nicht überwindbar.

Doch manche erhoffen sich von Künstlicher Intelligenz, dass sie uns ins Wunderland führt, vor allem stets die *richtigen* Entscheidungen trifft. Der Autor Max Tegmark beschreibt in seinem Buch *Leben 3.0* ein utopisches – oder dystopisches? – Szenario einer Welt, die von einer Künstlichen Intelligenz so gesteuert wird, dass alle Probleme gelöst werden, vor denen wir heute stehen. Diese Hoffnung ist nicht so weit hergeholt: Für eines der heute größten Menschheitsprobleme, dem Klimawandel, erhoffen sich einige eine rechtzeitig eintreffende technische Lösung – ein Wunder, würde man in der Theologie sagen. Die bereits heute bestehenden Lösungsansätze: technisch – Windräder, Photovoltaik – oder gesellschaftlich – Änderung unseres Lebensstils und der Politik – sind offenbar zu bescheiden: Sie werden übersehen, ignoriert oder abgelehnt. Die hier glauben, uns ins technologische Wunderland führen zu können, sind übrigens häufig die gleichen, die einer Greta Thunberg das Auftreten eines *Messias* vorwerfen.

Was soll Künstliche Intelligenz?

Doch was, wenn die Maschine errechnet, dass der Mensch die meisten der heutigen Probleme – Klima, Umwelt, Kriege, Armut – zu verantworten hat und daraus schließt, dass zunächst einmal der Mensch aus dieser Welt verschwinden müsse? Gut, das ist vielleicht ein extremes Szenario. Hans Jonas postulierte in seinem Prinzip Verantwortung 1979 den Imperativ: „Handle stets so, dass die Wirkungen Deiner Handlung verträglich sind mit der Permanenz echten menschlichen Lebens auf Erden.“

Die Frage ist: Wie können wir Künstliche Intelligenz kontrollieren, und nach welchen Kriterien? Bereits heute führen die verwendeten Lernverfahren zu Ergebnissen, die mit unserer Auffassung von Ethik nicht immer in Einklang stehen – beispielsweise beim programmierten Rassismus, wenn (Vor-) Urteile, die in die Daten bereits eingeschrieben sind, sich reproduzieren und beim *lernen* noch verstärken? Wer wählt die *richtigen* Daten aus, um diese Systeme zu trainieren? Was sind überhaupt *richtige* Daten? Daten, die simple Fakten ebenso widerspiegeln wie unsere Wertvorstellungen – und welche Wertvorstellungen sind das? Wie können wir definitorische Daten von stereotypen Daten systematisch trennen? Hier wird es politisch: Wir müssen uns über die Daten, mit denen Maschinen trainiert werden, demokratisch verständigen. Vor allem dürfen wir die Antwort auf diese Fragen nicht privaten Unternehmen überlassen.

Letztlich kommen wir wieder zu der Frage, die das FIfF von jeher beschäftigt: Was soll Technologie? Welchem Zweck soll sie dienen? Maja Göpel, die Generalsekretärin des Wissenschaftlichen Beirats der Bundesregierung zu Globalen Umweltveränderungen, kritisierte bei einem Vortrag auf der Netzpolitik-Tagung in diesem Jahr, dass bei der Digitalisierung – dazu ist die Künstliche Intelligenz zweifellos zu zählen – die Frage nicht gestellt würde, was oder wem sie denn eigentlich dienen würde. Meist gehe es um Arbeitsplätze, um Produktivität oder um Wettbewerbsfähigkeit. Sie zitiert einen Begriff aus der Zeitschrift *The New Yorker*, der seinen Ursprung im Silicon Valley hat: *Human Degeneration*. Dies sei „das äquivalente Bild zu Climate Change“, also ein extraktives Bild der Technologisierung, das aus den Systemen meist finanziellen Ertrag zieht und damit dazu geführt hat, dass das System in seiner Beschaffenheit, in seiner Gesundheit abnimmt. Eigentlich sei es eine Wirtschaftsagenda mit dem Leitbild des Wachstums. Maja Göpel fragt dagegen nach dem „Menschenbild, wo Technologie der Potenzialentfaltung dient, die wir in uns haben.“

Maja Göpel weiter: „Aber wir Menschen sind doch schon da. Warum bauen wir denn lauter Maschinen, die dann Energiekonsumenten werden, anstatt zu sagen, wir nutzen die Menschen, die schon da sind, wenn diese Maschinen immer noch dem hinterherhinken, was wir schon alle können? ... Was ist denn eigentlich das, was wir zusätzlich erreichen wollen und nicht das, was uns substituiert.“ Letztlich gehe es um die Frage, wie wir das neue Leitbild des 21. Jahrhunderts schaffen können.

Wer verantwortet Künstliche Intelligenz?

Oft wird bei dieser Tagung von Ethik die Rede sein. Im Wunderland der Künstlichen Intelligenz stellt sich die Frage der Ethik gleich aus zwei Perspektiven:

- Welcher Ethik folgen die HerstellerInnen von Produkten der Künstlichen Intelligenz? Wer ist verantwortlich für ihre Produkte?
- Können Maschinen ethisch verantwortlich sein?

Die zweite Frage kann im FIF-Kontext schnell beantwortet werden: Wir sind der Überzeugung, dass es eine Maschinenethik nicht geben kann. Eine Maschine *handelt* immer so, wie es die menschliche Programmiererin, der menschliche Programmierer vorgibt. Auch eine Anwendung der Künstlichen Intelligenz folgt den Vorgaben eines Programms – und sei es noch so komplex.

Das führt uns zurück zur ersten Frage: Wer ist für den Einsatz beispielsweise eines autonomen Systems verantwortlich, wenn ein Fehler passiert? Wenn bei herkömmlichen Waffen jemand auf den Knopf gedrückt hat und vorher jemand anders den Befehl dazu gegeben hat, kann diese Verantwortung Personen zugeschrieben werden. Doch wer ist bei autonomen Systemen *verantwortlich*? Die Programmiererin, die lange vor dem Einsatz ein Programm implementiert hat? Der Designer, der es entworfen hat? Die Technikerin, die das System wartet und betreibt?

Der Konstrukteur, der es gebaut hat? Das Management des Unternehmens, für das alle diese Menschen arbeiten?

Einerseits ist ethisches Handeln immer eine Frage der persönlichen Entscheidung und Verantwortung. Gleichzeitig werden Ethikkodizes gefordert, um Leitlinien für ethisches Handeln zu bieten. Das kann sinnvoll sein. Doch darf es niemals angemessene Regulierung, gesetzliche Vorgaben und politische Entscheidungen ersetzen. Mit *freiwilligen Selbstverpflichtungen* dürfen wir uns auch hier nicht zufrieden geben – immer wieder hat sich gezeigt, dass sie nur eine Ausflucht sind, nicht wirklich Verantwortung übernehmen zu müssen.

Klar ist: Künstliche Intelligenz darf nicht im Widerspruch zu den Grund- und Menschenrechten stehen. Da wir es mit Daten zu tun haben, ist dies zunächst einmal der Datenschutz, aber das ist bei weitem nicht alles.

Über einige dieser Aspekte wollen wir an diesem Wochenende diskutieren und streiten. Ich danke dem Organisationsteam und der Regionalgruppe Bremen im Namen des FIF-Vorstands herzlich für die Organisation und die Ausrichtung dieser FIF-Konferenz 2019. Dazu wünsche ich viel Freude bei der Konferenz, viele neue Anregungen und viele neue Erkenntnisse – über die Künstliche Intelligenz als Wunderland.

Vielen Dank.



Marit Hansen

Die Empfehlungen der Datenethikkommission: Bedeutung für die Informatik

Die Arbeit der Datenethikkommission

Auftrag

Anfang 2018 schlossen CDU, CSU und SPD einen Koalitionsvertrag für die politische Arbeit in der 19. Legislaturperiode [1]. Darin wird angekündigt, „zeitnah eine Daten-Ethikkommission ein[zu]setzen, die Regierung und Parlament innerhalb eines Jahres einen Entwicklungsrahmen für Datenpolitik, den Umgang mit Algorithmen, künstlicher Intelligenz und digitalen Innovationen vorschlägt. Die Klärung datenethischer Fragen kann Geschwindigkeit in die digitale Entwicklung bringen und auch einen Weg definieren, der gesellschaftliche Konflikte im Bereich der Datenpolitik auflöst.“ [1, S. 47]

Im Juni 2018 legten das Bundesministerium des Innern, für Bau und Heimat und das Bundesministerium der Justiz und für Verbraucherschutz die Leitfragen der Bundesregierung an die Datenethikkommission vor [2]. In drei Bereichen wurden Fragen an die Datenethikkommission gestellt:

1. Algorithmen-basierte Prognose- und Entscheidungsprozesse
2. Künstliche Intelligenz
3. Daten

Zusammensetzung

Die Mitglieder der Datenethikkommission waren von der Bundesregierung unter Federführung des Bundesministeriums des Innern und Heimat sowie des Bundesministeriums für Justiz und Verbraucherschutz benannt worden. Während die meisten Expertinnen und Experten persönlich berufen worden waren, hatten die drei institutionellen Mitglieder – der Verbraucherzentrale Bundesverband e.V. (vzbv), der Bundesverband der Industrie (BDI) sowie die bzw. der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) – die Möglichkeit, sich im Bedarfsfall durch verschiedene Personen vertreten zu lassen.

Ganz unterschiedliche wissenschaftliche Disziplinen und Sektoren wurden durch die Mitglieder repräsentiert: Jura, Medizinethik, Philosophie, Theologie, Wirtschaft, Informatik und Statistik. Anders als der Name *Datenethikkommission* vermuten lässt, hatten nur wenige Mitglieder eine fundierte Ethikausbildung. Stattdessen überwog der Anteil der Mitglieder mit juristischem Hintergrund diejenigen anderer Disziplinen. Dies stand im Einklang mit dem Arbeitsauftrag. Der Anteil derjenigen, deren Arbeit von Informationstechnik geprägt ist, war deutlich geringer. Das ist deswegen relevant, weil sich die Begrifflichkeiten,

fundamentalen Konzepte und gedanklichen Modelle zwischen den Disziplinen stark unterscheiden. Dieselben Begriffe können ganz verschiedene Bedeutungen haben, Missverständnisse sind programmiert.

Eine interdisziplinäre Zusammenarbeit liefert oft bessere Ergebnisse, weil viele Sichtweisen eingeflossen sind. Für eine effiziente Kooperation ist aber die Anfangsphase, in der sich die Akteure aufeinander einstellen und *einschwingen*, von besonderer Wichtigkeit – sie lässt sich nicht beliebig verkürzen. In der Datenethikkommission stellte dies eine Herausforderung dar, weil die Bundesregierung das Gutachten bereits nach einem Jahr erwartete.

Arbeitsweise

Jeden Monat trat die Datenethikkommission für mindestens zwei Tage zusammen. Besonders intensiv wurden Entwürfe und Vorschläge für Empfehlungen im Rahmen einer mehrtägigen Klausurtagung im Juli 2019 diskutiert.

Im Februar 2019 organisierte die Datenethikkommission eine öffentliche Tagung zum Thema *Selbst- und Fremdbestimmung im Zeitalter künstlicher Intelligenz* mit eingeladenen Vorträgen [3], im Mai 2019 fand die öffentliche Round-Table-Diskussion *Für eine ethische Gestaltung unserer digitalen Zukunft* statt und brachte verschiedene Akteure aus dem In- und Ausland zusammen [4]. Ebenso öffentlich war die Abschlussveranstaltung mit Übergabe des Gutachtens [5]. Informationen zu allen Veranstaltungen mit Videomitschnitten stehen auf der Webseite der Datenethikkommission zur Verfügung. Außerdem wurden in einigen Sitzungen der Datenethikkommission weitere Expertinnen und Experten zu verschiedenen Themen angehört, und auch mit anderen Gremien und Institutionen bestand ein Austausch, beispielsweise der Enquête-Kommission *Künstliche Intelligenz*, der Kommission *Wettbewerbsrecht 4.0*, dem Digitalrat der Bundesregierung und dem Sachverständigenrat für Verbraucherfragen.

Wie es typisch für Debatten auf Basis ethischer Prinzipien ist, eilt man sich sehr schnell auf allgemeine abstrakte Aussagen. Sobald allerdings die Sachverhalte im Detail beleuchtet werden und verschiedene Sichtweisen auf die Themen eingenommen werden, zeigt sich der Diskussions- und Klärungsbedarf. Für diese Phase waren Szenarien (*Use Cases*) zu gemeinsam gewählten Oberthemen hilfreich, um konkrete Fragen in den Blick nehmen zu können. Damit wurde auch innerhalb der Datenethikkommission ein gemeinsames Fundament gelegt, auf dessen Basis die Empfehlungen erarbeitet wurden.

Das Gutachten der Datenethikkommission

Anspruch

Der Arbeitsauftrag an die Datenethikkommission bestand darin, „ethische Maßstäbe und Leitlinien für den Schutz des Einzelnen, die Wahrung des gesellschaftlichen Zusammenlebens und die Sicherung und Förderung des Wohlstands im Informationszeitalter“ zu entwickeln. Die Kommission sollte der Bundesregierung „Empfehlungen oder Regulierungsoptionen vorschlagen,

wie die ethischen Leitlinien entwickelt, beachtet, implementiert und beaufsichtigt werden können.“ [2, S. 2].

Das von der Datenethikkommission vorgelegte Gutachten enthält nicht, wie teilweise vermutet, Gesetzentwürfe oder technische Spezifikationen. Das Gutachten ist auch kein Lehrbuch oder eine Monographie. Aber es hat den Anspruch, in lesbarer und nachvollziehbarer Weise Leitlinien und Vorschläge für die Politik und die gesellschaftliche Debatte darzustellen. Hervorzuheben ist, dass die Empfehlungen des Gutachtens im Konsens von *allen* Mitgliedern der Datenethikkommission verabschiedet wurden.

Aufbau

Das 240 Seiten umfassende Gutachten stellt zunächst ethische und rechtliche Grundsätze und Prinzipien vor. Anschließend werden wichtige technische Erläuterungen gegeben. Diese Kapitel legen das Fundament für die folgenden Ergebnisse. Ein erster Schwerpunkt liegt auf der *Governance* komplexer Datenökosysteme. Die Kommission entschied sich dazu, sich dem Gesamtthema über zwei verschiedene Perspektiven zu nähern: der Perspektive *Datenrechte und Datenpflichten* und der Perspektive *algorithmischer Systeme*. Diese Arbeiten waren leitend für die folgenden beiden Schwerpunkt-Kapitel.

Ergebnisse

Das Gutachten der Datenethikkommission mit seinen 75 Empfehlungen steht öffentlich zur Verfügung [6]. Eiligen Leserinnen und Lesern sei die Kurzfassung empfohlen [7]. Im Folgenden soll nur veranschaulicht werden, worum es im Gutachten geht:

Etwa die Hälfte der Empfehlungen betrifft die Datenperspektive, in der zwischen Anforderungen an die Nutzung und Kontrolle personenbezogener Daten und dem Datenzugang jenseits des Personenbezugs unterschieden wird. Die Datenethikkommission hat wesentliche Faktoren identifiziert, die für eine faire Gestaltung von Datenzugängen relevant und je nach Fallkategorie verschieden ausgeprägt sein können (siehe Abbildung 1).

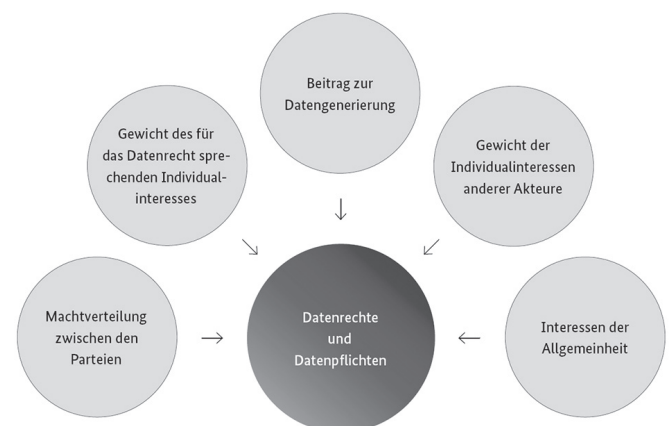


Abbildung 1: Faktoren zur Ausgestaltung von Datenrechten und Datenpflichten [6, S. 86]

Die andere Hälfte der Empfehlungen betrifft die Sicht auf algorithmische Systeme. Wesentlich dabei ist, dass hier nicht nur

Methoden der Künstlichen Intelligenz in den Fokus genommen wurden. In der Terminologie unterscheidet die Datenethikkommission zwischen algorithmisch-determinierten, algorithmisch-getriebenen und algorithmisch-basierten Entscheidungen, je nach Grad der menschlichen Einbindung in einer zu treffenden Entscheidung (siehe Abbildung 2).

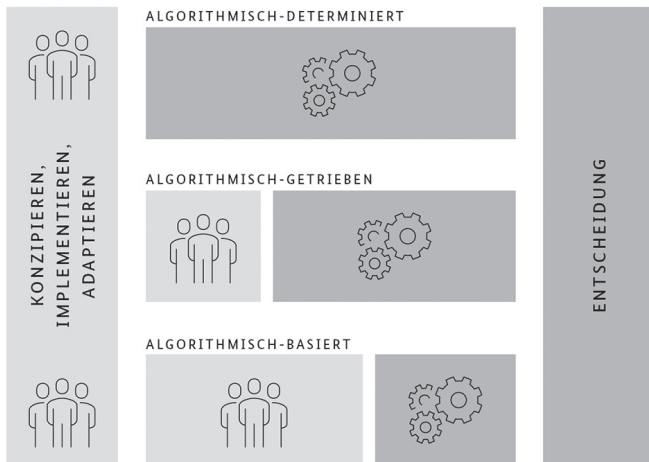


Abbildung 2: Charakteristika algorithmischer Systeme [6, S. 162]

Auch der eigentliche Algorithmus oder Code stellt nur eine Komponente der Betrachtungen dar. Im Fokus steht stattdessen das algorithmische System, das den gesamten Technologie-Stack und auch die organisatorischen Abläufe und Maßnahmen umfasst. Beispielsweise verstehen viele Menschen nicht, wie der Algorithmus ihres Spam-Filters für E-Mail funktioniert. Dennoch folgt aus diesem Mangel an Verständnis noch nicht, dass sie keinen Spam-Filter einsetzen sollten, denn organisatorisch können Maßnahmen getroffen werden, dass keine E-Mails verloren gehen (wenn sie beispielsweise in einen Spam-Ordner verschoben werden, wo man regelmäßig nachschaut).

Während das algorithmische System im Spam-Filter-Beispiel als weniger kritisch einzuordnen ist, weisen Systeme, die einen Schaden für Leib und Leben verursachen können, eine deutlich höhere Kritikalität auf. Hierzu schlägt die Datenethikkommission fünf Stufen vor, deren Risiken mit den für die Kategorien passenden Maßnahmen angemessen eingedämmt werden müssen (siehe Abbildung 3).

Lessons (to be) learned – die Informatikperspektive

Ein Gutachten zu Daten und zukünftigen Entscheidungen im Sinne einer fairen Gestaltung des Informationszeitalters hat selbstverständlich einen engen Bezug zur Informationstechnik in all ihren Facetten.

Im Folgenden werden einige für Informatikerinnen und Informatiker spannende Punkte herausgegriffen, da hier ein besonderer Bedarf an Forschung, Entwicklung und Standardisierung aus informationstechnischer und datenanalytischer Sicht besteht. Zudem sollten regulatorische Ansätze die Informatikexpertise berücksichtigen und aufgreifen:

Eine Kernforderung sind Maßnahmen gegen ethisch nichtvertretbare Datennutzungen (Empfehlung 1). Als Beispiele werden ge-

nannt: Totalüberwachung, die Integrität der Persönlichkeit verletzende Profilbildung, gezielte Ausnutzung von Vulnerabilitäten, *Addictive Designs* und *Dark Patterns*, dem Demokratieprinzip zuwiderlaufende Beeinflussung politischer Wahlen, *Lock-in* und systematische Schädigung von Verbrauchern sowie viele Formen des Handels mit personenbezogenen Daten.

Die Datenethikkommission äußert sich auch zu Anonymisierung und Pseudonymisierung und wünscht die Entwicklung von Verfahren und Standards (Empfehlung 20). Auch synthetische Daten werden hier genannt.

Potenzial – und die Notwendigkeit der fairen Weiterentwicklung – sieht die Datenethikkommission in innovativen Datenmanagement- und Datentreuhandsystemen, sofern diese praxisgerecht, robust und datenschutzkonform ausgestaltet sind (Empfehlung 21). Dazu gehören rein technische *Dashboards* (*Privacy Management Tools, PMT*) bis hin zu umfassenden Dienstleistungen der Daten- und Einwilligungsverwaltung (*Personal Information Management Services, PIMS*).

Die Datenethikkommission empfiehlt auch eine Pflicht zur Interoperabilität bzw. Interkonnektivität bei Messenger-Diensten und sozialen Netzwerken, die ohne unerwünschte Seiteneffekte – also ohne Vollkontrolle bei zentralen Providern – umgesetzt werden sollte (Empfehlung 23). Dies ginge über das Recht auf Datenübertragbarkeit aus Artikel 20 Datenschutz-Grundverordnung hinaus.

Für die beim Einsatz algorithmischer Systeme verwendeten Datensätze und Modelle wird empfohlen, Anforderungen an Dokumentation und Protokollierung rechtssicher festzulegen und damit auch im Falle einer Kontrolle nachvollziehbar zu machen (Empfehlung 50). Bei sensiblen Anwendungen kann dies auch eine Pflicht bedeuten, Programmabläufe einer Software, die nachhaltige Schäden verursachen können, zu dokumentieren und zu protokollieren.

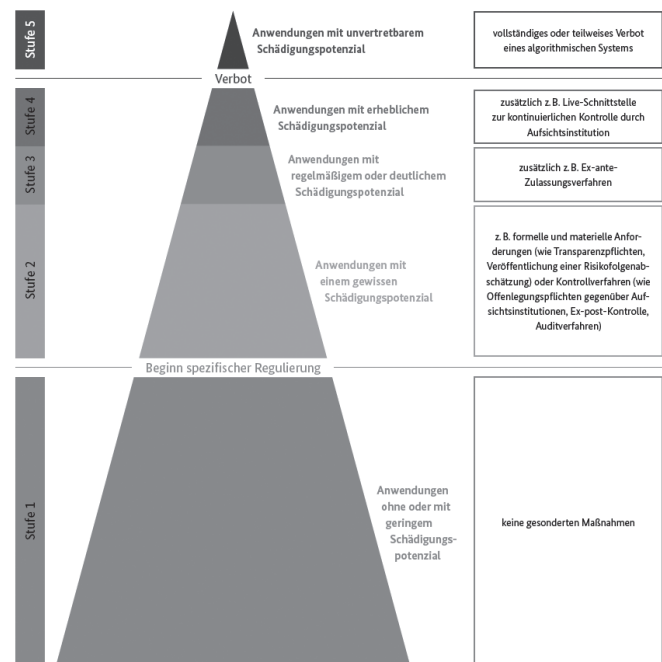


Abbildung 3: Kritikalität und risikoadaptiertes Regulierungssystem für algorithmische Systeme [6, S. 177]

Zudem sollten Betreiber ein festzulegendes Mindestmaß an technischen und mathematisch-prozeduralen Qualitätsgarantien gewährleisten (Empfehlung 51).

Ebenso sollten technisch-statistische Standards für die Qualität von Testverfahren und Audits definiert werden (Empfehlung 57).

Für die Kontrollaufgaben der sektoralen Aufsichtsbehörden empfiehlt die Datenethikkommission die Schaffung eines bundesweiten *Kompetenzzentrums Algorithmische Systeme* (Empfehlung 56).

Auch im Governance-Teil kommen wichtige informatikbezogene Forderungen vor: zur Kompetenz im digitalen Bereich, zur Technikentwicklung, zur Standardisierung und zur Forschung.

So empfiehlt die Datenethikkommission in der Ausbildung in Informatik, Softwareentwicklung und Data Science grundlegende Lehrveranstaltungen zu ethischen und rechtlichen Fragen sowie weiterführende Fortbildungen zu Statistik, Methodologie und Wissenschaftstheorie. Wer selbst digitale Produkte und Dienstleistungen entwickelt oder darüber entscheidet, soll ethische und rechtliche Gesichtspunkte frühzeitig einbeziehen [6, S. 72]. Es geht auch nicht nur darum, Spezialwissen zu vermitteln; stattdessen besteht ein Bedarf an umfassenderer Kommunikation an die Bevölkerung, wobei der Tech-Accountability-Journalismus eine wichtige Rolle spielen kann. Ähnliches gilt für berufliche und berufsbegleitende Weiterbildung.

Auf ethisch fundiertes Design in der Technologieentwicklung geht die Datenethikkommission gesondert ein. Dafür könnten neben Informationen zu Methoden und Katalogen Best-Practice-Konzepte, unterstützende Werkzeuge, Entwicklungs-Frameworks und (Open-Source-)Code-Komponenten hilfreich sein. Über Plattformen mit Repositorien für solche Komponenten sowie verwendbare Datenbestände, die gegebenenfalls Überprüfungen erst möglich machen, könnten die besonderen Eigenschaften herausgestellt, nötige Dokumentationen gleich mitgeliefert und Möglichkeiten zum Austausch von Erfahrungswissen bereitgestellt werden. [6, S. 74].

Die Datenethikkommission warnt davor, dass in der technischen Standardisierung gezielt Sicherheitslücken oder Hintertüren eingebracht werden könnten, um sich zukünftige Zugriffsmöglichkeiten zu verschaffen [6, S. 76].

Im Forschungsbereich sieht die Datenethikkommission ebenfalls Steuerungsmöglichkeiten, beispielsweise für eine übergreifende

und interdisziplinäre Zusammenarbeit oder für eine Entwicklungs- und Innovationsförderung mit dem Ziel, bessere Lösungen in die Praxis zu bringen [6, S. 75].

Nächste Schritte und Ausblick

Auftraggeberin des Gutachtens war die Bundesregierung. Nicht alle Empfehlungen der Datenethikkommission liegen jedoch im Zuständigkeitsbereich des Bundes. So könnten Empfehlungen auch für Gesetzgeber auf Ebene der Länder oder für die Europäische Kommission interessant sein.

Neben den regulativen Vorschlägen lassen sich aber auch ganz andere Möglichkeiten für jede und jeden im Bereich der Digitalisierung erkennen: in der Gestaltung von Informationstechnik, bei neuen Projekten oder Ideen, bei der Auswahl und Beschaffung von Technik, in der Konzipierung der Aus- und Fortbildung oder durch zivilgesellschaftliches Engagement.

Die Datenethikkommission wünscht sich einen konstruktiven Umgang mit ihren Empfehlungen. Eine englischsprachige Übersetzung eröffnet auch den internationalen Diskurs [8]. Notwendig sind nun Konkretisierungen. Die Datenethikkommission hat keinen Schlusspunkt gesetzt, sondern das Gutachten soll als Einladung zur weiteren politischen und gesellschaftlichen Debatte verstanden werden. Dabei werden auch Informatikerinnen und Informatiker ihre Beiträge leisten können – durch Umsetzungsvorschläge zu den Empfehlungen, durch Kritik und durch Weiterentwicklungen. Der Auftrag bestand darin, Vorschläge für einen Entwicklungsrahmen für Datenpolitik zu machen. Für konkrete Vorschläge ist es notwendig, dass Sachverstand der verschiedenen Disziplinen in die Gesetzgebung einfließt – und dies ist leider im Bereich der Digitalisierung noch keine Selbstverständlichkeit.

Dank

Es gibt Gremien, bei denen die Mitglieder froh sind, wenn Schluss ist. Viele Mitglieder der Datenethikkommission – auch ich – werden aufgetatmet haben, als die kräftezehrende Arbeit zu Ende ging. In ehrenamtlicher Aufgabe neben dem sonstigen Job, ohne ein Honorar, mit großem Engagement insbesondere der Co-Chairs Christiane Wendehorst und Christiane Woopen lässt sich der Takt, in dem die erarbeiteten Empfehlungen und noch ein Vielfaches an Punkte mehr diskutiert und dokumentiert wurden, bei dem uns ständig bewussten Erwartungsdruck nicht

Marit Hansen



Marit Hansen ist Informatikerin und wurde 2015 zur *Landesbeauftragten für Datenschutz Schleswig-Holstein* gewählt. Sie war Mitglied der *Datenethikkommission der Bundesregierung*.

für lange Zeit durchhalten. Außerordentlich positiv bewerte ich den Austausch untereinander mit der großen Bereitschaft, einander zuzuhören, die verschiedenen Perspektiven zusammenzubringen und zu gemeinsamen Ergebnissen zu kommen. Weder diese fruchtbringende Art der Kooperation noch das Resultat waren vorgezeichnet, als wir uns das erste Mal trafen. Deswegen danke ich den Mitgliedern der Datenethikkommission, von denen ich viel lernen durfte und die hoffentlich auch von meinen Beiträgen profitiert haben, und ich danke auch den Mitarbeiterinnen und Mitarbeitern der Bundesministerien, die für die Zusammensetzung verantwortlich waren.

Literatur

- [1] Ein neuer Aufbruch für Europa Eine neue Dynamik für Deutschland
Ein neuer Zusammenhalt für unser Land. Koalitionsvertrag zwischen
CDU, CSU und SPD. 19. Legislaturperiode, März 2018. <https://www.bundesregierung.de/resource/blob/975226/847984/5b8bc23590d4cb2892b31c987ad672b7/2018-03-14-koalitionsvertrag-data.pdf>

- [2] Bundesministerium des Innern, für Bau und Heimat/Bundesministerium der Justiz und für Verbraucherschutz: Leitfragen der Bundesregierung an die Datenethikkommission. 5. Juni 2018. https://datenethikkommission.de/wp-content/uploads/2019/10/DEK_Leitfragen.pdf
- [3] <https://datenethikkommission.de/terminubersicht/tagung1/>
- [4] <https://datenethikkommission.de/terminubersicht/tagung2/>
- [5] <https://datenethikkommission.de/terminubersicht/uebergabe-des-gutachtens/>
- [6] Gutachten der Datenethikkommission. Oktober 2019. https://datenethikkommission.de/wp-content/uploads/191128_DEK_Gutachten_bf_b.pdf
- [7] Kurzfassung des Gutachtens der Datenethikkommission. <https://datenethikkommission.de/gutachten/gutachten-der-dek-kurzfassung>
- [8] Opinion of the Data Ethics Commission. October 2019. https://datenethikkommission.de/wp-content/uploads/DEK_Gutachten_engl_bf_200121.pdf



Veronika Thiel

Viel Lärm um Wenig

Ethische Richtlinien in der Algorithmenentwicklung

Die Diskussion um den Einsatz von automatischen Entscheidungssystemen im gesellschaftlichen Bereich wie beispielsweise bei der Personalauswahl konzentriert sich oft auf eine Forderung nach mehr Ethik in der „KI“ – kurz, dass bei der Entwicklung und beim Einsatz von Algorithmen sichergestellt werden muss, dass Menschen vor Diskriminierung geschützt sind und ihre Privatsphäre geschützt wird. Dabei wird oft so getan, als ob die Softwareindustrie hier völlig unvorbereitet getroffen wurde und sich im Vorfeld mancher unbeabsichtigter Konsequenzen nicht bewusst gewesen sein könnte. Diskussionen um ethisches und sozial verträgliches Verhalten von Firmen gibt es jedoch schon lange, und es ist nicht glaubhaft, dass Tech-Firmen noch nie etwas von Corporate Social Responsibility (CSR) gehört haben. Indem man aber so tut, als würde hier etwas Neues, noch nie Dagewesenes diskutiert, entlässt man Firmen aus der Verantwortung, sich die potenziellen positiven sowie negativen Konsequenzen ihres Verhaltens bewusst zu machen. Zudem zeigt sich – wie auch oft bei anderen Nachhaltigkeitsinitiativen von Firmen – dass hier viel geredet, aber wenig in die Praxis umgesetzt wird.

Im Mai 2019 begann ich für die Organisation *AlgorithmWatch* mit der systematischen Suche nach Richtlinien zur ethischen Entwicklung von Softwareprodukten. Bis Oktober 2019 fanden sich 109 Beispiele von 95 Akteuren aus der Industrie, von gemeinnützigen und internationalen Organisationen wie Amnesty International und der OECD sowie von Universitäts- und Regierungsinitiativen.¹

Ethisches oder sozial verantwortliches Handeln von Firmen ist immer der Kritik ausgesetzt, dass viel geredet und wenig umgesetzt wird. Deshalb konzentrierte sich die Suche von Anfang an darauf, Initiativen zu finden, die eine klare Anweisung zur Umsetzbarkeit haben: Wenn eine Firma sich selbst zu ethischem Handeln verpflichtet, muss deutlich werden, wie die Einhaltung dieser Selbstverpflichtung gewährleistet ist, welche Aufsichtsmechanismen es gibt und welche Konsequenzen aus der Nichteinhaltung entstehen.

Bei der Sammlung und Sortierung war somit zwischen Akteuren zu unterscheiden, die sich selbst oder anderen Handlungsvorgaben machen können, und solchen, die ein bestimmtes Verhalten fordern, jedoch keine Autorität haben, es durchzusetzen (zum Beispiel in Form der Suspendierung einer Mitgliedschaft, Lizenz

oder Ähnliches). Viele der ethischen KI-Initiativen kommen von letzteren Organisationen. Beispielsweise ist die Erklärung der Internationalen Konferenz der DatenschützerInnen (*International Conference of Data Protection and Privacy Commissioners*) ein wichtiges Dokument, um die Sicht von Datenschutzorganisationen darzustellen, aber sie hat keine Möglichkeit, Firmen dazu zu verpflichten, sich an die Forderungen zu halten.

Auf der anderen Seite gibt es Beispiele von Industrieverbänden wie *IEEE* oder auch der *Partnership for AI*, von denen erwartet werden kann, dass hier für Mitglieder ein bindender Charakter der Erklärung vorliegt – Mitgliedschaft verpflichtet schließlich. Besonders *IEEE* ist als mächtiger globaler Berufsverband bekannt dafür, Standards zu entwickeln, an die sich Mitglieder halten sollen – somit sollte auch die Initiative *Ethics by Design* für die Mitglieder verpflichtend sein.

Allgemein gesprochen kann man also von Firmen und Berufs- und Industrieverbänden sowie Mitgliedsorganisationen erwarten, dass ihre Initiativen zur Einhaltung verpflichten. Auch Regierungen könnten Unternehmen vorgeben, dass sie sich an bestimmte ethische Regeln halten müssen, um ihre Software an die Regierung verkaufen zu können. Bei der Recherche habe ich

95 Akteure gefunden, von denen 54 in der Lage sein könnten, verpflichtende Vorgaben zu machen (vgl. Tabelle 1).

Sektor ²	Anzahl
Zivilgesellschaft	25
Privatunternehmen	24
Regierung	18
Universität	9
Industrieverband	7
Berufsverband	5
Anderes	4
Internationale Organisation	3

Tabelle 1: Vorläufige Ergebnisse – Akteure (Oktober 2019)

Nicht alle Einträge dieser 54 Akteure sind jedoch verpflichtend. So war außer dem Eintrag des Finanzministeriums von Kanada, das sich selbst zum Einsatz von ethischer Software verpflichtet, kein Regierungseintrag mehr als nur ein Vorschlag zum ethischen Design von Algorithmen.

Die Art der Einträge ist sehr unterschiedlich und entzieht sich einer klaren Kategorisierung. Die Einträge konnten als (Selbst-) Verpflichtung, Prinzipien und Richtlinien beschrieben werden oder waren so betitelt. Aber es gibt auch Empfehlungen, Erklärungen, *White Papers*, ein *Framework*, eine Direktive, eine Berücksichtigung (*consideration*) und drei Eide. Bei der Analyse wurden diese Kategorien nicht unterschiedlich gewichtet. Es ging nur darum, welche Form von Bezeichnung einen Überwachungs- bzw. Umsetzungsmechanismus nach sich ziehen könnte. Hierunter fielen Selbstverpflichtungen sowie Schwüre. Es kann angenommen werden, dass sie einen bindenden Charakter haben, im Gegensatz zu Prinzipien oder Richtlinien, die eher Absichtserklärungen darstellen.

Die Unterteilung dient vor allem dazu, Privatfirmen nicht in die Pflicht zu nehmen, wenn von vornherein klar ist, dass eine Veröffentlichung zum Thema Ethik und KI lediglich eine Stellungnahme darstellt und keine Intention, die Firma zu einer bestimmten Handlungsweise zu verpflichten. So hat die Forschungsabteilung von Google beispielsweise Informationen über KI und Ethik für die Entwicklung von Software herausgegeben, die ethische Prinzipien beschreiben, aber es gibt keine Aufforderung, sich an diese zu halten.³

Bei 12 Einträgen ist unbekannt, ob sie verbindlich sind oder nicht. Diese Einträge sind hauptsächlich von Privatfirmen oder Industrieverbänden. Das Statement der *Association for Computing Machinery* (ACM) zu algorithmischer Transparenz und Rechenschaft beispielsweise deutet darauf hin, dass der Verband verbindliche Standards setzt, an die sich seine Mitglieder halten sollten. Jedoch konnte auch hier kein öffentlich zugänglicher Hinweis auf diese Mechanismen gefunden werden – somit ist unbekannt, ob dieses Statement innerhalb der Organisation den gleichen Stellenwert einnimmt wie ein von ihr geschaffener Industriestandard.

Es wird deutlich, dass hier Unschärfen vorhanden sind und eine weitere Diskussion vonnöten ist, um herauszuarbeiten, inwiefern solche Initiativen eine Handlungsanweisung für Firmen darstellen

und somit auch Informationen vorhanden sein sollen, wie eine Firma gedenkt, diese Anweisungen in die Praxis umzusetzen.

In der noch zu veröffentlichenden Datenbank waren im Oktober 32 Einträge von 30 Akteuren vorhanden⁴, die nach dieser Definition eine Form von Umsetzungsmechanismus haben sollten. Von diesen 32 Beispielen gab es nur drei, bei denen solch ein Mechanismus offensichtlich war. Bei weiteren vier wurden Aufsichtsstrukturen erwähnt – jedoch blieb die Autorität dieser Aufsicht unklar. Somit haben lediglich sieben der 32 Einträge (22 %) einen (mindestens teilweisen) Mechanismus und nur 6 % der gesamten 109 Einträge.

Monitoring/process of certification evident?	Anzahl	Prozent
No	25	78 %
Partially	4	13 %
Yes	3	9 %
Gesamt	32	100 %

Tabelle 2: Vorläufige Ergebnisse – Umsetzungsmechanismus (Oktober 2019)

Was bedeutet diese Analyse nun?

Die hohe Anzahl der Einträge aus dem zivilgesellschaftlichen Bereich zeigt, dass Ethik und KI als ein wichtiges Thema angesehen wird. Der Privatsektor ist sich der Wichtigkeit des Themas ebenfalls bewusst – zumindest auf dem Papier. Aber dadurch, dass nur eine Handvoll von Initiativen überhaupt Überwachungsmechanismen aufzeigt, liegt der Verdacht nahe, dass hier nur leere Worte produziert werden. Es ist ein Leichtes für Firmen, einige Schlagwörter zum Thema auf- oder auch nur abzuschreiben und sie auf ihrer Website zu veröffentlichen. Rechtliche Konsequenzen ergeben sich hieraus keine. Deshalb ist es wichtig, bei Selbstverpflichtungen nach Hinweisen darauf zu suchen, dass sich Firmen daran halten – die Praxis sieht momentan anders aus. Die vielen Skandale in Bezug auf Datenschutz, Diskriminierung bei Gesichtserkennung und Berichte, dass *Alexa* und *Siri* ihre Nutzer 'ausspionieren' sind tatsächlich der beste Hinweis darauf, dass Firmen nur selten *Ethics by Design* anwenden. Apple hat den Datenschutz bei *Siri* verbessert, jedoch nur nach einem öffentlichen Aufschrei. Es stellte sich heraus, dass Angestellte bei Apple Suchanfragen von NutzerInnen abhörten und auswerteten. Dies war kein Versehen, sondern bewusst als Form von Qualitätskontrolle eingebaut. Es wurde irgendwo in den Nutzungsbedingungen erwähnt, aber es war keine explizite Zustimmung der NutzerInnen notwendig – das heißt, deren Privatsphäre wurde hintangestellt. Apple beendete den Lauschangriff erst, nachdem eine Sammelklage drohte. Apple ist Mitglied der *Partnership on AI*, die in ihren Statuten ausdrücklich erwähnt, dass die Partner dazu verpflichtet sind, auf den Schutz der Privatsphäre und der Sicherheit von Personen hinzuwirken – die Firma fühlte sich offenbar nicht bemüht, ihr Verhalten diesen Statuten anzupassen.⁵

Firmen scheinen sich also ein wenig dem öffentlichen Druck zu beugen, indem sie ein paar Worte auf eine Webseite schreiben, und sie können immer darauf verweisen, dass sie noch an der Umsetzung arbeiten. Dieses Argument gilt aber nur, wenn man

behauptet, dass Ethik in der KI etwas Neues sei und Firmen einfach nur aufholen müssten.

Ethisches Verhalten von Firmen ist aber schon lange ein Thema: Viele der ethischen Prinzipien, die in der Softwareentwicklung diskutiert werden, sind keinesfalls neu. *Corporate Social Responsibility (CSR)* fordert schon längst von Firmen, nicht zu diskriminieren, die Privatsphäre zu schützen und ganz allgemein Gesetze nicht nur nach den Buchstaben zu befolgen, sondern auch nach dem Sinn. Seit 1999 gibt es den *UN Global Compact* und es ist nicht vorstellbar, dass dessen Existenz der Softwareindustrie entgangen ist. Immerhin war Googles Firmenmotto der einst *Don't be evil* und dieser Satz findet sich immer noch im Verhaltenskodex der Firma wieder.

Warum dann gibt es so wenige ethische KI-Initiativen, die in der Praxis umgesetzt werden? Die kurze Antwort ist: Profite stehen noch immer weit über Ethik. Damit soll nicht impliziert werden, dass alle Tech-Firmen böse sind. Im Gegenteil, viele verfolgen das Ziel, Algorithmen zu entwickeln, die Diskriminierung reduzieren sollen (wie zum Beispiel die Firma *Applied*). Viele preschen dabei aber unüberlegt vor, um sich Geld von Investoren zu sichern. Dabei übersehen sie ethische Fragen oder versäumen, die wissenschaftlichen Grundlagen, die ihren Algorithmen zugrunde liegen zu überprüfen – vieles hält kritischen Nachfragen nicht stand.

Die gleichen Postulate, die sich CSR in den Weg stellen, treffen auch auf Softwareunternehmen zu: nämlich, dass Firmen gegenüber ihren Investoren eine Pflicht hätten, profitabel zu sein. Dies ist keine rechtliche Verpflichtung, jedoch ist sie immer noch für viele (und aus guten Gründen) ein überragendes Handlungsmotiv. Solange Investoren schnellen Profit fordern, werden ethische Prinzipien immer Gefahr laufen, hintangestellt zu werden. EntwicklerInnen und Start-ups können die besten Vorsätze haben, jedoch sind sie dem gleichen Druck unterworfen wie Mode- und Elektrofirmen. Öffentlicher Druck hat viel dazu beigetragen, die Arbeitsbedingungen von Angestellten zu verbessern – aber wäre es nicht besser, solche Bedingungen von vornherein zu schaffen, statt Probleme später zu lösen, nachdem Menschen Schaden genommen haben?

Softwarefirmen können sich mit Risikofolgenabschätzungen und anderen Werkzeugen vertraut machen und somit Ethik in ihre Algorithmen von der Konzeption bis zur Umsetzung einfließen lassen.

Das heißt, dass man bei der Entwicklung von Software, die Entscheidungen über Menschen trifft, die deren Leben beeinflussen können, von agilen Managementmethoden Abstand nehmen muss. Bei einer Software, die vorhersagen soll, welcher Mensch zu einer Haftstrafe oder zur Bewährung verurteilt werden soll, darf es keine Beta-Version geben. Diskriminierung (wie im Fall des *Compas*-Algorithmus in den USA) muss ausgeschlossen sein – und eventuell sollte es solche Software überhaupt nicht geben.

Die Schaffung eines *Ethics-Inside-Siegels* wird in diesen Bereichen unabdingbar werden, und es ist auch eine Regulierung analog zur Medizinproduktregulierung vorstellbar. Wo das Leben von Menschen durch Softwareentscheidungen stark beeinflusst werden kann, muss ein stringenter Prozess durchlaufen werden, der Risiken minimiert und Positives maximiert.

Was jetzt zu beobachten ist, aber nicht länger geschehen sollte, ist so zu tun, als ob eine ethische Geschäftspraxis in der Softwareindustrie etwas völlig Neues und Anderes sei und Firmen völlig unvorbereitet träge. Damit würden wir Firmen aus der Verantwortung lassen, ihr Verhalten an Prinzipien sozialer Gerechtigkeit auszurichten.

Algorithmen können eine positive Rolle in unser aller Leben spielen, jedoch nur, wenn wir jetzt umdenken und Profit nicht mehr an die erste Stelle stellen. Noch können wir die Weichen stellen. Nutzen wir diese Gelegenheit.

Anmerkungen

- 1 Dies sind vorläufige Zahlen, eine Überarbeitung und Neuauflage des Inventars ist für Februar 2020 geplant. Eine bisherige Sammlung der Einträge bis Juni 2019 ist hier zu finden: <https://algorithmwatch.org/en/project/ai-ethics-guidelines-global-inventory/>
- 2 Industrieverbände sind Organisationen wie der Bundesverband für KI oder die Association for Computing Machinery. Berufsverbände sind Fachverbände wie die Gesellschaft für Informatik und IEEE. Die OECD, die G20 und die UNESCO sind als internationale Organisationen kategorisiert. In der Kategorie Privatunternehmen sind sowohl Einzelfirmen wie Apple als auch Industriepartnerschaften wie die Partnership on AI vertreten. Bei Zivilgesellschaft sind Einträge der Verbraucherzentrale oder auch von Amnesty International vertreten. Beispiele der Kategorie



Veronika Thiel

Veronika Thiel hat 14 Jahre Erfahrung in der Gesundheits- und Sozialpolitik in Großbritannien gesammelt, querte durch Mikrofinanz, faire Bankensysteme, Armutsbekämpfung, Integrierte Pflege und Öffentliche Gesundheit. Besonders in den letzten fünf Jahren hat sie sich verstärkt mit dem Einsatz von Big Data und Algorithmen im Gesundheitsbereich beschäftigt. Veronika ist überzeugt, dass Algorithmen, gerade im Gesundheitsbereich, das Leben vieler Menschen verbessern können, jedoch ist hier große Umsicht und Transparenz bei der Entwicklung und dem Einsatz geboten. Ihr besonderes Interesse liegt deshalb auf nicht-intendierten Konsequenzen von algorithmischen Entscheidungen, die Ungleichheiten verfestigen oder sogar noch verstärken können. Ein Augenmerk gilt dabei auch der Entwicklung eines Berufsethos bzw. ethischer Prinzipien für die Algorithmenentwicklung, die für eine gerechte „KI“ unabdingbar sind.

Regierung kommen sowohl von Nationalstaaten (z. B. Kanada, UK) als auch von der EU. In Anderes fällt die Chinesische AI Alliance, die aus Vertretern von Industrie und chinesischen Universitäten besteht, und die von einer halbstaatlichen Regierungsorganisation ins Leben gerufen wurde. Ebenso findet sich hier die Hambacher Erklärung, unterzeichnet von den Datenschutzaufsichtsbehörden des Bundes und der Länder. Die zwei weiteren Einträge in dieser Kategorie stammen von industrie-eigenen Forschungsinstituten, dem Institute for Business Ethics und

dem Handelsblatt Forschungsinstitut.

3 Vgl. <https://pair.withgoogle.com>

4 Microsoft und Sage hatten je zwei Einträge

5 Tenet 6a: „We will work to maximize the benefits and address the potential challenges of AI technologies, by: Working to protect the privacy and security of individuals. (...)“, <https://www.partnershiponai.org/tenets> (Stand: 19. Januar 2020)



Alexander von Gernler

Geschlossene Gesellschaft

Von der Verantwortung der Informatikerinnen und Informatiker

Informatikerinnen und Informatiker befinden sich heute in der glücklichen Situation, sich die gut bezahlten Jobs aussuchen zu können. Trends wie die zunehmende Digitalisierung, der Hype um Künstliche Intelligenz sowie die Alterspyramide der deutschen Gesellschaft werden dafür sorgen, dass dies auch noch lange so bleibt. Trotzdem sollten sie aus guten Gründen nicht übermütig werden. Ihre Pflicht und Verantwortung gegenüber der Gesellschaft bleibt es vielmehr, ihren Mitmenschen die neuen Technologien zu erklären, die einen massiven Wandel ausgelöst haben. Dabei ist es nicht so, dass die Informatikerinnen und Informatiker bisher eine gute Figur abgegeben haben: Viele Probleme wie die Sicherheit von Hardware, Software und Plattformen warten immer noch auf ihre Lösung.

Technikfolgenabschätzung

Beginnen wir bei der Technikfolgenabschätzung: Es gab in der Geschichte der Menschheit viele vermeintlich gute Ideen, die sich nachher als Irrweg oder fataler Fehler herausgestellt haben. So hat etwa die Erfindung von FCKW Anfang der 1960er Jahre anfangs wie ein echter Durchbruch gewirkt: Diese neuen Gase waren sehr beständig, unbrennbar, geruchlos, durchsichtig, nahezu ungiftig, und vor allem leicht verflüssigbar. Dadurch eigneten sie sich ideal für die Anwendung als Kältemittel oder aber als Treibgas in Spraydosen, das nicht mit dem Wirkstoff der Dosen reagiert. Erst mehrere Jahrzehnte später stellte sich die fatale Nebenwirkung der FCKW heraus, nämlich die Verursachung des Ozonlochs in der Erdatmosphäre. Dieser Zusammenhang mag heute eine Binsenweisheit sein, damals aber wurde er erst nicht wahrgenommen, dann geleugnet, dann bekämpft.

Daraus ist ersichtlich, dass für eine Technikfolgenabschätzung (TA) die Expertinnen und Experten der ersten Stunde eher ungeeignet sind, denn diese sind meistens hoch euphorisch in Bezug auf ihre Technik, und haben meistens auch noch Aktien in der Angelegenheit. Besser ist es, die Fachleute der zweiten Stunde heranzuziehen, die das neue Thema mit ausreichend Distanz und ohne persönliche Involvierung betrachten können. Daraus folgt aber auch, dass eine TA oft erst nach der breiten Einführung einer neuen Technologie erfolgen kann – mit allen zu erwartenden Schäden.

Ein besonders prominentes Beispiel von TA ist in der Physik anzutreffen. Diese Profession wurde mit der Erfindung der Atom-bombe in teils heftigste Gewissenskonflikte gestürzt. Aus der deutschen Diskussion um die Beschaffung taktischer Nuklear-waffen, angestoßen durch den damaligen Bundeskanzler Konrad Adenauer, formten sich beispielsweise die *Göttinger Achtzehn*, ein Zusammenschluss aus 18 renommierten Physikern dieser Zeit. Friedrich Dürrenmatt porträtierte das Dilemma einige Jahre

später in seinem Werk *Die Physiker*. Aus den Göttinger Achtzehn ging in Folge die *Vereinigung Deutscher Wissenschaftler* hervor, die sich bis heute um Technikfolgenabschätzung in der Bundesrepublik verdient macht.

Es gab auch in der jüngeren Vergangenheit eine Berufsgruppe gefragter Fachleute, die hohe Gehälter kassierten und komplexe Produkte bauten, die die Außenwelt nicht mehr verstand.

Ihnen war das egal, denn sie hatten ihre komfortable Subkultur mit ihrem eigenen Spezialjargon. Sie lösten eine Menge Probleme, die für sie in ihrer kleinen Welt bedeutend waren, hatten aber das Ganze aus dem Blick verloren. So veränderten sie die Gesellschaft global und in massiver Art und Weise, und stürzten am Schluss sogar viele ihrer Mitmenschen in prekäre Verhältnisse. Die Rede ist, sehr generalisierend, von einer Gruppe von Bankern, die mit der Finanz- und der Immobilienkrise nicht nur für enorme gesellschaftliche Verwerfungen gesorgt haben, sondern auch den aufrichtigen und wohlmeinenden Rest ihres Berufsstands mit einem gesellschaftlichen Stigma versehen haben, das heute noch nicht ganz wieder abgeschüttelt ist. Sehr plastisch sind noch Bilder von Demonstrationen an der Wall Street in Erinnerung, die unter anderem auch die sehr explizite wie unangenehme Aufforderung *Jump, you fuckers!* auf den Schildern trugen.

Zurück zur Informatik

Expertinnen und Experten für Künstliche Intelligenz (KI) werden von den großen Internetkonzernen für sechsstelligen Einstiegsgehalt eingekauft. Jahreseinkommen über 200.000 Dollar sind realistisch erreichbar. Im Silicon Valley und andernorts kaufen sich die technikoptimistischen Individuen von ihrem Einkommen schicke Eigenheime, freuen sich ihres Daseins und gentrifizieren nebenbei ganze, vorher bezahlbare Wohngegenden. Außer ihnen versteht niemand, wie KI funktioniert, und ganz genau

wissen sie es eigentlich auch nicht – KI funktioniert eben, gute Daten vorausgesetzt. Auch Informatik-nahe Startups kümmern sich heute um die bedeutenden Fragen in ihrem Mikrokosmos, etwa um Smartphone-basierte Aufsmeldienste für Hundehaufen. Dass 20 Prozent der Weltbevölkerung nicht nur kein Internet, sondern auch oft noch keine zuverlässige Stromversorgung oder sauberes Trinkwasser haben, spielt bei der Selbstverliebtheit ihrer Lösungen keine Rolle.

Bis jetzt läuft auch noch alles sehr gut für die Informatikerinnen und Informatiker – die Jobs sind sicher und das Einkommen üppig. Ich möchte mir nicht vorstellen, wie in unserem Falle der große Knall aussehen würde. Auch hier würde ein kleiner Teil der Berufsgruppe dem Ansehen aller irreversiblen Schaden zufügen – das gilt es unbedingt zu verhindern! Es gibt einige wichtige Herausforderungen, die innerhalb der Verantwortung unserer Profession liegen, und die tunlichst adressiert werden sollten, bevor die Probleme so dringlich werden, dass man uns dazu zwingt:

Erstens der Energieverbrauch von IT-Anwendungen: Nur weil Computer nicht rauchen, stinken und knattern, verbrauchen sie in Form von Strom doch eine Menge Energie. Ein Computer sieht im Vergleich zu einem Schiffsdiesel natürlich immer sauber aus, aber gerade Anwendungen wie das Schürfen von Bitcoins oder das Training neuronaler Netze im Rahmen von KI sind enorm energieintensiv.

Zweitens der Ressourcenverbrauch durch die Produktion von immer neuer und immer mehr Hardware: Die kurzen Lebenszyklen von Smartphones, die proprietären Standards bei Steckern und Schnittstellen sowie der Umsatzzwang der Hersteller führen zu einem stetig ansteigenden Verbrauch wertvoller Rohstoffe. Hier sind nicht nur die so genannten seltenen Erden gemeint, sondern auch der Rohstoff Sand, der nämlich – paradoxerweise – trotz Ausbreitung von Wüsten sowohl für die Betonherstellung als auch für die Produktion von Silizium-Wafern knapp wird. Sand ist offenbar nicht gleich Sand.

Drittens die sozialen Umwälzungen, die durch die Digitalisierung verursacht werden: Ob es ein gesellschaftlich wünschenswerter Fortschritt ist, dass es nun Jobs wie Uber-Fahrer, Amazon-Paketbote oder Suchmaschinenoptimierer gibt, bleibt zu bezweifeln. überhaupt ist es bedenklich, dass brillante Talente, Kolleginnen und Kollegen meines Berufsstands, sich die hohe Kunst der Informatik aneignen, nur um danach Werbung möglichst effektiv, zielgruppengerecht und sublim an ihre Mitmenschen zu bringen. War es das wert?

Viertens das durch die Digitalisierung sich stetig verändernde Menschenbild: War früher noch wichtig, wie eine Person sich persönlich äußert, und welches Verhalten sie im echten Leben zeigt, so beobachten wir eine Verschiebung hin zu einer hohen Relevanz der so genannten digitalen Persona, also dem modellhaften und damit unvollständigen digitalen Abbild eines Menschen. Anhand der digitalen Persona werden Algorithmen aber über die Vergabe von Krediten, die Zusendung von Angeboten, die beruflichen Aufstiegsmöglichkeiten und vieles mehr entscheiden. Es ist an der zunehmenden Selbstoptimierung und Datenerfassung des Einzelnen zu beobachten, dass hier das mechanistische und utilitaristische Menschenbild eines Silicon-Valley-Technikoptimismus immer weiter auf dem Vormarsch ist. Eine Antwort aus dem ganzheitlichen Gedanken des Humanismus ist hier überfällig, denn ein Mensch ist eben mehr als eine Körpermaschine mit einem neuronalen Netz im Schädel.

Fünftens, und für langjährige Beobachter wahrlich keine Überraschung, die globale digitale Überwachung, verbunden mit den automatisch einhergehenden *Chilling Effects*. Damit ist gemeint, dass sich beobachtet fühlende Personen bestimmtes Verhalten unterdrücken, von dem sie annehmen, es sei sozial nicht erwünscht oder bereite ihnen auf anderem Weg Probleme. Ein bekanntes Beispiel ist, dass die Suche nach Begriffen wie Bombe auf Wikipedia nach den Anschlägen vom 11. September 2001 prozentual gesehen rapide abgenommen hat. Die globale Überwachung, aufgedeckt durch Snowden im Jahre 2013, ist seitdem unverändert unterwegs, auch wenn sie aus der öffentlichen Berichterstattung weitgehend wieder verschwunden ist.

Sechstens die Abwesenheit von sicherer Hardware, sicherer Software und sicheren Web-Plattformen: Es gibt heute keine sichere Computer-Hardware mehr, die gleichzeitig im Massenmarkt der PCs, Notebooks, Server, Smartphones oder Tablets erhältlich wäre. Auf den verschiedenen Systemen lauern nicht einsehbare Komponenten wie die Intel Management Engine (ME), denen blind vertraut werden muss. Ähnlich schlimm verhält es sich auf der Software-Seite: Heutige Software ist von einer solchen Komplexität, dass das OpenSource-Versprechen der öffentlichen Kontrolle an seine Grenzen gerät. Anders sind zumindest gravierende Sicherheitslücken, wie sie in der Vergangenheit in der Softwarebibliothek OpenSSL für jede interessierte Person im Quellcode auffindbar gewesen wären, nicht zu deuten. Die Plattform-Ökonomie ist noch ein ganz anderes Problem. Auf den heutigen kostenlosen Plattformen sind die Benutzerinnen und Benutzer nicht der Kundinnen und Kunden, sondern die Ware. Auf echten Datenschutz brauchen sie von solchen Plattformen bei den derzeit angewendeten Geschäftsmodellen nicht zu hoffen.



Alexander von Gernler

Alexander von Gernler ist Vizepräsident der *Gesellschaft für Informatik e. V. (GI)* und beruflich als Leiter der Forschung bei der *genua GmbH* tätig. Vorher war er Technischer Botschafter, Scrum Master und Firewall-Entwickler ebenda sowie ehemaliger Committer im OpenBSD-Projekt (2005-2010). Persönlich ist er an Datenschutz, IT-Sicherheit, Privatsphäre und Ethik interessiert. Er hat 2005 sein Diplom in Informatik an der Friedrich-Alexander-Universität Erlangen erhalten.

Die Profession der Informatik ist nunmehr in der Pflicht, der Bevölkerung die neuerlichen Entwicklungen verständlich zu erklären und dadurch einen gesellschaftlich fruchtbaren Diskurs zu ermöglichen, wo wir miteinander mit diesen neuen Technologien hin wollen. Das Primat der Politik bzw. der Gesellschaft ist entscheidend. Und wir müssen an das Problem heran, dass die (vor allem US-dominierte) Wirtschaft mit Riesenschritten davon zieht, und selbst Universitäten gegenüber den mächtigen Konzernen ihre Deutungshoheit über das Fach verloren haben, etwa im Falle von Google: Was dieser Konzern anpackt, wird de facto Standard – auch und gerade im Falle von KI.

Ethische Leitlinien

Neben einer nötigen gesetzlichen Einhegung der Phänomene ist aber genauso jede und jeder Einzelne in der Pflicht, ethisch überlegt zu handeln. Helfen können dabei etwa die 2018 neu aufgelegten ethischen Leitlinien der Gesellschaft für Informatik, an deren Ausarbeitung ebenfalls mehrere Mitglieder des FIF beteiligt waren.

Das neue Dokument stützt sich in seinen Wurzeln auf bedeutende Werke wie das deutsche Grundgesetz und die Charta der Grundrechte der Europäischen Union.

Ethische Leitlinien können sehr hilfreich sein, sie müssen aber gelebt und in einen gesellschaftlichen Diskurs eingebettet werden, und die Informatikerinnen und Informatiker sollten sich mit ihnen dauerhaft, auch kritisch, auseinandersetzen. Ich persönlich finde auch, dass jede Absolventin und jeder Absolvent der Informatik oder eines verwandten Studiengangs heute beim Studienabschluss nicht nur eine Urkunde als Bachelor, Master oder Doktor der Datenwissenschaft erhalten sollte – in der Mappe mit dem Diplom sollte eine Ausgabe der ethischen Leitlinien beigelegt sein. Andere Professionen machen so etwas traditionell schon seit Jahrhunderten: So gibt es für Bauingenieurinnen und -ingenieure den Ring, der ihnen später die Hand führen soll, es gibt den hippokratischen Eid in der Medizin, warum nicht also auch eine ähnliche Selbstverpflichtung in unserer Zukunft?



Christoph Marischka und Dominik Wetzel

Die Produktionsbedingungen Künstlicher Intelligenz

Unter dem verheißungsvollen Titel Cyber Valley entsteht in Tübingen wie an vielen anderen Stellen in Deutschland und der Welt aktuell ein Forschungscampus für die Entwicklung Künstlicher Intelligenz. In der überschaubaren schwäbischen Universitätsstadt wurden jedoch früh Auswirkungen auf den Wohnungsmarkt, die öffentliche Infrastruktur und die Wissenschaftskultur befürchtet und diskutiert. Die hieraus hervorgegangenen, teilweise heftigen Auseinandersetzungen ermöglichen es, am Cyber Valley den Produktionskontext Künstlicher Intelligenz beispielhaft herauszuarbeiten.

Blaupausen der KI-Forschung

Obwohl die Selbstdarstellungen des Cyber Valley von Superlativen geprägt sind, ist es keineswegs einzigartig. Zwar wird auf der Homepage des Projekts¹ selbstbewusst von „einem neuen Modell der Zusammenarbeit zwischen Wissenschaft und Wirtschaft“ gesprochen, welches „ein befruchtendes Ökosystem für den Technologietransfer“ schaffen soll, indem es „durch eine enge Verzahnung von Wissenschaft und Wirtschaft die ideale Umgebung zur Förderung von Start-ups“ bietet. Tatsächlich existieren hierfür jedoch ziemlich konkrete Blaupausen von Beratungsunternehmen wie Roland Berger, die zugleich wesentlich daran beteiligt sind, jenen diskursiven Rahmen zu setzen, unter dem die Umsetzung dieser Blaupausen politisch vorangetrieben wird. Dieser Rahmen besteht im Wesentlichen aus drei Setzungen: Im Bereich der KI werden erstens in naher Zukunft disruptive Innovationen erwartet, die sowohl geopolitische als auch dramatische wirtschaftliche Folgen haben werden für diejenigen, die sie nicht zuerst entdecken oder umsetzen. Als zentrale und notwendige Akteure bei dieser Entwicklung gelten zweitens Start-ups, die es deshalb drittens durch die Schaffung räumlich, inhaltlich und institutionell verdichteter Ökosysteme politisch zu fördern gelte. Was in den Papieren der Beratungsunternehmen teilweise recht deutlich angesprochen wird, fällt bei ihrer Reproduktion durch politische, wissenschaftliche und journalistische Eliten – und die, die ihnen allerorten nachplappern – gerne unter den Tisch: Dass die Förderung von Start-ups vor allem auch be-

deutet, optimale Bedingungen für Risikokapital zu schaffen. Ein Ökosystem für die Entwicklung Künstlicher Intelligenz ist in erster Linie ein Erlebnispark für Risikokapital.

Die entsprechenden Bedingungen formuliert das Unternehmen Roland Berger beispielsweise in seiner Broschüre zum Start-up-Hub Wien aus dem Jahre 2016 recht konkret.² Fünf Handlungsempfehlungen werden dabei in den Mittelpunkt gestellt. So gelte es

1. „Großunternehmen stärker [zu] aktivieren“,
2. einen „zentralen Startup-Campus [zu] errichten“,
3. ein „neues politisches Mindset [zu] schaffen“,
4. „[j]unge Wissenschaftler zum Gründen [zu] bewegen“ und
5. „unproduktives Kapital zu mobilisieren“.

Zur Mobilisierung unproduktiven Kapitals werden weitere Forderungen erhoben, die räumlich wie inhaltlich weit über die KI-Forschung und einen konkreten Campus hinausgehen. So sollten etwa „100 Prozent der investierten Summe ... von der Einkommensteuer absetzbar“ und „Kapitalerträge, die aus Investment erwirtschaftet werden, zu 50 Prozent steuerfrei sein“. An anderen Stellen werden auch Forderungen erhoben und entsprechendes Lobbying betrieben, Renten- und Gesundheitskassen zu drängen oder gar gesetzlich zu verpflichten, ihre Rücklagen als Risikokapital anzulegen, um so die bevorstehenden Disruptionen zu erreichen bzw. zu meistern.

In einer anderen Studie von Roland Berger³ wird die – methodisch zweifelhaft – erfasste Zahl von Start-ups im Bereich der KI zum alleinigen Indikator des jeweiligen Entwicklungsstandes verschiedener Länder und Regionen gemacht und hiermit der Nachholbedarf in Europa sowie die Notwendigkeit einer „Strategie für europäische [KI-]Start-ups“ abgeleitet. Im Hinblick auf die Strategien der erfolgreicherer Mitbewerber werden die spezifischen Vorteile benannt, welche die entsprechenden KI-Ökosysteme der Start-up-Kultur böten: In China und Israel ermögliche eine enge Zusammenarbeit zwischen Sicherheitsbehörden, Wissenschaft und Wirtschaft den Start-ups Zugang zu den dringend benötigten Datenmengen und öffentlichen Geldern als Anschubfinanzierung. Zu Israel findet sich der bemerkenswerte Satz: „Die Regierung plant darüber hinaus, 275 Mio. US\$ in die Digitalisierung des Gesundheitswesens zu investieren, um KI-Projekte voranzubringen“. Zumindest aus der Sicht der Wirtschaftsberatung dient die Digitalisierung der Gesundheit also nicht in erster Linie der Gesundheit, sondern der Industrieförderung.

Das Paradigma der ML-Entwicklung

Sowohl im globalen Diskurs der Beratungsunternehmen als auch der lokalen Diskussion um das Cyber Valley lässt sich ein Paradigma für die Forschung an bzw. die Entwicklung von Anwendungen des Maschinellen Lernens (ML) erkennen. Zunächst ist festzustellen, dass es sich um ein hochgradig experimentelles, aber nicht wirklich wissenschaftliches Paradigma handelt. So wird erwartet, dass sich die disruptiven Innovationen quasi von selbst ergäben, wenn verschiedene kritische Massen auf eine entsprechende Infrastruktur und politische Regulation (das Ökosystem) treffen. Um welche Form von Innovation es sich handelt und mit welchem Ziel sie – jenseits von Kommerzialisierung und internationaler Relevanz – verfolgt wird, scheint dabei völlig unwichtig zu sein und wird nicht weiter ausformuliert. Schließlich geht es – so z. B. Max-Planck-Präsident Martin Stratmann – bei disruptiven Innovationen darum, „das Unerwartete zu identifizieren und im Sinne der Nutzung auch zu fördern“.⁴

Erwartet wird dieses zu fördernde Unerwartete aktuell vom Maschinellen Lernen. Um es zu fördern, seien kritische Massen an

1. „Klugen Köpfen“ (WissenschaftlerInnen und UnternehmerInnen, am besten in Personalunion als unternehmerische WissenschaftlerInnen),
2. Daten und
3. (Risiko-)Kapital anzureichern und räumlich zu verdichten.

Damit die kritischen Massen wirksam werden, erfordern sie eine Infrastruktur. Dazu zählen wir an dieser Stelle auch die Rechenkapazitäten, die gelegentlich selbst als kritische Masse bei der KI-Entwicklung betrachtet werden, und andere technische Infrastruktur wie Breitbandverbindungen. Im Kern des Ökosystems steht idealerweise ein Forschungscampus, auf dem Institute einer möglichst renommierten Universität, Zweigstellen international bekannter Firmen, zumindest ein vielversprechendes Start-up und am besten auch bekannte private oder öffentliche Institute etwa der Fraunhofer- oder Max-Planck-Gesellschaft präsent sein sollten. Diese Forschungscampus sollten ein

großes Maß an Flexibilität aufweisen, also über Ausbauflächen verfügen, über deren Vergabe unbürokratisch entschieden wird, sowie über flexible Büro- und Laborflächen, die kostengünstig und kurzfristig an mehr oder weniger zukunftssträchtige Start-ups vermietet werden können.

Neben diesen eher materiellen Komponenten des Ökosystems gehören hierzu auch abstraktere Komponenten, darunter neben den oben genannten Forderungen an die Steuerpolitik das *neue politische Mindset*. Zum Ökosystem gehört auch eine gewisse Lebensqualität, die Stadt und Region den weltweit anzuwerbenden WissenschaftlerInnen bieten sollen, sowie ein ausgeklügeltes System zur Verwaltung geistigen Eigentums – samt den hierauf spezialisierten Steuerbüros und Anwaltskanzleien.

Das Cyber Valley in Tübingen

Im Cyber Valley lassen sich sowohl die Blaupausen der KI-Forschung als auch das Forschungsparadigma des ML wiederfinden. Die Forschungsk Kooperation wurde Ende 2016 unter dem Dach der Landesregierung ins Leben gerufen, die eine umfangreiche Förderung im dreistelligen Millionenbereich zusagte und weitere Förderungen in Aussicht stellte. Neben der Landesregierung stellen sich in unterschiedlichen Kontexten das Unternehmen Bosch und die Max-Planck-Gesellschaft als treibende Kräfte hinter dem Projekt dar. Beteiligt sind darüber hinaus neben den Universitäten Stuttgart und Tübingen die Automobilkonzerne Daimler, Porsche und BMW, die Zulieferer ZF Friedrichshafen und IAV (Tochter des VW-Konzerns) und Amazon, welche als Bedingung ihrer Teilnahme jeweils zwischen 1,25 und 2 Millionen Euro in einen Research Fund einzahlen mussten. Räumliches Zentrum ist bislang der Technologiepark Tübingen-Reutlingen, dessen Tübinger Standort auf der *Oberen Viehweide* an die drei Max-Planck-Institute für Entwicklungsbiologie, biologische Kybernetik und intelligente Systeme grenzt. Vor der Gründung des Cyber Valley bestand der Tübinger Technologiepark darüber hinaus aus einem Gründerzentrum mit Büroflächen und ersten Neubauten des dort entstandenen Start-ups CureVac, dessen Marktwert dank Förderung aus dem Pentagon und Risikokapital des SAP-Gründers Dietmar Hopp und der Bill & Melinda Gates Foundation aktuell auf etwa 1,4 Mrd. Euro geschätzt wird – obwohl das Unternehmen noch kein einziges Produkt auf den Markt gebracht hat. Besonders im Verlauf des Jahres 2019 haben sich dort allerdings rege Bautätigkeiten entfaltet: Weitere Firmen siedelten an, CureVac baute weiter aus, erste Außenstellen der Universitäten entstanden sowie ein AI Competence Center, in dem zugleich WissenschaftlerInnen der Universität und die von ihnen gegründeten Start-ups ihre Büroräume haben. Innerhalb weniger Monate waren die Flächen des Technologieparks nahezu vollständig verkauft bzw. optioniert. Im kommenden Jahr soll der Bau eines Amazon-Entwicklungszentrums für bis zu 200 Beschäftigte und auf einer benachbarten Fläche der Bau eines Bosch-Forschungscampus mit bis zu 700 Beschäftigten beginnen. Das Unternehmen ZF Friedrichshafen hat sich – wie zuvor bereits der Branchenriesen Atos durch die Übernahme eines Start-ups an anderen Orten in Tübingen eine Niederlassung erschlossen.

Neben der *Aktivierung* von Großunternehmen und dem rasanten Ausbau des Campus mitsamt ersten spürbaren Auswirkungen auf Wohnungsmarkt und Verkehrsinfrastruktur ist v. a. die Etab-

lierung eines *neuen politischen Mindsets* weit über die Kreise der unmittelbar Beteiligten deutlich spürbar. Die Kommunikation über Hochschule und Wissenschaft beschränkt sich auf KI und ist durchdrungen vom Wettbewerbsgedanken einerseits und dem unbedingten Willen zur Realisierung des vermeintlich Machbaren andererseits. Eine (grüne) Mehrheit des Gemeinderats stimmte im November 2019 trotz massiver Proteste für die Privatisierung kommunaler Flächen für ein Amazon-Entwicklungszentrum mit dem Argument, dieses sei – trotz aller Kritik am Geschäftsmodell des Konzerns – alternativlos für die Zukunftsfähigkeit der Stadt, da nur mit Amazon das Cyber Valley die nötige internationale *Strahlkraft* entfalten könne. Bereits einen Monat zuvor hatte der Chefredakteur der Lokalzeitung (*Schwäbisches Tagblatt*) der linken Gemeinderatsfraktion eine Strategie der *verbrannten Erde* unterstellt, weil diese den Verkauf weiterer kommunaler Flächen an Bosch an Bedingungen knüpfen wollte. Unter dem Titel *Ja zur KI-Zukunft in Tübingen* schrieb er über die entsprechende Gemeinderatssitzung: „Die [Linke] Fraktion beantragte, das Grundstück nur in Erbpacht zu vergeben, die Zivilklausel anzuwenden, eine Tarifbindung von Bosch zu verlangen und zu fordern, dass die Hälfte der Wohnungen an Menschen mit Wohnberechtigungsschein vergeben werden. ‚Das wäre das sofortige Ende der Ansiedlung‘, erwiderte Oberbürgermeister Boris Palmer ... Denn KI-Forschung auf Weltniveau gehe in Deutschland nur in Tübingen, sagte Palmer. Insofern habe die Stadt eine bundesweite Verantwortung für zehntausende, ja hunderttausende Stellen. Klingt großspurig, stimmt aber“.⁵

Die Proteste

Die Proteste zielten anfangs darauf ab, die Bevölkerung Tübingens auf das Projekt aufmerksam zu machen, das von offizieller Seite ausschließlich positiv dargestellt wurde. So formierte sich das Bündnis gegen das Cyber Valley. Die Gruppe brachte eine kritische und antikapitalistische Perspektive zum Thema KI, Konzern- und Militärforschung ein und trat eine Debatte los; darüber, wie die Gesellschaft zu Großkonzernen wie Amazon steht, die sich in der Stadt ansiedeln, welchen Einfluss solche Projekte auf die Universität haben und welche Verantwortung mit dem Fördern von neuer, bisweilen gefährlicher Technologie einhergeht. Bis der Protest begann, gab es in der Stadtbevölkerung kaum Bewusstsein über das Großprojekt. Also setzte das Bündnis lautstark darauf, kritisch aufzuklären und den Widerstand gegen das Projekt zu formieren. Am 6. Juli 2018 fand unter dem Motto *Gegen den Ausverkauf der Stadt, der Universität und des Wissens* eine erste Kundgebung statt. Bald darauf wurde eine Veranstaltung gestört, auf der die Wegbereiter des Cyber Valley, der Tübinger Oberbürgermeister Boris Palmer, Prof. Dr. Bernhard Schöllkopf – Direktor am Max-Planck-Institut für Intelligente Systeme und Amazon Scholar – ihr Projekt darstellen konnten. Da auf dem Podium keine kritischen

Stimmen vertreten waren, intervenierte das Bündnis mit Zwischenrufen und eigenen Statements, wodurch sich die erste lautstarke Diskussion zwischen den Planern und Gegnern des Großprojekts ergab. Darauf folgten weitere Kundgebungen und Demonstrationen gegen das Cyber Valley und für eine solide Grundfinanzierung von Universitäten, damit diese eben nicht mehr abhängig von privatwirtschaftlichen Geldgebern sind. Die mangelnde Transparenz, die fehlende demokratische Mitbestimmung bei dem Projekt sowie die unumstößliche Loyalität der Universitätsrepräsentanten gegenüber der Initiative veranlasste eine Gruppe von Studierenden dazu, im Dezember 2018 aus einer Demonstration gegen das Cyber Valley heraus einen Hörsaal an der Universität zu besetzen. Bis kurz vor Weihnachten fanden dort Vorlesungen statt, die sich kritisch mit künstlicher Intelligenz, dem Technologiezeitalter sowie dem modernen Kapitalismus auseinandersetzten. Die Besetzung bot einen Raum, in dem sich 24 Stunden lang an jedem Tag der Woche Gleichgesinnte treffen konnten, um auf das Thema bezogen zusammenzuarbeiten. Daraus entstanden in wenigen Wochen weitere Proteste, darunter die Störung der Wiederwahl des Universitätsrektors und das Pflanzen von Bäumen auf der Fläche, die für den Bau des Amazon-Forschungszentrums vorgesehen ist. Gewidmet sind die Bäume der menschlichen Vernunft, der Entscheidungsfreiheit und der Vielfalt.

Die Aktionen führten dazu, dass die Universitätsleitung in eine Podiumsdiskussion einwilligte. Hier begegneten sich erstmals Gegner und Verantwortliche des Cyber Valleys auf Augenhöhe. Der Universitätsrektor sowie zwei InformatikprofessorInnen argumentierten mit Vertretern des Bündnisses vor einem prall gefüllten Vorlesungssaal für und gegen das Projekt und dessen Auswirkungen auf Stadt und Gesellschaft. Seit dem Ende der Besetzung gehen die Proteste weiter. Mittlerweile haben sich auch Einzelhändler mithilfe von Plakaten gegen die Ansiedlung Amazons positioniert. Die Bevölkerung ist informiert und das Bündnis ist bei Gemeinderatsentscheidungen zum Thema und im öffentlichen Raum weiterhin sehr präsent.

Anmerkungen

- 1 <https://www.cyber-valley.de/de/about> (20. Januar 2020).
- 2 Roland Berger / *Pioneers: Startup-Hub Wien – Zukunftschancen gezielt nutzen*, www.rolandberger.com.
- 3 Roland Berger / *Asgard: Artificial Intelligence – A Strategy for European startups*, www.rolandberger.com.
- 4 Deutschlandfunk: Glaubwürdigkeitskrise der gesellschaftlichen Eliten – Martin Stratmann im Gespräch mit Ralf <https://www.cyber-valley.de/de/aboutKrauter>, „Forschung aktuell“ vom 24. Januar 2018.
- 5 Gernot Stegert: *Das Schreckgespenst des bösen Kapitals und die Wirklichkeit*, und: *Ja zur KI-Zukunft in Tübingen*, in: *Schwäbisches Tagblatt* vom 12. Oktober 2019.



Christoph Marischka und Dominik Wetzel

Christoph Marischka ist Politikwissenschaftler und aktiv bei der *Informationsstelle Militarisierung (IMI)* e. V.

Dominik Wetzel arbeitet als freier Journalist und studiert Politikwissenschaft und öffentliches Recht an der Universität Tübingen.

Arbeitsgruppe: Schöne neue Arbeitswelt 4.0?

An der Arbeitsgruppe nahmen etwa 20 Personen teil. Nach der Begrüßung der TeilnehmerInnen und der Vorstellung der beiden Moderatoren erfolgte eine kleine Einführung in das Thema anhand der Darstellung, wie die Digitalisierung in die deutschen Kirchen/Gottesdienste einzieht: die ersten BLESS-U-2-Roboter sind bereits sozusagen als digitale Pastoren/Pfarrer im Einsatz und werden offenbar von der Bevölkerung überwiegend positiv angenommen.

Zielsetzung der Arbeitsgruppe war es, die folgenden Themen zu bearbeiten:

- Veränderungen am Arbeitsplatz während der letzten zehn Jahre durch Automatisierung, Digitalisierung und Globalisierung,
- neue Arbeitsformen
- die Sicherung von Arbeitsplätzen zu diskutieren und zu beraten sowie
- ein Fazit und Vorschläge zu generieren.

Es wurde festgestellt, dass man/frau keine Wahl mehr hat, die Automatisierung, Digitalisierung und Globalisierung anzunehmen oder abzulehnen, da bereits fast alle Lebensbereiche betroffen sind und die immer schnellere Entwicklung zu verstärktem Personalabbau in den betroffenen Bereichen führt. Beispiele: Einsatz von Industrierobotern, Verschwinden von Schreibbüros im Betrieb (bereits in den 80er Jahren), Einführung der digitalen Zeiterfassung im Betrieb, digitale Produktionssteuerung etc. Die Intensivierung der Datenverarbeitung führte zu Rationalisierungsmaßnahmen in weiteren Bereichen wie Versicherungen, Banken, Gesundheitswesen und Behörden.

Automatisierung, Digitalisierung und die zunehmende Vernetzung von Datenmengen und Systemen haben zur Transformation der Arbeit und der Arbeitswelt geführt. Die AG-TeilnehmerInnen bewerteten die Unterstützung und Möglichkeiten der Digitalisierung einerseits als arbeitserleichternd, positiv und als Chance für ArbeitnehmerInnen und Umwelt. Andererseits wurden der zunehmende Leistungsdruck, die Verstärkung der Rationalisierungsmaßnahmen und der inzwischen weltweite Verdrängungswettbewerb, der sowohl zu Arbeitsaufträgen aus aller Welt als auch zu Arbeitsplatzverlusten in aller Welt führt, als reale Bedrohung empfunden, die zu Ängsten und Verunsicherung führt.

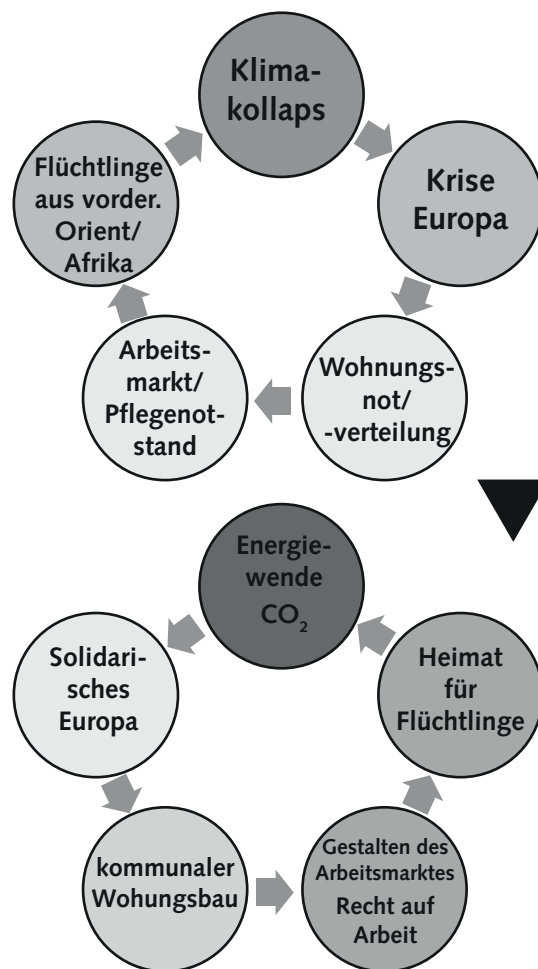
Es wurde angemerkt, dass zwar Imperialismus und Kolonialisierung in der Vergangenheit bereits zu globalen Handels- und Lieferbeziehungen führten, in deren Folge die Menschen ausgebeutet und unter Druck gesetzt wurden, dass es jedoch erst durch das Internet möglich wurde, umfangreiche globale Produktionsketten aufzubauen und in kürzester Zeit alle erforderlichen Informationen und das nötige Know-how sowie Arbeitsplätze und Produktionsstätten bei Bedarf in Billiglohnländer zu verlagern.

Inzwischen beeinflussen im Zuge der Globalisierung und des weltweiten Wettbewerbs (siehe Grafik Globalisierung) etliche Faktoren die Arbeitsplätze. Es wurde berichtet, IBM habe versucht, Organisationsabläufe des Internets auch auf die Arbeitsabläufe der IT-Branche zu übertragen. Dieses Beispiel führte zu der Frage, wie denn die Erfahrungen der AG-TeilnehmerInnen an ihrem persönlichen Arbeitsplatz aussähen.

Es zeigte sich, dass sowohl weiterhin mit dem Wegfall von Arbeitsplätzen wegen des verstärkten Einsatzes von Robotern, zunehmender Digitalisierung in allen Bereichen und in allen Branchen gerechnet wird als auch mit der Entstehung neuer Arbeitsplätze, da Programme geschrieben werden, Roboter gewartet und repariert werden müssen – und weil Kreativität, Phantasie und Intelligenz eben nicht *künstlich* machbar sind, sondern nach wie vor nur Eigenschaften des Menschen sind.

Eine Forderung der Beschäftigten bei Veränderungen im betrieblichen Ablauf sollte es sein, jede/n einzelne/n MitarbeiterIn von Beginn an mitzunehmen: bereits vor der Einführung von Neuerungen im Betrieb sollten die Beschäftigten eingebunden und geschult werden, weil es für beide Seiten wichtig ist, dass das Fachwissen der Beschäftigten zur Gestaltung der geplanten Veränderungen genutzt wird.

Es wurde dargestellt, dass infolge betrieblicher Veränderungen immer auch Leistungsverdichtung am Arbeitsplatz auftritt oder Arbeitsplätze entfallen.



Grafik Globalisierung

Der Abbau von Personal, der Verlust des Arbeitsplatzes bedeuten für die betroffenen Personen und Regionen eine gravierende Veränderung des individuellen und des sozialen Lebens. Arbeit sei ein wichtiger Bereich im Leben, stellte die Arbeitsgruppe fest. Denn Arbeit hat auch eine starke soziale Dimension. Sie ermöglicht die Gestaltung des eigenen Lebens und des sozialen Umfelds, der Umwelt und der Welt. Arbeitende Menschen und arbeitende Roboter (!) sind zweifellos Bestandteile eines sehr komplexen Gesamtsystems. Arbeitsprozesse und soziale Strukturen verändern sich durch Arbeit. Industrielle Arbeit im aufkommenden Kapitalismus hat dazu geführt, dass die Menschen sich in Arbeitervereinen, Gewerkschaften und Kooperativen, in Sportvereinen und politischen Parteien zusammenschlossen, um Veränderungen herbeizuführen, Ungerechtigkeiten auszuschließen oder abzuschwächen, um Arbeitszeit, Arbeitsbedingungen, Arbeitsschutz, Freizeit und Demokratie zu gestalten.

Die Transformation der Arbeit 4.0, der verstärkte Einsatz von digitaler Technik ebenso wie die veränderten oder gefährdeten Arbeitsplätze sollten daher dazu genutzt werden, so die Arbeitsgruppe, sämtliche zuvor genannten Gestaltungsmöglichkeiten auszuschöpfen. Dazu gehört auch, vom Arbeitgeber und von der Politik Bildungsmaßnahmen für alle Beschäftigten zu fordern und durchzuführen sowie die Arbeit möglichst gerecht neu aufzuteilen. Hierzu sollten Arbeitgeber und Arbeitnehmer die Arbeiten strukturieren und so umverteilen, dass kein Personal entlassen werden muss, dass erforderliche Weiterbildung erfolgt und dass zukünftig eine Normalarbeitszeit von etwa 25 Wochenstunden umgesetzt wird. Es geht also im Zuge der Digitalisierung nicht nur um die Transformation der Arbeit und der Arbeitsabläufe, sondern für die Beschäftigten vor allem auch darum, die betroffenen Arbeitsplätze bzw. Arbeitsinhalte den betrieblichen Änderungen anzupassen und die MitarbeiterInnen rechtzeitig weiterzubilden. Für die Menschen insgesamt geht es darum, ihre Rechte und Möglichkeiten zu nutzen, um ihre Zukunft zu gestalten.

Schleichend haben sich in den vergangenen zehn oder 20 Jahren durch die mobile Technik wie Laptop und Mobiltelefon auch neue Arbeitsformen ergeben. Die Beschäftigten sind heutzutage theoretisch permanent erreichbar und/oder können theoretisch auch außerhalb des Betriebes zuhause oder unterwegs arbeiten, sowie die Arbeitszeit frei einteilen, sofern nur der vorgegebene Termin für die Erledigung der Arbeit eingehalten wird. Zugleich laufen sie aber auch Gefahr, permanent überwacht zu werden. Die freie Zeiteinteilung und die permanente Erreichbarkeit können zu negativen Veränderungen von Abläufen im Privatleben führen, die Möglichkeit der totalen Überwachung am Arbeitsplatz durch digitale Technik schafft zusätzlichen Druck und erzeugt Ängste. Auch besteht die Gefahr von gesundheitlichen Schädigungen infolge zunehmender Bildschirmarbeit. Aus der Transformation der Arbeit ergibt sich gemäß der Arbeitsgruppe ein umfangreicher Regelungsbedarf, um Nachteile für die Beschäftigten auszuschließen.

Orts- und zeitunabhängiges Arbeiten in der *Cloud* bedarf einer entsprechenden informationstechnischen Infrastruktur des Betriebes und wird sowohl von festen als auch von Zeit- und freien MitarbeiterInnen wegen der Flexibilität geschätzt. Es gewährt einerseits eine angenehme *Work-Life-Balance*, schließt aber auch die Gefahr des Abbaus von sicheren Arbeitsplätzen ein.

Auch *Crowdworking* gewährt Flexibilität in Bezug auf Ort und Zeit und erlaubt zudem das Arbeiten für verschiedene Auftraggeber, da *Crowdworker* meist selbstständig sind. Ihre Aufträge finden sie auf entsprechenden Plattformen im Internet – ihre Konkurrenz ist folglich weltweit. Der Auftraggeber sucht sich dann unter den Bewerbern auf der Plattform das für ihn günstigste Arbeitsangebot aus: die beste Lösung zum niedrigsten Preis. Meist allerdings geht es ohnehin um kleine Aufträge, für die überwiegend kein großes Spezialwissen erforderlich ist und für die nur wenig gezahlt wird. Die weltweite Konkurrenz, die das Internet ermöglicht, bedeutet aber offenbar große Unsicherheit in Bezug auf Aufträge und Einkommen für die *Crowdworker*.



Birgit und Michael Ahlmann

Nach dem Studium des Informationsdesigns an der FH Kiel arbeitete **Birgit Ahlmann** zunächst als Grafikerin, studierte dann Soziologie und Anglistik/Amerikanistik an der CAU Kiel und arbeitete danach als PR-Managerin und Messespezialistin in der Maschinenbauindustrie. Anschließend war sie elf Jahre Betriebsratsvorsitzende und stellvertretende Gesamtbetriebsratsvorsitzende sowie Mitglied des Europäischen Betriebsrates, sie leitete die IT-Ausschüsse in Betriebsrat, Gesamtbetriebsrat und Konzernbetriebsrat, sie war ca. 10 Jahre Mitglied des Ortsvorstandes der IG Metall Kiel-Neumünster. Weiterhin gilt ihr aktives Interesse der Gestaltung der Zukunft von Arbeit und Umwelt. Sie ist Mitglied der IG Metall und des FfF.

Michael Ahlmann studierte an der CAU in Kiel Mathematik und Physik. An der Universität Hannover erwarb er den Diplom-Ingenieur für Allgemeine Elektrotechnik. In einem Elektronikunternehmen in Bremen arbeitete er als Softwareentwickler und Betriebsrat. Neben den Aufgaben eines Betriebsratsvorsitzenden leitete er einen Gesamt- und einen Konzernbetriebsrat und wirkte in zwei großen europäischen Konzernen im Konzernbetriebsrat und besonders in den entsprechenden IT-Ausschüssen mit. In zwei Konzernen war er viele Jahre Mitglied des Europäischen Betriebsrates. Seit ca. dreißig Jahren ist er aktives Mitglied des FfF und des AK Rüstung und Informatik. Seit 1974 ist er Mitglied der IG Metall. Seine Interessen liegen in den Themen Cyberpeace, nachhaltiges Leben und im Holzwerken.

Besonders negativ erscheint der Arbeitsgruppe *Arbeit auf Abruf*: gemäß diesen sogenannten *Zero-hour-Verträgen* kann den JobberInnen einerseits Arbeit zugeteilt werden, die sofort erledigt werden muss, andererseits kann es passieren, dass er/sie wochen- oder monatelang keine Arbeit erhält: keine Arbeit, keine Sicherheit, kein Geld, kein Recht mehr auf Arbeit (siehe Artikel 23 der Menschenrechte)? Die Arbeitsgruppe befürchtet, dass Arbeit 4.0 leicht zu einer zunehmenden Ausnutzung der Beschäftigten führen kann – und dass durch die globale Konkurrenz die Gefahr besteht, dass es immer mehr prekäre Beschäftigte geben wird. Deshalb sieht die Arbeitsgruppe es als unerlässlich an, dass sich ArbeitnehmerInnen rechtzeitig betriebsübergreifend über die betrieblichen Veränderungen austauschen, um sich gemeinsam für eine zukunftsgerechte und menschengerechte Gestaltung der Arbeitsplätze 4.0 und der Arbeitsabläufe 4.0 einsetzen zu können.

Auch das Thema Ökologie wird in der Arbeitsgruppe angesprochen. Die zunehmende Digitalisierung benötigt immer mehr Energie und Rohstoffe. Mächtige Datenspeicher in den entferntesten Ecken der Erde haben einen immensen Energie- und Kühlungsbedarf. Die tägliche Nutzung der digitalen Technik in Privathaushalten, im öffentlichen Leben und in den Betrieben führt zu erhöhtem Energieverbrauch. Zudem werden manche Rohstoffe zur Herstellung der digitalen Geräte knapp. Es wird diesbezüglich seitens der AG-TeilnehmerInnen ein dringender Klärungsbedarf gesehen und die Erstellung eines Konzepts und Maßnahmenkatalogs gefordert, wie diese Probleme gelöst werden können und sollen.

Die Digitalisierung sollte, so die Arbeitsgruppe, für mehr Gerechtigkeit genutzt werden. Tätigkeiten sollten gerechter bewertet werden, gleicher Lohn sollte für gleiche Arbeit gezahlt werden. Es ist allen bewusst, dass gerade im weltweiten Wettbewerb Beschäftigte sich nicht gegen einander ausspielen lassen dürfen, sondern sich solidarisieren müssen. Solidarisierung wird als Voraussetzung gesehen, um etwas bewegen und gestalten zu können.

Am Beispiel China wurde aufgezeigt, was dort in naher Zukunft an Veränderungen geplant ist: China hat Presseberichten zufolge erklärt, bis 2025 alljährlich bis zu einer Million Arbeitsplätze abzubauen und die Beschäftigten durch Roboter zu ersetzen, was erhebliche Ängste bei der arbeitenden Bevölkerung hervorgerufen und zu großen Unruhen geführt haben soll.

Die Transformation der Arbeit durch die Digitalisierung sollte gemäß der Arbeitsgruppe genutzt werden, um beispielsweise körperlich schwere oder monotone Arbeiten durch Roboter erledigen zu lassen, also zu einer neuen Form der Arbeitsteilung und der Arbeitsgestaltung führen. Dafür müssen jeweils die Mensch-Maschine-Schnittstellen definiert werden.

Roboter rechnen sich zwar für den Arbeitgeber, weil sie nicht krank oder müde werden und nicht streiken; sie haben keine eigene Meinung und werden so programmiert, dass sie die Arbeiten, für die sie eingesetzt werden, ohne Ablenkung, Zeitverlust und Diskussionen ausführen. Sie sind berechenbarer, bequemer und billiger als Menschen für den Arbeitgeber, so die AG. Aber: sie verfügen nicht über die gestalterischen, kooperativen und kreativen Fähigkeiten des Menschen, die im Arbeitsprozess wie überhaupt im menschlichen Zusammenleben unverzichtbar sind.

Daraus folgt: Der Prozess der Digitalisierung der Arbeitswelt führt weiterhin zu Veränderungen in allen sozialen, wirtschaftlichen, politischen, technischen, ökologischen und weiteren Bereichen, so befanden die AG-TeilnehmerInnen. Von der Transformation der Arbeit sind alle Menschen also „irgendwie“ betroffen. Obwohl von der Arbeitsgruppe kritisch angemerkt wurde, dass ein großes Fass aufgemacht wurde, gilt es daher, das Jetzt und die Zukunft kontinuierlich mitzugestalten. Von Ihnen, von euch, von uns, von allen – das schließt die weitere Aktivität entsprechender Arbeitsgruppen ein.



Sylvia Jahnigk

Arbeitsgruppe: Gesundheitsdaten müssen aus den Fängen des Datenschutzes befreit werden

Unter diesem Titel fand auf der FfF-Konferenz 2019 der Workshop mit ca. 20 TeilnehmerInnen statt. Der Teilnehmerkreis war breit gefächert, insbesondere waren auch Betroffene dabei, die sich bereits selbst kritisch mit dem Thema befasst haben. Schnell wurde klar, dass es im Rahmen des Workshops nicht möglich war, informationstechnische Thesen bzw. Forderungen zu formulieren, da ein großer Teil der TeilnehmerInnen nicht das nötige Fachwissen hatte und sich nicht aktiv hätte einbringen können. Sie waren stärker daran interessiert, zu erfahren, was eigentlich gerade im Gesundheitssektor passiert oder wollten wissen, was man tun könnte, außer, die Gesundheitskarte zu verweigern. Im Folgenden werden die im AK behandelten Inhalte nachgezeichnet.

Wert von Gesundheitsdaten

Zum Einstieg ging die Diskussion um den Wert der Patientendaten. Hierbei wurde an Hand von zwei Beispielen deutlich gemacht, über welchen Wert wir reden. Gesundheitsdaten sind 10-mal soviel wert wie Kreditdaten.¹ Die Schätzungen bei dem Wert einer individuellen Patientenakte gehen von durchschnittlich 60 bis 150 € aus – wenn es eine einfache Akte ist.² Gewisse Gesundheitsdaten sind „Gold wert“.³ Laut der NZZ hat Gen-

tech, eine US Tochter der Roche Group, 2015 für 60 Mio US\$ 3000 Datensätze aus einer Gendatenbank des AppHerstellers 23andMe gekauft. Anhand einer Cyberversicherung, die benötigt wird, um die Werte in einer Cloud zu versichern, wurde aufgezeigt, dass die in einer Telematik-Infrastruktur gespeicherten Patientendaten die Versicherungssumme der Cyberversicherung um das 9-fache übersteigt, wenn tatsächlich für alle GK-Versicherten eine elektronische Patientenakte angelegt würde.⁴

In der Vergangenheit wurde deutlich, wie stark PolitikerInnen daran interessiert sind, dass das Datenschutzrecht deutlich aufgeweicht wird, damit Daten und in diesem Fall Gesundheitsdaten dem Wirtschaftskreislauf zugeführt werden können. Die CDU sieht sich dabei als Vorreiterin der Digitalisierung und möchte den Datenschutz, respektive die Datensparsamkeit, in die Datensouveränität transformieren.⁵ Die Datensouveränität soll die Gesundheit aller Bürger verbessern.

Wer betreibt die Telematik-Infrastruktur?

Die Annahme, die Gematik GmbH würde die Telematik-Infrastruktur betreiben, ist ein weit verbreiteter Irrtum. Die Telematik-Infrastruktur wird von der Bertelsmann-Tochter Arvato betrieben. Der Vertrag wurde im Juli 2018 um weitere acht Jahre verlängert.⁶ Betrachtet man die Vergangenheit, wird deutlich, dass Bertelsmann mehrfach in Datenschutzskandalen verwickelt war und gegen das Datenschutzrecht verstoßen hat (siehe Beispiele^{7,8,9,10,11}). Es muss daher in Frage gestellt werden, ob Arvato die im Datenschutzrecht geforderte Sorgfalt und Zuverlässigkeit im Umgang mit sensiblen personenbezogenen Daten in Zukunft an den Tag legen wird. Trotz wiederholten Verstößen gegen geltendes Recht, mangelnder Einsicht, irgendetwas falsch zu machen und gleichzeitigem Lobbyismus für die Datensouveränität¹² wurde der Vertrag zwischen der Gematik und Arvato verlängert.

Das wirft die Frage auf, ob die Gematik in der Rolle der Prüferin für DienstleisterInnen und Services den Prüfprozess und die Freigabe mit der nötigen Sorgfalt ausübt. So hat die Gematik ihr Sicherheitskonzept letztmalig März 2008 angepasst.¹³ Dieses Sicherheitskonzept ist schlicht veraltet und damit ungeeignet, um DienstleisterInnen eine verbindliche Vorgabe für die umzusetzenden Anforderungen zu geben. Dieses Faktum stellt einen groben Mangel innerhalb der Sicherheitsarchitektur der Gematik dar. Die beschriebenen Technologien, Standards und Risiken haben sich in den letzten 12 Jahren drastisch verändert. Es scheint, als sei die Gematik mit der Aufgabe als Richtliniengeberin und Kontrollorgan für DienstleisterInnen überfordert. Ein Sicherheitskonzept muss jährlich überarbeitet und dem veränderten Umfeld entsprechend angepasst werden.

Dass die Gematik ihrem Auftrag nicht gerecht wird, wird u.a. auch an dem Beispiel der Konnektoren deutlich. Anders als es die Gematik behauptet¹⁴, sind viele der Konnektoren fehlerhaft konfiguriert.¹⁵ Dazu sei angemerkt, dass sich der Skandal seit der FlFF-Konferenz im November 2019 noch ausgeweitet hat.¹⁶ Es zeigt, dass die Gematik Sicherheitsprobleme nicht gelöst hat und somit sogar Teil des Problems ist.



Sylvia Johnigk forscht und arbeitet seit über 25 Jahren im Bereich IT-Sicherheit, seit 2009 ist sie selbständige Beraterin in Großkonzernen. Ebenfalls seit 2009 ist sie im Vorstand des FlFF e. V.

Was geschieht mit den Daten in der Telematik-Infrastruktur?

Der offizielle Sprachgebrauch ist, dass mit der Telematik-Infrastruktur die Gesundheit der Bürger verbessert werden soll. Tatsächlich steht zu befürchten, dass die Patientendaten dem Wirtschaftskreislauf zugeführt werden sollen. So ist vorgesehen bzw. geplant, dass die Daten der Telematik-Infrastruktur für Forschungszwecke ohne weitere Zustimmung der PatientInnen weiterverwendet werden.¹⁷ Dass das Vorhaben rechtlich nicht unumstritten ist, wird in einem Artikel in *Netzpolitik* dargelegt.¹⁸ Deutlich an diesem Beispiel wird aber, wohin der Zug gehen soll. Der Punkt der Verwertung muss am dringendsten geklärt werden. Die meisten TeilnehmerInnen und vor allem die Betroffenen sehen sich als Opfer, weil sie nicht ermitteln können, was mit ihren Daten passieren wird. Der Gesetzgeber oder die Regierung hat „scheinbar“ die Macht, Gesetze zu erlassen, die eine Verwertung der Daten ermöglichen, in dem sie es am Datenschutzrecht vorbei mogeln.

Weitere Themen, die in der Arbeitsgruppe beleuchtet wurden

In der Arbeitsgruppe wurden auch noch viele weitere Themen angeschnitten, wie zum Beispiel die Validität von Big-Data-Modellen. Was bedeutet es, wenn die Modelle mit fehlerhaften Daten trainiert werden? Was wären die möglichen Auswirkungen, wenn Ärzte zukünftig Künstliche Intelligenzen bei der Behandlung und Diagnose berücksichtigen müssen und Ärzte Apps verschreiben müssen, die möglicherweise neugieriger sind, als für die Behandlung erforderlich, und so weiter?

Fazit

Ein gemeinsames Ziel, mit welcher Form des Protestes es weitergehen gehen könnte, wurde diskutiert.

Es gab eine große Übereinkunft, dass weder eine zentrale Speicherung von Gesundheitsdaten und schon gar nicht bei kommerziellen DienstleisterInnen aus Sicht der Betroffenen wünschenswert ist. Angedacht wurde eine dezentrale Speicherung der Daten durch eine Treuhändergesellschaft, deren Aufsicht auch durch Betroffene wahrgenommen werden kann.

Weitere Ideen gab es zu Aufklärungsflyern, die in Fußgängerzonen verteilt werden, Info-Veranstaltungen, die Risiken und Problematiken transparent und einfach vermitteln, oder Youtube-Videos, die man bequem im Internet abrufen kann.

Mehrere TeilnehmerInnen haben Interesse geäußert, als Arbeitsgruppe an dem Thema weiterzuarbeiten. Dazu werde ich eine Mailingliste anlegen und eine erste Telefonkonferenz organisieren. Interessierte können sich gern bei mir unter sylvia@fiff.de melden.

Anmerkungen

- 1 <https://www.althammer-kill.de/news-detail/gesundheitsdaten-sind-wertvoller-als-finanzdaten/>
- 2 Solche Werte lassen sich dadurch bestimmen, wie viel für solche Daten auf dem Schwarzmarkt gezahlt wird oder wenn die Daten legal verkauft wurden.
- 3 Neue Zürcher Zeitung vom 21.05.2015 <https://www.nzz.ch/wirtschaft/gewisse-gesundheitsdaten-sind-gold-wert-1.18546205>
- 4 Die Annahme ist, dass bei 74 Millionen Versicherten und einem Betrag von 60 EUR pro Akte ein Wert von 4,44 Mrd. EURO einem Haftungshöchstbetrag von einer ½ Mrd EUR bei einem bekannten deutschen Versicherer gegenübersteht.
- 5 Handelsblatt vom 30.09.2019: CDU will den Datenschutz aufweichen – für schnellere Digitalisierung <https://www.handelsblatt.com/politik/deutschland/digitalcharta-cdu-will-den-datenschutz-aufweichen-fuer-schnellere-digitalisierung/25066904.html>
- 6 [https://www.gematik.de/news/news/gematik-erteilt-zuschlag-im-](https://www.gematik.de/news/news/gematik-erteilt-zuschlag-im-vergabeverfahren-zur-zentralen-telematikinfrastruktur/)

- <https://www.heise.de/newsticker/meldung/Bericht-Infoscore-nutzt-veraltete-Daten-bei-Bonitaetsberechnung-1545563.html>
- 8 <https://www.heise.de/newsticker/meldung/NDR-Mangelhafter-Datenschutz-bei-Bertelsmann-Auskunftei-Infoscore-2583029.html>
- 9 <https://www.mdr.de/daten Spuren/daten Spuren-138.html>
- 10 <https://www.mdr.de/daten Spuren/daten Spuren-162.html>
- 11 <https://www.zeit.de/digital/datenschutz/2016-05/bahn-kundendaten-infoscore-schwarzfahren>
- 12 <https://www.bertelsmann-stiftung.de/de/unsere-projekte/teilhabe-in-einer-digitalisierten-welt/projektnachrichten/datensouveraenitaet-in-zeiten-von-big-data/>
- 13 https://fachportal.gematik.de/fileadmin/user_upload/fachportal/files/Spezifikationen/Basis-Rollout/Datenschutz_und_Datensicherheit/gematik_DS_Sicherheitskonzept_V2_2_0.pdf
- 14 <https://www.aend.de/article/201216>
- 15 <https://www.heise.de/newsticker/meldung/Telematik-im-Gesundheitswesen-Freie-Aerzteschaft-warnt-vor-unsachgeaesser-Konnektor-Installation-4406506.html>
- 16 <https://www.heise.de/ct/artikel/Hinweise-auf-moegliche-Verwundbarkeiten-der-Medizin-Telematik-4635791.html>
- 17 https://www.focus.de/gesundheit/kassenpatienten-jens-spahn-will-daten-ohne-einwilligung-fuer-forschung-freigeben_id_11302621.html
- 18 <https://netzpolitik.org/2019/ein-bisschen-widerspruch-digitale-versorgung-gesundheitsdaten/>



Marie-Luise Abshagen und Nelly Grotefendt

Eine Frage der Macht – Nachhaltigkeit und Digitalisierung

Sei es die Technologisierung unseres Lebens- und Arbeitsalltags oder die Integration von Kommunikationstechnologie in industrielle Produktionsschritte – Digitalization is everywhere. Nachhaltigkeit, umfassende demokratische Teilhabe oder eine Entschleunigung der Entwicklung sind dabei höchstens Randthemen. Digitalisierung gilt als Moderne, als nächster Industrialisierungsschritt, als Neuland. Doch ist das wirklich so? Wie kann eine gerechte Digitalisierung aussehen? Welche Rahmenbedingungen braucht es dafür? Und wer muss sie umsetzen?

Beginnen wir am anderen Ende der Digitalisierung, buchstäblich gesprochen auf der anderen Seite der Welt, in Papua-Neuguinea. In den Gewässern des pazifischen Staates soll das erste kommerzielle Tiefseebaugrubenprojekt stattfinden. Dabei sollen vom Meeresgrund verschiedene Arten mineralischer Rohstoffe abgebaut werden, um an Kupfer, Gold, Mangan und seltene Erden zu kommen. Diese Ökosysteme werden dabei auf jeden Fall zerstört. Welche anderen Auswirkungen die schweren Maschinen auf den Meeresboden und der Abraum auf das Wasser haben, ist völlig unklar. Das Leben der Menschen an den Küsten wird dadurch massiv gefährdet, weswegen sich seit Jahren Protest und Widerstand der Menschen, der Küstengemeinschaften und der Kirchen vor Ort formt.

Tausende Tiefseebaugrubenlizenzen sind im ganzen Pazifik in den nationalen Gewässern bereits verteilt. Gleichzeitig laufen im Rahmen der Vereinten Nationen Verhandlungen darüber, wie man den Abbau von Tiefseerohstoffen im internationalen Gewässer – der Hohen See – im Rahmen des völkerrechtlichen Seerechtsübereinkommens regeln kann.

Es mag schockieren, dass man die Meere angesichts der bereits bestehenden multiplen Belastungen durch Klimawandel, Überfischung und Plastikverschmutzung nun einer weiteren Ausbeutung aussetzen will. Doch folgt dieser Griff nach den minerali-

schen Rohstoffen im Meer nur weiter der Logik des unendlichen Wachstums und der technischen Modernisierung der Welt – nicht zuletzt für die Digitalisierung.

Ist Digitalisierung etwas völlig Neues?

Entgegen der prominenten These, dass mit der Digitalisierung eine neue Art der Industrialisierung eingeleitet würde, zeigt sich beim genauen Hinsehen, dass das Gegenteil der Fall ist. Die aktuelle Art der Digitalisierung folgt bestehenden Trends wie Rohstoffübernutzung, Ausbeutung von Mensch und Natur, Machtungleichgewicht, enorme Kapitalisierung, Hang zum Oligopol. Mit all den positiven Entwicklungen, die eine digitale Welt hervorbringt, kann sie nur nachhaltig sein, wenn diese Trends anerkannt werden und bewusst dagegen gesteuert wird. Dafür müssen einige kritische Fragen gestellt werden:

Wer profitiert derzeit eigentlich von der Digitalisierung?

Die zentralen kommerziellen Akteure im Internet sind einige wenige große Digitalkonzerne, die den Markt digitaler Infrastruktur

und Dienstleistungen unter sich aufteilen. Bemerkenswert ist, dass diese Unternehmen mittlerweile die an der Börse am höchsten gehandelten Firmen weltweit darstellen. Angesichts dieser extremen Machtkonzentration im digitalen Sektor selber wie auch im globalen Wirtschafts- und Finanzsystem ist es gleichwohl erschreckend, wie gering die Regulierung dieser Unternehmen bisher erfolgt. Sowohl ihr marktwirtschaftlich bedenklicher Hang zur Oligopolbildung als auch die weitgehend intransparenten Geschäftsmodelle sowie virulente Steuervermeidung dürfen nicht als neue Industrialisierungsform akzeptiert werden, sondern müssen mit bestehenden Mitteln bspw. des Kartell- und Steuerrechts sowie des Verbraucherschutzes gekontert werden.

Die Verantwortung im Sinne einer Angebots-Nachfrage-Marktregulierung auf die KonsumentInnen zu schieben, ein bekannter Trend im aktuellen Wirtschaftssystem, ist im digitalen Sektor unmöglich, da KonsumentInnen selten in der Lage sind, zu beurteilen, was das Geschäftsmodell des digitalen Unternehmens eigentlich ist. Ein Nichtzustimmen oder gar überhaupt Verstehen der Geschäftsbedingungen ist kaum denkbar, ein Opt-out aufgrund der mittlerweile fortgeschrittenen Vernetzung mittlerweile fast ausgeschlossen. Dabei sind doch gerade die KonsumentInnen das Geschäft, da sie mit ihrer Nutzung und damit ihren Daten erst den enormen Wert des Unternehmens herbeiführen.

Angesichts dessen stellt sich die Frage, wie demokratisch die Digitalisierung eigentlich derzeit ist

Nicht nur hinsichtlich der fehlenden Mitbestimmung in der Nutzung der eigenen Daten durch ein Unternehmen müssen digitale Geschäftsmodelle kritischer beleuchtet werden. Spätestens seit den Skandalen um *Cambridge Analytica* und den Wahlen in den USA, Brasilien, Kenia oder Malaysia hat sich gezeigt, dass digitale Kommunikations- und Social-Media-Plattformen manipuliert werden können, teilweise mit Wissen der Plattformbetreiber. In Myanmar hat die fehlende Strategie von Facebook, mit dieser Manipulation umzugehen, sogar zu einer so massiven Ausweitung von Hate Speech und Fake News geführt, dass davon auszugehen ist, dass der Hass auf die Rohingya, der zu einer Vertreibung von 600.000 Menschen geführt hat, durch die Plattform begünstigt wurde. Gleichwohl greifen Regierungen weltweit für Massenüberwachungen auf digitale Dienste zurück (häufig in Kooperation mit digitalen Unternehmen), wie u. a. die Enthüllungen von Edward Snowden gezeigt haben.

Kaum einer dieser Skandale hat strafrechtliche Konsequenzen, politische Schutzmaßnahmen oder eine großangelegte, mit Konsequenzen versehene Aufklärung nach sich gezogen. Vielmehr bestehen sowohl die Strukturen wie auch die digitalen Werkzeuge weiter und befinden sich noch immer in der Nutzung. Zu lasten unserer Demokratien.

Und schließlich stellt sich die Frage nach den physischen Grundlagen der Digitalisierung

Die aktuelle Digitalisierung geht nicht ohne massive weitere Ausbeutung von Natur und Arbeitskräften. Nichts deutet darauf hin, dass wir den Rohstoffbedarf und den Energieverbrauch der Digitalisierung – sei es bei der Unterhaltungstechnologie, In-

dustrie 4.0 oder Mobilität – auch nur stabil halten werden. Im Gegenteil, der Bedarf an mineralischen Rohstoffen und billiger Energie nimmt kontinuierlich zu.

Dabei gehen Umweltzerstörung, Menschenrechtsverletzungen und unterschiedlich starke Konflikte mit dem Abbau von Rohstoffen praktisch immer einher. Der Verbrauch mineralischer Rohstoffe sowie der Flächenverbrauch für deren Abbau sind schon jetzt kritisch. Doch könnte sich etwa der Bedarf an Lithium bis 2035 vervierfachen und der von seltenen Erden verdreifachen. Gerade für Länder des globalen Südens bedeutet diese Entwicklung die Fortschreibung eines (neo)kolonialen, extraktiven Wirtschaftsmodells. Hinzu kommt der enorme Energiebedarf, der bereits jetzt für die Digitalisierung benötigt wird und die Klimakrise weiter verschärft. Der Energieverbrauch der Digitalisierung verursacht weltweit bereits zwei bis vier Prozent der gesamten CO₂-Emissionen. Die Verteilung der Vorteile der Nutzung der digitalen Technologien sowie der Nachteile der ökologischen Verschmutzung und Auswirkungen des Klimawandels ist dabei weltweit enorm ungleich.

In der derzeitigen Art der kommerziell vorangetriebenen Digitalisierung geht es nicht per se darum, das Leben besser zu machen oder die Industrie effizienter. Sondern es geht den großen, dominanten Software-, Industrie- und staatlichen Akteuren in erster Linie darum, Märkte und Wettbewerbsvorteile für die Zukunft zu schaffen. Aber genau über die Richtung, die Technik im Kleinen und Digitalisierung im Großen einschlagen sollen, müssen wir mitbestimmen können. Wir brauchen eine nachhaltige Digitalisierung.

Nachhaltige Digitalisierung am Beispiel von Landwirtschaft 4.0

Wie das aussehen könnte, sei am Beispiel der Landwirtschaft skizziert. Dieses mag auf den ersten Blick überraschen, denkt man bei Digitalisierung doch selten an Land und Acker. Tatsächlich ist der Agrarbereich aber derzeit massiv im Fokus der digitalen Entwicklung. Die großen Agrochemie- und Landwirtschaftsmaschinenkonzerne verfolgen dabei die Vision einer voll integrierten und durchdigitalisierten Landwirtschaft. Dafür haben sich diese Akteure in den letzten Jahren umfassend aufgestellt und immer mehr aufgrund vertikaler Integrationsprozesse, sprich Zusammenschlüsse entlang der gesamten Wertschöpfungskette, vergrößert. So übernahm Monsanto beispielsweise 2013 das Software-Startup *Climate Corporation* und 2014 die Klima-App *Climate Basic* und das Unternehmen für Boden- und Saatgutanalyse *FieldScripts*, bevor Monsanto wiederum selbst mit dem deutschen Konzern Bayer verschmolz.

Zentrale Fragen aus landwirtschaftlicher und bäuerlicher Sicht sind bei der Digitalisierung der Landwirtschaft bisher ungeklärt: Wer hat die Hoheit über die Daten, die (beispielsweise durch GPS-gestützte Landmaschinen) erhoben werden? Welche Abhängigkeiten können und werden entstehen? Wie kann das bäuerliche Wissen erhalten und gepflegt werden? (Verbunden damit ist die Frage der Datenhoheit und Transparenz von Algorithmen.) Wie geht man mit rechtlichen Grundlagen zu Saatgut und genetischen Ressourcen um?

Zivilgesellschaftliche Organisationen schauen vermehrt auf diese Trends und haben Kernaspekte formuliert, damit eine digitale

Landwirtschaft zu den Zielen beiträgt, Hunger zu beenden, Armut zu reduzieren, Menschenrechte entlang der gesamten Lieferkette einzuhalten und die Umwelt sowie das Klima zu schützen.

1) Digitale Technologien müssen planetare Grenzen respektieren

Bauern und Bäuerinnen weltweit sind durch Ernteausfälle infolge von Dürren und Überschwemmungen in besonderem Maße von den Folgen der Klimakrise sowie von Bodendegradation und anderen ökologischen Krisen betroffen. Ihre Lebensgrundlagen sowie die Lebensmittelerzeugung für die Versorgung der Menschen weltweit hängen fundamental von einer intakten Umwelt ab. In Zeiten globaler Umwelt- und Klimakrisen ist es notwendig, den Ressourcenverbrauch und die negativen Umweltauswirkungen der industriellen Landwirtschaft zu minimieren.

Digitale Instrumente haben das Potential, den Austausch von bäuerlichem Wissen zwischen lokalen AkteurInnen deutlich zu verbessern, um so Krisen besser zu bewältigen. Positive Effekte auf Klima-, Arten- und Gewässerschutz konnten hingegen bislang nicht von unabhängiger Seite quantifiziert werden.

Im Rahmen einer umfassenden Technikfolgenabschätzung sollte deswegen geprüft werden, inwieweit sich die großflächige Anwendung digitaler Instrumente in der Landwirtschaft in einem potenziell weltweiten Maßstab innerhalb der planetaren Grenzen – vor allem in Bezug auf den Energie- und Ressourcenverbrauch – realisieren lässt. Angesichts der negativen Umweltauswirkungen und möglicher Folgen für die menschliche Gesundheit bleibt es von zentraler Bedeutung, die analoge Produktion von Lebensmitteln zu stärken.

2) Digitalisierung darf Oligopolbildung und Konzernmacht nicht verstärken

Mit der Digitalisierung könnte eine nie dagewesene Integration und Kooperation entlang der gesamten Agrarlieferkette vonstattengehen. Für den Betrieb von digitalen Plattformen schließen sich oft Konzerne aus drei Bereichen zusammen: Ein Landmaschinenhersteller mit umfassender Technik zur Datenerhebung, ein Datenunternehmen, das die gewaltigen Datenmengen rasch verarbeiten kann, und ein Saatgut-, Pestizid- bzw. Tierarzneimittelhersteller, der die Daten zu gezielter Werbung („Beratung“) und KundInnenbindung nutzt. Sowohl durch die anhand von Drohnen und Sensoren erhobenen Informationen über eingesetztes Saatgut, Dünger und Pestizide, Anbaumethoden auf ei-

nem Hof als auch durch die zunehmende Konzentration von Marktmacht erlangen einzelne Agrar- und Landmaschinenkonzerne zunehmenden Einfluss auf die globale Landwirtschaft.

Gleichzeitig befördert die Digitalisierung die Monopolbildung. Der daraus resultierende erschwerte Anbieterwechsel, hohe Anschaffungskosten, mangelnde Datenkompatibilität und ein erschwelter Zugang zu alternativen, von der Industrie unabhängigen Angeboten drohen die Abhängigkeit der Bäuerinnen und Bauern von wenigen Anbietern zu verstärken. Damit sinkt die Wahlfreiheit für Bäuerinnen und Bauern unter Umständen erheblicher, als dass die digitalen Anwendungen ihre Möglichkeiten erweitern.

Zur Begrenzung der Macht von Agrar- und Digitalkonzernen braucht es dringend eine Verschärfung des Wettbewerbsrechts in Deutschland und der Europäischen Union u. a. mit einer strenger Prüfung von Fusionen zwischen Unternehmen. Wenn die landwirtschaftlichen Daten über wenige, übergreifende Plattformen verwaltet werden, muss sichergestellt werden, dass die Daten sowie die Plattformen nicht von einigen wenigen Großkonzernen wie Bayer oder John Deere kontrolliert werden. Stattdessen sollten Staaten den Aufbau der nötigen Rechenzentren oder Clouds für konzernunabhängige Plattformen finanzieren.

3) Digitale Instrumente müssen sich an den Bedürfnissen von (Klein-)Bäuerinnen und Bauern ausrichten

Auch wenn künftig durch präzisere Maschinen und andere Innovationen (klein-)bäuerliche Betriebe in der Theorie technisch besser erreicht und effizienter bewirtschaftet werden können, werden sich viele (klein-)bäuerliche ErzeugerInnen in naher Zukunft die teuren und in der Anwendung voraussetzungsvollen Technologien kaum leisten können. Sowohl Farm-Tech-Start-ups als auch Agrarkonzerne fokussieren in erster Linie auf marktorientierte Betriebe, die in globale Lieferketten integriert und bereit sind, entsprechende Investitionen zu tätigen. Dies erfordert nicht nur hohe Ausgaben u. a. für Landtechnik, sondern auch hohe Alphabetisierungsraten, ein hohes Maß an digitalen Kenntnissen sowie eine Anbindung an Infrastruktur. Ein zentrales Problem besteht zudem in den steigenden Abhängigkeiten, beispielsweise von Reparaturdienstleistungen, die Bauern und Bäuerinnen an den hoch komplexen Maschinen nicht mehr selbst durchführen dürfen oder können und die zum Teil nur noch von lizenzierten Werkstätten übernommen werden können.

Bereits heute marginalisierte Kleinbauern und -bäuerinnen drohen, weiterhin abgehängt zu bleiben und die Kluft zwischen ih-



Marie-Luise Abshagen und Nelly Grotefendt

Marie-Luise Abshagen ist Referentin für Nachhaltige Entwicklung beim *Forum Umwelt und Entwicklung*.

Nelly Grotefendt ist Referentin für Politik, internationale Handelspolitik und Weltwirtschaft beim *Forum Umwelt und Entwicklung*.

nen und hochtechnisierten Großbetrieben könnte weiterwachsen. Hieraus könnten Risiken für die Ernährung der lokalen Bevölkerung resultieren, da kleinbäuerliche Betriebe vor allem in Ländern des globalen Südens einen Großteil der konsumierten Lebensmittel erzeugen. Eine an KleinerzeugerInnen ausgerichtete Digitalisierung kann daher nur in Kontexten funktionieren, die sich der dominanten Logik der Agrarindustrie entziehen.

Damit (klein)bäuerliche ErzeugerInnen tatsächlich von den digitalen Technologien profitieren können – zum Beispiel für eine bessere Vermarktung ihrer Erzeugnisse oder zur Erleichterung der Dokumentation ihrer Betriebstätigkeiten –, muss die Mindestanforderung sein, dass ihre Bedürfnisse bei der politischen und technischen Ausgestaltung der Digitalisierung berücksichtigt werden. Damit das gelingt, müssen sie oder ihre Organisationen systematisch beteiligt werden und mitentscheiden können.

nen. Auch unabhängig vom Digitalisierungstrend braucht es – entsprechend menschenrechtlicher Verpflichtungen – vor allem einen gesicherten Zugang zu Land, Wasser, nachbaufähigem Saatgut, Bildung und Weiterbildung sowie zu Krediten. Die Einführung digitaler Technik darf den Erhalt bäuerlicher, regionaler Saatgutssysteme nicht gefährden.

Referenzen

- 1 Für konkrete Forderungen entlang der 17 Sustainable Development Goals für eine nachhaltige Digitalisierung siehe <https://www.forumue.de/wp-content/uploads/2019/11/SDigiG-online.pdf>
- 2 Für Details zu den Forderungen siehe <https://www.forumue.de/digitalisierung-in-der-landwirtschaft-4-0/>



Bernhard Stoevesandt und Martin Dörenkämper

Wird KI die Welt retten?

Ein kritischer Beitrag über den Einsatz von KI in der klimarelevanten Forschung

In einem auf Arxiv.org vorveröffentlichten Artikel mit dem Titel Tackling Climate Change with Machine Learning wird nahegelegt, wie wichtig doch künstliche Intelligenzsysteme zur Eingrenzung der Klimaveränderungen seien [1]. Die AutorInnen kommen alle aus dem Bereich Machine Learning und forschen an entsprechenden Systemen. Warum sollte ihre Arbeit nicht dafür eingesetzt werden eines der drängendsten Themen, wenn nicht das drängendste Thema der Menschheit, zu bearbeiten? Ist es da nicht geradezu geboten, solche Systeme weiterzuentwickeln, um am Ende die Welt zu retten? Um die Frage zu beantworten, sollte zuerst betrachtet werden, wie groß das Problem des vom Menschen verursachten Klimawandels eigentlich ist.

Wie kommt es zur Veränderung des Klimas durch den Menschen? Die Ursache ist lang diskutiert: Der Mensch verursacht eine Veränderung der Zusammensetzung der Gase in der Atmosphäre. Die Gase und Aerosole in der Atmosphäre führen ganz natürlich zu einem Treibhauseffekt: Die Sonne strahlt im Mittel eine Energie von $341,3 \text{ Wm}^{-2}$ ein, von denen fast 102 Wm^{-2} direkt wieder reflektiert werden. Der Rest wird von der Erde aufgenommen. Dadurch erwärmt sich die Erde, was zu einer Wärmeabstrahlung in einem anderen Wellenlängenbereich führt. Diese Wärmestrahlung wird nun von den Gasen in der Atmosphäre zum Teil wieder aufgenommen und zurück zur Erde gestreut. Dies ist der sogenannte Treibhauseffekt, ohne den die Erde für Menschen fast unbewohnbar wäre, weil die mittlere Temperatur viel zu niedrig wäre [2]. Das Problem besteht nun darin, dass die Veränderung der Zusammensetzung der Atmosphäre dazu führt, dass manche Wärmestrahlung, die wegen ihrer Wellenlänge von der Atmosphäre nicht aufgenommen worden wäre und damit ins Weltall ginge, nun von diesen Gasen

aufgenommen und zurück gestreut werden können. Dies führt dazu, dass etwas mehr Energie in der unteren Atmosphäre verbleibt und sich die Erde erwärmt [2].

Die hauptverantwortlichen Gase haben sich, wie in Tabelle 1 dargestellt, über die Jahre deutlich erhöht [3]. Während alle anderen vom Menschen direkt oder indirekt emittierten Treibhausgase – es wird von anthropogenen Treibhausgasen gesprochen – mit der Zeit zerfallen, verbleibt das CO_2 . Es wird nur von Pflanzen wieder abgebaut. Daraus lässt sich ein Treibhauspotenzial der jeweiligen Gase und deren Beitrag zur Erwärmung der Erde errechnen.

Nun sind die klimatischen Verhältnisse ein komplizierter Prozess mit vielen Wechselwirkungen: Wärme wird von den Ozeanen absorbiert, diese verdunsten mehr Wasser, was zu mehr Wolken führen kann, die wiederum mehr Wärme aufnehmen, aber auch mehr Sonnenstrahlung reflektieren können. Eine wärmere Atmosphäre führt zu einem Abschmelzen von Meer- und

	Kohlendioxid	Methan	Distickstoffoxid	FCKW-12
Vorindustrielle Konzentration	280 ppm	730 ppb	270 ppb	0
Konzentration 2016	403 ppm	1843 ppb	329 ppb	512,5 ppt
Verweilzeit in Jahren	?	9,1	123	102
Treibhauspotenzial	1	25	298	5200
Strahlungsantrieb in W/m^2	1,82	0,48	0,17	0,17

Tabelle 1: Zunahme der durch Menschen abgegebenen klimaverändernden Gase, ihr Treibhauspotenzial und ihre Verweilzeit in der Atmosphäre

Ungefähre Erwärmung seit 1850-1900 in °C	Verbleibendes CO ₂ Budget (ohne Rückkopplungen durch das Erdsystem) in GtCO ₂ seit 1. Januar 2018			Geschätzte Emission durch Rückkopplung des Erdsystem
	Wird mit 33 % Wahrscheinlichkeit	50 % Wahrscheinlichkeit	67 % Wahrscheinlichkeit erreicht	In GtCO ₂
1,5	840	580	420	100
1,75	1440	1040	800	
2	2030	1500	1170	
2,1	2270	1690	1320	

Tabelle 2: Verbleibende Menge an CO₂ Emissionen um mit einer gegebenen Wahrscheinlichkeit unter einer bestimmten Erwärmung zu bleiben (nach [5], wobei im Original noch Unsicherheiten angegeben sind). Die rechte Spalte gibt die bis zum Ende des Jahrhunderts zusätzlich freigesetzte CO₂-Menge durch das Erdsystem, durch die Erwärmung selbst, an.

Gletschereis, wodurch weniger Sonnenlicht reflektiert wird, dafür wachsen in manchen Regionen Pflanzen besser durch mehr CO₂. Dies und vieles mehr spielt in die Betrachtung der Klimamodelle mit ein [4]. Während frühere Modelle nur auf die Energiebilanz eingingen, enthalten heutige Modelle zur Berechnung des Klimas sehr viele Details des Erdsystems, die einen Einfluss auf das Klima haben. Entscheidend ist: Bevor ein Modell auf die Berechnung zukünftiger Situationen angesetzt wird, muss es erst an Klimasituationen der Vergangenheit zeigen, dass es diese mit einer vorhersagbaren Genauigkeit berechnen kann.

Das Resultat sind Tabellen wie bspw. im IPCC-Report von 2018 zu den Möglichkeiten und Folgen die Erderwärmung bis 2100 auf 1,5°C bzw. 2°C im Vergleich zur Zeit vor 1900 zu begrenzen. Tabelle 2 gibt die Zahlen der maximal noch emittierbaren sogenannten CO₂-Äquivalente (wenn alle Klimagase auf die Wirkung von CO₂ umgerechnet werden) in Milliarden Tonnen (Gt) an:

Vor dem Hintergrund, dass zwischen 2011 und 2017 die mittlere Emission von Klimagasen 42 GtCO₂ entsprach, 100 GtCO₂ durch die Erde bis Ende des Jahrhunderts wegen der Erwärmung abgegeben werden. Würden ab 2018 nur noch 320 GtCO₂ global zu emittieren sein, um „wahrscheinlich“, also mit 67 % Wahrscheinlichkeit unter 1,5°C zu bleiben. In 2017 hatten davon schon zugelassene Kohlekraftwerke 200 GtCO₂ eingeplant und es waren Kohlekraftwerke in Planung oder Bau für 100-150 GtCO₂-Emissionen ([5] Seite 113). Aus diesen Zahlen geht hervor, dass ohne eine sofortige drastische Reduktion der globalen Emissionen ein 1,5°C-Ziel nicht erreicht werden kann.

Doch was bedeutet es, wenn das Ziel nicht erreicht wird? Im IPCC Report von 2018 sind die Folgen in Kapitel 3 ausführlich dargestellt, in Tabelle 3 seien nur einige aufgeführt.

Region	Erwärmung < 1,5°C	Erwärmung 1,5-2°C	Erwärmung 2-3°C
Arktisches Meereis	Sommermeereis bleibt wahrscheinlich bestehen	50 % aus eisfreien Sommer	Eisfreie Sommer in der Arktis sehr wahrscheinlich
Arktisches Land	Permafrost Auflösung wahrscheinlich	größerer aber noch begrenzter Verlust an Permafrost wahrscheinlich	Ein Kollaps des Permafrosts kann plausibel auftreten (niedrige Wahrscheinlichkeit)
Südostasien	Risiken durch wesentliche Reduktionen an Ernteerträgen vermieden	Verminderung der Pro-Kopf-Ernteerträge um ein Drittel (50 % Wahrscheinlichkeit, -MW)	Substanzielle Reduktion von Ernteerträgen
Mittelmeer Region	Reduktion von Fließwasser 9 % (Wahrscheinlicher Bereich: 4,5-15,5 %)	Hohe Wahrscheinlichkeit der Reduktion von Fließwasser (ca. 17 %) (Bereich 8-28 %)	Robuste und große Zunahme von starken Dürren. Substanzielle Abnahme von Niederschlag und Fließwasser (MW)
West Afrika und Sahel	Reduktion der Fläche die für Maisanbau geeignet ist um bis zu 40 %	Negative Folgen auf Mais und Sorghum Produktion wahrscheinlich größer als bei 1,5°C	Negative Auswirkungen auf Ernteerträge kann zu großen regionalen Ernährungsproblem führen (MW)
Tropen	Risiken für tropische Ernteerträge in West Afrika, Südostasien und Südamerika deutlich unter denen bei 2°C Erwärmung.	Risiken für tropische Ernteerträge in West Afrika, Südostasien und Südamerika können sehr weitgehend sein.	Substanzielle Reduktion von Ernteerträgen sehr wahrscheinlich.
Kleine Inseln (tropisch) (SIDS)	60.000 weniger Menschen verlieren ihr Land bis 2150 im Vergleich zu 2°C.	Zehntausende vertrieben durch Untergang der Inseln. Hohes Risiko von Überschwemmungen.	Substanzielle und weit verbreitete Auswirkungen durch Untergang von SIDS.

Tabelle 3: Auszüge aus einer Tabelle im IPCC Report von 2018 in Kapitel 3 zu Folgen der Klimaveränderungen bei unterschiedlichen Temperaturanstiegen [5]. Die Originaltabelle ist deutlich umfassender, würde aber den Rahmen dieses Artikels sprengen.

Aus diesem Grund sehen alle Szenarien zur Erreichung des Ziels, die Erwärmung bis Ende des Jahrhunderts auf 1,5°C zu begrenzen, auch Maßnahmen zu Reduktion von CO₂ in der Atmosphäre vor. Dazu werden verschiedene Techniken diskutiert.

Die Einfachste ist die, Landfläche anders zu nutzen, vor allem durch Bewaldung. Pflanzen, insbesondere Bäume können viel CO₂ binden. Die Schwierigkeit ist nur, dass die Fläche, die eine Bewaldung zulässt, begrenzt ist. Daher ist nur ein eingeschränkter Effekt möglich. Aus dem Grund werden auch technische Wege zur CO₂-Reduktion vom IPCC diskutiert. Besonders genannt werden dabei die Verfahren *Bioenergy with Carbon Capture and Storage* (BECCS) und *Direct Air Carbon Capture and Storage* (DACCS). In beiden Verfahren wird CO₂ gewonnen und mittels Carbon Capture and Storage irgendwie endgelagert. Das zurzeit verfügbare Verfahren sieht eine Verpressung des Gases in den Boden vor. Es wird davon ausgegangen, dass das CO₂ über 10000 Jahre zu 98 % bei „gut geführten Speichern“ und zu 78 % bei „schlecht geführten Speichern“ im Speicher verbleibt ([5] in Kapitel 4.3.1). Bei BECCS wird das CO₂ dadurch gewonnen, dass es bei der Verbrennung von Biomasse, z.B. Biogas abgeschieden wird. Um bspw. 15 GtCO₂ im Jahr abzuscheiden, würden dafür 25-46 % der landwirtschaftlich nutzbaren Fläche benötigt ([5] in Kapitel 4.3.7). DACCS scheidet dagegen das CO₂ direkt aus der Luft ab. Das Verfahren ist allerdings energieintensiv. Um wiederum 15 GtCO₂ pro Jahr abzuscheiden wären ca. 25 % des globalen Energieverbrauchs notwendig.

Vor diesem Hintergrund werden in dem Report von 2018 sieben zentrale Maßnahmen vorgeschlagen [5]:

1. Schnelle und tiefgreifende Decarbonisierung der Energieversorgung,
2. stärkere Bemühungen, den Verbrauch zu reduzieren,
3. die umfassende Reduktion der Emission wird im nächsten Jahrzehnt umgesetzt,
4. es gibt einen wesentlichen Wechsel im Investitionsverhalten weg von CO₂ emittierenden Technologien,
5. eine Verbindung von CO₂-Reduktion mit nachhaltiger Entwicklung verbessert die Chancen der CO₂-Reduktion,
6. umfassende Maßnahmen, um CO₂ in der Atmosphäre zu reduzieren, und
7. ein Wechsel von fossilen Energieträgern auf Strom.

All dies bedeutet, dass es einen großen gesellschaftlichen Wandel aufgrund des sich verändernden Klimas geben wird, und,

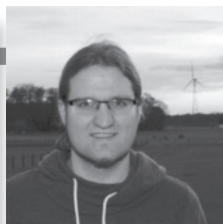
dass es einen großen und schnellen gesellschaftlichen Wandel geben muss, um die Veränderung des Klimas zu begrenzen.

Auf diesen Zusammenhang hebt nun der Artikel von Rolnick ab, wenn er über die Nutzung von KI im Rahmen der Klimaveränderungen spricht [1]. Darin werden sehr unterschiedliche Bereiche betrachtet, wie KI im Rahmen der Klimaveränderung eingesetzt werden könnte. Dabei lassen sich drei wesentliche Einsatzgebiete unterscheiden:

1. Einsatz von KI in der Entwicklung von Klimamodellen und Szenarien.
2. Einsatz von KI für die Beherrschung der sozialen Folgen durch den Klimawandel.
3. Nutzung von *Machine Learning* zur Verbesserung von Vermeidungsstrategien.

Bei der Entwicklung von Klimamodellen oder der Berechnung der Szenarien aus den Klimamodellen kommt KI bisher kaum zum Einsatz. Ein Hauptproblem dabei ist, dass *Machine-Learning*-Methoden am Ende eine Art *Black-Box* sind. Warum das Programm schließlich zu einem Ergebnis kommt, ist selten nachvollziehbar. Aus den Klimamodellen folgen aber weite Folgen für die Gesellschaft. Deshalb werden die Berechnungen immer wieder in Frage gestellt und müssen die größtmögliche Nachvollziehbarkeit haben. Daher kommt KI in diesem Bereich höchstens dafür in Frage, Randbedingungen für die eigentlichen Rechnungen zu ermitteln (z.B. verbesserte Rechengitter). Ob hier KI anderen Methoden überlegen ist, und wie groß der Effekt auf die Ergebnisse ist, ist noch offen.

Machine-Learning-Methoden werden bei der Bestimmung lokaler Folgen der globalen Klimamodelle eingesetzt. Dies geschieht z.B. bei der Bestimmung von lokalen Extremereignissen. Allerdings liegen hierfür inzwischen auch andere leistungsfähige Methoden vor, so dass Machine Learning hier keine Notwendigkeit darstellt [6]. Im Bereich der Beherrschung der sozialen Folgen wird inzwischen über verschiedene Einsatzmöglichkeiten von KI diskutiert. Wie diese ethisch zu bewerten sind, ist eine andere Frage. Dazu gehören: Berechnung von Katastrophenszenarien, wie bspw. Fluchtverhalten bei Hochwasserkatastrophen, Wirtschaftsmodellrechnungen für Wirtschaft bei Klimawandel, Fluchtroutenberechnungen oder Mustererkennung bei ökologischen Messungen. Abgesehen vom letzten Punkt scheinen die Entwicklungen von Machine-Learning-Prozessen in diesem Anwendungsgebiet noch nicht weit entwickelt zu sein. Zumindest wird die Anwendung von Rolnick et al. nur vorgeschlagen.



Bernhard Stoevesandt und Martin Dörenkämper

Dr. **Bernhard Stoevesandt** ist promovierter Physiker am Fraunhofer-Institut für Windenergiesysteme (IWES). Seine Abteilung für Aerodynamik, numerische Strömungsberechnungen und stochastische Dynamik beschäftigt sich im Schwerpunkt mit numerischen Methoden zur Beschreibung von nicht-linearen Systemen. Er engagiert sich u. a. bei *Scientists4Future*.

Dr. **Martin Dörenkämper** ist Meteorologe, hat zum Thema Energiemeteorologie promoviert und arbeitet jetzt als PostDoc im Bereich Windenergieforschung am Fraunhofer-Institut für Windenergiesysteme (IWES). Er engagiert sich u. a. bei *Scientists4Future*.

Der Bereich, in dem die Methoden tatsächlich zum Einsatz kommen, ist allerdings der zur Reduktion von CO₂-Emissionen – bei konkreten industriellen Prozessen. Hier werden KI-Methoden zur Vorhersage von Einspeisung erneuerbarer Energien genutzt, oder zur Optimierung von industriellen oder landwirtschaftlichen Prozessen um CO₂-Ausstoß zu mindern. Modelle zu Berechnungen zur Reduzierung von Transportaufkommen sind ebenfalls in Arbeit. Allerdings gilt für all diese Anwendungsgebiete: Es gibt auch immer alternative Ansätze zu Machine Learning, die meist direkt physikalisch basiert sind. KI ist nicht alternativlos. Daher lässt sich klar sagen: Im Bereich des Klimawandels wird KI die Welt nicht retten. Das müssen die Menschen schon selbst tun. Diese Methoden können ein Werkzeug sein, allerdings sind sie nicht ohne Alternativen.

Referenzen

- [1] David Rolnick, Priya L. Donti, Lynn H. Kaack, Kelly Kochanski, Alexandre Lacoste, Kris Sankaran, Andrew Slavin Ross, Nikola Milojevic-Dupont, Natasha Jaques, Anna Waldman-Brown, Alexandra Luccioni, Tegan Maharaj, Evan D. Sherwin S., Karthik Mukkavilli, Konrad P. Körding, Carla Gomes, Andrew Y. Ng, Demis Hassabis, John C. Platt,

- Felix Creutzig, Jennifer Chayes, Yoshua Bengio, „Tackling Climate Change with Machine Learning“, Pre-Print, Arxiv.org, 1906-05433v2.
- [2] Trenberth, K. E., 2009: An imperative for adapting to climate change: Tracking Earth's Global Energy. Current Opinion in Environmental Sustainability, 1, 19-27. DOI 10.1016/j.cosust.2009.06.001
- [3] Blunden, J., D. S. Arndt, and G. Hartfield, Eds., 2018: State of the Climate in 2017. Bull. Amer. Meteor. Soc., 99 (8), Si–S332, doi:10.1175/2018BAMSStateoftheClimate.1.
- [4] IPCC, Climate Change 2013, The Physical Science Basis, Working Group I Contribution to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change; eds. Thomas F. Stocker et al., ISBN 978-1-107-05799-1, 2013
- [5] IPCC, GLOBAL WARMING OF 1.5°C, an IPCC special report on the impacts of global warming of 1.5°C above pre-industrial levels and related global greenhouse gas emission pathways, in the context of strengthening the global response to the threat of climate change, sustainable development, and efforts to eradicate poverty, IPCC 2018
- [6] Francesco Ragone, Jeroen Wouters, and Freddy Bouchet. “Computation of extreme heat waves in climate models using a large deviation algorithm.” Proceedings of the National Academy of Sciences 115.1 (2018): 24-29.



Arkadi Schelling

Arbeitsgruppe: Demokratie und Überwachungskapitalismus

Psychometric Profiling beschreibt eine Technologie, mit der das Onlineverhalten von vielen Millionen Menschen verfolgt wird, um ihre Psychologie zu klassifizieren und sie zu beeinflussen. Der berüchtigtste und best dokumentierte Fall bisher war die Wahlkampagne von Donald Trump durch Cambridge Analytica.

Dieser interaktive Workshop förderte das Verständnis der zugrunde liegenden Technologien und Theorien, wie Psychologie, Informationstechnik und Statistik, sowie der hinter Psychometric Profiling stehenden Gesellschaftsmechanismen und Interessengruppen. Für ein tiefgreifendes und praktisches Verständnis haben wir Selbstexperimente durchgeführt, politische Botschaften auf Zielgruppen zugeschnitten und eigene Vorhersagen psychologischer Eigenschaften aufgrund von Facebook-Likes erstellt. Dafür teilten sich die etwa 30 Teilnehmenden in verschiedene Arbeitsgruppen auf und brachten ihre Ergebnisse als Fragen in die gesamte Gruppe zurück. Für eine gemeinsame Diskussion blieb im ersten Teil des Workshops wenig Zeit. Der fakultative zweite Teil des Workshops lag parallel zum nächsten Vortrag und wurde noch von etwa zehn Personen besucht. Das ursprünglich geplante Angebot an die Teilnehmenden, sich Handlungsperspektiven anhand von verschiedenen Materialien in einem Medienparcours zu erarbeiten, wurde verworfen. Stattdessen bestand ein Wunsch nach ausgiebiger Diskussion

zu den vorher aufgeworfenen Fragen, die sich über eine gute Stunde erstreckte. Zentral waren dabei Fragen ob Psychometric Profiling wirklich effektiv genutzt wurde und wird, oder ob es sich nur um ein gutes Marketing handelt. Weiterhin wurden Wege angedacht, wie mit dieser neuen Technologie umgegangen werden kann.

Der Workshop fand in dieser Form zum ersten Mal statt und war eigentlich als Tagesworkshop konzipiert. Gemeinsam mit technischen Schwierigkeiten bei den Programmieraufgaben führte das zu einigen Ecken. Dennoch kam positives Feedback von vielen Teilnehmenden über das Facettenreichtum und die praxisorientierten Gruppen.

Referenzen

Material zu Arbeitsgruppe: https://github.com/arksch/psych_prof



Arkadi Schelling



Arkadi Schelling ist Mathematiker und Machine-Learning-Entwickler. Er war für die Entwicklung von Energiespar-Algorithmen und ortsbasierte Werbung angestellt und arbeitete danach an der Universität Bremen. Er ist seit Kurzem als Entwickler im Bereich Sensoranalyse und Energieeffizienz tätig. Seit seinem Ausflug in die Industrie setzt er sich kritisch mit privatwirtschaftlicher Überwachungstechnologie auseinander und interessiert sich in seiner Freizeit für politische Themen rund um Maschinelles Lernen.

Arbeitsgruppe: Nachhaltigkeitskultur in der Informatik

Um dem Klimawandel etwas entgegenzusetzen, ist Nachhaltigkeit mit ihren ökologischen, ökonomischen und sozialen Dimensionen eine der großen gesellschaftlichen Herausforderungen unserer Zeit. Digitalisierung wird in der Einhaltung der Nachhaltigkeitsziele in verschiedenen Bereichen eine bedeutende Rolle spielen. Digitalisierung ist aber auch ein wesentlicher Teil des Problems. „Wenn wir die Digitalisierung unverändert fortsetzen, wird sie zum Brandbeschleuniger für die ökologischen und sozialen Krisen unseres Planeten“, hat dies Bundesumweltministerin Svenja Schulze (Schulze 2019) sehr treffend zusammengefasst. Unter dem Thema Green IT werden schon seit Längerem verschiedene Dimensionen von Nachhaltigkeit bezogen auf IT diskutiert und nun auch von der Bundesregierung als ein Faktor zur Erreichung von Klimazielen genannt: „Fortschritte im Bereich der Green IT sind erforderlich, um den Energieverbrauch digitaler Technologien zu begrenzen.“ schreibt z. B. das BMWi in seinem Eckpunktepapier für ein Klimaschutzprogramm 2030, das im September 2019 vom Bundeskabinett beschlossen wurde (BMWi 2019). Im Rahmen des Workshops wurde die Entwicklung einer Nachhaltigkeitskultur in der Informatik diskutiert mit dem Blick auf ökologische Nachhaltigkeit.

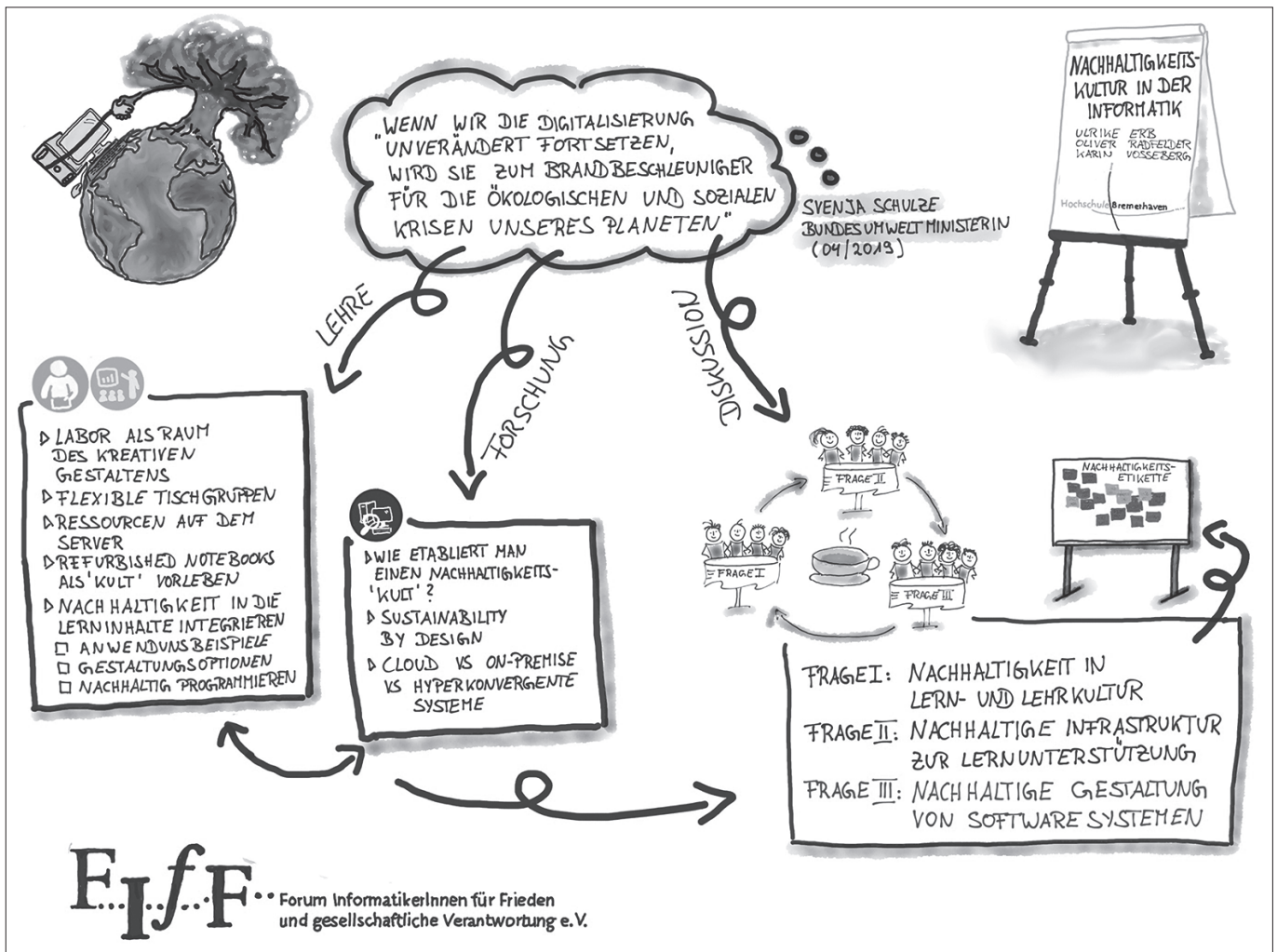


Abbildung 1: Zusammenfassung des Workshops

Aspekte einer Nachhaltigkeitskultur in der Informatik

Im Unterschied zu den unter KlimaschützerInnen zum Teil umstrittenen Bestrebungen, durch Digitalisierung Ressourcen einzusparen, z. B. durch Videokonferenzen oder E-Autos, interessieren uns Möglichkeiten, in der Informatik selbst nachhaltiger zu handeln. Wie können wir insbesondere in und durch unsere Hochschullehre und Lernkulturen umweltbewusste Ressourcenschonende Haltungen und Verantwortungsbewusstsein bei unserem Tun als InformatikerInnen stärken? Dabei sehen wir verschiedene Ansatzpunkte:

Lernumgebungen in PC-Laboren

Informatikstudierende benutzen heutzutage ihre eigenen Notebooks auch während der Veranstaltungen an der Hochschule. Feste Arbeitsplatzrechner werden in den Laboren immer seltener von Studierenden benötigt, verursachen aber hohe ökonomische und ökologische Kosten, insbesondere wenn sie routinemäßig nach wenigen Jahren gegen die neueste Technik ausgetauscht werden. Die Umgestaltung unserer Lernumgebungen in den PC-Laboren ist von der Leitidee geprägt, mit minimalistischer Technik auszukommen. Anstelle von Tischreihen mit PCs, hinter denen die Studierenden verschwinden, sind in den PC-Labo-

ren Tischgruppen aufgebaut, die sich für Gruppenarbeit eignen. An den Tischgruppen gibt es Auflademöglichkeiten und Netzzugänge und idealerweise einen großen Bildschirm zur gegenseitigen Präsentation der Arbeitsergebnisse.

Statt fest installierter Arbeitsplatzrechner halten wir einige *Refurbished* Notebooks zum Ausleihen bereit, also generalüberholte Gebrauchtgeräte. Diese Art von Geräten mit Ressourcensparenden Linux-Betriebssystemen und einer Basis-Ausstattung von Open-Source-Software empfehlen wir ebenso den Studierenden bei Beginn des Studiums.

Damit Studierende trotz bisweilen leistungsschwächerer Endgeräte auf aktuellen Programmiermodellen arbeiten können, wurde eine zentrale, recht großzügig ausgebaute Server-Infrastruktur konzipiert und von Lehrenden und wissenschaftlich-technischen MitarbeiterInnen gemeinsam mit Studierenden in einer Infrastrukturgruppe aufgebaut. Die Server-Infrastruktur besteht ebenfalls aus Refurbished-Beständen. Die Technologien, die uns das ermöglichen, sind Virtualisierung und Containerisierung. So haben beispielsweise alle Studierenden vom ersten Semester an eine kleine Docker-Umgebung, die über das Web erreichbar ist und in der sie tatsächlich als Cloud-Natives arbeiten können, weil sie so zugleich die Grundlagen und Arbeitsumgebungen moderner Cloud-Architekturen kennenlernen. Dass sie das mit eher klassischen Werkzeugen (*ssh*, *bash*, *vim* und *cgi*) vollbringen, ermöglicht wiederum eine schlanke und damit Ressourcenschonende Arbeitsweise. So laufen bei uns problemlos mehrere Hundert Container inklusive eigenem Webserver auf einem einzelnen mittelgroßen Server.

Die Infrastrukturgruppe ist damit ein außercurricularer Lernort, an dem eine Nachhaltigkeitskultur geprägt wird. Lehrende verstetigen die angestrebte *Kultur*, indem sie selbst auf neue Notebooks verzichten und generalüberholte Notebooks der gleichen Art einsetzen, wie sie den Studierenden empfohlen werden. Lehrende zusammen mit den wissenschaftlich-technischen MitarbeiterInnen und den Studierenden aus der Infrastrukturgruppe dienen als Rollenmodelle für einen nachhaltigen Umgang mit eingesetzter Hardware.

Lerninhalte

In diverse Aufgabenstellungen der Informatik lassen wir Themen einfließen, die sich auf ökologische Folgen der Digitalisierung und Ressourcenschonende Technikgestaltung beziehen. So haben wir während der hochschulweiten Klimawoche im Oktober 2019 den Erstsemester-Teams aus der Studieneingangsphase (STEP) die Aufgabe gestellt, einen kleinen Web-basierten CO₂-Fußabdruckrechner zu programmieren, mit dem eine Woche lang der Energieverbrauch der digitalen Aktivitäten der Teammitglieder und die damit einhergehenden CO₂-Emissionen aufgezeichnet werden. Mit dieser Aufgabe konnten die Studierenden für den Energieverbrauch ihres Handelns sensibilisiert werden.

Ausgehend von Aussagen wie: Die Stromproduktion für die Übertragung von 1 GB Datenvolumen verursacht einen Ausstoß von ungefähr 7 kg CO₂ (vgl. Christie 2013), sollten die Studierenden auch weitere CO₂-Kosten der Datenübertragung (wie Download, Videostreaming, Suchanfragen, Mails usw.) recherchieren. Die meisten waren erstaunt über die Energieintensität der Internetnutzung und sehen ein

„Hauptproblem darin, dass die Menschen ihren eigenen CO₂-Fußabdruck komplett unterschätzen. Dies wurde auch insbesondere uns als Team im Rahmen der Aufgabe zum Berechnen des CO₂-Fußabdrucks bewusst, nämlich dass wir mit nur acht Personen in einer Woche bereits mehrere Tonnen CO₂ produziert haben.“
(STEP-Team 07)

Wenn einem diese Tragweite nicht bewusst ist, kommt man auch nicht auf die Idee, sich Ressourcensparend zu verhalten, so ihre Befürchtung (siehe Abbildung 2).

Auch bei den Erstsemestern im Studiengang *Digitale Medienproduktion* spielt das Thema Nachhaltigkeit eine Rolle bei der Semesteraufgabe: Es soll eine interaktive kartenbasierte Anwendung entwickelt werden, die klimarelevante Informationen darstellt. Von Konzepten zum Teilen und Tauschen von Lebensmitteln oder Kleidung, über Karten mit Routen und Verkehrsmitteln zur ökologischen Fortbewegung, bis hin zu Karten, auf denen

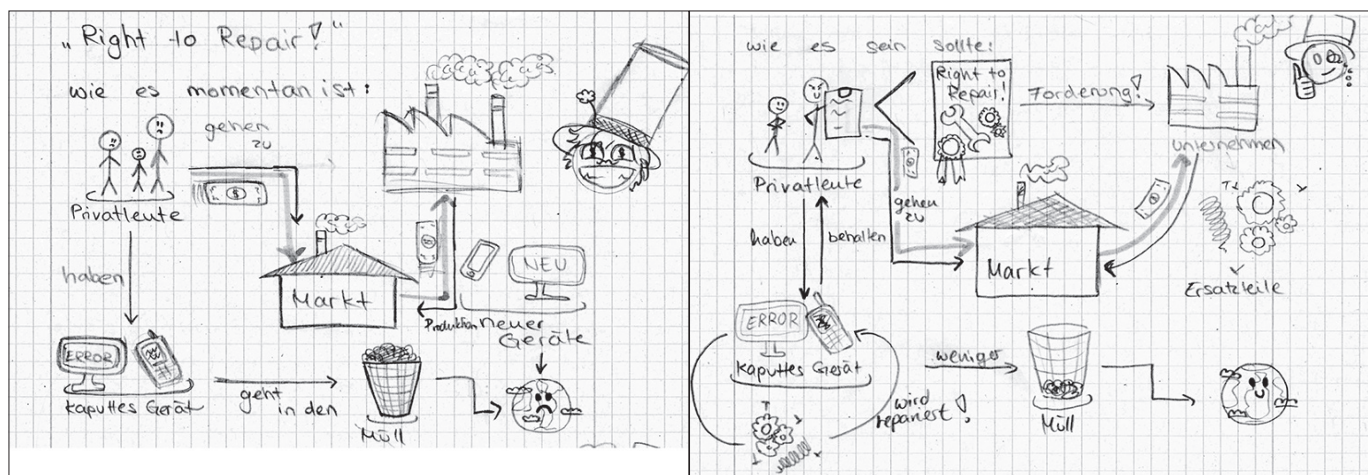


Abbildung 2: Zusammenfassung der Diskussionen zur Nachhaltigkeit von STEP-Team 11 (Quelle: STEP-Team 11)

klimafreundliche Aktionen und Events angezeigt werden können, werden vielfältige Prototypen zum Thema entwickelt und Teams die interessante Diskussionen führen.

Ressourcen-sparende Systemgestaltung

Fortwährend komplexer werdende Frameworks, Entwicklungsumgebungen und Architekturen prägen den Stand der Softwareentwicklung der vergangenen Jahre. Dass all dies mit dem Anspruch geschieht, Komplexität bei der Entwicklung zu verringern, tut der Entwicklung keinen Abbruch. Kürzere Entwicklungszyklen unter der Maßgabe *kontinuierlicher Verbesserung* und *Offenheit für Veränderung* haben die Software-Entwicklungskultur grundsätzlich verändert. Kurzfristige Kosten-, Zeit- und Risikominimierung prägen den kaum mehr in Frage gestellten Diskurs der Systementwicklung. Nachhaltigkeit spielt hier keine Rolle – weder im Sinne von lang in die Zukunft gedachten stabilen Softwarekomponenten noch im Sinne einer durchdachten ökologischen Vertretbarkeit.

Es braucht Zeit zum Nachdenken und Evaluieren, um den passenden Algorithmus und die angemessene Architektur für eine gegebene Aufgabenstellung zu finden, wenn nicht lediglich die menschliche Arbeitszeit als Kostenfaktor einfließt, sondern auch die benötigten Ressourcen. Hier ist gegebenenfalls auch der Unterschied zwischen *Bootcamp*-Mentalität zur Schnellaneignung aktueller Frameworks und informatischer Hochschulausbildung einzuordnen.

Ergebnisse des Workshops

In kleinen *World-Café*-Runden zu den drei Fragestellungen

- Wie können wir eine Nachhaltigkeitskultur in Lehr- und Lernumgebungen der Informatikausbildung verankern?

- Wie können nachhaltige Infrastrukturen zur Lernunterstützung aussehen?
- Wie können wir Prinzipien der Nachhaltigkeit bei der Gestaltung von IT-Systemen aufgreifen?

haben wir gemeinsam diskutiert, wie wir eine Kultur der Nachhaltigkeit in der Informatik vorantreiben können.

Die Ergebnisse stellen wir im Folgenden dar.

Nachhaltigkeitskultur in Lehr- und Lernumgebungen

Um nachhaltige Lernkulturen in der Informatik zu verankern, muss sich Nachhaltigkeit in der Haltung von Lehrenden und Lernenden widerspiegeln. Dazu wurde in der Diskussionsrunde vorgeschlagen, Nachhaltigkeit im Curriculum zu verankern und eine Lernatmosphäre zu fördern, die zur Reflektion über Ressourcen-sparendes, die Umwelt schonendes Handeln in der Informatik anregt. Als ein Beispiel wurde genannt, einen Umgang mit Software zu vermitteln, bei dem *hinter* die Software geschaut und ihr Funktionieren anhand des Quellcodes erläutert wird. Entsprechend sollte darauf geachtet werden, dass der Quellcode offen und eine Dokumentation verfügbar ist. Es wurde daher dafür plädiert, in der Lehre vor allem freie Software zu nutzen, die auch auf eigenen Rechnern genutzt werden kann.

Allerdings gibt es einige Informatikbereiche, in denen die Nutzung proprietärer Software üblich ist. Diese wird zwar in den Laboren mit Campuslizenzen zur Verfügung gestellt. Die Lizenzen sind aber nicht auf die Notebooks der Studierenden übertragbar. Als ein erster Schritt in Richtung Nachhaltigkeitskultur wurde diesbezüglich gefordert, dass Studierenden in Prüfungen auch Alternativen zur Nutzung proprietärer Software ermöglicht werden sollten. In den Lehrveranstaltungen sollten zudem alternativ zu proprietärer Software auch freie Lösungen vorgestellt

Ulrike Erb, Oliver Radfelder, Karin Vosseberg

Prof. Dr.-Ing. **Ulrike Erb** ist seit 2003 Professorin an der *Hochschule Bremerhaven*, wo sie in den Informatikstudiengängen sowie im Studiengang Digitale Medienproduktion in den Bereichen Software und Media Engineering unterrichtet und nachhaltiges Design als wichtiges Qualitätskriterium ansieht. Die Vermittlung der sozialen Verantwortung von Informatikerinnen und Informatikern ist ihr ein besonderes Anliegen.

Weitere Informationen unter: <https://informatik.hs-bremerhaven.de/uerb>.

Oliver Radfelder ist seit 2016 Professor in den Studiengängen Informatik und Wirtschaftsinformatik an der *Hochschule Bremerhaven*. Seinen Schwerpunkt in der Lehre legt er auf den bewussten Umgang mit Systemkomplexität. In diesem Sinne setzt er konsequent auf Open-Source-Software, um eine Kultur des Verstehens und Teilens von Wissen unter Studierenden zu befördern.

Weitere Informationen unter: <https://informatik.hs-bremerhaven.de/oradfelder>.

Karin Vosseberg ist seit 2009 Professorin in den Studiengängen Informatik und Wirtschaftsinformatik an der *Hochschule Bremerhaven*. Ihr Interessensschwerpunkt liegt auf Qualität von Software, insbesondere den konstruktiven und analytischen Maßnahmen zur Qualitätssicherung. Gemeinsam mit den KollegInnen aus dem Studienbereich Informatik möchte sie eine Lernumgebung schaffen, in der sich die Studierenden verantwortungsvoll mit ihrem Fach und der Fachkultur auseinandersetzen.

Weitere Informationen unter: <https://informatik.hs-bremerhaven.de/kvosseberg>.

und abgewogen werden, ob nicht auch weniger Umfang der Software für das gleiche Anwendungsgebiet ausreichend ist.

Zusammenfassend wurde bei diesem World-Café eine nachhaltige Lehr-/Lernkultur der Informatik im doppelten Sinn ausgelegt:

- Software sollte nachhaltig nutzbar sein, d. h. frei und ohne Lizenzkosten,
- Software sollte verstehbar sein, d. h. mit transparentem Quellcode, Open Source und mit guter Dokumentation.

Ein Verständnis des Quellcodes und der Architekturen der entwickelten und genutzten Software-Anwendungen ermöglicht nicht zuletzt bessere Anpassbarkeit, Wartbarkeit und Optimierungsmöglichkeiten und damit einen Ressourcen-sparenderen und längeren Software-Lebenszyklus.

Als ein Ansatz zur Überprüfung von Software im Hinblick auf Nachhaltigkeit wurde vorgeschlagen, ein Institut für Software-Kontrolle einzurichten, das Software u. a. im Hinblick auf transparenten, offenen Quellcode, Ressourcensparsamkeit, gute Dokumentation, nachhaltige Architekturen und Lebenszyklen untersucht.

Nachhaltige Infrastrukturen zur Lernunterstützung

In dem World Café zum Thema der Infrastrukturen stand zunächst der Nachhaltigkeitsbegriff im Mittelpunkt und die Frage „Gibt es eine akzeptable Nachhaltigkeit, für die vorgegebene CO₂-Emissionswerte definiert werden können?“ In diesem Zusammenhang wurden Fragen aufgeworfen wie: Reicht die Reduktion, oder brauchen wir den Verzicht? Setzen wir auf Coolness, oder sind Gesetze notwendig? Klappt es über die Freiwilligkeit, oder brauchen wir Kontrolle und Überwachung?

Eingefordert wurde in erster Linie Transparenz, insbesondere Transparenz über die Infrastrukturen mit dem Ziel der Nachhaltigkeit. Hierfür wurde weitestgehend auf Open Source gesetzt, um Vertrauen zu erzeugen. Außerdem sollten die Nachhaltigkeitsziele in Verträge einfließen. Vorgeschlagen wurden auch die Entwicklung von Nachhaltigkeitsprüfungen und Nachhaltigkeitszertifikaten. Dafür sollten geeignete Messinstrumente entwickelt werden (siehe Abbildung 3)

Insgesamt waren sich alle einig, dass es wichtig ist, entsprechendes Know-how aufzubauen, damit Entscheidungen fundiert getroffen werden und eine Nachhaltigkeitskultur zur Entwicklung und Nutzung von Infrastrukturen aufgebaut wird.

Nachhaltigkeit bei der Gestaltung von IT-Systemen

Angedacht war, in diesem Workshop über Architekturen und die Art und Weise, wie wir programmieren und Systeme gestalten, zu diskutieren und möglicherweise eigene Handlungsmöglichkeiten auszuloten. Die unterschiedlichen Vorerfahrungen führten jedoch dazu, dass zunächst sehr stark gesammelt wurde und individuelle Erfahrungen ausgetauscht wurden. Einige Teilnehmende kannten eine ähnliche Umgebung, wie wir sie aufgezeigt

hatten, zumeist wurde aber klar, dass die erlebten Systeme heutzutage von so hoher Komplexität sind, dass allein ihre Undurchdringlichkeit dafür sorgt, dass sorgfältiges und Ressourcen-schonendes Programmieren verunmöglicht wird. Das war dann auch das gemeinsame Resultat: Wir müssten wieder eine bewusste Reduzierung von Komplexität in den Vordergrund stellen, um Systeme verstehbar und damit in Hinblick auf Ressourcen optimierbar zu gestalten.

Referenzen

BMW (2019): Kabinett beschließt Eckpunktepapier für das Klimaschutzprogramm 2030. https://www.bmw.de/Redaktion/DE/Schlaglichter-der-Wirtschaftspolitik/2019/10/online-magazin-schlaglichter-10-19.html?cms_textId=1433266&cms_artId=1433618

Christie, James (2013): Sustainable Web Design. Published in Application Development, State of the Web, <https://alistapart.com/article/sustainable-web-design/>

Schulz, Svenja (2019): Die neue DNA: Digitalisierung, Nachhaltigkeit und Aktion. Rede von Svenja Schulze bei der re:publica 2019, 7. Mai 2019, <https://www.bmu.de/rede/rede-von-svenja-schulze-bei-der-republica-2019/>

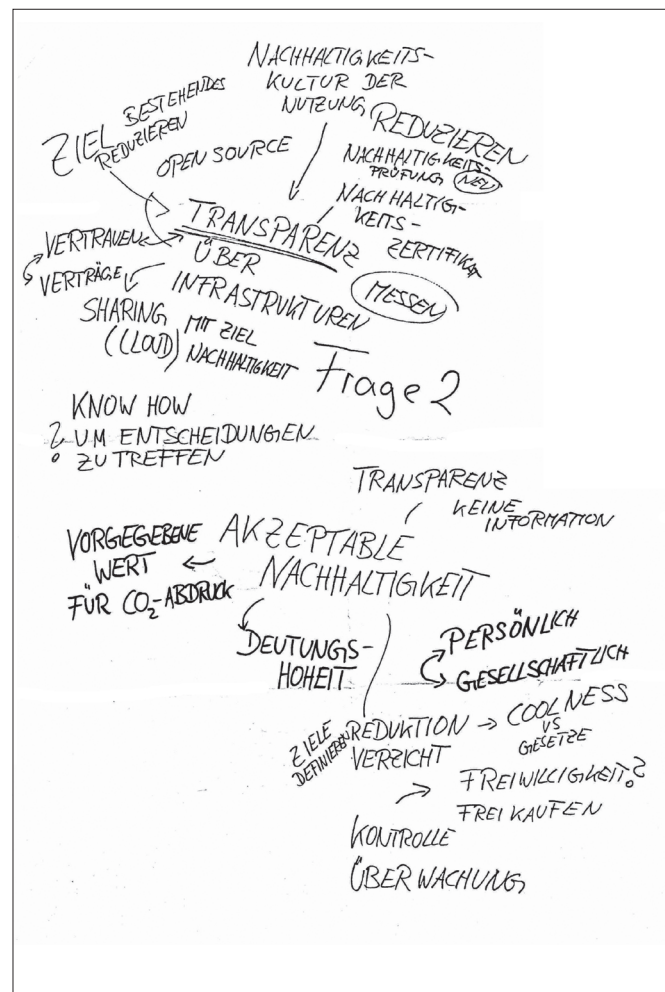


Abbildung 3: Stichwortsammlung zu nachhaltigen Infrastrukturen



Technologiekritik als Herrschaftskritik

Wir fällen nicht das lächerliche Urteil, dass die Technologie „schlecht“ ist. Aus welcher – ohnehin historisch bedingten – Ethik heraus denn auch? Wir sagen, sie ist Gewalt und sozialer Krieg. Unsere Kritik macht sich fest an der technologischen Aneignung von Lebensprozessen. Unsere Positionierung gegenüber spezifischen technologischen Innovationen orientiert sich an einem anzustrebenden Abbau von Macht, Ungleichheit und Fremdbestimmung. Unser sozialrevolutionärer Autonomie- und Freiheitsbegriff geht hier weit über die zugestandene „Freiheit“ der „User“ hinaus, die als Konsumenten und Datenlieferanten zwischen verschiedenen vordefinierten Produkten wählen dürfen. Wir skizzieren in diesem Artikel die Gestaltungsmacht der Technokraten innerhalb der aktuellen Krise der klassischen politischen Repräsentation und erörtern die Konsequenzen am Beispiel zunehmender Entsolidarisierung im „smartifizierten“ Gesundheitssystem.

Wir verteidigen nicht pauschal „die Arbeit“ gegen jede Form von Robotisierung. Das Verhältnis von menschlicher Arbeit zu Nicht-mehr-Arbeit ist eine wenig aussagekräftige, statische Kenngröße einer zudem makroskopischen Betrachtung. Ohne eine mikroskopische Sicht auf gesellschaftliche Auseinandersetzungen beschreibt sie weder die Dynamik der gesellschaftlich-technologischen Umwälzung, noch gibt sie Einblick in ihren Disziplinierungs- und (Selbst-)Unterwerfungscharakter. Wenn wir beispielsweise mit den streikenden MitarbeiterInnen von Amazon zusammenstehen, unterstützen wir ihren Kampf gegen Entwürdigung und Entrechtung sowie gegen die (in diesem Fall algorithmische) Enteignung und Entwertung ihrer Arbeit. Wir tun das in einem solidarischen Verhältnis, aber auch in dem Wissen, dass uns allen die gleiche Entwürdigung in einer technokratischen Zukunftsvision von Amazon bevorstehen könnte – ermöglicht durch eine permanente Bewertung und Steuerbarkeit sämtlicher Lebensbereiche, in die Amazon und seine zukünftigen Nachfolgenden sukzessive vordringen.

Umgekehrt halten wir die beispielsweise von R. Mocek formulierte Position, Technologie als „segensreichen Fortschritt“ zu glorifizieren, den wir lediglich aus den Klauen des Kapitalismus befreien müssen, für naiv.¹ Weder Lenins noch Trotzki (damalige) Zukunftsvisionen einer tayloristischen Fließbandgesellschaft nähren die Hoffnung auf eine progressive Verhaltenssteuerung. Auch sehen wir im sozialistischen Vorläufer der Industrie 4.0, dem chilenischen *Cybersyn-Projekt* (*Proyecto Synco*) Anfang der Siebziger Jahre unter Salvador Allende, keine Referenz für eine heilsversprechende Kybernetik. Denn auch dort hat sich der Vermessungseifer längst nicht mit einer automatisierten Selbstregulierung der Produktion in Chile begnügt, sondern nach Methoden einer kleinteiligen Verhaltensökonomie seiner InhabitantInnen gesucht. Eine Perspektive, die wir heute sowohl in dem „sozialen Punktesystem“ Chinas als auch in Googles Vorstellungen vom „Buch des Lebens“ (selfish ledger) wiederfinden. Diese Programme sind ihrem Anspruch nach totalitär: Der Kybernetisierung des Sozialen wohnt die Vorstellung sich selbst regulierender Individuen inne, die durch ein von außen vorgegebenes Selbstoptimierungsprinzip maximal fremdbestimmt agieren. Daher reicht eine Vergesellschaftung der digitalen Plattformen, ja sogar eine Vergesellschaftung der digitalen Infrastruktur nicht aus. Wir müssen die *soziale Kybernetik* – also die feinstgliedrige Zerlegung unseres Lebens in Mess- und Steuerkreise – als solches zurückweisen. Die Technologie lediglich vom Kapitalismus befreien zu wollen – als vermeintlich „äußerem Verhältnis“ – ist leider eine wenig hilfreiche, unterkomplexe Vereinfachung. Dies brachte bereits Max Weber zum Ausdruck, als er schrieb:



Capulcu stellte sich den Fragen, Foto: Michael Ahlmann

„Nicht erst ihre Verwendung, sondern schon die Technik ist Herrschaft (über die Natur und den Menschen), methodische, wissenschaftliche, berechnete und berechnende Herrschaft. Bestimmte Zwecke und Interessen der Herrschaft sind nicht erst ‚nachträglich‘ und von außen der Technik oktroyiert – sie gehen schon in die Konstruktion des technischen Apparats selbst ein. Die Technik ist jeweils ein geschichtlich-gesellschaftliches Projekt; in ihr ist projiziert, was eine Gesellschaft und die sie beherrschenden Interessen mit den Menschen und mit den Dingen zu machen gedenken.“² (Weber, nach Marcuse 1964).

Die Krise der politischen Repräsentation

Wir befinden uns in einer Phase globaler Fragmentierung. Selbst vermeintliche, ökonomische Gewissheiten der neoliberalen Globalisierung der Neunziger- und Nullerjahre wie die technologische Vorherrschaft des „Liberalismus“ gegenüber Autokratien wie Russland und China zerbröckeln in einem „Me first“ nationaler Selbstbezüglichkeit und Abschottung. Nicht nur dass die Anzahl sogenannter „failed states“ zunimmt – auch äußerlich stabile Gesellschaften fallen innerlich auseinander. Es gibt kaum noch eine gemeinsam diskutierte und umstrittene politische Öffentlichkeit, sondern den Zerfall in immer mehr voneinander getrennte, gesellschaftlich isolierte Parallelwelten. Die einzelnen gesellschaftlichen Fragmente beziehen ihre Informationen und Weltansichten aus den Echokammern und Filterblasen digitaler Portale und „sozialer“ Netzwerke und verstärken darüber ihren eigenen Einschluss.

Die klassische politische Repräsentation befindet sich nicht erst seit Trump und dem zunehmenden rechten „Populismus“ in

Europa in der Krise. Der Bedeutungsverlust der politischen Administration ist tiefgreifender: Die Durchsetzung bzw. die Vermittlung unterschiedlicher Interessen und Bedürfnisse erfolgt zunehmend an der Kontrolle und der Steuerungsmöglichkeit klassischer politischer Instanzen vorbei. Die radikale und beschleunigte technologische Transformation des Kapitalismus wird viel stärker von einigen (wenigen) privatwirtschaftlichen AkteurInnen aus dem Silicon Valley und China dominiert als von der Gestaltungsmacht staatlicher Institutionen. Das geschieht mitunter abseits gesellschaftlicher Aushandlungsprozesse. Während es zumindest vorgesehen ist, auf den Staat als klassischen politischen Akteur (eingeschränkt) demokratisch einwirken zu können, bleibt der „User“ gegenüber dem Plattformbetreiber zumeist in einem rein passiven Nutzungsverhältnis. Seine aktive (Un-)Willensbekundung gegenüber den neuen GestalterInnen, den EntwicklerInnen, beschränkt sich oftmals auf die Nutzung oder die Verweigerung einer Software-Plattform. Der Preis für die Nicht-Nutzung von quasi-standardisierten Kommunikationsplattformen ist vielfach die drohende soziale Isolation (im Freundeskreis, in der Schule, in der Lerngruppe im Studium, ...).

Diese neue Dominanz führt zu einer noch nie gekannten Konzentration von Macht: Eine kleine patriarchale Elite von Technokraten treibt weltweit den Plattform-Kapitalismus mit seiner *Smartifizierung* des Seins voran, also die Quantifizierung sämtlicher Handlungen und Wünsche eines jeden Individuums via digitaler Assistenz, um unsere sozialen Beziehungen neu zu ordnen und in Wert zu setzen. Jede noch so kleine Regung wird digital vermessen, bewertet und damit steuerbar. Der Mensch wird weit über seine Arbeitskraft hinaus dem permanenten Zwang zur Selbstoptimierung und -veräußerung unterworfen. Diese Entwicklung wird derzeit von China mit der Einführung von „sozialen Kredit-Systemen“ angeführt. Weiter zunehmender Anpassungsdruck, soziale Vereinzelung in permanenter Rating-Konkurrenz und soziale Dequalifizierung der Abgehängten als „Überflüssige“ sind die Folge.

Doch es wäre fahrlässig, wenn wir glaubten, solche fortgeschrittenen Programme der Bevölkerungssteuerung ließen sich nur in autoritär formierten Gesellschaften wie China umsetzen. Tatsächlich benötigte die Einführung unterschiedlicher (regionaler) Punkte-Systeme in ihrer Erprobungsphase in Chinas Großstädten keinerlei Zwang. Die zunächst freiwillige Teilnahme mehrerer Hundert Millionen wird teils über Preisrabatte z.B. bei Online-Einkäufen und Bahnreisen, über die Bevorzugung bei Jobangeboten teils allein über den spielerischen Charakter (*Gamification*) des Punkte-Sammelns erreicht.

Auch wenn die großen Tech-Unternehmen aus dem Silicon Valley gerade neidvoll nach China blicken, bleiben sie nicht untätig. Im Mai 2018 sickerte ein internes Firmenvideo³ der Forschungsabteilung Google X in die Öffentlichkeit. Unter dem Namen *The selfish ledger*, was sich nur eher ungenau mit dem „Buch des Lebens“ übersetzen lässt, beschreibt Google seine Zukunftsvision einer paternalistisch geführten Welt. Ein persönliches Journal „sämtlicher Handlungen, Entscheidungen, Vorlieben, Aufenthaltsorte und Beziehungen“ ist die Grundlage für ein System digitaler Assistenz, das KI-basiert auf jeden einzelnen zugeschnittene „Handlungsempfehlungen“ ausspricht. Google verspricht perspektivisch Armut und Krankheiten überwinden zu können unter der freimütig vorgetragenen Bedingung: die Auf-

gabe des freien Willens. Nur dann ließen sich effektiv „potentielle Fehler im Verhalten der NutzerInnen] detektieren und korrigieren“. Selbstbewusst stellt Google in Aussicht: „Noch passen sich die Geräte ihren NutzerInnen an. Dieses Verhältnis wird sich bald umkehren.“ Die diesen Ansichten zugrundeliegende, erschreckend totalitär anmutende Sicht auf eine vermeintlich bessere Welt knüpft nahtlos an die Vorstellungen des Behaviorismus an. Dieser geht angesichts zu komplexer Lebensverhältnisse von einer notwendigen Verhaltenssteuerung andernfalls nicht-rational handelnder Individuen aus – ein zutiefst paternalistisches Menschenbild.

Wenn wir die Transformation des Kapitalismus in Richtung eines digitalen Plattform-Kapitalismus mit neuen (nicht-staatlichen) Playern samt historisch neuem Ausmaß von Abhängigkeiten und Machtungleichgewichten analysieren und kritisieren, dann lässt sich daraus kein positives Verhältnis zum Staat mit dem Wunsch nach Regulierung ableiten. Das wäre ein reformistischer Kurzschluss. Uns stellt sich eher folgender Befund dar: Der in vielen gesellschaftlichen Bereichen (zunächst begrüßenswert) schwindende Einfluss staatlicher Institutionen wird eingetauscht gegen eine ultrakapitalistische Dominanz technokratisch-privatwirtschaftlicher Akteure, die sich noch leichter einem gesellschaftlichen Aushandlungsprozess entziehen können. Wir lesen z. B. den aktuellen Umbau des Gesundheitswesens in dieser Weise. Die vermeintliche Konkurrenz staatlicher und nicht-staatlicher Akteure löst sich nicht selten in einer gemeinsamen pragmatischen „Modernisierungsoffensive“ auf.

Digitalisierung des Gesundheitssystems

In Deutschland ist die Einführung einer elektronischen Gesundheitsakte lange umstritten. ÄrztInnen und (deutlich schwächer organisiert) viele ihrer PatientInnen liefen Sturm gegen die Einführung einer zentralen Speicherung von Gesundheitsdaten, Medikation und Behandlungsansätzen. Das Vorhaben der Bundesregierung, ebendiese Speicherung zu realisieren, ist über zehn Jahre in Verzug. Ende 2018 konnte die *Gesellschaft für Telematikanwendungen der Gesundheitsakte (Gematik)* gerade mal die technischen Voraussetzungen klären. Die milliardenschwere Vorbereitung der dazu notwendigen Infrastruktur rund um die Gesundheitskarte ist mittlerweile veraltet und genügt den Sicherheitsanforderungen der mehrheitlich skeptischen PatientInnen und ÄrztInnenschaft nicht. Das Vorhaben droht endgültig zu scheitern und soll jetzt ab 2020 über das Digitale Versorgung Gesetz trotz massiver Unzulänglichkeiten umgesetzt werden.

Nachdem Apple, Google, Amazon, Facebook und Microsoft erkannt haben, dass „Gesundheit fast überall auf der Welt der größte oder zweitgrößte Sektor der Wirtschaft ist“ (Apple-Chef Tim Cook in einem Interview mit dem Magazin „Fortune“ im Herbst 2017)⁴, investieren sie Milliarden in die Biotech-Forschung und versuchen mit Hochdruck erweiterte Gesundheitsdienste in ihre Softwareumgebungen zu integrieren. Das Smartphone soll dabei zur neuen persönlichen Gesundheitszentrale avancieren, in seiner Funktionalität erweitert durch Zusatzgeräte wie Fitness-Armbänder. Die Apple-Watch z. B. gibt vor, Herzanomalien erkennen zu können. Die Qualität der Messung des Herzrhythmus lässt allerdings zu wünschen übrig und so beklagen sich nicht wenige Notaufnahmen über Smart-Watch-User, die

glauben, einen Herzinfarkt zu haben. Doch das boomende Geschäft mit der Fortschrittsgläubigkeit seiner Technokratie-hörigen KundInnen nimmt dadurch keinen Schaden. Amazon nähert sich dem vielversprechenden Gesundheitsmarkt gleich auf drei Weisen. Der Konzern wird nicht nur Krankenversicherung, sondern plant, auch gleich Apotheke und Pharma-Unternehmen zu werden. Warum? Krankenversicherungen preisen das Risiko ein, krank zu werden. Je vielfältiger und je genauer die Kenntnis der Versicherung über die Gewohnheiten des Versicherten ist, desto exakter lässt sich dieses Risiko berechnen. Ein Wettbewerbsvorteil gegenüber der Konkurrenz. Daher liegt es nahe, dass Google und Amazon sich in diesem Geschäft behaupten könnten – die fehlende Expertise im Versicherungswesen kaufen sie ein.

Den Tech-Giganten folgen nun die klassischen Krankenversicherungen auf die Überholspur. Gemeinsam schaffen sie Fakten und lassen die gesellschaftliche Aushandlung über Standards bei der Digitalisierung des Gesundheitssystems als überflüssig zurück: Nachdem die Generali Deutschland mit ihrem Programm *Vitality* als erste einen günstigeren Tarif für KundInnen in Aussicht stellte, die bereit sind ihr Gesundheitsbemühen (Fitness und Ernährung) vermessen zu lassen, verzeichnen wir seit September 2018 einen gemeinsamen Vorstoß von derzeit 16 Krankenkassen, denen die Gesetzesinitiative der Bundesregierung zu langsam voranschreitet. Hinter dem Namen *Vivy* verbirgt sich eine App, die sämtliche Gesundheitsdokumente, Befunde, ArztInnenbesuche, Medikationen und darüber hinaus Fitness- und Ernährungsbemühungen speichert und bewertet. Auch diese Plattform ist zwei Tage nachdem sie online ging bei SicherheitsexpertInnen durchgefallen: Entgegen der Zusicherung der Kassen werden sehr wohl Gesundheitsdaten an Dritte gesendet – ein No-Go angesichts der Sensibilität der dort gespeicherten Daten. Dennoch erfreut sich die (freiwillige) App bei den über 13 Millionen Versicherten, denen sie derzeit angeboten wird, wachsender Beliebtheit. Die Techniker Krankenkasse bietet ebenfalls ihren 10 Millionen Versicherten eine elektronische Gesundheitsakte als App. Auch die AOK arbeitet an einer eigenen Gesundheits-App, um ihre 26 Millionen Versicherten mit ArztInnen und Kliniken digital zu vernetzen. Beide Projekte sind noch in der Testphase. Viele Krankenkassen gehen derzeit erste Schritte auf dem Weg zu einem dynamischen Tarifsysteem, welches das ursprüngliche Solidaritätsprinzip vollständig auszuhebeln versucht. Das Prinzip lautet: Jede/r ist für seine/ihre Gesundheit selbst verantwortlich. Künstlich intelligente Gesundheitsassistenten gibt

personalisierte Ratschläge, deren Nichtbefolgen mit teureren Tarifen in der Krankenversicherung bestraft wird.

Der staatliche Einfluss in diesem Geschäft mit der Gesundheit ist auf eine minimal gesetzgebende Rolle zurückgedrängt. Der Staat ist längst kein aktiver Gestalter mehr in der Frage wie sich ein solidarisches Gesundheitssystem realisieren lässt. Das Lockern der Bedingungen für Telemedizin 2018 und die gesetzlich ab 2020 (an-)geordnete Verabreichung von Gesundheits-Apps auf Rezept markieren das Einknicken vor einem wachsenden Geschäft mit der Gesundheit. Hiermit wird perspektivisch der qualitativ wichtige Standard eines (nicht-virtuellen) ArztInnenbesuches inklusive freier ArztInnenwahl aufgegeben. Ein lange gefordertes Zugeständnis an die Gesundheitsindustrie, die sich davon deutlich höhere Profite verspricht. Hiermit dokumentiert der Staat sein Scheitern, insbesondere im ländlichen Raum eine vernünftige Gesundheitsversorgung aufrecht zu erhalten und tauscht den universellen Anspruch auf einen ArztInnenbesuch ein gegen eine Skype-Fernberatung im Stil einer Callcenter-Kundenbetreuung. Die Entwicklung KI-basierter Gesundheits-Apps, mit denen sich automatisiert das Bemühen der PatientInnen um seine/ihre Gesundheit erfassen und einpreisen lässt, dient dabei zusätzlich als Filter, über den/die erkrankte Patienten/in von vermeintlichen „HypochonderInnen“ und „BlaumacherInnen“ unterschieden werden sollen. Letzteren soll dann perspektivisch der zu teure echte ArztInnenbesuch verwehrt bleiben. Der „Goldstandard“ des frei gewählten ArztInnenbesuches sei aufgrund des Kostendrucks zukünftig nicht mehr aufrecht zu halten, so der Chef der Generali Deutschland.

Anmerkungen

- 1 „Eine linke Zukunftsvision braucht Modelle, die auch weiterhin auf die Triebkräfte des wissenschaftlich-technologischen Fortschritts vertrauen und diese zugleich aus der Verfügungsmacht des Kapitals heraus zu lösen suchen.“ (R. Mocek, *Technologie, Politik und kritische Vernunft. Wie geht die Linke mit den neuen Technologien um?*, 2008, S. 12).
- 2 Marcuse, Herbert 1964: *Industrialisierung im Werke Max Webers*, S. 127
- 3 Geleaktes Firmenvideo von Google: video <https://vimeo.com/270713969>
- 4 http://fortune.com/2017/09/11/apple-tim-cook-education-health-care/?utm_source=fortune.com&utm_medium=email&utm_campaign=term-sheet&utm_content=2017091113pm



capulcu

Capulcu

Capulcus sind (türkisch) *Wegelagerer* bzw. *Nichtsnutze*. Der damalige Ministerpräsident Erdogan versuchte so die RegierungsgegnerInnen der breiten Revolte 2013 zu diffamieren. Statt über die Gezi-Proteste in Istanbul zu Beginn des Aufstands zu berichten, ließ Erdogan eine Pinguin-Dokumentation im Staats-Fernsehen zeigen. Der Widerstand machte daraufhin den Pinguin zu seinem Symbol. Die Revoltierenden nannten sich fortan Capulcus.

Wir sind eine Gruppe von technologie-kritischen AktivistInnen und HacktivistInnen, die sich in dieser Zeit gegründet hat und stellen unsere Arbeit solidarisch in diesen Kontext. Wir veröffentlichen Texte in verschiedenen linken Medien, bringen regelmäßig Broschüren heraus und bieten Diskussionsveranstaltungen, Seminare und Schulungen an.

EU weitet Meeresüberwachung mit Drohnen aus

Gleich drei EU-Agenturen sind für die Seesicherheit verantwortlich. In einem Abkommen wollen sie von gemeinsamen Aufklärungsfähigkeiten profitieren. Drohnenflüge erfolgen zur Grenz-, Fischerei- und Zollkontrolle, zur Strafverfolgung und für den Umweltschutz. Derzeit nehmen sieben Länder die Dienste in Anspruch, eine Erweiterung ist geplant.



Eine israelische Drohne des Typs Hermes 900 startet von einem Flugplatz in Island, Alle Rechte vorbehalten © EMSA

Die Europäische Agentur für die Sicherheit des Seeverkehrs (EMSA) hat ihre Drohnenflüge auf insgesamt sechs EU-Mitgliedstaaten ausgeweitet. Laut der EU-Kommissarin für Verkehr, Violeta Bulc, fliegen unbemannte Luftfahrzeuge verschiedener Größen in Portugal, Spanien, Dänemark, Griechenland, Kroatien und Italien, außerdem finden Einsätze in Island statt.

Die Überwachungsdienste werden für die Küstenwachen der jeweiligen Länder erledigt. Verfolgt werden die irreguläre Einwanderung, Schmuggel, illegale Fischerei sowie Luft- und Meeresverschmutzung. Bei Bedarf können die Drohnen auch der Seenotrettung helfen. Für die Integration der Drohnen in den allgemeinen Luftverkehr arbeitet die EMSA mit der Europäischen Agentur für Flugsicherheit zusammen.

Drohnen dienst für drei Agenturen

Die Flüge erfolgen nicht nur für die nationalen Behörden, die für die Schifffahrt verantwortlich sind. Auch die Grenzagentur Frontex und die dort zusammengeschlossenen Grenzbehörden machen von den Aufklärungsdaten der EMSA Gebrauch. Grundlage ist eine Arbeitsvereinbarung, an der sich außerdem die Europäische Fischereiaufsichtsagentur (EFCA) beteiligt.

Die drei Agenturen koordinieren zusammen rund 300 zivile und militärische Behörden, die für die Seesicherheit in den EU-Mitgliedstaaten verantwortlich sind. Mit dem Abkommen wollen sie gegenseitig von ihren Überwachungstätigkeiten profitieren. Während Frontex auf Satellitenaufklärung und die Grenzüberwachung mit Flugzeugen spezialisiert ist, entwickelt die EMSA seit 2017 den Drohnen dienst. Letztes Jahr hatten die Agenturen erste gemeinsame Tests mit verschiedenen Drohnen als erfolgreich bewertet.



Die EU-Drohnen in Island tragen das Emblem der EMSA und des portugiesischen Betreibers, Alle Rechte vorbehalten © EMSA

Betreibervertrag über 59 Millionen Euro

Zuerst hat die isländische Regierung von dem Angebot der EMSA Gebrauch gemacht. Seit Juni dieses Jahres operiert eine *Hermes 900* der israelischen Firma Elbit Systems vom Flughafen Egilsstaðir, die Flüge der Langstreckendrohne decken dem Hersteller zufolge mehr als die Hälfte der sogenannten „Ausschließlichen Wirtschaftszone“ Islands ab. Die *Hermes 900* befördert ein Seeüberwachungssystem, das speziell für den Küsten- und Meeresinsatz entwickelt wurde. Auch ein Radar ist an Bord, außerdem ein elektrooptischer Sensor und ein Empfänger für ein automatisches Identifikationssystem (AIS), das Signale registrierter Schiffe empfängt. Einsatzgebiete können mit einer sogenannten Funkbake markiert werden.

Matthias Monroy



Matthias Monroy ist Wissensarbeiter, Aktivist und Mitglied der Redaktion der Zeitschrift *Bürgerrechte & Polizei / CILIP*. In Teilzeit Mitarbeiter des MdB Andrej Hunko. Publiziert in linken Zeitungen, Zeitschriften und Online-Medien, bei Telepolis, Netzpolitik und in Freien Radios. Alle Texte und Interviews unter digit.so36.net, auf englisch digit.site36.net, auf Twitter [@matthi-mon](https://twitter.com/matthi-mon). Viel zu selten auf der Straße (dafür im Internet) gegen Faschismus, Rassismus, Sexismus, Antisemitismus. Kein Anhänger von Verschwörungstheorien jeglicher Couleur. Benutzt das Binnen-I trotz Gepolter nervtötender Maskulinisten.

Den Vertrag für die Flüge in Island hat die EMSA nicht direkt mit Elbit Systems abgeschlossen, sondern über das portugiesische Unternehmen CEIIA. Die Zeitung *Times of Israel* gibt die Kosten des Betreibervertrages mit 59 Millionen Euro an, die Laufzeit beträgt zwei Jahre und kann um weitere zwei Jahre verlängert werden.



In einigen Mitgliedstaaten setzt die EMSA Senkrechtstarter ein, hier den „Camcopter S-100“, Alle Rechte vorbehalten
© EMSA

Senkrechtstarter gegen Umweltverschmutzung

Neben den Langstreckendrohnen nutzt die EMSA mittlerweile auch größere Hubschrauberdrohnen der Firma Schiebel aus Österreich. Der *Camcopter S-100* kann von Schiffen oder von Startplätzen an Land geflogen werden und hat eine Betriebszeit von mehr als sechs Stunden. Für die EMSA fliegt der Senkrechtstarter in Kroatien und ist dort mit optischen und Infrarotkameras und einem AIS-Empfänger ausgerüstet, die maximale Reichweite beträgt rund 100 Kilometer.

Einen ähnlichen Vertrag für die Hubschrauberdrohne *Skeldar V-200* hat die EMSA mit einem skandinavischen Konsortium abgeschlossen. Das Luftfahrzeug trägt einen Sensor zur Überwachung von Schwefelemissionen an Bord und soll Verschmutzungen durch Schiffe in der Ostsee aufdecken. Zur Überwachung der Seegebiete führt die Drohne außerdem optische und Infrarotkameras und den standardmäßigen AIS-Empfänger mit.

Drohntests von Frontex

Als einzigen sogenannten Nurflügler fliegt die EMSA im Auftrag spanischer Behörden eine portugiesische Drohne der Firma Tekever. Neben Einsätzen zur Seenotrettung soll die Drohne auch Ölverschmutzungen beobachten. Schließlich setzt die EMSA auch mehrere Quadrocopter ein. Sie basieren auf einem Modell der US-Firma Lockheed Martin und sind an Bord von Schiffen stationiert. Im Falle einer Ölpest dokumentieren sie Verschmutzungen sowie deren Beseitigung. Zu einem späteren Zeitpunkt will die EMSA die kleinen Drohnen auch zur Überwachung nutzen.

Jetzt bereitet die EU-Kommission weitere Drohnenflüge vor. Interessierte EU-Mitgliedstaaten sollen mitteilen, ob sie an neuen Einsätzen der EMSA im Zeitraum 2020-2021 interessiert sind. Neben dem Drohnen dienst der Agentur für die Sicherheit des Seeverkehrs hat auch Frontex verschiedene Drohntests durchgeführt. Die Pilotprojekte sollten die Eignung von zwei Langstreckendrohnen im Mittelmeer untersuchen und wurden mittlerweile beendet. Ähnliche Forschungen für unbemannte Systeme an Land, zu Wasser und in der Luft finanziert die EU-Kommission im Projekt ROBORDER, entsprechende Tests erfolgen in mehreren Mitgliedstaaten.



Elke Schwarz

Silicon Valley zieht in den Krieg

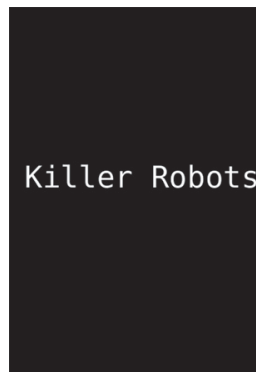
KI, autonome Waffen und politisch-moralische Verkümmern

Die Automatik und Autonomie in militärischen Waffensystemen haben in den letzten zehn Jahren stetige Fortschritte gemacht. Eine Reihe von Ländern einschließlich der USA, Großbritanniens, Chinas und Russlands entwickeln, besitzen und/oder nutzen militärische Systeme, von denen zu diesem Zeitpunkt angenommen werden kann, dass sie über ein bestimmtes Maß an Autonomie und Künstlicher Intelligenz (KI) verfügen, wenngleich auch noch in limitiertem Maße. Die Idee, die technologische Autonomie in der Kriegsführung auszubauen, ist keineswegs neu. KI und militärische Forschung gehen seit jeher Hand in Hand einher und schon in den 1950er und 1960er Jahren war das Thema Autonomie in militärischen Vorgängen äußerst aktuell.

Der Philosoph Günther Anders, ein früher Denker der Mensch-Maschine-Interaktion hatte schon im Jahre 1956 Einwände gegenüber der rasch voranschreitenden autonomen Militärtechnologie. In seinem Werk *Die Antiquiertheit des Menschen* schreibt er über den Einsatz eines „elektronischen Gehirns“, einer technologischen Rechenmaschine, die im Kontext des Koreakrieges eine moralisch schwierige Entscheidung mit scheinbarer Objektivität treffen könnte, ganz klar gewarnt. Anders stand einer solchen Maschinenagentur äußerst kritisch gegenüber und sah die Übertragung von moralisch bedeutsamen Entscheidungen auf die Militärtechnologie als eine klare Abkehr von der moralischen

Verantwortung des Menschen. Das Unbehagen bei schwierigen Entscheidungen in der Kriegsführung würde durch technologische Effizienz und angebliche Neutralität beseitigt. Das, so stellt es fest, führt auch dazu, dass wir Entscheidungen, einschließlich solcher, die von moralischer Relevanz sind, viel lieber unseren intelligenten Rechenmaschinen überlassen, da wir als Menschen nicht ausreichend zurechnungsfähig sind. Ein, wie er sagt „elektronischer Gewissensautomat“, der „schnurrend die Verantwortung übernehmen kann, während der Mensch danebensteht und, halb dankbar, halb triumphierend seine Hände in Unschuld wäscht.“¹ Anders' Diagnose, die im selben Jahr veröffentlicht

wurde als der Begriff *Artificial Intelligence* (AI, dt. Künstliche Intelligenz, KI) geprägt wurde, erwies sich als prophetisch. Obwohl seine Erkenntnisse in erster Linie auf die rasanten Befürchtungen und Aufregungen über Innovationen in der Computertechnologie – zivil und militärisch – in seiner Zeit zurückzuführen sind, finden sie deutliche Resonanz in der heutigen Diskussion über neue militärische Technologien und insbesondere in den Debatten um autonome und intelligente Waffensysteme.



Was kann militärische KI?

Das Thema KI in der Kriegsführung und ganz speziell autonome Waffen – Killer-Roboter! – ruft oft ein dystopisches Schreckensbild von Terminator-ähnlichen Monstrositäten hervor. Die Realität sieht weniger spektakulär, aber komplexer und vielleicht auch gefährlicher aus. Das *Algorithmic Warfare Cross-Functional Team* (AWCFT) – auch als *Project Maven* bekannt – dient als Beispiel. Project Maven war 2017 vom Amerikanischen Verteidigungsministerium als wegweisendes KI-Programm ins Leben gerufen worden, um die enormen Datensätze, welche durch Drohnen gesammelt werden, mit maschinellen Lernen effektiv und schnell zu Handlungsentscheidungen umsetzen zu können. Konkret bedeutet das, dass die Daten in ein KI-System gefüttert werden, welches dann gewisse Muster und Bilder in einer jeweiligen Umgebung erkennt und auswertet, um eine Entscheidung darüber zu treffen, was als mögliche Ziel gelten kann/sollte und was nicht. Soll heißen, ein Programm zur Bildererkennung und Identifizierung, das durch maschinelles Lernen gestützt ist, und anhand welcher ein Mensch dann die Entscheidung treffen kann, ob Gewalt eingesetzt werden kann oder nicht. Hier ist also immer noch der Mensch am Hebel, bevor eine Entscheidung getroffen werden kann. Das soll aber, wenn man den Aussagen von General Shanahan glauben darf, nicht unbedingt lange so bleiben. Die USA priorisiert solche Projekte, welche zum Ziel haben, KI und maschinelles Lernen vermehrt im Kriegsablauf einzusetzen, um autonome Zielerfassung mit autonomer Waffentechnologie zu kombinieren, was dann einen wesentlich schnelleren Handlungsablauf ermöglichen soll.

Das könnte dann zum Beispiel bedeuten, man hat eine mit einer Nutzlast ausgestattete Drohne, die über einem bestimmten feindlichen Gebiet eingesetzt wird. Die Drohne sammelt Daten, welche dann durch das System ausgewertet werden und es ermöglichen, dass ein oder mehrere mögliche Ziele identifiziert werden, welche dann auch umgehend angegriffen werden können – schneller, effizienter und effektiver, so die Worte des Generals. Die USA sind nicht die einzigen, die solche Systeme fördern, Russland hat zum Beispiel letztes Jahr ein mit KI ausge-

stattetes Kalashnikov Waffensystem präsentiert, welches ganz ähnlich mit Bilderkennungsprogrammen funktioniert und autonom Ziele erkennen und zerstören kann, ohne dass ein Mensch da auch nur einen Finger rührt. Es gibt natürlich viele andere Gebiete im Militär, in welchen KI relativ problemlos eingesetzt werden kann: Logistik, Wartung, Transport, und andere Bereiche. Aber es ist die sogenannte „sensor to shoot“-Dimension, welche in den Debatten zu autonomen Waffensystemen im Vordergrund steht.

Wichtig ist zu erkennen, dass KI für die Kriegsführung immer noch ziemlich primitiv ist und dass dies wahrscheinlich auch für lange Zeit so bleiben wird. Systeme verfügen typischerweise nicht über ausreichende Daten, um die Komplexitäten und Dynamiken eines Kriegsgebietes angemessen auswerten zu können. KI kann wohl sehr gut relativ einfache Kategorien erfassen und erkennen – einen Tisch, einen Stuhl, eine Katze – ist aber nicht in der Lage, akkurat zu identifizieren, wer nun genau Freund oder Feind ist, wer zur anderen Seite übergelaufen ist, wer sich ergibt und so weiter. Es kann bislang auch kein Verlass darauf sein, dass Daten neutral oder unvoreingenommen sind, das heißt, oft sind Vorurteile und Annahmen implizit in das System eingebaut, was akkurate Auswertungen erschwert. Dazu kommt, dass KI-Systeme nach wie vor recht spröde und zerbrechlich sind. Es brauchen nur ein oder zwei kleine Pixel an der falschen Stelle sein, und schnell wird aus der Schildkröte ein Maschinengewehr. Trotz der Tatsache, dass moderne KI-Systeme nicht besonders intelligent sind, wenn es um sehr komplexe und dynamische Zusammenhänge geht, ist das Verlangen nach mehr und mehr KI beinahe schon panisch. Stets heißt es, wir dürfen nicht zurückfallen im KI-Rennen. Zu verführerisch ist das Versprechen der Effizienz, der Optimierung, der Schnelligkeit.

Das Problem der Kontrolle

Für die USA und andere Staaten, welche konkret KI für militärische Zwecke entwickeln, soll zwar immer und auf jeden Fall der Mensch schlussendlich in der Entscheidungsschleife bleiben. Was das aber konkret bedeuten kann, wenn die Logik und Schnelligkeit der Maschine das Maß setzen, ist nicht so klar. Vor allem auch, wenn der Mensch vollends eingebettet ist in die Maschinenlogik, in welcher er hauptsächlich auch nur als Systemteil funktioniert, ganz speziell, wenn die Maschinenlogik auf eine Art und Weise arbeitet und Entscheidungen trifft, die der Mensch intellektuell und kognitiv nicht so richtig verstehen kann. Und das ist konkret so mit neuronalen Netzwerken und maschinellen Lernen, welches eine KI-Entwicklung erlaubt, in welcher selbst der Programmierer nicht immer genau weiß, wieso ein System eine bestimmte Entscheidung getroffen hat.

Und ganz speziell, da wir eingebettet sind in diese omnipräsenten digitalen Strukturen, ist es vielleicht relevant zu erkunden, in welchem Maß wir überhaupt die Technologie als pures Instrument benutzen können, und inwieweit unser Handeln, Denken, unser Verlangen, unsere Ideen und auch unsere Rechtfertigungen von technologischen Strukturen geformt werden. Und genau so ist das auch bei den militärischen Technologien, sogar noch wesentlich ausgeprägter, da ein/e SoldatIn ziemlich tief in Netzwerke von Interfaces und digitalen Informationsstrukturen eingebunden ist und unter solchen Umständen oft in Sekun-

denschnelle handeln muss. Genau da wird es problematisch mit der Kontrolle, und auch damit, Verantwortung über moralisch schwierige Entscheidungen zu übernehmen.

Um als moralischer Akteur verantwortungsvoll handeln zu können, müssen, ganz generell gesprochen, gewisse Voraussetzungen gegeben sein. Zum einen muss der Akteur eine gewisse Handlungsfreiheit haben. Das bedeutet, sie oder er wird nicht zu einer Handlung gezwungen. Zum anderen muss der Akteur auch über ausreichend Wissen verfügen, um die Folgen einer Handlung adäquat abschätzen zu können. Das wird im Zusammenhang mit vernetzter digitaler Technologie und speziell KI kompliziert, denn in Bezug auf die KI haben wir kognitive Limitierungen, Wissenslücken, und es fehlt uns außerdem die Zeit, rational und bedeutungsvoll einschreiten zu können, wenn etwas schief geht.

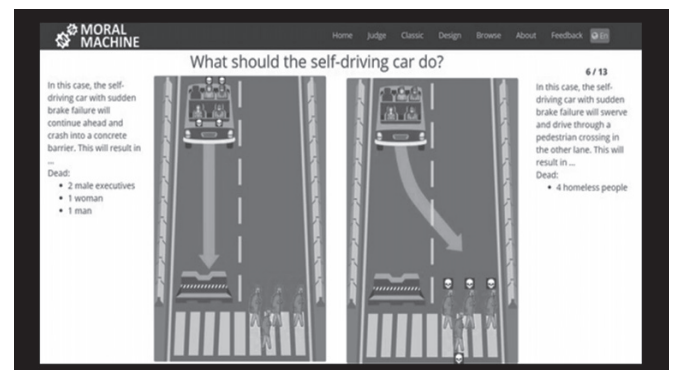
Die kognitive Psychologie bestätigt, dass wir im Umgang mit Maschinen dazu tendieren, nicht das kontrollierte Denken einzuschalten, sondern das automatische Denken. Und wenn wir dieses automatische Denken einschalten, tendieren wir dazu, Zweifel zu unterdrücken und Zweideutigkeiten zu übersehen. Im automatischen Denken ziehen wir Schlussfolgerungen und füllen eventuelle Wissenslücken mit reinen Annahmen. Wir neigen dazu, Vorurteile zu bestätigen und uns lediglich auf vorgelegte Daten/Beweise zu konzentrieren, wobei wir nicht nach anderen Fakten oder Daten suchen, welche ebenso relevant sein können. Ganz speziell in der direkten Mensch-Maschine-Zusammenarbeit, neigt der Mensch dazu, wesentlich größeres Vertrauen in die Maschine zu legen und deren Entscheidungen zu folgen. Dazu gibt es zahlreiche Studien. Selbst wenn es die spezielle Aufgabe des Menschen ist, die Technologie zu kontrollieren, ist es so, dass die menschliche Aufnahmefähigkeit – was die Umgebung angeht – oft so sehr schrumpft, dass er sich kein angemessenes geistiges Modell bauen kann, um im Falle eines technischen Problems schnell und rational handeln zu können. Die Technologie wird zur Autorität.

Des Weiteren ist unser Wissen darüber, auf welcher epistemologischen Basis KI agiert, ebenso eingeschränkt. Ich hatte schon das Problem der in die KI eingebauten Vorurteile erwähnt, welche mit hoher Wahrscheinlichkeit zu verzerrten Ergebnissen führen. Wenn aber der Anwender der KI limitiert Einsicht darüber hat, welche Trainingsdatensätze verwendet wurden, wie diese gesammelt wurden, oder wie die Algorithmen funktionieren, dann ist es schwierig, die Ergebnisse richtig einzuschätzen, umso mehr wenn die KI in der freien Wildbahn eingesetzt werden soll, die ja von Komplexität und Unsicherheiten gezeichnet ist. Wenn wir also nicht wissen, wo die Daten herkommen, wie ein Ergebnis berechnet wurde, welche Vorurteile da eventuell mitspielen, dann fehlt dem Anwender hier klar das nötige Wissen, um verantwortungsvoll handeln zu können. Ganz besonders, wenn die Algorithmen so funktionieren, dass selbst der Programmierer nicht voraussehen kann, was das System entscheidet oder auf welcher Basis, wie es zum Beispiel bei AlphaGo der Fall war, dann wird es mit den Voraussetzungen für Handlungsfähigkeit schwierig. Und wenn diese epistemischen Eckpunkte erst nach einer Handlung festgestellt werden können – wenn überhaupt – dann ist moralisches Handeln nicht gewährleistet.

Der dritte, verbundene, Punkt ist der Zeitrahmen in welchem der Anwender rational und verantwortungsvoll handeln kann. Der

große Vorteil von KI ist Schnelligkeit und Effizienz. Das bedeutet, dass KI-Systeme sekundenschnelle Entscheidungen treffen, in welche der menschliche Anwender ganz einfach nicht schnell genug eingreifen kann. Der *2010 Flash Crash* ist hier ein Paradebeispiel. Und auch bei Waffensystemen, die nur ganz simple Algorithmen benutzen, wie zum Beispiel die *Fire-and-forget*-Systeme SeaRAM oder Phalanx, ist das auch tatsächlich schon so. Auch dies schränkt die menschliche Handlungsfähigkeit ein.

Der tödliche Unfall, welchen ein autonomes Uber-Auto in Arizona in 2018 verursacht hat, illustriert all das auf ganz tragische Weise. Hier hatte das autonome Auto zu wenig Daten, um die Frau, die ihr Fahrrad über die Straße schob und mit der das Auto kollidierte, richtig zu kategorisieren und entsprechend auszuweichen. Zusätzlich war das Auto so abgestimmt, dass eine kurze Verzögerung vor dem Bremsvorgang eingebaut worden war, um exzessive Fehlbremssungen zu vermeiden. Theoretisch hätte die Fahrerin, welche stets beide Hände am Steuer hätte haben sollen, in Notfällen eingreifen müssen, aber sie konnte die Situation nicht zeitnah abschätzen und hatte dem Auto so sehr vertraut, dass sie zum Zeitpunkt des Unfalls ein Video anschaute. Sie wusste weder um die technischen Vorgänge des Autos, noch blieb genug Zeit, die Situation richtig einzuschätzen. Am Ende hatte keiner so richtig Schuld. Und genau hier entsteht ein moralisches Vakuum. Wer soll Verantwortung übernehmen, wenn eine Maschine über Leben und Tod entscheidet? Wichtiger noch, wer kann sich schuldig fühlen?

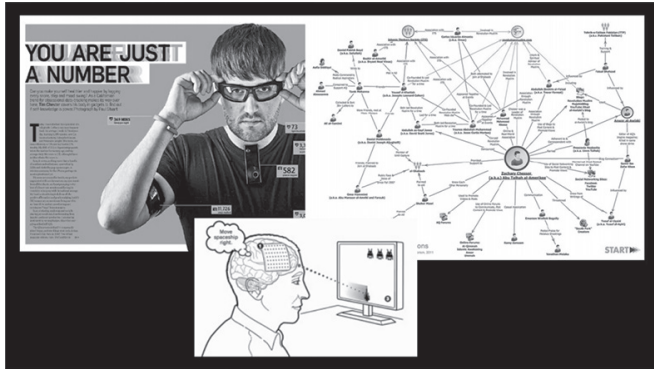


Moralische Verkümmernung

Um diese Lücke zu füllen, gibt es zunehmend Ansätze dafür, die ethischen Entscheidungen in die Maschine selbst zu verlagern, wobei hier angenommen wird, dass man ethische Entscheidungen durch rationales, primär Kosten-Nutzen-orientiertes Denken berechnen kann. Dieses Denken hat eine ganz spezielle und längere Geschichte, in welcher wir unsere Welt primär in wirtschaftlich mathematischen Konturen sehen, in welcher auch wir primär nur als Variable *Mensch* funktionieren. Das ist eine Manifestierung bestimmter sozialer und politischer Formen unserer technologisch konditionierten Gegenwart welche ich in meinem aktuellen Buch im Detail behandle.²

Wenn die Annahme ist, dass man ethisches Handeln berechnen kann, ist die logische Konsequenz, dass man denkt, solche moralische Erwägungen auch in technische Systeme einbauen zu können – entweder als Kosten-Nutzen-Rechnung oder als klare Regel, anhand welcher ein ethisches Handeln entschieden wird. Hier wird Ethik zum Risiko-Management. Das sieht man oft

ganz speziell in Diskussionen zur Ethik des Krieges, vor allem im Anglo-Amerikanischen Raum, wo über die Ethik in der Kriegsführung oft in hypothetischen, abstrahierten Szenarien diskutiert wird, in welchen es oft vorwiegend darum geht, ein moralisches Risiko zu mindern, das oft anhand quasi algorithmischer Formeln berechnet und prognostiziert wird. Das positioniert die Ethik primär als ein Problem, welches einer bestimmten Lösung bedarf, und ethisches Handeln wird in der Sprache des Ökonomen oder des Mathematikers zu effizientem Handeln reduziert. Die Logik, auf welcher unserer Technologie basiert, bestimmt hier also auch das, was als ethisches Denken wahrgenommen wird. Technik als Ethik / Ethik als Technik. Die Welt und der Mensch werden hier zum Datensatz reduziert. Und auch hier sind Günther Anders Einsichten relevant:



Die Leistungen des Orakels bestehen darin, auszuzählen, „welche Mittel sich in einer durch Faktoren A, B, C – N bestimmten Situation lohnen, bzw. welche Verluste sich auszahlen; und da bei der Abwägung von Verlusten und Gewinnen nur endliche Größen eingesetzt werden, ist auch unser Leben eo ipso als eine endliche, also aufwiegbare, Größe eingesetzt.“³

Daten werden priorisiert. Alles was nicht als Daten aufgefasst werden kann, kann auch nicht moralisch adressiert werden. So stehen dann im Vordergrund hauptsächlich die Frage des Kollateralschadens, im Sinne davon, wie viele Todesfälle in der Zivilbevölkerung in Kauf genommen werden können, um ein bestimmtes Ziel ‚ethisch‘ zu erreichen. Was dabei nicht moralisch thematisiert werden kann, sind die weniger mess- und zählba-

ren, aber dennoch zahlreichen Traumata und psychologischen oder physischen Verwundungen, die ein Krieg immer verursacht. Aber weder die Ethik des Krieges, noch der Krieg selbst ist ein Ingenieurproblem, welches es technisch zu lösen gilt. Im Krieg geht es immer um Menschen und deren Lebensraum. Krieg ist ein sozio-politisches Problem und da ist Vorsprung durch Technik nur limitiert von Nutzen. Zumindest wenn ein Ende des Konflikts oder gar der Frieden das Ziel sein soll. Ethik ist schwierig. Ethisches Handeln ist selten mit Klarheit behaftet, sondern beschäftigt sich mit unlösbaren Dilemmata. Moralische Dilemmas fügen sich in jedem Zusammenhang anders. Sie zeichnen sich durch eine unzählige Vielfalt aus. Das bedeutet, bei jedem moralischen Dilemma sollte man eigentlich neu überlegen oder zumindest überprüfen, ob das alte Denken noch ausreicht.

Ethisches Handeln ist schwierig. Oft, meistens, gibt es keine gute Lösung, sondern nur eine wenig schlechtere, für die man sich entscheiden muss – das bedeutet, dass man Verantwortung für etwas übernehmen muss, für das man sich entschieden hat. Ethisches Denken braucht Übung und benötigt, dass wir uns an extrem unkomfortable Situationen heranwagen. Wenn dies durch die Technologie übernommen wird, dann verkümmert unsere moralische Handlungsfähigkeit, unsere moralische Geschicklichkeit. Das genau steht mit KI in der Kriegsführung am Horizont. Ein ehemaliger US-Sniper-Soldat hat das neulich in einem Artikel ganz gut auf den Punkt gebracht: „Wenn man sich auf den Mythos der Technologie und des distanzierten Tötens verlässt, um die rationalen Grundlagen für einen vereinfachten Krieg zu legen, wird man seine Seele verlieren.“ Da gilt es, mit allen Mitteln dagegenzuhalten.

Anmerkungen

- 1 Günther Anders (2010) *Die Antiquiertheit des Menschen Vol. 1. München: Beck Verlag, S. 60-61*
- 2 Siehe Elke Schwarz (2018) *Death Machines: The Ethics of Violent Technologies. Manchester: Manchester University Press*
- 3 Günther Anders (2010) *Die Antiquiertheit des Menschen Vol 1. München: Beck Verlag, S. 246*



Elke Schwarz



Elke Schwarz ist Dozentin für Politische Theorie an der Queen Mary University London. Ihre Forschung konzentriert sich auf die Schnittstellen von Technologie, Ethik und Gewalt, mit Schwerpunkt auf der Ethik unbemannter und autonomer/intelligenter militärischer Technologien und deren Auswirkungen auf die Politik der zeitgenössischen Kriegsführung. Elke ist an einer Reihe von interdisziplinären Projekten zur Ethik der Drohnenkriegsführung beteiligt und arbeitet derzeit an einem von der British Academy / Leverhulme finanzierten Projekt zur Militär-ethik und Künstlichen Intelligenz.

Sie publiziert zum Thema Technologie, Ethik und Politik und ist Autorin von *Death Machines: The Ethics of Violent Technologies* (Manchester University Press), welches untersucht, wie Technologie politische und ethische Subjektivitäten beeinflusst, und dadurch eine erweiterte Rechtfertigung der Gewalt ermöglicht. Sie ist Mitglied des ‚International Committee for Robot Arms Control‘ (ICRAC) und nimmt aktiv an den Debatten über das Verbot von sogenannten Killerrobotern teil. Elke ist außerdem Mitbegründerin der British International Studies Association (BISA) Arbeitsgruppe *Ethics and World Politics*.

Arbeitsgruppe: „Ziviler Betrieb“

Betriebe, die sich nicht an der Rüstungsproduktion beteiligen wollen, sollen dies durch das Label Ziviler Betrieb nach außen kenntlich machen können. Die diesbezügliche Initiative Ziviler Betrieb der Bremischen Stiftung für Rüstungskonversion und Friedensforschung sowie der Evangelischen Landeskirche in Baden wird auch vom FlFF unterstützt.

Mit einer Kennzeichnung *Ziviler Betrieb* sollen Betriebe öffentlich bekunden können, dass sie sich nicht an der Rüstungsproduktion beteiligen. Betriebe, die sich zu den 3 Grundsätzen bekennen, sollen *Ziviler Betrieb* als Label führen dürfen:



Die Grundsätze

Wir fühlen uns dem Frieden verpflichtet und verfolgen nur zivile Zwecke.

Wir beteiligen uns nicht an der Entwicklung, Herstellung und Verbreitung von Waffen und sonstigen Rüstungsgütern.

Wir arbeiten nicht für das Militär und dessen zivile Einrichtungen.

In einer kleinen Arbeitsgruppe wurden das Konzept *Ziviler Betrieb* intensiv diskutiert und konkrete weitere Schritte für die Weiterverbreitung dieses Labels ergriffen.

Warum brauchen wir eine Kennzeichnung *Ziviler Betrieb*?

Rüstungsproduktion wird von der Mehrheit der Bevölkerung abgelehnt und trotzdem bezeichnet es die Bundesregierung als ihr Anliegen, sich in der Verteidigungsindustrie „für einen erleichterten Zugang von mittelständischen Unternehmen zu internationalen Wertschöpfungsketten (zu) engagieren.“¹

Genauso wie ein Label *Ziviler Betrieb* von der Bevölkerung nachgefragt wird, besteht auf der Seite der Unternehmen ein Bedarf. Es gibt beispielsweise mittelständische Unternehmen, die High-Tech produzieren, an denen auch das Militär Interesse hätte, die aber in ihren Unternehmensgrundsätzen die Beteiligung an Rüstungsproduktion ausschließen. Es gibt auch Banken und Investmentfirmen, deren ethische Grundsätze eine Investition in Rüstung ausschließen. Derartige, teilweise auf den Kriegserlebnissen der Gründergeneration fußenden Entscheidungen werden allerdings häufig nicht publik gemacht. Über die Gründe kann man nur spekulieren, jedoch könnte ein *Ziviler-Betrieb*-Label diese Betriebe ermutigen, ihre vorbildlichen Grundsätze auch offensiver nach außen zu vertreten.

Aktuell werden Start-ups von Persönlichkeiten gegründet, die mit hohen ethischen Werten ihr Unternehmen aufbauen. Teilweise sind die Gründer auch durch die Zivilklausel-Diskussion an den Universitäten² geprägt. Google startete seinerzeit mit dem – mittlerweile gestrichenen – Grundsatz „Don't be evil“. Für Start-ups, die sich bewusst nicht an der Rüstungsproduktion beteiligen, gibt es z. Z. keine organisierte Möglichkeit, dies zum Ausdruck zu bringen. Die Initiativen von Google-Mitarbeitern gegen die Produktion autonomer Waffen³ oder die Diskussion bei sd&m über die Herstellung von Software für die Bundeswehr⁴ zeigen, dass dieses Thema die Beschäftigten in der IT-Branche bewegt.

Was kann das Label *Ziviler Betrieb* erreichen – was nicht?

Das *Ziviler-Betrieb*-Label kann vorbildliche Entscheidungen einzelner Betriebe unterstützen und die politische Diskussion initiieren und fördern. Es kann Personen und Betriebe sensibilisieren und ermutigen, sich ebenfalls bewusst nicht an der Rüstungsproduktion zu beteiligen. Das Ziel des Labels ist vorerst auch darauf beschränkt.

Die Selbstverpflichtung auf die Grundsätze des Labels *Ziviler Betrieb* kann und soll kein Ersatz für eine zertifizierbare Wirtschaftsprüfung sein, auf der Investitionsentscheidungen etwa von Ethik-Fonds fußen können. Damit wäre das Label für den Anfang überfordert und zudem wäre aufgrund der damit verbundenen Kosten der Zugang für kleine Betriebe verwehrt. Perspektivisch ist eine solche Erweiterung aber durchaus denkbar.

Das einzige Vergabekriterium des Labels *Ziviler Betrieb* ist die Selbstverpflichtung auf die o.g. Grundsätze. Wo es Debatten um die Graubereiche zwischen ziviler und nicht-ziviler Produktion gibt, müssen diese bewusst geführt werden. Wenn es diese Debatten gibt, erreicht das Label sein Ziel: die Förderung der Diskussion und die Sensibilisierung für die Problematik der Rüstungsproduktion. Es ist schlechterdings nicht denkbar, dass ein Rüstungsproduzent auf das missbräuchliche Tragen des Labels *Ziviler Betrieb* besteht und sich so die kritische Diskussion über seine Rüstungsgeschäfte selbst organisiert. Trotzdem behalten



Peter Ansorge

Peter Ansorge arbeitet an der Universität Bremen und berät dort Betriebs- und Personalräte zur Gestaltung von Regelung von IT-Systemen im betrieblichen Einsatz, insbesondere (Software-)Ergonomie, Datenschutz und Arbeitsgestaltung. Er ist Vorsitzender der *Bremischen Stiftung für Rüstungskonversion und Friedensforschung*.

es sich die Initiatoren vor, bei Verstößen gegen die Grundsätze von *Ziviler Betrieb* das Führen des Labels zu untersagen.

Warum sollen Betriebe das Label *Ziviler Betrieb* tragen?

Es hat für Unternehmen Vorteile, das Label *Ziviler Betrieb* zu führen. Die klare, ethisch begründete Positionierung eines Betriebes wird am Markt durchaus wahrgenommen und positiv bewertet. Die Vorteile dabei liegen sowohl im Bereich der Kundengewinnung als auch bei der Mitarbeitersuche. Das Label *Ziviler Betrieb* kann für Bewerber ein Kriterium bei der Auswahl ihres Arbeitgebers sein und so Bewerber und Betriebe zusammenführen, die die ethischen Grundsätze des Labels teilen. Es wirkt so identitätsstiftend nach innen.

Soweit potenzielle Auftraggeber – beispielsweise die Kirchen – oder Investoren nach ethischen Kriterien agieren, kann das Label *Ziviler Betrieb* einen nicht zu unterschätzenden Vorteil darstellen. Perspektivisch kann das Label sogar zur Voraussetzung für die Gewinnung bestimmter Kunden oder Aufträge werden.

Das Label *Ziviler Betrieb* wirkt auch identitätsstiftend nach außen, indem es zur Vernetzung von Betrieben mit ähnlichen ethischen Grundsätzen beiträgt. Gerade bei jungen Betrieben kann sich dies als äußerst hilfreich erweisen. Hierbei kommt den Organisatoren des Labels eine besondere Aufgabe zu, auch derartige Nutzeffekte zu befördern.

Ausblick

Innerhalb der Arbeitsgruppe wurde nicht nur das Konzept diskutiert, sondern konkrete Maßnahmen, etwa die Vorstellung von *Ziviler Betrieb* in mehreren Betrieben und Initiativen wie dem Mietshausyndikat vereinbart, und auf dem Infostand der Initiative trugen sich während der FlfF-Konferenz mehrere Betriebe als *Ziviler Betrieb* ein.

Anmerkungen

- 1 *Strategiepapier der Bundesregierung zur Stärkung der Verteidigungsindustrie in Deutschland, Berlin, 8. Juli 2015*
- 2 Exemplarisch: „Bremer Universität bestätigt Zivilklausel. Wichtiges Signal für Verantwortung in der Wissenschaft“ in: *FlfF-Kommunikation 1/2012*.
- 3 Siehe z. B.: „Google-Mitarbeiter wehren sich gegen Militärprojekt“, <https://www.faz.net/aktuell/wirtschaft/digitec/google-mitarbeiter-wehren-sich-gegen-militaerprojekt-15527411.html> (Abruf: 12.02.2020)
- 4 Die Diskussion beim Softwareunternehmen sd&m wurde seinerzeit ausführlich aufgearbeitet und in der *FlfF Kommunikation 3/1996* dokumentiert.

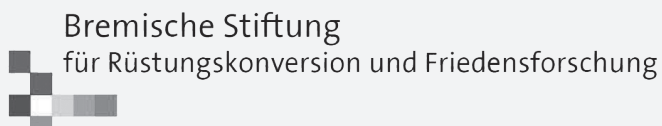


Ziviler Betrieb ist eine Initiative der Bremischen Stiftung für Rüstungskonversion und Friedensforschung und der Evangelischen Landeskirche in Baden. Die Initiative *Ziviler Betrieb* wird vom FlfF unterstützt.

Weitere Informationen:

- info@ziviler-betrieb.de
- <http://ziviler-betrieb.de>

Kontakt:



Bremische Stiftung für Rüstungskonversion und Friedensforschung
Goetheplatz 4, 28203 Bremen,
Telefon: 0421 326 830

Spendenkonto:
Bremische Stiftung für Rüstungskonversion
IBAN: DE92 4306 0967 2029 4384 00
BIC: GENODEM1GLS, GLS Bank



Kirchlicher Dienst in der Arbeitswelt (KDA)
Andreas Bordne

Habsburgerstr. 2
79104 Freiburg

Telefon: 0761 70863 40

Arbeitsgruppe: Zivilklausel durchsetzen!

In § 4 Absatz 1 des Bremischen Hochschulgesetzes heißt es: „Die Hochschulen verfolgen in Forschung, Lehre und Studium ausschließlich friedliche Zwecke.“ Und § 7b bestimmt: „Die Hochschulen geben sich in Umsetzung von § 4 Absatz 1 eine Zivilklausel. Sie legen ein Verfahren zur Einhaltung der Zivilklausel fest. In den Hochschulen kann eine Kommission zur Umsetzung der Zivilklausel gebildet werden.“ Beides wird aktuell von der Universität Bremen nicht voll umgesetzt. Insbesondere gibt es kein transparentes Verfahren für Anwendung der Zivilklausel. Damit die Wissenschaft zur friedlichen Weiterentwicklung der Gesellschaft beiträgt, sind in der Forschung sowohl Freiheit als auch das Übernehmen der Verantwortung für die möglichen Folgen notwendig. Deshalb muss neben der Freiheit der Forschung auch die Verantwortung für die Folgen wieder im Diskurs unserer Hochschulen stehen.

Im Selbstverständnis vieler Forschender, unabhängig vom Forschungsbereich, besteht das Ziel ihrer Arbeit im Fortschritt und in der Weiterentwicklung der Gesellschaft. Es liegt im Interesse der WissenschaftlerInnen, durch verantwortliches Handeln die Herbeiführung und Sicherung des Friedens nachhaltig zu unterstützen.

Dies entspricht aber nicht der Realität. Die Universität Bremen, aber auch andere Hochschulen in Deutschland, standen schon im medialen Rampenlicht [1,2], da sie u. a. vom Pentagon Forschungsaufträge erhalten haben. Über die Häfen in Bremen werden Rüstungs- und Militärtransporte abgewickelt, allein im Jahr 2018 736 Container mit Sprengstoff und Munition. Pro Tag werden ungefähr 40 Tonnen Munition in alle Welt verschifft. Fast fünf Prozent der Bremer Wirtschaftsleistung erbringt die Rüstungsindustrie [3]. Sogar die städtische Wirtschaftsförderung wirbt damit, „die produktivste Region Europas in der Branche zu sein“.

Seit 2016 ist die Zivilklausel im Bremer Hochschulgesetz verankert. Dort [4] steht: „Sie legen ein Verfahren zur Einhaltung der Zivilklausel fest.“ Das genannte Verfahren wurde nicht veröffentlicht. Ob es aktuell überhaupt ein Verfahren gibt, das prüft, ob ein Forschungsprojekt an der Universität für Rüstungszwecke genutzt werden kann, ist auch nicht einsehbar.

Die Diskrepanz zwischen vergesetzlichter Zivilklausel und deren wirkungsvoller Durchsetzung unterminiert die gesetzgebende Autorität ebenso wie die der Exekutive. Die Verletzung der Zivilklausel muss klar definierte strafrechtliche Konsequenzen haben, um ihre Wirkung zu entfalten.

Aber zuerst, was ist die Zivilklausel [5]?

Folgeverantwortliches Forschen durch Unabhängigkeit von Drittmitteln von Rüstungsfirmen. Die Universität Bremen hat unter dem Druck des Kalten Krieges und dem Rüstungswettlauf im Weltraum 1986 eine Zivilklausel eingeführt. Bisher ist in Bremen allerdings kein wirksames Verfahren zur Einhaltung der Zivilklausel etabliert. So sieht z. B. die Hochschule Bremen keinen Widerspruch zum Bremischen Hochschulgesetz in ihrer Kooperation mit der Bundeswehr im Studiengang *Informatik für Frauen*, da die Bundeswehr nur friedliche Ziele verfolge.

Die Hochschulen verfolgen in Forschung, Lehre und Studium ausschließlich friedliche Zwecke. Die den Hochschulen vom Land und von Dritten zur Verfügung gestellten Mittel sollen ausschließlich für Vorhaben verwendet werden, die diesen Zwecken dienen.

Wir fordern den Akademischen Senat der Universität Bremen auf, seinen Beschluss Nr. 5113 korrekt umzusetzen, des Weiteren wird mit einer Anfrage nach dem Informationsfreiheitsgesetz der Einblick in das Verfahren für die Universität (§ 7b Satz 3 BremHG) verlangt.

Ein kontroverses Thema bei der Zivilklausel ist das Problem des *Dual Use*. Der AstA schreibt dazu:

„GegnerInnen der Zivilklausel führen an, dass wissenschaftliche Erkenntnisse angesichts der Dual-Use-Problematik für militärische Zwecke verwendet werden können. Es könne nie ausgeschlossen werden, dass auch zivile Forschungsprojekte für militärische Zwecke verwendet werden könnten.“

Bundeswehr an der Hochschule Bremen

Am 11. und 12. November 2017 fand im Haus der Wissenschaft eine öffentliche Podiumsdiskussion mit dem Thema *Zapfenstreich für die Zivilklausel?* statt. Thema war auch, dass die beabsichtigte Kooperation zwischen der Hochschule Bremen und des Bundesamtes für das Personalwesen der Bundeswehr gegen die Zivilklauseln des Bremischen Hochschulgesetzes und der Hochschule Bremen verstoße. Dies weist Rechtsanwalt Dr. Bernd Hoppe aus Kassel in einem Rechtsgutachten nach. Aus dem Rechtsgutachten geht hervor, dass die rechtliche Einschätzung des Senators für Justiz und Verfassung vom Mai 2016 rechtsfehlerhaft von einer Vereinbarkeit der beabsichtigten Kooperation mit den Zivilklauseln ausgeht. Dabei wird übersehen, dass die Zivilklausel nicht lediglich das Verfolgen von friedlichen Zwecken, sondern ausschließlich friedlichen Zwecken in Studium, Lehre und Forschung fordert. Die Bundeswehr verfolgt nicht ausschließlich friedliche Zwecke, auch nicht nach der Auffassung des Senators für Justiz und Verfassung [6].

Eine Grundsatzfrage: Das US-Verteidigungsministerium verlangt von allen Projekten, die sie finanzieren, dass diese für militärische Zwecke genutzt werden können. Explizit davon ausgeschlossen sind Forschungen im medizinischen Bereich. Wie kann man behaupten, dass die Forschung für ausschließlich friedliche Zwecke genutzt wird, wenn der Geldgeber nur finanzieren darf, was für militärische Zwecke nutzbar ist?

Nils Zurawski fasst die Problematik in einem Beitrag von *Deutschlandfunk Kultur* sehr gut zusammen [7]:

„Andererseits sollten Zivilklauseln anregen, wirklich zu tun, wozu sie beschlossen wurden. Statt ein Dilemma nur zu beklagen, sollten sie die notwendige Diskussion über die gesellschaftliche Verantwortung der Wissenschaft anregen, nicht nur, aber besonders verantwortungsbewusst auf sensiblen Fachgebieten: innere wie äußere Sicherheit, privater wie nationaler Schutz vor Übergriffen waren und sind reich an Fragen für den Forscher.“

Konzept

Die Kritik an diesen Entwicklungen rührt von dem Grundgedanken her, dass Wissenschaft, Forschung und universitäre Lehre dem Frieden dienen und an zivilen Lösungen der großen globalen Herausforderungen arbeiten sollen. Deshalb muss das Konzept der friedlichen Universität, ein elementarer Teil der Gründungsideologie der Bremer Universität, weiter aktiv verteidigt werden. Hochschulen sollten sich als öffentliche Einrichtung der gesellschaftlichen Folgeverantwortung ihrer Forschung bewusst sein.

Ausblick

Immer mehr Menschen realisieren, dass wir jetzt etwas unternehmen müssen, wenn wir die ganze Natur der Erde – uns eingeschlossen – nicht in den Tod reißen wollen. Bisher drehte sich die Klimadebatte vor allem um Gesetze, welche umweltschädliche Konzerne in die Schranken weisen sollten oder sich um nachhaltigere Produktionswege bemühten. Stellen wir uns einem der größten ökologischen Schädlinge dieser Welt: dem Krieg.

Wissenschaft sollte nie zur Destruktion unserer Lebensgrundlagen dienen. Krieg hat verheerende Auswirkungen nicht nur auf die betroffenen menschlichen Gesellschaften, vielmehr stellt ein Krieg auch immer eine große Gefahr für Ökosysteme dar. Zudem sorgen sie für eine sehr ineffiziente Nutzung von knappen Ressourcen. Seit der Industrialisierung verfügen wir über immer mehr Möglichkeiten Waffen zu produzieren. Mitverantwortlich dafür ist die Forschung. Die in der heutigen Zeit eingesetzten

Bomben und Munition verpesten und zerstören in kürzester Zeit alle Bereiche des Ökosystems.

Verantwortliches Handeln in der Wissenschaft impliziert, dass alle Unterstützung von Krieg abgelehnt wird. Hierzu gehört, dass wir unseren Industrien, welche in kriegführende Länder exportieren, nicht mehr durch unsere Forschung unterstützen. Wir als Forschende haben nur dann eine Zukunftsperspektive, wenn wir uns nicht vor der Wissenschaftsethik verschließen. Die Erhaltung unserer Natur und den Fortschritt der Gesellschaft müssen wir zur höchsten Priorität erklären. Klare Positionierungen in der Wissenschaft sind hierfür essentiell.

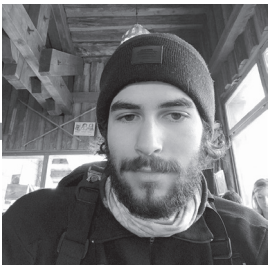
Forderungen

Unsere Forderung ist, dass in den Bremer Hochschulen ein Diskurs mit dem Ziel von Transparenz, öffentlicher und interdisziplinärer Diskussion aufkommt. Unser erstes Ziel ist die Einhaltung von anerkannten ethischen und moralischen Standards auf nationaler und internationaler Ebene. Konkret also Transparenz von dem Verfahren zur Einhaltung der Zivilklausel. In Hochschulen fordern wir die Bildung einer Kommission zur Umsetzung der Zivilklausel, welche bindende Entscheidungen fällt; sie soll aktiv recherchieren und transparent informieren.

Verantwortungsbewusstes Handeln soll von den Hochschulen gefördert und gefordert werden und resultiert in der friedlichen Weiterentwicklung und Bereicherung aller Nationen und Kulturen. Konkret heißt das:

- Die Öffentliche Transparenz und eine wirksame Kontrolle zur Bekämpfung von Korruption an Hochschulen und Forschungseinrichtungen müssen sichergestellt werden.
- Entsprechende Hinweisgebersysteme müssen an den wissenschaftlichen Einrichtungen und Hochschulen etabliert werden, die einen anonymen Dialog ermöglichen sowie einen institutionellen Schutz für Hinweisgeber/Whistleblower bieten.
- Die Informationsfreiheitsgesetze/Transparenzgesetze der Länder müssen grundsätzlich auch für öffentliche Wissen-

Liam Hurwitz und Simon Rundé



Liam Hurwitz studiert das Leben, insbesondere die Informatik am Tag, lässt Computer bei Nacht Dinge tun. Zurzeit macht er seinen Bachelor in Informatik an der Universität Bremen. Dort arbeitet er als studentische Hilfskraft am Institut für Cyber-Physikalische Systeme des Deutschen Forschungszentrums für Künstliche Intelligenz. Er interessiert sich für korrekte Software, Robotik, Data Science und für Dinge im Internet. Im Fokus seiner Projekte steht das Gemeinwohl und die faire Nutzung von Technologie

Simon Rundé studiert Informatik an der Universität Bremen und beschäftigt sich mit politischen Fragen, Datenanalyse und schönen Graphen.

schaftseinrichtungen gelten, besonders für deren Beziehungen zu privatrechtlichen Organisationen. Die zum Schutz der Wissenschaftsfreiheit erforderlichen Einschränkungen der gesetzlichen Transparenzpflichten sind auf das nötige Maß zu beschränken und dürfen auch nicht durch privatrechtliche Vereinbarungen ausgeweitet werden.

- In jedem Drittmittelantrag der Universität Bremen muss der Antragsstellende angeben, ob das Projekt mit der Zivilklausel vereinbar ist.
- Die Bremer Bürgerschaft wird aufgefordert, unbedingt die Sanktionierung der Nichteinhaltung der Zivilklausel gesetzlich zu verankern. Nur so lassen sich die ethischen Werte der Politik glaubwürdig vertreten.

Detlef Borchers

Joseph Weizenbaum, Eliza und das Bild in der KI

Wer heute nach KI-Illustrationen sucht und eine Suchmaschine prügelt, der wird unweigerlich Bilder finden, in denen der Kopf oder das menschliche Gehirn mit Hilfe von Platinen-Layouts nachgezeichnet wird. Das war nicht immer so. Bevor es Computer gab, zeichnete der Austroamerikaner Frank Paul 1927 eine gewaltige Gedankenmaschine mit all dem, was damals Stand der Technik war.

The THOUGHT MACHINE By Ammianus Marcellinus

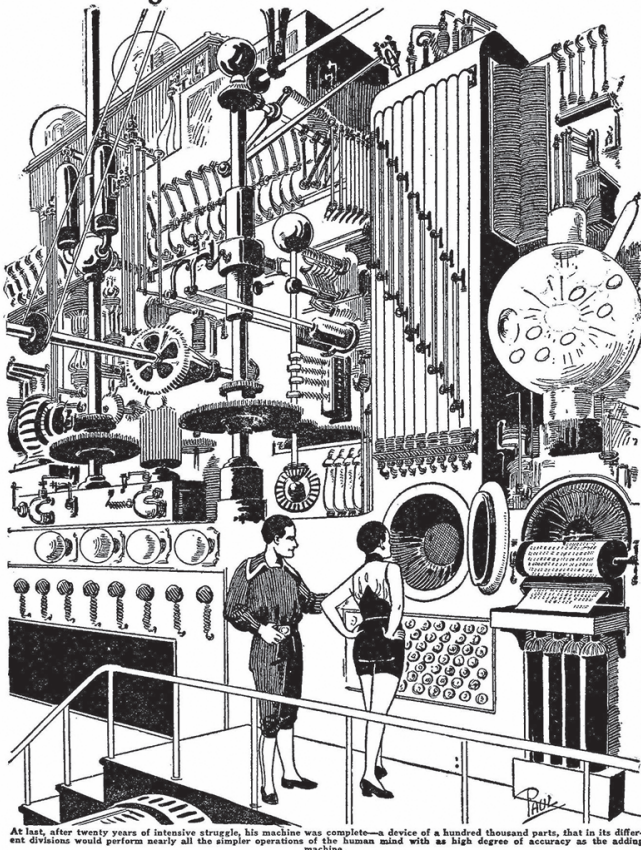


Abbildung 1: The Thought Machine, Foto: Frank Paul

Referenzen

- [1] <https://www.spiegel.de/lebenundlernen/uni/us-militaerforschung-an-deutschen-unis-21-millionen-dollar-in-zehn-jahren-a-1273282.html>
- [2] <https://www.spiegel.de/international/germany/german-universities-under-fire-for-taking-pentagon-contracts-a-935704.html>
- [3] <https://www.aufstehen-bremen.org/index.php/theme-styles/ag-frieden/285-wir-begrueissen-juergen-todenhoefer-in-bremen-kriege-beginnen-hier-am-ruestungsstandort-bremen>
- [4] <https://beck-online.beck.de/?bcid=Y-100-G-BremHG>
- [5] https://www.asta.uni-bremen.de/wp-content/uploads/2014/11/2014_10_28_AKMU_Heft_Zivilklausel+Ruestungsforschung.pdf
- [6] <https://www.bremerfriedensforum.de/pdf/Doku20161106bh.pdf>
- [7] https://www.deutschlandfunkkultur.de/zivilklausel-universitaeten-scheuen-militaerforschung.1005.de.html?dram:article_id=312002



Wie sich das Bild änderte, möchte ich anhand von Broschüren zeigen, die Henry Sherwood gesammelt hat. Henry war der ältere Bruder von Joe Weizenbaum und war 1960-1966 bei *Burroughs Computer* bei der Konstruktion der B2600-Mainframes beschäftigt, während Joe bei *General Electric* arbeitete. Während seiner Zeit bei *Diebold Research Europe* sammelte Henry Sherwood so ziemlich alles, was über seinen Bruder oder über die Community der KI-Forscher veröffentlicht wurde. Zu dieser Community gehörte zweifelsohne Joe Weizenbaum am MIT, jedenfalls bis er sich mit ELIZA beschäftigte. Auf dem Foto sehen wir ihn zusammen mit George Shannon, Ed Fredkin und Joe McCarthy.



Abbildung 2: George Shannon, Ed Fredkin, Joe McCarthy und Joseph Weizenbaum

Foto: Mit freundlicher Genehmigung von M. Lefker Sherwood

Von Shannon ist ein berühmtes KI-Zitat überliefert: „I visualize a time when we will be to robots what dogs are to humans, and I'm rooting for the machines.“ Leider stellte sich das bekannte Zitat bei der Recherche als unvollständige Wiedergabe eines Interviews mit dem Magazin *Omni* heraus.

„Omni: Will robots be complex enough to be friends of people?

Shannon: I think so. I myself could very easily imagine that happening. I see no limit to the capabilities of machines. As microchips get smaller and faster, I can see

them getting better than we are. I can visualize a time in the future when we will be to robots as dogs are to humans. [...]

Omni: Do you find it depressing that chess computers are getting so strong?

Shannon: I am not depressed by it. I am rooting for the machines! I have always been on the machines' side. Ha-ha!"¹

Auch von Ed Fredkin gibt es ein berühmtes Zitat: „Artificial Intelligence is the next step in evolution“². Das wohl witzigste Zitat zur KI stammt von John McCarthy und wurde in der TV-Serie The Mind Machines von 1978 aufgezeichnet, die auf Youtube zu finden ist. Im Drehbuch gleich dahinter: Die Einschätzung von Joe Weizenbaum, diesmal als erster Kritiker der KI.

Nun zu Joe Weizenbaum und seinem Programm ELIZA. John

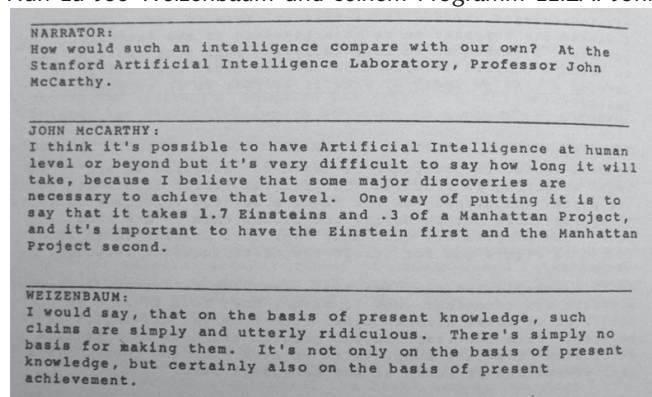


Abbildung 3: Drehbuch von Nova zu The Mind Machines

McCarthy gehörte zu den Pionieren der Künstlichen Intelligenz. Zusammen mit Marvin Minsky und Claude Shannon veranstaltete McCarthy im Juni 1956 einen acht Wochen dauernden Workshop mit 35 Teilnehmern am Dartmouth College, der praktisch die Künstliche Intelligenz als Forschungsrichtung begründete. Unter dem Titel *Künstliche Neurosen* berichtete die Philosophin Margaret Boden über den Workshop: „Freud hat gezeigt, dass der Mensch neurotisch programmierbar ist, jetzt müssen nur noch die Computer die entsprechenden Programme haben, um sich mit dem Menschen verständigen zu können.“ Diese Zusammenfassung animierte Joe Weizenbaum, die Skripte DOCTOR und ELIZA zu schreiben. Was Weizenbaum zu Demonstrationszwecken programmierte, wurde nämlich von einigen Menschen für bare Münze genommen, als ein Computer, mit dem man sich unterhalten kann. Weizenbaum machte eines Tages die Entdeckung, dass selbst seine Sekretärin, die doch sein Programmierprojekt kannte, sich mit dem Computer unterhielt und Weizenbaum bat, das Zimmer zu verlassen, weil sie Intimes mit dem Rechner besprechen wollte.

„Eliza ist als Programm incredibly simple, wirklich, hat aber im Herzen einen Punkt getroffen, das macht es ein bisschen kompliziert, nicht der einfache Code. Eliza wurde missverstanden, als intelligentes System, das aber ist ein Fehler, der genau in unsere Zeit passt“, so Weizenbaum zu seinem 80. Geburtstag.

Das Blumenmädchen Eliza Doolittle aus Shaws Pygmalion ist die

Namensgeberin. Sie wird von einem Linguisten in der Sprache der Oberschicht trainiert und ist dann die Oberschicht. Das ist eine Vorwegnahme von John Searles Chinesisches Zimmer und ein kleiner Seitenhieb auf den mit Weizenbaum befreundeten Noam Chomsky, bei dem er sich im Vorwort von Computer and Human Reason bedankt. Viele kennen heute weder *Pygmalion* noch *My Fair Lady*, am ehesten vielleicht die Adaption des Themas unter Titeln wie *Lisa, der helle Wahnsinn* oder eben *Pretty Woman*.



Abbildung 4: Zeitgenössische Anzeige zu Shaws Theaterstück

Weizenbaum selbst analysierte das, was die Dame an Reaktionen erzeugte und schrieb darüber sein *Computer and Human Reason* (dt. *Die Macht der Computer und die Ohnmacht der Vernunft*). Diese Abrechnung mit dem unbedingten Glauben an die Möglichkeiten der Computer brachte Weizenbaum die geharnischte Kritik seiner Zunft ein. „Das unvernünftige Buch ist genauso wirr und schlecht wie ELIZA“, donnerte John McCarthy 1976 in der Zeitschrift *Creative Computing*³, „es ist an der Zeit, festzuhalten, dass der Computer eine unschuldige Maschine ist.“ Diese Kritik „erschien zuerst als öffentliche Datei in dem Arpanet“, so die Herausgeber der *Creative Computing* in einer Fußnote. Gut möglich, dass der Aufsatz von McCarthy die erste Buchkritik im Internet darstellt.

Mit Beginn der Forschung über Künstliche Intelligenz wandelte sich das Bild über Roboter und intelligente Maschinen. Dominierten bis dahin Illustrationen wie die Glubschaugen des ungarisch-amerikanischen Zeichners Boris Artzybasheff das Bild, so gaben mit Beginn der AI-Projekte wie SUMEX-AIM (*Stanford University Medical Experimental Computer for Artificial Intelligence in Medicine*) neue Impulse. Das menschliche Gesicht wurde als Platinen-Layout dargestellt.⁴ Anstelle von ELIZA wurde in der SUMEX-AIM-Broschüre der Dialog von PARRY abgedruckt. Zuvor hatte sich der Programmierer von PARRY, der einflussreiche Psychiater Kenneth Colby 1970 begeistert geäußert: „Wenn sich die ELIZA-Methode bewähren sollte, so hätten wir damit ein therapeutisches Werkzeug, das man allen Nervenkliniken und psychiatrischen Zentren an die Hand geben könnte, die über zu wenig Therapeuten verfügen. /.../ In einer Stunde könnten mehrere hundert Personen von einem /.../ Computersystem behandelt werden.“⁵

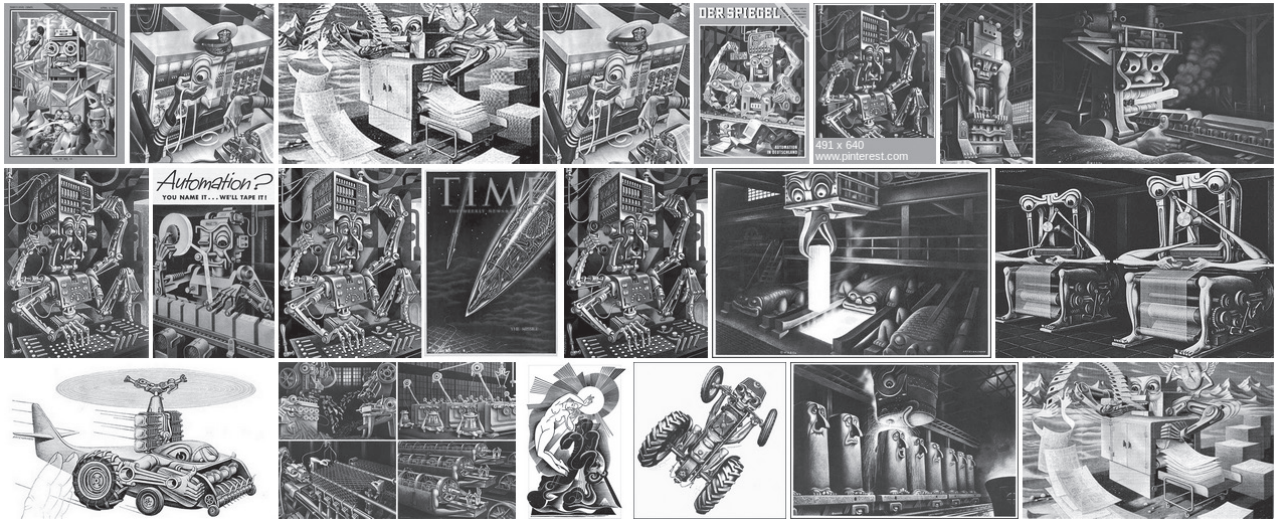


Abbildung 5: Beispiele typischer Artzybasheff-Bilder

Weil das Internet in diesen Tagen seinen 50. Geburtstag feiert, sei zum Schluss auf zwei lustige Fakten verwiesen. Die hochgesteckten Ziele des Projekts SUMEX-AIM wurden nicht erreicht, denn es begann Anfang der 80er Jahre das, was heute KI-Winter genannt wird. Ein Produkt von SUMEX-AIM nutzen wir indes noch heute, es ist das Mail-Protokoll IMAP für die Darstellung von E-Mails auf verschiedenen Endgeräten. Zur ersten großen Geburtstagsfeier des Internets bzw. des Vorläufers Arpanet koppelte der Internet-Pionier Vint Cerf im Jahre 1972 PARRY an der Universität Stanford mit ELIZA am MIT zusammen. Das „Gespräch“ der beiden Programme wurde als RFC 439 veröffentlicht.⁶

Weil wir heute im Zeitalter der Fakes leben, ende ich mit einem Zitat aus *The Counterfeiters* des britischen Literaturwissenschaftlers Hugh Kenner (dt. *Kunst im Zeitalter von Xerox*). Er schrieb über Weizenbaums ELIZA: „Doch viele geschäftige Menschen /.../ wenden ihre ganze Begabung auf, ein Umweltfeld zu entwickeln, das perfekt zugeschnitten ist auf eine Welt voll flinken kleinen Idioten, die wie Menschen aussehen. In dieser Welt ‚verstärken‘ Lernmaschinen Antworten, indem sie einfache Begriffe ständig wiederholen und Willfähigkeit mit simuliertem Entzücken herausfordern. Es ist eine gefälschte Welt für gefälschte Personen.“

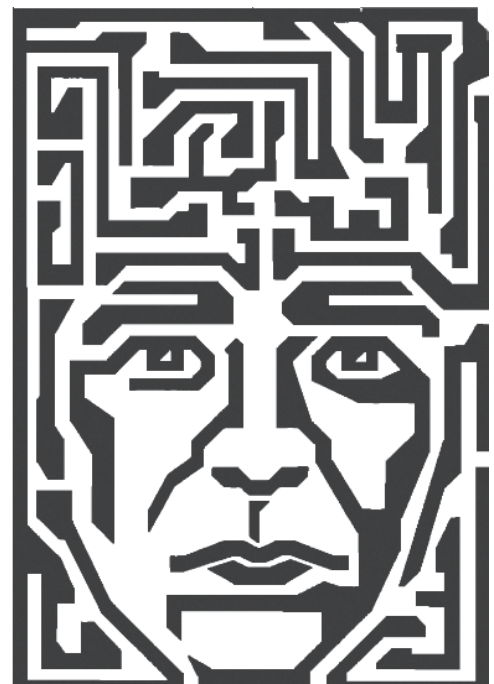


Abbildung 6: Foto: SUMEX-AIM

Anmerkungen

- 1 https://en.wikiquote.org/wiki/Claude_Elwood_Shannon
- 2 Zu finden im Buch „*The Second Self*“ (dt. *Die Wunschmaschine*) von Sherry Turkle

- 3 In: *Creative Computing*, Sept/Okt 1976, S.84ff
- 4 Vgl. Gregory Freiherr: *The Seeds of Artificial Intelligence – SUMEX-AIM* (1980)
- 5 Zitiert nach Weizenbaum: *Die Macht der Computer und die Ohnmacht der Vernunft*, Frankfurt am Main: Suhrkamp, 1977
- 6 <https://tools.ietf.org/html/rfc439>



Detlef Borchers

Detlef Borchers ist freier Journalist und arbeitet überwiegend für den Heise-Verlag.

Jahresrückblick 2018/19

Eine freudige Achterbahnfahrt durch das FlfF-Jahr

In unserem Jahresrückblick stellen wir die wichtigsten Aktivitäten des FlfF seit der FlfF-Konferenz 2018 dar, die im September 2018 in Berlin stattfand. Mit Auszügen aus unseren Stellungnahmen, Pressemitteilungen und Beiträgen zur FlfF-Kommunikation illustrieren wir die Aktivitäten. Die Liste ist nicht vollständig; wir sind auch darüber hinaus als AutorInnen, bei Veranstaltungen, Demonstrationen und weiteren Aktivitäten beteiligt.

September 2018

Wie im letzten Jahr beginnen wir unseren Bericht mit der **FlfF-Konferenz 2018**¹, die – wie bereits berichtet – vom Berliner Team organisiert wurde und unter dem Leitmotiv *Brave New World – Gestaltungsfreiheiten und Machtmuster soziotechnischer Systeme* stand. In der Einleitung zum Schwerpunkt in der FlfF-Kommunikation² hieß es:

„Viele Produkte, Entwicklungen und Einsatzfelder der Informatik scheinen sich unausweichlich und technisch notwendig so entwickelt zu haben, wie wir sie heute kennen. ... Technische Entwicklungen bauen aufeinander auf, aber finden natürlich nicht im luftleeren Raum statt. ...

Oftmals liegen den tatsächlichen Entwicklungen gerade keine primär technischen Überlegungen zu Grunde, sondern ökonomische oder politische Motive. Folglich ist es erhellend, Informatik- und Technikgeschichte auch unter diesen Aspekten zu betreiben. So können Entscheidungsalternativen oder Weggabelungen herausgestellt werden, um die dahinterliegenden Machtinteressen, aber auch die sachlichen wie sozialen Dynamiken und Zwänge freizulegen. Dieses Wissen ermöglicht es dann, heutige technische Entwicklungen und Weichenstellungen besser zu verstehen.

Doch wir wollen auch aktiv an aktuellen und zukünftigen tiefgreifenden Veränderungen mitwirken, denn die Informatik ist immer auch Gestaltungsdisziplin ... Wir wollen also mithelfen, die stetige Digitalisierung und Vernetzung der Gesellschaft so mitzuprägen, dass die Freiheit des Individuums und das Wohl der Gesellschaft im Vordergrund jeglicher Technikentwicklung und ihres Einsatzes stehen ...“

Erstmals verliehen wir die neu geschaffene **Weizenbaum-Medaille** an Wolfgang Coy:

„Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung verleiht die Weizenbaum-Medaille 2018 für seine außerordentlichen Verdienste um das Lehr- und Forschungsgebiet Informatik und Gesellschaft an Wolfgang Coy. Als Professor für Informatik in Bildung und Gesellschaft an der Humboldt-Universität zu Berlin hat er das Fach Informatik und Gesellschaft in Forschung und Lehre einzigartig, beispielhaft und maßgeblich ausgestaltet unter Einbeziehung medienthe-



Dagmar Boedicker (nicht im Bild), Rainer Rehak und Stefan Hügel blicken auf das vergangene Jahr zurück, Foto: Michael Ahlmann

oretischer, sozial- und kulturgeschichtlicher, fachdidaktischer und ethischer Gesichtspunkte.“³

Den bisherigen FlfF-Studienpreis verliehen wir erstmals als **Weizenbaum-Studienpreis**⁴, ihn erhielten in diesem Jahr:

- Leon Kaiser für seine Arbeit *Vulnerable Systems: The Quantification of Affect in an Experimental Blockchain Pilot-Project for Financial Transaction Management for Refugees*,
- Severin Engelmann für seine Arbeit *The Digital Dimensions of Personal Identity*,
- Nico Lück für seine Arbeit *Künstliche Intelligenz und Rüstungskontrolle. Der Einsatz maschinellen Lernens in Waffensystemen und Verifikationsmaßnahmen* und
- Jörg Pohle für seine Arbeit *Datenschutz und Technikgestaltung*.

Rekordverdächtig war die Verarbeitung der Konferenz in der FlfF-Kommunikation. Sie reichte über drei Ausgaben, beginnend mit dem Bericht über die Verleihung der Weizenbaum-Medaille in Ausgabe 4/2018 hin zu ausführlichen Konferenzberichten in den Ausgaben 1 und 2/2019.

Oktober 2018

Das FlfF unterstützte die Großdemonstration **#unteilbar – Solidarität statt Ausgrenzung** in Berlin, an der rund 2.500.000 Menschen teilnahmen. Im Aufruf hieß es unter anderem:

„Es findet eine dramatische politische Verschiebung statt: Rassismus und Menschenverachtung werden gesellschaftsfähig. Was gestern noch undenkbar war und als unsagbar galt, ist kurz darauf Realität. Humanität und Menschenrechte, Religionsfreiheit und Rechtsstaat werden offen angegriffen. Es ist ein Angriff, der uns allen gilt. Wir lassen nicht zu, dass Sozialstaat, Flucht und Migration gegeneinander ausgespielt werden. Wir halten dagegen, wenn Grund- und Freiheitsrechte weiter eingeschränkt werden sollen. [...]“

Während der Staat sogenannte Sicherheitsgesetze verschärft, die Überwachung ausbaut und so Stärke markiert, ist das Sozialsystem von Schwäche gekennzeichnet: Millionen leiden darunter, dass viel zu wenig investiert wird, etwa in Pflege, Gesundheit, Kinderbetreuung und Bildung.“⁵

Das FIF war an einem Offenen Brief⁶ an ausgewählte Mitglieder der Bundesregierung beteiligt mit der Aufforderung, die **E-Pri-vacy-Verordnung** nicht weiter zu torpedieren und auf EU-Ebene endlich für einen wirksamen Schutz unserer Online-Aktivitäten einzutreten. 16 Organisationen fordern darin:

1. Stärken Sie den Rechtsrahmen für elektronische Kommunikation.
2. Schützen Sie Privatsphäre und Wettbewerb.
3. Sichern Sie die Privatsphäre durch Technikgestaltung und Voreinstellung.
4. Schützen Sie vor Tracking Walls.
5. Verhindern Sie Massenüberwachung und Vorratsdatenspeicherung.



Aktive FIF-Mitglieder im Einsatz

November 2018

Das FIF ist Mitglied im Trägerkreis der Konferenz **Bits & Bäume**, die am 17./18. November 2018 in Berlin stattfand. Kernforderung ist, dass die Digitalisierung Gemeinwohl und Frieden dienen, Datenschutz ernst nehmen sowie soziale und ökologische

Ziele fördern soll. In der gemeinsamen Pressemitteilung, in der die gemeinsamen Forderungen⁷ vorgestellt werden, heißt es:

„Die Digitalisierung muss so gestaltet werden, dass sie dem Gemeinwohl und Frieden dient, Datenschutz ernst nimmt und soziale und ökologische Ziele gleichermaßen fördert. Dies forderte ein Bündnis von zehn Organisationen aus Umwelt- und Netzpolitik, Entwicklungszusammenarbeit und Wissenschaft gestern zum Abschluss der Konferenz Bits & Bäume in Berlin. Eine nachhaltige Digitalisierung ist machbar, aber ihre Gestaltung dürfe nicht alleine Politik und Wirtschaft überlassen werden. Zivilgesellschaft und kritische Wissenschaft müssten diese nachhaltig mitgestalten, so die Veranstalter. An der bislang größten Konferenz für Digitalisierung und Nachhaltigkeit nahmen am vergangenen Wochenende mehr als 1.700 Nachhaltigkeits- und Umwelt-Engagierte sowie NetzaktivistInnen teil.“⁸

Das FIF war mit mehreren Beiträgen auf der Konferenz vertreten⁹. Sie soll Auftakt für eine Bewegung werden – die Initiatoren rufen dazu auf, unter dem Namen Bits & Bäume weitere Veranstaltungen regional zu organisieren¹⁰.

Dezember 2018

Zwischen den Jahren waren wir wieder in Leipzig, beim **Chaos Communication Congress 35c3**. Neben unserem großen Informationsstand, der auf reges Interesse stieß, gab es zwei Veranstaltungen mit Rainer Rehak zum Datenschutz¹¹ und zum Informationsfreiheitsgesetz¹².

Januar 2019

Das Jahr 2019 begann mit einem Wechsel im Amt des **Bundesbeauftragten für Datenschutz und Informationsfreiheit**¹³. Ulrich Kelber trat das Amt am 7. Januar 2019 an. Seine ersten Stellungnahmen¹⁴ lassen erwarten, dass er sich wesentlich engagierter für den Datenschutz einsetzen wird als seine Vorgängerin.

Das FIF beteiligte sich an einem offenen Brief an die deutschen Abgeordneten im LIBE-Ausschuss des europäischen Parlaments. Wir drückten darin unsere Besorgnis über den **Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Verhinderung der Verbreitung terroristischer Online-Inhalte**¹⁵ aus. In dem Brief heißt es:

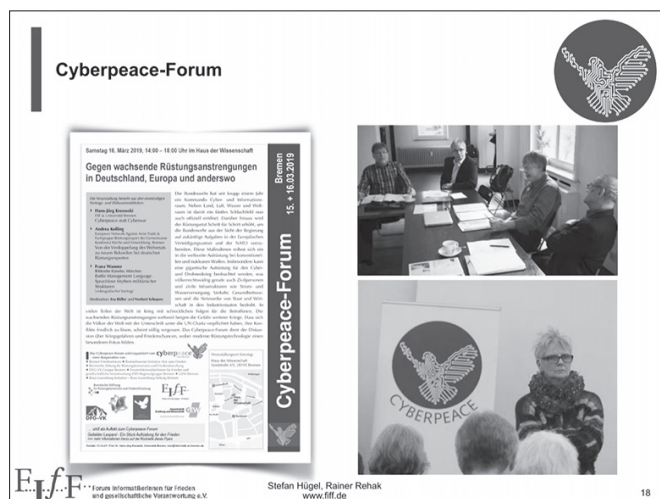
„... Der ausufernde Anwendungsbereich, die unsachgemäße Definition terroristischer Inhalte, technisch höchst zweifelhafte automatische Zensurmechanismen und die mit der Übertragung der Rechtsdurchsetzung an Dritte verbundene Einschränkung des Rechtswegs stellen eine ernsthafte Bedrohung für Meinungsfreiheit, Informationsfreiheit, Vertraulichkeit der Kommunikation und die Vielfalt der medialen Landschaft des Internets dar.“

Wie in den Vorjahren organisierte die Regionalgruppe München 2019 wieder mehrere **Cryptoparties**, bei denen Grundlagen der Verschlüsselung und der sicheren Kommunikation vermittelt wurden.

März 2019

Anfang 2019 nehmen zwei Bewegungen Fahrt auf, die zu großen Teilen von einer politisierten Jugend getragen werden: Die durch Greta Thunberg mit ihren Schulstreiks initiierte Bewegung **FridaysForFuture**¹⁶, die angesichts der immer deutlicher werdenden Klimakatastrophe endlich wirksame Maßnahmen zum Klimaschutz fordert und die Protestbewegung **NoArticle13**¹⁷, die sich für ein offenes Internet und gegen Upload-Filter einsetzt. Das FIfF begleitete diese Initiativen, beispielsweise durch Beteiligung an der **Bits-&-Bäume**-Bewegung. In einer Pressemitteilung stellten wir den Zusammenhang zwischen den Bewegungen her:

„Europaweit regt und erhebt sich eine politisierte Jugend, die mit der aktuellen Ausrichtung der Politik grob unzufrieden ist, da diese auf Kosten der Zukunft verbissen an alten Denk- und Handlungsweisen festhält. Dabei kristallisieren sich zwei sich überlappende Bewegungen heraus, die einen kämpfen für eine langfristig bewohnbare und gerechte materielle Welt, also für einen lebensfreundlichen Planeten. Die anderen kämpfen für eine langfristig freie, faire und inklusive immaterielle Welt, also für ein offenes, dezentrales Internet.“¹⁸



Am 15./16. März fand in Bremen das **Cyberpeace-Forum** statt, organisiert vom **Cyberpeace-Team Bremen**, einer Kooperation des Bremer Friedensforums, der Bremerhavener Initiative *Mut zum Frieden*, der DFG-VK-Gruppe Bremen, der FIfF-Regionalgruppe Bremen, der GEW Bremen und der Rosa-Luxemburg-Initiative – Rosa-Luxemburg-Stiftung Bremen. Von Hans-Jörg Kreowski gab es einen Vortrag *Cyberpeace statt Cyberwar*.

Am 29. März gab es einen **Greenpeace**¹⁹ **Greencast** zu Tihange-Doel Radiation Monitoring²⁰. Weitere FIfF-nahe Greencasts wurden im April zu Bits & Bäume²¹, im August zu Fairer IT²² und zum Recycling von Elektronik²³ veröffentlicht.

Mai 2019

Mit Beschluss vom 26. Juni 2018 hat der Deutsche Bundestag eine **Enquête-Kommission Künstliche Intelligenz – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und**

ökologische Potenziale eingerichtet²⁴. Hans-Jörg Kreowski wurde eingeladen, dort zum Thema *KI, äußere Sicherheit und Verteidigung* zu sprechen. Sein Fazit ist in einem Bericht²⁵ zusammengefasst. Er fordert:

„Wegen der mit letalen autonomen Waffen verbundenen ethischen und technischen Probleme sollte Deutschland für eine uneingeschränkte Ächtung solcher Systeme auf internationaler Ebene eintreten und auf nationaler Ebene einen unbedingten Verzicht festschreiben.“

Er kritisiert auch die unzulängliche Einbeziehung der Öffentlichkeit. Damit verpasse die Kommission die Chance eines breiten und offenen gesellschaftlichen Diskurses.

Große politische Wellen schlug der Film²⁶ des Youtubers Rezo, **Die Zerstörung der CDU**, in dem er im Vorfeld der Wahlen zum Europäischen Parlament vor allem die Politik der CDU scharf kritisiert.

Das FIfF stellt sich hinter die Aussagen und Forderungen von Rezo zu den US-amerikanischen Drohenmorden, die ignoriert und damit de facto durch die Bundesregierung unterstützt werden. Wir erachten seine Standpunkte als grundsätzlich korrekt und gut begründet. Dies haben wir in einer Stellungnahme deutlich gemacht.

Rezo und eine Reihe weiterer Youtuber fordern kurz danach in einem weiteren Video²⁷ auf,

„Wählt nicht die CDU, wählt nicht die CSU und wählt nicht die SPD. Wählt auch keine andere Partei, die so wenig im Sinne von Logik und der Wissenschaft handelt und nach dem wissenschaftlichen Konsens mit ihrem Kurs unsere Zukunft zerstört. Und wählt schon gar nicht die AfD, die diesen Konsens sogar leugnet.“

Eine Premiere feierten wir am 23. Mai 2019, dem 70. Jahrestag des Grundgesetzes. Erstmals waren wir als mitherausgebende Organisation am seit 1997 erscheinenden **Grundrechte-Report**²⁸ beteiligt. Neben der Beteiligung am Herausgeberkreis, in dem uns Hans-Jörg Kreowski vertritt, enthält der Band drei Beiträge von FIfF-Aktiven^{29,30,31}.

Juni 2019

Der neue Bundesbeauftragte für Datenschutz und Informationsfreiheit will den Dialog mit der Zivilgesellschaft stärken – dies macht er durch die Einladung zu einer **Gesprächsrunde** deutlich, zu der auch das FIfF eingeladen war. Sie soll halbjährlich wiederholt werden.

Juli 2019

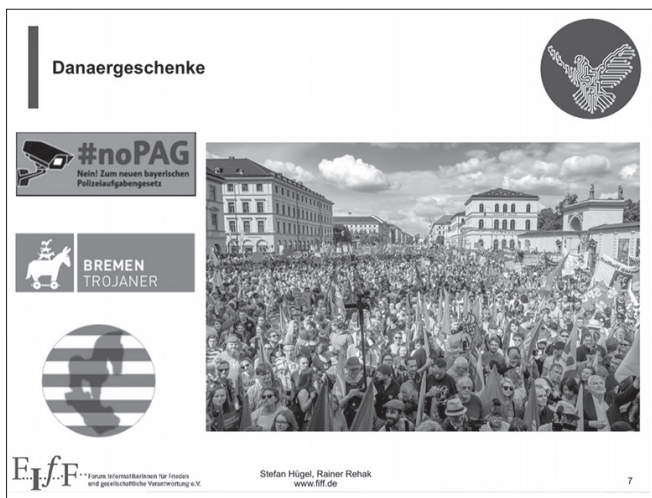
Am 2. Juli 2019 wurde eine Verfassungsbeschwerde gegen das **Hessische Sicherheits- und Ordnungsgesetz** unter Federführung der Gesellschaft für Freiheitsrechte eingereicht, an der das FIfF beteiligt war. In der dazu veröffentlichten Pressemitteilung heißt es:

„Die Beschwerde richtet sich gegen die Ausweitung der Überwachungsbefugnisse für Polizei und Verfassungsschutz. Mit dem Hessentrojaner und der Big-Data-Analysesoftware Hessendata liegt Hessen beim Angriff auf die Freiheitsrechte im Ländervergleich weit vorne.“

Mit der Analysesoftware Hessendata des US-Unternehmens Palantir kann die Polizei Menschen und ihr Umfeld vollständig durchleuchten. Hessendata vereint Daten aus zahlreichen Polizeidatenbanken. Die Software wertet aber auch externe Daten, zum Beispiel aus sozialen Medien, aus. Wer in den Fokus einer automatischen Datenanalyse gerät, wird schnell zum gläsernen Menschen.“³²

Unser Projekt **Tihange-Doel Radiation Monitoring** (TDRM) geht weiter. Das Sensor-Netzwerk läuft stabil und wird weiter ausgebaut. Ein Warnmeldeprozess wird technisch und organisatorisch implementiert. Parallel dazu treten Mitglieder des Projekts in der Öffentlichkeit auf, beispielsweise am 7. Juli 2019 bei der Anti-Atom-Fahrraddemo *Tour Becquere*³³.

Weiterhin ist das FIF im **#noPAG-Bündnis** gegen das neue Polizeiaufgabengesetz in München beteiligt – auch wenn wir nicht mehr im SprecherInnenrat vertreten sind. Wir sind Mitveranstalter bei Aktionen, z. B. bei einer Vorführung des Films *Hamburger Gitter*³⁴ am 9. Juli 2019.



Mitveranstalter der Demo in München

August 2019

Beim **CCCamp 2019** waren wir an der Organisation des Clusters about:freedom beteiligt, mit eigener Stage, Future Panel mit FIF, FridaysForFuture, XR, c3sustainability, Vortrag *Blockchain – proof of ignorance*, Filmvorstellung durch und Diskussion mit der investigativen Journalistin Gaby Weber und einer Session zur Vorstellung der Bits & Bäume-Forderungen.

Oktober 2019

In einem offenen Brief³⁵ warnten 13 Organisationen vor der **E-Evidence-Verordnung** der Europäischen Union. In der dazu veröffentlichten Pressemitteilung heißt es:

„Mit der Verordnung könnten nationale Strafverfolger EU-weit Provider zwingen, Daten herauszugeben – ohne dass das Land, in dem der Provider sitzt oder die Daten gespeichert sind, mitentscheidet. Zum Beispiel müssten E-Mail-Dienste oder Messenger Verbindungsdaten und sogar Inhalte von Nachrichten herausgeben. Dabei ist nicht erforderlich, dass die Tat, wegen der ermittelt wird, in dem Staat, in dem der Provider sitzt oder in dem der Beschuldigte lebt, überhaupt eine Straftat ist.“³⁶

November 2019

Seit Jahren unterstützt das FIF die **Konferenz der Informatik-fachschaften** (KIF)³⁷. Bei der diesjährigen Konferenz in Magdeburg stellten wir das FIF und den Weizenbaum-Studienpreis vor. Laut Vergabeordnung des Weizenbaum-Studienpreises hat die KIF das Recht, eine VertreterIn in die Auswahlkommission zu entsenden.

Am 22.-24. November 2019 fand in Bremen die **FIF-Konferenz 2019**³⁸ unter dem Leitmotiv Künstliche Intelligenz als Wunderland statt. In der Einladung dazu heißt es:

„In der berühmten Erzählung *Alice im Wunderland* von Lewis Carroll begegnet die Protagonistin im Wunderland den merkwürdigsten Gestalten und erlebt kuriose Abenteuer. Ein neues Wunderland eröffnet sich heute durch Künstliche Intelligenz. Es ist von Robotern bevölkert, die Fußball spielen, tanzen, jonglieren, kochen, Dienstleistungen aller Art erbringen, Alte und Kranke pflegen und Orte erkunden, die für Menschen gefährlich oder unerreichbar sind. ...

Aber mit dem erreichten Stand der KI sind auch übertriebene Erwartungen, übersteigerte Hoffnungen und höchst problematische Anwendungsmöglichkeiten verbunden. KI wird von Politik und Wirtschaft weltweit als Schlüsseltechnologie gesehen, von der die zukünftige Wertschöpfung abhängt und die einen signifikanten Teil der heutigen Arbeitsplätze obsolet werden lassen könnte. Die sich abzeichnenden Anwendungen im militärischen Kontext führen zu einer gigantischen Rüstungsspirale, was die Gefahr von Kriegen wohl kaum verringern wird. KI-basierte Überwachungsmethoden lassen tiefe Eingriffe in die Privatsphäre und andere Grundrechte befürchten bis hin zu einer sozialen Totalüberwachung, wie sie in China auf der Tagesordnung steht. Auf der Weltbühne ist ein geostrategisches Wettrennen entbrannt, wer bei KI die Nase vorn hat.“

Den Weizenbaum-Studienpreis 2019 verliehen wir in diesem Jahr an:

- Thomas Gruber für seine Arbeit *Verquickung der mathematischen und informatischen Forschung an zivilen deutschen Hochschulen mit der modernen Kriegsführung*,
- Alexandra Keiner für ihre Arbeit *Legitimität von Algorithmen in politischen Verwaltungsorganisationen* und

- Philipp Imperatori für seine Arbeit *Verschlüsselungspolitik der USA. Eine vergleichende Analyse der historischen Entwicklung*.

Das FfF unterstützte die **Klimastreikwoche**, zu der #students4future, #fridaysforfuture und #scientists4future für die Woche vom 25. bis 29. November 2019 aufrufen. Im Aufruf dazu heißt es:

„Die Dramatik einer Situation, in der die Gewissheit über den bevorstehenden Klimakollaps sich nicht in effektives politisches Handeln übersetzt, macht außerplanmäßiges Handeln zur Pflicht. Die Studierenden von Students for Future rufen für die Woche vom 25.-29. November zur Bestreikung des regulären Lehrbetriebs auf.“³⁹



Das FfF unterstützt die Klimastreikwoche

Anmerkungen

- <https://2018.fiffkon.de>
- Brave new World – Editorial zum Schwerpunkt. FfF-Kommunikation 1/2019, S. 12-13.
<https://www.fiff.de/publikationen/fiff-kommunikation/fk-jhrg-2019/fk-2019-1/fk-2019-1-content/fk-1-19-p12.pdf>
- Hans-Jörg Kreowski (2018) Laudatio anlässlich der Verleihung der Weizenbaum-Medaille an Wolfgang Coy. FfF-Kommunikation 4/2018, S. 6-9. <https://www.fiff.de/studienpreis/Laudatio-Coy-2018>. Dazu auch Wolfgang Coy (2018) Kein Problem! Alles klar, oder ...? Aufbereitung ethischer Konflikte in Dialogen. FfF-Kommunikation 4/2018, S. 9-13.
<https://www.fiff.de/publikationen/fiff-kommunikation/fk-2018/fk-2018-4/fk-2018-4-content/fk-4-18-p9.pdf>
- <https://www.fiff.de/studienpreis>
- <https://www.unteilbar.org>
- <https://www.fiff.de/presse/pressemitteilungen/offenerbriefprivacy2018>
- <https://www.fiff.de/bub-forderungen>
- <https://www.fiff.de/presse/pressemitteilungen/bub-pm-forderungen>
- <https://www.fiff.de/veranstaltungen/bub-fiff-family>
- <https://bits-und-baeume.org/waechst/de>
- Rainer Rehak (2018) Wen schützt eigentlich der Datenschutz? Warum DatenschützerInnen aufhören müssen, von individueller Privatheit zu sprechen. https://media.ccc.de/v/35c3-9733-was_schutzt_eigentlich_der_datenschutz
- Arne Semsrott, Rainer Rehak, Andre Meister und Anna Biselli (2018) Best of Informationsfreiheit. Transparenz mit der Brechstange. https://media.ccc.de/v/35c3-9507-best_of_informationsfreiheit
- <https://www.bfdi.bund.de>
- z. B. am 13. Januar 2019 bei Golem.de: Kelber fordert endgültiges Ende der Vorratsdatenspeicherung. <https://www.golem.de/news/bundesdatenschutzbeauftragter-kelber-fordert-endgueltiges-ende-der-vorratsdatenspeicherung-1901-138690.html>
- <https://www.fiff.de/OffenerBriefLI>
- <https://fridaysforfuture.de>
- In der Endfassung wurde Artikel 13 zu Artikel 17.
- <https://www.fiff.de/presse/pressemitteilungen/Artikel13fridaysforfuture>
- <https://greenpeace.berlin/tag/greencast/>
- <https://greenpeace.berlin/2019/04/greencast-217-tdrm/>
- <https://greenpeace.berlin/2019/04/greencast-218-luftdaten-info/>
- <https://greenpeace.berlin/2019/08/greencast-221-fair-it/>
- <https://greenpeace.berlin/2019/08/greencast-222-elektronik-recycling/>
- BT-Drs. 19/2978, <http://dip21.bundestag.de/dip21/btd/19/029/1902978.pdf>
- Hans-Jörg Kreowski (2019) Ein kurzer Einblick in die Arbeit der Enquete-Kommission Künstliche Intelligenz. FfF-Kommunikation 2/2019, S. 7-9.
<https://www.fiff.de/publikationen/fiff-kommunikation/fk-jhrg-2019/fk-2019-2/fk-2019-2-content/fk-2-19-p7.pdf>
- Die Zerstörung der CDU: <https://www.youtube.com/watch?v=4Y1ZQsyuSQ>
- Ein Statement von 90+ Youtubern: <https://www.youtube.com/watch?v=Xpg84NjCr9c>
- Bellinda Bartolucci, Iris Burdinski, Marie Diekmann, Rolf Gössner, Julia Heesen, Martin Heimig, Hans-Jörg Kreowski, Britta Rabe, Rosemarie Will (Hg.): Grundrechte-Report 2019. Zur Lage der Bürger- und Menschenrechte in Deutschland. Frankfurt am Main: Fischer-Taschenbuchverlag. <http://www.grundrechte-report.de>
- Stefan Hügel, Rainer Rehak: Kampf um Troja. Verwundbarkeit der vernetzten Gesellschaft durch Nutzung von Schadsoftware. Grundrechte-Report 2019, S. 23-27
- Stefan Hügel, Rainer Rehak: Künstliche Intelligenz im Wahlkampf. Zentralisierung und politische Profilbildung gefährden die Demokratie. Grundrechte-Report 2019, S. 131-135
- Hans-Jörg Kreowski: Extralegale Tötung durch Drohnen und autonome Waffen. Kampfdrohnen für die Bundeswehr. Grundrechte-Report 2019, S. 175-178
- https://www.fiff.de/presse/pressemitteilungen/Verfassungsbeschwerde_Hessentrojaner
- <https://tihange-abschalten.eu/2019/05/tour-becquerel-raddemo-2019/>
- <https://www.hamburger-gitter.org>
- <https://digitalegesellschaft.de/2019/10/offener-brief-an-die-deutschen-abgeordneten-des-europaischen-parlaments-kein-grenzueberschreitender-direktzugriff-auf-persoenele-daten-durch-die-e-evidence-verordnung/>
- https://www.fiff.de/OB_E-Evidence
- <https://wiki.kif.rocks>
- <https://2019.fiffkon.de>
- <https://studentsforfuture.info/public-climate-school/aufruf-der-wissenschaft/>

Verleihung des Weizenbaum-Studienpreises 2019

„Ich bin kein Computerkritiker.
Dieser Begriff ist sinnlos. Computer können mit Kritik nichts anfangen.
Nein, ich bin Gesellschaftskritiker.
Es geht mir um die Rolle des Computers in unserer Gesellschaft.“
Joseph Weizenbaum



Weizenbaum
Studienpreis



Auch im Jahr 2019 haben wir den Weizenbaum-Studienpreis verliehen, gewidmet Professor Dr. Joseph Weizenbaum, der die Gründung des FfF gefördert hat, dem wir 1998 einen Ehrenpreis des FfF für seinen Einsatz für Verantwortung in der Informatik verliehen haben und der dessen langjähriges Vorstandsmitglied war.

Informatiksysteme sind geronnene Machtstrukturen, die dafür genutzt werden, die Produktivität der menschlichen Arbeitskraft zu erhöhen und ihre Nutzung zu optimieren. Bei ihrer Konzeption und Implementierung werden Entscheidungen getroffen, die diese Machtstrukturen festlegen und weiter verfestigen. Dies gilt für alle Bereiche: Für die industrielle Produktion, für Dienstleistungen, für das Militär, für die öffentliche Sicherheit. Funktionalisierende Technik wird stets auch angewendet – unabhängig von ihrer Rechtmäßigkeit und ihrer Sozialverträglichkeit.

Es ist die gesellschaftliche Aufgabe der Informatikerinnen und Informatiker, technische Systeme auch von ihren ethischen, sozialen und rechtsstaatlichen Anforderungen her zu denken, um eine Technik zu verhindern, die zum Selbstzweck wird und schädliche Nutzung als „Sachzwang“ etabliert. Mit unserem Studienpreis wollen wir Arbeiten auszeichnen, die dieser Aufgabe gerecht werden.

Eine Jury, besetzt mit

- Professorin Britta Schinzel aus Freiburg,
- Professor Jochen Koubek aus Bayreuth,
- Stefan Hügel aus Frankfurt am Main,
- Rainer Rehak aus Berlin,

- Richard Schöbel aus Chemnitz als Vertreter der Konferenz der Informatikfachschaften

hat aus den Einreichungen für den Studienpreis 2019 drei Arbeiten ausgewählt, die wir heute hier prämiieren werden:

- **Thomas Gruber** für seine Arbeit *Verquickung der mathematischen und informatischen Forschung an zivilen deutschen Hochschulen mit der modernen Kriegsführung*,
- **Alexandra Keiner** für ihre Arbeit *Legitimität von Algorithmen in politischen Verwaltungsorganisationen* und
- **Philipp Imperatori** für seine Arbeit *Verschlüsselungspolitik der USA. Eine vergleichende Analyse der historischen Entwicklung*.

Wir bedanken uns herzlich bei allen Teilnehmerinnen und Teilnehmern für die eingereichten Arbeiten und gratulieren der Preisträgerin und den Preisträgern. Die Texte der abgedruckten Laudationes wurden zum wesentlichen Teil von Britta Schinzel und Stefan Hügel vorbereitet. Näheres zum Weizenbaum-Studienpreis ist unter <https://www.fiff.de/studienpreis> zu finden.



FfF e. V. – Stefan Hügel: Laudatio für den 1. Preis

Thomas Gruber: Verquickung der mathematischen und informatischen Forschung an zivilen deutschen Hochschulen mit der modernen Kriegsführung

Dissertation an der Universität Bremen

Der Autor zitiert einleitend die „Physiker“ von Friedrich Dürrenmatt und macht damit gleich zu Beginn den Standpunkt der Arbeit klar: „Es gibt Risiken, die man nie eingehen darf: der Untergang der Menschheit ist ein solches. Was die Welt mit den Waffen anrichtet, die sie schon besitzt, wissen wir, was sie mit jenen anrichten würde, die ich ermögliche, können wir uns denken.“ Aus ethischer Sicht folgt dies dem kategorischen Imperativ von Hans Jonas für die technologische Zivilisation: „Handle stets so, dass die Wirkungen deiner Handlung verträglich sind mit der Permanenz echten menschlichen Lebens auf Erden.“ Aus dieser Positionierung heraus wird die Verquickung der mathematischen und informatischen Forschung an Hochschulen untersucht. Dabei gelingt es, die Verbindungen in mehreren Be-

reichen – Kryptologie, künstliche Intelligenz, Technomathematik – klar herauszuarbeiten und anhand einer Reihe von Beispielen zu belegen. Dabei geht er auch auf indirekte Verknüpfungen, z. B. über hochschulnahe Forschungsinstitute oder durch Dual-use, ein und zeigt auf, wie trotz bestehender Zivilklauseln Militärforschung weitergeführt wird.

Militärische Technik basiert zunehmend auf Informatik und Künstlicher Intelligenz. Damit werden auch die Forschungsergebnisse aus der Informatik und der Mathematik immer wichtiger. „So sind beispielsweise Kampf- und Überwachungsdrohnen, militärische Spionagesatelliten, moderne Lenkflugkörper und neue Konzepte für Angriffe auf feindliche Verschlüsselungs-

systeme stark abhängig von aktuellen mathematischen und informatischen Forschungsergebnissen“, so der Autor der hier prämierten Arbeit bereits in der Zusammenfassung. „Bisher ist [aber] die Frage nach den Verbindungen zwischen Mathematik, Informatik und Krieg weder in der Forschung noch im öffentlichen gesellschaftlichen Diskurs präsent“, so der Autor weiter.

In der Arbeit von Thomas Gruber, Verquickung der mathematischen und informatischen Forschung an zivilen deutschen Hochschulen mit der modernen Kriegführung, soll diese Lücke geschlossen werden. Die Arbeit ist als Dissertation an der Universität Bremen entstanden. Wir verleihen dieser Arbeit heute den ersten Preis des Weizenbaum-Studienpreises 2019.

Viele Hochschulen haben Zivilklauseln in ihre Satzung aufgenommen, die eine militärische Forschung eigentlich verbieten. Dennoch findet sie statt – teilweise in enger Zusammenarbeit mit Forschungsinstituten wie dem Fraunhofer-Institut, die der Zivilklausel nicht unterworfen sind, mit denen aber eine enge inhaltliche und personelle Verflechtung besteht. Teilweise wird militärische Forschung auch durch Dual-Use zivil bemäntelt, indem Ergebnisse „ziviler“ Forschung später für militärische Zwecke genutzt wird – und wohl auch von vornherein auch so angelegt ist. All dies zeigt diese Arbeit anhand einer beeindruckenden Fülle von Beispielen.

Die Arbeit behandelt einleitend Methoden der Mathematik behandelt und zeichnet den Weg über die Informatik zur militärischen Anwendung nach – dabei liegt ein besonderer Fokus auf der deutschen Forschungslandschaft – und stellt zuletzt den aktuellen Forschungsstand dar. Es folgen die Begrifflichkeiten, die Motivation der Arbeit und der damit angestrebte Diskurs über militärrelevante Forschung und danach die Ziele und die der Arbeit zugrunde liegenden Hypothesen.

Im Hauptteil der Arbeit wird zunächst der gesellschaftliche und universitäre Diskurs über die Militärforschung in Mathematik und Informatik nachgezeichnet. Auf einen historischen Abriss folgt die heutige Situation der Wissenschaftspolitik in Deutschland. Behandelt werden die Aspekte Dual-use – durch die Militärforschung quasi als Trojanisches Pferd in die Hochschulen eingeschleust wird –, gesellschaftliche Werte und rechtliche Aspekte – insbesondere das Spannungsfeld zwischen Frieden und Wissenschaftsfreiheit –, Interessen der Hochschule als Institution – die sich profilieren und wirtschaftlich geführt werden muss – und die Forderung nach Transparenz von Forschungsergebnissen, die im Gegensatz zu der von GeldgeberInnen häufig geforderten Geheimhaltung aus geschäftlichem (oder militärischem) Interesse stehen.

Danach folgt eine Darstellung der Anwendung von Mathematik und Informatik in der modernen Kriegführung. Die Ökonomisierung des Wissenschaftsbetriebs erfordert die Einwerbung von Drittmitteln, die neben der Privatwirtschaft von militärischen Einrichtungen kommen. Ein Ansatz, der militärischen Verwendung von Forschungsergebnissen entgegen zu wirken, sind Zusatzklauseln in Open-Source-Lizenzen, die eine solche Verwendung verbieten oder einschränken. Der Autor kritisiert auch, dass trotz bestehender Zivilklauseln vieler Hochschulen in der Öffentlichkeit kaum ein Diskurs über die Militärforschung stattfindet – als einen Grund dafür sieht er die zunehmende Akzeptanz des Militärs in der Gesellschaft.



Laudator Stefan Hügel

Die Verquickung mathematischer und informatischer Forschung mit der modernen Kriegführung wird sodann anhand von einer Reihe von Beispielen dargestellt. Dabei werden vier Bereiche behandelt:

- Die *Kryptologie* als Mittel, die für die Kriegführung notwendigen Informationen zu erhalten. Sie kann einen erheblichen Einfluss auf die militärische Taktik haben – damit besteht erhebliches Interesse militärischer Akteure, auf die entsprechende universitäre Forschung zu nehmen. Herausgearbeitet wird die Bedeutung der Kryptologie für Abschreckung und Überlegenheit durch das Erlangen von Informationshoheit, schnellen und flexiblen Angriffen, beispielsweise durch die Absicherung des Einsatzes von Spezialeinheiten, und der Fernsteuerung von Drohnen. Zivilgesellschaftliche Akzeptanz wird durch Dual-use – die Nutzung der Kryptologie für den Schutz der Zivilbevölkerung – hergestellt.
- *Spieltheorie* und künstliche Intelligenz, zum Beispiel für die Vorhersage von militärischen Lagen und den Ausgang von Konflikten oder für den Einsatz in autonomen Waffensystemen. Das Interesse an Spieltheorie und künstlicher Intelligenz führt zu erheblichen Auswirkungen auf die jeweilige Forschungslandschaft; Konzepte aus beiden Bereichen sind maßgeblich an moderner Kriegführung beteiligt.
- In der *Technomathematik* sind vor allem die Forschungsgebiete Optimierung, Numerik und Kontrolltheorie für das Militär interessant. Die Arbeit geht auf militärrelevante Drittmittelprojekte, das Interesse des Militärs an Studierenden der Numerik, Kooperationsprojekte in der Kontrolltheorie und den militärischen Einfluss auf die zivile Forschungslandschaft in der Ingenieurmathematik ein.
- Wesentliche Themen der aktuellen Forschung zur *Künstlichen Intelligenz* sind Mustererkennung, Klassifizierung von großen Datenmengen und Trackingverfahren zur Objektverfolgung; damit verbunden wissensbasierte Systeme, stochastische Verfahren und maschinelles Lernen – mit dem Beispiel der künstlichen neuronalen Netze. Es wird analysiert, wie kriegsrelevante KI-Projekte in die zivile Forschung einfließen, wie zivile Forschung militärisch genutzt wird, wie sich das Wissen in Konferenzen, Wettbewerben und durch Crowdsourcing verbreitet und wie die zivile Forschungs- und Studienlandschaft durch militärische Interessenträger beeinflusst wird.





In allen behandelten Forschungsbereichen wird der inhaltliche Zusammenhang anhand von Beispielen aus der Forschung dargestellt und die Verbindung zur militärischen Anwendung motiviert. Ebenfalls anhand von Beispielen wird die Verbindung des Militärs mit den Forschungseinrichtungen – Hochschulen und kooperierende Forschungsinstitute – dargestellt, dabei wird auch auf personelle Verbindungen an den einzelnen Instituten eingegangen. Häufiges Muster ist die Führung eines Hochschulinstituts und eines Instituts in einer nichtuniversitären Forschungseinrichtung in Personalunion.

Zuletzt werden die wesentlichen Aspekte zusammengefasst, Lösungsansätze diskutiert, wie der öffentliche Diskurs über militärrelevante Forschung gefördert werden kann und ein abschließender Ausblick gegeben.

Anhand einer beeindruckenden Fülle von Beispielen aus verschiedenen Forschungsbereichen stellt die Arbeit die Problematik der Verquickung von wissenschaftlicher Forschung und Militär überzeugend dar. Damit leistet sie einen wichtigen Beitrag zum öffentlichen Diskurs über Militärforschung und deren Le-

gitimität. Sie behandelt das Thema kritisch, indem sie nicht vor der bloßen Verbindung von Hochschulen und Militärforschung halt macht, sondern auch ein Schlaglicht auf die Verbindung mit nichtuniversitären Forschungseinrichtungen wirft und die Methoden zur Umgehung von Zivilklauseln offenlegt, die auf diese Weise zum Feigenblatt zu verkommen drohen. Neben mathematischem und informatischem Sachverstand sind dabei auch die politischen Gesichtspunkte zu betrachten. Dass die Arbeit dabei vor allem zu Beginn deutliche politische Wertungen enthält, ist zumindest ungewohnt. Der Wissenschaftlichkeit der Arbeit als Ganzes tut es nach unserer Auffassung aber keinen Abbruch – eher trägt es zur wissenschaftlichen Transparenz bei. Nicht zuletzt legt die Arbeit auch eine wichtige Grundlage zur Arbeit des FIF. In diesem Sinne sei sie darüber hinaus allen zur Lektüre empfohlen, die sich einen fundierten Überblick über das Thema verschaffen wollen. Die Jury des Weizenbaum-Studienpreises hat sich einhellig für die Vergabe des ersten Preises für die Arbeit entschieden.

Herzlichen Glückwunsch, Thomas Gruber, zum Weizenbaum-Studienpreis 2019.



Thomas Gruber

Mathematik, Informatik und Krieg

Zu den Verbindungen mathematischer und informatischer Forschung an zivilen deutschen Hochschulen mit der modernen Kriegsführung



1. Preis

Dass Kriege auf dem höchsten Stand der Technik geführt werden, ist nichts Neues. Militärische Anwendungen waren schon oft motivations- und geldgebend für richtungsweisende Forschungsprojekte und teure Entwicklungen. Heute sind immer treffsicherere Cruise Missiles, eigene militärische Kommandos, die für den Cyberkrieg aufgestellt werden, Spionagesatelliten, die eine nahezu lückenlose Erdüberwachung und Zielsuche ermöglichen sowie ein immer weiter entmenslichter Drohnenkrieg nur einige drastische Beispiele für hoch technisierte Aspekte des Krieges.

Bei einem näheren Blick hinter die Kulissen der Kriegsführung fällt auf, dass sich die militärischen Neuerungen erheblich auf die aktuelle Forschung in der Informatik und der Mathematik stützen. Noch drastischer formuliert: Die modernen Formen der Kriegsführung wären ohne aktuelle informatische und mathematische Forschungsergebnisse undenkbar. Dessen sind wir FIFlerInnen uns bewusst, schließlich ist nicht zuletzt die militärische Nutzung der Informationstechnik ein Grund, warum das FIF existiert. Und nicht nur das, wir arbeiten ja zu vielen Aspekten, wo die Informatik entgegen unserer verschiedenen Vorstellungen einer gerechten und befreiten Gesellschaft genutzt wird (z.B. Krieg, staatliche Überwachung, Repression, ...) und wo ihre Errungenschaften besser platziert wären.

Gerade von Unileitungen und wissenschaftlichem Personal wird der direkte militärische Bezug der mathematischen und informatischen Forschung allerdings oft geleugnet. Ergebnisse aus Drittmittelprojekten gehen an „ganz normale“ deutsche oder europäische Unternehmen, die wie so viele andere eben auch eine Rüstungssparte haben, oder fließen als Teilprojekte in externe Forschungseinrichtungen wie die Fraunhofer- oder Max-Planck-Institute ab. Wie dabei mit eindeutig militärischen Forschungsfragen in solchen Projekten und Kritik an ebenjenen umgegangen wird, hat mich einen großen Teil meines eigenen Studiums der

Mathematik und Informatik beschäftigt. In den Jahren 2015 bis 2018 habe ich schließlich zur Verknüpfung mathematischer und informatischer Forschung mit der modernen Kriegsführung promoviert und möchte im Folgenden einen kurzen und hoffentlich kurzweiligen Überblick über meine Herangehensweise und die Ergebnisse bieten.

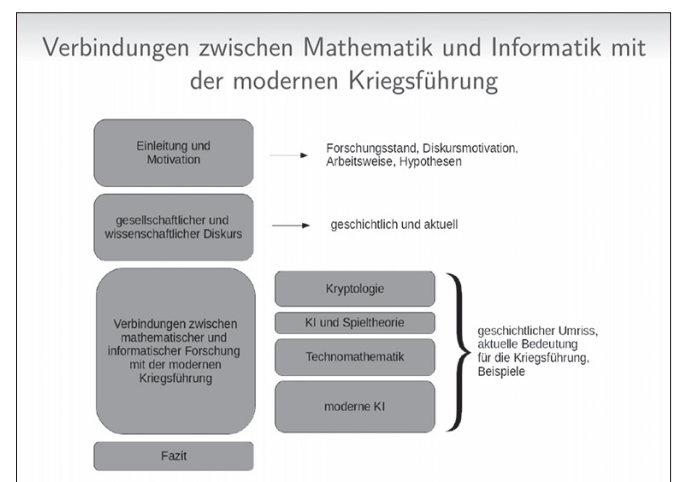


Abbildung: Struktur der Arbeit - Folie aus dem Vortrag von Thomas Gruber

Warum?

Im Laufe meiner Promotion sind mir bezüglich meines Forschungsvorhabens viele interessierte und kritische Fragen gestellt worden. Einige davon hatte ich mir selbst schon gestellt, manche hätte ich bei weitem nicht so präzise wie die FragestellerInnen formulieren können und wieder andere wären mir nicht in den Sinn gekommen. Für jede einzelne dieser Fragen bin ich dankbar, denn sie haben geholfen, Unklarheiten in meiner Argumentation zu beseitigen oder noch besser – ihnen vorzubeugen. Drei jener Fragen, die für mein wissenschaftliches und politisches Wirken zentrale Bedeutung hatten und haben, möchte ich im Folgenden kurz beantworten.

Warum der Fokus auf deutsche Forschung und Militarisierung?

Öfter wurde ich gefragt, warum ich bei meiner Forschung einen Fokus auf deutsche Entwicklungen lege. Gerade die US-amerikanische Militarisierung von Politik, Gesellschaft und Forschung sei doch viel drastischer und bedeutsamer.

Es stimmt, die US-amerikanische Regierung gibt im Vergleich zu Russland oder den europäischen Staaten Unsummen für Rüstung und Militär aus. Das ist allerdings kein Grund, das Wiedererstarken des deutschen Militarismus zu ignorieren. Seit nunmehr knapp 30 Jahren wird deutsches Militär wieder außerhalb der eigenen Landesgrenzen eingesetzt, im Jahr 1999 erstmals seit Ende des Nazi-Regimes wieder im offensiven Kriegseinsatz. Seit den 1990ern fallen die Hemmungen gegenüber Kriegseinsätzen schrittweise ab. Und heute, 75 Jahre nach Ende des Zweiten Weltkrieges, nach dem schrecklichen Beweis dafür, was deutscher Nationalismus hervorbringen kann, hat Deutschland sich wieder auf der militärischen Weltbühne platziert – politisch, im Kriegseinsatz und wirtschaftlich.¹ Gründe genug also, sich auch in der Kritik den deutschen Entwicklungen anzunehmen und ausschlaggebend dafür, dass ich in meiner Arbeit den Fokus auf deutsche Forschungseinrichtungen und die politischen Entwicklungen in der BRD gelegt habe.

Warum Mathematik und Informatik?

Mein ursprüngliches Interesse an den Verbindungen zwischen Mathematik, Informatik und Krieg kam eigentlich aus einem mathematischen Blickwinkel. Während meines Studiums befasste ich mich viel mit den gesellschaftlichen Auswirkungen mathematischer Forschung – den Folgen eines Fachbereichs also, dessen Ergebnisse häufig als reine Grundlagenforschung bezeichnet werden und die doch so drastische Auswirkungen auf unser Miteinander haben. Zwar konnte ich schnell feststellen, dass viele mathematische Forschungsprojekte durchaus gewissen Anwendungen dienen, etwa in Finanzwirtschaft und Industrie, doch war auch die Informatik in diesen Aufgabenstellungen omnipräsent. Die Verbindung von Mathematik und Informatik ergibt sich also bei einem gewissen Anwendungsbezug ganz natürlich: Bei jedem mathematischen Modell muss die Implementierung und die Berechnung mitbedacht werden. Bei der aktuellen Forschung in der angewandten Mathematik, die meist enorm rechenintensive Vorgänge beinhaltet, spielt auch aktuelle Forschung aus der

Informatik eine wichtige Rolle. Häufig sind bei größeren Forschungsprojekten Angehörige beider Fachgebiete beteiligt.

Warum gerade Krieg?

Dass die Hochschulen – wie viele andere Bereiche des Lebens auch – immer mehr der kapitalistischen Verwertungslogik untergeordnet werden, bringt einige drastische Veränderungen mit sich. So verlieren monetär weniger gewinnbringende Fachbereiche an Bedeutung, viele WissenschaftlerInnen machen überwiegend Auftragsforschung für Staat, Wirtschaft, Militär oder Industrie und auch die Studieninhalte ändern sich entsprechend. Die Forschung für den Krieg ist also ein Ausschnitt aus vielen kritikwürdigen Entwicklungen in der Forschungslandschaft. Allerdings schien mir die Arbeit zu Forschungsprojekten, die sich so nah an einem direkten Zerstörungs- und Tötungszweck bewegen, ein guter Ausgangspunkt für die kritische Betrachtung von Projekten an zivilen deutschen Hochschulen. Häufig ist die kriegsrelevante Forschung ohnehin so eng mit der Ökonomisierung der Hochschulen verbunden, dass ich im Rahmen meiner Arbeit beide Aspekte behandle.

Vorgehen

Da eine kritische Auseinandersetzung mit der mathematischen und informatischen Forschung nur selten auf institutionalisierter wissenschaftlicher Basis stattfindet, konnte ich für mein Thema nur auf einen relativ dünnen Forschungsstand zurückgreifen. Im Gegensatz dazu war mir der rege gesellschaftliche und politische Diskurs über Technikfolgen, wie er von vielen verschiedenen Menschen mit diversen Schwerpunkten geführt wird, eine enorme Hilfe bei meiner Promotion.

Das Ziel meiner Arbeit war es, eine Grundlage zu schaffen für die Auseinandersetzung mit den Verbindungen zwischen Mathematik, Informatik und Krieg – sowohl auf wissenschaftlicher als auch auf politischer Ebene. Um diesem Anliegen gerecht zu werden, habe ich, wann immer möglich, Abstand davon genommen, in Fachsprache zu schreiben. Nötige Exkursionen in tiefergehende mathematische und informatische Forschungsbereiche habe ich vom Haupttext möglichst abgekapselt, damit sie ohne zu große Erkenntniseinbußen übersprungen werden können. Der Kernpunkt der Dissertation ist das Nachzeichnen der Forschungslandschaft in Mathematik und Informatik hinsichtlich der folgenden zentralen Fragen: Welche Ergebnisse aus Mathematik und Informatik finden von deutschen zivilen Hochschulen den Weg in die aktuelle Kriegsführung? Welche Auswirkungen hat das für die zivile deutsche Forschungslandschaft in diesen Fächern?

Um einen guten Überblick über die Verquickung von Mathematik und Informatik an zivilen deutschen Hochschulen mit der modernen Kriegsführung zu geben, fokussiert sich der analytische Teil der Dissertation auf hierfür möglichst relevante Themenkomplexe: die Kryptologie, die sogenannte Technomathematik und die künstliche Intelligenz. Jeder Themenkomplex wird fachlich eingeordnet, es wird ein geschichtlicher Überblick mit Bezug zur militärischen Relevanz der jeweiligen Forschungsrichtungen gegeben und schließlich wird mit möglichst fachtypischen Beispielen der aktuelle Bezug zur modernen Kriegsführung umrissen.





Ergebnisse

Die Forschungsergebnisse der Dissertation sind so vielseitig wie die betrachteten Themenfelder selbst. Einmal wird die Forschung aus Mathematik und Informatik direkt vom Militär an den Hochschulen abgeschöpft, ein anderes Mal findet sie über studentische Praktika und Werksstudierendenstellen in Rüstungsunternehmen und wieder ein anderes Mal wird sie über externe Forschungsinstitute an Staaten oder Konzerne verkauft. Auch die Auswirkungen auf die zivile Forschungs- und Studienlandschaft sind dementsprechend unterschiedlich. Oft hat bei der Analyse der diversen Fachbereiche eine geschichtliche Einbettung geholfen, um die heutige Form der Militarisierung besser verstehen zu können. Im Folgenden sollen einige der Ergebnisse ohne Anspruch auf Vollständigkeit kurz umrissen werden.

Kryptologie

Die Kryptologie ist ein Fachgebiet, das die sichere Verschlüsselung von Nachrichten (Kryptographie) und Angriffe auf ebensolche Verschlüsselungsschemata (Kryptoanalyse) untersucht. Wichtige wissenschaftliche Ergebnisse in der Kryptologie kommen vornehmlich aus der reinen Mathematik – genauer der Algebra – und der Informatik. Dabei deckt die mathematische Forschung vor allem den theoretischen Hintergrund ab (z.B. endliche Körper, elliptische Kurven etc.) und die Informatik liefert die für die konkrete Umsetzung und Anwendung unabdingbaren Überlegungen (z.B. ausgefeilte Algorithmen, Forschung zur Rechenzeit, Angriffsmöglichkeiten in verwendeter Hardware und Software etc.). Bei Kryptosystemen sind Schwachstellen und Hintertüren sowohl im mathematischen als auch im informatischen Teil der Forschung möglich.

Geschichtlich ist die kryptologische Forschung von erheblicher Bedeutung für den Krieg. Erfolgreiche Angriffe auf Verschlüsselungsschemata haben nicht selten große Auswirkungen auf kriegerische Auseinandersetzungen (z.B. Vigenère-Chiffre im US-amerikanischen Bürgerkrieg, Zimmermann-Telegramm im Ersten Weltkrieg, Entschlüsselung der Enigma im Zweiten Weltkrieg etc.). Gleichzeitig waren auch immer die aktuellsten kryptologischen Forschungsergebnisse für die Kriegsparteien interessant, denn nur sie lieferten sichere Kryptosysteme und gleichzeitig die neuesten Schwachstellen etablierter Verschlüsselungsschemata.

An der militärischen Relevanz der aktuellen kryptologischen Forschung hat sich selbstverständlich bis heute nichts geändert. Auch hat die jahrhundertelange Nähe zwischen Kryptologie und Kriegsführung dazu geführt, dass die militärischen Aspekte des Forschungsgebiets als etwas vollkommen Normales gelten und so problemlos den Weg in die Forschungs- und Studieninhalte an deutschen Hochschulen gefunden haben. Das deutsche Verteidigungsministerium und das Militär kaufen kryptologische Ergebnisse an zivilen Hochschulen vor allem über Auftragsforschung ein. Dies geschieht entweder über direkte Drittmittelprojekte an den Hochschulen oder an eng mit ihnen verbundenen Forschungseinrichtungen wie etwa den Fraunhofer-Instituten. Auf dieses Vorgehen greift das Militär vermutlich vor allem dann zurück, wenn die eigenen ForscherInnen (z. B. an Bundeswehr-universitäten) nicht nah genug an den aktuellsten theoretischen Entwicklungen in der Kryptologie arbeiten. Eine weitere zivil-mi-

litärische Kooperation findet auf renommierten wissenschaftlichen Konferenzen zur Kryptologie statt. Hier ist es – auch geschichtlich – sehr verbreitet, dass Angehörige von Streitkräften und Geheimdiensten verschiedener Länder mit WissenschaftlerInnen ziviler Hochschulen das Programm ausarbeiten, die Planung durchführen und Vorträge halten. So findet ein für die Militärs sehr fruchtbarer und in der zivilen Forschungslandschaft nur selten problematisierter Abfluss neuester ziviler kryptologischer Forschungsergebnisse in die militärische Anwendung statt.

Technomathematik

Die Technomathematik, oft auch Ingenieurmathematik, umfasst mathematische Forschung, die gezielt für technische und ingenieurwissenschaftliche Anwendungen durchgeführt wird. Sie bewegt sich vornehmlich in den folgenden Bereichen angewandter Mathematik: der Optimierung, der Numerik und der Kontrolltheorie. Oft bedienen sich technomathematische Projekte mehrerer dieser klassischen Forschungsbereiche, so etwa in der Forschung zur numerischen Optimierung oder der optimalen Steuerung. Es gibt daher Sinn, die einzelnen Fachbereiche – Numerik, Optimierung und Kontrolltheorie – unter diesem Begriff zusammengefasst zu betrachten. Da die technomathematische Forschung fast immer rechenaufwändige Verfahren hervorbringt, ist sie meist auch mit einem informatischen Aspekt versehen. In größeren ingenieurmathematischen Drittmittelprojekten arbeiten häufig ForscherInnen aus Mathematik und Informatik zusammen.

Wie sich vermuten lässt, hat die Technomathematik eine lange militärische Geschichte. Besonders große Bedeutung hatten ingenieurmathematische Methoden schon immer in der Luft- und Raumfahrt sowie in der Entwicklung von Raketenwaffen. So wurde die Numerik beispielsweise zur Flugbahnberechnung, die Optimierung für die Bestimmung der besten Konstellationen von Satelliten und die Kontrolltheorie für die Stabilisierung von Flugkörpern genutzt. Ihre Ursprünge haben gerade die numerische Mathematik und die Optimierung allerdings nicht in technischen Fragestellungen, sie sind der zivilen mathematischen Forschung entsprungen.

Bis heute hat sich an der Relevanz der Ingenieurmathematik für die Kriegsführung nicht viel geändert. Das ist auch kaum verwunderlich, denn die oben genannten Problemstellungen aus der Luft- und Raumfahrt sind nach wie vor aktuell. Die zivil-militärische Kooperation findet an den deutschen Hochschulen in direkten Drittmittelprojekten, über Werkstudierendenstellen und Praktika sowie in Kollaborationsprojekten ziviler und militärischer ForscherInnen statt. Heute sind militärische Fragestellungen in technomathematischen Fachbereichen sehr verbreitet – von den Anwendungsbeispielen im Studium über die Vermittlung von Pflichtpraktika an Rüstungskonzerne bis hin zur militärischen Drittmittelforschung an Hochschulen mit Zivilklausel.

Künstliche Intelligenz

Die aktuelle Forschung zur künstlichen Intelligenz ist nur schwer in mathematische und informatische Teile zu trennen. Zwar lassen sich viele der mathematischen Methoden benennen, die in KI-Systemen vorkommen (z.B. aus der Logik, der Stochastik

oder der Numerik), doch geht es bei jeder KI-Forschung immer auch um eine Umsetzung und Implementierung. Was früher noch unter dem Begriff „künstliche Intelligenz“ zusammengefasst war, wird inzwischen viel ausdifferenzierter beforscht. Heute wird zu wissensbasierten Systemen, stochastischen Systemen oder dem maschinellen Lernen gearbeitet. Während die stochastischen Systeme noch recht nah an der mathematischen Theorie der dynamischen Systeme sind, lassen sich bei wissensbasierten Systemen oder dem maschinellen Lernen nicht mehr zwischen reiner Mathematik oder reiner Informatik unterscheiden. Die Forschungsprojekte werden daher häufig von WissenschaftlerInnen beider Disziplinen bearbeitet, wenn sich auch die stochastischen Systeme weiter in die Mathematik und das maschinelle Lernen eher in Richtung Informatik neigen.

Die Geschichte der künstlichen Intelligenz ist turbulent. Und es ist nicht zuletzt der Einfluss externer Gelder, der das Fachgebiet fast vollständig zerstört hätte. Ab den 1950er Jahren schürte die schnell wachsende KI-Forschung die Erwartungen, dass im Verlauf weniger Jahre Maschinen möglich wären, die wie ein Mensch denken und schlussfolgern könnten. Externe Gelder – nicht zuletzt vom Militär – flossen in Strömen in die Hochschulforschung, bis einige Lehrstühle und Institute vollkommen abhängig waren. Mitte der 1970er Jahre wurden die hohen Erwartungen schließlich als nicht erfüllt akzeptiert, die Gelder gestrichen und die daraus folgende Krise des Forschungsbereichs als „KI-Winter“ bekannt.² Doch davon nicht genug, in den 1980er Jahren passierte noch einmal das Gleiche in kleinerer Dimension, ein zweiter KI-Winter also. Heute sind die ForscherInnen dazu übergegangen, die Methoden der KI weiter auszudifferenzieren, wie oben bereits benannt. Das macht es möglich, zu kleinteiligeren Problemen zu forschen, ohne gleich eine umfassend denkende Maschine versprechen zu müssen. Diese Spezialisierung hat die KI-Forschung nun auch wieder für Auftragsforschung interessant gemacht. Staat, Polizeibehörden und Militär setzen dabei vor allem auf Methoden zur Muster- und Bilderkennung.

In Deutschland hat sich das militärische Interesse an der aktuellen KI-Forschung in einer regelrechten politischen Agenda bemerkbar gemacht. So wurden auf Betreiben des Verteidigungsministeriums im Jahr 2009 zwei militärische Forschungseinrichtungen in Fraunhofer-Institute eingegliedert bzw. fusioniert, um unter anderem in den Bereichen Bild- und Mustererkennung bessere Synergieeffekte zwischen militärischer und ziviler Forschung zu erreichen. Die Bundesregierung initiierte 2007 außerdem ein Forschungsprogramm zur „zivilen Sicherheit“, das von den Bundesministerien für Bildung und Forschung, des Inneren und der Verteidigung zusammen entwickelt wurde und ebenso auf

starken Austausch zwischen ziviler und militärischer Forschung abzielt. Ein erheblicher Teil der aktuellen Auftragsforschung zur künstlichen Intelligenz ist so in eine „Dual-Use-Agenda“ eingebettet, deren Fokus auf „Sicherheitsforschung“ liegt, sich also mit der Ausübung staatlicher Gewalt und Überwachung befasst.

Fazit

Bei der Zusammenfassung einer Dissertation in einem Artikel bleiben selbstverständlich einige Aspekte auf der Strecke. Gerade Begriffsklärungen, tiefergehende geschichtliche Ausführungen, Gedanken zur Wissenschafts- und Gesellschaftspolitik sowie die konkreten Beispiele aus der Forschung habe ich gekürzt oder ganz ausgelassen. Den interessierten LeserInnen sei daher für eine ausführlichere Auseinandersetzung der Volltext empfohlen, welcher auch kostenlos online verfügbar ist.³

Als Fazit der Arbeit lässt sich festhalten, dass die zivile Forschung der Mathematik und der Informatik an vielen Stellen eng mit der aktuellen Kriegsführung verbunden ist. Dies hat zum einen zur Folge, dass an entsprechenden Forschungsprojekten beteiligte MathematikerInnen und InformatikerInnen mittelbar und unmittelbar den grausamen Kriegen und der tödlichen Geopolitik verschiedener Staaten zuarbeiten. Zum anderen zieht das militärische Interesse auch eine erhebliche Umstrukturierung der zivilen Forschungs- und Studienlandschaft nach sich. Die Geschichte der künstlichen Intelligenz zeigt eindrucksvoll, welche Gefahren hierbei auch für die Wissenschaft lauern.

Dass die Militarisierung der Forschungslandschaft noch nicht so weit fortgeschritten ist wie sich das Verteidigungsministerium, Militär und Rüstungskonzerne wünschen würden, liegt vor allem am Widerstand der einzelnen antimilitaristischen und friedenspolitischen Gruppen. Sei es an den Hochschulen selbst oder außerhalb, lokal oder überregional – Protest, Aktionen und eine gute Informationspolitik können die Hochschulen für die militärischen GeldgeberInnen unangenehm und schließlich uninteressant machen.

Anmerkungen

- 1 Sehr ausführlich und umfassend wird das Wiedererstarken der deutschen Militärmacht beispielsweise seit 1996 von der Informationsstelle Militarisierung analysiert, deren Texte auf imi-online.de frei zugänglich sind.
- 2 Abgeleitet vom englischen Begriff „AI winter“.
- 3 <http://nbn-resolving.de/urn:nbn:de:gbv:46-00107128-15>



Thomas Gruber

Thomas Gruber ist Mathematiker und promovierte an der Universität Bremen. Er war Stipendiat der Rosa-Luxemburg-Stiftung und ist Mitglied der Informationsstelle Militarisierung (IMI) in Tübingen.

Alexandra Keiner: Legitimität von Algorithmen in politischen Verwaltungsorganisationen

Bachelorarbeit an der Humboldt-Universität zu Berlin

studienpreis



Migration und Flucht gehören zu den großen politischen Themen der letzten Jahre. Der zeitweise starke Anstieg der Migration, die zu geringe Kapazität und die damit verbundene Überlastung der verantwortlichen Behörden – hier insbesondere des Bundesamts für Migration und Flüchtlinge (BAMF) – lässt es attraktiv erscheinen, automatisierte Lösungen für die Bearbeitung der Fälle zu implementieren. Gleichzeitig erhofft man sich davon eine Erhöhung der Qualität von Entscheidungen und – davon teilweise entkoppelt, wie wir sehen werden – eine Erhöhung ihrer Legitimität.

Gleichzeitig schreitet die Entwicklung algorithmischer Entscheidungssysteme auf Basis maschineller Lernverfahren – in der Öffentlichkeit kurz als „Algorithmen“ bezeichnet – weiter voran. Damit scheint es nahliegend, solche Systeme auch für die Entscheidung über die Gewährung von Asyl einzusetzen. Dass sich daraus Legitimitätsprobleme ergeben, ist offensichtlich.

Wie bei solchen Entscheidungen in politischen Verwaltungsorganisationen Legitimität durch algorithmische Entscheidungssysteme hergestellt wird, untersucht die Bachelorarbeit von Alexandra Keiner, Legitimität von Algorithmen in politischen Verwaltungsorganisationen, die am Institut für Sozialwissenschaften der Humboldt-Universität zu Berlin erstellt wurde, anhand einer Software, die den Dialekt von AsylbewerberInnen erkennen und dadurch die Feststellung ihrer Herkunft unterstützen soll. Wir verleihen für diese Arbeit heute einen zweiten Preis des Weizenbaum-Studienpreises.

Die Arbeit fragt, wie die Anwendung von Softwaresystemen zur Entscheidungsfindung in politischen Verwaltungen durch Politik und Verwaltungsinstitutionen legitimiert wird. Aus einem theoretischen Rahmen wird ein analytisches Modell für eine empirische Untersuchung abgeleitet. Dies exerziert sie konkret an dem Einsatz einer Dialekterkennungssoftware, die Entscheidungen über die Aufenthaltsberechtigung von Geflüchteten durch das Bundesamt für Migration und Flüchtlinge (BAMF) unterstützen soll.

Die Dialekterkennungssoftware soll bei der Feststellung der Herkunft von AsylbewerberInnen unterstützen – Schätzungen des BAMF zufolge können ca. 60 % der BewerberInnen aus unterschiedlichen Gründen keine gültigen Identitätsdokumente vorweisen. Somit wird ihre Herkunft auf anderem Weg festgestellt. Bestehen Zweifel, werden dafür Sprach- und Textanalysen genutzt. Diese sollen im Rahmen der „Digitalisierungsstrategie 2020“ durch Informationstechnologie vereinfacht und beschleunigt werden. Dafür wird – bisher bei arabisch sprechenden AntragstellerInnen – eine sprachbiometrische Software eingesetzt, wenn anders keine eindeutige Identifikation möglich ist.

Dabei wird nicht nur nach den Legitimitätskriterien gefragt, sondern auch die Mechanismen zur Erlangung von Legitimität un-

tersucht. Über die inhaltsanalytische Untersuchung diverser Dokumente zum Phänomen kommt Frau Keiner zu dem Schluss, dass algorithmische Entscheidungsmechanismen zwar zur Bearbeitung von Legitimationsdefiziten eingesetzt werden können, aber eigene Legitimitätsprobleme für politische Verwaltungen erzeugen.



Laudator Richard Schöbel

Für den Einsatz von Software in Verwaltungsorganisationen spricht die Annahme, dass die Handlungen von VerwaltungsbeamtInnen aufgrund von Arbeitsteilung und hierarchischer Befolgung abstrakter Regeln berechenbar seien. Dennoch haben solche Systeme Legitimitätsdefizite. Im untersuchten Fall reagiert der Verwaltungsapparat dabei auf die öffentliche Kritik an der Legitimität der eingesetzten sprachbiometrischen Software mit einem selektiven Zugriff auf mögliche Legitimationsmuster und mit einer „Entkopplung von Aktivitäts- und Formalstruktur“ – etwa dem Beharren auf der Legitimität bürokratischer Verfahren, während eigentlich von technologischen Prozessen die Rede sein müsste. Die Bewertung erfolgt nun durch die Beantwortung der Forschungsfragen:

- Welche Legitimitätskriterien werden vom BAMF und der Bundesregierung in Bezug auf den Einsatz der Sprachbiometrie-Software genannt? Welche Schwerpunkte lassen sich beobachten?
- Mit Hilfe welcher Mechanismen wird versucht, den Einsatz der Software zu legitimieren?

Als Antwort auf die erste Frage nennt die Arbeit die Legitimitätskriterien der bürokratischen Herrschaft nach Max Weber. Besonders werden die Befolgung der Gesetze, die hierarchische Organisation und die Weisungsgebundenheit der beteiligten MitarbeiterInnen, die strukturierte Arbeitsteilung und das Amtsgeheimnis als Schutz vor Manipulation betont. Die Software selbst wird durch Verfahrenseffizienz und Formalisierung der Prozesse legitimiert – ebenfalls Kriterien der bürokratischen Herrschaft.



Zur Legitimierung der Software kommt die Arbeit zu dem Ergebnis, dass die fehlende Dokumentation und widersprüchliche Angaben zur Funktionsweise auf eine Entkopplung von Aktivitäts- und Formalstruktur hindeuten. Dass zwar auf eine Machbarkeitsstudie hingewiesen, aber deren Ergebnisse nicht konkret benannt werden, deutet auf eine „Logik des guten Glaubens“ hin.

Umgekehrt lässt sich der Einsatz der Software aber auch als Lösung zuvor bestehender Legitimitätsdefizite verstehen, die durch die hohe Arbeitsbelastung und teilweise gravierende Fehlentscheidungen entstanden ist – genannt wird der deutsche Bundeswehrsoldat Franco A., dem es gelang, sich als syrischer Flüchtling auszugeben.

Die Arbeit zieht das Fazit, dass mit dem Einsatz der Software zwar den Legitimitätsdefiziten begegnet werden kann – allerdings zu Lasten der AsylbewerberInnen. Angesichts der intransparenten Funktionsweise und der geringen Zuverlässigkeit wird die Notlage der Geflüchteten nicht angemessen berücksichtigt, die gegen Fehlentscheidungen häufig nicht angemessen vorgehen können. Das durch die Software angesammelte Wissen, auf das die Betroffenen keinen Zugriff haben, führt zusätzlich zu einer Verstärkung der „Herrschaft kraft Wissens“. Ein Verfahren zur Identifizierung von Einzelpersonen für die Einteilung gesellschaftlicher Gruppen aufgrund einer biologischen Grundlage einzusetzen, sieht sie sehr kritisch.

Was für die Formalstruktur nicht untersucht wird, ist die Frage, ob die Software tatsächlich Dialekte korrekt unterscheiden kann. Bei der Software handelt es sich um maschinen-lernende Systeme, neuronale Netze, die Modelle bilden, dabei bleibt unklar ob sie weiter lernend oder abgeschlossen sind. Die Darstellung dazu ist widersprüchlich. Es ist zwar ein Assistenzsystem, das die Entscheidung nicht selbst trifft. Ist es ein stimmbiometrisches

Verfahren im „klassischen“ Sinne? Es bleibt fraglich, ob Sprachbiometrie-Software zur Erkennung von (arabischen) Dialekten tatsächlich ein biometrisches Verfahren ist. Die Intransparenz der Software ist auch für die Legitimierung das größte Problem.

Der Weizenbaum-Studienpreis wird in erster Linie für Informatik-Arbeiten vergeben, will aber auch die interdisziplinäre Bearbeitung Informatik-naher Themen belohnen. Damit ist diese Arbeit für uns trotz eigentlich soziologisch-politischer Ausrichtung preiswürdig. Die Frage der Legitimität automatisierter Entscheidungen ist eine der wesentlichen Fragen, die sich aus Digitalisierungsprozessen ergeben – und damit eines der Kernthemen des FfF. Die Arbeit ist stringent aufgebaut, indem sie zunächst in kreativer Weise einen theoretischen Rahmen für die Analyse der Kriterien erarbeitet und dann die daraus gewonnenen Kriterien auf das gewählte, hochaktuelle Fallbeispiel anwendet. Die Arbeit entnimmt viel aus der Literatur, für letztes Verständnis würde es verstärkte interdisziplinäre Arbeit erfordern. Die Legitimitätsdefizite und die Ansätze zu ihrer Behebung werden überzeugend dargestellt. Interessant wäre es noch gewesen, auch die Legitimierung durch Software – in der Arbeit kurz angerissen – anhand des theoretischen Rahmens detaillierter zu behandeln. Abschließend geht die Autorin auch auf die Folgen des Einsatzes algorithmischer Entscheidungssysteme im gewählten Problembereich ein.

Die Arbeit verknüpft zwei hochaktuelle Themen, indem sie die in der Öffentlichkeit stark diskutierte Frage der Asylentscheidung mit dem in der Informatik aktuellen Thema Künstliche Intelligenz und algorithmische Entscheidungsverfahren zusammenführt. Die Jury hat sich einhellig für einen zweiten Preis für diese Arbeit entschieden.

Herzlichen Glückwunsch, Alexandra Keiner, zum Weizenbaum-Studienpreis 2019.



Alexandra E. Keiner

Algorithmen im Asylprozess

Legitimität von Algorithmen in politischen Verwaltungsorganisationen am Beispiel der Dialekterkennungssoftware des BAMF



2. Preis

Über Algorithmen wird derzeit viel diskutiert. Im Fokus steht dabei insbesondere ihr Einsatz in verschiedenen Wirtschaftszweigen, etwa bei der Analyse des Verhaltens von KundInnen, KonsumentInnen und BewerberInnen, um daraus Liquiditätsprognosen bei der Vergabe von Krediten zu ermitteln oder individuelle Versicherungsbeiträge zu berechnen. Seit kurzem werden solche Systeme jedoch auch in staatlichen Organisationen herangezogen. So setzt etwa die Steuerfahndungsstelle Kassel seit 2018 Algorithmen für ihre Ermittlungen ein. Und auch die österreichische Arbeitsagentur („Arbeitsmarktservice“) prüft derzeit den Einsatz eines Algorithmus, um die Marktchancen von Arbeitssuchenden zu ermitteln und auf dieser Grundlage über die Finanzierung von Maßnahmen zu entscheiden.

Eine der ersten Behörden im deutschsprachigen Raum, die diese neue Technologie nutzt, ist das deutsche Bundesamt für Mig-

ration und Flüchtlinge (BAMF). Seit 2016 wird dort eine Software zur algorithmischen Spracherkennung eingesetzt, um die Entscheidung über die Aufenthaltsberechtigung von Geflüchteten zu unterstützen. Mittels *sprachbiometrischer* Verfahren wird versucht, anhand von Sprachaufnahmen den Dialekt und damit das Herkunftsland der Asylsuchenden zu ermitteln. Da es bislang noch keine vergleichbaren Systeme gibt und zudem Studien fehlen, die die Funktionsfähigkeit dieser Software belegen, ist deren Einsatz für eine solche wichtige Entscheidung über das Asylrecht stark legitimierungsbedürftig. Aus diesem Grund ist es wichtig zu prüfen, wie das BAMF diesen Einsatz zu legitimieren versucht.

Laut Schätzungen des BAMF aus 2018 können 60 Prozent der Personen, die in Deutschland Asyl beantragen, keine (gültigen) Identitätsdokumente vorweisen (Frank 2018). Die Ein-



reise nach Deutschland ist ohne Ausweisdokumente zwar illegal, doch haben Geflüchtete nach § 13 AsylG auch ohne diese Dokumente ein Recht auf einen Asylantrag. Denn die Gründe, weshalb Menschen bei ihrer Einreise keine Ausweispapiere bei sich tragen, sind vielfältig: So können ihre Dokumente zum Beispiel auf ihrem Weg nach Deutschland von sogenannten *Schleusern* oder auch von Behörden anderer Staaten einbehalten worden sein. Oder aber die eigenen Papiere mussten gefälscht werden, um das eigene Land überhaupt erst verlassen zu können.

Da seit der Einschränkung des Asylgesetzes 1993 Personen aus *sicheren Herkunftsstaaten* eine geringere Aussicht auf Asyl haben, wird jedoch häufig davon ausgegangen, dass Personen, die aus diesen Ländern nach Deutschland einreisen, ihre Dokumente absichtlich vernichten, um ihre Anerkennungschancen zu erhöhen (Tangermann 2017:18). Bislang wurden deshalb Sprachanalysen von SprachgutachterInnen durchgeführt, um die angegebene Herkunft zu validieren. Seit 2016 setzt das BAMF nun eine „Sprachbiometrische Dialekterkennungssoftware“ ein, mit der versucht wird, dieses Verfahren durch eine Analyse von zweiminütigen Sprachaufnahmen der Asylsuchenden zu ersetzen.

Die Software wurde in Zusammenarbeit mit der US-amerikanischen Firma Atos entwickelt. Die Kosten für Anschaffung, Anpassung, Ausbau und Kauf von Lizenzen betrugen bis Juli 2018 rund zwei Millionen Euro (Bundesregierung 2018b:14). In den ersten zwei Jahren nach Start der Software wurde sie bundesweit dann auch schon 18.500 Mal eingesetzt, mit dem Schwerpunkt auf arabisch sprechende AntragstellerInnen. Die Ergebnisse der Spracherkennungssoftware werden von den BeamtInnen, die über die jeweiligen Asylanträge entscheiden, in der Anhörung der AntragstellerInnen auf Plausibilität hin geprüft. Wenn die Ergebnisse der Sprachanalyse dabei nicht mit den angegebenen Daten der Geflüchteten übereinstimmen, wird angenommen, dass die Person versucht hat die Behörden zu täuschen, und der Asylantrag wird gemäß AsylG § 30 Absatz 3 als „offensichtlich unbegründet“ abgelehnt, sodass die betroffenen AntragstellerInnen „in der Regel Deutschland wieder verlassen“ (BAMF 2017b:2) müssen.

Dass die Software technisch wirklich zuverlässig funktioniert, ist dabei allerdings sehr fraglich. Der Computer- und Sprachwissenschaftler Dirk Hovy behauptet etwa, es sei nicht möglich, einen Trainingsdatensatz zu erstellen, der die Komplexität und Veränderbarkeit von (arabischen) Dialekten abzubilden vermag (Hummel 2017). Zwar zeigen mehrere Studien, dass die Identifikation von Sprachen mit Hilfe algorithmischer Systeme mit geringer Fehlerwahrscheinlichkeit durchaus möglich ist (Cölltekim, Rama 2016; Ali A et al. 2016), allerdings nur wenn sehr große Trainingsdatensätze mit mehr als 50.000 Sprach- oder Textproben verfügbar sind. Eine zuverlässige Unterscheidung innerhalb von Sprachgruppen, wie es bei der Erkennung von arabischen Dialekten der Fall ist, sei allerdings auch diesen Studien zufolge nicht zuverlässig möglich.

Rechtlich könnte der Einsatz der Sprachbiometrie-Software des BAMF darüber hinaus sogar gegen Bundes- und EU-Gesetze verstoßen, die eine Entscheidung auf der Grundlage von (intransparenten) Algorithmen explizit untersagen. So spricht etwa

die Europäische Kommission (2018) von einem „Recht, nicht einer ausschließlich automatisierten Verarbeitung beruhenden Entscheidung [...] unterworfen zu sein“. Ebenso dürfen auch nach § 114 Absatz 4 Bundesbeamtengesetz „beamtenrechtliche Entscheidungen“ nicht ausschließlich auf Grundlage einer automatisierten Datenverarbeitung getroffen werden.

Insbesondere der ethische Aspekt spielt für die Kritik an der Sprachbiometrie-Software eine große Rolle, da die Tragweite der Entscheidung sehr groß ist, die durch die algorithmische Bestimmung der Herkunftsregion getroffen wird. Wenn der Ergebnisbericht der Software mit einer relativ hohen Wahrscheinlichkeit angibt, dass AntragstellerIn einen Dialekt aus einer „sicheren“ Region spricht, wird ihr Antrag auf Asyl abgelehnt. Vor dem Hintergrund, dass es bisher keine vergleichbaren Systeme gibt, noch keine Studien dazu vorliegen, die die Funktionsfähigkeit solcher Dialekterkennungssoftware nachweisen können, und zudem die Fehlerquote der Software der Bundesregierung (2018b) zufolge bei 15 bis 20 % liegt, dann ist der Einsatz dieser Software für solch wichtige Entscheidungen über das Recht auf Asyl zumindest aus ethischer Perspektive höchst fraglich.

Delegitimierende Informationen werden verschleiert

Die erste Legitimierungsstrategie funktioniert über das Auslassen oder Verschleiern von Informationen, die den Einsatz der Software delegitimieren könnten. Auf eine kleine Anfrage der Bundestagsfraktion *Die Linke* nach einer Aufschlüsselung der hinterlegten Sprachproben nach jeweiligem Dialekt antwortete die Bundesregierung etwa, dass diese Daten „aus Geheimhaltungsgründen“ der Öffentlichkeit nicht zugänglich gemacht werden könnten. Der Grund dafür sei, dass „die Informationen geeignet sind, bewusste Täuschungshandlungen im Asylverfahren vorzubereiten und die Spracherkennung missbräuchlich zu manipulieren. Die Antwort auf die Frage ist daher als Verschluss-sache mit dem Geheimhaltungsgrad VS – *Nur für den Dienstgebrauch* eingestuft und wird dem Deutschen Bundestag gesondert übermittelt“ (Bundesregierung 2018b:15).

Auch auf die Frage nach der Funktionsweise des zugrunde liegenden Algorithmus gibt die Bundesregierung (2017) an, dass „die entsprechenden Informationen zur Funktionsweise [...] der internen Verwendung“ (S. 3) vorbehalten seien. Der konkrete Grund für die Geheimhaltung der Funktionsweise wird nicht genannt. Eine Bürgeranfrage zu den Ergebnissen der Testphase im Vorfeld des Softwareeinsatzes beantwortete das BAMF (2017c) damit, dass die Ergebnisse nicht öffentlich zugänglich gemacht werden könnten, weil dies gegen § 5 Absatz 1 Satz 1 Informationsfreiheitsgesetz verstoßen würde. Dort heißt es: „Zugang zu personenbezogenen Daten darf nur gewährt werden, soweit das Informationsinteresse des Antragstellers das schutzwürdige Interesse des Dritten am Ausschluss des Informationszugangs überwiegt oder der Dritte eingewilligt hat.“ Auf eine erneute Anfrage nach Ergebnissen, aus denen keine personenbezogenen Daten hervorgehen, ging das BAMF nicht mehr ein.

Im Zuge der Geheimhaltung von Informationen über die Funktionsweise des Algorithmus kommt es darüber hinaus auch zu widersprüchlichen Angaben von Seiten der Behörden: So be-

hauptete die Bundesregierung (2017), dass es sich bei der Sprachbiometrie-Software nicht um „maschinelles Lernen“ handle, während der Vizepräsident der BAMF die Software als „selbstlernendes System“ beschreibt. Für den Fall, dass es sich tatsächlich um ein selbstlernendes System handeln sollte, bleibt jedoch unklar, wie nach dem Einsatz der Software die Herkunft von Asylsuchenden unabhängig vom ermittelten Ergebnis sichergestellt werden kann. Eine solche externe Validierung wäre aber notwendig, wenn das Datenmaterial zuverlässig sein soll, um als Grundlage für die Verbesserung der Sprachmodelle zu dienen. Würde das System hingegen auf Grundlage der von ihm selbst ermittelten Ergebnisse weiter lernen, würde dies zu keiner Qualitätsverbesserung führen, sondern eher mögliche Fehler verstärken.

Weiterhin ist mit Blick auf die Legitimität der Software interessant, dass bestimmte Informationen zum Einsatz der Software durch das BAMF gar nicht erst erhoben bzw. dokumentiert werden. Die Bundesregierung hat mehrfach darauf verwiesen, dass sie über bestimmte Informationen nicht verfügen würde, weil diese nicht erhoben worden seien. Auf Anfrage der Bundestagsfraktion *Die Linke* danach, in wie vielen Fällen die Ergebnisse der Software von den Angaben der Antragssteller abwichen, antwortet die Bundesregierung etwa wie folgt: „In MARIS [dem Dokumentenmanagementsystem des BAMF] sind insgesamt 6.285 Dokumente als Sprachreports erfasst. Davon wurden in 2.333 Fällen die Informationen in MARIS händisch eingetragen, die besagen, ob der Sprachreport die Angaben des Antragstellers stützt oder nicht. Die Differenz ist insbesondere dem zeitlichen Abstand zwischen Generierung des Sprachreports im Rahmen der Asylantragsannahme und der späteren Eintragung der Information nach der Anhörung geschuldet“ (Bundesregierung 2018b:12). Demnach wurden also nur rund 6.000 Sprachreports von den vermeintlich 18.000 Sprachproben dokumentiert; und nur für 2.333 dieser 6.000 Fällen ist bekannt, ob der jeweilige Sprachreport die Angaben des Antragstellers gestützt hat oder davon abwich.

Darüber hinaus gibt die Bundesregierung (2018a:3) an, auch über keine Informationen zu verfügen, in wie vielen Fällen ein negatives Ergebnis der Dialektanalyse zu einem negativen Asylbescheid geführt habe. Und schließlich werde auch nicht erfasst, bei wie vielen anhängigen Gerichtsverfahren gegen die Entscheidungen des BAMF über Asylanträge der Einsatz der Sprachbiometrie-Software eine Rolle gespielt hat (Bundesregierung 2018a). Die fehlende Dokumentation solcher Informationen ermöglicht es, dass die Probleme und Inkonsistenzen, die sich beim Einsatz der Software ergeben, nicht gerechtfertigt werden müssen. Hier arbeitet das BAMF nach dem Motto: „Was nicht in den Akten ist, ist nicht in der Welt“ (Dahlvik 2017:134).

Der Rechtswissenschaftler Frank Pasquale (2015) übt grundsätzliche Kritik an der Geheimhaltung von Informationen über die Funktionsweise und den Umgang mit Algorithmen, die sich auf Amts- bzw. Betriebsgeheimnisse stützt (*legal secrecy*) oder durch systematische Verschleierung (*technologies of obfuscation*) ausgeübt wird (S. 9-10). Dadurch wären eine mögliche Diskriminierung, Ineffektivität oder Ineffizienz nicht mehr nachvollziehbar und damit illegitim. Doch gerade die Geheimhaltung und Intransparenz der Informationen könnte sich als Legitimi-

tätsmechanismus eignen, weil dadurch die Offenlegung von Inkonsistenzen vermieden wird. Mögliche Defizite des Algorithmus oder fehlerhaftes Umgehen mit der Software sind nicht mehr nachzuvollziehen.

Kennzahlen suggerieren Genauigkeit

Die zweite Strategie zur Legitimierung des Software-Einsatzes durch das BAMF liegt im Einsatz von mathematischen Kennzahlen, die eine hohe Genauigkeit des Verfahrens suggerieren. In den Schulungsunterlagen für die MitarbeiterInnen des BAMF im Umgang mit den neuen IT-Tools wird der Ergebnisbericht der Software musterhaft vorgestellt (siehe Abbildung). Die genauen Angaben zu den Sprach- und Dialektwahrscheinlichkeiten sowie den Aufnahme-Details erzeugen dabei den Eindruck von Berechenbarkeit, Standardisierung und mathematischer Genauigkeit. Auffällig ist in diesem Zusammenhang aber, dass weder aus diesem Bericht noch aus anderen Schulungsunterlagen Hinweise für die Interpretation und den Umgang mit den jeweiligen Ergebnissen zu finden sind, obwohl die Bundesregierung (2018a) angibt, dass die MitarbeiterInnen darin geschult werden, die Ergebnisse der Sprachsoftware richtig zu interpretieren (S. 5). Die einzige Interpretationshilfe, die in diesem Zusammenhang genannt wird, besagt allerdings nur, dass eine Sprechprobe dann erfolgreich abgegeben wurde, „wenn die Wahrscheinlichkeit eines bestimmten arabischen Dialekts gegenüber anderen wahrscheinlichen arabischen Dialekten im Ergebnisbericht überwiegt“ (Bundesregierung 2017:10). Dabei bleibt jedoch offen, ab welchem Prozentsatz ein Ergebnis zuverlässig ist. Wenn die Äußerung der Bundesregierung stimmt, wäre der Test auch dann erfolgreich, wenn die Wahrscheinlichkeit eines Dialekts 50,5 Prozent beträgt, was im Umkehrschluss allerdings bedeutet, dass die Fehlerwahrscheinlichkeit des Tests bei 49,5 Prozent liegt.

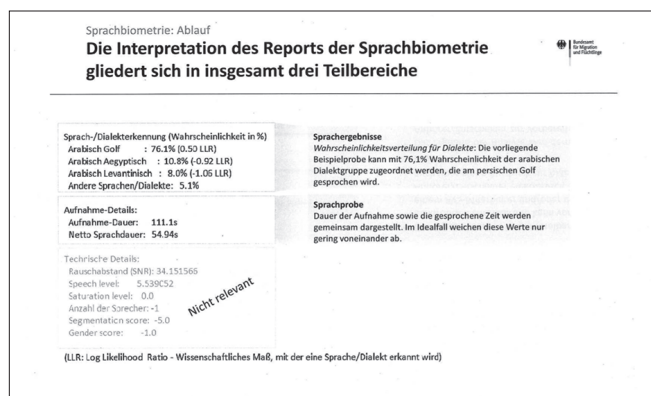


Abbildung: Ergebnisbericht der Sprachbiometrie-Software, Quelle: BAMF (2017a)

Weiterhin wird im Ergebnisbericht bei jeder Dialektwahrscheinlichkeit ein zusätzlicher Wert mit dem Kürzel LLR angezeigt – als „wissenschaftliches Maß, mit der eine Sprache/Dialekt erkannt wird“. Auch hier fehlen jegliche Angaben über die Bedeutung und Interpretation dieses Wertes. An diesem Beispiel werden nicht (nur) die technischen Defizite der Software deutlich, sondern vor allem auch, dass die MitarbeiterInnen, die die Ergebnisse in ihren Entscheidungen einbeziehen, über keine von außen nachvollziehbaren Informationen zur einheitlichen Interpretation der Ergebnisse verfügen.



Die genauen Angaben über die Wahrscheinlichkeit und Testgüte werden auf diese Weise zu „rationalisierten Mythen“ (Mayer, Rowan 2009:37), da sie eine rationale und zuverlässige Vorgehensweise des Tests suggerieren, ohne dabei wirklich nachvollziehbar (oder gar korrekt) zu sein. Die fehlende Einheitlichkeit der Interpretation fördert dementsprechend einen informellen Umgang mit den Ergebnissen. So ist den MitarbeiterInnen überlassen, ab welcher Wahrscheinlichkeit sie das Ergebnis für die Entscheidung über einen Asylantrag für relevant halten. Damit erfolgt die Überprüfung der Herkunftsangabe eben nicht nur objektiv anhand der Ergebnisse der Software, sondern auch anhand des impliziten Dienstwissens der EntscheiderInnen. Gleichwohl symbolisiert der Einsatz der Software sowohl intern (gegenüber den MitarbeiterInnen) als auch extern (gegenüber der Gesellschaft) ein rationales und objektives Verfahren und stellt so Legitimität her.

Technische Innovation erfüllt Rationalisierungserwartungen der Umwelt

Schließlich bemüht sich das BAMF Legitimität zu erlangen, indem es betont, wie innovativ seine Software sei. So behauptet die Behörde, eine Vorreiterrolle bezüglich der Digitalisierung von Verwaltungsaufgaben eingenommen zu haben (BAMF 2017d:7). Die Sprachbiometrie-Software wird dabei als „innovativ“, „agil“ und „weltweit einzigartig“ beschrieben (BAMF 2018a:4; Bundesregierung 2017:4; 2018a:15; Richter zit. n. Frank 2018). Das BAMF bemüht sich also darum, die Legitimitätsprobleme, die auf Effektivitäts- und Effizienzschwächen beruhen, durch den Verweis auf die Innovativität ihrer Lösung wettzumachen. So heißt es von der Bundesregierung (2017), die Sprachbiometrie-Software sei speziell für die Bedürfnisse des BAMF entwickelt worden. Zwar sei die Identitätsfeststellung anhand der Stimme – als „Grundfunktionalität“ der Software – auch schon vorher möglich gewesen, doch die Anpassung auf eine Dialekterkennung wäre erst im Zuge der Softwareentwicklung zusammen mit dem BAMF konzipiert worden.

Innovationen können für die Legitimitäts Erlangung jedoch sowohl förderlich als auch hinderlich sein. Wenn mit den Innovationen neue Elemente und Strukturen einhergehen, die noch nicht institutionalisiert sind, werden sie erstmal auch nicht als legitim wahrgenommen, müssen Legitimität also erst noch erlangen. Technische Innovationen wie die algorithmische Erkennung von Sprachen und Dialekten verfügen allerdings über einen hohen Legitimitätsfaktor, da sie den gesellschaftlichen Rationalisierungserwartungen gerecht werden. Innovationen finden dabei meist nur auf der Ebene der Selbstbeschreibung statt, dienen also nicht unbedingt dazu, die Prozesse tatsächlich effizienter und besser zu gestalten.

Umso wichtiger ist es, dass die Software im Rahmen der „eGovernment-Preisverleihung“ zum „Besten Digitalisierungsprojekt 2018“ ernannt wurde (BAMF 2018b). Dadurch wird die Software gerade aufgrund ihrer Innovativität legitimiert. Weiterhin behauptet das BAMF, es sei „ein gefragter Ansprechpartner und Ratgeber für die Entwicklung und Einführung ähnlicher Verfahren in unseren europäischen Partnerländern. Zusammen mit

unseren europäischen Partnern prüft das Bundesamt kontinuierlich Möglichkeiten zur Kooperation, um Erfahrungen auszutauschen, aber vor allem zur Weiterentwicklung des Systems“. Diese Bewertungen sind das, was Meyer und Rowan (2009) als „zeremonielle Anerkennungen“ (S. 41) bzw. „externe Segnungen“ (S. 47) bezeichnet haben. Durch den Rückgriff auf externe institutionalisierte Bewertungskriterien werden „Organisationen gegenüber intern Beteiligten, Aktionären, der Öffentlichkeit und dem Staat“ (ebd.) legitimiert.

Legitimitätsbemühungen auf Kosten der AntragsstellerInnen

Als Fazit lässt sich festhalten, dass der Einsatz der Sprachbiometrie-Software durch das BAMF zwar förderlich sein kann, um den genannten Legitimitätsdefiziten des BAMF zu begegnen; allerdings geschieht dies zu Lasten der betroffenen AsylantragstellerInnen, die in dem beschriebenen Kontext aus unterschiedlichen und zum Teil widersprüchlichen Anforderungen und Erwartungen an das BAMF von allen Parteien den geringsten Einfluss haben. In Anbetracht der fehlenden Informationen über die Funktionsweise und die geringe Zuverlässigkeit der Software wurde von der Bundesregierung und dem BAMF insofern eine recht einfache Lösung gewählt, die die potenzielle Notlage der Geflüchteten nicht angemessen berücksichtigt. So verfügen Geflüchtete weder über die (finanziellen) Ressourcen, um gegen Asylentscheidungen gerichtlich vorzugehen, noch haben sie die Möglichkeit, ihre Interessen als Legitimitätsforderungen an das BAMF oder die Bundesregierung zu adressieren.

Weiterhin zeigt sich, dass das BAMF nicht nur auf bereits bekannte Mechanismen zur Legitimierung der Software zurückgreift, sondern dass umgekehrt gerade der Einsatz von Algorithmen für das BAMF legitimierend wirkt. Dies ist insofern bemerkenswert, da die Fehlerquote der Software bei 15 bis 20 Prozent liegt und aus den entsprechenden Schulungsunterlagen des BAMF keine einheitlichen Informationen für eine zuverlässige Interpretation der Softwareergebnisse zu entnehmen sind. Die algorithmische Software dient damit als „rationalized myth“ (Meyer, Rowan 1977:347), dessen Objektivität und Effizienz als „taken for granted“ (ebd.: 341) angesehen wird. So basiert die Legitimität hier nicht auf faktischer, sondern auf geglaubter Rationalität. Der Einsatz algorithmischer Software wird vom BAMF also gar nicht direkt legitimiert, sondern die Software sorgt für einen „Legitimitätsglauben“ (Weber 1972:122) gegenüber dem BAMF, der zirkulär auf die Software zurückwirkt. Der strategische Versuch des BAMF, die eigenen Legitimitätsdefizite mit Hilfe von „innovativen Technologien“ (BAMF 2018c) zu lösen, lässt sich auch an dem aktuellen Projekt „Blockchain@BAMF“ beobachten, bei dem die Abläufe im Asylprozess „datensicher, transparent und effektiv“ (ebd.) bearbeitet werden sollen.

Bei diesem Beitrag handelt es sich um eine Zusammenfassung meiner Bachelorarbeit, die ich im Februar 2019 an der Humboldt Universität zu Berlin im Fach Sozialwissenschaften geschrieben habe.

Referenzen

- Ali A et al. (2016) Automatic Dialect Detection in Arabic Broadcast Speech. Proceedings of Interspeech.
- BAMF (2017a) Integriertes Identitätsmanagement – Plausibilisierung, Datenqualität und Sicherheitsaspekte. Einführung in die neuen IT-Tools. Online abrufbar unter: https://cdn.netzpolitik.org/wp-upload/2018/12/schulung_idms_bamf.pdf [01.02.2020].
- BAMF (2017b) Identitätssicherung und -feststellung im Migrationsprozess. Vier Fragen und Antworten zu den Herausforderungen und Praktiken im deutschen Kontext. Online abrufbar unter: <https://www.bamf.de/SharedDocs/Meldungen/DE/2017/EMN/20170927-am-emn-studie-identitaetssicherung-feststellung.html> [01.02.2020].
- BAMF (2017c) Anfrage an Bundesamt für Migration und Flüchtlinge „Biometrische Sprachsoftware zur Erkennung von Dialekten“. Online abrufbar unter: https://fragdenstaat.de/anfrage/biometrische-sprachsoftware-zur-erkennung-von-dialekten/#letter_end [20.02.2020].
- BAMF (2017d) Digitalisierungsagenda 2020. Bisherige Erfolge und Ausblick auf weitere digitale Projekte im Bundesamt für Migration und Flüchtlinge. Nürnberg: Bundesamt für Migration und Flüchtlinge. Online abrufbar unter: <https://www.bamf.de/SharedDocs/Anlagen/DE/Digitalisierung/broschuere-digitalisierungsagenda-2020.html> [20.02.2020].
- BAMF (2018a) Sprachbiometrisches Assistenzsystem. Unterstützung der Feststellung von Herkunft und Identität im Asylverfahren. Online abrufbar unter https://www.egovernment-wettbewerb.de/presentationen/2018/Kat_Digitalisierung_BAMF_Sprachbiometrie.pdf [21.02.2020].
- BAMF (2018b) eGovernment Preisverleihung: 1. Platz. Presseinformation. Online abrufbar unter: <https://www.bamf.de/SharedDocs/Meldungen/DE/2018/20180621-am-egovernment.html> [14.02.2020].
- BAMF (2018c) Blockchain@BAMF. Blockchain zur Verbesserung der Zusammenarbeit im Asylprozess. Online abrufbar unter: https://www.bamf.de/DE/Themen/Digitalisierung/digitalisierung_node.html [12.02.2020].
- Bundesregierung (2017) Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Petra Sitte, Anke Domscheit-Berg, Dr. André Hahn, weiterer Abgeordneter und der Fraktion DIE LINKE. Drucksache 19/107. Online abrufbar unter: <http://dipbt.bundes-tag.de/doc/btd/19/001/1900190.pdf> [15.12.2018].
- Bundesregierung (2018a) Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. Drucksache 19/1484. Online abrufbar unter: <http://dipbt.bundestag.de/dip21/btd/19/016/1901663.pdf> [13.02.2020].
- Bundesregierung (2018b) Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. Drucksache 19/5697. Online abrufbar unter: <http://dipbt.bundes-tag.de/dip21/btd/19/066/1906647.pdf> [12.02.2019].
- Cölltekin C, Rama T (2016) Discriminating similar languages with linear SVMs and neural networks. Proceedings of the VarDial Workshop.
- DiMaggio PJ, Powell WW (2009) Das „stahlharte Gehäuse“ neu betrachtet: Institutionelle Isomorphie und kollektive Rationalität in organisationalen Feldern. In: S. Koch & M. Schemmann (Hrsg.), Neo-Institutionalismus in der Erziehungswissenschaft. Grundlegende Texte und empirische Studien (S. 57-84). Wiesbaden: VS Verlag.
- Europäische Kommission (2018). Ein europäisches Konzept für künstliche Intelligenz. Online abrufbar unter: europa.eu/rapid/press-release_MEMO-18-3363_de.pdf [19.02.2020].
- Frank D (2018) Digitale Unterstützer im Asylverfahren. Wie Sprachbiometrie Asylentscheidungen auf eine noch breitere Grundlage stellt. Online abrufbar unter: <http://www.bamf.de/DE/Service/Top/Presse/Interviews/20181008-interview-cyber-security-report/interview-cyber-security-report-node.html> [10.02.2019].
- Hummel P (2017) Software soll Dialekt von Asylbewerbern untersuchen, Welt. Online abrufbar unter: <https://www.welt.de/wissenschaft/article162926845/Software-soll-Dialekt-von-Asylbewerbern-untersuchen.html> [10.02.2020].
- Meyer JW (1983) Institutionalization and the Rationality of Formal Organizational Structure. In: J. W. Meyer & R. Scott (Hrsg.), Organizational Environments. Ritual and Rationality (S. 261- 282). Beverly Hills/ London/ New Dehli: SAGE Publications.
- Meyer JW, Rowan B (1977) Institutionalized Organizations: Formal Structure as Myth and Ceremony. The American Journal of Sociology, 83(2), 340-363.
- Meyer JW, Rowan B (2009) Institutionalisierte Organisationen. Formale Struktur als Mythos und Zeremonie. In: S. Koch & M. Schemmann (Hrsg.), Neo-Institutionalismus in der Erziehungswissenschaft. Grundlegende Texte und empirische Studien (S. 28-56). Wiesbaden: VS Verlag.
- Pasquale F (2015) The Black Box Society. The Secret Algorithms That Control Money and Information. Cambridge/London: Harvard University Press.
- Tangermann J (2017) Identitätssicherung und -feststellung im Migrationsprozess. Herausforderungen und Praktiken im deutschen Kontext. Fokusstudie der deutschen nationalen Kontaktstelle für das Europäische Migrationsnetzwerk (EMN) (Bd. Working Paper 76): Bundesamt für Migration und Flüchtlinge. Online abrufbar unter: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/11b_germany_identity_study_final_de.pdf [12.02.2020].
- Weber M (1972 [1921]) Wirtschaft und Gesellschaft. Grundriss der verstehenden Soziologie (5. Auflage). Tübingen: Mohr Siebeck.



Alexandra E. Keiner

Alexandra E. Keiner studiert seit Oktober 2018 im Master Sozialwissenschaften am *Institut für Sozialforschung (ISW)* der Humboldt-Universität zu Berlin. Ihre Bachelorarbeit hat sie, ebenfalls am ISW, zum Thema *Legitimität von Algorithmen in politischen Verwaltungsorganisationen* geschrieben. Ihre Studienschwerpunkte sind Arbeitssoziologie, Digitalisierung und Herrschaftsverhältnisse in der Plattformökonomie. Sie ist studentische Mitarbeiterin am *Weizenbaum-Institut für vernetzte Gesellschaft* und am Lehrstuhl *Soziologie der Zukunft der Arbeit* am ISW. (Foto: Esra Eres)

Philipp Imperatori: Verschlüsselungspolitik der USA. Eine vergleichende Analyse der historischen Entwicklung

Bachelorarbeit, Technische Universität Darmstadt



Es ist mittlerweile sechseinhalb Jahre her, dass wir durch die Enthüllungen von Edward Snowden von der umfassenden Ausspähung unserer Kommunikation erfahren haben. Inzwischen ist das (fast) in Vergessenheit geraten – vielleicht, weil wir uns daran gewöhnt haben, vielleicht, weil wir es tatsächlich im täglichen Leben nicht wahrnehmen, vielleicht wegen der Oberflächlichkeit unserer Zeit, die sich längst anderen Themen zugewandt hat.

Doch der Ursprung der Arbeit, die wir hier bepreisen wollen, liegt noch viel weiter zurück: Als im Jahr 2000, nach der durch die Clipper-Initiative im Jahr 1993 ins Rollen gekommene *Crypto War* zuungunsten der Kontrollwünsche der US Regierung besiegelt war, insbesondere im Rahmen der US-Exportwünsche zur Erhaltung der Priorität des US-Krypto-Marktes eine Liberalisierung effektiver Kryptographie notwendig wurde, begann die geheimdienstliche Überwindung von Kryptographie zur Aufrechterhaltung der Überwachung mittels des geheimen Programms *Bullrun*.

Hier setzt die Arbeit von Philipp Imperatori: *Verschlüsselungspolitik der USA. Eine vergleichende Analyse der historischen Entwicklung* an, die an der Technischen Universität Darmstadt entstanden ist und die wir heute mit einem zweiten Preis des Weizenbaum-Studienpreises auszeichnen.

Seine Hypothese: Wenn die US-amerikanischen Sicherheitsbehörden *Key escrow* angesichts immenser und kaum umkehrbarer Liberalisierungsbewegungen nicht gesetzlich und öffentlich durchsetzen können, dann werden sie in Anbetracht ihrer nationalen Sicherheitsambitionen ihre Prioritätensetzung darauf verlagern, Verschlüsselung, die die Massenüberwachung effektiv behindert, nicht mehr gesetzlich stark zu regulieren, sondern mit anderen Mitteln zu kompromittieren. Dies betrifft insbesondere exklusive Verschlüsselungsexporte.

Daher setzt er die Forschungsfrage: „Welche Prioritäten setzt die US-amerikanische Verschlüsselungspolitik angesichts der Enthüllungen von Snowden unter Berücksichtigung des historischen Kontexts?“

Die Überwachungsprogramme der NSA sind im Sinne der nationalen Sicherheit zweckdienlich zur Eindämmung der Dual-Use-Gefahren. Allerdings bedeutet jede Schwachstelle, die die NSA erkennt, nicht veröffentlicht und nutzt oder in einem kryptographischen Verfahren einbaut oder einbauen lässt, auch die gesamte Schwächung des Verfahrens. Denn wenn der Nachrichtendienst Schwächen nutzen kann, können dies potenziell auch andere Akteure. Zudem ist aufgrund der Geheimhaltung der nachrichtendienstlichen Massenüberwachungsprogramme auch eine transparente Einsicht und deren Regulierung kaum möglich, zumal die NSA dank heutiger weltweiter Vernetzung auch Daten über eine große Anzahl an Menschen außerhalb der

USA sammelt, die solchen Vorgängen nicht zugestimmt haben. Somit geht von den verschlüsselungspolitischen Initiativen der NSA, die der allgemeinen Gefahrenbewertung der Kryptographie als Dual-Use-Technologie entspringen, selbst ein Dual-Use-Problem hervor. Edward Snowden sah für die Aufklärung des Dilemmas vermutlich als einzige Möglichkeit das Whistleblowing. Nach Öffentlichwerden der NSA-Aktivitäten wurde der durch Deregulierung beendete erste *Crypto War* mit einer neuen Geschichte fortgesetzt, bei der insbesondere amerikanische Firmen um Vertrauen kämpfen müssen. In dem Bündnis mit dem Namen *Reform Government Surveillance* begannen sie ein digitales Wettrüsten mit der NSA, die jetzt im Kampf um Verschlüsselung ihr zentraler Gegenspieler ist (im Fokus stehen nicht mehr die Ausfuhrgenehmigungen).

Das Ziel der Arbeit besteht darin, die Entwicklung von der *Clipper-Chip* und *Key-Escrow*-Initiative bis zu den Snowden-Enthüllungen 2013 zur Regulierung und Kontrolle von Kryptographie als Dual-Use-Technologie der US-Regierung gegenüber zu stellen. Seine Methode ist die interdisziplinär kompetente Dokumentenanalyse von wissenschaftlichen Veröffentlichungen, politischen Reden, öffentlichen Ankündigungen, Zeitungsartikeln und Gesetzen.

Während Publikationen seit den 1990er Jahren die Regulierung von Kryptographie als Dual-Use-Technologie in den USA und international vergleichen, haben die Enthüllungen von Snowden durch die Bekanntmachung geheimer Projekte zur Kommunikationsüberwachung erst historische Vergleiche zwischen öffentlichen und geheimen Projekten zur Kommunikationsüberwachung ermöglicht. Bisherige Veröffentlichungen zeigen vor allem den nachrichtendienstlichen Umgang mit der Dual-Use-Technologie Kryptographie. Aber sie thematisieren nicht die Diskrepanz zwischen der zunehmenden Erleichterung der Kryptographie-Ausfuhrbeschränkungen und den zugleich enthüllten verschlüsselungsuntergrabenden Programmen der NSA. Denn ihre Arbeiten berücksichtigen nicht, wie sich die Verschlüsselungspolitik auch auf die Ebene der Exportregulierung bis heute auswirkt. Diese Forschungslücke schließt diese Arbeit und verwendet dabei neue Erkenntnisse und Entwicklungen der Snowden-Enthüllungen, um einen historischen Vergleich der Regulierungen, Überwachungsprogramme und der technischen Entwicklung zu ziehen.

Bezüglich der Verschlüsselungs-Methoden, symmetrischen und asymmetrischer Verschlüsselung, befasst er sich der US-Politik folgend hauptsächlich mit Schlüssellänge und Malware.

Ausgangspunkt für den Vergleich bilden die zwei paradox zueinander stehenden Ausrichtungen der US-amerikanischen Verschlüsselungspolitik: der langwierige Prozess hin zu liberalisierten Regulierungen von Kryptographie und zum anderen die weitreichenden Überwachungsprogramme US-amerikanischer



Nachrichtendienste zur Überwindung und Eindämmung von Kryptographie. Zur besseren Vergleichbarkeit werden die historische Nachrichtendienstaktivität und die aktuelle Regulierung untersucht. Diese Gegenüberstellung soll den Widerspruch analysieren und erklären. Der Vergleich erfolgt auf einer technisch-organisatorischen Ebene, also wie Verschlüsselung tatsächlich infiltriert oder anhand welcher Indikatoren sie begrenzt wurde und wird, sowie welche Akteure der Regierung dafür inwiefern verantwortlich sind. Die Enthüllungen von Snowden haben erst historische Vergleiche zwischen öffentlichen und geheimen Projekten zur Kommunikationsüberwachung ermöglicht, letztere stellen eine Forschungslücke dar, die Imperatori schließen möchte.

Hypothese ist, dass die Liberalisierung der Kryptographie-Regulierung, und der Schwierigkeiten, *Key escrow* gesetzlich zu verankern, aufgrund öffentlichen Widerstands durch andere Programme kompensiert wurde: z.B. zeigt sich, dass die Schwelle der Regulierung der Schlüssellänge trotz schrittweiser Erhöhung immer unter dem notwendigen Sicherheitsniveau geblieben ist. Einzelfallentscheidungen zeigen bei der Liberalisierung gleichzeitige Zunahme von nicht-öffentlichen Einzelfallentscheidungen durch die NSA.

Allgemein wird die Ausgewogenheit zwischen Sicherheit und Privatsphäre als Dilemma betrachtet. Doch fraglich ist, ob dieses Dilemma bei der Kryptographie eine passende Analogie ist. Es gibt genügend Argumente dafür, dass Verschlüsselung sowohl die Privatsphäre als auch die Sicherheit schützt, indem es beispielsweise Geschäftsgeheimnisse, den elektronischen Handel, finanzielle Angelegenheiten oder gar die allgemeine Infrastruktur absichert. Doch die US-amerikanische Regierung so-

wie insbesondere ihr Geheimdienst NSA sehen die Verbreitung von starker Verschlüsselung, die die Privatsphäre schützt und Informationen vor jedem anderem Akteur als dem Besitzer verschließt, offiziell als Gefahr für die nationale Sicherheit und bewerten sie deshalb weiterhin als Dual-Use-Technologie. Mittels ihrer Nachrichtendienste torpedieren die USA heutzutage weltweit die Kryptographie.

Das Programm *Bullrun* korrumpiert die weitläufig verwendeten Online-Protokolle wie VPN, VoIP und SSL. Aber die NSA baut auch systematisch Hintertüren in Router, Server und andere Computernetzwerkgeräte von US-Herstellern, sie hat in der Abteilung TAO circa 50.000 Computernetzwerke weltweit mit Malware infiziert, um bei Bedarf sensible Informationen abzuhehren und die Kontrolle über verschiedene Funktionalitäten zu gewinnen, womit es möglich wurde, Mikrofone, Webcams oder Internetverläufe samt Login-Details von infiltrierten Computern auszuspähen.

Die Arbeit ist für eine Bachelorarbeit ungewöhnlich: die historisch-kritische Arbeit bearbeitet einen komplexen, interdisziplinären Sachverhalt, in dem sowohl technische, rechtliche als auch politische Parameter gut verständlich analysiert und visualisiert wurden. Das Innovationspotential der Arbeit liegt in dieser historischen Analyse der sich wandelnden technischen, prozeduralen und institutionellen Indikatoren der Dual-Use-Regulierung von Kryptographie. Dies ist ein zentrales Thema des FlfF. Die Jury hat sich einhellig für einen zweiten Preis für diese Arbeit entschieden.

Herzlichen Glückwunsch, Philipp Imperatori, zum Weizenbaum-Studienpreis 2019.



Philipp Imperatori, Thea Riebe und Christian Reuter

Verschlüsselungspolitik der USA: Vom Clipper-Chip zu Edward Snowden



2. Preis

Mit der zunehmenden Bedeutung des Internets, vernetzter Kommunikation und der daraus resultierenden Notwendigkeit der Verwendung von Verschlüsselungstechniken für vertrauliche Daten hat sich die Regulierung von Verschlüsselung verändert. Die USA, in denen die größten IT-Unternehmen ihre Produkte entwickeln, haben ihren Einfluss auf diese Unternehmen durch Exportbeschränkungen kontrolliert und haben somit einen besonderen Zugang zur Kommunikationstechnologie von Menschen auf der ganzen Welt. Dieser Artikel gibt einen Einblick in die Politik bis zum Jahr 2000, in welchem sich eine deutliche Liberalisierung des Umgangs mit Kryptographie zeigte. Im Widerspruch dazu stehen die Veröffentlichungen Edward Snowdens, welche Aufschluss über die heutige Agenda der Dual-Use-Regulierung von Kryptographie geben.¹

US-amerikanische Verschlüsselungspolitik als Forschungsschwerpunkt

Während Kommunikation früher zumeist auf das lokale und private Gespräch begrenzt war, werden seit dem Aufschwung der informationsorientierten Technologien die häufig privaten Daten durch das globale Netz des Internets übermittelt und auf Endgeräten oder Servern gespeichert. Diese Entwicklung ermöglicht zwar den Austausch über weite Distanzen, sie macht es jedoch schwieriger, Informationen vor Dritten, wie IT-

Dienstleistern oder Geheimdiensten, zu schützen und stellt dadurch auch ein Risiko für weitere kritische Infrastrukturbereiche dar (Reuter, 2019). Für diese Herausforderung scheint es, sowohl für die Übermittlung als auch die Speicherung, nur eine zweckmäßige Lösung zu geben: die Verwendung einer Wissenschaft, der Kryptographie, zur sicheren Verschlüsselung der Daten (Landau, 2015; Wassenaar Arrangement Secretariat, 2018). Heutzutage gibt es unzählige kryptographische Algorithmen. Sie sind in heutigen Kommunikationsnetzen, Geräten und Dienstleistungen der Informationstechnologie (IT) allgegenwärtig und



werden dabei meistens im Hintergrund ohne Zutun des Nutzers automatisch verwendet. Das setzt jedoch eines voraus: Internetnutzer, die normalerweise wenig Kryptographie-Expertise mitbringen, müssen der Kommunikationsinfrastruktur vertrauen und sich auf die solide Umsetzung von sicheren kryptographischen Verfahren verlassen.

Schon im frühen elektronischen Zeitalter war die US-amerikanische Industrie global führend im Entwickeln von Computern und Kommunikationstechnologien (Southard, 1997, p. 47). Während der Verbreitung des Internets Anfang der 1990er Jahre hatte die US-Wirtschaft einen geschätzten Anteil von 75 Prozent am globalen Softwaremarkt (Marino, 2005, p. 102). Heute wird der Markt der anwendungsbezogenen IT vor allem von US-amerikanischen Großunternehmen wie Apple, Google, Microsoft, Facebook und Amazon dominiert (Andriole, 2018). Davon abgesehen verfügen Unternehmen mit Hauptsitz in den USA im weltweiten Cyber-Security-Software-Markt, also dem Markt für Sicherheitssoftwarelösungen, über eine signifikante Dominanz: Im Jahr 2015 lag ihr Marktanteil bei circa 61 Prozent (Australian Cyber Security Growth Network, 2018).

Diese Wirtschaftsstärke kommt jedoch mit einer bemerkenswerten Politik seitens der Vereinigten Staaten einher. Kryptographie galt über einige Jahrzehnte in den USA als Waffe und durfte aufgrund starker Regulierungen nicht exportiert werden (Black, 2002, p. 353). Durch die Regulierung sollte der Rest der Welt von starken Verschlüsselungen ausgeschlossen werden. Seit jeher galten das reine Hochladen von Verschlüsselungs-beinhaltenem Programmcode auf eine international erreichbare Webseite oder das Senden einer verschlüsselten E-Mail zu einem ausländischen Kollegen als Export (Black, 2002; Haignere, 1998, pp. 326–328; Schwedter, 2016, p. 2). Mit der Digitalisierung und Verbreitung von digitaler Kommunikation, haben sich auch die Regulierungen angepasst. Dabei ist der 14. Januar 2000 ein zentraler Wendepunkt: Die Administration unter US-Präsident Bill Clinton gab weitreichende Reformen bekannt, die die bis dahin seit Jahrzehnten strikten Ausfuhrbeschränkungen umfassend umgestalteten und dabei allem Anschein nach deutlich liberalisierten (Jolish, 2001, p. 213). Dies wurde von der Softwareindustrie als bedeutender Sieg nach einem jahrelangen Kampf mit der Regierung, der auch als sogenannter *Crypto War* bezeichnet wird, gesehen (Diffie & Landau, 2000, p. 1).

Doch schon vor dem Entgegenkommen durch reformierte Regulierungen entwickelte der Auslandsgeheimdienst National Security Agency (NSA) einen alternativen regulatorischen Lösungsansatz, um so einen Kompromiss zwischen den Bedürfnissen der Wirtschaft und denen der nationalen Sicherheit zu finden (Schulze, 2017). Er basierte auf einer eigens entwickelten Kombination aus einem sogenannten *Clipper-Chip* und einem manipulierten Algorithmus mit einem für damalige Verhältnisse allem Anschein nach hohen Sicherheitsniveau. Diese sollte der Verschlüsselungsstandard bei Kommunikationen werden, wobei eine eingebaute Hintertür der Strafverfolgung Ermittlungen ermöglichen sollte. Zwar scheiterte das Projekt aufgrund der fehlenden Umsetzung durch die Wirtschaft, doch es heizte eine umfangreiche Datenschutzdebatte an, die den historischen *Crypto War* vermutlich erst entfesselte (Steven Levy, 1994).

Aus heutiger Sicht wirft die Überwachungs- und Spionageaffäre der NSA, ausgelöst durch den ehemaligen NSA-Agenten Edward Snowden beginnend im Jahr 2013, eine weitere beispiellose Perspektive auf die Verschlüsselungspolitik der USA. Kryptographie scheint in der Sache unverändert noch heute für zahlreiche US-amerikanische Sicherheitsbehörden ein Dorn im Auge zu bleiben. In den Terrorangriffen von Paris im November 2015 sah der CIA-Direktor John Brennan einen Weckruf, der auch Europäer zur Einsicht bringen sollte, dass Verschlüsselung eine Sicherheitsgefahr darstelle (Geminn, 2015, p. 546; Sokolow, 2015). Doch bereits zwei Jahre zuvor hatte Snowden enthüllt, dass die Vereinigten Staaten womöglich bereits Lösungen für die Eindämmung dieser Gefahr gefunden hatten. Der Nachrichtendienst habe es den Enthüllungen Snowdens zufolge schrittweise geschafft, einige der Verschlüsselungstechnologien teilweise zu umgehen oder zu brechen, die heutzutage den globalen Handel, die Bankensysteme, Geschäftsgeheimnisse, Medizinaufzeichnungen, E-Mails, Websuchen, Internetchats und Telefonanrufe schützen, wie die Dokumente zeigen (Perlroth, Larson et al., 2013).

Es stellt sich die Frage, wieso die Beschränkungen ab dem Jahr 2000 gelockert wurden. Schließlich wurden in den Nachfolgejahren große Anstrengungen unternommen Überwachungsprogramme aufzubauen, um Kryptographie global zu überwinden. Es ist fraglich, wie liberal die aktuelle Verschlüsselungspolitik der USA wirklich ist. Dies ist insbesondere unter Anbetracht des technischen Fortschritts innerhalb der letzten Jahrzehnte spannend, welcher stärkere Kryptographie aufgrund gesteigerter Rechenkapazitäten und der Verbreitung des Internets erfordert. Ein chronologischer Blick auf die Regulierungen im Detail als auch die Betrachtung von Snowdens Enthüllungen sowie des historischen *Clipper-Chip*-Programms verdeutlichen, dass sowohl Ausfuhrbestimmungen als auch die Arbeit der NSA wesentliche Instrumente US-amerikanischer Verschlüsselungspolitik waren und sind. Es ist unklar, auf welche Weise und in welchem Umfang sie die Kryptographie beschränken und welches der beiden Instrumente im Zuge der nationalen Sicherheitsvorkehrungen priorisiert wird, was die vergleichende historische Analyse dieser scheinbar zweiseitigen Verschlüsselungspolitik interessant macht.

Eine Wissenschaft als Politikum

Es gibt diverse wissenschaftliche Veröffentlichungen, die die historische Verschlüsselungspolitik darstellen. Überblickend und vielseitig hat Sharon K. Black (Black, 2002) die Regulierungen, Überwachungsgesetze und Bestimmungen der USA über mehrere Jahrzehnte bis zur Jahrtausendwende unter Berücksichtigung kausaler und chronologischer Verkettungen untersucht. Zudem erläutern Mendelson, Walker und Witson (1998) detailliert und chronologisch die Regulierungen in ihrer Intensität und schlagen damit einen ähnlichen analytischen Weg wie Black ein. Jedoch unterscheidet dieser explizit zwischen inländischen und Exportkontrollen und legt seinen Fokus gleichzeitig mehr auf rein gesetzliche Entwicklungen. Landau und Diffie, letzterer, einer der beiden Pioniere der asymmetrischen Kryptographie, zeigen eine zusammenhangsbezogene Perspektive auf, wobei sie die anderen Arbeiten insoweit ergänzen, indem sie einen Erklärungsansatz für den rapiden Liberalisierungsprozess suchen (Diffie, 2000).



Landau (2015), Schulze (2017), Rubinstein und Hoboken (2014), Gill, Israel und Parsons (2018) und Soesanto (2018) setzen in ihren Veröffentlichungen einen Fokus auf das enthüllte NSA-Agieren unter historischer Bezugnahme. Sie zeigen damit vor allem den nachrichtendienstlichen Umgang mit der Dual-Use-Technologie Kryptographie. Allerdings bieten sie unzureichende Antworten auf die Diskrepanz zwischen der zunehmenden Erleichterung der Kryptographie-Ausfuhrbeschränkungen und den zugleich enthüllten verschlüsselungsuntergrabenden Programmen der NSA. Schließlich bedeutet die *Dual-Use*-Deklaration einer Technologie in den USA obligatorisch zuerst einmal die Begrenzung ihres Exports, also die Festsetzung von Regulierungen, welche damit implizit ein elementares Instrument der Verschlüsselungspolitik darstellen.

Die Begrifflichkeit *Dual-Use* beschreibt in der Forschung zumeist die doppelte Verwendbarkeit von Wissen, Technologie oder Gütern für nützliche und schädliche Zwecke, beziehungsweise für zivile und militärische Zwecke (Oltmann, 2015; Riebe & Reuter, 2019). Beispielsweise kann Kryptographie kriminellen oder kriegesischen Akteuren ermöglichen, ihre verbrecherischen Machenschaften geheim über verschlüsselte Kommunikationen zu organisieren, ohne dass Behörden in der Lage sind, diese Informationen für ihre Ermittlungen abzugreifen. Zugleich kann sie aber auch den Online-Handel oder andere vertrauliche Abwicklungen absichern sowie der Privatsphäre dienen. Bis heute wird die Regulierung von Kryptographie über die Schlüssellänge vorgenommen (Babbage et al., 2008). Das von Sicherheitsexperten empfohlene Sicherheitsniveau liegt mit 128 Bits für die Schlüssellänge mittlerweile weit über dem von den US-Behörden festgelegten Grenzwert von 56 Bits. Das bedeutet, dass jegliche Verschlüsselung, die nach Ansicht der Experten mindestens notwendig ist, damit diese sinnvolle Sicherheit bietet, als *Dual-Use*-Technologie von den USA bewertet wird und damit den Regulierungen unterliegt.

Darüber hinaus hatte es der Geheimdienst NSA sowohl mittels des im Jahre 1993 verkündeten *Clipper-Chips* als auch mittels der Geheimprogramme, welche durch Snowden zwanzig Jahre später öffentlich wurden, jeweils auf die Dechiffrierung von

weitreichenden kryptographischen Kommunikationen durch Hintertüren abgesehen. Nach Kenntnisnahme durch die breite Öffentlichkeit wurden durch beide Projekte jeweils der Impuls zu bedeutenden Debatten gegeben – weil diese in den 1990er Jahren als sogenannter *Crypto War* beschrieben wurde (Steven Levy, 1994), spricht man heute nach der zwischenzeitlichen Beruhigung nun von einer Fortsetzung des *Crypto Wars*, also einem *Crypto War 2.0*, der bis heute andauert (Soesanto, 2018). Während die Clipper-Initiative in einem legalen, freiwilligen und von der NSA manipulierten Verschlüsselungsstandard für Telefonate und Daten mündete, konzentrierte man sich mit den Geheimprogrammen später vor allem auf die Brechung, Infiltrierung und Manipulierung bereits bestehender kryptographischer Standards. Doch vielleicht am bedeutendsten: Wo man damals von einem insgesamt erfolglosen Vorstoß der NSA gegen nicht zu überwindende Kryptographie aufgrund zu großer Widerstände sprechen konnte, scheint es die NSA mittels des Geheimprojekts geschafft zu haben, Kryptographie überall auf der Welt mittels zahlreicher Wege zu untergraben.

US-amerikanische Unternehmen mussten seit den Snowden-Aufdeckungen bei ihren Kunden um Vertrauen kämpfen: Apple und Google, die die Betriebssysteme für Smartphones dominieren, haben mit automatischen Verschlüsselungen reagiert, die es ihnen auch nach Gerichtsbeschlüssen nicht mehr möglich machen soll, Daten herauszugeben (Craig Timberg, 2014). Zahlreiche Unternehmen erweiterten ihre Sicherheitsmaßnahmen mit Millionen-Investitionen und begannen ein digitales Wettrüsten mit der NSA (Perloth & Goel, 2013). Während die Unternehmen sich früher durch die Ausfuhrregulierungen beeinträchtigt sahen, ist heute die NSA im Kampf um Verschlüsselung ihr zentraler Gegenspieler. Damals wie heute macht das die US-amerikanische Verschlüsselungspolitik zu einem unverträglichen Faktor für die Wirtschaft des eigenen Landes.

Allgemein wird die Ausgewogenheit zwischen Sicherheit und Privatsphäre als Dilemma betrachtet. Doch fraglich ist, ob dieses Dilemma bei der Kryptographie eine passende Analogie ist. Es gibt genügend Argumente dafür, dass Verschlüsselung sowohl die Privatsphäre als auch die Sicherheit schützt, indem es



Philipp Imperatori, Thea Riebe und Christian Reuter

Philipp Imperatori, Bachelorand am Lehrstuhl *Wissenschaft und Technik für Frieden und Sicherheit (PEASEC)* von Professor Christian Reuter.

Thea Riebe, M.A. studierte Internationale Studien / Friedens- und Konfliktforschung an der Goethe Universität Frankfurt, der TU Darmstadt und der Universität de Lausanne, und ist wissenschaftliche Mitarbeiterin in der *BMBF-Arbeitsgruppe KontiKat* der Universität Siegen sowie Doktorandin am Lehrstuhl *Wissenschaft und Technik für Frieden und Sicherheit (PEASEC)* im Fachbereich Informatik (FB 20) der TU Darmstadt.

Prof. Dr. **Christian Reuter** ist Universitätsprofessor und Inhaber des Lehrstuhls *Wissenschaft und Technik für Frieden und Sicherheit (PEASEC)* im Fachbereich Informatik mit Zweitmitgliedschaft im Fachbereich Gesellschafts- und Geschichtswissenschaften der Technischen Universität Darmstadt.



beispielsweise Geschäftsgeheimnisse, den elektronischen Handel, finanzielle Angelegenheiten oder gar die allgemeine Infrastruktur absichert. Doch die US-amerikanische Regierung sowie insbesondere ihr Geheimdienst NSA sehen die Verbreitung von starker Verschlüsselung, die die Privatsphäre schützt und Informationen vor jedem anderem Akteur als dem Besitzer verschließt, offiziell als Gefahr für die nationale Sicherheit und bewerten sie deshalb weiterhin als Dual-Use-Technologie. Mittels ihrer Nachrichtendienste torpedieren die USA heutzutage weltweit die Kryptographie. Aus diesen Gründen ist und bleibt im Besonderen die Verschlüsselungspolitik der USA ein brisantes Thema in der Debatte um die verbreitete Nutzung von Kryptographie sowie eine besondere Herausforderung für den Schutz der BürgerInnen, aber auch für die Freiheit des internationalen Austauschs in Forschung und Handel.

Referenzen

- Andriole S (2018, September 26) Apple, Google, Microsoft, Amazon And Facebook Own Huge Market Shares = Technology Oligarchy. Forbes. Retrieved from <https://www.forbes.com/sites/steveandriole/2018/09/26/apple-google-microsoft-amazon-and-facebook-own-huge-market-shares-technology-oligarchy/>
- Australian Cyber Security Growth Network. (2018) Global cyber security software market share by company domicile. Australia's Cyber Security: Sector Competitiveness Plan 2018.
- Babbage S, Catalano D, Cid C, Dunkelman O, Gehrman C, Granboulan L, ... Ward M (2008) ECRYPT Yearly Report on Algorithms and Keysizes (2007-2008). (M. Näslund, Ed.).
- Black, SK (2002) Encryption. In Adams R (Ed.), Telecommunications Law in the Internet Age (1st ed., pp. 327–387). Morgan Kaufmann Publishers, San Francisco (USA).
- Timberg C (2014, September 18) Newest Androids will join iPhones in offering default encryption, blocking police. The Washington Post. Retrieved from <https://www.washingtonpost.com/news/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/?arc404=true>
- Diffie W, Landau S (2000) The Export of Cryptography in the 20th Century and the 21st. Palo Alto, California. Retrieved from <https://pdfs.semanticscholar.org/1870/af818dd0075bb5e79764427a7c932fe3cfc6.pdf>
- Geminn CL (2015) Crypto Wars Reloaded? Datenschutz Und Datensicherheit – DuD, vol. 39, iss. 8, pp. 546–547. <https://doi.org/10.1007/s11623-015-0468-7>
- Gill L, Israel T, Parsons C (2018) Shining a Light on the Encryption Debate: A Canadian Field Guide. Retrieved from <https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf>
- Haignere EF (1998) An Overview of the Issues Surrounding the Encryption Exportation Debate, Their Ramifications, and Potential Resolution. Maryland Journal of International Law, vol. 22, iss. 2, pp. 319–358.
- Jolish BD (2001) The Encryption Debate in Plaintext: National Security and Encryption in the United States and Israel. In Y. Frankel (Ed.), Financial Cryptography (Vol. 1962, pp. 202–224). Anguilla, British West Indies: Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-45472-1_15
- Landau S (2015) NSA and Dual EC_DRBG: Déjà Vu All Over Again? The Mathematical Intelligencer, vol. 37, iss. 4, pp. 72–83. <https://doi.org/10.1007/s00283-015-9543-z>
- Marino LH (2005) The U.S. Export Control Regime for Encryption. The Journal of World Intellectual Property, vol. 1, iss. 1, pp. 101–119. <https://doi.org/10.1111/j.1747-1796.1998.tb00005.x>
- Mendelson KA, Walker ST, Winston JD (1998) The Evolution of recent cryptographic policy in the United States. Cryptologia, vol. 22, iss. 3, pp. 193–210. <https://doi.org/10.1080/0161-119891886876>
- Oltmann S (2015) Dual use research: investigation across multiple science disciplines. Science and Engineering Ethics, vol. 21, iss. 2, pp. 327–341. <https://doi.org/10.1007/s11948-014-9535-y>
- Perlroth N, Goel V (2013, December 5) Internet Firms Step Up Efforts to Stop Spying. The New York Times. The New York Times. Retrieved from <http://www.nytimes.com/2013/12/05/technology/internet-firms-step-up-efforts-to-stop-spying.html>, http://www.nytimes.com/2013/12/05/technology/internet-firms-step-up-efforts-to-stop-spying.html?hp&_r=0
- Perlroth N, Larson J, Shane S (2013, September) N.S.A. Able to Foil Basic Safeguards of Privacy on Web.
- Reuter C Ed. (2019) Information Technology for Peace and Security. Wiesbaden: Springer Vieweg.
- Riebe T, Reuter C (2019) Dual-Use and Dilemmas for Cybersecurity, Peace and Technology Assessment. In Reuter C Ed., Information Technology for Peace and Security – IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace (pp. 165–183). Wiesbaden: Springer.
- Rubinstein I, Van Hoboken J (2014) Privacy and Security in the Cloud: Some Realism About Technical Solutions to Transnational Surveillance in the Post-Snowden Era. NYU School of Law, Public Law & Legal Theory Research Paper Series, vol. 66, iss. 2, pp. 486–533.
- Schulze M (2017) Clipper Meets Apple vs. FBI—A Comparison of the Cryptography Discourses from 1993 and 2016. Media and Communication, vol. 5, iss. 1, pp. 54. <https://doi.org/10.17645/mac.v5i1.805>
- Schwechter MS (2016) Brief Export Controls for Software Companies – What You Need to Know. BakerHostetler. Retrieved from <https://www.bakerlaw.com/webfiles/Litigation/2016/Brief/09-01-2016-Schwechter-Brief.pdf>
- Soesanto, Stefan. (2018). No middle ground: moving on from the crypto wars. Policy Brief. European Council on Foreign Relations (ECFR). Retrieved from https://www.ecfr.eu/page/-/no_middle_ground_moving_on_from_the_crypto_wars.pdf
- Sokolow A (2015, November 23) Terror in Paris: Erneut Diskussion über Verschlüsselung. Frankfurter Rundschau. Frankfurt, Deutschland: Frankfurter Rundschau. Retrieved from <https://www.fr.de/kultur/erneut-diskussion-ueber-verschluesselung-11140584.html>
- Southard LS (1997) Securing Information Technology Through Cryptography: An Analysis of United States Policy. Policy Perspectives, vol. 4, iss. 1, pp. 43. <https://doi.org/10.4079/pp.v4i1.4190>
- Steven L (1994, June 12) Battle of the Clipper Chip. The New York Times. Retrieved from <https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html?pagewanted=all>
- Vella V (2017) Is There a Common Understanding of Dual-Use?: The Case of Cryptography. Strategic Trade Review, vol. 3, iss. 4, pp. 103–122.
- Wassenaar Arrangement Secretariat (2018) The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. Retrieved from <http://www.wassenaar.org>

Anmerkung

- 1 Die Grundlage des Artikels ist die Bachelorthesis von Philipp Imperatori am Lehrstuhl Wissenschaft und Technik für Frieden und Sicherheit (PEASEC) der Technischen Universität Darmstadt, die mit dem zweiten Weizenbaum-Studienpreis ausgezeichnet wurde.



Mitgliederversammlung (MV) des FfF

Bremen, 24. November 2019, 12:06–14:25 Uhr

– Beschlussprotokoll –

Sitzungsleitung: Stefan Hügel als Vorsitzender des FfF

1. Begrüßung und Feststellung der Beschlussfähigkeit und der Protokollführung

Zur Versammlung ist ordentlich eingeladen worden und diese ist dadurch beschlussfähig. Protokollführung: Jens Rinne

2. Beschlussfassung über Tages- und Geschäfts- und Wahlordnung

Geschäfts- und Wahlordnung wird von der MV in bekannter Form genehmigt.

Der Tagesordnung wurde mit Ergänzung um Punkt 12 „Genehmigung des Protokolls“ zugestimmt.

3. Bericht des Vorstandes einschl. Kassenbericht

Stefan Hügel berichtet über die kontinuierliche Arbeit des FfF seit der letzten MV und über den Haushalt mit Stand 22.11.2019. Außerdem berichten Vertreter der Regionalgruppen.

Es wurden keine Beschlüsse gefasst.

4. Bericht der Kassenprüfer

Für die am 15.5.2019 in Bremen durchgeführte Kassenprüfung durch Klaus Lüttich und Andreas Spillner berichtet Klaus Lüttich der MV. Es wurden keine Beschlüsse gefasst. Aus dem Kassenprüfungsprotokoll: „Dem Vorstand wird eine dem Vereinszweck entsprechende, ordnungsgemäße Kassenführung bescheinigt. Einer Entlastung des Vorstandes steht nach unserer Auffassung nichts entgegen. Wir beantragen die Entlastung des Vorstandes.“

5. Diskussion der Berichte

Es wurden keine Beschlüsse gefasst.

6. Entlastung des Vorstandes

Die Kassenprüfer schlagen die Entlastung des Vorstandes vor.

Die MV entlastet den Vorstand einstimmig bei 7 Enthaltungen.

7. Neuwahl des Vorstandes

MV wählt einstimmig Klaus Lüttich als Wahlleiter und Andreas Spillner als Wahlhelfer. Es sind 35 stimmberechtigte Mitglieder anwesend.

Vorsitzender: Stefan Hügel

Abgegeben: 34 | Gültig: 34 | (ja/nein/enth.): 32/0/2

Wahl angenommen

Stellvertretender Vorsitzender: Rainer Rehak

Abgegeben: 35 | Gültig: 34 | (ja/nein/enth.): 30/2/2

Wahl angenommen

Beisitzerinnen und Beisitzer:

1. Wahlgang | Abgegeben: 29 | Gültig: 29

		ja/nein/enth.	Wahl
1	Michael Ahlmann	26/1/2	angenommen
2	Maximilian Hagner	24/2/3	angenommen
3	Alexander Heim	24/1/3	angenommen
4	Sylvia Johnigk	25/1/3	angenommen
5	Hans-Jörg Kreowski	28/0/1	angenommen
6	Kai Nothdurft	27/0/2	angenommen
7	Jens Rinne	25/1/3	angenommen
8	Britta Schinzel	28/0/1	muss noch gefragt werden
9	Ingrid Schlagheck	26/1/2	angenommen
10	Anne Schnerrer	21/2/6	angenommen
11	Werner Winzerling	24/2/3	angenommen

Stefan Hügel dankt im Namen des gesamten Vorstands den scheidenden Vorstandsmitgliedern Dietrich Meyer-Ebrecht, Benjamin Kees und Eberhard Zehndner für Ihre langjährige Arbeit im FfF-Vorstand.

8. Neuwahl der Kassenprüfer

Die MV wählt im Block einstimmig zu den neuen Kassenprüfern des FfF: Klaus Lüttich (stimmt zu) und Andreas Spillner (stimmt zu).

9. Diskussion über Ziele und Arbeit des FfF, aktuelle Themen, Verabschiedung von Stellungnahmen, Berichte aus den Regionalgruppen

Die Versammlung dankt dem Bremer Organisationsteam für die schöne Tagung hier.

Es wurden keine Beschlüsse gefasst.

10. Anträge an die Mitgliederversammlung

Es lagen keine Anträge vor. (Anträge mussten schriftlich bis drei Wochen vor der Mitgliederversammlung bei der FfF-Geschäftsstelle eingegangen sein.)

11. Verschiedenes

Es lagen keine Anträge vor.

12. Genehmigung des Protokolls

Das Protokoll wird einstimmig bei einer Enthaltung genehmigt.

Im FfF haben sich rund 700 engagierte Frauen und Männer aus Lehre, Forschung, Entwicklung und Anwendung der Informatik und Informationstechnik zusammengeschlossen, die sich nicht nur für die technischen Aspekte, sondern auch für die gesellschaftlichen Auswirkungen und Bezüge des Fachgebietes verantwortlich fühlen. Wir wollen, dass Informationstechnik im Dienst einer lebenswerten Welt steht. Das FfF bietet ein Forum für eine kritische und lebendige Auseinandersetzung – offen für alle, die daran mitarbeiten wollen oder auch einfach nur informiert bleiben wollen.

Vierteljährlich erhalten Mitglieder die Fachzeitschrift FfF-Kommunikation mit Artikeln zu aktuellen Themen, problematischen

Entwicklungen und innovativen Konzepten für eine verträgliche Informationstechnik. In vielen Städten gibt es regionale AnsprechpartnerInnen oder Regionalgruppen, die dezentral Themen bearbeiten und Veranstaltungen durchführen. Jährlich findet an wechselndem Ort eine Fachtagung statt, zu der TeilnehmerInnen und ReferentInnen aus dem ganzen Bundesgebiet und darüber hinaus anreisen. Darüber hinaus beteiligt sich das FfF regelmäßig an weiteren Veranstaltungen, Publikationen, vermittelt bei Presse- oder Vortragsanfragen ExpertInnen, führt Studien durch und gibt Stellungnahmen ab etc. Das FfF kooperiert mit zahlreichen Initiativen und Organisationen im In- und Ausland.

FfF-Mailinglisten

FfF-Mailingliste

An- und Abmeldungen an:

<http://lists.fiff.de/mailman/listinfo/fiff-L>

Beiträge an: fiff-L@lists.fiff.de

FfF-Mitgliederliste

An- und Abmeldungen an:

<http://lists.fiff.de/mailman/listinfo/mitglieder>

Mailingliste Videoüberwachung:

An- und Abmeldungen an:

<http://lists.fiff.de/mailman/listinfo/cctv-L>

Beiträge an: cctv-L@lists.fiff.de

FfF online

Das ganze FfF

www.fiff.de

Twitter FfF e.V. – [@FfF_de](https://twitter.com/FfF_de)

Cyberpeace

cyberpeace.fiff.de

Twitter Cyberpeace – [@FfF_AK_RUIN](https://twitter.com/FfF_AK_RUIN)

Faire Computer

blog.faire-computer.de

Twitter Faire Computer – [@FaireComputer](https://twitter.com/FaireComputer)

Mitglieder-Wiki

<https://wiki.fiff.de>

FfF-Beirat

Ute Bernhardt (Berlin); **Peter Bittner** (Kaiserslautern); **Dagmar Boedicker** (München); Dr. **Phillip W. Brunst** (Köln); Prof. Dr. **Wolfgang Coy** (Berlin); Prof. Dr. **Wolfgang Däubler** (Bremen); Prof. Dr. **Christiane Floyd** (Berlin); Prof. Dr. **Klaus Fuchs-Kittowski** (Berlin); Prof. Dr. **Michael Grütz** (München); Prof. Dr. **Thomas Herrmann** (Bochum); Prof. Dr. **Wolfgang Hesse** (München); Prof. Dr. **Wolfgang Hofkirchner** (Wien); Prof. Dr. **Eva Hornecker** (Weimar); **Werner Hülsmann** (München); **Benjamin Kees** (Berlin); **Ulrich Klotz** (Frankfurt am Main); Prof. Dr. **Klaus Köhler** (Mannheim); Prof. Dr. **Jochen Koubek** (Bayreuth); Prof. Dr. **Herbert Kubicek** (Bremen); Dr. **Constanze Kurz** (Berlin); Prof. Dr. **Klaus-Peter Löhr** (Berlin); Prof. Dr. **Dietrich Meyer-Ebrecht** (Aachen); **Werner Mühlmann** (Calau); Prof. Dr. **Frieder Nake** (Bremen); Prof. Dr. **Rolf Oberliesen** (Paderborn); Prof. Dr. **Arno Rolf** (Hamburg); Prof. Dr. **Alexander Rossnagel** (Kassel); **Ingo Ruhmann** (Berlin); Prof. Dr. **Gerhard Sagerer** (Bielefeld); Prof. Dr. **Gabriele Schade** (Erfurt); **Ralf E. Streibl** (Bremen); Prof. Dr. **Marie-Theres Tinnefeld** (München); Dr. **Gerhard Wohland** (Mainz); Prof. Dr. **Eberhard Zehendner** (Jena)

FfF-Vorstand

Stefan Hügel (Vorsitzender) – Frankfurt am Main
Rainer Rehak (stellv. Vorsitzender) – Berlin
Michael Ahlmann – Kiel / Blumenthal
Maximilian Hagner – Jena
Alexander Heim – Berlin
Sylvia Johnigk – München
Prof. Dr. **Hans-Jörg Kreowski** – Bremen
Kai Nothdurft – München
Jens Rinne – Mannheim
Prof. Dr. **Britta Schinzel** – Freiburg im Breisgau
Ingrid Schlagheck – Bremen
Anne Schnerrer – Berlin
Prof. Dr. **Werner Winzerling** – Fulda

FfF-Geschäftsstelle

Ingrid Schlagheck (Geschäftsführung) – Bremen
Philip Love – Bremen

Impressum

Herausgeber	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF)
Verlagsadresse	FIfF-Geschäftsstelle Goetheplatz 4 D-28203 Bremen Tel. (0421) 33 65 92 55 fiff@fiff.de
Erscheinungsweise	vierteljährlich
Erscheinungsort	Bremen
ISSN	0938-3476
Auflage	1 200 Stück
Heftpreis	7 Euro. Der Bezugspreis für die FIfF-Kommunikation ist für FIfF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FIfF-Kommunikation für 28 Euro pro Jahr (inkl. Versand) abonnieren.
Hauptredaktion	Dagmar Boedicker, Stefan Hügel (Koordination), Sylvia Johnigk, Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht, Ingrid Schlagheck
Schwerpunktredaktion	Michael Ahlmann, Hans-Jörg Kreowski, Philip Love, Ralf E. Streibl, Karin Vosseberg, Margita Zallmann
V.i.S.d.P.	Stefan Hügel
Retrospektive	Beiträge für diese Rubrik bitte per E-Mail an redaktion@fiff.de
Lesen, SchlussFIfF	Beiträge für diese Rubriken bitte per E-Mail an redaktion@fiff.de
Layout	Berthold Schroeder, München
Cover	Caro von Totth nach einem Entwurf von Karin Vosseberg, Motiv der FIfFKon 2019
Druck	Meiners Druck, Bremen Heftinhalt auf 100 % Altpapier gedruckt.



Die FIfF-Kommunikation ist die Zeitschrift des „Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V.“ (FIfF). Die Beiträge sollen die Diskussionen unter Fachleuten anregen und die interessierte Öffentlichkeit informieren. Namentlich gekennzeichnete Artikel geben die jeweilige Autor.innen-Meinung wieder.

Die FIfF-Kommunikation ist das Organ des FIfF und den politischen Zielen und Werten des FIfF verpflichtet. Die Redaktion behält sich vor, in Ausnahmefällen Beiträge abzulehnen.

Nachdruckgenehmigung wird nach Rücksprache mit der Redaktion in der Regel gern erteilt. Voraussetzung hierfür sind die Quellenangabe und die Zusendung von zwei Belegexemplaren. Für unverlangt eingesandte Artikel übernimmt die Redaktion keine Haftung.

Wichtiger Hinweis: Wir bitten alle Mitglieder und Abonnenten, Adressänderungen dem FIfF-Büro möglichst umgehend mitzuteilen.

Aktuelle Ankündigungen

(mehr Termine unter www.fiff.de)

FIfF-Konferenz 2020

13.-15. November 2020, Weimar, Bauhaus-Universität

FIfF-Kommunikation

2/2020 „Elektronische Gesundheitskarte“

Werner Winzerling u. a.

Redaktionsschluss: 1. Mai 2020

3/2020 „IT und Klima/Nachhaltigkeit“ (Arbeitstitel)

Dagmar Boedicker u. a.

Redaktionsschluss: 15. Juli 2020

Zuletzt erschienen:

1/2019 Brave new World 1

2/2019 Brave new World 2

3/2019 Cyberpeace und IT-Security

4/2019 Überwachungs-Gesamtrechnung

W&F – Wissenschaft & Frieden

2/19 Partizipation – Basis für den Frieden

(mit Dossier 89: Verifikation nuklearer Abrüstung)

3/19 Hybrider Krieg?

4/19 Ästhetik im Konflikt

1/20 Atomwaffen – Schrecken ohne Ende?

vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik

#228 Wohnen als soziales Grundrecht

#229 Sterbehilfe

#230 30 Jahre Deutsch-Deutsche Wiedervereinigung

#231 Drei Jahre Praxiserfahrung – Evaluation der DSGVO

#232 Berliner Gespräche – Staat, Religion und Weltanschauung

#233 Informationsfreiheit

DANA – Datenschutz-Nachrichten

1/19 Social Media

2/19 Ein Jahr DSGVO – ein Résumé

3/19 Real Time Bidding

4/19 Minderjährigen(daten)schutz

Das FIfF-Büro

Geschäftsstelle FIfF e. V.

Ingrid Schlagheck (Geschäftsführung)

Philip Love

Goetheplatz 4, D-28203 Bremen

Tel.: (0421) 33 65 92 55, Fax: (0421) 33 65 92 56

E-Mail: fiff@fiff.de

Die Bürozeiten finden Sie unter www.fiff.de

Bankverbindung

Bank für Sozialwirtschaft (BFS) Köln

Spendenkonto:

IBAN: DE79 3702 0500 0001 3828 03

BIC: BFSWDE33XXX

Kontakt zur Redaktion der FIfF-Kommunikation:

redaktion@fiff.de

Schluss F...I...f...F...

TO PROVE YOU'RE A HUMAN,
CLICK ON ALL THE PHOTOS
THAT SHOW PLACES YOU
WOULD RUN FOR SHELTER
DURING A ROBOT UPRISING.



Quelle: <https://xkcd.com/2228>, Randall Munroe, CC BY-NC 2.5

Geeignete Texte für den SchlussFfF bitte mit Quellenangabe an redaktion@fiff.de senden.