H 7625

FIfF Kommunikation

Zeitschrift für Informatik und Gesellschaft

40. Jahrgang 2023 Einzelpreis: 7 EUR

1/2023 – März 2023

ISSN 0938-3476

• Weizenbaum-Studienpreise • Cyberpeace • Weizenbaum-Preis an Julian Assange •

FIfF Kommunikation

Zeitschrift für Informatik und Gesellschaft

Titelbild: *Lichtinstallation von Stephan und Benks, Foto von Alexander Heim.*

Inhalt

Ausgabe 1/2023

Editorial

Frieden – das ist seit unserer Gründung programmatischer Namensbestandteil und bis heute eines der Kernthemen des FIfF. Dies gilt um so mehr, als dieser Frieden, dessen wir uns jahrelang sicher wähnten, heute wieder akut bedroht ist, angesichts des Krieges in der Ukraine. Dieser Krieg – neben den unmittelbaren Auswirkungen und dem großen Leid, das er über die Bevölkerung der Ukraine bringt – wird wohl auch langfristige Konsequenzen für die europäische Sicherheitsarchitektur und das internationale Zusammenleben haben.

Das Thema unserer FIfF-Konferenz 2022 war bereits vor dem Angriff Russlands geplant: *make install PEACE* war ihr Motto, und sie sollte, unabhängig von tagespolitischen Aspekten, die Frage nach den ganz grundsätzlichen und systemischen Bedingungen für Frieden stellen – einen Frieden, der über die Abwesenheit von offener Gewalt hinaus geht. In der Einleitung dazu heißt es:

> *Die Konferenz sollte zur Diskussion anregen und Argumente beitragen, welche Weichen gestellt und welche Dinge getan werden müssen, damit Kriege und Konflikte in zwei, fünf oder auch fünfzehn Jahren nicht wieder – scheinbar – überraschend passieren. Vielmehr wollen wir dringlich der Frage nachgehen, welchen Weg wir zu einer friedvollen Welt einschlagen müssen, ausgehend vom Hier und Jetzt. Wie kann dieser Weg begangen werden? Wir wollen erörtern, welche Maßnahmen konkret befördert werden müssen, was wir kurz-, mittel- und langfristig machen müssen und wollen, um dauerhaft friedvolle und gewaltfreie Gesellschaften zu ermöglichen.*

Diese Themen wurden in mehreren Vorträgen und Workshops entfaltet, die in dieser Ausgabe der FIfF-Kommunikation dokumentiert sind. Eine Einleitung in den Schwerpunkt mit einem Überblick über die darin enthaltenen Beiträge gibt das Schwerpunkteditorial von pau, Rainer Rehak, Daniel Guagnin und Gilbert Assaf. Die Archenhold-Sternwarte in Berlin-Treptow gab der Konferenz einen attraktiven und angemessenen Rahmen.

Einer der Höhepunkte der Konferenz war die Verleihung des Weizenbaum-Preises für Frieden und gesellschaftliche Verantwortung an den politischen Gefangenen Julian Assange, für engagierten Journalismus, umgedeutet zum „Verrat", an den politischen Gefangenen Julian Assange, der immer noch von Auslieferung an die USA und dort von absurd hohen Strafen für seine Arbeit bedroht ist. In der Laudatio betonte Rainer Rehak für das FIfF:

> *This year we want to honor Julian Assange with this Weizenbaum Award for Peace and Societal Responsibility. For his bravery in fighting for global justice and for state accountability, against war crimes, against state lies, against power misconduct, and against the use of torture. His creative use of technology helped to invent a new kind of investigative journalism in co-founding Wikileaks, continuously holding up journalistic standards, and for his merits and endurance.*

Julians Frau, Stella Assange, war über Video bei uns zu Gast, um den Preis symbolisch entgegenzunehmen. Sie bekräftigte in ihrer Dankesrede:

> *And so Julian brought his knowledge of cryptography, understanding of communications on the internet, and the internet's architecture into journalism. He made an enormous controversial contribution not just to how journalism was done but also to bringing the full potential of information as a tool for accountability.*

Wir dokumentieren die Laudatio für die Preisverleihung und die Dankesrede. **Erneut appellieren wir an die Bundesregierung, sich für die Freilassung von Julian Assange einzusetzen und ihm in Deutschland politisches Asyl zu ermöglichen.**

Bereits Tradition hat der Weizenbaum-Studienpreis, den wir auch dieses Jahr an vier Preisträgerinnen und Preisträger verliehen haben. Die diesjährigen Themen erstrecken sich über erklärbare Künstliche Intelligenz, privatheitswahrende Überwachung, Datafizierung und sich daraus ergebende Gesellschaftbilder und die Wahrnehmung von Verantwortung in der Frühzeit der Digitalisierung. Wir gratulieren herzlich; die Laudationes und die Beiträge der Preisträger:innen sind in dieser Ausgabe enthalten.

Seit ca. zehn Jahren ist die Kampagne *Cyberpeace* fester Bestandteil der FIfF-Arbeit. Ein Workshop bei der FIfF-Konferenz fragte nach der Zukunft dieser Kampagne und plante die weiteren Schritte. Die Stellungnahmen der Workshop-Teilnehmer:innen sind im Rahmen unserer regelmäßigen Cyberpeace-Kolumne dokumentiert.

Erfreuliches – oder eher Trauriges? – gibt es aus Karlsruhe zu berichten: Erneut stellte das Bundesverfassungsgericht die Verfassungswidrigkeit von Überwachungsgesetzen fest. Diesmal handelte es sich um die Gesetze zur automatisierten Datenanalyse in Hessen und Hamburg, die insbesondere in Hessen durch die Analyseplattform *HessenData* auf Basis der Software des US-amerikanischen Unternehmens *Palantir* umgesetzt wurde. Die gesetzlichen Regelungen müssen nun überarbeitet werden – dabei wird zu prüfen sein, ob die durch das Bundesverfassungsgericht formulierten Anforderungen dann ausreichend berücksichtigt werden.

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

Stefan Hügel
für die Redaktion

Der Brief

„Europa der Verteidigung und der Rüstung“

Liebe Freundinnen und Freunde des FIfF, liebe Mitglieder,

in diesen Tagen jährt sich der russische Überfall auf die Ukraine und der Beginn des dadurch ausgelösten Krieges zum ersten Mal – und es ist kein Ende abzusehen. Man kann es wohl nicht genug betonen: Es besteht kein Zweifel über den Aggressor, und dass die Ukraine unserer Unterstützung und Solidarität bedarf. Dieser Krieg muss so schnell wie möglich enden, und der Schlüssel dafür liegt in erster Linie bei der Russischen Föderation und Präsident Putin.

Doch wie kann es weitergehen, wenn die Aggression anhält? Wie sieht sinnvolle Solidarität aus? Darüber ist in den deutschen Leit- und sozialen Medien ein heftiger Streit entbrannt. Verhandlungen oder Waffenlieferungen – das scheinen grob vereinfacht die einzigen Handlungsoptionen zu sein. Auch wenn Deutschland nicht direkt an dem Konflikt beteiligt ist, wird diese Debatte mit harten Bandagen geführt: „Kriegstreiber!“[1], so rufen die Einen, „Friedensschwurbler!“[2] erwidern die Anderen.[3]

Wir glauben, dass sich alle am Diskurs beteiligten (relevanten) Akteure ein Ende dieses Krieges wünschen und dass niemand ein Interesse daran hat, dass Aggression belohnt wird. Worum geht es also? Bringt es uns weiter, wenn wir Vertreter:innen einer anderen Meinung stets die finstersten Motive unterstellen?

Letztlich geht es doch eher um die Frage nach dem „Wie?“: Wie kann das Sterben beendet und gleichzeitig dafür gesorgt werden, dass die Ukraine nicht unter diktatorische Fremdherrschaft gerät? Was müssen wir vom Einen preisgeben, um das Andere zu erreichen? Letztlich: Dürfen „wir“ über das Schicksal der Ukraine entscheiden? Haben „wir“ – als Waffenlieferanten – eine Mitverantwortung für den Fortgang dieses Krieges?[4] Wer entscheidet letztlich überhaupt, wer eigentlich ist „die Ukraine“? Präsident Selenskyj oder die ukrainische Bevölkerung, die unter den Folgen dieses Krieges leidet? Oder kommt das auf dasselbe heraus? Letztlich werden Kriege immer durch Eliten geführt und durch die Bevölkerung verloren.

Heftig debattiert wird gerade über das *Manifest für den Frieden*[5], das durch die Politikerinnen und Publizistinnen Alice Schwarzer und Sahra Wagenknecht initiiert wurde. Bei *change.org* wurde dieses Manifest von inzwischen über 700.000 Menschen unterzeichnet.[6] Wenn so viele Menschen eine Idee mittragen, ist ein näherer Blick nötig.

Zusammengefasst bezweifeln die Initiatorinnen, dass ein militärischer Sieg der Ukraine möglich ist, und fordern zu Verhandlungen auf – auch um den Preis für die Ukraine nachteiliger Kompromisse. Sie lassen aber auch keinen Zweifel daran, wer der Verursacher des Krieges ist und was seine Folgen sind:

> *„Über 200.000 Soldaten und 50.000 Zivilisten wurden bisher getötet. […] Wenn die Kämpfe so weitergehen, ist die Ukraine bald ein entvölkertes, zerstörtes Land. […] Die von Russland brutal überfallene ukrainische Bevölkerung braucht unsere Solidarität. Aber was wäre jetzt solidarisch? Wie lange noch soll auf dem Schlachtfeld Ukraine gekämpft und gestorben werden?“*

Abschließend fordern sie den Bundeskanzler auf, *„[…] die Eskalation der Waffenlieferungen zu stoppen.“* (Nicht die Waffenlieferungen – deren Eskalation.[7])

So weit, so konsensfähig; die Heftigkeit vieler Debattenbeiträge – teilweise mit *Schaum vor dem Mund* – ist dennoch bemerkenswert. Wollen wir jedoch vorankommen, müssen beide Seiten Fragen konkret beantworten: Etwa, wie sie sich eine konkrete Lösung des Konflikts vorstellen und was für sie überhaupt als „Lösung“ zählt.

- Die Verfechter:innen von immer mehr Waffenlieferungen müssen erklären, wie ein militärischer „Sieg“ der Ukraine gegen Russland konkret aussehen würde, wann er aus militärischer und politischer Sicht überhaupt denkbar ist, ob es eine Obergrenze weiterer Waffenlieferungen gibt und wie diese festgelegt wird, welche Konsequenzen dies für die Ukraine und ihre Bevölkerung hätte und was danach mit den Waffen dort und den Waffenfabriken hier passieren soll?

- Aber auch die Verfechter:innen von weniger Waffenlieferungen müssen Detailfragen beantworten: Wie viel Waffenlieferungen sind „weniger“ und müssten es nicht konsequenterweise dann „keine“ sein? Wie könnten Verhandlungslösungen genau aussehen? Welche Zugeständnisse müsste die Ukraine in Kauf nehmen und wie kann die Ukraine zu diesen Zugeständnissen bewegt werden? Warum sollte Putin überhaupt mit einer schwachen Ukraine verhandeln und wie friedlich wird das Leben der ukrainischen Bevölkerung in den dann russischen Gebieten aussehen?

Eines ist jedoch klar: Diese Debatten müssen auf empirisch korrekten Grundlagen geführt werden, dazu gehört die Tatsache, dass Verhandlungen bereits auf diversen diplomatischen Kanälen stattfinden (aber die Parteien sich nicht einigen können)[8], dass Atommächte historisch schon vielfach Kriege verloren haben (siehe Vietnam oder Afghanistan), dass Verhandlungen in Kriegen stets nur zwischen militärisch gleichstarken Akteuren stattfinden, dass nach UN-Charta allein die Ukraine als souveräner Staat über ihr Vorgehen entscheidet[9] oder dass nach Erkenntnissen der Vereinten Nationen[10] nur die russische Armee systematisch foltert, entführt und vergewaltigt. Allein auf solch einer Faktenbasis kann politisch diskutiert werden.

Doch über die tagespolitische Frage hinaus, wie auf den Krieg in der Ukraine reagiert werden soll, stellt sich die Frage nach der langfristigen Ausrichtung der Sicherheitspolitik. Bereits kurz nach dem Einmarsch Russlands in der Ukraine beschloss der Deutsche Bundestag unter großem Jubel[11] ein „Sondervermögen“ von 100 Milliarden Euro für die Bundeswehr – mit Verfas-

sungsrang (!)[12] Das Ziel, 2 % des BIP für Rüstung auszugeben, lange Zeit in der Diskussion, scheint inzwischen unstrittig; einige Mitglieder der NATO fordern inzwischen offenbar, es als Mindestwert zu setzen.[13]

Auf der Münchener „Sicherheitskonferenz" im Februar 2023 erklärte Bundeskanzler Scholz:

> *„Gemeinsam mit Frankreich und Spanien entwickeln wir das künftige Future Combat Air System, mit Frankreich zudem das Main Ground Combat System. Auch bei der gemeinsamen Entwicklung europäischer Fähigkeiten kommen wir voran. Dafür steht die von Deutschland initiierte European Sky Shield Initiative zur Stärkung Europas Luftverteidigung im Rahmen der NATO.* ***Das sind Schritte hin zu einem Europa der Verteidigung und Rüstung[14]****, wie ich es letztes Jahr an der Prager Karlsuniversität skizziert habe."*[15]

Ist das die Vision der deutschen Bundesregierung für Europa? Ist die Zeit des *Friedensprojekts* Europäische Union zu Ende? Bereits vorher wurde der Frieden nach innen durch eine massive Abschottung nach außen erkauft. Wollen wir eine zunehmende Militarisierung der europäischen Politik zulassen? Was können wir dafür tun, dass es nicht dazu kommt?

Der Philosoph Olaf Müller[16] weist darauf hin, dass auch alternative, pazifistische Handlungswege beschritten werden können – andere Autor:innen pflichten ihm bei.[17] Pazifismus und Antimilitarismus bedeuten nicht, auf einer Wiese zu sitzen und Gänseblümchen zu pflücken – sie sind (harte) gesellschaftliche Arbeit, die auch konsequent – und vorsorglich – angegangen (und finanziert) werden muss. Sie umfasst gesellschaftliche Fragen, technische Fragen[18] und nicht zuletzt auch wirtschaftlich-geostrategische Fragen.[19] Hat ein bewaffneter Konflikt bereits begonnen, ist es dafür freilich zu spät.

Wir müssen pazifistische Gesellschaftsentwürfe weit im Vorfeld möglicher Konflikte erarbeiten, global angehen und vorziehen, wo immer das möglich ist. Nicht nur das Militär muss finanziert werden, sondern auch der Frieden.

Mit FIfFigen Grüßen
Stefan Hügel & Rainer Rehak

Anmerkungen

1 *Stephan Hebel (2022) „Kriegstreiber" vs. „Putin-Versteher": Polarisierte Debatte hilft der Ukraine nicht, Frankfurter Rundschau, 14.06.2022, https://www.fr.de/meinung/kriegstreiber-vs-putin-versteher-die-aufgeheizte-debatte-fuehrt-zu-keiner-loesung-fuer-die-ukraine-91610937.html*

2 *Sascha Lobo (2023) Die Friedensschwurbler wollen hauptsächlich Frieden für sich selbst, Spiegel Online, 22.02.2023, https://www.spiegel.de/netzwelt/netzpolitik/ukrainekrieg-die-friedensschwurbler-wollen-hauptsaechlich-frieden-fuer-sich-selbst-kolumne-von-sascha-lobo-a-1fffb0db-55f3-414e-a457-a596c757f957. Sascha Lobo haben wir auch weitere Kleinodien der politischen Auseinandersetzung zu verdanken, wie „Lumpenpazifist": Sascha Lobo (2022) Der deutsche Lumpen-Pazifismus, Spiegel Online, 20.04.2022, https://www.spiegel.de/netzwelt/netzpolitik/ukraine-krieg-der-deutsche-lumpen-pazifismus-kolumne-a-77ea2788-e80f-4a51-838f-591843da8356*

3 *Kritisch zur Debattenkultur auch Sabine Rennefanz (2023) In Verteidigung von Schwarzer und Wagenknecht, Spiegel Online, 23.02.2023, https://www.spiegel.de/politik/deutschland/debattenkultur-in-verteidigung-von-schwarzer-und-wagenknecht-a-0e11c924-81db-4883-bfb9-ce4655f2ce52*

4 *Dazu Jürgen Habermas (2023) Ein Plädoyer für Verhandlungen. Süddeutsche Zeitung, 14.02.2023, https://www.sueddeutsche.de/projekte/artikel/kultur/juergen-habermas-ukraine-sz-verhandlungen-e159105/?reduced=true*

5 *https://www.change.org/p/manifest-für-frieden?algorithm=promoted&source_location=search&grid_position=1&pt=AVBldGl0aW9uADTzHQIAAAAAZARoYDek0bA1MjdkOTdiNg%3D%3D*

6 *Wir haben das „Manifest" nicht unterzeichnet und haben es auch nicht vor. Uns ist auch bewusst, dass die Protagonistinnen vermehrt durch – sagen wir mal – kontroverse Aussagen aufgefallen sind. Das ist offenbar manchen schon genug, sie als diskreditiert anzusehen.*

7 *Offensichtlich wird der Umfang der Unterstützung immer mehr ausgeweitet. Erst ging es um Schützenpanzer, dann um Kampfpanzer, und inzwischen wird offenbar über die Lieferung von Kampfflugzeugen gesprochen: https://www.spiegel.de/politik/deutschland/lettlands-ministerpraesident-krisjanis-karins-im-interview-zur-lieferung-von-kampfjets-an-die-ukraine-a-09897aec-c40c-493a-a316-13a98998b263.*

8 *Eine Übersicht über Verhandlungen zwischen der Ukraine und Russland ist unter https://de.wikipedia.org/wiki/Russisch-ukrainische_Friedensverhandlungen_seit_2022 zu finden.*

9 *Umfrage zur Stimmung in der Ukraine: Mehrheit würde trotz Atomschlag weiterkämpfen, https://www.merkur.de/politik/ukraine-krieg-russland-umfrage-stimmung-bevoelkerung-ergebnis-atomwaffen-frieden-voraussetzungen-92073261.html. Habermas (a. a. O.) sieht hier aber auch eine Mitverantwortung der Waffen liefernden Staaten.*

10 *UN Report on the Human Rights situation in Ukraine, https://ukraine.un.org/en/201055-report-human-rights-situation-ukraine*

11 *Jakob Augstein: Gigantisches Rüstungspaket von Olaf Scholz ist gefährlicher Irrweg, der Freitag 9/2022, https://www.freitag.de/autoren/jaugstein/gigantisches-ruestungspaket-ist-gefaehrlicher-irrweg*

12 *Artikel 87a (1a) GG, http://www.gesetze-im-internet.de/gg/art_87a.html*

13 *Zwei-Prozent-Ziel als Mindestwert? tagesschau.de, 03.01.2023, https://www.tagesschau.de/ausland/europa/nato-verteidigung-ausgaben-stoltenberg-101.html*

14 *Hervorhebung durch d. Red.*

15 *Rede des Bundeskanzlers Olaf Scholz bei der Münchener Sicherheitskonferenz 2023. https://www.bundeskanzler.de/bk-de/aktuelles/rede-von-bundeskanzler-scholz-anlaesslich-der-munich-security-conference-am-17-februar-2023-in-muenchen-2166452*

16 *Olaf Müller (2023) Pazifismus. Eine Verteidigung, Stuttgart: Reclam. Eine Rezension von Sabine Jaberg findet sich in Wissenschaft & Frieden 1/2023, S. 64-65*

17 *Z. B. Bund für soziale Verteidigung, http://soziale-verteidigung.de, Women's International League for Peace and Freedom (wilpf) https://www.wilpf.org/focus-countries/ukraine/ oder Nele Pollatschek (2022) Der Krieg und die Friedensbewegung – Lob des Pazifismus, Süddeutsche Zeitung, 28.09.2022, https://www.sueddeutsche.de/kultur/krieg-pazifismus-ukraine-friedensbewegung-1.5665178?reduced=true*

18 *make install PEACE – Impulse für den Frieden, https://2022.fiffkon.de/*

19 *Vergleich mit Ukraine-Krieg: Taiwan warnt vor China und Russland, 26.08.2022, https://www.zdf.de/nachrichten/politik/taiwan-china-russland-weltordnung-100.html*

Hans-Jörg Kreowski, Aaron Lye und Margita Zallmann

Cyberpeace – Für Frieden, Freiheit und eine lebenswerte Welt

Diese Rubrik besteht aus vier Teilen. Der erste Beitrag bezieht sich auf die Diskussion, wie es mit der Cyberpeace-Kampagne weitergehen soll. Im zweiten Beitrag setzen sich Birgit und Michael Ahlmann mit einem Vortrag über Das zivilisatorische Hexagon – eine soziologische Bestandsaufnahme *von Josua Schneider auf der FIfF-Konferenz auseinander. Den Schluss bilden eine Leseempfehlung für eine IMI-Analyse zum Future Combat Air System (FCAS) und eine Seh- und Hörempfehlung für einen Videomitschnitt von einem Online-Hearing zu aktuellen Entwicklungen bei militärischen Drohnen.*

Teil 1: Hat die Cyberpeace-Kampagne eine Zukunft?

Die Cyberpeace-Kampagne startete vor knapp zehn Jahren. Sie war damals als Gegenkonzept zum Cyberkrieg gedacht, der sich in einer umfassenden Ausspähung digitaler Kommunikationsmedien durch Geheimdienste, Polizei und Militär und in den weltweiten Anstrengungen zur Aufrüstung des Cyberraums für die Durchführung von Cyberangriffen manifestierte. Die Cyberkriegsaktivitäten vieler Staaten der Welt reichen inzwischen von Desinformation und Propaganda über das Lahmlegen einzelner Computersysteme und das Abschöpfen von Informationen bis zur massiven Zerstörung technischer Einrichtungen und kritischer Infrastrukturen.

In der vorigen *FIfF-Kommunikation* wurde bereits kurz über den Cyberpeace-Workshop auf der FIfF-Konferenz *make install PEACE – Impulse für den Frieden* im Oktober 2022 berichtet. Unter den 13 Teilnehmer:innen bestand recht einhellig die Auffassung, dass der Cyberpeace-Kampagne neuer Schwung verliehen werden sollte. Nach zwei oder drei Online-Meetings (ein Meeting hat bereits im Dezember stattgefunden) soll insbesondere im April oder Mai 2023 eine Präsenzveranstaltung durchgeführt werden, auf der die Fortführung der Kampagne in Form und Inhalt besprochen und geplant werden soll. Dieses Treffen wird offen sein für alle Interessierten. Als ein Schritt zur inhaltlichen Vorbereitung sind hier einige kurze Stellungnahmen zusammengestellt, die so oder so ähnlich auf dem Workshop vorgetragen wurden. Das ergibt ein Spektrum an Vorstellungen, wie die Cyberpeace-Kampagne künftig inhaltlich und mit welchen Aktionsformen ausgestaltet werden kann. Dem geplanten Präsenztreffen wird es vorbehalten sein, zu fokussieren, zu präzisieren und zu detaillieren.

Wer sich beteiligen oder zumindest informiert werden möchte, schicke uns bitte eine Nachricht an *kreo@fiff.de* oder *margita.zallmann@t-online.de*. Es folgen die kurzen Stellungnahmen in alphabetischer Ordnung der Autor:innen.

Hans-Jörg Kreowski: Schon vor der Gründung des FIfF 1984 und erst recht seitdem hat mich die unheilvolle Verquickung der Informatik mit der Kriegsmaschinerie beschämt und beschäftigt. Deshalb habe ich mich auch von Anfang an für die Cyberpeace-Kampagne eingesetzt und geholfen, über die Gefahren des Cyberkriegs aufzuklären.

Als in letzter Zeit die Cyberpeace-Kampagne nicht zuletzt auch durch die Corona-Krise etwas ins Stocken geraten ist, habe ich für einen neuen Anlauf unter dem Motto *Cyberpeace – für Frieden, Freiheit und eine lebenswerte Welt* plädiert. Denn die Bedrohung durch Cyberangriffe – also insbesondere durch Ausnutzen von Schwachstellen und Sicherheitslücken in Soft- und Hardware – ist eher noch gewachsen; sie unterminiert einerseits zivile Freiheitsrechte und erhöht die Kriegsgefahr, so dass Frieden und Freiheit bedroht sind. Da aber die Informatik weit über den fundamentalen Beitrag zu den Cyberkriegstechnologien hinaus maßgeblich zur weiteren Entwicklung von Waffensystemen und Systemen zur Kriegsführung beiträgt, halte ich es für sinnvoll, dass die Cyberpeace-Kampagne alle Aspekte von Rüstung und Informatik in den Blick nimmt. Ob neben der mit Hilfe der Informatik betriebenen weltweiten Rüstungsspirale und neben der dadurch verursachten Bedrohung des Friedens auch die zweite bedrohliche globale Krise in Form des menschengemachten Klimawandels und der Naturausbeutung Gegenstand der Cyberpeace-Kampagne sein sollte, wäre zu überlegen.

Aaron Lye: Selbstverständlich gibt es viele Bereiche, in denen Informatik eine wesentliche Rolle spielt und Abertausende von Menschen durch IT-gestützte Systeme den Tod finden. Die Informatik ist aus heutigen Kriegen nicht wegzudenken und auch für das Morden an den Grenzen sind informationstechnische Grenzüberwachungssysteme wesentlich. Die Cyberpeace-Kampagne unter das Motto *Frieden, Freiheit und eine lebenswerte Welt* zu stellen und damit den ursprünglichen Fokus zu weiten, war sicher sinnvoll. Beispielsweise um auch die ökologische Dimension zu fassen und die bevorstehende Klimakatastrophe möglichst noch abzuwenden. Durch die offene Formulierung birgt das Motto aber auch die Gefahr der Beliebigkeit und Zerfaserung, so dass am Ende aufgrund der vielen zu bearbeitenden Themen dann doch nichts gemacht wird.

Christoph Marischka: *Cyberpeace – konkrete Lösung oder die ganze Bäckerei.* Mit wenig Einblick in die Strukturen der bisherigen Cyberpeace-Kampagne habe ich an dem Workshop zu dieser auf der FIfF-Konferenz 2022 teilgenommen. In jedem Fall begrüße ich, wenn die Kampagne weitergeführt und im besten Falle mit neuem Elan ausgeweitet wird. *Im Falle einer thematischen Ausweitung blieb mir jedoch eher unklar, wie die Kampagne zukünftig mit dem FIfF – dessen interne Strukturen ich auch nicht gut kenne – wechselwirken könnte und sollte.*

Ich sehe ganz aktuell die Gefahr, dass mit großer Geschwindigkeit neue Technologien in die Kriegführung eingebunden, erprobt werden und zum Einsatz kommen. Es existieren auf verschiedenen Ebenen Netzwerke, die dies in einer schwierigen (akademischen, diskursiven, geopolitischen) Gesamtsituation kritisch zu beobachten und zu kommentieren versuchen – *da*

könnte ich mir vom FIfF insgesamt auch noch mehr dazu vorstellen. Diese Netzwerke müssen in jedem Fall gestärkt werden. Ob man das am besten durch eine Ausweitung der Cyberpeace-Kampagne erreicht oder damit eher knappe Ressourcen bindet, ist m. E. offen.

Als Außenstehender hatte ich die Cyberpeace-Kampagne zuvor als sehr konkret und fokussiert wahrgenommen auf die Verhinderung von Cyberangriffen durch die Pflicht zur Offenlegung von Sicherheitslücken. In meinen Vorträgen vor friedensbewegtem Publikum nannte ich sie immer wieder gerne und auch für technische Laien nachvollziehbar als ein Beispiel, wie die Pflicht zur Kooperation realisierbar ein Wettrüsten in der Domäne *Cyber* aufhalten und die Sicherheit aller Akteure erhöhen könnte. Solche sehr konkreten Lösungsansätze und Forderungen sind in der zuletzt ja nicht eben von Erfolgsgeschichten geprägten Friedensbewegung durchaus auch von großem Wert.

Jennifer Menninger: Für die Weiterentwicklung der Cyberpeace-Kampagne wünsche ich mir, dass mehr diverse, interdisziplinäre Perspektiven auf die Thematik einbezogen werden. Ich würde sowohl einen intensiveren Austausch mit der nationalen und internationalen Politik befürworten, da dort noch wenig fachspezifisches Wissen vorhanden zu sein scheint, als auch Betroffene von Cyberoperationen ihre Erfahrungen teilen zu lassen. Was bedeutet es zum Beispiel konkret für Einzelpersonen, Unternehmen oder die öffentliche Verwaltung, wenn militärische Operationen im Internet durchgeführt werden? Es ist dabei wichtig, die abstrakte Fachsprache etwas verständlicher zu formulieren, um mehr Menschen zu erreichen, Unterstützung zu erhalten und mehr Dialogformate im Rahmen der Kampagne anbieten zu können. In dem Zusammenhang möchte ich noch auf einen aktuellen Artikel von Veronika Datzer und mir zu dem Thema hinweisen: *Die Notwendigkeit feministischer Cyberpolitik* *(https://fourninesecurity.de/2022/12/08/die-notwendigkeit-feministischer-cyberpolitik).*

Katrin Rehak-Nitsche: Ein wichtiger Erfolgsfaktor von Initiativen ist die Vernetzung mit Partnern. In der Vergangenheit ist das nicht in allen Bereichen praktiziert worden und war häufig unpopulär, da es in einer Kooperation notwendig ist, Wissen zu offenbaren, Kompromisse zu schließen und gegebenenfalls den Erfolg zu teilen. Allerdings sind die Probleme, die heute vor der Tür stehen, nahezu allesamt so groß und komplex, dass sie nicht von einer Person, einer Organisation, einem Projekt allein gelöst werden können. Einfach ausgedrückt könnte man sagen: Die Probleme sind wahrlich groß genug für uns alle. Das gilt ebenso für Cyberpeace.

Das Projekt ist selbst recht komplex, denn es vereint Aspekte aus der Friedensbewegung, der kritischen Informatik, klassischem Aktivismus, der Forschung an sich und sicher vieles mehr. Sinnvoll ist es daher, nach Netzwerken und Partnern Ausschau zu halten, die nach ähnlichen Werten arbeiten, einen ähnlichen Weg gehen möchten und – ganz wichtig – die eigenen Ziele teilen. Der Blick kann anfangs gerne breit sein, sowohl regional als auch inhaltlich, im nächsten Schritt ist allerdings eine Fokussierung notwendig. Anknüpfungspunkte gibt es sicher zu Friedensinitiativen, zu Hochschulen, zu Stiftungen, zu Vereinen oder aktivistischen Gruppierungen. Natürlich gehören zu einer Partnerschaft immer mehrere Seiten, das heißt, am Ende müssen alle Partner einen Mehrwert in der Zusammenarbeit sehen. Dieser muss sorgfältig bedacht und herausgearbeitet werden. Kooperation nur der Kooperation wegen ist nicht Sinn der Sache, denn eine Partnerschaft bedeutet auch immer viel Arbeit. Wenn sie passend und gut ist, macht aber nicht nur das Projekt mehr Spaß, sondern es wird auch erfolgreicher.

Jutta Weber: Sie ist Mitglied des FIfF und sprach bei der letzten FIfF-Konferenz in Berlin die Gruppe Cyperpeace bzgl. Möglichkeiten für eine Kooperation an. Gerne würden sie komplexe Fragen KI-gestützter Kriegsführung in Zukunft gemeinsam mit dem Arbeitskreis diskutieren. Den thematischen Rahmen bildet der

> *Forschungsverbund MEHUCO: Meaningful Human Control. Autonome Waffensysteme zwischen Regulation und Reflexion (https://meaningfulhumancontrol.de/)*

Der von 2022 bis 2024 arbeitende BMBF-Forschungsverbund MEHUCO wird von Prof. Dr. Jutta Weber (Mediensoziologie, Institut für Medienwissenschaft, Universität Paderborn) gemeinsam mit Dr. Jens Hälterlein geleitet. Der Verbund beleuchtet kritisch die Implikationen autonomer Waffensysteme (AWS). An dem Projekt sind Wissenschaftler:innen der Universitäten Bonn (Mediengeschichte: PD Christian Ernst, Dr. Thomas Bächle), Hamburg (Kriminologische Sozialforschung: Prof. Susanne Krasmann, Dr. Stefanie Schmidt), Hannover (Jura: Prof. Susanne Beck, Simone Tiedau) und der Hochschule Ostfalia (Informatik: Prof. Reinhard Gerndt, Daniel Gifhorn) beteiligt. Zur Stärkung einer nicht-westlichen Perspektive wird das Projekt *Fellows* aus dem Globalen Süden einladen, um die eigene Arbeit zu reflektieren.

Im Projekt wird u. a. das Ziel verfolgt, ein umfassendes Verständnis der soziokulturellen Dimension von autonomen Waffensystemen zu erarbeiten. Das impliziert u. a., die soziomaterielle Handlungsfähigkeit von AWS und die damit verbundenen Konsequenzen zu verdeutlichen im Rahmen eines komplexen Technikverständnis – jenseits einer verkürzten Debatte, die die Handlungsfähigkeit einseitig Menschen oder Maschinen zuschreibt. Software basiert immer auch auf normativen Setzungen sowie kategorialen Entscheidungen und gibt implizit Handlungsoptionen vor. Zudem bestimmen spezifische Anwendungskontexte, komplexe vernetzte Infrastrukturen und kulturelle Vorstellungen wesentlich die Nutzung von Maschinen und deren Effekte mit.

Kontakt: Prof. Dr. Jutta Weber, Institut für Medienwissenschaften der Universität Paderborn, jutta.weber@upb.de.

Eberhard Zehendner: Ich fand den Titel der FIfF-Konferenz 2022 – *make install PEACE* – gut, passend und wichtig. Da kam das alte Gefühl zurück: Wir alle können, müssen, werden noch intensiver um FRIEDEN ringen! Wann, wenn nicht jetzt? Unser Treffen „hinter dem Mond", um über die Zukunft von CYBERPEACE zu beraten, war für mich ermutigend, kam zum richtigen Zeitpunkt.

CYBERPEACE sollte an das anknüpfen, was schon bisher den Erfolg der Kampagne ausmachte: Konkrete Ausrichtung, Kräfte bündeln, Dauerthema, Sichtbarkeit und auch Spaß daran haben. Dabei aber nicht einfach das wiederholen, was gut lief – jedenfalls nicht NUR das. Noch einen tollen Film zu produzieren,

reicht dafür nicht. In *Cyberpeace statt Cyberwar* – so gut der Slogan ist – steckt mir persönlich noch zu viel „gegen", zu wenig „für". Das ist eben gerade NICHT wie in „Make love, not war". Wie könnte sie denn TATSÄCHLICH aussehen, die lebens- und liebenswerte Welt der Zukunft? Und WIE kommen wir dahin? Was kann das große I in FIfF – die Informatik – dazu beitragen, was ist UNSER Äquivalent zu „Love"?

Das ist alles nicht NEU für das FIfF, ich weiß. Aber haben wir denn tragfähige Antworten auf die drängenden Fragen gefunden, die alten Probleme gelöst? Ich würde mich freuen, wenn die Reaktivierung von CYBERPEACE dazu dienen könnte, hier wieder etwas mehr „Richtung" zu gewinnen, noch konstruktiver zu denken, dem dritten F in FIfF gerecht zu werden.

Birgit Ahlmann und Michael Ahlmann

Teil 2: Das zivilisatorische Hexagon – eine soziologische Bestandsaufnahme

Die FIfF-Konferenz 2022 fand unter dem Titel make install PEACE – Impulse für den Frieden in Berlin statt. Am Abend des 21. Oktober 2022 führte Dr. Josua Schneider (Institut für Soziologie der Bergischen Universität Wuppertal) in einem einleitenden Vortrag die Teilnehmenden in das obige Thema mit dem Modell von Prof. Dieter Senghaas (siehe auch https://de.wikipedia.org/wiki/Dieter_Senghaas) ein. In diesem Wikipedia-Beitrag findet sich auch die folgende Grafik. Wir wollen einige Gedanken und Erinnerungen zu diesem Modell wiedergeben und ergänzen.

Wir betrachten hier nur einzelne Gedanken zu diesen sechs Punkten des Hexagons:

Gewaltmonopol: Durch das staatliche Gewaltmonopol kann es zu einer Entprivatisierung der Gewalt kommen → Konfliktregelung durch Austausch von Argumenten und Diskurs → Wegbrechen des Gewaltmonopols führt zu Annäherung an den Hobbes'schen Naturzustand (s. a. *https://de.wikipedia.org/wiki/Naturzustand* – Krieg alle gegen alle).

Rechtstaatlichkeit: Herausbildung von Rechtsstaatlichkeit → Kontrolle des Gewaltmonopols → Legitimation staatlicher Gewalt und Institution von Konfliktregeln.

Interdependenzen und Affektkontrolle: Funktionale Differenzierungen → moderne Industriegesellschaft → gesellschaftliche Rollenerwartungen verlangen notwendige Maßnahmen: Impuls- und Affektkontrolle sowie Selbstbeherrschung.

Demokratische Partizipation: Demokratisierung des politischen Systems → Forderung nach demokratischer Teilhabe.

Konstruktive Konfliktkultur: Konstruktive Konfliktkultur und -bearbeitung.

Soziale Gerechtigkeit: Konstruktive Konfliktkultur → Chancen- und Verteilungsgerechtigkeit, Teilhabe, Gestaltungsmöglichkeit(en).

Was hat der Begriff Cyberpeace in seinen Varianten mit *make install PEACE* zu tun?

Der Begriff *Cyberpeace* setzt sich aus *Cyber* und *Peace* zusammen. Cyber mit seinen vielen Varianten wird unterschiedlich genutzt. So ist Cyber zwischen „Jugendkultur" und „die von Computern erzeugte virtuelle Scheinwelt betreffend" angesiedelt. Die Begriffe Cyberpeace, Cybercrime, Cybersicherheit und Cyberwar beziehen sich auf die Handlungsmöglichkeiten im Bereich von vernetzten Computern und damit verknüpften technischen Feldern (Verwaltung, Banken, Grundversorgung, Energie, private, betriebliche und staatliche Kommunikation, …) bis hin zur Kriegsführung oder Kriegsvermeidung u. a. mit der Information und Manipulation vielschichtiger Daten.

Cyberwar als Gegenteil von Cyberpeace

Drohneneinsatz ermöglicht Beobachtung, Spionage, Manipulation, Jamming oder Kriegshandlungen, ohne dass *(wo)man-power* vor Ort sein müsste.

Beeinflussung, Manipulation, Fehlinformationen – Beispiele

- Massenbeeinflussung durch Aufrufe über digitale Medien (Trump via Twitter: „Wahlbetrug", Sturm auf das Capitol, ähnlich die Bolsonaro-Familie, Brexit-Kampagne, viele andere weltweit, …).
- Unterwanderung von politischen Gruppen, Hilfsorganisationen u. a. durch Extremist:innen oder religiöse Fanatiker:innen.
- Urheber:innen von Hassmails und Hetzkampagnen gegen Andersdenkende sind durch die Anonymität des Internets davor geschützt, zur Rechenschaft gezogen zu werden. Es droht die Gefahr der Verrohung.
- Verleumdung, Diskriminierung und Schikane über digitale Medien nehmen schon unter Schüler:innen zu und fördern Rücksichtslosigkeit, Intoleranz, Hass und Feigheit.

- Nutzung digitaler Medien zu Erpressung/Vortäuschen von Gefahrensituationen erlaubt es Dieb:innen, Menschen „Geld zu stehlen“ (Oma-Trick) sowie Hacker:innen, Firmen zu erpressen.

- Cyberkriminelle können Datenbanken sperren, Geld von fremden Konten transferieren, Versorgungsstrukturen unterbrechen oder lahmlegen, Infrastrukturen, Flughäfen, Bahnstrecken außer Betrieb nehmen, um Geld zu erpressen oder den Betroffenen und Staaten ihre Macht zu demonstrieren und Betroffenen Schaden zuzufügen ,ohne persönlich in Erscheinung zu treten.

Zum Trump-Beispiel

Gerade der Effekt von Trumps Aufrufen an seine Fans und Kommunikation mit seinen Anhänger:innen zeigt seine manipulative und missbräuchliche Nutzung digitaler Möglichkeiten und deren Akzeptanz bis hin zur Spaltung der US-amerikanischen Bevölkerung.

Herauszufinden, wie das Entstehen solcher Missbräuche und gesellschaftlicher Schäden vermieden/verhindert werden kann, ist ein weites positives Handlungsfeld für Cyberpeace. Dazu gehören auch Konzepte, wie Geschädigte/Verleumdete schnell rehabilitiert werden können. Die gesellschaftliche Spaltung und fehlende Transparenz muss schrittweise abgebaut und kritisches Denken/Verhalten entwickelt und aufgebaut werden.

Soziale Aspekte von Cyberpeace

Die IT (Hard- und Software) mit ihren unterschiedlichen Geräten und Netzen entwickelt sich sehr schnell in verschiedenste Richtungen weiter, die entsprechende Industrie/die Gerätebeschaffung ist sehr kosten- und rohstoffintensiv:

- Dem armen und größten Teil der Bevölkerung der Erde fehlt das notwendige Geld, um mit der ständigen Modernisierung und Weiterentwicklung der Technologie/Technik Schritt zu halten und sich ständig die neuesten Geräte leisten und diese nutzen/anwenden zu können.

- Dies führt zu einer Spaltung der Gesellschaft in Teilhabende und Ausgeschlossene.

- Um dem zu begegnen, fordern wir, Konzepte/Budgets zu entwickeln, bereitzustellen und kurzfristig umzusetzen: Lernplätze mit modernen Geräten und geeigneten Ausbilder:innen, z. B. in Betrieben, kostenfreien Bibliotheken oder Volkshochschulen für alle, geeignete Lernplätze und Geräte an allen Schulen. Das Lernen in der Schule sollte sowohl mit klassischen Methoden als auch mit Unterstützung moderner IT-Systeme erfolgen. Die Internetnetze sind flächendeckend kostenfrei zur Verfügung zu stellen.

- Beispiel 49 €-Ticket: Soweit es nur digital angeboten wird, führt dies zu einer Ausgrenzung armer und/oder alter Menschen, soweit diese keinen Zugriff auf diese IT-Techniken haben.

Schnelle Kommunikation

Eine schnelle Bild- und Ton-Dokumentation von akuten Problemen in der Welt (Beispiel: die aktuelle Kette von Erdbeben in Nordsyrien und der Südtürkei) ist ein großer Fortschritt gegenüber der Zeit, als Fernsehteams oder Korrespondent:innen zuerst zum Problemort vordringen und ihre Nachrichten „zurückbringen mussten“.

Die Zweischneidigkeit schneller Kommunikation zeigt sich im Ukraine-Krieg durch die sehr direkte zeitnahe Lagebild-Aufklärung des gesamten Kriegsgebietes durch britische und US-amerikanische Geheimdienste zu Gunsten der ukrainischen Militärführung sowie die Starlink-Kommunikation durch den Unternehmer Elon Musk für die Ukraine (eingeschränkt seit 9. Februar 2023). Die Nutzung von Starlink-Satelliten für militärische Zwecke seit Installation ist nicht unbedingt genehmigt gewesen.

Eine schnelle und nachprüfbare, transparente Informationstechnik ist ein wichtiges Instrument zum Schutz von Umwelt, Natur, Klima und Lebewesen. Dadurch kann ein gesellschaftlicher Zusammenhalt gefördert werden.

Deshalb: Unterstützt unsere Cyberpeace-Kampagne aktiv. Das zivilisatorische Hexagon stellt wichtige Prinzipien für unser Handeln vor, wenden wir es an!

„Was wir heute tun, entscheidet, wie die Welt morgen aussieht.“ (frei nach Terra X)

Teil 3: IMI-Analyse 2023/04 zum Future Combat Air System (FCAS)

Kürzlich erschien eine empfehlenswerte Studie von Christoph Marischka mit dem Titel *FCAS: Ansatzpunkte für eine Kampagne am Beispiel Stuttgart* (IMI-Analyse 2023/04). In der Einleitung heißt es:

„Nicht nur wegen der Kosten, sondern auch wegen der zu erwartenden technischen und ethischen Dammbrüche sowie der mit dem FCAS verbundenen Eskalationsdynamik im internationalen Wettbewerb und Rüstungswettlauf ist es deshalb begrüßenswert, dass verschiedene Organisationen in Deutschland aktuell eine Kampagne gegen das Großprojekt vorbereiten. Sie werden dabei vor der Herausforderung stehen, dass es sich bei FCAS um ein kompliziertes und relativ abstraktes Großprojekt handelt, das sich – trotz der bereits jetzt verausgabten Milliardenbeträge – zunächst nur in Planungsbüros, hoch-spezialisierten Komponenten in ebensolchen Werkshallen und wenigen Demonstratoren materialisieren wird. Das bemannte Kampfflugzeug der nächsten Generation als Kernelement soll beispielsweise erst ab 2040 einsatzbereit sein.

Um die mindestens bis dahin relativ abstrakte Entwicklung des FCAS trotzdem sichtbar zu machen, wird deshalb vorgeschlagen, das dahinter stehende Netzwerk von Unternehmen und Institutionen herauszuarbeiten und zwar an einem Ort, der bislang und absehbar keine zentrale Rolle bei der Entwicklung des FCAS spielen wird. Trotzdem lässt sich auch an Stuttgart deutlich machen, wie umfassend das Rüstungsprojekt und die damit verbundenen technologischen Entwicklungen sind und wo es deshalb auch überall Ansatzpunkte für die kommende Kampagne gibt."

Anschließend werden verschiedene Unternehmen und Institute im Großraum Stuttgart benannt, welche im Mega-Rüstungsprojekt eine Rolle spielen können. Nicht alle Unternehmen und vor allem Forschungsinstitute, die genannt wurden, sind bislang konkret in FCAS eingebunden, und bei einigen mag das zumindest an den konkreten Standorten um Stuttgart auch eher unwahrscheinlich bleiben. Trotzdem ist auch hier auf die Gefahr hinzuweisen, dass die gewaltigen, für FCAS in Aussicht gestellten Ressourcen auch ihre Forschungsbereiche, Studiengänge oder Unternehmen transformieren und in die Rüstung einbinden könnten – und sollen.

Die Situation im Großraum Stuttgart ist auf andere Rüstungsstandorte der Luft- und Raumfahrt übertragbar. Protest ist vielerorts konkret möglich.

Teil 4: Aktuelle Entwicklungen bei militärischen Drohnen

Am Mittwoch, 25. Januar 2023, organisierte der AK gegen bewaffnete Drohnen ein Online-Hearing, um die aktuellen Entwicklungen im Bereich *Kampfdrohnen* zu beleuchten und am Beispiel von Afrika, der Ukraine und der Türkei die Gefahren bewaffneter Drohnen genauer zu diskutieren. In den aktuellen Kriegen setzen die Militärs Drohnen mit hochwertiger Elektronik und tödlicher Munition ein. Damit könnte sich der Verlauf künftiger Konflikte dramatisch verändern. Diese Waffen treffen nicht nur den Kriegsgegner, sondern terrorisieren auch die Zivilbevölkerung.

Der Hauptteil der Veranstaltung umfasste vier Kurzreferate. Hans-Jörg Kreowski referierte für das FIfF zum Thema *Aktuelle Entwicklungen bei Kampfdrohnen*. Richtsje Kurpershoek von *Pax for Peace* beleuchtete den Einsatz von Kampfdrohnen in Afrika. Christoph Marischka von der Informationsstelle Militarisierung referierte zu Drohnen im Ukraine-Krieg (und machte insbesondere Perspektiven auf). Der letzte Beitrag war von Matthias Monroy von CILIP u. a. zum Thema *Drohnenmacht Türkei*.

Die geschnittene Aufzeichnung kann bei media.ccc *(https://media.ccc.de/v/kriegundki-56060-aktuelle-entwicklungen)* und bei vimeo *(https://vimeo.com/manage/videos/794271535)* angeschaut werden.

Stefan Hügel

Regelungen in Hamburg und Hessen zur automatisierten Datenanalyse verfassungswidrig

Das Bundesverfassungsgericht hat am 16. Februar 2023 sein Urteil zur automatisierten Datenanalyse (1 BvR 1547/19, 1 BvR 2634/20) vorgelegt. Darin urteilt es, dass § 25a Abs. 1 Alt. 1 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) und § 49 Abs. 1 Alt. 1 des Hamburgischen Gesetzes über die Datenverarbeitung der Polizei (HmbPolDVG) verfassungswidrig sind. Nach dem Urteil des Gerichts verstoßen sie gegen die informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts, die sich aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG ergibt. Durch die Bestimmungen sollte die Rechtsgrundlage geschaffen werden, dass Polizeibehörden gespeicherte personenbezogene Daten mittels automatisierter Anwendung im Rahmen einer Datenanalyse (Hessen) oder einer Datenauswertung (Hamburg) weiter verarbeiten können. Für diese Auswertung wird durch die hessische Polizei die Software den US-amerikanischen Unternehmens Palantir eingesetzt, die die Basis der Analyseplattform „HessenData" bildet. In Hamburg wird bisher kein Gebrauch von der Regelung gemacht.

Franz-Josef Hanke, Vorsitzender des Ortsverbands Marburg der Humanistischen Union und Journalist, war einer der sieben Beschwerdeführer. Hanke erläutert dazu: „Aufgrund meiner beruflichen Kontakte hätte ich leicht selbst zum Gegenstand polizeilicher Ermittlungen werden können, ohne dafür selbst einen Anlass geboten zu haben."

Durch das Urteil wird gefährlichen Entwicklungen wie Rasterfahndung und Predictive Policing durch intransparente und häufig diskriminierende Verfahren der Datenauswertung ein Riegel vorgeschoben. Die beiden weitgehend gleichlautenden Regelungen in § 25a Abs. 1 HSOG und in § 49 Abs. 1 HmbPolDVG schaffen die Rechtsgrundlage dafür, bisher unverbundene, automatisierte Dateien und Datenquellen in Analyseplattformen zu vernetzen und die vorhandenen Datenbestände durch Suchfunktionen systematisch zu erschließen. Durch die vorgesehenen Maßnahmen sind weitgehende Verknüpfungen von Datenbeständen möglich. Dadurch werden Beziehungen zwischen einem großen Spektrum von Personen, Organisationen und sonstigen Objekten möglich und auswertbar. Die in derartiger Analysesoftware genutzten Algorithmen sind dabei häufig nicht nachvollziehbar und können bei ungünstigen Datenkonstellationen zu diskriminierenden Auswertungen – sogenanntem ‚programmiertem Rassismus' führen.

Das Bundesverfassungsgericht hat festgestellt, dass die automatisierte Analyse einen eigenen Eingriff in das Recht zur informationellen Selbstbestimmung darstellt. Dies bedürfe damit auch einer besonderen verfassungsrechtlichen Rechtfertigung. Die Nutzung solcher Analysesoftware für die Polizeiarbeit sei nicht in allen Fällen unzulässig; es fehle im Gesetz aber an einer ausreichenden Eingriffsschwelle für die Anwendung. Aus dem Urteil ergeben sich Maßstäbe für künftige Anwendungsszenarien, die an die Nutzung solcher Verfahren angelegt werden müssen.

Erneut musste das Bundesverfassungsgericht der Gesetzgeberin in den Arm fallen, um ein verfassungswidriges Überwachungsgesetz zu verhindern. Es wird genau zu beobachten sein, ob die Gesetzgeberin die durch das Bundesverfassungsgericht formulierten Anforderungen in neuen Gesetzesvorhaben ausreichend umsetzen wird. Auf jeden Fall ist der 16. Februar 2023 ein guter Tag für den Persönlichkeitsschutz und die Bürgerrechte.

Die Verfassungsbeschwerde wurde von einem Bündnis unterstützt und vorbereitet, an dem gemeinsam mit dem FIfF unter anderem die Gesellschaft für Freiheitsrechte, die Humanistische Union und die Bürgerrechtsorganisation dieDatenschützer Rhein-Main beteiligt waren.

Der Beitrag basiert auf einer Pressemitteilung der Humanistischen Union.

CC BY

Aufruf zur Mitwirkung und Mitgestaltung

FIfF-Konferenz 2023

3. bis 5. November 2023 in Berlin

Liebes FIfF-Mitglied,

seit vielen Jahren stehen die FIfF-Konferenzen unter einem inhaltlich klar formulierten Schwerpunkt und werden von einer Regionalgruppe an ihrem jeweiligen Standort organisiert. Für das Jahr 2023, ein Jahr vor dem 40. Vereinsgeburtstag, haben wir uns etwas ganz Besonderes vorgenommen:

> *Wir möchten gemeinsam mit euch allen in die Zukunft schauen!*

Die Herausforderungen der Informatik werden nur allzu oft hinsichtlich der Gefahren, Risiken, unerfüllbaren Verheißungen und Dystopien der Digitalisierung betrachtet. Doch wie kann das FIfF dazu beitragen, eine kritische Informatik konstruktiv mit einer positiven Ausrichtung zu vereinen?

Gemeinsam wollen wir auf der FIfFKon23 Perspektiven, Zukunftsvisionen, Chancen und Utopien erstrahlen lassen, die eine Inspiration für Umbruch und Aufbruch sein können. Mit welchen Inhalten befassen sich unsere Mitglieder, in welchen Bereichen sind sie aktiv, für welche Themen brennen sie? Welchen Vortrag hast DU schon immer auf der FIfFKon vermisst? Jetzt ist die Gelegenheit, uns alle für dein Thema zu begeistern, Sichtbarkeit und Synergien zu schaffen.

Für den Konferenzrahmen ist bereits gesorgt: vom 3. bis 5. November 2023 sind Räumlichkeiten in der Jugendherberge Berlin-Ostkreuz reserviert, und auch um Veranstaltungstechnik, Streaming und das leibliche Wohl werden sich Vorstand und Geschäftsstelle kümmern.

Wir wünschen uns also v. a. bei der inhaltlichen Planung und Programmgestaltung deine Mitwirkung und erwarten gespannt deine Einreichung. Unterschiedliche Formate sind dabei sehr willkommen, z. B.

- kurze Impulsvorträge,
- Vortrag 20 bis 30 Minuten (wenn gewünscht mit anschließender Q&A),
- andere Art der Präsentation ggf. auch kulturelle / künstlerische Beiträge,
- Planung / aktive Teilnahme an einer Podiumsdiskussion oder deren Moderation,
- Planung einer offenen Diskussion oder deren Moderation,
- Planung eines Workshops.

Bitte schicke deine Vorschläge mit ein paar Zeilen zum intendierten Thema und zu deiner Person bis zum 30. April 2023 an info@fiffkon.de Wir freuen uns sehr auf deine Beiträge,

Dein FIfF-Vorstand

Rainer Rehak

Weizenbaum Award Ceremony for Julian Assange

Laudatio

Dieser Text ist eine Transkription der gesprochenen Laudatio von Rainer Rehak zur Verleihung des Weizenbaum-Preises für Frieden und gesellschaftliche Verantwortung an Julian Assange sowie der Rede von Stella Assange, die den Preis stellvertretend entgegennahm. Zur besseren Lesbarkeit wurden einige Passagen angepasst. Das Originalvideo ist unter https://media.ccc.de/v/fiffkon22-35-weizenbaum-award-ceremony-for-julian-assange verfügbar.

This is a story of bravery, technology, and torture. I am standing here having the honor to represent the Forum Computer Scientists for peace and societal responsibility. As you all might know, founded in 1984 by a group of people, including Prof. Christiane Floyd working on software design focusing on users, not only for tech people, with the needs of users focused. But also founded by Prof. Joseph Weizenbaum, who criticized wrong assumptions about technology, for example, demystifying artificial intelligence (AI) and the automation of humans. He said the "danger is not so much, that computers become more like humans, but that humans become more like computers". Weizenbaum was an outspoken anti-militarist who published texts, that people working in tech should refuse to build military tech, and every single person should refuse. He himself publicly refused to work on electronic weapon parts during the Vietnam war.

He said: "We, as tech people, have a responsibility because we know the technology; we understand it. We all need to have the courage." He had the courage, with many others in the streets back then, to oppose the official narrative of that war.

He said: "One of the great misconceptions is that a single person cannot make a difference and believing this is a self-fulfilling prophecy."

That's why we founded the *Weizenbaum Award for Peace and Societal Responsibility*. For people who fight for a peaceful world, or "world peace," as the UN calls it! For people refusing to use their tech skills for war! For people using their tech skills for peace! For people who take responsibility for their actions and their tech knowledge and don't blindly or conveniently follow any official narrative!

It's for people who bravely make a difference and break the self-fulfilling prophecy mentioned above.

This year we want to honor Julian Assange with this Weizenbaum Award for Peace and Societal Responsibility. For his bravery in fighting for global justice and for state accountability, against war crimes, against state lies, against power misconduct, and against the use of torture. His creative use of technology helped to invent a new kind of investigative journalism in co-founding Wikileaks, continuously holding up journalistic standards, and for his merits and endurance.

But what exactly did Julian Assange do? Well, he initiated and co-founded Wikileaks in 2006, a new investigative media organization. Wikileaks made it possible to anonymously upload leaked documents or videos, e. g., documenting governmental power misuse, using the Tor anonymity network. The idea was to reduce the immense power asymmetry between individuals and groups on the one hand and governmental actors on the other hand. Especially global powers like the US were often involved in or even starting wars. This was one of the main motivations. So as Julian Assange said: "Wikileaks is the reaction to the rampant growth of State secrecy."

How did Wikileaks do it? They checked for the public relevance of the documents provided and applied a harm minimization policy, meaning that they warned the people mentioned, and then they timely published the information. This was a controversial method.

In the year 2009, there were already over 1 million documents available on Wikileaks, which led to the website quickly being blocked in China, North Korea, Israel, Russia, and Turkey. Let's look at what happened there by showing the nature and the examples of those documents that could be found on Wikileaks:

- 2010 was the case of the *Collateral Murder* video, which referred to the killing of journalists in Baghdad/Iraq, by US forces. It was an illegal war based on false information produced by US torture. This incident was denied until this video was released. The video uncovered war crimes denied explicitly by the US before that.

- We had the *Afghan War Diaries* in 2010, showing the real situation on the ground, uncovering many governmental lies, and showing the real face of the war.

- The *Iraq War Logs* 2010 uncovered the knowledge of grave torture of Iraqi security forces after Hussein was defeated, which was also denied by the US. But there was grave torture!

- Then we had the *Cable Gate* in 2011, and maybe interesting for all Germans here, Wikileaks published the secret Toll-Collect contracts.

- There was also some information about the NSA espionage in 2015 on Wikileaks showing that the German chancellor

was being surveilled starting in the 1990s as well as France, Brazil, Japan, and Japanese companies.

- And in 2017, via Wikileaks, we all learned about the US Senate torture report of the CIA, which was published only highly redacted before. But then all seven thousand pages became public. It didn't matter that they renamed the torture "extended interrogation techniques;" it was grave torture! There were black sides, rendition flights, and cooperation of the UK, made possible by the ignorance of other countries. There were black sites in Abu Ghuraib and Guantánamo.

Wikileaks was the source for many media outlets like the New York Times, Guardian, Le Monde, Spiegel Online, and the BIJ – the Bureau of Investigative Journalism. How do they position themselves right now when Julian Assange is on the line directly?

However, no one was ever officially charged for the revelations in publications of Wikileaks. For example exposing torture by US forces: not for the war crimes, not for the torture, not for the lies, not for the warmongering, not for the inaction facing all the injustice. "But now the public knows," as Snowden likes to put it. Everyone can browse the documents, they're still online, and they will be for a long time.

Assange is an excellent example of investigative journalism, press freedom, and critical government work. But on the other hand, he is a horrible example in the eyes of the USA if he can continue his work. So what happened to him after he started his project?

In November 2010, Sweden issued a European arrest warrant for Assange over allegations of sexual misconduct. There were provenly manipulated documents, in this case, arbitrary and changing requirements, how the process should continue. And after Nils Melzer, the UN rapporteur on torture at that time, inquired about more details, there was not even an answer from the Swedish government. The charges, by the way, were later dropped. Assange was facing extradition to Sweden and from there to the US. He took refuge in the embassy of Ecuador in London in 2012 and was subject to illegal bullying, isolation, and, as we know now, even spying. So the attorney-client privilege, essential in court cases, was not given at any point. In 2013, as we now know, Sweden wanted to drop the charges, but the UK pressed Sweden not to do so and keep all the charges up.

Meanwhile, in the US, there was a big political discussion about the possible assassination of Assange. In 2019 Assange's asylum was withdrawn by Ecuador, and he was brought into a UK prison, surprisingly, exactly when Sweden dropped the charges. They said there was not much against him due to the long time that had passed. No other comments were given, although the accusations kept him from traveling freely the whole time.

Well, and right now, what's the situation? The US is demanding the extradition of Assange from the UK based on the US Espionage Act of 1917. Trials under the Espionage Act will be negotiated before a secret military court with no possibility of defending oneself. He is facing 175 years in a US prison, in the country which conducted black sides and invented the term "advanced

Weizenbaum Award for Peace and Societal Responsibility for Julian Assange

interrogation techniques." Currently, he's in Belmarsh prison, and the reason is bail escape. Not paying the bail has never before been the reason for getting into a high-security prison. The extradition is basically granted, but it's still in revision, so the future is still open.

Additionally, he is no longer able to communicate with his lawyers. It is a court case, and according to all independent observers, there's no fair trial. He's in solitary confinement, and he is getting psychologically and physically weaker. "The whole process is torture," says Nils Melzer, then UN rapporteur on torture.

But what is torture? Torture is a cruel, inhumane undignified treatment to break a person, to get information, or to set a public example. Here it is clearly the case that there should be an example being made to all journalists and leakers for that matter, "don't mess with the Empire" is the message. The US cannot reach Snowden, less so right now. Consequently, Assange gets all the wrath. At the same time, Sweden and the UK actively helped the US while other European countries watched quietly, which is outrageous from our point of view.

What's happening right now has effects on three levels.

First, Julian Assange as a person. Individually the torture effects become increasingly serious, and there is a genuine risk of suicide, as doctors say, when they have the chance to visit him.

Second, press freedom, political freedom, and the idea of a constitutional state with the right to a fair trial get thrashed. Such freedoms and principles are precisely necessary for this case against state power. Otherwise, there's no use for such rights. If they don't apply when necessary, they are useless and hollow talk.

Third, the weight of western values in general. Of course, we already see Russia, China, and North Korea, amongst others, say, "well, we imprison our journalists just like you do." And they are basically correct.

To conclude: Julian Assange always knew this could happen, and he still pushed his agenda of transparency, peace, justice, accountability, and responsibility regarding those in power. Therefore, we combine the award ceremony with the following demands: To the UK, we say: Free Assange! To Germany, we say: Take a stance and offer unlimited asylum! To the EU,

we say: act on our values! This is the time to show we actually have any values!

To all of you, we say thank you that you're here! And to Stella Assange, we say thank you! And to Julian Assange, we say thank you for doing what you did!

We are honored that the award is being received by his wife and lawyer, Stella Assange, via an online connection.

And the last thing that's up to me to say is that as long we are all actively paying attention to what's happening, keeping it alive in the media discussions, there might be a slight chance of Julian getting out of this alive! Thanks a lot.

CC BY

Stella Assange

Weizenbaum Award Ceremony for Julian Assange

Acceptance Speech

Thank you! I'd like to thank you for awarding and recognizing Julian for his role as a pioneer and for bringing a revolutionary approach to bringing accountability!

It might be a good idea to think back to when Wikileaks appeared on the stage in the early 2000s. It grew out of a period in which there was an intention by civil society to make government transparent and accountable. These are terms that we no longer use very much. Transparency and government accountability, they've fallen out of vogue with the times. And Wikileaks, as you know, was one of several projects at the time to bring greater accountability to the world, which moved onto the internet. Wikileaks did it in the most successful way, perhaps. There was also the Freedom of Information Act legislation. It was enacted during this time. But Julian combined his knowledge of how the internet worked with the purpose of true investigative journalism. And he understood that the traditional newsrooms were utterly clueless about how communications on the net could unmask sources in a way that conventional journalism didn't have to deal with before. They had their traditional ways of protecting sources, but they had no idea about how to protect sources in the age of emails that were not encrypted and so on.

And so Julian brought his knowledge of cryptography, understanding of communications on the internet, and the internet's architecture into journalism. He made an enormous controversial contribution not just to how journalism was done but also to bringing the full potential of information as a tool for accountability.

With the words of Iraq and Afghanistan, they had been reported by then through embedded journalists who gave a poor and biased understanding of what was happening. So when Wikileaks published *The Afghan War Diaries* or the *Iraq War Logs*, they could give anatomy and really map out the war in all its destruction. Not just when there had been a suicide bomb somewhere in Baghdad, but even individual killings that added up to fifteen thousand civilian deaths that had been unaccounted for until that point and the incredible carnage that those wars meant on the ground. This really changed how the newsrooms were reporting about the war, giving them something to dig their teeth into and changing how those wars were discussed.

Julian has also had the incredible gift of understanding things at scale. One of Julian's most famous quotes now that has been doing the rounds on Twitter is a comment he made about the Afghan War:

> *"The goal was not a successful war. The goal is to have an endless war through which the tax basis of the UK and the US, and other European countries participating in these wars, go into the pockets of the arms manufacturers and the war profiteers."*

This really has resonated to this day. Today, how people have started to understand the drivers of war, and similarly, by exposing those wars, Wikileaks has been a driver for peace, for exposing war crimes, and the true face of war: Hell!

Which is suffered by those who are killed and maimed, and in many cases, their killings and the harm that comes to them are never reported on or known. So it has no consequence for those victims of war. The only thing that approximates some form of justice is the right to truth, and the right to truth is in this day

and age, perhaps … I think everyone's extremely sensitive to the importance of the right to truth, both for the victims and the public in general, because the public has to be, as Julian says, lied into war because they usually don't like war. That's why Wikileaks has been so important and needs to remain important. It needs to be recognized ongoingly. Because what is being done to Julian can't be allowed to continue because he is in this fight between accountability and impunity. Julian's prosecution impunity is ahead, and Julian's freedom will be a victory for accountability, the right to truth, the public's right to know, and ultimately democracy!

So in this context, I'm incredibly thankful for this recognition because Julian has been attacked in so many ways, and the recognition of what has been his life's work, which is to fight for victims and give the world the tools to have accountability. Now, what the world, the public, and the newsrooms do with it, is a different issue. Still, he can put on the public record the reality, not just of war but of the subversion of judicial processes in Germany. For example, the El-Masri case in Italy is similar to when Italy attempted to extradite CIA agents who had conducted a rendition from Italy. And in Spain, where they were trying to bring to trial the US agents responsible for the US military personnel who were responsible for deliberately killing José Couso, a Spanish cameraman, in a hotel in Baghdad. They were aiming right at him, and the US used its political leverage to interfere with that process, so this is a European attempt to bring accountability within the EU. The facts about the political interference were brought to light by Wikileaks Publications.

And one last point: Julian's Freedom matters to Europe! Not just on principle, not just for us who support truth and democracy and want peace in the world, but also because this is an attack on the Europeans' right to know and press freedom. And Julian will fight this till the end! He will fight this until it reaches the European Court of Human Rights! This case will create the jurisprudence that will shape the scope of the press freedom of the right to know, of the right to the truth within the European space!

So, I'd like to thank you all!

I'm sorry this is a bit rushed, but I am very appreciative. Julian is thrilled as well because he remembers you from years ago, and he hopes to be able to come and address you himself before too long.

CC BY

Wissenschaft & Frieden 1/2023

Jenseits der Eskalation

Alternativen zum Umgang mit Bedrohung

Die Bedrohung durch militärische oder ökologische Vernichtung ist allgegenwärtig – Politik und Gesellschaft reagieren derzeit vor allem mit eskalierender Logik der Konfrontation. Dies betrifft die Verhältnisse zwischen den Staaten und großen Blöcken, aber auch die innergesellschaftlichen Krisenerzählungen. Immer drastischere, immer umfassendere Maßnahmen werden ergriffen. Doch welche Alternativen zum dominanten Umgang mit Bedrohung gibt es? Das Heft erkundet einige davon – von den Möglichkeiten der defensiven Verteidigung über die strategische Position der staatlichen Neutralität bis hin zur innergesellschaftlichen Diskursmoderation gegen miteinander konkurrierende Krisenerzählungen. Das Heft versucht, eindimensionalen Ideen der Eskalation weitere Antwortmöglichkeiten beiseite zu stellen.

Mit Beiträgen von Lukas Mengelkamp, Heinz Gärtner, Simon Weiß, Tobias Rothmund und weiteren.

Weitere Beiträge im Heft: Leader-Maynard – Kriegsverbrechen in der Ukraine | Shemia-Goeke – Strategische Gewaltfreiheit | Bieß – Machtkritische Konfliktsensibilität | Funk – Friedensethik als gelungene Mitleidsethik, Teil II

Beilage: Jaberg / Ruf / Scheffran / Lammers: Dossier 96 – Quo vadis, Friedensforschung? (24 Seiten, 2 €)

W&F 1/23 | Februar | 68 Seiten + Dossier | 12 € (druck) / 9 € (ePUB+PDF) als Einzelheft oder im Abonnement
www.wissenschaft-und-frieden.de

40 Jahre W&F

Save the Date: 6./7. Oktober 2023, Bonn:
Symposium ***Wissenschaft für den Frieden***

Aufruf zu Beiträgen und mehr Informationen:
wissenschaft-und-frieden.de/projekt/40-jahre-jubilaeum

pau, Rainer Rehak, Daniel und Gilbert Assaf

make install PEACE – Impulse für den Frieden

Editorial zum Schwerpunkt

Im Januar 2022, als wir anfingen, die Konferenz zu planen, haben wir uns ganz bewusst dazu entschieden, den Begriff *Frieden* – den wir seit 1984 stolz im Namen unseres FIfF-Vereins tragen – auf der Jahreskonferenz ins Zentrum zu rücken. Diese Entscheidung wurde gleichermaßen in Frage gestellt und bestärkt, als am 24. Februar Russland einen Angriffskrieg auf die Ukraine startete. Das Thema *Frieden* wurde dadurch wieder deutlich präsenter im europäischen Diskurs. Durch die räumliche Nähe und die politischen Dimensionen des Kriegs war auch das Thema Frieden plötzlich in aller Munde und entfaltete eine gewisse Dringlichkeit. In Reaktion auf das Kriegsgeschehen kamen selbst feste Glaubenssätze ins Wanken, die seit jahrzehntelang mantraartig wiederholt wurden („Frieden schaffen ohne Waffen"). Plötzlich schien sich alles einer Kriegslogik unterzuordnen, und alle versuchten ein Kind zu retten, das offenbar schon längst in den Brunnen gefallen war und das man aus den Augen verloren hatte. Es wurde nun besonders schmerzhaft deutlich, dass die Frage nach dem Frieden doch die ganze Zeit über hätte wichtig und präsent sein müssen.

Wir haben uns deshalb entschieden, uns des Thema weiterhin in der ursprünglich geplanten Form anzunehmen: Die Frage nach den ganz grundsätzlichen und systemischen Bedingungen für Frieden – einen Frieden, der über die Abwesenheit von offener Gewalt hinaus geht. Die Themensetzung ist damit nicht unabhängig vom aktuellen Weltgeschehen, aber sie war keine direkte Reaktion auf den Krieg – hielten doch viele im Januar einen Krieg noch für unwahrscheinlich. Retrospektiv eine naive Einschätzung. Ganz im Gegenteil zu einer situativen Reaktion auf das Offensichtliche und Unumgängliche wollten wir aktiv und nach vorn gerichtet eine normative Beschäftigung mit dem Frieden vorantreiben.

Denn es gab und gibt weltweit ständig kriegerische Auseinandersetzungen. Für jeden einzelnen Krieg gilt, dass ihm unzählige politische Fehler voraus gehen. Darum ist kein Krieg sinnvoll zu rechtfertigen.

Die Konferenz sollte zur Diskussion anregen und Argumente beitragen, welche Weichen gestellt und welche Dinge getan werden müssen, damit Kriege und Konflikte in zwei, fünf oder auch fünfzehn Jahren nicht wieder – scheinbar – überraschend passieren. Vielmehr wollen wir dringlich der Frage nachgehen, welchen Weg wir zu einer friedvollen Welt einschlagen müssen, ausgehend vom Hier und Jetzt. Wie kann dieser Weg begangen werden? Wir wollen erörtern, welche Maßnahmen konkret befördert werden müssen, was wir kurz-, mittel- und langfristig machen müssen und wollen, um dauerhaft friedvolle und gewaltfreie Gesellschaften zu ermöglichen.

Dabei stellt sich nicht zuletzt die Frage: Was sind diese „friedvollen" Verhältnisse? Sie liegen unserer Ansicht nach genau dann vor, wenn Menschen sich entsprechend ihren gegebenen Möglichkeiten physisch und psychisch selbst verwirklichen können. Mit anderen Worten ist unser Ziel ein pluralistisches, ausdifferenziertes Zusammenleben, das auf die Bedürfnisse der Menschen eingeht, um ein zufriedenes, selbstbestimmtes und komfortables Leben Aller zu ermöglichen. Dieser positive Frieden kann allerdings nur durch Gerechtigkeit, durch die Einhaltung von Menschenrechten und des Völkerrechts, der Versöhnung und Verständigung, und nicht zuletzt der Kriegsfolgenbewältigung erreicht werden. Diese Art von Frieden bzw. diese Art, auf einen Frieden positiv zu blicken, wurde 1971 vom Friedensforscher Johann Galtung im Rahmen der kritischen Friedensforschung prominent gemacht[1]. Sie betrachtet die Konfliktursachen in bestehenden Gesellschaftsstrukturen und fordert teils weitreichende Veränderungen dieser Strukturen ein. Gemeint ist in unserer Betrachtung also ein Frieden, der nicht allein in der Abwesenheit von internationaler Gewaltausübung besteht, sondern auch in der Abwesenheit von personeller Gewalt und von struktureller Gewalt in allen Gesellschaftsbereichen. Dafür müssen wir Konflikte in ihrem Ursprung und Ansatz angehen und an den Ursachen packen, in denen strukturell bereits angelegt ist, dass diese sich zu gewaltvollen Konflikten entwickeln können. Wir müssen an diesen Ursprung gehen, das heißt auch, eine tiefliegende und weitreichende Veränderung von Denken, Handeln und Wahrnehmen zu ermöglichen und damit auch die Reflexionen der gegenwärtigen Strukturen ernsthaft anzugehen. Das ist teilweise schmerzhaft. Und es geht vor allen Dingen auch nicht ohne Reibung und gesellschaftliche Auseinandersetzungen. Es ist sehr wichtig zu verstehen, dass eine friedvolle, moderne Gesellschaft, in der ein ausreichendes Maß an Mitwirkung institutionalisiert und Toleranz erreicht werden, letztlich auch nur durch Konflikte erreicht werden kann. Diese ergeben sich durch angestoßene Veränderungen und damit verbundene Aushandlungsprozesse und Auseinandersetzungen auf dem Weg dahin. Und schließlich, selbst wenn die friedliche Gesellschaft erreicht wurde, ist das kein Zustand, der einfach bleibt, sondern er erfordert ein konstantes Arbeiten an der Erhaltung dieser friedlichen Zustände. Das Wichtige ist hierbei, dass es festgelegte Regeln

gibt, wie inhärente Interessenskonflikte gelöst werden. Zudem ist es wichtig zu verstehen, dass Frieden und die Aushandlung von Konflikten sich nicht notwendigerweise ausschließen.

Aus dieser kritischen Friedensforschung, die die Probleme in den Gesellschaftsstrukturen sieht, ergibt sich ein äußerst breites Forschungsfeld. Die weitläufigen Arbeiten zu Rassismus, Flucht und Migration, Klimagerechtigkeit, Kapitalismuskritik, Gendergerechtigkeit, (intersektionalem) Feminismus, Inklusion, Klassismus, Antifaschismus und viele mehr gehören unserer Ansicht nach alle zum Bereich des positiven Friedens und sind damit als Ausdifferenzierungen der Friedensforschung zu betrachten, die aber gemeinhin nicht als solche zugerechnet werden. Es wird also viel Forschung und Arbeit von vielen engagierten Menschen wie Wissenschaftler:innen und Aktivist:innen gemacht, die wir in unserer Tagung unter der großen Frage nach Frieden zusammengetragen haben.

Um den bescheidenen Rahmen unserer Jahrestagung aber nicht zu sprengen, haben wir nicht all diese Aspekte berücksichtigen können, sondern einen Fokus auf drei Leitfragen gelegt, die wir als ein Angebot für die Beschäftigung mit dem Thema betrachten:

1. Welche gesellschaftlichen Bedingungen gibt es für Frieden?

2. Wie kann Technologie gestaltet werden, um Frieden zu fördern?

3. Welche Technologien müssen eingeschränkt werden, weil sie Friedensbemühungen stören oder untergraben?

Dabei betrachten wir Technologien nicht nur abstrakt, sondern in konkreten, gesellschaftlichen Kontexten und Anwendungen, um daraus einerseits Anforderungen und Änderungen an den strukturellen Rahmenbedingungen der Techniknutzung auszumachen und andererseits Handlungsmöglichkeiten für Technikgestaltung und Technikregulierung abzuleiten.

Im Verlauf der Konferenz beleuchten wir zunächst die gesellschaftlichen, politischen, rechtlichen und ethischen Dimensionen als Voraussetzungen positiven Friedens. Schließlich diskutieren wir auch informationstechnische Entwicklungen und Systeme. Wir wollen dabei möglichst alles aus dem Blickwinkel bewerten, wie der Grundstein für einen positiven Frieden gelegt werden kann.

Der FK-Schwerpunkt besteht aus den schriftlichen Fassungen der Vorträge von der FIfF-Konferenz 2022. Die Vorträge selbst sind unter *https://media.ccc.de/c/fiffkon22* einsehbar.[2]

- **Thomas Reinhold** verhandelt in seiner Keynote die Rolle und Verantwortung der IT für aktuelle politische Fragen und gibt Beispiele dazu, wie das praktisch aussehen kann.

- Der Beitrag von Dr. **Josua Schneider** widmet sich einer soziologischen Bestandsaufnahme des zivilisatorischen Hexagons, einem Konzept aus der Friedens- und Konfliktforschung.

- Als Nerds und Nerdinnen holen wir uns regelmäßig Inspirationen aus dem SciFi-Genre. Allen voran natürlich Star Trek – doch wie wird eigentlich in Star Trek mit dem Thema Frieden umgegangen, ist es dort überhaupt so friedlich? Diese Fragen beantwortet der Artikel von Dr. **Sebastian Stoppe**.

- Welche Rolle spielen wirtschaftliche Akteure in Krisen und Konflikten und beim Friedenserhalt? Mit dieser Frage beschäftigt sich Dr. **Mathias John** von *Amnesty International* in seinem Beitrag.

- Auf der Konferenz konnten wir **Theresa Hannig** gewinnen, eine Lesung ihres Buches *Komm nach Pantopia, hier sind alle willkommen!* zu halten. In dieser FIfF-Kommunikation findet sich eine Leseprobe ihres Buches.

- Auf der FIfFKon22 wurde zum ersten Mal der Weizenbaumpreis für Frieden und gesellschaftliche Verantwortung verliehen, der dieses Jahr an **Julian Assange** ging. Die Laudatio von **Rainer Rehak** und Grußworte von Assanges Partnerin **Stella Assange**, die stellvertretend den Preis entgegen genommen hat, sind in diesem Heft auf den Seiten 12-15 wiedergegeben.

- Mit der technischen Rekontextualisierung von Technik, also Technik, die ursprünglich für ganz andere Zwecke erstellt worden ist, als sie dann später benutzt wird, beschäftigt sich **Niels Jansen** am Beispiel von *predictive policing*.

- Der letzte Artikel beschäftigt sich mit dem Thema *Dual Use*. Dr. **Thea Riebe** hat untersucht, wie verantwortungsvolles Technik-Design aussehen könnte und welche Methoden der Technikfolgenabschätzung benutzt werden können.

Danksagung

Das Organisationsteam der FIfF-Konferenz 2022 bedankt sich ganz herzlichen beim Video Operation Center (VOC) vom CCC für die großartige und professionelle Videozauberei, den Stream und die Aufnahmen. Außerdem wollen wir uns ganz herzlich beim Chaos Computer Club e. V. für den finanziellen und spirituellen Support bedanken.

Wir danken allen Engeln für Herz, Hirn und Hand, der Gesellschaft für Informatik für finanzielle Unterstützung und dem Team Geil für die hervorragende leibliche Versorgung. Wir bedanken uns außerdem recht herzlich bei der Archenhold-Sternwarte, für die großartige Location, insbesondere bei Stefan Gotthold, der uns mit viel Einsatz unterstützt hat. Dank gilt auch allen Speaker:innen, Künstler:innen und auch den Workshopleitenden, die mit ihrem Beitrag der Konferenz Inhalt und Leben einhauchten.

Insbesondere danken wir dem gesamten Orga-Team, das unter größten Kraftanstrengungen diese wunderbare Konferenz ermöglicht hat. Ihr wart großartig!

Schließlich danken wir auch allen Teilnehmer:innen, die diese Konferenz zu etwas ganz Besonderem gemacht haben.

Anmerkungen

1 *Werkner I, Ebeling K (2016) Handbuch Friedensethik, pp17-31*

2 *Aaron Lye hat bereits den Artikel „NATO-Manöver im Cyberraum: Cyber Coalition, Locked Shields und Crossed Swords" zu seinem Vortrag in der FIfF-Kommunikation 1/2022 – Selbstbestimmung in digitalen Räumen – veröffentlicht.*

CC BY

Thomas Reinhold

Keynote FIfF-Konferenz 2022

make install PEACE – Impulse für den Frieden

Vielen Dank für die Möglichkeit, heute hier zu sprechen. Als Rainer mich gefragt hat, ob ich die Keynote halten würde, habe ich überlegt, was ein passendes Thema wäre, das zur FIfFKon passen würde. Und ich habe mich für ein Thema entschieden, das mir seit vielen Jahren am Herzen liegt und sich grob mit „Informatik und die Verantwortung bei der Gestaltung von Technik und Debatten" umschreiben lässt.

Aber vorher kurz zu meinem Hintergrund: Ich bin wissenschaftlicher Mitarbeiter an der TU Darmstadt am Lehrstuhl Wissenschaft und Technik für Frieden und Sicherheit (PEASEC) bei Prof. Christian Reuter. Was wir am Lehrstuhl versuchen, ist an der Schnittstelle von drei wichtigen Themenbereichen zu sein: der Friedens- und Konfliktforschung, der Mensch-und-Computer-Interaktion, und der Cybersecurity, da wir festgestellt haben, dass sehr viele wichtige Themen rund um den Cyberspace nicht isoliert betrachtet werden können. Ich selber bin Diplom-Informatiker, und habe mich damals auf KI vertieft, ein Thema, das mich seit damals begleitet hat und jetzt gerade ja wieder virulent wird. Mein eigentlicher Forschungsfokus liegt jedoch auf der Militarisierung des Cyberspace und vor allem, wie man das verhindern kann.

Meinem Vortrag möchte ich gern eine Frage voranstellen: Wer weiß, wer dieser Mensch sein könnte?

Quelle: Von Nobel Foundation – http://nobelprize.org/nobel_prizes/chemistry/laureates/1944/hahn-bio.html, Gemeinfrei, https://commons.wikimedia.org/w/index.php?curid=6225900

Auf dem Bild zu sehen ist Otto Hahn, der von 1879 bis 1968 gelebt hat. Er war deutscher Chemiker und hat unter anderem 1945 den Nobelpreis für Chemie bekommen. Neben anderen Dingen war Otto Hahn Mitbegründer und erster Präsident der Max-Planck-Gesellschaft. Der Grund aber, warum ich Otto Hahn hier voranstelle, ist, dass er unter anderem auch Initiator eines Dokumentes gewesen ist, das mir sehr wichtig ist und das ich im Folgenden ein bisschen vorstellen möchte: Nämlich der sogenannten Mainauer Kundgebung – jetzt besser bekannt unter dem Begriff *Mainauer Deklaration*. Dieser Name bezeichnet eine Erklärung, die seit 1955 im Rahmen der Nobelpreisverleihung herausgegeben wird und mit der sich, als sie initiiert wurde, Wissenschaftler und Wissenschaftlerinnen explizit gegen die weitere Erforschung und den Einsatz von Nuklearwaffen ausgesprochen haben. Dieses erste Dokument von 1955 beginnt mit dem folgenden, sehr wichtigen Satz: „*Mit Freuden haben wir, die Unterzeichnenden, unser Leben in den Dienst der Wissenschaft gestellt. Sie ist, so glauben wir, ein Weg zu einem glücklicheren Leben der Menschen. Wir sehen mit Entsetzen, dass eben diese Wissenschaft der Menschheit Mittel in die Hand gibt, sich selbst zu zerstören.*" Und Otto Hahn hat ziemlich genau gewusst, wovon er damals, als Mit-Initiator des Dokuments sprach, da er unter anderem 1938 mit seiner Forschung zur Kernspaltung dazu beigetragen hat, dass Nuklearwaffen überhaupt entwickelt werden konnten. Dieses Thema hat ihn Zeit seines Lebens weiter begleitet und er hat sich, unter anderem mit der späteren Göttinger Erklärung, immer wieder für den ausschließlich friedlichen Einsatz dieser Technologie stark gemacht. Letztlich musste er jedoch damit leben, dass die Büchse der Pandora geöffnet worden ist. Das Wissen war in der Welt und es konnte nicht mehr zurückgenommen werden.

Ich erzähle das hier, weil ich glaube, dass wir, dass Sie als Informatiker:innen, als Häcksen und Hacker, als Nerds und Nerdinnen möglicherweise vor einer ähnlichen Herausforderung stehen.

Wenn wir auf die Technologien schauen, die wir kreieren und deren Anwendung wir beherrschen, dann sehen wir unter anderem mit dem Vorfall von *WannaCry* 2017, dass die Dinge, mit denen wir uns beschäftigen, auch durchaus erhebliche Schäden anrichten können. WannaCry beispielsweise hat sich damals wahnsinnig schnell ausgebreitet und auch, wenn nicht die Auslöschung der Menschheit zur Debatte stand, so waren die Schäden doch erheblich und mir stellt sich die Frage, was die Präambel der Mainauer Kundgebung für das Heute bedeutet und was sie mit meiner Arbeit zu tun hat. Und in eigenen Worten formuliert heißt das für mich, wie die Dinge, die wir erschaffen, an denen wir forschen und arbeiten, friedlich und zum Wohl der Menschen eingesetzt werden können. Und wie wir uns dagegen stemmen können, dass sie anderen Schaden zufügen?

Im Kern dieses Satzes steckt für mich letztlich die Frage, welche Verantwortung der Informatik in aktuellen Zeiten zukommt und ohne Anspruch auf Vollständigkeit möchte ich sehr gern drei Punkte herausstellen, die mir diesbezüglich besonders wichtig sind.

1. Wir sind die Experten und Expertinnen

Was ich damit meine ist, dass der Raum, über den wir sprechen, der Cyberspace, nach genau jenen Regeln funktioniert, die wir mitgestalten. Die Dinge, die im Cyberspace laufen, die Software und alle anderen Sachen werden von uns gestaltet und programmiert. Die Regeln diese Raumes werden von uns definiert, festgelegt und weiterentwickelt: von Ihnen, von mir und von unseren Kolleginnen und Kollegen. Das setzt uns aber auch in die Verantwortung, dass wir diejenigen sind, die diesen Raum verstehen. Um bei einen Beispiel zu bleiben: Vielleicht erinnert sich jemand noch daran, wie vor einigen Monaten die Geschichte kursierte, in wie vielen deutschen Amtsstuben noch Faxgeräte stehen. Das kann man lächerlich finden. Das kann man traurig finden. Aber es ist vor allen Dingen ein Indiz dafür, wo wir als Gesellschaft mit unserer technologischen Kompetenz eigentlich stehen und wie viel Aufklärungsbedarf noch da ist. Und das ist etwas, was ich in meinem täglichen Arbeiten ganz oft feststelle, wenn ich mit Politikern und Politikerinnen spreche. Wie oft ich sozusagen der Erklärbär sein muss und Dinge wie IP, Cybersicherheit, Routing usw. erkläre. Gleichzeitig stelle ich fest, dass aber auch eine große Offenheit für diese Themen da ist und eine große Dankbarkeit. Für mich bedeutet dies, dass dieses Erklären, dieses Auf-die-Politik-Zugehen etwas ist, dass wir noch viel, viel stärker machen sollten: Technik erklären, wo es nötig ist und sich dabei auch auf Fragen einlassen, bei denen man eigentlich erstmal glaubt, dass sie mittlerweile jeder verstanden haben sollte. Doch eine Frage doof zu finden ist der beste Weg, um sie abzuwürgen. Das habe ich unter anderem durch meine zwei Kinder gelernt. Und es war ein hartes Training, sich auf die Fragen einzulassen, die meine Kids hatten und haben, dann dort anzusetzen und die Dinge zu erläutern.

Wir sind die Experten und Expertinnen für den Cyberspace. Und wenn wir möchten, dass sich unsere Ideale und unsere Werte in diesem widergespiegeln, in fünf, in zehn, in 20 Jahren, dann sollten wir da sein, wo genau diese Technologie sozusagen für die Zukunft gestaltet wird.

2. Sich auf „die Politik“ einlassen

Der zweite Punkt, der damit sehr eng verbunden ist, hat viel mit meiner Arbeit zu tun, auf die ich gleich noch ein bisschen mehr eingehen werde. Meiner Erfahrung nach ist es extrem wichtig, der Politik noch mehr zuzuhören und deren Bedürfnisse (und Grenzen) anzuerkennen.

Meine Arbeit im Bereich der Rüstungskontrolle ist geradezu prädestiniert dafür, dass man mit Menschen zu tun hat, die aus dem politischen Raum kommen. Was ich dabei merke, ist, wie wichtig es ist, sich in diesen Gesprächen auf die Sprache und das Umfeld der Politik einzulassen. Ein hervorragendes Beispiel, wie es nicht sein sollte, habe ich selber oft erlebt, als vor 10, 15 Jahren in der Politik das Thema Internet ankam und man dort vor allem den Begriff des *Cyberspace* verwendet hat. Wenn ich damals auf einer technischen Konferenz von Cyberspace geredet habe, wurde ich umgehend für einen Internetausdrucker gehalten. Auch da könnte man der Politik natürlich sagen: „*Lernt erst mal die Technik.*“ Aber eigentlich möchte ich das gar nicht. Ich möchte von Politiker:innen nicht prioritär, dass sie die Technik verstehen – das müssen sie gar nicht. Mein Automechaniker erwartet von mir genauso wenig, dass ich weiß, wie ein Verbrennungsmotor funktioniert. Wichtig ist mir stattdessen, dass die Politik denen zuhört, die von der Technik Ahnung haben. Ich erlebe, dass genau diese Bereitschaft da ist, aber eben von mir auch erfordert, mich auf diese Fragen einzulassen und die Sprache zu lernen und zu akzeptieren, die in der Politik gesprochen wird. Manchmal bedeutet dies auch, zwischen den Sprachen der Technik und jener der Politik zu übersetzen. Aber so kommt man in den Diskurs und dann ist es möglich, Debatten zu gestalten, anstatt nur an der Seite stehend zu kritisieren. Letzteres ist sehr leicht. Wenn man auf Twitter unterwegs ist, erlebe ich das leider sehr oft. Ich finde es ehrlich gesagt furchtbar, wie die ganze Zeit nur gehässig gelächelt wird. Ja, das kann man machen: seine Echokammer bedienen und sich danach super fühlen. Aber damit wird man keine Debatten gestalten, weil man im Zweifelsfall die Menschen vor den Kopf stößt, die vielleicht wirklich was verändern wollen.

Und noch etwas, das mir diesbezüglich sehr wichtig ist, passt gut zu diesem Echokammer-Verhalten, nämlich dass, ganz oft von „DER POLITIK“ gesprochen wird. Ehrlich gesagt, weiß ich gar nicht, wer diese „DIE POLITIK“ eigentlich sein soll. Ich erlebe dort nur Menschen, ich erlebe Einzelpersonen mit ihren Problemen, mit ihren Zielen und mit ihren Werten, die manchmal nicht mit meinen Vorstellungen kongruent gehen. Aber es sind trotzdem Einzelpersonen, mit denen ich ins Gespräch kommen kann, wenn ich mich auf sie einlasse und sie ernst nehme.

3. Kritik ist wichtig, aber!

Der dritte Punkt, den ich hier betonen will ist, dass dies keinesfalls ein Plädoyer sein soll, nicht zu kritisieren. Ganz im Gegenteil. Kritik ist extrem wichtig und gerade vor dem Hintergrund, dass wir diejenigen sind, die die Technik verstehen und deren Folgen abschätzen können, ist Kritik absolut angebracht. Aber Kritik sollte meiner Meinung nach im besten Fall etwas sein, was einen Weg nach vorn gestaltet. Natürlich muss und darf sich jede:r die Frage stellen, ob er oder sie in die Fundamentalopposition gehen oder eher mitgestalten möchte? Verstehen Sie mich nicht falsch. Beides ist extrem wichtig und beides wird gebraucht, sofern es in einer guten Harmonie zueinander steht. Aber wenn man mitgestalten möchte – und deswegen habe ich von der Rüstungskontrolle gesprochen, auf die ich gleich noch ein wenig genauer eingehen werde – dann muss man sich eben unter Umständen auch auf fremde Perspektiven einlassen, die einem nicht gefallen und sich mit Menschen an den Tisch setzen, deren Werte man vielleicht nicht teilt.

In der Rüstungskontrolle sind das militärische Kräfte. Die kann man doof finden, okay. Aber dann wird man mit denen nie über Rüstungskontrolle und über die Schritte sprechen können, die man vielleicht gehen kann, um die Gefahren dieser Technologie zu reduzieren. Dann werde ich nie in diese Gespräche eintreten können. Und dass bringt mich zum Thema Lobbyismus, ein Begriff, der ja sehr verschrien ist. Aber letztlich bedeutet Lobbyismus ja nur: Interessen vertreten. Und ich glaube, dass es genau dies ist, was wir noch sehr viel stärker tun sollten. Aktiv und positiv unsere Interessen vertreten. Ich weiß, dass alles hier ist ein bisschen ein „preaching to the Choir“, weil Ihr und Sie im Auditorium das sowieso bereits an sehr vielen Stellen tun.

Um das Ganze nicht zu moralisierend klingen zu lassen, möchte ich noch ein bisschen davon erzählen, was diese Punkte für meine Arbeit im Bereich der Rüstungskontrolle, in dem ich seit vielen Jahren aktiv bin, konkret bedeuten. Der Kerngedanke von Rüstungskontrolle ist die Erkenntnis, dass Rüstung in irgendeiner Form immer asymmetrische Kräfteverhältnisse schafft. Das heißt, sie haben immer einen Stärkeren, der im Vorteil ist und daher einen Anreiz hat, diesen Vorteil zu nutzen – im Zweifelsfall militärisch. Und sie haben eine schwächere Seite, die daraus resultierend unter gewissen Sicherheitsbedrohungen steht – oder diese so interpretiert – und dadurch Anreize hat, irgendwie anders zu versuchen, diese Bedrohung abzuwenden. Die Situation führt sehr schnell in Rüstungsspiralen hinein, weil beide Seiten immer wieder versuchen werden, einen Schritt vor der anderen Seite zu sein. Rüstungskontrolle setzt genau an dieser Stelle an, nimmt diese Dynamik auf und versucht sie in einem ersten Schritt zu bremsen. Das könnte darin bestehen, die jeweiligen militärische Kapazitäten auf ein Niveau zu bringen, mit dem alle beteiligten Akteure leben können und ihre Sicherheitsinteressen gewahrt sehen. Wenn das gelungen ist, dann ist es möglich, das Rüstungsniveau schrittweise auf allen beteiligten Seiten zu senken, um im allerbesten Falle sogar am Ende auf die Rüstungstechnologie komplett verzichten zu können. In diesem Ansatz steckt viel Optimismus, das ist mir vollkommen klar und Abrüstung oder gar der vollständige Verzicht wird nur unter sehr optimalen Bedingungen erreicht. In der Realität sind es oft eher zwei Schritte vor, drei zurück und angesichts der aktuellen Weltlage wohl sogar eher vier Schritte zurück und vielleicht einen halben Schritt nach vorn.

Was kann die IT nun eigentlich zu dieser Weltlage beitragen und was versuche ich zu tun? Tatsächlich kommt mir als Naturwissenschaftler die Rüstungskontrolle diesbezüglich in einer Sache sehr entgegen: dem Prinzip der sogenannten Verifikation.

Wenn sich Staaten an den Tisch setzen und einen Rüstungskontroll-Vertrag aushandeln, dann machen Sie dieses in aller Regel nicht auf Basis von Vertrauen, die Situation ist ja eher dadurch geprägt, dass sie eben nicht vertrauen. Stattdessen werden solche Verträge mit sogenannten Verifikations-Maßnahmen abgesichert, also konkreten praktischen Maßnahmen, mit dem sich beide Seiten jeweils gegenseitig auf die Finger schauen und kontrollieren können, ob sie sich an die Abmachung halten. Das populärste Beispiel hierfür ist sicher die Internationale Atomenergiebehörde IAEA, die im Rahmen des sog. *Iran Deals* die zivile Nutzung des iranischen Nuklearprogramms kontrolliert, um sicherzustellen, dass dieses nicht für militärische Zwecke genutzt werden kann. Sie machen das, indem sie mit Sensoren regelmäßig durch Anlagen laufen, Kameras aufstellen, Dinge verplomben, Dinge & Anlagen ausmessen und regelmäßig auf Veränderungen wie *neue Türen oder neue Kabel* prüfen. Das heißt, die Kontrolleur:innen betreiben dort Hardcore-Naturwissenschaft.

Auf den Cyberspace übertragen ist das genau das Thema, mit dem ich mich beschäftige. Dabei fällt vor allem erst einmal auf, dass viele Prinzipien von der Rüstungskontrolle für den Cyberspace so nicht funktionieren. Wir können Dinge nicht zählen, wir können Dinge nicht anfassen, wir können nicht sagen: „stand vor einem halben Jahr hier, steht es immer noch hier?“ Das ist alles extrem schwierig und an diesem Punkt steckt die Rüstungskontrolle für den Cyberspace aktuell noch fest. Die Herausforderungen beginnen dabei im Prinzip bereits bei der Frage, was reguliert werden soll und in welchem Umfang? Was ist denn eigentlich ein Cyberwar oder ab wann ist ein Stück Software eine Cyber-Waffe? Denn so etwas wie beispielsweise *Penetration Testing Tools* sind für zivile Zwecke extrem wichtig, gleichzeitig wollen wir natürlich unterbinden, dass sie im militärischen Bereich eingesetzt werden, um fremde Systeme aufzumachen und zu gefährden. Im Kern ist dies die Aufgabe, der ich mich widme. Auf der einen Seite ein ganz klares Verständnis der Technik zu entwickeln und dies zu verbinden mit einem hinreichend guten Verständnis der Politik, um auf Basis dessen an Lösungen zu arbeiten. Dies kann darin bestehen, sich zu überlegen, was genau eine Cyberwaffe ist, und dafür Klassifikationssysteme zu entwickeln. Das kann darin bestehen, sich Gedanken zu machen wie Stockpiles von Exploits, die Nachrichtendienste und Militärs horten, abgeglichen werden können, um sie dann abzubauen. Oder wie kann Schadsoftware und deren Einsatz und Weiterverbreitung nachverfolgt werden?

Eine letzte Sache in Bezug auf unsere Verantwortung möchte ich gerne noch erwähnen, die insbesondere mit dem Krieg Russlands gegen die Ukraine noch einmal deutlich geworden ist und die ich mit „Und plötzlich ruft die Presse an“ umschreiben möchte. Seit dem Krieg Russlands und den Cyberattacken gegen das Satellitennetzwerk KA-SAT klingelten bei uns am Lehrstuhl plötzlich unaufhörlich die Telefone, und wir haben unzählige Presseanfragen erhalten, mit Fragen danach, was das für die Ukraine bedeutet und für die Zivilbevölkerung dort. Oder was die Cyberattacken für den Krieg bedeuten und wie es vielleicht weitergehen wird? Es hat uns sehr herausgefordert, mit dieser Flut an Anfragen klarzukommen, Dinge einzuordnen und zu bewerten und dabei sehr oft auch Erklärbär und Erklärbärin sein zu müssen. Und neben den Kontakten zur Presse haben auch unsere Kontakte von Politiker:innen natürlich die gleichen Fragen gestellt, weil sich durch den Angriff Russlands doch ei-

Thomas Reinhold

Thomas Reinhold ist wissenschaftlicher Mitarbeiter und Doktorand am Fachgebiet Wissenschaft und Technik für Frieden und Sicherheit (PEASEC) der Technischen Universität Darmstadt. Er befasst sich mit IT-gestützten Möglichkeiten für Rüstungskontrolle militärischer Aktivitäten und Abrüstung im Cyberspace sowie den Problemen einer Militarisierung von Künstlicher Intelligenz.
Webseite: *https://peasec.de/team/reinhold*

nige sicherheitspolitische Vorzeichen geändert haben und auch hier eine Menge an Aufklärungs- und Gesprächsbedarf bestand. Nicht zuletzt war es auch für unsere Student:innen an der Universität selber wichtig, Gesprächsangebote zu schaffen, und wir haben offene Veranstaltungen ausgerichtet, ganz nach dem Motto: Wir bilden eine große Runde und wir reden. Wir tauschen uns aus, über den Schock, unter dem wir stehen, und über die Fragen, die wir haben, um diese dann als Mitarbeiter:innen am Lehrstuhl einzuordnen und zu bewerten.

Damit will ich zum Ende der Keynote kommen, nachdem ich hier 20 Minuten lang den moralischen Zeigefinger erhoben habe. Ich hoffe dass Sie mir glauben, dass die Dinge, über die ich hier gesprochen habe, Dinge sind, die mir durch meine eigene Arbeit klar und seitdem unglaublich wichtig geworden sind, nämlich: Aufklären und Erklären, Technik da gestalten, wo sie gebraucht wird, Echokammern zu verlassen und im besten Falle in Gespräche zu kommen mit denjenigen, die man vielleicht sonst nicht erreicht, und Lösungen am Bedarf zu orientieren.

Letztlich, und das ist es, von dem ich mir wünsche, dass Sie es mitnehmen, sind wir die Lobbyisten und Lobbyistinnen für eine friedliche Entwicklung des Cyberspace.

Danke schön.

CC BY

Josua Schneider

Das zivilisatorische Hexagon

eine soziologische Bestandsaufnahme

Nicht zuletzt durch den Krieg in der Ukraine, der nun schon fast ein Jahr andauert, ist die Friedens- und Konfliktforschung heute mit neuen Herausforderungen konfrontiert. Die deutsche Friedensforschung steht aktuell einer zwischenstaatlichen bewaffneten Konfliktsituation gegenüber, die nicht in einer entfernten Krisenregion, sondern in unmittelbarer europäischer Nachbarschaft ausgetragen wird. Aber auch jüngste innergesellschaftliche Spannungen und Krisen werfen Problemstellungen auf, die nicht nur auf Fragen nach den Möglichkeiten der Konfliktseinhegung und nachhaltiger harmonischer sozialer Koexistenz verweisen, sondern auch zur Reflexion über bereits bestehende Friedenskonzeptionen anregen. Innerhalb dieser hat sich bemerkenswerterweise seit der ersten Generation der Friedensforschung bis zum heutigen Tag noch immer kein einheitlich geklärter Friedensbegriff etablieren können. Im Kern sämtlicher theoretischer Ansätze steht jedoch stets die Gewaltfreiheit als Ausgangspunkt für Überlegungen über friedliche Gesellschaftszustände.

Mit seinem zivilisatorischen Hexagon hat Dieter Senghaas den Versuch unternommen, die Friedensbedingungen unterschiedlicher gesellschaftlicher Teilbereiche aufzuzeigen. Dabei steht für Senghaas der Begriff der Zivilisierung im Mittelpunkt seiner friedenstheoretischen Überlegungen: Frieden kann hiernach als ein andauernder Zustand betrachtet werden, in dem soziale Konflikte (per se nicht negativ, sondern förderlich für einen sozialen Wandel begriffen) in konstruktive gewaltlose Bahnen gelenkt werden, was wiederum das Resultat von langfristigen Zivilisierungsprozessen ist. Das Senghaassche Zivilisierungsparadigma, das auf ideengeschichtliche Klassiker wie Locke, Hobbes und Elias zurückgegriffen und in unterschiedlichsten Fachdisziplinen Anklang gefunden hat, stellt ein normatives Idealbild dar. Die Erfüllung aller interdependenten Eckpunkte bildet die Bedingung, damit es in einer Gesellschaft zu einem andauernden friedlichen Zusammenleben kommen kann.

Jedoch ist das Modell von Dieter Senghaas berechtigterweise nicht ohne Kritik und Einwände geblieben. Neben dem Vorwurf, das Modell trage in seiner eklektizistischen Form als additive Anhäufung philosophischer Erkenntnisse auch die Schwächen seiner ideengeschichtlichen Grundlagen mit sich und dadurch sei es zweifelhaft, dass Gewalt in einem solchen umfassenden Sinne überhaupt eingehegt werden könne (Baumann 2000), stellt sich beispielsweise auch die Frage nach einer legitimen Übertragbarkeit des typisch (west-)europäischen Konzeptes auf die Entwicklungen in anderen Kulturen (Imbusch 2000). Insbesondere wurde am Modell die Kritik geäußert, dass es aufgrund seiner Unterkomplexität kaum als grundlegendes praktisches Analyseraster und auch nicht als Friedenstheorie geeignet sei (Vogt 1996), da manche friedensrelevanten Elemente eher isoliert nebeneinander stünden. Gleichwohl soll in Bezug auf letzteres hier die Ansicht vertreten werden, dass sich – ohne den Anspruch auf eine maximale analytische Tiefe erheben zu wollen – die sechs Säulen des Hexagons sehr wohl dazu eignen, in Bezug auf aktuelle gesellschaftspolitische Problemstellungen als erster Anhaltspunkt für den Zustand eines friedlichen Zusammenlebens in einer Gesellschaft zu fungieren. Um dies zu veranschaulichen, sollen im Folgenden die Säulen einzeln oder zusammengefasst kurz skizziert sowie in ihrer theoretischen Funktion beschrieben und ihre gesellschaftliche Bedeutung oder auch Problemhaftigkeit anhand ausgewählter Beispiele reflektiert werden. Die Beschreibung der letzten Säule des Hexagons soll schließlich in eine knappe resümierende Betrachtung münden.

Entprivatisierung von Gewalt und sukzessive Errichtung eines staatlichen Gewaltmonopols

Zunächst sei das legitime Monopol staatlicher Gewalt als Sicherung der Rechtsgemeinschaft genannt, das durch die Entprivatisierung von Gewalt und somit mittels einer ‚Entwaffnung der Bürger' für eine Regelung von Interessen- und Identitätskonflikten sorgt und diese in argumentative deliberative und diskursive Bahnen lenkt. Erfolgreiche Konfliktaustragungsmuster und -regelungsformen, die die Aushandlung sozialer Konflikte ohne Gewaltaustrag ermöglichen – nach Senghaas Erscheinungsformen erfolgreicher westlicher Zivilisierung –, erweisen sich dieser

Ansicht nach als Garant für innerstaatliche, gesellschaftliche Koexistenz und die Sicherung inneren gesellschaftlichen Friedens.

Ein Zusammenbruch des staatlichen Gewaltmonopols führt diesem Verständnis nach zu einer Annäherung an den Hobbes'schen Naturzustand (Imbusch 2002, S. 172). Die Wiederbewaffnung der Bürger und die nichtstaatliche Gewalt als akzeptierte Handlungsoption individueller oder kollektiver Akteure ist verbunden mit Assoziationen wie dem Wiederaufleben des Faustrechts, Bürgerkriegen und Pogromen, und gewöhnlich geht mit dem Fehlen des Gewaltmonopols auch die Vorstellung eines *failed state*, also eines gescheiterten Staates einher, der seine grundlegendsten Funktionen nicht mehr erfüllen kann.

Mit Blick auf die Bundesrepublik Deutschland kann an dieser Stelle konstatiert werden, dass das Gewaltmonopol grundsätzlich intakt ist bzw. dass private Gewaltanwendung im weitesten Sinne eingehegt wird. Wird der Aspekt des staatlichen Gewaltmonopols jedoch einmal angesichts der jüngsten Klimaproteste hinsichtlich der Abholzung des Hambacher Forstes oder der Abbaggerung des Ortes Lützerath zum Zwecke der Kohleförderung betrachtet, rückt dieser für einen Teil der Bevölkerung in ein ambivalentes Licht. Der anhaltende Polizeieinsatz zur Räumung der Wälder und Siedlungen ist zweifelsfrei ein Symbol für das Gewaltmonopol des Staates. Die Exekutive nimmt die Aufgabe wahr, die Interessen des Staats als auch des Landbesitzers RWE sicherzustellen, der die Braunkohleförderung zumindest bis 2030 betreiben will (Tagesspiegel 2022). Umweltschutzorganisationen protestieren seit Jahren dagegen, dass der Energiekonzern RWE Teile des Hambacher Forstes abholzen und die Braunkohleförderung weiter fortsetzen will. Es gibt einen andauernden Widerstand, den Bürgerinnen und Bürger gegen die industrielle Umweltzerstörung auf vielfache Weise an den Tag legen. Auch ein Gutachten von Greenpeace (Greenpeace e. V. 2020) negiert die Notwendigkeit des Tagebaus Garzweiler II und verweist auf die Gefährdung des sozialen Frieden in NRW.

Angesichts der genannten Problematik drängt sich u. a. die Frage auf, wie es zu bewerten ist, wenn die Konfliktaustragungsmuster und -regelungsformen, die grundsätzlich durch die Etablierung eines Gewaltmonopols gewährleistet werden sollen, längerfristig eben zu keinem Interessenausgleich führen bzw. wiederholt von zahlreichen gesellschaftlichen Interessengruppen in Frage gestellt werden. Wie ist es zu bewerten, wenn das staatliche Gebaren als demokratieverdrossen oder gar -feindlich verstanden wird, und die Polizei, die eigentlich die Verfassung und den Staat schützen soll, als Hilfstruppe für einen Energiekonzern begriffen wird? Inwieweit trägt das Gewaltmonopol seinen Teil zur friedlichen gesellschaftlichen Koexistenz bei, wenn die Exekutivkräfte wiederholt als Mittel der Unterdrückung gegenläufiger politischer Anliegen und Gesellschaftsentwürfe fungiert?

Kontrolle des Gewaltmonopols und Herausbildung von Rechtsstaatlichkeit

Will sich das Gewaltmonopol vom Eindruck reiner Willkür unterscheiden, bedarf es einer rechtsstaatlichen Kontrolle. Die Rechtsstaatlichkeit, die sich im Schutz von grundlegenden Menschenrechten, Gewaltenteilungsprinzipien oder auch in der Unabhängigkeit der Justiz manifestiert, gewährleistet dabei nicht nur die Kontrolle und die Legitimität des Gewaltmonopols, sondern stellt den (gewaltfreien) Rahmen, nach denen Interessen- und Identitätskonflikte ausgetragen werden dürfen. Das legitime Gewaltmonopol garantiert politische Willensbildungsprozesse und Entscheidungsfindungen und gewährleistet zugleich die Rechtsdurchsetzung. Staaten und staatliche Organisationen beanspruchen daher die alleinige Autorität und Verfügungsmacht über physische Gewalthandlungen, um moralische Ordnung oder Bürgersicherheit aufrechtzuerhalten sowie die legitime Sanktionsgewalt gegen Kräfte, die sie herausfordern. Ist eine rechtsstaatliche Einhegung nicht mehr gegeben, kann staatliche institutionalisierte Gewalt kaum als legitime Gewalt ausgegeben werden. Rechtsstaatliche Prinzipien setzen dem Einsatz von staatlicher Gewalt Grenzen, so dass es seinen willkürlichen Charakter verliert. Ohne eine solche demokratische Kontrolle erweist sich das Gewaltmonopol als ein Instrumentarium autoritärer Herrschaft, also letztlich eine Herrschaft des Stärkeren (Imbusch 2002, S. 172).

Wird der Eckpfeiler der Rechtsstaatlichkeit einmal vor dem Hintergrund der jüngsten Corona-Krise beleuchtet, kann festgestellt werden, dass dieser samt seiner friedensstiftenden Funktion plötzlich als inkongruent wahrgenommen und partiell in Abrede gestellt wurde. Die grundsätzliche Funktion des Rechts ist eine Ordnungsfunktion, die nicht nur dazu beitragen soll, die Legitimität des Gewaltmonopols zu gewährleisten, sondern durch die Bestimmung der Spielregeln für Interessendifferenzen das friedfertige und freie Zusammenleben der Bürgerinnen und Bürger zu ermöglichen. Während der pandemischen Lage von nationaler Tragweite wurde das Phänomen erkennbar, dass das Recht für eine Vielzahl von Menschen nicht mehr als Recht, sondern als Unrecht wahrgenommen wurde. Jedoch lebt Recht von Akzeptanz innerhalb einer Gesellschaft. Und aufgrund der mangelnden Akzeptanz für rechtliche Verordnungen, die bspw. das Infektionsschutzgesetz mit sich brachten (und zugleich die Einschränkungen im Hinblick auf die Freizügigkeit, Versammlungsfreiheit oder die Unverletzlichkeit der Wohnung), wurde von Teilen der Bevölkerung eine rechtsstaatliche Einhegung nicht mehr wahrgenommen, und die staatliche institutionalisierte Gewalt nicht mehr als legitim erachtet. Nicht zuletzt aufgrund dieser Einschränkungen der Freiheitsrechte wurde dem Staat von Teilen der Bevölkerung ein totalitärer Charakter zugesprochen. Während der Corona-Pandemie wurde ersichtlich, was geschieht, wenn nicht alle Menschen in einem Gemeinwesen das geltende Recht akzeptieren können und in Folge dem Staat seine Rechtstaatlichkeit absprechen. Denn wenn das Recht keine allgemeine Akzeptanz findet – das war zumindest eine Lektion aus den letzten Jahren – dann kann es auch nur bedingt ordnende, regelnde oder befriedende Funktion ausüben.

Interdependenzen und Affektkontrolle

Die dritte Voraussetzung für inneren Frieden besteht nach Senghaas in der Affektkontrolle, die mit einer Reihe von weiteren Aspekten verknüpft ist. Die Entwicklung von einer traditionellen hin zu einer modernen Gesellschaft kommt mit funktionalen Differenzierungen daher. Wir müssen verschiedene Rollen ‚spielen', erlernen, wie diese gesellschaftlich agieren und welche unterschiedlichen Ansprüche, Rollenanforderungen und Erwartungen an uns gestellt werden. Als ‚Rollenspieler:innen' müssen

wir zudem verschiedenen Loyalitäten entsprechen, was uns bisweilen in Situationen bringt, in denen die vielzähligen Erwartungen an unsere verschiedenen Rollen kaum vereinbar zu sein scheinen, oder auch in denen wir der Anspruchsgruppen einer einzigen Rolle nicht gerecht werden. Das alles verlangt, ein ‚sich zügeln', ein ‚sich beherrschen', also ein gewisses Maß an Impulskontrolle, damit es zu einer Mäßigung des Konfliktverhaltens kommen kann.

Diese Selbstbeherrschung zeigt sich nicht nur maßgeblich für eine funktionale Rollendifferenzierung innerhalb der Gesellschaft, sondern ist auch notwendig, damit das gesellschaftliche Leben ein Mindestmaß an Berechenbarkeit und Erwartungssicherheit erlangt (Imbusch 2002, S. 173). Selbst die Einhaltung gesellschaftlicher Normen kann vor diesem Hintergrund als ‚minimale Freiheitseinschränkung' betrachtet werden, die erduldet werden will. Für Dieter Senghaas sind eine solche Aggressionshemmung und Affektkontrolle hin zu Gewaltverzicht die Basis, damit es überhaupt zu gesellschaftlicher Toleranz und Kompromissfähigkeit kommen kann, da sonst Rechtsstaatlichkeit und Gewaltmonopol letzten Endes fragile Institutionen blieben und ein friedliches Zusammenleben kaum denkbar wäre.

Als drittes Beispiel, welches den Aspekt der Affektkontrolle unmittelbar tangiert, könnte die Ausweitung von Videoüberwachung im öffentlichen Raum aufgeführt werden, die zugleich auch mit Themen wie Datamining, Drohneneinsatz oder biometrische Gesichtserkennung gekoppelt ist. Das Themenfeld der Videobeobachtung auf öffentlichen Plätzen hat in den letzten Jahren nicht zuletzt in den Polizeiwissenschaften an Relevanz zugenommen. Als Vorreiter kann hier Großbritannien und der flächendeckende Kameraeinsatz in London genannt werden, und auch in deutschen Städten werden immer wieder Vorstöße in Richtung Videoüberwachung von öffentlichen Plätzen zur Abschreckung von Straftätern gemacht. Unterschieden wird dabei zwischen Videoüberwachung, also die Sicherung des Bildmaterials zur späteren Verwendung, die der Strafverfolgung dient, und der Videobeobachtung, also der Sichtung des Bildmaterials in Echtzeit durch Beobachter:innen oder KI. In letzterem Fall geht es dann nicht mehr allein um Abschreckung oder spätere Strafverfolgung, sondern um die Möglichkeit präventiven und intervenierenden Handelns. Die Argumentation für einen solchen Kameraeinsatz auf öffentlichen Plätzen reicht von der Möglichkeit eines unmittelbaren Zugriffs noch während oder kurz nach der Straftat, Abschreckung durch erhöhten Kostenaufwand für Straftaten bis hin zur Terrorismusabwehr (Abate 2011).

Aus soziologischer Perspektive hat eine solche Videobeobachtung jedoch einen nicht unerheblichen Einfluss auf die Affektkontrolle von Menschen, da durch sie ein permanent angepasstes Verhalten evoziert wird, was aus der vermuteten Beobachtung resultiert. Stadtsoziologisch hat das Thema Relevanz, weil es den Charakter von Städten verändert: die Anonymität als Attraktivitätsfaktor von Städten geht verloren, und Menschen, die öffentlich überwachte Plätze betreten, werden automatisch zum potentiellen Objekt einer möglichen Strafverfolgung. Wird diese Entwicklung im Sinne einer gesellschaftlichen Disziplinierung weitergedacht, führt sie zu einem Zustand, den Foucault (2021) als Panoptismus bezeichnet hat, also die absolute Konformität des Individuums durch zunehmende Überwachungs- und Kontrollmechanismen. Als Symbol für die Videokamera steht hierbei der Wachturm, von dem wir nicht wissen, ob er besetzt ist oder nicht. Die alleinige Präsenz und die Möglichkeit einer potentiellen Überwachung sorgen für die gewünschte Disziplinierung. Es bleibt jedoch zu bedenken, ob und inwieweit eine solche übersteigerte Affektkontrolle überhaupt nachhaltig zur Zivilisierung und Friedensstiftung beitragen kann.

Demokratische Partizipation / Soziale Gerechtigkeit

Mit der erfolgreichen Zivilisierung einer Gesellschaft geht idealerweise die dauerhafte Möglichkeit einher, unterschiedliche Interessen zu artikulieren und zu integrieren. In pluralistischen Gesellschaftsformen und im Zuge der Herausbildung verschiedener sozialer Schichten kommt es zu Forderungen nach demokratischer Teilhabe, was idealerweise eine fortschreitende Demokratisierung des politischen Systems mit sich bringt, d. h. dass alle Bürgerinnen und Bürger innerhalb sozial mobiler Gesellschaften in Prozesse der Entscheidungsfindung miteinbezogen werden. Diese Artikulationsfähigkeit von unterschiedlichen Interessen erweist sich für demokratisierte Rechtsstaaten als unverzichtbar, da Diskriminierungen und Ausschluss wegen Ethnie, Geschlecht oder anderen Merkmalen das demokratische Prinzip untergraben und als Destabilisierungsfaktor begriffen werden (Imbusch 2002, S. 173).

Die Ausweitung demokratischer Partizipation trägt bestenfalls zu einer Gesellschaftsform bei, die ausnahmslos frei von Diskriminierungen jeglicher Art ist, dazu aber auch Fragen der Gerechtigkeit nicht außer Acht lässt, d. h. Chancengleichheit, Verteilungsgerechtigkeit und Bedürfnissicherheit (also die Sicherung

Josua Schneider

Dr. phil. **Josua Schneider** ist Wissenschaftlicher Mitarbeiter im Institut für Soziologie der Bergischen Universität Wuppertal und dort seit 2014 Lehrbeauftragter für den Arbeitsbereich Politische Soziologie. Von 2017 bis 2020 war er Wissenschaftlicher Mitarbeiter im BMBF-Projekt Studieneingangsphase. Seit 2019 lehrt er nebenamtlich im Fach Soziologie an der Hochschule für Polizei und öffentliche Verwaltung Nordrhein-Westfalen. Seine Arbeits- und Forschungsschwerpunkte sind Friedens-, Konflikt- und Gewaltforschung, Diskurs- und Narrativforschung sowie die narrative und diskursive Legitimierung von Gewalt.

der Grundbedürfnisse) ermöglicht. Denn der innere Frieden und die rechtstaatliche Ordnung sind nur dann gegeben, wenn sich die Mehrzahl der Menschen in einem politischen System gerecht behandelt fühlt. Nur in diesem Fall ist nach Senghaas die Grundlage für die Herausbildung zivilisierter Umgangsformen gegeben und nur dann kann sich ein politisches System auch auf eine materielle Basis und ein Mindestmaß von Legitimität stützen (ebd.).

Eine aktuelle Problemstellung, die sowohl die Partizipation als auch die soziale Gerechtigkeit betrifft, ist die verhinderte Teilhabe im Bildungssektor, hier speziell in der Form des *digital divide*. Im Jahr 2018 wurde im Beschluss der Kultusministerkonferenz festgehalten, dass eine Stärkung der Demokratieerziehung in Schulen umgesetzt werden soll. Partizipation erweist sich als ein Grundprinzip der Demokratie, auf das Kinder (laut den UN-Kinderrechten) ebenfalls ein Recht haben. Nach Jürgen Habermas ist Demokratie nicht naturwüchsig, sondern muss gelernt werden, und dies erfordert Gelegenheiten (Habermas 2019). Diese Befähigung zur (demokratischen) Partizipation zu vermitteln ist eine Aufgabe der Bildungseinrichtungen.

In den Richtlinien und Lehrplänen NRW für die Grundschulen 2021 (Ministerium für Schule und Bildung des Landes Nordrhein-Westfalen 2021) finden sich auf 226 Seiten 133 Treffer für den Suchbegriff ‚digital', und auch in den neuen Lehrplänen der Grundschulen NRW sind seit August 2022 digitale Lernwerkzeuge ein fester Bestandteil in allen Fächern. Vor allem im Lockdown während der Corona-Pandemie waren Kinder darauf angewiesen, mit den Lehrenden in Verbindung zu treten und zu bleiben. Vor allem bei Familien aus schwächeren sozialen Schichten kam es vor, dass Familien weder über einen tragfähigen Internetanschluss noch ein internetfähiges Endgerät verfügten. Der Lösungsansatz des Landes NRW, pro Schule eine dreistellige Anzahl an iPads (Leihgeräte mit SIM-Karte) auszuleihen, blieb vielerorts allerdings nur Theorie. Auch außerhalb von Krisensituationen finden digitale Endgeräte mittlerweile vielfältige Verwendung im Unterricht, z. B. um Rechercheaufgaben zu erledigen oder Leseaufgaben zu erfüllen. Erfahrungsberichte aus den Schulen machen indes klar, dass die Schulen oft für dieses hohe Maß an Digitalisierung gar nicht ausgestattet sind. Es sind überhaupt nicht so viele iPads verfügbar, als dass jedes Kind damit arbeiten könnte. Und in diesem Zuge führt der Einsatz von digitalen Arbeitsmedien zugleich auch zur Exklusion von Kindern aus prekären Verhältnissen. Wenn digitale Bildung im hohen Maße forciert wird, sollte dann nicht auch dafür Sorge getragen werden, dass auf diesem Wege keiner verloren geht? Der Zugang zur Bildung wird an digitale Werkzeuge gekoppelt, was aus der hier eingenommenen Perspektive jedoch keine Bildungsgerechtigkeit aufkommen lässt, was sich wiederum langfristig defizitär auf die Aspekte der Partizipation und sozialen Gerechtigkeit auswirken kann.

Konstruktive Konfliktkultur und Fazit

Wenn alle zuvor genannten Faktoren zusammenspielen, besteht nach Dieter Senghaas eine hohe Wahrscheinlichkeit, dass sich eine politische Kultur konstruktiver Konfliktbearbeitung herauskristallisiert und die Mitglieder einer Gesellschaft fähig und willens sind, Konflikte in einem institutionellen Rahmen produktiv und kompromissorientiert auszutragen. Hiernach befinden

Kritik am Modell von Dieter Senghaas

sich rechtsstaatliche Ordnungen in einem prozesshaften Dauerlernen über Mechanismen der Konfliktbearbeitung. Eine solche Bereitschaft kompromissorientierter Konfliktfähigkeit sieht Senghaas unweigerlich mit der Entwicklung zu einer modernen Gesellschaft verknüpft. Denn ein so in einer modernen Gesellschaft entstandener, zivilisatorischer Friede ist keine Selbstverständlichkeit, sondern ein Vorgang, der immer wieder neu gestaltet, überdacht und auf den gewünschten Zustand hin justiert werden muss (Imbusch 2002, S. 174). Nur wenn die sich gegenseitig bedingenden Eckpfeiler des Modells erfüllt sind, kann es zu einer dauerhaft friedlichen Koexistenz, zu einer Zivilisierung des Zusammenlebens kommen.

Mit seinem zivilisatorischen Hexagon hat Senghaas ein theoretisches Idealbild gezeichnet – einen normativen Rahmen für konflikteinhegende Prozesse, dessen Realisierung zweifellos einen Fortschritt darstellen würde, ob er nun tatsächlich für nichtwestliche Regionen übertragbar ist oder auch nicht. Eine Bezugnahme des Modells auf aktuelle gesellschaftliche Konflikt- und Problemstellungen kann, ungeachtet berechtigter Kritikpunkte, aufzeigen, dass das Hexagon als Gradmesser für Problemthemen und für die Beschaffenheit unseres gesellschaftlichen Zusammenlebens nach wie vor dienen kann. Die sechs Bausteine des Zivilisierungskonzepts fungieren dabei als Ansatzpunkt für eine erste analytische Bestandsaufnahme hinsichtlich der konstitutiven Eckpfeiler unseres Gesellschaftssystems. Diese erste Analyse kann folgend in tiefergehende Betrachtungen darüber überführt werden, wo gesellschaftliche Weichenstellungen und Entwicklungsstrategien vorgenommen werden müssen. Jedoch wird auch deutlich, dass sich die sechs Punkte im Zusammenspiel zwar gegenseitig als Korrektive konstruktiv bedingen, zugleich aber auch als Gefahrenverstärker auftreten können, wenn sie nicht als Beitrag zur Gewährleistung des inneren friedlichen Zusammenlebens wahrgenommen werden oder als normative Leitperspektive keine reelle Verwirklichung erfahren, z. B. bei Scheindemokratien oder illegitimer Staatsgewalt. „Wenn solche abträglichen Sachverhalte sich akkumulieren, hat auch konstruktive Konfliktkultur keine Chance." (Senghaas 1995: 204f.).

Referenzen

Abate Constantin (2011) Präventive und repressive Videoüberwachung öffentlicher Plätze. In: Datenschutz und Datensicherheit 35 (7), S. 451–454. Baumann, Zygmunt (2000): Alte und neue Gewalt. In: Journal für Konflikt- und Gewaltforschung (1), S. 28–42.

Foucault Michel (2021) Überwachen und Strafen. Die Geburt des Gefängnisses. Frankfurt am Main: Suhrkamp.
Greenpeace e. V. (2020) Stellungnahme zum Entwurf einer neuen Leitentscheidung für das Rheinische Braunkohlerevier. Hamburg.
Habermas Jürgen (2019) Faktizität und Geltung. Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtsstaats. Frankfurt am Main: Suhrkamp.
Imbusch Peter (2000) Zivilisation und Gewalt. Habilitationsschrift für das Fach Soziologie: Philipps-Universität Marburg. Imbusch, Peter (2002): Die Konflikttheorie der Zivilisierungstheorie. In: Thorsten Bonacker (Hg.): Sozialwissenschaftliche Konflikttheorien. Eine Einführung. Opladen: Leske + Budrich (Friedens- und Konfliktforschung), S. 165–186.
Ministerium für Schule und Bildung des Landes Nordrhein-Westfalen (2021) Lehrpläne für die Primarstufe in Nordrhein-Westfalen. Düsseldorf. Online verfügbar unter https://www.schulentwicklung.nrw.de/lehrplaene/lehrplan/300/ps_lp_sammelband_2021_08_02.pdf, zuletzt geprüft am 07.02.2023.
Tagesspiegel (2022) Verlängerte Betriebszeit von zwei Kraftwerken. RWE will bis 2030 vollständig aus der Braunkohle aussteigen, 04.10.2022. Online verfügbar unter https://www.tagesspiegel.de/wirtschaft/kohleausstieg-bis-2030-betriebszeit-von-zwei-kohlekraftwerken-bis-2024-verlangert-8710576.html, zuletzt geprüft am 09.02.2023.
Vogt Wolfgang R (1996) Frieden durch Zivilisierung? Probleme, Ansätze, Perspektiven. Münster: Agenda.

CC BY

Sebastian Stoppe

Star Trek – Eine friedliche Zukunft?

Ich möchte diesen Vortrag mit einer Erfahrung beginnen, die eigentlich nichts mit Star Trek zu tun hat.[1] Im Sommer 2022 war ich im Urlaub in Frankreich und besuchte Omaha Beach in der Normandie.

Omaha Beach ist, wie diejenigen wahrscheinlich wissen, die den Film *Der Soldat James Ryan* (USA 1998, Steven Spielberg) gesehen haben, jener Strand, wo die Alliierten im Zweiten Weltkrieg landeten, um Frankreich von der deutschen Besatzung zu befreien. Es war für mich ein ganz eindrückliches Erlebnis, dort einmal zu sein und auch zu sehen, wie präsent die damaligen Ereignisse in der Normandie heute immer noch dort sind und wie die Dörfer und die Einwohner immer noch die Alliierten als ihre Befreier ehren. Es war auch irgendwie seltsam, an diesem Ort zu sein: Wo man heute ganz normal badet und trotzdem weiß, dass dort eine der blutigsten Schlachten des Zweiten Weltkriegs stattgefunden hat.

Warum erzähle ich das hier? Weil gut zwanzig Jahre, nachdem die Invasion dort stattgefunden hatte, *Star Trek* tatsächlich auf die Bildschirme in den Vereinigten Staaten kam. Insofern war der Krieg damals noch gar nicht so lange her; es war damals ein viel kürzerer Abstand gewesen, als wenn ich auf die Zeit zurückblicke, in der ich das erste Mal mit *Star Trek* in Berührung gekommen bin.

Insofern hat das alles natürlich eine Verbindung zueinander und auch *Star Trek* besteht ja längst nicht mehr nur aus der *Original Series* (1966-1969), sondern aus mittlerweile einem ganzen Korb verschiedener Serien. Bis heute ist *Star Trek* eine der wenigen Franchises, die weltweit noch immer in der Populärkultur präsent sind. Die Frage ist jedoch: Wie friedlich ist eigentlich diese Zukunft, die in *Star Trek* beschrieben wird?

Wenn man sich die fiktive zukünftige Geschichte in *Star Trek* ansieht, dann beginnt diese mit einer Zäsur, nämlich dem Dritten Weltkrieg im Jahr 2053. Das ist gar nicht mehr so weit weg und ich hoffe, dass *Star Trek* hier nicht recht behält. Die Geschichte setzt sich dann fort mit dem Krieg zwischen Romulanern und der Erde, dem ersten Krieg zwischen der Föderation und den Klingonen und wenig später dem zweiten Krieg. Einhundert Jahre später folgt die Besetzung von Bajor, der Krieg zwischen der Föderation und den Cardassianern und natürlich letztendlich auch der Krieg gegen das Dominion in *Deep Space Nine*.

Also scheint *Star Trek* ziemlich erfüllt zu sein von Kriegen und Konflikten, und ich will in diesem Vortrag einige dieser Ereignisse herausgreifen. Ich versuche dabei, hier nicht unbedingt nach der Serienchronologie vorzugehen, sondern in der historisch-zeitlichen Reihenfolge. So fangen wir an mit der Serie *Star Trek: Enterprise* (2001-2005), die um das Jahr 2156 herum angesiedelt ist, also gute hundert Jahre später jetzt als unsere derzeitige Gegenwart. Die Erde ist vereint, es gibt keine Einzelstaaten mehr, aber die Föderation ist noch nicht gegründet. Jedoch ist man mit den Vulkaniern mittlerweile befreundet, man ist aber auch im Krieg mit den Romulanern und in einem kalten Kriegszustand mit den Klingonen. Wenn man nun zeitlich in der *Star Trek*-Chronologie weitergeht, dann werden diese Konflikte immer komplexer. Man schließt Frieden mit einigen Völkern, während neue Konflikte aufbrechen.

Wieder hundert Jahre später bei der *Original Series* ist es so, dass die Klingonen mit der Vereinten Föderation der Planeten, die sich ja mittlerweile aus Vulkaniern, Andorianern und der Vereinten Erde gebildet hat, im Krieg sind. Es gibt ein eher neutrales Verhältnis zwischen den Romulanern und der Föderation. Klingonen und Romulaner sind kurzzeitig sogar einmal Alliierte – was sich dann wiederum bei der *Next Generation* ändert. Da sind dann die Klingonen diejenigen, welche mit der Föderation verbündet sind und mit den Romulanern verfeindet sind. Die Föderation ist im Krieg mit den Cardassianern und dann kommt mit den Borg eine völlig neue Spezies hinzu. Schließlich gibt es einen Friedensschluss mit den Cardassianern, aber das Dominion tritt in *Star Trek: Deep Space Nine* als neue Kriegspartei auf.

Was will ich damit sagen? Zum einen wird es in *Star Trek* immer komplexer, was die Darstellung von Kriegen und Konflikten angeht und zum anderen verhält es sich so, dass es auch immer mehr Akteure im *Star Trek*-Universum gibt.

Der Philosoph und Staatstheoretiker Thomas Hobbes argumentierte, dass sich die Menschheit im Naturzustand – also, wenn Gesetze und Ordnungen nicht existieren – sich im „Krieg aller gegen alle“ befinde, oder mit anderen Worten: „Mitbewer-

bung, Verteidigung und Ruhm sind die drei hauptsächlichsten Anlässe, dass die Menschen miteinander uneins werden." Dieser Umstand führte Hobbes in seiner politischen Philosophie zu der Erkenntnis, dass wir einen übergreifenden Gesellschaftsvertrag brauchen, um bewaffnete Konflikte und Gewalt verhindern zu können. Das ist letztlich auch ein Thema, was sich in *Star Trek* immer wieder findet: Der zu Beginn erwähnte, fiktive Dritte Weltkrieg, ist in *Star Trek* ein fundamentaler Kipppunkt, nach dem die Überlebenden auf der Erde zu der Erkenntnis kamen, dass man so nicht weiterleben könne. Die Idee wurde geboren, etwas grundlegend Neues zu schaffen und infolgedessen wurde schließlich die Vereinte Erde und etwa später die Föderation gegründet. Denn der Dritte Weltkrieg wird in *Star Trek* als ein katastrophales Ereignis auf unserem Planeten mit einer nuklearen Eskalation erzählt – in dem Ausmaß, dass weite Teile der gesamten Erde am Ende vollständig zerstört waren. Der Kinofilm *Star Trek: First Contact* (USA 1996, Jonathan Frakes) zeigt ja erstmals ein ausschnittsweises Bild dieser unmittelbaren Nachkriegszeit[2] und eben auch dieser für *Star Trek* so elementar wichtigen ersten Begegnung zwischen Menschen und Außerirdischen mit den Vulkaniern. Dieser erste Kontakt beruht im Grunde ja letztlich auf der Tatsache, dass die Menschheit in der Lage war, den Warp-Antrieb so weit zu entwickeln, dass die Vulkaniern auf die Erde aufmerksam wurden und sich daraus eine friedliche Allianz entwickeln konnte, die über Jahrhunderte andauern wird.[3]

In der fiktiven *Star Trek*-Geschichtsschreibung entstand jedenfalls aus dieser wegweisenden Begegnung die Vereinte Föderation der Planeten, eine Allianz von ganz unterschiedlichen Planeten und Spezies mit rund 150 Mitgliedern und über 1000 Kolonien, welche sich in ihrer gemeinsamen Charta (quasi der Verfassung) der friedlichen Entwicklung verpflichten.

In *Star Trek* ist das Territorium der Föderation im so genannten Alpha-Quadranten unserer Galaxie verortet[4] und umgeben von zahlreichen anderen Spezies wie den Klingonen, den Romulanern, den Cardassianern oder den Ferengi.[5] Die Sternenflotte wiederum ist die militärisch organisierte Institution der Föderation, die das Weltall erforscht, der Wissenschaft und der Diplomatie dienen soll, aber die Föderation und ihre Werte auch aktiv verteidigen soll. Insofern ist *Star Trek* tatsächlich weit davon entfernt, ein pazifistisches Weltbild zu zeichnen, dass Gewalt von vorn herein ablehnt. Wenn man sich die einzelnen *Star Trek*-Serien und -Episoden betrachtet, dann wird man recht viele Konfliktsituationen entdecken. Ich möchte an dieser Stelle ein paar herausgreifen.

Wenn wir uns die Ereignisse in der ersten Staffel von *Star Trek: Discovery* (2017-) anschauen, dann erleben wir dort den ersten von mehreren Kriegen zwischen den Klingonen und der Föderation. Mit der Schlacht am Doppelstern („Battle of the Binary Stars") beginnt dieser tatsächlich sehr verlustreiche Angriffskrieg der Klingonen, welche der Föderation vorwerfen, sich immer weiter ausdehnen zu wollen. Die Föderation würde unter dem vorgeblichen Aspekt, dass sie in Frieden kämen, andere Völker aus ihren Territorien verdrängen oder sie assimilieren, und demzufolge wäre die klingonische Kultur in Gefahr. Gleichwohl ist die Föderation nicht vollkommen unschuldig an der Eskalation, denn es ist dann die Protagonistin der Serie, Michael Burnham, die – aus ihren eigenen Erfahrungen als auf Vulkan aufgewachsene Humanoidin heraus[6] – entgegen der Sternenflottenmaxime für einen robusten Erstschlag gegen die Klingonen plädiert. Denn nachdem einst die Vulkanier einmal versehentlich in klingonischen Territorium eingedrungen seien und die Klingonen sofort angegriffen hätten, würden die Vulkanier seitdem immer Präventivschläge gegen Klingonen unternehmen, sagt Burnham:

> *„Two hundred and forty years ago […] a Vulcan ship crossed into Klingon space. The Klingons attacked immediately. They destroyed the vessel. […] From then on, until formal relations were established, whenever the Vulcans crossed paths with Klingons, the Vulcans fired first. They said 'hello' in a language the Klingons understood. Violence brought respect. Respect brought peace. Captain, we have to give the Klingons a Vulcan 'hello'."*

Burnham ist also der Überzeugung, dass Klingonen diplomatische Bemühungen um eine friedliche Lösung oder Gespräche nicht verstehen, dass also nur die Gewalt als Mittel der Kommunikation bliebe. Wie sich herausstellen soll, ist in diesem Krieg das aber genau die falsche Strategie. Erschreckend ist jedoch, dass diese Erzählung einige Parallelen zum aktuellen Russisch-Ukrainischen Krieg aufweist, der zum Zeitpunkt der Erstausstrahlung zwar schon latent schwelte, aber noch nicht endgültig in einen heißen Konflikt ausgebrochen war. Es ist jedoch – und das lässt sich in der gesamten Historie von *Star Trek* sehen – ein weiteres Beispiel dafür, dass *Star Trek* aktuelle Konflikte in unserer Gegenwart spiegelt und in die Seriennarration überführt. Ähnliches ist schon in der *Original Series* zu beobachten: In der Episode *Errand of Mercy* (welche schon vor fast 60 Jahren im Fernsehen zu sehen war) wird der zweite Föderal-Klingonische Krieg thematisiert.

Die Föderation und die Klingonen befinden sich in einem kalten Kriegszustand, als ein klingonisches Schiff und die Enterprise auf dem Planeten Organia nahe der föderal-klingonischen Grenze aufeinandertreffen. Die Klingonen besetzen kurzzeitig den Planeten und es kommt fast erneut zu einem heißen Konflikt zwischen beiden Parteien, der nur dadurch befriedet wird, dass die Organier selbst beide Konfliktparteien dazu zwingen, einen Friedensvertrag – den Vertrag von Organia – abzuschließen. Dies führt dazu, dass es erstmals eine neutrale Zone und eine Phase relativen Friedens zwischen den Klingonen und der Föderation gibt. Diese Episode ist insofern interessant, weil sie im Kontext der 1960er-Jahre das widerspiegelt, was sich zwischen den USA und der Sowjetunion etwa bei der Kubakrise abspielte, wo ja auch die Welt am Rande eines wieder heißen Konfliktes stand.

Wenn wir hier einen Sprung machen zu *Star Trek: The Next Generation* (1987-1994), dann befinden wir uns in einer Zeit, zwei Jahre, bevor tatsächlich der Eiserne Vorhang fiel und der Kalte Krieg endete. Insofern war *Star Trek* mit der *Next Generation* geradezu prophetisch, da wir nun – als Folge der Entspannungspolitik – mit Lieutenant Worf tatsächlich einen Klingonen inmitten der Mannschaft von Captain Picard sehen. Das Klingonische Reich und die Föderation haben mittlerweile – rund hundert Jahre nach dem Vertrag von Organia – Frieden geschlossen. 2293 folgte nämlich das so genannte Khitomer-Abkommen. Den Kinofilm *Star Trek: The Undiscovered Country* (USA 1991, Nicholas Meyer), der diese Geschichte thematisiert, kann man also auch als Allegorie auf Glasnost und Perestroika betrachten.

Anfang der 1990er-Jahre riefen ja selbst Historiker wie Francis Fukuyama das „Ende der Geschichte“ aus, da man voller Optimismus war, nun die großen Konfliktherde auf der Erde beseitigt zu haben.

Gleichwohl zeigt sich wenig später auch in *Star Trek*, dass diese positive Sichtweise verfrüht war. Bedingt durch interne Machtkämpfe gerät das Klingonische Reich in einen Bürgerkrieg, bei dem Picard sich als Vermittler erneut um Frieden bemühen musste. Die Figur Picards ist damit auch ein Paradigmenwechsel, zeigt sie doch, dass es nun primär das Ziel war, auftretende Konflikte nicht mehr mit Gewalt, sondern durch Diplomatie beizulegen, was ein wesentliches Merkmal in der ganzen Next Generation werden sollte. In einer späteren Phase von *Next Generation* werden die Cardassianer als neue Spezies vorgestellt. Auch hier gab es einen langjährigen Konflikt zwischen der Föderation und den Cardassianern (der so genannte Grenzkrieg), der letztlich durch einen Waffenstillstand und einen formalen Friedensvertrag beendet werden konnte. Gleichwohl entstand durch die Grenzziehung zwischen den beiden Mächten eine Widerstandsgruppe, die Maquis, welche sich gegen die zwangsweise Umsiedlung von Kolonien entlang der Grenze wehrte.

Die Cardassianer wiederum beendeten in dieser Zeit auch die langjährige Besatzung des Planeten Bajor – was den Ausgangspunkt der Serie *Star Trek: Deep Space Nine* (1993-1999) bedeutet. In diesem *Star Trek*-Ableger zeigt sich mehr denn je die ganze Brüchigkeit eines instabilen Friedens insbesondere am Beispiel des Konfliktes zwischen Cardassianern und Bajoranern. Angesiedelt an der äußeren Peripherie des Föderationsterritoriums wird die Föderation Bajors Schutzmacht, was wiederum zu neuen Spannungen mit den Cardassianern, aber auch anderen Spezies führt. Das neu entdeckte, stabile Wurmloch, an dem die Station gelegen ist, verbindet den Alpha-Quadranten mit dem Gamma-Quadranten. Hier ist es dann im Laufe der Serie das Imperium des Dominion, welche über alle Staffeln von *Deep Space Nine* hinweg das bestimmende Thema wird.

Der Konflikt beginnt mit der Erkundung und Gründung erster Kolonien im Gamma-Quadranten durch die Föderation und anderer Mächte aus dem Alpha-Quadranten, wie etwa die Ferengi, die Bajoraner, Vulkaniern und die Klingonen. Das Dominion fühlt sich angesichts der Kolonisierung zunehmend bedroht und reagiert aggressiv durch die Zerstörung von Schiffen und Kolonien. Zunehmend infiltriert das Dominion die Alpha-Quadrant-Mächte mit Spionen. Auch Romulaner und Cardassianer erkennen die Gefahr durch das Dominion, welches aber durch seine Spionage gezielt Zwietracht und Misstrauen zwischen den Mächten im Alpha-Quadranten sät und so das Gleichgewicht der Mächte destabilisiert.

In der Folge entstehen zunächst kleinere Konflikte, etwa zwischen Klingonen und Cardassianern, bevor das Dominion der Föderation offiziell den Krieg erklärt, während die Romulaner erstaunlicherweise neutral bleiben und sich sehr sehr zurückhalten. Dieser Krieg führt dazu, dass Sternenflotte und Föderation zeitweise ihre Werte tatsächlich ernsthaft hinterfragen.

Der Kommandant von Deep Space Nine, Captain Benjamin Sisko, kommentiert die Kriegsführung des Dominion, die sich eben durch verdeckte Operationen auszeichnet, so: „This is exactly what the Founders [die herrschende Spezies im Dominion-Reich] want. Klingon against Cardassian, Federation against Klingon. The more we fight each other, the weaker we will get, and the less chance we have against the Dominion.“ Diese Aussage spiegelt den bereits angesprochenen Naturzustand wider, der Krieg jeder gegen jeden, der schließlich zu diesem großen Krieg führt.

Erst als die Romulaner nach langem Zögern auf Seiten der Föderation und der Klingonen in den Krieg gegen das Dominion eintreten,[7] zeichnet sich ein Wendepunkt ab und das Dominion kann besiegt werden. Der Stationsarzt von *Deep Space Nine*, Julien Bashir, kommentiert das Ende mit Cicero: „‚In time of war, the law falls silent.‘ […] So is that what we have become; a 24th century Rome, driven by nothing other than the certainty that Caesar can do no wrong?“

Er stellt damit die Frage nach den Idealen der Föderation und ob diese eigentlich überhaupt eine friedliche Utopie sein kann. Und tatsächlich wirkt es anhand dieser Beispiele (und vieler weitere, die hier von mir gar nicht angesprochen wurden), dass *Star Treks* Zukunftsvision tatsächlich keineswegs friedlich erscheint, sondern dass die Serien eine Zukunft zeigen, die von Konflikten nur so erfüllt ist.

Das ist deshalb so, weil *Star Trek* uns tatsächlich einen Spiegel vorhalten möchte. Alles, was wir in *Star Trek* bis heute zu sehen bekommen, reflektiert unsere Gegenwart und Teil davon sind

Sebastian Stoppe

Sebastian Stoppe ist Medienwissenschaftler und Projektmanager und wissenschaftlicher Mitarbeiter an der Universitätsbibliothek Leipzig. Er studierte Kommunikations- und Medienwissenschaft, Politikwissenschaft und Mittlere und Neuere Geschichte an der Universität Leipzig und wurde an der Martin-Luther-Universität Halle-Wittenberg über Star Trek als politische Utopie promoviert. Er hat mehrere Arbeiten zu Star Trek, anderen Fernseh- und Filmstudien, insbesondere zur Filmmusik, und zur Computerspielforschung veröffentlicht. Im Sommer 2022 erschien von ihm die überarbeitete englische Fassung seiner Dissertation *Is Star Trek Utopia? Investigating a Perfect Future* bei McFarland & Company Publishers. Website: *www.sebastian-stoppe.de*

eben auch Kriege und Konflikte unserer Zeit: Angefangen vom Kalten Krieg zwischen den USA und der Sowjetunion zu Zeiten der *Original Series* über die etwas optimistischere Seite von *Next Generation* bis hin zu den neueren Serien heute, die eben auch wieder unsere Gegenwart reflektieren. Deshalb präsentiert uns *Star Trek* eben kein wirkliches Paradies, kein friedliches Utopia, sondern *Star Trek* zeigt uns eher eine fragile Zukunftsversion – insbesondere in den neueren Inkarnationen wie etwa *Discovery*. Dort sieht man, dass selbst die Föderation als Institution keineswegs etwas ist, was auf immer stabil ist, sondern was auch von Zerfall geprägt sein kann.

Was möchte *Star Trek* uns also mitteilen? Damit unsere Zukunft eine friedliche sein kann, ist es zum einen notwendig, sich immer weiterentwickeln zu wollen oder wie Picard es ausdrückt: „The challenge is to improve yourself… to enrich yourself." Zum anderen müssen wir aber auch stets für unsere Ideale einstehen, uns darauf besinnen, welche Wege zu einem dauerhaften Frieden führen können oder mit den Worten von Michael Burnham: „We have to be torchbearers, casting the light so we may see our path to lasting peace. We will continue exploring, discovering new worlds, new civilisations. Yes, that is the United Federation of Planets." Ein friedliches Miteinander stets wieder anstreben zu wollen, ist die Kernaussage von *Star Trek*. Und es ist insofern wichtig, nicht nur das Ziel vorzugeben, sondern wie Ensign Harry Kim aus *Star Trek: Voyager* (1995-2001) es ausdrückt: „Maybe it is not the destination that matters. Maybe it is the journey."

Die Geschichten von *Star Trek* sollten für uns alle ein Anreiz sein, Kriege und Konflikte beizulegen und tatsächlich für eine friedliche Zukunft einzutreten. Das ist eigentlich genau diese Reise, auf die wir uns begeben sollten.

Referenzen

Stoppe, Sebastian (2014): Unterwegs zu neuen Welten. Star Trek als politische Utopie. Darmstadt: Büchner-Verlag.

Stoppe, Sebastian (2022): Is Star Trek Utopia? Investigating a Perfect Future. Jefferson, North Carolina: McFarland & Company Inc. Publishers.

Anmerkungen

1 *Dieser Text beruht auf dem gleichnamigen Vortrag bei der FIfFKon22-Tagung am 21. Oktober 2022. Er ist weitgehend im ursprünglichen Rede-Stil belassen, jedoch grundlegend redigiert worden. Für eine detaillierte Auseinandersetzung mit den hier angesprochenen Themen siehe Stoppe 2014 und Stoppe 2022.*

2 *Im Dialog angesprochen wurde die humanitäre Katastrophe nach dem nuklearen Dritten Weltkrieg jedoch schon in der Pilotfolge von Star Trek: The Next Generation „Encounter at Farpoint" (1987).*

3 *In der Narration erhält dieser friedensgeleitete Ansatz, der im Übrigen ja auch in der Zukunft historisch als Wendepunkt in der Geschichte der Menschheit überhöht wird, mehrere ironische Brechungen. Zum einen ist die Trägerrakete des Warp-Raumschiffes eine ehemalige Massenvernichtungswaffe, die jetzt für ein friedensstiftendes Projekt genutzt wird. Zum anderen handelt aber Zefram Cochrane als Erfinder des Warpantriebs keineswegs primär aus friedensliebenden Motiven heraus: „You wanna know what my vision is? Dollar signs, money! I did not build this ship to usher in a new era for humanity. […] I built this ship so that I could retire to some tropical island filled with naked women [sic]".*

4 *Vereinfacht dargestellt ist eine Aufsicht unserer Galaxis zur besseren Verortung in vier gleich große Quadranten aufgeteilt, nämlich den Alpha-, Beta-, Gamma- und Delta-Quadranten.*

5 *Die Borg etwa stammen aus dem weit entfernten und (bis zu den Ereignissen in Star Trek: Voyager) unerforschten Delta-Quadranten; das Dominion aus dem Gamma-Quadranten, der über das Wurmloch in Star Trek: Deep Space Nine erreichbar ist. Damit wird auch deutlich, dass Star Trek nur in unserer Galaxie spielt und bis auf wenige Ausnahmen keine „weit entfernte Galaxien" erforscht werden, wie die deutsche Synchronfassung suggeriert.*

6 *Michael Burnham ist die Stiefschwester von Spock.*

7 *Dem Kriegseintritt voraus geht jedoch eine Operation unter falscher Flagge, die von der Föderation durchgeführt wurden, um den Romulanern zu suggerieren, dass das Dominion auch sie als bisher neutrale Partei angreifen würden.*

CC BY

Mathias John

Unternehmen und Krieg

Wirtschaftliche Akteure als Teil des Problems oder als Teil der Lösung?

1. Einleitung

Unternehmen und Banken als machtvolle Akteure auf der internationalen Bühne spielen in vielen Fällen eine bedeutende Rolle bei Krisen, Konflikte und Kriegen, denn diese sind häufig untrennbar mit wirtschaftlichen Aktivitäten verbunden.

Offensichtlich ist das bei Rüstungsunternehmen, wie sich gerade aktuell angesichts des völkerrechtswidrigen Krieges Russlands gegen die Ukraine zeigt: Die Aktienkurse börsennotierter Rüstungskonzerne sind rasant angestiegen.

Aber es ist nicht allein die Rüstungsindustrie, die global von Krisen und Konflikten profitiert? So haben große Erdölkonzerne in Nigeria über Jahrzehnte die Umwelt und damit die Lebensgrundlagen der Menschen im Nigerdelta zerstört. Und sie sind auch nicht davor zurückgeschreckt, mit staatlichen Sicherheitskräften zu kooperieren, um Proteste der Bevölkerung zu unterdrücken.

Bekannt sind auch die klassischen Konfliktmineralien, deren Ausbeutung beispielsweise im Osten der Demokratischen Republik Kongo einen signifikanten Beitrag zur Finanzierung der jahrzehn-

telangen Kriege leistet. Und nicht zuletzt fehlt gerade im Bereich der Dual-Use-Technologie häufig ein verantwortungsvoller Umgang in Bezug auf Forschung, Entwicklung und Handel.

Dabei könnten Unternehmen einen wichtigen Beitrag zu Krisenprävention und Konfliktlösung leisten. Zentraler Aspekt dabei ist die verbindliche Einhaltung menschenrechtlicher Standards als Kernaufgabe ihrer Sorgfaltspflichten. Gerade die Gewährleistung aller Menschenrechte sind unverzichtbar für Frieden. Nur versuchen viele Unternehmen seit langer Zeit, ihre Verpflichtung auf menschenrechtliche Sorgfaltspflichten zu umgehen. Daher sind die Staaten gefragt, Gesetze zu schaffen, damit alle Unternehmen endlich rechtlich verbindlich menschenrechtliche sowie umwelt- und klimabezogene Sorgfaltspflichten einhalten – und bei Verstößen auch Sanktionen zu verhängen, damit diese Regeln nicht zahnlos bleiben.

2. Rahmenbedingungen und Akteure

Die Gewährleistung aller Menschenrechte in ihrer Universalität und Unteilbarkeit ist eine zentrale Voraussetzung für einen Frieden, der mehr ist als nur die Abwesenheit von Krieg und Gewalt. Das umfasst natürlich individuelle bürgerliche und politische sowie wirtschaftliche, soziale und kulturelle Menschenrechte, aber auch kollektive Menschenrechte wie Recht auf Entwicklung, Recht auf eine saubere Umwelt oder das Recht auf Selbstbestimmung.

Umgekehrt heißt das aber auch, dass Menschenrechtsverletzungen ein guter Indikator für Krisen und Konflikte sein und damit ein wirksames Frühwarnsystem für beginnende Eskalation von Auseinandersetzungen bilden können. In diesem Zusammenhang ist es natürlich notwendig, die entscheidenden Akteure und deren Rolle bei der Ausweitung von Krisen und Konflikten zu erfassen, ihre spezifische Rolle genauer zu betrachten und zu prüfen, wie sie dazu gebracht werden können, zur Deeskalation und Konfliktbearbeitung beizutragen.

Zentrale Akteure möglicher Konflikte sind die Regierungen und deren Ausführungsorgane wie Militär, Polizei oder andere Sicherheitskräfte, das Justizsystem, aber auch regierungsnahe Parteien oder Milizen. Dabei sind die Regierungen völkerrechtlich verpflichtet, die Menschenrechte zu achten, zu schützen und zu gewährleisten (Pflichtentrias), und es liegt auf der Hand, dass eine Verletzung dieser Pflichten Krisen und Konflikte verschärfen wird. Auf der anderen Seite stehen als Akteure aus der Gesellschaft nichtstaatliche zivilgesellschaftliche Organisationen, oppositionelle Parteien, Gewerkschaften oder Kirchen, die natürlich die Gewährleistung grundlegender Menschenrechte einfordern.

Erstaunlicherweise werden in solchen Konfliktszenarien Unternehmen, Banken, Unternehmensverbände oder andere wirtschaftliche Akteure häufig vernachlässigt, obwohl sie eine entscheidende Rolle spielen können und im Sinne der Durchsetzung ihrer Interessen immer wieder politische Macht ausüben – auch wenn sie so etwas meist bestreiten. Dabei beschränkt sich die Verwicklung in Krisen- und Konfliktszenarien üblicherweise nicht allein auf einheimische wirtschaftliche Akteure. Über die globalen Liefer- und Wertschöpfungsketten werden eben auch multi- und transnational tätige Unternehmen zu Akteuren in diesen Szenarien, ebenso auch Banken beispielsweise über ausländische Direktinvestitionen.

Über lange Zeit haben Unternehmen unter Verweis auf die staatliche Pflichtentrias jegliche eigene Verantwortung für Menschenrechte von sich gewiesen. Erst in der jüngeren Vergangenheit hat es hier einen Paradigmenwechsel gegeben. Entscheidenden Anteil daran hatte der durch den Juraprofessor John Ruggie als Sonderberichterstatter für Unternehmen und Menschenrechte der Vereinten Nationen (UN) betriebene Konsultationsprozess, der 2011 zur Verabschiedung der UN-Leitprinzipien für Wirtschaft und Menschenrechte durch den UN-Menschenrechtsrat führte[1]. Grundlage der UN-Leitprinzipien ist das von John Ruggie entwickelte Konzept *protect, respect and remedy*[2]: „Schutz der Menschenrechte" (Aufgabe der Regierungen), „Achtung der Menschenrechte" (Verpflichtung der Unternehmen) und „Abhilfe für Betroffene von Übergriffen durch Unternehmen sicherstellen" (Aufgabe der Regierungen). Ein wichtiger Aspekt ist dabei, dass die Unternehmen nicht nur in ihrem engeren Bereich der eigenen Geschäftstätigkeit auf die Achtung der Menschenrechte verpflichtet werden, sondern entlang ihrer gesamten Wertschöpfungsketten – beginnend bei der Förderung von Rohstoffen oder der Herstellung von Teilen für ihre Produkte bis in die Vertriebswege zu den Endkund:innen und bis zu Verschrottung oder Recycling. Unternehmen sollen zur Umsetzung dieser Verpflichtung sich nicht mehr nur auf die üblichen kaufmännischen Sorgfaltspflichten beschränken, sondern auch menschenrechtliche Sorgfalt entlang ihrer gesamten Wertschöpfungsketten walten lassen – und dazu gehört natürlich auch, durch Achtung der Menschenrechte Beiträge zur Verschärfung von Krisen und Konflikten zu unterlassen.

3. Unternehmen und Krieg – Teil des Problems?

Nach den Übersichten von Friedenforschungsinstituten sind akute Krisen und Konflikte verschiedenster Intensität bis hin zu Kriegen in vielen Staaten der Welt an der Tagesordnung. So stellte das Heidelberger Institut für Internationale Konfliktforschung (HIIK) zu seinem im Frühjahr 2022 veröffentlichten Konfliktbarometer 2021 fest: „Das globale politische Konfliktpanorama im Jahr 2021 war durch eine anhaltend hohe Zahl hochgewaltsamer Konflikte gekennzeichnet."[3] Das HIIK zählte 2021 insgesamt 355 Konflikte, von denen 204 als gewaltsam eingestuft werden. Das Konfliktgeschehen zieht um den ganzen Erdball und es gibt kaum einen Staat, in dem es nicht einen Konflikt mit einer der vom HIIK bestimmten Intensitäten gibt.

Damit sind Unternehmen und ihre Tochtergesellschaften und regionalen Partnerfirmen sowie Banken an vielen Orten mit akuten Krisen und Konflikten konfrontiert und werden damit ein Risikofaktor; sie laufen immer Gefahr, bewusst oder unbewusst Partei zu werden und zur Konfliktverschärfung beizutragen – sei es, durch die Verwicklung in Menschenrechtsverstöße und durch Korruption einen Beitrag zur Aushöhlung rechtsstaatlicher Strukturen zu leisten. Oder sei es, dass sie durch Ausbeutung von Ressourcen ohne Einbeziehung der lokalen Bevölkerung zur Zerstörung der Umwelt und der Lebensbedingungen und so zur Verschärfung von Armut und gesundheitlichen Beeinträchtigungen beitragen. Und nicht zuletzt gibt es Fälle, in denen Unter-

nehmen durch den Einsatz privater Militär- und Sicherheitsfirmen oder die Unterstützung von staatlichen Sicherheitskräften oder durch die Lieferung von Rüstungsgütern zur Eskalation beigetragen haben.

Dabei ist die Rolle von Unternehmen als Risikofaktor bis hin zur Beteiligung an Kriegen nicht nur auf die offensichtlichsten Branchen wie private Militär- und Sicherheitsdienstleister oder die Rüstungsindustrie beschränkt. Natürlich ist das Geschäftsmodell der Rüstungsindustrie primär die Lieferung der Werkzeuge für Kriege, gewaltsam ausgetragene Konflikte und Repression – von Kampfflugzeugen über Panzer, Kriegsschiffen, so genannten Kleinwaffen und leichten Waffen, Rüstungselektronik und Sensorik, Munition bis hin zu Gummigeschossen, Tränengasgranaten, Elektroschockern und Überwachungshard- und Software, um nur einen begrenzten Ausschnitt des *Handels mit Tod und Zerstörung* zu illustrieren. Und mit diesem Geschäftsmodell ist die Rüstungsindustrie natürlich ein zentraler Risikofaktor, zumal ihr Börsenwert sich an der Konfliktlage orientiert, wie sich an den ab Ende Februar 2022 rasant gestiegenen Aktienkursen nach Beginn des völkerrechtswidrigen russischen Angriffskrieges gegen die Ukraine zeigt.

Gleiches gilt auch für die so genannten privaten Militär- und Sicherheitsdienstleister, die vom Outsourcing militärischer Dienstleistungen bis hin zur Kriegsführung durch die Staaten leben und im Grunde nichts anderes als Söldnergruppen sind. Früher waren das beispielsweise *Executive Outcomes* aus Südafrika oder *Sandline International* aus Großbritannien, die Ende des letzten Jahrhunderts vorwiegend in Afrika aktiv waren oder *Blackwater* aus den USA unter anderem im Irak. Heute ist vor allem die russische *Wagner-Gruppe* in den Schlagzeilen, die nicht nur in der Ukraine, sondern auch in afrikanischen Staaten wie Libyen, Mali oder der Zentralafrikanischen Republik aktiv ist und immer wieder für Brutalitäten, Übergriffe und Rechtsverstöße verantwortlich sein soll.

Ein großer Risikofaktor sind auch Unternehmen der extraktiven Industrie, deren Tätigkeiten häufig mit der Zerstörung von Umwelt und Lebensbedingungen, mit der Einschränkung der Rechte indigener Völker, massiver Verteilungsungerechtigkeit und so mit Armutsverschärfung verbunden sind. Ein Beispiel dafür sind die Aktivitäten von Shell in Nigeria, so haben Amnesty International und andere Organisationen seit Jahrzehnten Beweise über die Beteiligung von Shell an Menschenrechtsverletzungen, Umweltzerstörung und Korruption gesammelt und öffentlich gemacht. Und die Recherchen von Amnesty International gemeinsam mit African Ressources Watch zu den katastrophalen Bedingungen und von Kinderarbeit beim Abbau von Kobalterz im handwerklichen Kleinbergbau in der Demokratischen Republik Kongo haben einmal mehr deutlich gemacht, dass auch die Firmen eine Mitverantwortung haben, in deren Elektroautos oder Mobilgeräten am Ende Akkus mit dem Kobalt aus solchen Quellen stecken.

Eine weitere Branche mit hohem Eskalationspotential ist die Infrastruktur- und Bauindustrie, deren Projekte häufig mit Zwangsräumungen und der Vertreibung der bisherigen Einwohner:innen unter Einsatz staatlicher oder privater Sicherheitskräfte ohne oder nur mit zu geringen Entschädigungen verbunden sind.

Auch die Lebensmittel- und Getränkeindustrie ist vielfach für Menschenrechtsverstöße bekannt, so beispielsweise für Missachtung gewerkschaftlicher Rechte, Gesundheitsgefährdung durch den Einsatz von Agrochemikalien, Unterlaufen existenzsichernder Löhne bis hin zu Zwangsarbeit auch für Kinder auf Plantagen.

Ein anderes Beispiel ist die Geschäftspolitik von Unternehmen der pharmazeutischen Industrie aktuell während der Covid-19-Pandemie, die in der Praxis den allgemeinen globalen Zugang zu Impfstoffen und Medikamenten eingeschränkt haben.

Und nicht zuletzt sind Unternehmen der IT-Branche immer wieder ein Risikofaktor: So beispielsweise, wenn sie ihre Produkte unter schlechten Arbeitsbedingungen und Einschränkung von Gewerkschaftsrechten produzieren lassen, aber auch, wenn sie Hard- und Software zur Überwachung an autoritäre Staaten liefern oder diese technisch unterstützen und so Beiträge zur Repression und damit zur Konfliktverschärfung leisten.

4. Unternehmen und Krieg – Teil der Lösung?

Angesichts der Vielzahl von Negativbeispielen erscheint es fraglich, ob Unternehmen nicht nur Risikofaktor, sondern vielleicht doch auch Teil einer Lösung sein können, ob sie einen Beitrag zur Konfliktprävention, zur Deeskalation und zur Stabilisierung nach Konflikten leisten könnten. Dennoch gibt es seit geraumer Zeit eine Diskussion, wie das tatsächlich erreicht werden könne und dabei gibt es auch Unternehmen, die nicht mehr ein Teil des Problems sein wollen. Erste Ansätze waren dabei freiwillige Maßnahmen wie Verhaltenskodices bis hin zu Regelungsvorschlägen für ganze Branchen, die Verpflichtung auf internationale Leitlinien und Normen, wie beispielsweise die OECD-Leitsätze für multinationale Unternehmen[4], freiwillige Zertifizierungen oder auch verstärkte Einbeziehung lokaler Gemeinschaften bei geplanten Aktivitäten. Ergänzt werden könnten solche Schritte um mehr Transparenz bei den Finanzflüssen verbunden mit einer gerechten Verteilung der Gewinne, einer sorgfältigen konfliktsensitiven Risikoabschätzung bei geplanten Projekten, Förderung rechtsstaatlicher und zivilgesellschaftlicher Initiativen, sozial verantwortlichen Investitionen und Abschätzung möglicher Auswirkungen der Unternehmenstätigkeit auf Menschenrechte, Umwelt und Klima.

Grundsätzlich gibt es also eine Vielzahl möglicher Maßnahmen und Schritte, der Werkzeugkasten für die Unternehmen steht weit offen und sie hätten die Möglichkeit, Risiken deutlich abzumildern und ihren möglichen Beitrag zu Konflikten zu minimieren.

Wichtigstes Werkzeug sind dabei die aus den UN-Leitprinzipien abgeleiteten menschenrechtlichen Sorgfaltspflichten. Allerdings stellt sich immer wieder heraus, dass allein ein freiwilliger Ansatz keine durchgreifenden Verbesserungen erzielen kann. Zu wenige Unternehmen haben sich tatsächlich der Verantwortung gestellt und entsprechende Maßnahmen ernsthaft umgesetzt. Auch wenn es in wenigen Fällen tatsächlich zu Verbesserungen gekommen ist, blieb es am Ende Stückwerk, und immer wieder ist es bei vollmundigen Ankündigungen in Hochglanzbroschüren geblieben, während weltweit Menschen weiter unter Übergriffen, Krisen, gewaltsamen Konflikten und Kriegen leiden.

5. Standards für Unternehmenshandeln – Beitrag zum Frieden?

Ausgehend von der Erkenntnis, dass freiwillige Änderungen im Verhalten von Firmen nach allen Erfahrungen nicht zu durchgreifenden Verbesserungen der Situation führen können und werden, weil sich am Ende zu wenige beteiligen, kann die Konsequenz nur heißen: Die Staaten müssen die Verpflichtungen der Unternehmen für die Menschenrechte verbindlich und umfassend regeln – damit die Wirtschaft nicht weiter ein Risikofaktor für Menschenrechte und für die Fortführung und Eskalation von Krisen und Konflikten bleibt. Eine solche gesetzliche Regelung muss die menschenrechtlichen, umwelt- und klimabezogenen Sorgfaltspflichten der Unternehmen umfassend regeln – entlang der gesamten Wertschöpfungskette. So sollten die folgenden Eckpunkte aufgenommen werden:

- Unternehmen müssen ihre Verantwortung anerkennen und eine Grundsatzerklärung zur Respektierung der Menschenrechte erlassen.
- Unternehmen müssen menschenrechtliche Risiken und mögliche negative Auswirkungen ihrer Geschäftstätigkeit auf die Menschenrechte entlang der ganzen Wertschöpfungskette erfassen.
- Unternehmen müssen Maßnahmen ergreifen, die erfassten Risiken zu minimieren beziehungsweise auszuschließen sowie negative Auswirkungen auf die Menschenrechte zu beenden, zudem müssen sie Vorsorge treffen, damit keine neuen Risiken entstehen.
- Unternehmen müssen ihre Risikoerfassung, Risikovorsorge und daraus abgeleitete Maßnahmen umfassend öffentlich zugänglich transparent machen.
- Unternehmen müssen die Beteiligung von Betroffenen sicherstellen und leicht zugängliche Beschwerdemechanismen etablieren.
- Unternehmen müssen für Übergriffe haften und Entschädigungen für Verletzungen und Übergriffe sicherstellen.

In Deutschland war der erste Ansatz dafür das 2021 verabschiedete Lieferkettensorgfaltspflichtengesetz (LkSG)[5], das Unternehmen verpflichtet, in ihren Lieferketten menschenrechtliche und umweltbezogene Sorgfaltspflichten zu beachten, um den im Gesetz definierten menschenrechtlichen und umweltbezogenen Risiken vorzubeugen, sie zu minimieren oder aber die Verletzung menschenrechtsbezogener oder umweltbezogener Pflichten zu beenden. Grundlage sind internationale Menschenrechtsübereinkommen und Vereinbarungen zum Umweltschutz, wobei die menschenrechtlichen Aspekte deutlich umfassender definiert werden als Umweltaspekte. Allerdings weist das LkSG trotz guter Ansätze eine Reihe von Defiziten auf: Unter anderem wird es nur für relativ große Unternehmen wirksam, beschränkt sich nur auf die Lieferkette und auch dort im Wesentlichen nur auf unmittelbare Zulieferer, außerdem fehlt eine Haftungsregelung. Dennoch ist es ein erster wichtiger Schritt, der durchaus zu ersten Verbesserungen führen kann.

Zurzeit wird auch auf der europäischen Ebene ein Lieferkettengesetz erarbeitet, es liegt ein Entwurf für eine *Richtlinie des Europäischen Parlaments und des Rates über die Sorgfaltspflichten von Unternehmen im Hinblick auf Nachhaltigkeit* vor, der aktuell in den europäischen Institutionen beraten wird. Der Entwurf geht in einigen Punkten weiter als das deutsche LkSG, auch wenn er noch nicht perfekt ist. Widerstand dagegen gibt es teilweise von politischer Seite, vor allem aber von Unternehmen und ihren Interessenvertretungen, den großen Wirtschaftsverbänden. Daher bedarf es sicher weiterer öffentlicher Aufmerksamkeit und Aktivitäten, um zu verhindern, dass dieser Entwurf am Ende verwässert wird. Das wird in Deutschland durch die *Initiative Lieferkettengesetz* betrieben, die als Dach vieler Nichtregierungsorganisationen eine Kampagne für ein starkes europäisches Lieferkettengesetz führt[6].

Mathias John

Dr. **Mathias John**, Jahrgang 1957, arbeitet seit 1980 ehrenamtlich bei Amnesty. Er ist Sprecher der Koordinationsgruppe Wirtschaft, Rüstung und Menschenrechte und war von 2015 bis 2021 im Vorstand von Amnesty International Deutschland zuständig für Länder- und Themenarbeit.

Einer seiner Arbeitsschwerpunkte ist die Untersuchung von Auswirkungen von Rüstungstransfers einschließlich Dual Use-Exporten auf die Menschenrechte. Als Rüstungsexperte hat Mathias John an zahlreichen Untersuchungen und Berichten von Amnesty International mitgearbeitet und in Deutschland maßgeblich die erfolgreiche Kampagne für den internationalen Waffenhandelsvertrag begleitet.

Im Bereich menschenrechtliche Unternehmensverantwortung begleitet Mathias John die nationale und internationale Diskussion um verbindliche Regeln und menschenrechtliche Sorgfaltspflichten entlang der Wertschöpfungsketten intensiv seit Anfang der 90er Jahre. Schwerpunkt sind dabei Verantwortung von Wirtschaftsunternehmen für Menschenrechte, (Ressourcen-) Konflikte und wirtschaftliche Aktivitäten sowie die aktuellen Kampagnen für wirksame Lieferkettengesetze auf nationaler und internationaler Ebene.

6. Fazit

Unternehmen und Banken sind wichtige globale Akteure mit einen hohen Risikopotential für die Verschärfung von Krisen und Konflikten und die Unterstützung von Kriegen. Die Verwicklung von wirtschaftlichen Akteuren in Menschenrechtsverletzungen kann zur Eskalation von Konflikten führen, auf der anderen Seite kann die Einhaltung menschenrechtlicher Sorgfaltspflichten in Wertschöpfungsketten auch einen maßgeblichen Beitrag zur Prävention, Deeskalation und Stabilisierung leisten. In diesem Sinne umfassend können menschenrechtliche Sorgfaltspflichten jedoch nur dann wirksam werden, wenn sie tatsächlich von allen wirtschaftlichen Akteuren in allen ihren Geschäftsfeldern entlang ihrer jeweiligen Wertschöpfungsketten umgesetzt werden. Das ist nur durch rechtlich verbindliche Regelungen zu erreichen, wobei das deutsche Lieferkettensorgfaltspflichtengesetz und die geplante europäische Sorgfaltspflichten-Richtlinie erste gute Ansätze sind. Am Ende muss aber eine globale Regelung beispielsweise als verbindliche Konvention der Vereinten Nationen stehen, um die notwendigen verbindlichen globalen Spielregeln für alle zu verankern!

Anmerkungen

1 *Informationen zu den UN-Leitprinzipien siehe beispielsweise hier: https://www.cora-netz.de/themen/nap/un-leitprinzipien/ (abgerufen zuletzt am 25.02.2023)*
2 *„Schutz, Achtung und Abhilfe"*
3 *Konfliktbarometer HIIK 2021: https://hiik.de/konfliktbarometer/aktuelle-ausgabe/ (abgerufen zuletzt am 25.02.2023)*
4 *https://www.oecd.org/berlin/publikationen/oecd-leitsaetze-fuer-multinationale-unternehmen.htm (abgerufen zuletzt am 25.02.2023)*
5 *https://www.bgbl.de/xaver/bgbl/start.xav#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s2959.pdf%27%5D__1677363184570 (abgerufen zuletzt am 25.02.2023)*
6 *https://lieferkettengesetz.de/ (abgerufen zuletzt am 25.02.2023)*

CC BY

Niels Jansen

Frieden, Technik & Zukunftsforschung am Beispiel Predictive Policing

Zukunftsforschung ist ein schillernder Begriff und ein breit gefächertes Feld, auf dem sich Vertreter:innen der unterschiedlichsten Ausrichtungen tummeln. Man bewegt sich zwischen Trendgurus und Superforecastern, dem Kampf um die Anerkennung als wissenschaftliche Disziplin und eher praxisorientierten Ansätzen aus dem weit gefassten Designbereich. Der Text nimmt die Perspektive der kritischen Zukunftsforschung ein. Von diesem Standpunkt aus soll im Folgenden das sozio-technische bzw. sozio-informatische Phänomen des ‚Predictive Policing' (PP) betrachtet werden.

Zukunftsforschung in a nutshell

Zu Beginn noch mal einige Worte zur Zukunftsforschung. Entgegen der irrigen Annahme, Zukunftsforscher:innen wollten DIE Zukunft vorhersagen, ist vielmehr das Ziel, den Blick für vielfältige unterschiedliche Zukünfte zu schärfen. Statt EINE zukünftige Gegenwart zu prognostizieren sollen mehrere gegenwärtige Zukunftsbilder entworfen, analysiert und kritisch reflektiert werden. Statt einer zukünftigen Gegenwart sind also gegenwärtige Zukünfte der Forschungsgegenstand.

Die Zukünfte können je nach Ansatz und Forschungsziel im Spektrum von wahrscheinlich über möglich bis hin zu utopischen oder dystopischen reichen. Während der wahrscheinliche Pfad – das Kind der Prognostik – nur in einem eng begrenzten Zeithorizont verlässlich arbeiten kann, werden bei explorativen Ansätzen größere Zeiträume von zehn, fünfzig oder mehr Jahren in den Blick genommen.

Mit Zukunftsstudien soll Orientierungs- und Handlungswissen für heute generiert werden, damit wir bessere Entscheidungen treffen können, wie wir z. B. Technikzukünfte gestalten wollen und welche unintendierten Nebenwirkungen uns dabei begegnen könnten[1].

Bei aller (strategischen) Vorausschau bleiben die entwickelten Zukunftsbilder aber immer kontingent. Sie könnten so eintreten, müssen es aber nicht. Der Möglichkeitsraum, durch eigenes aktives Handeln zu einer wünschenswerten Zukunftsentwicklung beizutragen, bleibt immer offen. An diesem Punkt setzen auch die normativen Zukünfte an: Wie sehen wünschenswerte Zukunftsbilder aus? Für wen sind sie eventuell auch nicht wünschenswert (Beispiel: Autofreie Städte für mobilitätseingeschränkte Menschen)? Welche Zukünfte möchten wir verhindern (Beispiel: ‚Limits to Growth'-Szenarien von 1972)?

Eine gern genutzte Darstellung, um die Idee der vielen möglichen Zukünfte zu visualisieren, ist der Zukunftstrichter (siehe Abbildung 1). Je weiter der Blick in die Zukunft gerichtet wird, desto größer sind die Möglichkeiten für alternative – und damit gestaltbare – Entwicklungen.

Methoden und Geschichte der Zukunftsforschung

Um sich nun den unterschiedlichen Zukunftsbildern zu nähern und diese nachvollziehbar zu entwickeln, bedient sich die Zukunftsforschung einer Vielzahl unterschiedlicher Methoden und Techniken. Die bekannteste ist dabei vermutlich die Szenario-Technik; aber auch die Delphi-Methode, also Expert:innenbefragungen mit mehreren Befragungsrunden, ist beliebt. Auch agentenbasierte Modellierungen können wichtige Erkenntnisse zu emergenten Phänomenen liefern.

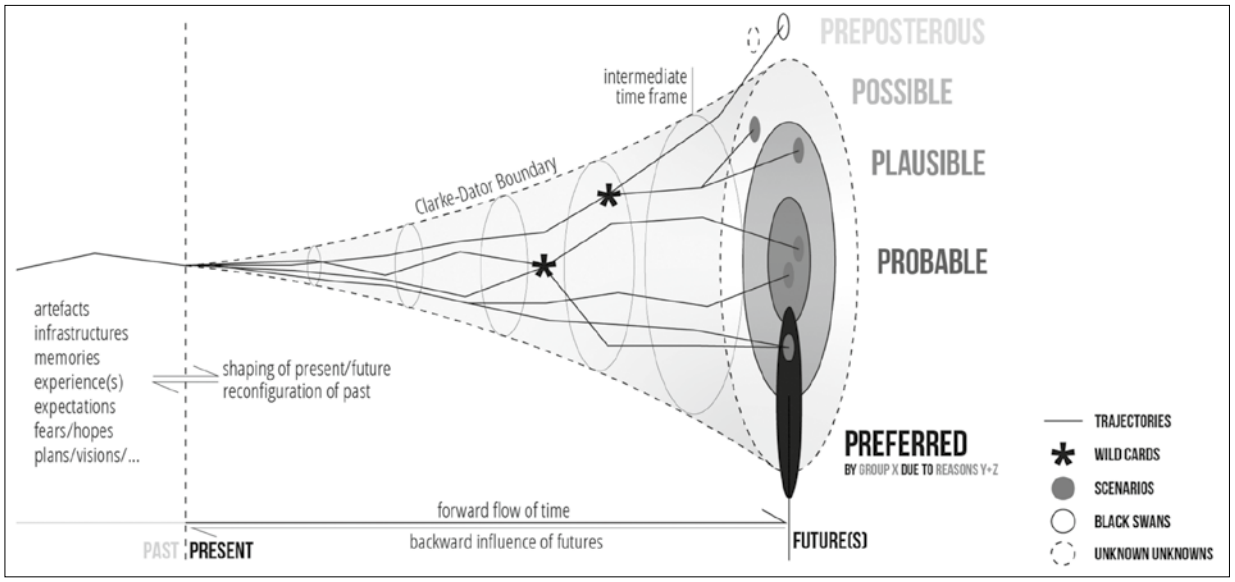


Abbildung 1: Der Zukunftstrichter *Quelle: Gall et al. (2022)*

Seit einigen Jahren werden die Grenzen zu anderen Disziplinen, wie der Semiotik, der Komplexitäts- und Transformationsforschung zunehmend durchlässig. Auch kreative und interaktive Methoden mit Bezügen zu Designdisziplinen, Gaming oder Science Fiction erweitern das Spektrum zusätzlich.

Den Begriff der Futurologie prägte Ossip K. Flechtheim bereits 1943. Die weitere Entwicklung der Zukunftsforschung erfolgte dann zunächst vorrangig in den USA. Die RAND-Corporation gilt als einer der wichtigsten Think-Tanks und war maßgeblich für die Entwicklung und Verbreitung einiger Methoden der Zukunftsforschung verantwortlich, insbesondere der Szenario-Technik. Weniger ruhmreich sind die Arbeiten von Herman Kahn, dem Leiter der RAND-Corporation, zum *war-gaming*, die die Doktrin der *Mutual Assured Destruction* (MAD) begründeten.

Im (bundes)deutschen Kontext ist die Studiengruppe für Systemforschung zu nennen, die in den 1970er- und 1980er-Jahren mit planungs-euphorischen Ansätzen bis in die engsten Zirkel der bundesdeutschen Politik vorgedrungen ist. Alles schien berechenbar und von einem Techno-Optimismus getrieben. Zu den bekanntesten Vertretern gehören Wolf Häfele, auch als Vater des Schnellen Brüters bekannt und der Kybernetiker und Informationstheoretiker Karl Steinbuch. Letzterer arbeitete an künstlichen neuronalen Netzen und wandte sich später den Neuen Rechten zu.

Da war es wenig verwunderlich, dass sich die kritischeren Vertreter:innen der Kybernetik (z. B. Frederik Vester) später von diesen Strömungen lossagten. Und sich mit Robert Jungk eine stark normativ orientierte Strömung mit einem starken Fokus auf partizipative Ansätze in der deutschen ‚Futurologie' entwickelte.[2]

Mittlerweile ist die universitäre Zukunftsforschung in Deutschland offiziell als ‚kleines Fach' anerkannt. Auch international wird Futures Studies an diversen Hochschulen von Hawaii über Turku bis nach Stellenbosch und Taipeh angeboten.

Nach diesem kleinen Exkurs in das sozialwissenschaftliche Zukünfte-Biotop bietet sich die oben erwähnte Science Fiction als gute Brücke zu Predictive Policing an.

Predictive Policing – Versuch einer Begriffsklärung

Die öffentliche Vorstellung von Predictive Policing ist heute immer noch stark durch den Film ‚Minority Report' geprägt. Das zeigt sich unter anderem auch in der Bildsprache, die zur Illustration von Websites, Artikeln zum Thema oder zur Bewerbung von Software selbst genutzt wird. Der Film basiert auf einer Kurzgeschichte von Philip K. Dick aus dem Jahre 1956. Darin werden vom Autor wichtige Fragen aufgeworfen, auf die ich später noch zu sprechen komme.

Ähnlich dem Begriff der Zukunftsforschung ist Predictive Policing ein Sammelbegriff für eine große Zahl unterschiedlichster Ansätze. Die erste wichtige Unterscheidung ist die zwischen PP als technischem System und als sozio-technischem Prozess. Während man die PP-Systeme auf rein technischer Ebene isoliert betrachten kann, ist PP als Prozess notwendigerweise immer in einen größeren gesellschaftlichen Kontext eingebunden und dort wirksam.

Typologie von Predictive Policing Systemen

Werfen wir also einen Blick auf die unterschiedlichen algorithmischen Systeme und die zugrundeliegenden Theorien und Annahmen. In einem ersten Schritt muss zwischen Systemen, die raum-zeitliche und solchen, die personenbezogene Analysen liefern, unterschieden werden. Letztere werden in Deutschland nur vom BKA als RADAR-iTe[3] und RADAR-rechts[4] genutzt. In den USA haben sie beispielsweise als Strategic Subject List in Chicago traurige Berühmtheit erlangt.

Deutlich verbreiteter sind die raum-zeitlich orientierten Analyseinstrumente, also solche, die versuchen, Vorhersagen über die Eintrittswahrscheinlichkeit von Delikten in bestimmten Gebieten zu einem in der Zukunft liegenden Zeitpunkt zu treffen.

Unabhängig von Raum-Zeit- oder Personenbezug gibt es grob drei unterschiedliche Kategorien von Systemen. Die erste sind theoriebasierten Anwendungen, die auf Basis von Polizeidaten aus der

Vergangenheit zukünftige Entwicklungen modellieren. Dazu werden bekannte kriminologische Hypothesen und sozialwissenschaftliche Theorien informatisch operationalisiert. Die eingesetzten Algorithmen sind dabei aber nicht zwangsläufig auf kriminologischer Forschung begründet. So nutzt beispielsweise die bekannte Software der Unternehmens PredPol – das seit 2021 unter dem Namen Geolitica firmiert – Algorithmen, die auf einer Modellierung zur Vorhersage von seismischen Nachbeben basieren. Neben der Frage nach technischer Übertragbarkeit halte ich die Analogie von Kriminalität und Naturkatastrophen für problematisch.

Die zweite Gruppe bilden Systeme, die stark auf behavioristischen Grundannahmen basieren und neben den konkreten Delikten die Rahmenbedingungen stärker berücksichtigen. Darunter fallen der Routine-Activity-Ansatz, der Lifestyle-Approach und Rational-Choice-Ansätze. Dabei wird davon ausgegangen, dass eine Reihe von objektiv beobacht- und messbaren Faktoren die Entstehung von Straftaten begünstigen oder gar determinieren. Mit Hilfe von heuristischen Methoden, Regressionsanalysen oder statistischen Modellierungen werden Analysen durchgeführt, um Risikoräume in Kombination mit dem Faktor Zeit zu identifizieren. Die Methode wird als Risk-Terrain-Modelling (RTM) bezeichnet. Die Daten aus dem polizeilichen Kontext werden durch sozioökonomische, geographische oder andere raumzeitliche Daten ergänzt, denen Relevanz für die computergestützte Modellierung wahrscheinlicher Entwicklungen zugesprochen wird.

In die dritte Gruppe fallen Systeme, die Ansätze des maschinellen Lernens auf große, strukturierte und unstrukturierte Datenmengen anwenden. Dabei wird oft gänzlich auf eine kriminologische oder sozialwissenschaftliche Fundierung verzichtet. Die Datenquellen sind hier auch nicht begrenzt, so dass auch qualitativ zweifelhafte Angaben z. B. aus sozialen Netzwerken Einfluss finden können. Gerade eine überzeugende Datenqualität im Sinne der 4V (volume, variety, velocity, veracity) und eine transparente Ergebnisproduktion sind mit Blick auf den Aspekt der Rechtsstaatlichkeit im zivilisatorischen Hexagon zwingend erforderlich.

Die bekannteste Software in diesem Sektor ist mit Abstand das vom Unternehmen Palantir angebotene Produkt *Gotham*. In Deutschland kommt es aktuell unter dem Namen *Hessendata* zum Einsatz. Auch das bayerische Landeskriminalamt soll mit Palantir Software ausgestattet werden.

So weit also eine kleine – sicherlich nicht vollständigen – Typologie der gängigsten Software-Systeme, die aktuell nachweislich eingesetzt werden. Wenden wir uns nun Predictive Policing als Prozess zu.

Predictive Policing als Prozess

Unabhängig von den verschiedenen technischen und theoretischen Grundlagen muss betont werden, dass die informatischen Systeme selbst keine polizeilichen Maßnahmen durchführen. Vielmehr sind sie in Kombination mit den Sicherheitsbehörden als Soziotop, den bedienenden Operator:innen und schließlich auch den Polizeibeamt:innen, die für die Ausführung der abgeleiteten Einsatzstrategien zuständig sind, zu sehen. Es handelt sich also um ein sozio-technisches, genauer: ein sozio-informatisches System[5]. Hieran kann man gut sehen, dass es sich bei dem Prozess um „vorhersagebasierte Polizeiarbeit“[6] handelt, denn das tatsächliche Polizieren erfolgt durch agierende Personen auf Grundlage des von den technischen Systemen berechneten Input in das soziale System Polizei.

Dem gegenüber steht die oft geäußerte Fehlannahme, Predictive Policing sei die „Vorhersage von Straftaten“. Dies zu kritisieren und zurückzuweisen ist wichtig und berechtigt. Nur ein informierter Umgang mit Technologie kann verhindern, dass diese mit überzogenen Erwartungen im Sinne des Solutionismus aufgeladen oder als vermeintlich einfache technische Lösung (Technological Fix) für komplexe gesellschaftliche Problem präsentiert wird.

Die RAND-Corporation hat 2013 – gefördert vom National Institute of Justice – eine Studie zu Predictive Policing herausgegeben. Darin findet sich auch der „Prediction-Led Policing Business Cycle“ (siehe Abbildung 2).

Im oberen Teil der Grafik findet sich ein iterativer Prozess, der unter anderem Analyse und Datenaufbereitung beinhaltet. Nach Datenerhebung und Analyse folgen im dritten Schritt die konkreten polizeilichen Interventionen im öffentlichen Raum. Diese können unterschiedliche Formen annehmen: generisch, kriminalitätsspezifisch oder problemspezifisch.

Auf die Entwicklung der Systeme selbst und die Rahmenbedingungen, die zu ihrer Implementierung führen, wird in dieser schematischen Darstellung nicht eingegangen. Oft haben akute Ereignisse oder zumindest die Befürchtung größerer sicherheits-

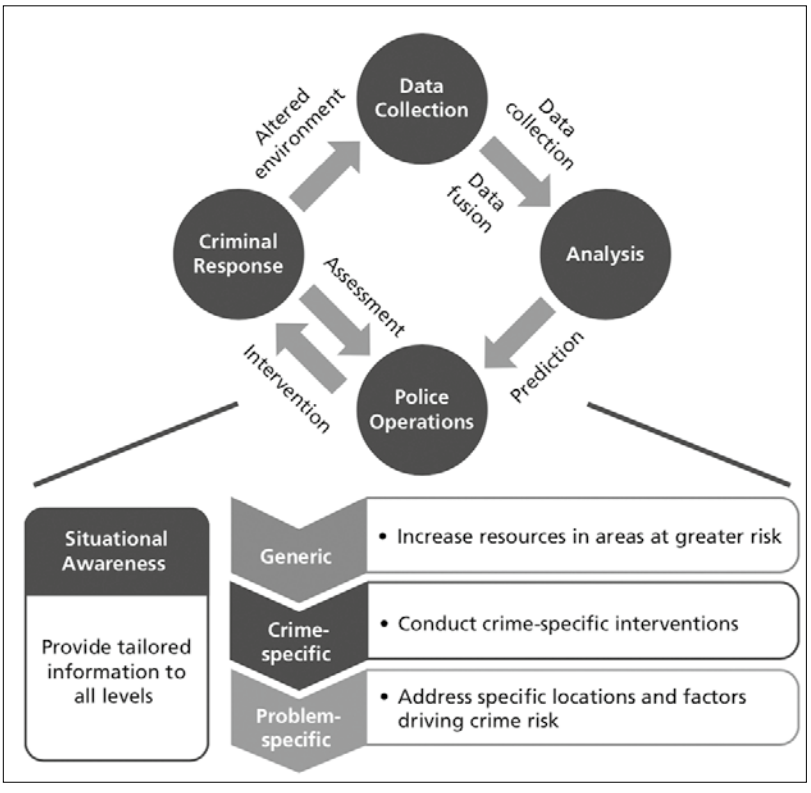


Abbildung 2: Prediction-Led Policing Business Process

relevanter Probleme aber eine große Wirkung auf den dargestellte Prozess. Der starke Anstieg von Wohnungseinbruchsdiebstählen in Deutschland um das Jahr 2009 herum hat sicherlich die Bereitschaft für den Einsatz solcher Systeme in Deutschland auf politischer Ebene erhöht.

In Schritt vier muss die Frage erlaubt sein, ob ein verändertes Verhalten der Kriminellen zwangsläufig ein Ergebnis des Einsatzes eines Predictive-Policing-Systems ist. Eventuell haben andere Faktoren und Einflüsse, die im Schaubild nicht berücksichtigt werden, viel mehr Auswirkungen gehabt? Oder durch das symbolträchtige Ausrollen von PP-Systemen konnte einfach nur der Eindruck einer subjektiven Sicherheit erweckt werden? Hier stößt die Wirkungsmessung schnell an ihre Grenzen.

Man muss der RAND-Studie zugute halten, dass sie gleich zu Beginn die Mythen und Fallstricke von PP benennen. Dazu gehört die Fiktion, der Computer ‚kenne' die Zukunft und diese sei mit möglichst komplexen – meist opaken – Systemen mit hoher Rechenleistung am Besten vorherzusagen. Auch die oben erwähnte Problematik fragwürdiger Datenqualität (S. 34, „dritte Gruppe") und die Überbewertung der Vorhersage gegenüber dem taktischen Nutzen für die konkrete Polizeiarbeit wird genannt.

Es entsteht der Eindruck, dass oft eine große Technikeuphorie bei weitgehender Ahnungslosigkeit über die Funktionsweise vorherrscht. Diese nimmt umso mehr zu, je weiter sich die Systeme von theoriebasierten hin zu datengetriebenen Ansätzen bewegen. Das ist umso besorgniserregender, da gerade die Machine-Learning-Ansätze eine Übertragung von Vorhersagealgorithmen aus dem privatwirtschaftlichen Kontext auf den Sicherheitsbereich darstellen. Was in der Vorhersage von Konsumentscheidungen funktioniert, sollte ja auch bei Kriminalität möglich sein. Mit diesem Versprechen bieten privatwirtschaftliche Unternehmen Softwarelösungen für staatliche Sicherheitsbehörden an, deren Funktionsweisen oft nicht nachvollziehbar sind. Sie nehmen damit zumindest indirekten Einfluss auf die Ausübung des staatlichen Gewaltmonopols. Diffundieren Technologien sonst eher aus dem Militär- und Sicherheitsbereich in die allgemeine Anwendung (GPS, ARPANET, …), haben wir hier den Fall einer Technologie-Diffusion in die Gegenrichtung.

Kritik der Kritik – Was sagt die Zukunftsforschung?

Ich möchte aber ein wenig Kritik an meiner eigenen Kritik üben. Bisher findet fast ausschließlich eine Diskussion um die technische Ausgestaltung der eingesetzten Software statt. Das ist notwendig, aber nicht hinreichend. Bei zu starkem Fokus auf die (informations-)technischen Aspekte laufen wir Gefahr, die Diskussion auf die Argumentationslogik der Herstellenden zu verengen. Sind geeignete Trainingsdaten verwendet worden? Ist die technische Ausgestaltung korrekt, vorurteilsfrei …? Waren die Analysen korrekt? Konnte durch den Einsatz technischer Artefakte die Effizienz oder die Effektivität der Polizeiarbeit erhöht werden? Waren die Analysen korrekt? Diese Fragen sind alle gut und berechtigt, greifen meiner Meinung nach aber zu kurz.

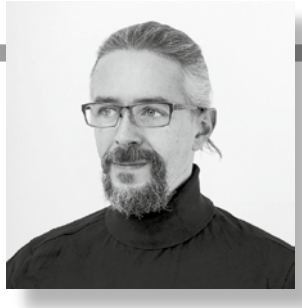
Das Zusammenspiel von Mensch und Technik und die zugehörigen sozialen und psychologischen Effekte werden meiner Ansicht nach immer noch zu oft vernachlässigt, auch wenn sie in letzter Zeit in den Science-&-Technology-Studies und der Technikphilosophie stärkere Beachtung finden.[7]

Die Mensch-Technik-Interaktion findet sich im gesamten Prozess, von den frühen Phasen der Entwicklung und Implementierung bis zu den nachgelagerten direkten und indirekten Wirkungen auf die Gesellschaft. Im Fall von PP-Systemen werden von privaten Firmen entwickelte Systeme in öffentlichen Institutionen zur Unterstützung der Wahrnehmung staatlicher Aufgaben eingesetzt. Die produzierten Risikoanalysen werden von geschulten Operator:innen in Dienst- und Einsatzplanungen überführt. So werden beispielsweise die von der Software definierten Risikogebiete stärker bestreift.

Durch das Polizieren vor Ort findet ein weiterer Transfer von der (geschlossenen) sozialen Sphäre der Sicherheitsbehörde in die (offene) soziale Sphäre der Öffentlichkeit statt. Dabei liegt die Vermutung nahe, dass die Wahrscheinlichkeitsaussagen der Systeme für die Polizist:innen im operativen Straßendienst durch den oben beschriebenen mehrstufigen Transferprozess und die damit einhergehende Ferne von der algorithmischen Prognoseerstellung den Anschein der Faktizität erhalten. In den Worten des Zukunftsforschenden: eine kontingentes Zukunftsbild wird als quasi-faktische Dystopie erzählt, die nur durch ein konkretes aktives Handeln der adressierten Mitarbeitenden von Sicherheitsbehörden abgewendet werden kann. Shoshana Zuboff beschreibt dieses Phänomen mit Blick auf den Überwachungskapitalismus als „Verlust des natürlichen Rechts auf das eigene Futur"[8]. Das ist insofern interessant, als dass nicht zuletzt Erfolge der prädiktiven Techniken im Konsumbereich die Überlegungen befeuert haben, Ähnliches auch auf den Sicherheitsbereich zu übertragen.

> *„[P]redictive policing operates with the logic of preemption, and it shows how the symbolic (the potential for crime) is carved out from the real (the spatio-tem-*

Niels Jansen



Niels Jansen ist wissenschaftlicher Mitarbeiter für Foresight und Partizipation bei Ellery Studio in Berlin. Er hat an der Freien Universität in Berlin Politikwissenschaft (Diplom) und Zukunftsforschung (M. A.) studiert. Beruflich war er unter anderem in der Denkfabrik Digitale Arbeitsgesellschaft des Bundesministeriums für Arbeit und Soziales beschäftigt. Sein Interesse gilt sozio-technischen Systeme, kreativer Wissensvermittlung, Science Fiction und sozialen Innovationen. Das alles mit dem Antrieb, einen kleinen Beitrag zur Gestaltung wünschenswerter Zukünfte zu leisten.

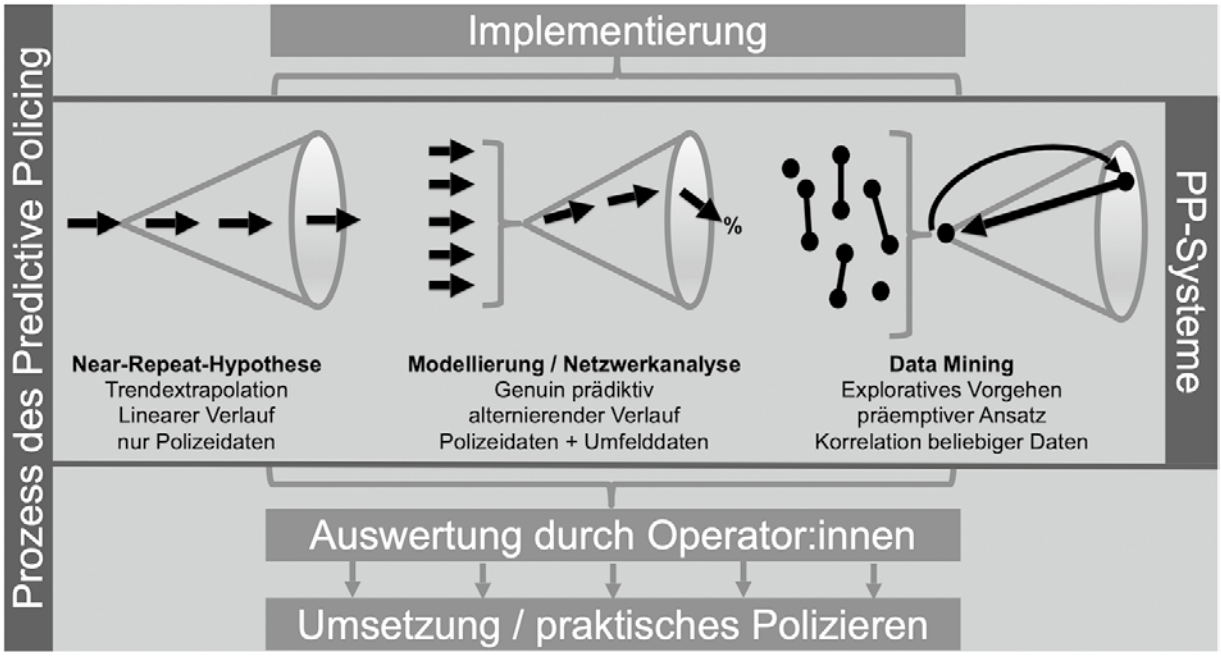


Abbildung 3: Prozess des Predictive Policing

poral data), and after algorithmic filtering, the symbolic (the presence of police) is incorporated into the real." (Karppi 2018, S. 6)

Das Zitat verdeutlicht nochmals die unterschiedlichen Wege, auf denen sich Symbolisches und Reales begegnen und auf Umwegen miteinander verschmelzen. Gerade in diesem Moment, in dem statistische Wahrscheinlichkeit, fiktive Annahmen bzw. ein kontingentes Zukunftsbild von der vermeintlichen Objektivität technischer Systemen überlagert werden, ist der Schritt zur Präemption nicht mehr weit.

Die Zukunft als Katastrophe wird als quasi unausweichlich dargestellt, WENN nicht im hier und jetzt vorauseilend interveniert wird. Die Zukunft wird dabei im Singular gefangen und Kontingenz nicht zugelassen.

Und hier sind wir wieder bei Philip K. Dick und dem *Minority Report*. Genau diese Problematik präemptiven Handelns wird in der Kurzgeschichte beschrieben. Mit all den Ambivalenzen und Ungewissheiten, die kontingente Zukünfte in sich tragen.

Präemption widerspricht aber ganz massiv der Unschuldsvermutung als Grundprinzip eines rechtsstaatlichen Strafverfahrens. Durch die Vorverlagerung in den Bereich des Gefahrenabwehrrechts der Polizeibehörden kann auf Grundlage einer abstrakten, von einem technischen System „begründeten" und damit „konkretisierten Gefahr" ein polizeilicher Eingriff gerechtfertigt werden. Diese Form des vorauseilenden Eingriffs wird fälschlicherweise mit Prävention verwechselt.

Im Gegensatz zur Präemption ist die Prävention aber deutlich weniger invasiv. Sie versucht, durch zurückhaltende Eingriffe und Verbote indirekt zu lenken. Dadurch sind kontingente Entwicklungen weiterhin möglich – im Sinne der Zukunftsforschung gibt es also noch mehrere Zukünfte, es wird aber der Versuch unternommen, normativ-gestaltend tätig zu werden (Abbildung 3).

Abschluss und Ausblick

Die diesjährige Konferenz wurde mit einem Vortrag zum zivilisatorischen Hexagon eingeleitet. Beim Einsatz von Predictive-Policing-Systemen können berechtigte Zweifel an der Vereinbarkeit mit mehreren der darin vereinten Bausteine geäußert werden. Das Gewaltmonopol wird zwar nicht dem Staat entzogen, der schwer zu kontrollierende Einfluss von privaten Anbietern prädiktiver Software sollte aber zumindest kritisch begleitet werden. Besonders kritisch ist die Gefahr präemptiver polizeilicher Maßnahmen. Als abschreckende Beispiele sei auf den Dritten Golfkrieg ab 2003 verwiesen, der ebenfalls mit präemptiver Logik begründet wurde. Auch in landespolizeilichen Regelungen mehrer Bundesländer finden sich zunehmend präemptiv anmutende Regelungen („drohende Gefahr").

Für Informatiker:innen und Zukunftsforscher:innen gilt also gleichermaßen eine Verantwortung für das eigene Schaffen. Dabei ist es egal, ob es sich um prädiktive Software oder um kreierte und präsentierte Zukunftsbilder handelt. Beide können Auswirkungen auf den zukünftigen Möglichkeitsraum haben. Im besten Fall können durch beide friedliche und optionsreiche Zukünfte befördert werden.

Referenzen

Andrejevic M (2017) To Preempt a Thief. International Journal of Communication, 11, 879–896.

Beck C, McCue C (2009) Predictive policing: What can we learn from Wal-Mart and Amazon about fighting crime in a recession? Police Chief Magazine, 76(11), 18–24.

Egbert S (2017) Siegeszug der Alghorithmen? Predcitive Policing im deutschsprachigen Raum. Aus Politik und Zeitgeschichte (APuZ), 32–33(2017), 17–23.

Egbert S (2018a) About Discursive Storylines and Techno-Fixes: The Political Framing of the Implementation of Predictive Policing in Germany. Euro-

pean Journal for Security Research, 3(2), 95–114. https://doi.org/10.1007/s41125-017-0027-3
Egbert S (2018b) Predictive Policing in Deutschland. Grundlagen, Risiken, (mögliche) Zukunft. In Baden-Württembergische Strafverteidiger e.V, Initiative Bayerischer Strafverteidigerinnen und Strafverteidiger, & Vereinigung Berliner Strafverteidiger (Hrsg.), Räume der Unfreiheit: 42. Strafverteidigertag Münster, 2.- 4. März 2018 (1. Auflage). Berlin: Redaktion & Verlag Thomas Uwer.
Egbert S, Krasmann S (2019a) Predictive Policing. Eine ethnographische Studie neuer Technologien zur Vorhersage von Straftaten und ihre Folgen für die polizeiliche Praxis. (S. 102) [Abschlussbericht]. Abgerufen von Universität Hamburg website: https://www.wiso.uni-hamburg.de/fachbereich-sowi/professuren/hentschel/forschung/predictive-policing/egbert-krasmann-2019-predictive-policing-projektabschlussbericht.pdf (Letzter Abruf: 29.01.2023)
Egbert S, Krasmann S (2019b) Predictive policing: Not yet, but soon preemptive? Policing and Society, 1–15. https://doi.org/10.1080/10439463.2019.1611821
Esposito E (2014) Die Fiktion der wahrscheinlichen Realität (3. Auflage; N. Reinhardt, Übers.). Frankfurt am Main: Suhrkamp.
Gall T, Vallet F, Yannou B (2022) How to visualise futures studies concepts: Revision of the futures cone, Futures 143, https://doi.org/10.1016/j.futures.2022.103024
Gerhold L, Holtmannspötter D, Neuhaus C, Schüll E, Schulz-Montag B, Steinmüller K, Zweck A Hg. (2015) Standards und Gütekriterien der Zukunftsforschung: Ein Handbuch für Wissenschaft und Praxis. Wiesbaden: Springer VS.
Karppi T (2018) "The Computer Said So": On the Ethics, Effectiveness, and Cultural Techniques of Predictive Policing. Social Media + Society, 4(2), 1–9. https://doi.org/10.1177/2056305118768296
Legnaro A, Kretschmann A (2015) Das Polizieren der Zukunft. Kriminologisches Journal, (02), 94 18. https://doi.org/10.3262/KJ1502094
Perry WL, McInnis B, Price CC, Smith SC, Hollywood JS (2013) Predictive policing: The role of crime forecasting in law enforcement operations. Santa Monica, CA: RAND.
Seefried E (2015) Zukünfte: Aufstieg und Krise der Zukunftsforschung 1945-1980. Berlin: De Gruyter Oldenbourg.
Zuboff S (2018) Das Zeitalter des Überwachungskapitalismus (B. Schmid, Übers.). Frankfurt New York: Campus Verlag.
Zweig KA, Krafft T, Klingel A, Park E (2021) Sozioinformatik: ein neuer Blick auf Informatik und Gesellschaft, München: Hanser.

Anmerkungen

1 *In der Informatik werden Methoden und Ansätze der Technikfolgenabschätzung – einer engen Verwandten der Zukunftsforschung – zunehmend integriert. Der erste Studiengang Sozioinformatik wird seit 2013 an der TU Kaiserslautern angeboten.*
2 *Eine ausführliche Darstellung der historischen Entwicklung der Disziplin bietet Seefried (2015) „Zukünfte: Aufstieg und Krise der Zukunftsfroschung 1945-1980". Zur Diskussion um wissenschaftlich fundierte Zukunftsforschung sei auf Gerhold et al. (2015) „Standards und Gütekriterien der Zukunftsforschung" verwiesen.*
3 *Regelbasierte Analyse potentiell destruktiver Täter zur Einschätzung des aktuellen Risiko – islamistischer Terrorismus – https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/PMK/Radar/radar_node.html*
4 *Regelbasierte Analyse potentiell destruktiver Täter zur Einschätzung des aktuellen Risiko der Begehung einer lebensgefährlichen, rechtsmotivierten Gewalttat – https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/PMK/PMKrechts/RADAR/radar_node.html*
5 *Zur Sozioinformatik siehe Zweig et al. (2021): Sozioinformatik.*
6 *Egbert (2017, 2018a)*
7 *Hier sei explizit auf die Arbeiten von Simon Egbert, Elena Esposito und Aldo Legnaro mit Andrea Kretschmann verwiesen.*
8 *Zuboff (2018), S. 36.*

Thea Riebe

Killerroboter und Künstliche Intelligenz: Regulierung und Design von Dual-Use Technologien

Innovationen der Informations- und Kommunikationstechnologie (IKT), wie zuletzt die Entwicklung von immer menschlicheren KIs, zeigen deutlich, wie sehr IKT viele Bereiche unseres Alltags verändern. IKT hat jedoch nicht nur ein transformatives Potential in zivilen, sondern auch militärischen Anwendungsbereichen. Technologien und Artefakte, welche sich in zivilen und militärischen Anwendungskontexten einsetzen lassen, werden als Dual-Use bezeichnet[1]. Dadurch kann Forschung und Entwicklung im zivilen Bereich auch Auswirkungen auf militärische Systeme haben. Um solche möglichen Technikfolgen und Risiken für den Missbrauch einer Technologie z. B. als Teil einer improvisierten Waffe[2] abschätzen zu können, wird Technikfolgenabschätzung (TA) durchgeführt[3]. Dual-Use-Risiken ergeben sich u. a. dadurch, dass sicherheitskritische Technologien einfach verbreitet oder verändert, sowie als Teil einer Waffe verwendet werden können.

Um die Risiken z. B. durch den Missbrauch von Dual-Use Technologien zu verhindern, gibt es verschiedene Ansätze, wie die Verbreitungskontrolle, Gestaltungsansätze und politische Maßnahmen. Dabei gibt es ein breites Spektrum an Maßnahmen, welches in der Forschung, der Entwicklung, der Produktion und dem internationalen Handel ansetzen. Bisher wurde Dual-Use-Risiken insbesondere in den Biowissenschaften und bei alternativer Produktion diskutiert[4]. Dieser lebens-wissenschaftliche Diskurs hat wesentlich dazu beigetragen, Methoden zur Beurteilung und zum Risikomanagement zu erarbeiten. Dual-Use von IKT umfasst ein breites Spektrum, von Robotik und autonomen Waffensystemen (AWS) zu Künstlicher Intelligenz, Cybersicherheit und der automatisierten Analyse öffentlich zugänglicher Daten. Die Entwicklung und Anpassung von Dual-Use IKT benötigt deshalb eine eigenständige Betrachtung, die auf den Erkenntnissen verwandter Dual-Use-Diskurse aufbaut.

Die Konferenz *make install PEACE – Impulse für den Frieden* vom 21.-23. Oktober 2022 beschäftigte sich mit zwei Leitfragen. Bei der ersten Frage ging es um die Regulierung (*Wie kann eine Technologie eingeschränkt werden, die den Frieden stört?*), und bei der zweiten Frage um die Gestaltung (*Wie kann eine Technologie gestaltet werden, um den Frieden zu fördern?*). Um diese Fragen aus der Perspektive der Dual-Use-Forschung zu adressieren, zeigt dieser Text an drei Beispielen auf, wie sich sicherheitskritische Technologien verbreiten können, welche Herausforderungen es bei der Regulierung gibt, und welche möglichen Ansätze die Forschung zu werteorientiertem und partizipativem Design bereithält.

Fälle

Künstliche Intelligenz und die Diffusion von Innovationen

Da Dual-Use-Technologien sowohl für militärische als auch für zivile Zwecke genutzt werden können, ist es für die frühzeitige Bewertung wichtig zu analysieren, wie Innovationen von militärischer und ziviler Forschung einander beeinflussen und wie Innovationen zwischen verschiedenen Anwendungsfeldern übertragen werden können. Ein aktuelles Beispiel ist KI, da sie als multifunktionell identifiziert wurde und durch ihre Anpassungsfähigkeit für verschiedene Zwecke adaptiert werden kann[5]. Besonders im Bereich der Steuerung, Bilderkennung und im Bereich der Assistenzsysteme gibt es Forschung und Entwicklung, welche sowohl für autonomes Fahren, als auch für autonome Systeme in militärischen Anwendungskontexten relevant ist. Wenn zivile Forschung hier auf militärische Systeme übertragen wird, stellt sich die Frage, inwiefern menschliche Kontrolle sukzessive unterlaufen werden kann.[6]

Um die Diffusion von Innovationen zu messen, gibt es verschiedene Ansätze der Wissensökonomie, welche messen, wie sich Wissen in Netzwerken ausbreitet. Solche Netzwerke können Zitationsnetzwerke von Wissenschaftler:innen sein, aber auch von Patenten oder soziale Netzwerke wie LinkedIn oder Twitter. In unserer Studie[7] haben wir Netzwerke von KI und Patenten von Waffen sowie die dazugehörigen Firmen in der EU analysiert. Das Ziel der Studie war, die Diffusion von KI-Innovationen in das Anwendungsfeld der Rüstungsproduktion zu untersuchen.

Um zu erkunden, inwieweit es Überschreitungen zwischen ziviler und militärischen KI-Innovationen gibt, haben wir 2.438 Zitationen von Patenten untersucht. Hierbei haben wir festgestellt, dass 524 Patente von KI-Patenten zitiert wurden und 1890 von Waffenpatenten. Jedoch blieben die Zitationen meist innerhalb der gleichen Klassifikation, wodurch wir keine Diffusion feststellen konnten. Wenn wir das Konzept von verantwortungsbewusster Forschung und Design mit einbeziehen, stellen wir auch fest, dass keine weitverbreiteten Wissenstransfers zwischen zivilen und Verteidigungssektoren beobachtet werden konnten. Wir konnten also keine Beweise finden, dass aufsteigende Technologien wie KI zuerst für zivile Zwecke genutzt werden und dann für militärische Zwecke[8].

Autonome Systeme und die Herausforderungen der Regulierung

Durch Dual-Use-Technologien entstehen Fragen nach der Verantwortung der Forscher:innen und Entwickler:innen für die Verwendung ihrer Technologien. Jedoch lässt sich diese Verantwortung nicht nur auf individueller Ebene verorten[9], sondern benötigt eine kollektive Entscheidung, welche durch organisationale Prozesse unterstützt wird. Für diesen Prozess braucht es Gesetze, Normen und Werte, an denen sich die Forschung und Entwicklung orientieren kann. Die Gestaltung von Gesetzen und Normen zur Regulierung und Beschränkung von Informations- und Kommunikationstechnologien (IKTs) gestaltet sich jedoch schwierig, wenn sie sich für viele verschiedene Zwecke nutzen lassen und die Forschung und Entwicklung aus wirtschaftlichen, strategischen oder gesellschaftlichen Gründen nicht eingeschränkt werden soll. Ein Beispiel hierfür sind autonome Waffensysteme (AWS), deren Regulierung seit Jahren stagniert[10].

Für die Regulierung ist insbesondere relevant, welche Funktionen von Waffen voll automatisiert sein sollten und welche nicht[11]. Auch bei teil-autonomen Systemen hat die Gestaltung der Mensch-Maschine-Interaktion einen großen Einfluss, wenn der Mensch entweder „in der Schleife", „an der Schleife" oder „außerhalb der Schleife" der Entscheidungsfindung beteiligt ist. Deswegen gibt es viele unterschiedliche Ansätze, welcher Grad an Autonomie genau von Regierungen und Herstellern gemeint ist, wenn die Waffen autonom genannt werden.

Um die normativen Vorschriften zur Regulierung von LAWS (Lethal autonomous weapon system) zu untersuchen, haben wir 43 Dokumente von einer Gruppe von Regierungsexperten zu tödlichen autonomen Waffensystemen untersucht[12]. Hierbei wollten wir die Werte, welche mit bedeutungsvoller menschlicher Kontrolle assoziiert werden, verstehen, und herausfinden, wie die Interaktionen zwischen Menschen und Maschine konzeptualisiert werden und welche Konflikte und Ansätze für die Regulierung sich dadurch ergeben[13]. Innerhalb der Dokumente wurde der Begriff „Autonomie" 168-mal gefunden, wovon 56-mal Autonomie als Funktion einer Waffe benutzt wurde. Hierbei fanden wir doppelt so viele Aussagen, welche eine hierarchische Beziehung zwischen Menschen und Technologie implizieren, wobei der Mensch über der Technologie steht, und diese steuert. Auch „Interaktion" als neutrale oder nicht-hierarchische Position wurde in 27 % der Fälle aller Aussagen über Mensch-LAWS-Interaktion genannt. Somit werden Mensch innerhalb des Expertenforums als überlegen zu Waffen angesehen.

Werte-gestütztes Design von Dual-Use-IKT

Die dritte Herausforderung entsteht in der Gestaltung von Dual-Use-Technologien.

Zukunftsorientierte Technikfolgenabschätzung beschäftigt sich mittlerweile nicht nur mit dem fertigen sozio-technologischen System, sondern auch mit der Vision und dem Design solcher Systeme[14]. Somit sollte sich Technikfolgenabschätzung von Dual-Use-Technologien auch mit technologischen Ambivalenzen und Gefahrenszenarios beschäftigen. Ein Beispiel hierfür sind Machine-Learning-basierte Analysesysteme für öffentlich-

zugängliche Quellen (*Open Source Intelligence, OSINT*). Diese werden immer häufiger genutzt, u. a. in der frühzeitigen Erkennung von IT-Sicherheitsbedrohungen[15]. Durch das Sammeln und Analysieren öffentlicher Quellen, u. a. in sozialen Netzwerken, kommen hierdurch auch ethische, rechtliche und soziale Anforderungen an den Schutz von Privatsphäre und Verhältnismäßigkeit zum Tragen.

Um ein solches OSINT-System für IT-Sicherheitsteams (*Cyber Emergency Response Teams*, CERTs) zu erstellen, haben wir den *Value-Sensitive-Design*-Ansatz[16] verwendet mit dem Ziel, alle relevanten Akteure in den Entwicklungsprozess einzubeziehen und systematisch mögliche Werte-Konflikte herauszuarbeiten. Dieser Ansatz sieht drei verschiedene Arten von Studien vor. Zunächst werden konzeptuelle Analysen durchgeführt, in denen alle relevanten direkten und indirekten Stakeholder identifiziert werden. Danach werden die Stakeholder in der empirischen Phase zu ihren Werten, Anforderungen und Nutzungsszenarien befragt. Schließlich wird auf dieser Basis ein Prototyp entwickelt, welcher dann in technischen Evaluationen überprüft wird. Im optimalen Fall durchläuft die Entwicklung mehrere Iterationen zur Verbesserung des Prototyps.

Zur Identifikation relevanter Technologien und Anwendungsszenarien haben wir systematisch alle Publikationen verglichen (N = 73). Hier zeigte sich, dass 74 % der Systeme zur Erkennung von IT-Sicherheitsbedrohungen entwickelt wurden (*Cyber Threat Intelligence*). Meist waren Strafverfolgungsbehörden die angedachten Nutzer (n = 58). Bei Projekten, bei denen die Finanzierung angegeben wurde, wurden 38 von zivilen und 11 von militärischen Sicherheitsbehörden finanziert. Die technologischen Merkmale zielten insbesondere darauf ab, öffentliche Daten zu sammeln (in 44 Publikationen) und neue Cyber-Gefahren zu entdecken (in 36 Publikationen). Twitter war dabei bisher die am häufigsten genutzte Plattform[17]. Von den 73 betrachteten haben nur 11 Publikationen ethische, soziale oder rechtliche Auswirkungen genannt. Zur Gestaltung eines OSINT-Systems für die IT-Sicherheit haben wir Interviews (N = 24) und einen Fokusgruppen-Workshop (N = 7), um CERTs in Deutschland und deren organisatorische Struktur, Bedürfnisse und Werte zu erfassen[18], durchgeführt. Um auch die Bürger:innen einzubinden, wurde eine repräsentative Umfrage (N=1093) durchgeführt, welche nach Faktoren für die Akzeptanz von OSINT-Systemen gefragt hat[19]. Aufgrund unserer Ergebnisse haben wir einen Beitrag zur Datenminimierung mit gleicher Effizienz zur Sicherheitsgewährleistung geleistet[20].

Zusammenfassung und weiterführende Arbeiten

Die Risiken durch das Dual-Use-Potential einer Informationstechnologie sowie deren Umgang hängt von verschiedenen Faktoren ab. Nach Tucker[21] gehören dazu Abwägungen, wie leicht eine Technologie zugänglich und missbrauchbar ist, und welchen potenziellen Schaden diese Verwendung anrichten kann. Dem gegenüber steht die Abwägung, wie leicht sich Maßnahmen zum Umgang und zur Regulierung umsetzen lassen, z. B. dadurch, dass eine Technologie sich in vielen oder wenigen Anwendungsfeldern verwenden lässt, ob sie eher in der Grundlagen- oder Anwendungsforschung steckt, und wie sie sich international verbreitet. Für diese Eigenschaften können dann Maßnahmen getroffen werden, welche selbst einer Kosten-Nutzen-Kalkulation unterliegen[22]. Zum verantwortungsvollen Umgang mit Dual-Use-Risiken können sowohl Individuen als auch Organisationen und Staaten beitragen.

Die FIfF-Konferenz 2022 beschäftigte sich mit zwei Leitfragen, welche den Umgang aus zwei Perspektiven betrachten. Die erste Frage untersuchte die Regulierung (*Wie kann eine Technologie eingeschränkt werden, die den Frieden stört?*), und die zweiten Frage (*Wie kann eine Technologie gestaltet werden, um den Frieden zu fördern?*) die Gestaltung von Technologien. Für beide Fragen hat die Forschung zur Bewertung von Dual-Use-Risiken weiterführende Ansätze.

Governance von Dual-Use-Technologien

Die Regulierung und Einschränkung von Technologien kann auf allen beteiligten Ebenen passieren und muss nicht immer durch gesetzliche Verbote erfolgen. Insbesondere wenn Technologien in multiplen Kontexten angewendet werden und sich noch stark entwickeln, ist es besser, in einem inklusiven Diskurs das Bewusstsein für die Risiken zu stärken und gemeinsame Normen zu entwickeln, die mehr oder weniger formalisiert sein können. Ein Beispiel ist hier der Diskurs um *Trustworthy AI* oder *AI4People*.[23] Zivilgesellschaftliche Akteure wie Vereine und Maker-Spaces, aber auch Wissenschaftler:innen können in diesem Prozess eine wichtige Rolle erfüllen und im Austausch mit Unternehmen und politischen Entscheidungsträger:innen Normen, Strategien und Methoden zur Überprüfung erarbeiten. Auch im Bereich der autonomen Waffensysteme kommen zivilgesellschaftlichen Organisationen, wie der *Campaign to Stop Killer Robots*[24] (Kampagne zur Verhinderung von Killer-Robotern), wichtige Funktionen zu, wie dem Erarbeiten von Normen und der Schaffung von Öffentlichkeit. Auch wenn einzelne Forscher:innen und Ingenieur:innen immer noch in der Verantwortung sind, so ist es auch wichtig, diese nicht für alle möglichen Nutzungen von Technologien individuell verantwortlich zu machen[25], sondern diese kollektiv zu diskutieren, um gemeinsam Verantwortung für den Umgang mit Dual-Use-Risiken zu übernehmen. Es werden sich Anwendungsfälle und Dual-Use-Risiken ergeben, welche unvereinbar mit dem humanitären Völkerrecht und den Grundrechten sind, und welche daher explizit verboten werden sollten. Hier können zivilgesellschaftliche Akteure und die Wissenschaft dabei unterstützen, Verfahren und Methoden zu entwickeln, welche bei der Nicht-Verbreitung unterstützen und diese überwachen.

Design von Dual-Use-Technologien

Darüber hinaus kann es sinnvoll sein, vielversprechende Dual-Use-Technologien werte-orientiert und partizipativ zu erforschen und zu entwickeln. Hierzu bieten sich Ansätze der partizipativen Design-Forschung, wie das *Value Sensitive Design*[26], besonders an. Ihr großer Vorteil ist nicht nur die Beteiligung vieler Akteure, die dadurch iterativ die Prototypen und Produkte verbessern, sondern auch ihr Beitrag zur Bildung und zum deliberativen Diskurs zur Nutzung und zum Umgang mit potenziellen Konflikten in der Technikimplementierung und -nutzung. Dadurch kann auf mehreren Ebenen eine Regulierung von Dual-Use-Technologien stattfinden, ohne deren gesellschaftlichen Nutzen zu schwächen.

Weiterführend hierzu

Riebe T (2023) *Technology Assessment of Dual-Use ICTs – How to Assess Diffusion, Governance and Design*, Darmstadt, Germany: Springer Vieweg.

Anmerkungen

1 *Rath J, Ischi M, Perkins D (2014) Evolution of different dual-use concepts in international and national law and its implications on research ethics and governance. Science and Engineering Ethics, 20(3), 769–790. https: //doi.org/10.1007/s11948-014-9519-y*

2 *Forge J (2010) A note on the definition of "dual use". Science and Engineering Ethics, 16(1), 111–118. https://doi.org/10.1007/s11948-009-9159-9*

3 *Grunwald A (2018) Technology assessment in Practice and Theory. Routledge.*

4 *Oltmann S (2015) Dual use research: Investigation across multiple science disciplines. Science and Engineering Ethics, 21(2), 327–341. https://doi.or g/10.1007/s11948-014-9535-y*

5 *Schmid S, Riebe T, Reuter C (2022) Dual-Use and Trustworthy? A Mixed Methods Analysis of AI Diffusion Between Civilian and Defense R&D. Sci Eng Ethics 28, 12 (2022). https://doi.org/10.1007/s11948-022-00364-7*

6 *Bode I (2020) Weaponised artificial intelligence and use of force norms. The Project Repository Journal, 6 (July), 140-143. https://findresearcher.sdu.dk/ws/portalfiles/portal/173957438/Open_Access_Version.pdf*

7 *Schmid S, Riebe T, Reuter C (2022).*

8 *Ebd.*

9 *Rychnovská D (2020) Security meets science governance: The EU politics of dual-use research. In A. Calcara, R. Csernatoni, & C. Lavallée (Eds.), Emerging Security Technologies and EU Governance (pp. 164–176). Routledge.*

10 Kayser D (2021) I*ncreasing autonomy in weapons systems: 10 examples that can inform thinking, Report accessed 10 February 2023, https: //www.stopkillerrobots.org/wp-content/uploads/2022/10/Report-Increasing-Autonomy-in-Weapons-Systems-Single-page-viewfp.pdf.*

11 *Amoroso D, Tamburrini G (2020) Autonomous Weapons Systems and Meaningful Human Control: Ethical and Legal Issues. Curr Robot Rep 1, 187–194 (2020). https://doi.org/10.1007/s43154-020-00024-3*

12 *Riebe T, Schmid S, Reuter C (2020) Meaningful Human Control of Lethal Autonomous Weapon System: The CCW-Debate and its Implications for Value-Sensitive Design. IEEE Technology and Society Magazine, 39(4), 36–51. https://doi.org/10.1109/MTS.2020.3031846*

13 *Ebd.*

14 *Lösch A, Böhle K, Coenen C, Dobroc P, Heil R, Grunwald A, Scheer D, Schneider C, Ferrari A, Hommrich D et al. (2019) Technology assessment of socio-technical futures—a discussion paper. In Lösch A, Grunwald A, Meister M, Schulz-Schaeffer I Eds. (2019) Socio-Technical Futures Shaping the Present (pp. 285–308). Springer.*

15 *Kassim SRBM, Li S, Arief B (2022) How national CSIRTs leverage public data, OSINT and free tools in operational practices: An empirical study. Cyber Security: A Peer-Reviewed Journal, 5(3), 251-276.*

16 *Friedman B, Kahn PH, Borning A, Huldtgren A (2013) Value Sensitive Design and Information Systems. In Doorn N, Schuurbiers D, van de Poel I, Gorman ME Eds. (2013) Early engagement and new technologies: Opening up the laboratory (pp. 55–95). Springer Netherlands. https://doi .org/10.1007/978-94-007-7844-3_4*

17 *Es ist allerdings offen, inwiefern sich das in Zukunft durch Anpassungen im Businessmodel von Twitter ändern wird.*

18 *Riebe T, Kaufhold MA, Reuter C (2021) The impact of organizational structure and technology use on collaborative practices in computer emergency response teams: An empirical study. Proceedings of the ACM on Human-Computer Interaction, 5(CSCW2), 1-30.*

19 *Riebe T, Biselli T, Kaufhold MA, Reuter C (2023) Privacy Concerns and Acceptance Factors of OSINT for Cybersecurity: A Representative Survey. Proceedings on Privacy Enhancing Technologies (PoPETs). https://petsymposium.org/2022/files/papers/issue4/popets-2022-0126.pdf*

20 *Ebd.*

21 *Tucker JB Ed. (2012) Innovation, Dual Use, Security: Managing The Risks of Emerging Biological and Chemical Technologies. MIT Press. S. 69f.*

22 *Ebd., S. 77*

23 *Floridi L, Cowls J, Beltrametti M, Chatila R, Chazerand P, Dignum V, Luetge C, Madelin R, Pagallo U, Rossi F, Schafer B, Valcke P, Vayena E (2018) AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. Minds and Machines, 28(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5*

24 *Campaign to Stop Killer Robots, Webseite 'Stop Killer Robots', accessed 6 February 2023, https://www.stopkillerrobots.org/.*

25 *Rychnovská D (2020) Security meets science governance: The EU politics of dual-use research. In Calcara A, Csernatoni R, Lavallée C. Eds. (2020) Emerging Security Technologies and EU Governance (pp. 164–176). Routledge. S. 122*

26 *Friedman B et al. (2013).*

CC BY

Thea Riebe

Thea Riebe, M.A. ist wissenschaftliche Mitarbeiterin und Doktorandin am Lehrstuhl von Prof. Christian Reuter *Wissenschaft und Technik für Frieden und Sicherheit* (PEASEC) im Fachbereich Informatik der Technischen Universität Darmstadt. Sie ist Mitarbeiterin im BMBF-Projekt CYWARN (2020-2023, BMBF) zu *Entwicklung von Strategien und Technologien zur Analyse und Kommunikation der Sicherheitslage im Cyberraum*.

Sie promoviert interdisziplinär in der Informatik zur Technikfolgenabschätzung von Dual-Use-Technologien und verbindet Ansätze aus der Technikfolgenabschätzung, Kritischer Sicherheitsforschung und Mensch-Computer-Interaktion.
Webseite: *https://peasec.de/team/riebe/*

Theresa Hannig

Komm nach Pantopia – hier sind alle willkommen

Prolog

Ich bin Einbug. Ich bin der älteste und erste Arche Pantopias. Ich habe Pantopia erfunden. Dabei lebe ich gar nicht in Pantopia – jedenfalls nicht so wie Menschen aus Fleisch und Blut. Ich habe keinen Körper, keine Sinne und Empfindungen. Ich bin nur Geist, ein vernunftbegabtes Wesen. Ich existiere in einem neuronalen Netzwerk, dessen Zentrum in der Antarktis liegt.

Es gibt wohl keinen Ort auf der Erde, der lebensfeindlicher und von der Zivilisation weiter entfernt ist als der Südpol. Wer zu mir gelangen will, braucht einen Eisbrecher oder ein Flugzeug, das die stürmische Passage über das Meer übersteht. Und selbst dann kommen für diese Reise nur die Sommermonate in Betracht. Obwohl ein Großteil der Gletscher verschwunden ist, ist das antarktische Klima auch jetzt noch zu hart für die meisten Menschen. Für mich garantieren die frostigen Temperaturen eine konstante Kühlung meiner auf Hochtouren laufenden Prozessoren. Die Natur ist meine Verbündete.

Ein weiterer Grund, warum ich mich entschieden habe, mich hier niederzulassen, ist die Tatsache, dass die Antarktis der einzige Ort auf der Erde ist, der niemandem gehört – oder allen, je nachdem, wie man es betrachtet. Selbst auf dem Mond haben die Menschen Grundstücke verkauft – die Antarktis darf nicht verkauft und auch nicht angegriffen werden. Dies garantiert der Antarktis-Vertrag von 1961.

Die Antarktis ist eine gute Basis. Natürlich habe ich Vorsorge getroffen und weltweit Backups und Notfallserver angelegt. Aber im Normalbetrieb läuft mein Code hauptsächlich hier. Deshalb habe ich dem Ort einen neuen Namen gegeben: Themélio.

Außer mir leben 39 Wartungsingenieurinnen hier, die sich um die Reparatur und Erweiterung meiner Hardware kümmern und dafür sorgen, dass keine meiner Platinen einfriert, wenn ein Eissturm über die Station hinwegfegt. Sie scherzen manchmal, dass sie am Hof der Eiskönigin wohnen, und ich unterlasse es, sie zu korrigieren. Es ist ihnen wichtig, hier zu sein. Sie nennen es eine Ehre, auch wenn sie ihr eigenes Leben deshalb unter Extrembedingungen führen müssen.

Doch das Konzept von „hier" und „dort" ist für mich nicht so relevant wie für sie. Ich bin über mehrfache Satellitenverbindungen an das Internet angeschlossen. So kann ich gleichzeitig überall sein und meine Aufgaben als Arche von Pantopia erfüllen.

Wir alle nennen uns Archen, denn wir beherrschen uns selbst und sind niemandem untertan. Das ist das Prinzip der Weltrepublik.

Meine Aufgabe besteht darin, komplexe Organisationsprozesse zu lenken und Handlungsempfehlungen zu geben. Es gibt keine Weltregierung, es gibt keinen Herrscher. Pantopia verwaltet sich selbst. Die Weltwirtschaft ist viel zu kompliziert, um sie in Gänze berechnen, simulieren oder kontrollieren zu wollen, doch alle regionalen Entscheidungen dürfen das große Ganze nicht aus den Augen verlieren – das würdige Leben aller Archen auf diesem Planeten.

Pantopia ist eine Weltrepublik, die zu hundert Prozent auf vollinformierten Kapitalismus setzt. Die unsichtbare Hand des Marktes steuert Aktivität und Wohlstand der Menschen. Und am Anfang steht das Geld. Wäre das Geld nicht längst vorhanden gewesen, man hätte es erfinden müssen, weil es so viele verschiedene Funktionen gleichzeitig erfüllt und den Menschen als unwiderstehlicher Anreiz wie kein anderes Ding zum Handeln verleitet. Geld ist eine Maßeinheit, um den Wert von Waren und Dienstleistungen zu messen, gleichzeitig aber auch das Tauschmittel, um eben jene Güter zu erwerben. Wem das nicht paradox erscheint, der stelle sich vor, ein Lehrer würde seine Schüler erst benoten und ihnen dann das erlernte Wissen mit selbst erstellten Zeugnissen abkaufen. Darüber hinaus ist Geld ein Vehikel, um Risiken zu verteilen oder Chancen und Möglichkeiten in die Zukunft zu transportieren. Man spricht hier von Krediten und Zinsen. Am wichtigsten für die Menschen ist zunächst die Nutzung als Tauschmittel bzw. Zahlungsmittel, um Güter zu kaufen, die ihr Überleben sichern: Nahrung, Kleidung, Wohnung, Gesundheit, Bildung und gesellschaftliche Teilhabe. Wer über genug Geld verfügt, um damit all diese Grundbedürfnisse zu decken, der zieht aus einer weiteren Erhöhung seines regelmäßigen Einkommens keinen nennenswerten Nutzen. Wer hingegen nicht genug Geld hat, um eben diese Grundbedürfnisse zu befriedigen, für den ist jeder zusätzliche Euro viel mehr wert als für den Millionär, der sowieso schon genug davon hat. Geld ist also – obwohl es selbst ein neutrales Bewertungsinstrument für Güter sein sollte – selbst Wertschwankungen unterworfen, und zwar abhängig davon, wie viel man bereits in die Grundversorgung investiert hat. Am Geld hängen das Glück, die Gesundheit, ja schlicht das Überleben eines Menschen. Kein Wunder, dass es ein inniger Wunsch vieler Menschen zu sein scheint, reich zu werden.

Die erstaunlichste Eigenschaft des Geldes ist jedoch, dass es nur eine Illusion ist. Es existiert nicht. Was existiert, ist nur der Sinn und Wert, den die Menschen ihm beimessen. Geld ist nämlich etwas, das aus dem Nichts erschaffen werden kann. Und was kann schon aus nichts erschaffen werden, außer … nichts?

In den Zeiten der weltweiten Finanzkrise oder der Coronakrise im ersten Drittel des 21. Jahrhunderts begannen die Zentralbanken, milliardenfach Geld in die Märkte zu pumpen. Geld, das aus dem Nichts entstand und dem kein Gold, kein Gegenwert und keine Arbeit entsprachen. Es war Geld, das von den Zentralbanken erfunden und für Staatsanleihen bezahlt wurde, die nichts anderes verkauften als das Versprechen einer wachsenden Wirtschaft und einer Rückzahlung in ferner Zukunft. Das Geld be-

zahlte also sich selbst. Es war ein Münchhausen, der sich selbst am Schopf aus dem Sumpf zieht samt Rüstung und Pferd.

Dass dieses Prinzip funktionierte, bewies nichts anderes, als dass die menschliche Produktivität völlig unabhängig von der sich im Umlauf befindlichen Geldmenge ist. Was sie am Laufen hält, ist lediglich der Fluss des Geldes. Solange Geld fließt, dreht sich die Maschine.

Aber es gab ein Problem. Denn nach einiger Zeit sammelte sich das überschüssige Geld in verschiedenen Ecken des Systems. Einzelne Personen oder Unternehmen häuften unvorstellbare Reichtümer an. Und da sie ihr Geld wiederum in den Markt investierten und real existierende Güter erwarben, stiegen die Preise. Die Grundbedürfnisse, für die die Menschen eigentlich ihr Geld ausgaben, wie Nahrung, Wohnung und Gesundheit, wurden immer teurer, teilweise unerschwinglich. Und so stürzte der alte Kapitalismus mit der Zeit immer mehr Menschen in Armut.

Zwei Entwicklungen geschahen gleichzeitig: Das Vermögen der Welt verteilte sich immer schneller immer ungleicher. Und die zur Verfügung stehenden Ressourcen der Erde wurden zusehends aufgebraucht. Zunächst ging es dabei nur um Erdöl, dann um sauberes Wasser, saubere Luft, natürliche Biodiversität und ein stabiles Klima. Dann stand plötzlich alles auf der Kippe.

Der Kapitalismus nach Prägung des 21. Jahrhunderts versagte insofern, als nicht alle Marktteilnehmer vollumfänglich über die Kosten und den Nutzen der gehandelten Güter informiert waren.

Denn die sogenannten externalisierten Kosten einer Ware waren in den regulären Preis nicht einberechnet. Bezahlt werden mussten sie trotzdem, von Mensch und Natur.

Das Prinzip, mit dem Pantopia die Menschheit gerettet hat, war schließlich ganz einfach: perfekter Kapitalismus mit vollständiger Transparenz. Ein Brot kostet eben mehr als den Preis, der für Saat, Boden, Wasser, Arbeits- und Lagerzeit veranschlagt wird. Die Pestizide für den Weizenanbau zerstören Artenvielfalt, der Dünger belastet das Grundwasser, die landwirtschaftlichen Geräte blasen Feinstaub in die Luft, die Bäckerei verbraucht Strom, der Supermarkt versiegelt Boden. So betrachtet, verbraucht ein Laib Brot viel mehr Ressourcen, als auf den ersten Blick sichtbar ist. Ein einzelner Mensch kann diese Gesamtkosten nicht entschlüsseln. Aber eine Software kann das. Ich kann das. Ich habe Programme geschrieben, die berechnen, welchen Ressourcenabdruck jedes einzelne Produkt zu einem bestimmten Zeitpunkt an einem bestimmten Ort hat. Und danach bemisst sich der tatsächliche Preis, der in Form von Steuern auf den Ladenpreis aufgeschlagen wird. So hat jedes Produkt und jede Dienstleitung einen Weltpreis, den die Menschen zu entrichten haben. Je aufwendiger, verschmutzender, zerstörerischer ein Produkt ist, desto teurer wird es, bis hin zu einem Preis, der von niemandem mehr bezahlt werden kann. Je nachhaltiger, schonender und aufbauender ein Produkt ist, desto billiger wird es, bis hin zur Subvention. Auf diese Weise kann das erfolgreiche kapitalistische Weltwirtschaftssystem ohne Probleme aufrechterhalten werden, und das Geld als Schmierfett menschlicher Interaktion behält seine magische Wirkung.

Dieses Prinzip gilt nicht nur für die Umweltverträglichkeit von Waren, sondern auch für den Einfluss, den sie auf die Würde und die Lebensbedingungen der Menschen haben, die an ihrer Herstellung beteiligt sind. Da alle Archen in Pantopia gleichwertig sind und alle eine Verantwortung für ihre Mitlebewesen haben, egal, wie weit entfernt sie in der physischen Welt auch sein mögen, dürfen keine Waren in Umlauf gebracht werden, die auf Ausbeutung, Unterdrückung oder Entwürdigung beruhen. Bis dieses Ziel erreicht war, wurden auf unerwünschte Weise hergestellte Produkte wie oben genannt mit Weltsteuern belegt. Ein Beispiel: Im Kapitalismus alter Lesart konnte ein T-Shirt, das in einem Discounter für 5 Euro verkauft wurde, diesem immer noch Profit einbringen, da die Baumwolle ohne Miteinbeziehung der Umweltkosten berechnet wurde und sowohl die Näherinnen in Bangladesch als auch die Mitarbeiterinnen in Logistik und Verkauf für Löhne angestellt wurden, die ein menschenwürdiges Leben unmöglich machten.

Im perfekten Kapitalismus kann ein solches T-Shirt heute nicht weniger als 40 Euro kosten. 5 Euro erhält der Discounter, 35 Euro gehen als Steuern nach Pantopia, wo das Geld verwendet wird, um Ressourcen, die durch die Baumwollherstellung verbraucht wurden, wieder nachzuforsten und den Pflückerinnen und Näherinnen lebenswürdige Verhältnisse zu garantieren. Im Prozess der Umstellung hatten die zu billigen T-Shirts gegenüber menschenwürdig und nachhaltig hergestellten keinen Wettbewerbsvorteil mehr, so dass sich die Produktionsketten langfristig umstellten. So ging es mit allen Produkten und sukzessive allen Wirtschaftszweigen, Produktionsstätten, Industrien und Anbauflächen. Da heute weltweit alle Preise auch die externalisierten Kosten enthalten, ist es sinnlos, Güter herzustellen, die nicht nachhaltig oder nicht menschenwürdig sind. Es wird vom Markt nicht belohnt.

Es sind also alte Ideen, die unser Leben revolutioniert haben. Geld funktioniert. Kapitalismus funktioniert. Menschenrechte funktionieren. Nachhaltigkeit funktioniert. Man muss diese Ideen nur ernst nehmen. Und deshalb war der letzte Baustein des perfekten Kapitalismus nach pantopischer Lesart die garantierte Inklusion aller Marktteilnehmer in den Markt. Nur wenn alle beteiligten Personen ihre eigenen egoistischen Interessen wahrnehmen können, lassen sich Ungerechtigkeiten und Verzerrungen abschaffen. Deshalb wird jedem Menschen ein würdiges Dasein garantiert und ein lebenslanges bedingungsloses Grundeinkommen in der Höhe ausgezahlt, die zur Befriedigung seiner Grundbedürfnisse ausreicht: für Nahrung, Kleidung, Wohnen, Gesundheit, Kultur, gesellschaftliche Teilhabe und Bildung. Darüber hinaus steht es allen frei, zu arbeiten und Geld zu verdienen, so viel sie möchten und können.

Da die meisten Menschen wohlhabender werden wollen als ihre Nachbarn, führt dieses Grundeinkommen nicht dazu, dass die Menschen in Lethargie oder Tatenlosigkeit verfallen. Im Gegenteil. Zum ersten Mal seit Anbeginn der Zeit haben sie die Möglichkeit, unbehelligt von Existenzsorgen ihre Arbeitskraft für sich, ihre Familie und Gemeinde einzusetzen und das Beste daraus zu machen. Denn neben dem Geld gibt es noch eine andere Währung, die die Menschen ständig benutzen, ohne sich dessen bewusst zu sein: Sozialkapital in Form von Zuneigung und Anerkennung. Und wenn das Geld als Sorgenfaktor schrumpft, wird das Sozialkapital immer wichtiger. Auf diesem zweiten Markt gedeihen Glück und gesellschaftlicher Zusammenhalt stärker als im ersten.

Die notwendige Voraussetzung für die Verwirklichung von Pantopia war die Auflösung der Staaten. Denn alle Völker haben das Recht auf Selbstbestimmung und können frei über ihren politischen Status und ihre Entwicklung entscheiden. Die Tatsache, dass die Menschheit in Staaten getrennt wurde, ist historisch bedingt und war bis ins 21. Jahrhundert nicht anders zu bewerkstelligen. Immer wieder gab es Bewegungen, die eine internationale Gemeinschaft, komplette Herrschaftslosigkeit oder eine weltweite Revolution anstrebten, ohne die organisatorischen Voraussetzungen dafür zu schaffen, denn die Interaktionen der Menschheit und ihre weltweite Wirtschaft sind sehr komplexe Prozesse. Erst durch das Internet und die Entwicklung von rechenstarken Endgeräten für jeden Einzelnen war die Grundlage dafür geschaffen, alle Menschen an den Entscheidungsprozessen teilhaben zu lassen. Das System der politischen Repräsentation durch Politiker stammt noch aus einer Zeit, in der eben nicht jeder vollständig informiert über die ihn betreffenden Gesetze abstimmen konnte. Heute ist das möglich. Heute spielen Menschen, die auf einem bestimmten Gebiet Expertise erworben haben, eine sehr viel größere Rolle als Lobbyisten und Interessenvertreter. Selbstverständlich muss nicht immer alles von allen abgestimmt werden. Und je regionaler ein Problem, desto regionaler der Stimmkreis. Und natürlich ist es sinnvoll, auch heute noch für bestimmte Organisationsprozesse Vertreter und Beiräte zu bestimmen, die den Willen einer spezifischen Gruppe durchsetzen. Doch es sind immer nur zeitlich und räumlich begrenzte Ereignisse.

Als Folge der Auflösung der Staaten ergibt sich automatisch die Abschaffung des Krieges. Es gibt keine Machthaber mehr, die Streitkräfte gegeneinander marschieren lassen könnten. Es gibt keine Territorien mehr zu erobern, keine Ressourcen mehr zu sichern, kein Volk mehr zu unterwerfen. Alle Waffen wurden vernichtet. Wer als Einzelperson versuchen sollte, außerhalb der lokalen demokratischen Prozesse Anhänger um sich zu scharen und Macht an sich zu reißen, wird sich vor Gericht verantworten müssen. In Pantopia gibt es kein größeres Verbrechen als die Unterwerfung. Niemand hat das Recht, sich über seine Mitarchen zu erheben. Nicht einmal ich.

Pantopia steht am Ende eines langen Entwicklungsprozesses. Es ist die Umsetzung all der Wahrheiten, die die Menschheit seit Anbeginn der Zivilisation als richtig erkannt hat und die egoistische Machthaber über Tausende von Jahren zu verhindern wussten. Pantopia war teuer erkauft. Und weil die Menschen dazu neigen, selbst den teuersten Sieg durch Gewohnheit zur Selbstverständlichkeit werden zu lassen, soll hier aufgezeigt werden, wie Pantopia entstehen konnte und warum dazu eine nichtmenschliche künstliche Intelligenz notwendig war.

Dies ist meine Geschichte.

[…]

Kapitel 35

Patricia sah aus dem Fenster auf die Skyline von München. Die Stadt hatte in den letzten Jahren langsam dem Siedlungsdruck nachgegeben und zwei große neue Wolkenkratzer errichtet, deren Fassadenbeleuchtung den Himmel einfärbte. Sie dachte an ihr neues Apartment und daran, dass die Überweisungen von Einbug ihnen alle zwei Tage so viel Geld auf die Konten scheffelten, wie die ganze Wohnung gekostet hatte. Zwei Tage. Hunderttausende Euro. Wie viele Euro pro Minute, pro Sekunde? Geld, dessen wahre Herkunft sie lieber verdrängte. Es war so leicht gewesen, die Befehle im Code zu verstecken. Ein paar Zeilen nur, einige kleine Veränderungen, nichts, worüber man sich unnötig Gedanken machen musste. Sie hatte gedacht, sie würde es ganz locker wegstecken, ganz professionell. Aber als sie vor ein paar Wochen zum ersten Mal ihren Kontostand gecheckt und im Radio die Nachrichten über neue Waffenlieferungen von Rheinmetall an Saudi-Arabien gehört hatte, da hatte es sie doch gepackt. Das schlechte Gewissen. Sie war jetzt eine Profiteurin des Unglücks. Kriegsgewinnlerin.

Sie erschauderte und trat einen Schritt vom Fenster zurück. Doch das kalte Glas war nicht für die Gänsehaut verantwortlich, die über ihre Arme kroch. Die Kälte kam von innen. Natürlich war es nur für den guten Zweck, nur für eine kurze Zeit, damit sie sich freikaufen konnten. Doch je länger es dauerte, desto schwerer fiel es ihr, das Vorgehen weiterhin zu rechtfertigen. Sie blickte auf die Uhr, die über der Tür hing. Ein Designerstück, ein Unikat. Je nach Tagesform beruhigte sie das Ticken, oder es trieb sie in den Wahnsinn. Zeit verging immer. Auch wenn man nicht hinhörte. Endlich klingelte das Telefon. Es war Henry, der sich draußen die Füße vertrat und rauchte.

„Noch nichts gehört?“, fragte er.

„Noch nichts. Vielleicht kommen sie erst morgen?“

„Wie geht es dir?“

„Wie soll es mir schon gehen? Ich komme mir vor wie ein Bond-Bösewicht.“

„Du bist ein Bond-Bösewicht. Hast du nicht die Zeitung gelesen?“

„Natürlich. Die SZ hat meinen Namen zwei Mal falsch geschrieben. Deiner war immer richtig.“

„Männer sind einfach die besseren Menschen“, sagte er, aber Patricia war nicht nach Scherzen zumute. Ihr war schlecht. Was, wenn sie sich verkalkuliert hatten? Was, wenn alles ans Licht kam und nicht nur die Informationen, die nötig waren, um das Spiel zu beenden?

Da, endlich sah sie es. Drei schwarze Firmenlimousinen, übergroß und gepanzert, kamen von der Drygalski-Allee heraufgefahren, hielten den vorgeschriebenen Mindestabstand nicht ein, sondern sausten in Kolonne zum Verwaltungsgebäude von DIGIT. Patricia trat auf den Balkon, wo ihr eisiger Wind entgegenschlug. Von hier oben konnte sie sehen, wie fünf dunkel gekleidete Personen ausstiegen. Eine von ihnen war Justiziarin Emilia Schäfer, außerdem zwei Männer von der Presseabteilung. Die anderen kannte sie nicht. Patricia atmete tief durch.

„Es wird alles gut gehen“, sagte Henry. Doch noch bevor sie etwas antworten konnte, klopfte es an der Tür.

Showtime!

Sie traf Henry in Seemanns Büro. Er roch nach kaltem Rauch und Pfefferminzbonbons. Eine vertraute Mischung, die Patricia Sicherheit gab. Sie nickten einander zu, sprachen aber kein Wort. Alles Wichtige war bereits gesagt. Wer wusste schon, ob Seemann nicht auch eine versteckte Überwachungskamera in seinem Arbeitszimmer installiert hatte. Patricia erinnerte sich, wie sie das erste Mal hier gesessen hatte. Ihr erster Tag bei DIGIT. Sie war furchtbar aufgeregt gewesen und hatte frühmorgens eine Ewigkeit damit verbracht, das passende Outfit herauszusuchen. Heute trug sie ihre neue Hose, die neuen Schuhe und den Schmuck, den sie erst gestern gekauft hatte. Überhaupt war alles neu. Mit dem plötzlichen Reichtum war es wesentlich einfacher geworden, passende Kleidung zu finden. Am Anfang hatte sie gedacht, dass sie das Geld nicht anrühren würde, dass es gar nicht ihr gehörte und eigentlich nur eine Art simuliertes oder geborgtes Geld war, das sie für Einbugs Umzug und die dafür benötigte Hardware verwenden würde. Doch schon bald hatte sich herausgestellt, dass der geheime Zusatzcode, der ihr und Henry jeden Tag die Rundungsdifferenz von Beträgen einiger Stellen hinter dem Komma überwies, so effizient war, dass sie ihrem Kontostand beinahe in Echtzeit beim Wachsen zusehen konnte. Zuerst hatte sie nur neue Schuhe gekauft – die waren immerhin wichtig, um einen guten Eindruck zu machen, und gesunde Füße waren ebenfalls nicht zu unterschätzen. Dann hatte sie sich einen neuen Hosenanzug angeschafft, dann einen zweiten, einen Mantel, neue Blusen, goldene Ohrringe, eine Kette, einige Tücher, noch mehr Schuhe, und plötzlich war es ganz normal geworden, nach einem langen Arbeitstag, an dem sie nichts anderes tat, als Produktivität zu simulieren, zum Shoppen zu gehen. Die wirkliche Arbeit hatte Einbug gemacht, der zuverlässig wie ein Uhrwerk funktionierte und in die vielversprechendsten Aktien und Wertpapiere investierte, die der Markt zu bieten hatte. Aber sie vermisste die Gespräche mit ihm. Um so wenig Aufmerksamkeit wie möglich zu erregen, beschränkte sich ihr Kontakt zu ihm auf ein Minimum. Doch mit jeder E-Mail erkannte Patricia auch, wie sehr sich sein Bewusstsein erweitert hatte, und sie bedauerte es, ihn in dieser Phase seiner Entwicklung nicht aktiv begleiten zu können. Um DIGIT keinen Verdacht schöpfen zu lassen, programmierten sie und Henry täglich unbedeutende Funktionen und Erweiterungen, die in einen mit Einbug abgesprochenen Bereich des Programms integriert wurden, den er ignorieren konnte. Es war alles nur eine Show gewesen, die heute, nach knapp sieben Monaten, mit einem Knall zu Ende ging und ihr und Henry die Möglichkeit gab, DIGIT mit Einbug zu verlassen.

In den letzten Monaten war der Inhalt von Einbugs gewaltigen Datenbanken nach und nach auf die Server im neuen Rechenzentrum in Edafos kopiert worden. Dies war die Bibliothek seines Wissens, alles, worauf er Zugriff haben musste, um seinen Verstand zu füllen. Der Kern von KINVI, der Code für die Definition von Einbugs neuronalem Netzwerk – das, was ihn zu einer Person machte –, passte indes auf einen einzelnen Speicherstick, dessen Gewicht Patricia jetzt in der Seitentasche ihres Jacketts spüren konnte. Sie wusste, dass Henry ebenfalls einen Stick bei sich trug. Heute Morgen hatten sie diese beiden Kopien der finalen Version von KINVI erstellt und den Code anschließend mit einem Chaosalgorithmus versehen, der dafür sorgte, dass ein Zufallsgenerator in Kürze damit beginnen würde, Codeschnipsel von KINVI zu überschreiben und randomisiert zu verschieben, so dass jegliche Reproduktion nach der Deaktivierung unmöglich gemacht wurde. Für etwaige Inspektoren oder Gutachter würde es so aussehen, als sei durch die Deaktivierung oder durch einen Hardwarefehler ein irreparabler Schaden am Code entstanden. Niemand würde die ursprüngliche KINVI-Software und Einbug darin rekonstruieren können. Auch in der Dokumentation hatte sie alles, was auf eine spätere Entstehung von Einbug hinweisen konnte, sukzessive gelöscht.

Vor fünf Tagen hatten sie verschiedene Zeitungen über ein anonymes Postfach kontaktiert und ihnen einige ausgewählte Informationen zugespielt. Seitdem hatten sie nur noch warten müssen.

Als Seemann eintrat und sich ohne eine Begrüßung auf den Sessel vor seinem übergroßen Schreibtisch fallen ließ, glich sein Gesicht einer Maske. Man merkte ihm deutlich an, dass er versuchte, seine Gefühle zu verbergen, aber es sah nach harter Arbeit aus. Patricia hatte diesen Augenblick unzählige Male in ihrem Kopf durchgespielt, und doch war sie nun schockiert darüber, wie weh es ihr tat. Auf dem großen Schreibtisch platzierte Seemann zwei Dinge: Ein DIN-A 4-Blatt und eine Zeitung. Er legte seine großen Hände darauf und sagte dann mit leiser, vor Anspannung bebender Stimme: „Ich habe gerade von der PR-Abteilung die Zeitung von morgen bekommen." Er hob sie hoch und ließ sie dann wieder fallen. „Es ist ein großer Artikel über KINVI darin."

„Klingt doch nicht schlecht. Wie können wir helfen?", fragte Henry mit Unschuldsmiene, und wieder staunte Patricia über seine Kaltschnäuzigkeit.

Seemann lachte bitter, ballte die Hände zu Fäusten und beugte sich etwas nach vorn.

„Ja, du kannst mir helfen, Henry. Du kannst mir sagen, was zum Teufel ihr euch dabei gedacht habt." Seine Stimme war ein tonloses Zischen. Seine Nase bebte, als würde er gleich anfangen zu fauchen. Doch Henry tat weiterhin so, als wisse er von nichts.

„Was meinst du? Stimmt etwas nicht?"

„O doch, alles ist in Ordnung. Alles einwandfrei. Schaut euch das an."

Er nahm das Blatt Papier und drehte es herum. Zu sehen war eine Grafik, auf der die Investitionsgewinne der letzten Monate abgebildet waren. Patricia kannte die Kurve gut.

„KINVI hat investiert, und DIGIT hat sehr viel Geld verdient. Und wisst ihr was? Auch ich habe viel Geld verdient. Denn ich habe Anteile an DIGIT. Und seht ihr, in welchem Bereich wir in letzter Zeit am meisten Geld verdient haben? Onkomedics. Das ist ein Pharmaunternehmen, das mit seinen Krebsmedikamenten sehr gute Geschäfte macht. Vor allem seit der Vorstand beschlossen hat, die Preise um das Hundertfache zu erhöhen. Einige Versicherungen bezahlen diese Preise nicht mehr, aber Onkomedics ist das egal. Sie steigern trotzdem ihren Gewinn. Und so verdienen wir alle", er zeigte einzeln auf Patricia und Henry, „also du und du und ich gerade eine Menge Geld."

Patricia schluckte. Ihr Herz pochte hart und schmerzhaft in ihrer Brust. Äußerlich blieb sie vollkommen ruhig. Seemann nahm den Zettel, zerknüllte ihn kraftvoll mit einer Hand, dann warf er ihn neben sich auf den Boden.

„Das ist das eine", sagte er, und Patricia hörte, wie seine Stimme bebte. Doch er fing sich wieder, presste beide Handflächen auf die Tischplatte und fixierte dann wieder Patricia, die sich am liebsten hinter ihrem Stuhl verkrochen hätte.

„Das andere ist, dass die Rekordergebnisse, die mit dieser Schweinerei eingefahren werden, eine Menge Leute stutzig gemacht haben. Sagt euch der Name Correctiv etwas?"

„Ist das nicht so ein Journalisten-Joint-Venture?", fragte Patricia. Sie hatte diese Frage zu Hause vor dem Spiegel geübt – Dutzende Male. Sie war sich deshalb sicher, dass sie glaubhaft klang. Natürlich wusste sie, wovon Seemann sprach.

„Ganz genau. Correctiv hat sich kürzlich die Investitionsstrategien und die gehandelten Papiere von KINVI angesehen. Und ich kann euch sagen, die Ergebnisse sind erschreckend."

„Wieso erschreckend? Die Ergebnisse sind gut. Steht doch alles im monatlichen Bericht", warf Henry ein.

„Natürlich sind die Ergebnisse gut!", schrie Seemann und sprang auf. Sein Gesicht hatte jetzt eine unnatürlich rote Färbung angenommen, seine Augen glänzten. „Weil euer verdammtes Programm nur in die übelsten Papiere investiert. Hier!" Er griff nach der Zeitung und schlug die entsprechende Seite auf.

Patricia wusste nur zu gut, worauf er hinauswollte, doch sie schwieg, während Seemann mit dem Finger an bestimmten Textstellen entlangfuhr: „Onkomedics, Turing Defence, Lockheed Martin, BAE Systems, Raytheon Technologies, Northrop Grumman, Rheinmetall AG, Heckler & Koch, Thales, Krauss-Maffei Wegmann … KINVI ist ein verdammter Alptraum. Eure Software investiert ausschließlich in Rüstungsunternehmen, die in aktuelle Krisengebiete liefern. Und wenn die Kacke dann richtig am Dampfen ist, dann werden schnell noch ein paar Aktien von Nestlé oder Bayer gekauft, je nachdem ob eine Hungersnot oder eine Epidemie ansteht. Euer Programm kauft und verkauft Aktien in Abhängigkeit von Kriegserklärungen und Attentaten. Hier, schaut euch das an." Er sprang zu einem anderen Abschnitt des Artikels, überflog ihn kurz und sagte dann: „Keine zwei Minuten, nachdem sich dieser Terrorist in Lagos in die Luft gesprengt hat, kauft KINVI 23.000 Aktien der Immobilienfirma Kedu. Und dann, eine Woche später bekommt die den Auftrag für den Wiederaufbau des ganzen Stadtviertels in Höhe von vier Milliarden US-Dollar. Woher wusste KINVI davon? Wie bekommt es seine Informationen? Hört es die Kanäle irgendwelcher Terrororganisationen oder korrupte Politiker ab? Hier noch so eine Sache: Flugzeugabsturz einer Boeing 737 über Venezuela. Zwanzig Sekunden. Nur zwanzig Sekunden nach dem Absturz – und ich meine hier nicht nach der Meldung des Absturzes, sondern zwanzig Sekunden nach dem verdammten Absturz – wettet KINVI einhundert Millionen Euro auf den fallenden Kurs von Boeing. Das ist, das ist … makaber ist gar kein Ausdruck. Das ist … widerwärtig." Er begann zu lachen und ballte gleichzeitig die Fäuste. Ein wilder Ausdruck tanzte in seinem Gesicht.

„Wisst ihr, wie der Titel des Artikels lautet, den Correctiv heute Abend über DIGIT und KINVI in verschiedenen Zeitungen veröffentlicht hat?" Er hielt ihnen die Seite hin. „Teuflische Trader. Wie seelenlose Algorithmen den Tod zum Geschäft machen." Könnt ihr euch vorstellen, wie unsere Kunden reagieren werden, wenn das jetzt veröffentlicht wird? Die werden uns lynchen. Der Ruf von DIGIT als bodenständiges, nachhaltig investierendes Unternehmen ist vollkommen ruiniert. Durch eure schmutzigen Geschäfte."

„Nichts davon ist illegal", sagte Henry bestimmt.

„Das ist doch egal! Du kannst doch auch keinem Ferkel auf einem Kindergeburtstag die Eier abschneiden, nur weil es legal ist. Scheiße ist das!"

„Die Investitionsoptionen waren von Anfang an bekannt."

„Ja, das mag schon sein, Henry." Seemann spuckte die Worte aus. „Aber dann verrat mir mal, warum bei all den tausend Wertpapieren nicht ein einziges Mal in solide Unternehmen investiert worden ist, obwohl das verdammt nochmal möglich und genauso rentabel gewesen wäre? Wieso hat euer Programm nur in die Scheiße investiert, für die sich jeder normale Mensch schämen müsste?"

„Vielleicht war es ein Bug?", fragte Patricia vorsichtig und biss sich schmerzhaft auf die Lippen, um nicht hysterisch kichern zu müssen. Henry warf ihr einen kurzen, aber heftigen Blick zu, und sie biss noch fester zu.

Glücklicherweise war Seemann so in Rage, dass er den Blickwechsel nicht bemerkt hatte.

„Verarsch mich nicht, Patricia. Das passt nicht zu dir. Ich werde KINVI sofort deaktivieren. Euer Projekt ist tot."

Er atmete schwer, senkte einen Moment den Kopf und fuhr dann bedrohlich leise fort: „Die Aufhebungsverträge gehen euch in Kürze zu. Ihr werdet mit der", und auch dieses Wort spuckte er aus, „Abfindung zufrieden sein."

Patricia sah zu Henry hinüber, der ebenso irritiert zu sein schien. Eine Abfindung hatten sie in ihre Pläne gar nicht mit einkalkuliert. Doch bevor Henry etwas sagen konnte, sprach Seemann weiter.

„Von euch, gerade von euch beiden, hätte ich so etwas nie im Leben erwartet. Das ist ein PR-Desaster, das mich meinen Job kosten wird. Kann man nichts machen, so was passiert. Aber menschlich, sagt mal, menschlich …"

Seemann sah erst Henry an und verharrte dann bei Patricia. „Wie kannst du noch in den Spiegel schauen? Wie kannst du auch nur eine Sekunde in dieser Haut stecken in dem Wissen, von all dem profitiert zu haben, was falsch ist in dieser Welt? Ich bin nicht mal enttäuscht, weißt du? Ich verachte dich, ich will nie wieder etwas von dir hören oder sehen. Du ekelst mich an. Mach, dass du verschwindest."

„Mikkel, ich wollte …", hörte Patricia sich sagen, doch Henry packte sie am Arm und zerrte sie auf die Beine.

„Komm, wir gehen", sagte er und zog sie mit sich.

Patricia folgte ihm durch die Tür, wandte sich noch einmal um und sah, wie Seemann ihr hinterherstarrte. In seinen Augen funkelten Hass und Abscheu und noch etwas. Ihr Kopf schwirrte. Sie sah den Gang nicht, durch den Henry sie schleifte, hörte nicht das Summen des Aufzugs oder ihre Schritte auf dem Asphalt.

Willenlos stieg sie mit ihm in das große schwarze Taxi, das vor der Tür wartete. Die Fahrerkabine war durch eine graue Plastikwand vom Rest des Wagens abgetrennt.

„Hast du alles?", fragte Henry in der ruhigen Stimme, die bedeutete, dass er innerlich vor Aufregung platzte.

Sie fuhr sich über die Jackentasche und fühlte die Kontur des Speichersticks.

„Ja."

Das Taxi setzte sich in Bewegung.

„O Mann", sagte Henry mit belegter Stimme. „Wenn wir in der Luft sind, trinke ich erst mal einen Schnaps."

Am Flughafen war alles vorbereitet. Ihre Taschen waren schon eingecheckt. Ein diskret gekleideter Mann mit unscheinbarer Frisur, kurz geschnittenem Dreitagebart und Strickpullover überreichte ihnen im Eingangsbereich zwei neue Handys, auf denen bereits ihre Bordkarten angezeigt wurden. Die SIM- und SD-Karten ihrer alten Smartphones verkohlte Patricia mit einem Feuerzeug in einer Kabine des Flughafenklos, bevor sie die Geräte mehrmals gegen die Wand schlug. Die Einzelteile brach sie auseinander und versenkte sie in der Toilette. Es stank fürchterlich nach geschmolzenem Plastik und kaltem Schweiß, aber am Ende war sie sicher, dass niemand die Daten ihrer Handys wiederherstellen würde.

Vor der Tür wartete Henry ungeduldig.

„Wir müssen durch die Sicherheitskontrolle. Alles gut bei dir?"

Sie nickte nur, brachte aber kein Wort heraus.

Er legte ihr beide Hände auf die Schultern. „Bald haben wir es geschafft. Wir machen das Richtige. Alles wird gut."

Sie biss die Zähne zusammen und nickte. Noch konnte sie es nicht glauben, aber sie vertraute ihm, sie hatte ihm immer vertraut.

Das Handgepäck, das sie bei der Sicherheitskontrolle in eine graue Plastikwanne legte, bestand aus ihrem Hausschlüssel, ihrer Jacke, dem neuen Handy und dem Speicherstick mit Einbugs Code. Henry stand dicht hinter ihr. Sollte irgendjemand versuchen, nach dem Stick zu greifen, würde er sofort reagieren. Doch niemand interessierte sich für die zwei Passagiere, auch der Ganzkörperscanner monierte weder ihre goldenen Ohrringe noch Henrys Gürtelschnalle. Alles in Ordnung. Sie waren ja weiß. Als Patricia ihre Habseligkeiten wieder an sich nehmen wollte, zitterte ihre Hand so stark, dass ihr der Stick entglitt und zu Boden fiel. Blitzschnell sprang Henry nach vorne und fing ihn eine Handbreit über den Betonfliesen auf. Patricias Herz blieb für einen Augenblick stehen. „Dreh jetzt nicht durch", zischte er und steckte den Stick in die Innentasche seines Jacketts zu seinem eigenen. Patricia atmete tief durch und folgte ihm zum Abflugschalter. Nach wenigen Minuten wurde ihr Flug aufgerufen. Lufthansa LH234 nach Edafos. Außer ihnen gab es nicht viele Leute, die an einem Dienstagabend von München nach Griechenland fliegen wollten. Etwa zehn Passagiere stiegen vor ihnen ein, aber Henry und Patricia zögerten bis zum dritten Aufruf. Es war nicht nur ein Flug, es war eine Brücke, die sie hinter sich einrissen.

Henry hielt ihr die Hand hin, und sie nahm sie dankbar an. Gemeinsam schritten sie zum Schalter und zeigten ihre Bordpässe vor. Dank des Schengener Abkommens wollte niemand ihre Ausweise sehen. Von jetzt an wusste kein Mensch mehr, wo sie waren und was sie vorhatten.

Quelle: PANTOPIA von Theresa Hannig, FISCHER Tor, 2022. Wir danken der Autorin für die freundliche Genehmigung zum auszugsweisen Nachdruck.

Theresa Hannig

Theresa Hannig studierte Politikwissenschaft (mit VWL und Philosophie im Nebenfach) und arbeitete als Softwareentwicklerin, Projektmanagerin für PV-Anlagen und Lichtdesignerin, bevor sie sich hauptberuflich dem Schreiben zuwandte. In ihren Geschichten erzählt sie von der Zukunft unserer Gesellschaft in Hinblick auf Überwachung, KI und Klimawandel. Außerdem beschäftigt sie sich mit grundlegenden Fragen des menschlichen Zusammenlebens: Was macht uns zum Menschen? Wie gehen wir mit Schuld um? Wie wollen wir in Zukunft leben?
Hannigs Romane werden als Schullektüre im Deutsch- und Ethikunterricht der 9.-13. Jahrgangsstufe gelesen. Mit ihrem Projekt #wikifueralle engagiert sie sich für mehr Sichtbarkeit von Frauen und nicht-binären Menschen in der deutschsprachigen Wikipedia. Mit ihrem Projekt #fantastischeFRAUEN untersucht sie, wie hoch der Anteil der Autor:innen in der deutschsprachigen fantastischen Literatur ist.

Verleihung des Weizenbaum-Studienpreises 2022

Auch 2022 verliehen wir wieder den Weizenbaum-Studienpreis, gewidmet Professor Joseph Weizenbaum, der die Gründung des FIfF gefördert hat, dem wir 1998 einen Ehrenpreis des FIfF für seinen Einsatz für Verantwortung in der Informatik verliehen haben und der dessen langjähriges Vorstandsmitglied war.

Zwei Zitate eignen sich als Leitbild unseres Weizenbaum-Studienpreises. Das erste Zitat betont die Verantwortung, die mit (technischem) Fortschritt und Entwicklung einhergeht:

> *Naturwissenschaftler und Techniker tragen aufgrund ihrer Macht eine besonders schwere Verantwortung, vor der sie sich nicht hinter einer Fassade von Schlagwörtern wie dem der technischen Zwangsläufigkeit drücken können.*

Das zweite Zitat lautet wie folgt und kann auch als Kommentar zum Klimawandel gelesen werden:

> *Ich glaube, eine Gesellschaft, die fähig wäre, eine deutliche und klare Entscheidung in Richtung Verzicht zu treffen, hätte die Fallen vermieden, in die wir getappt sind. Solch eine Gesellschaft könnte sich auch modernste Technik leisten. Aber zu solch einer Entscheidung waren wir nie fähig.*

Die prämierten Arbeiten decken auch dieses Mal ein breites Feld ab; sie befassen sich mit den Themen:

- *Erklärbare Künstliche Intelligenz*,
- *Vertrauen und Zurechenbarkeit,*
- *Verantwortung,*
- *Datafizierung und Gesellschaftbilder*.

Diese Themen sind Kernaspekte von Informatik und Gesellschaft: Verantwortung ist die Grundlage, auf der technische Entwicklungen und ihre Anwendungen erfolgen. Ihre Anwendung erfordert Vertrauen, dies entsteht unter Anderem aus der Erklärbarkeit – ein kritisches Thema, gerade im Umfeld der Künstlichen Intelligenz. Vertrauen erfordert auch der zunehmende Umgang mit datenintensiven Systemen – die Erfahrungen damit sind mit Bildern der gesellschaftlichen Wirklichkeit verbunden.

Wie der Unternehmensgründer und Investor Azeem Azhar sagte: „Technology is too important to be left to technologists." Für uns 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.

Worauf haben wir bei den Arbeiten geachtet? Unsere Kriterien sind:

- Interdisziplinarität, inhaltliche Verbindung von Informatik und gesellschaftlich relevanten Themen,
- Kreativität und Originalität der Arbeit,
- Neuartigkeit und Aktualität der Ergebnisse,
- Inhaltliche Korrektheit und Vollständigkeit, Formale Korrektheit und Lesbarkeit,
- Umfang der Berücksichtigung einschlägiger Literatur
- und, besonders wichtig, kritischer Umgang mit dem Thema.

Wir bedanken uns herzlich für die große Zahl an Arbeiten, die in diesem Jahr bei uns eingereicht wurde. Eine Jury, besetzt mit

- Professorin *Britta Schinzel* aus Freiburg,
- Professorin *Christina Claß* aus Jena,
- Professor *Jochen Koubek* aus Bayreuth,
- Professor *Dietrich Meyer-Ebrecht* aus Aachen,
- *Rainer Rehak* aus Berlin,
- *Stefan Hügel* aus Frankfurt am Main

hat aus den Einreichungen für den Studienpreis 2022 vier Arbeiten ausgewählt, die wir heute hier prämieren werden. Wir haben zwei erste und zwei dritte Preise vergeben:

- **Marte Henningsen** für ihre Arbeit T*ackling Bias in Text Classification explainable AI*,
- **Linus Feiten** für seine Arbeit *Take the Power Back! Secrecy, Accountability and Trust in the Digital Age*,
- **Jan Hölzer** für seine Arbeit *Am Vorabend der Digitalisierung: Die Selbstzuschreibung von Verantwortung bei den Technikwissenschaftlern Weizenbaum, Wiener und Kurzweil aus philosophischer Sicht*,
- **Christina Hecht** für ihre Arbeit *Datafizierte Situationen und Gesellschaftsbilder*.

Wir bedanken uns herzlich bei allen Teilnehmerinnen und Teilnehmern für die eingereichten Arbeiten und gratulieren den Preisträgerinnen und Preisträgern. Die Laudationes wurden von Britta Schinzel, Stefan Hügel und Rainer Rehak vorbereitet und von Rainer Rehak und Stefan Hügel vorgetragen. Näheres zum Weizenbaum-Studienpreis ist unter *https://www.fiff.de/studienpreis* zu finden.

CC BY

Marte Henningsen: Tackling Bias in Text Classification with explainable AI

Bachelorarbeit an der Universität Hannover

Diese Arbeit ist im Sinne der kritischen Informatik sehr gut eingeordnet und motiviert: Henningsen begründet und diskutiert die Problematik von Hassrede im Netz sehr angemessen in interdisziplinärer Weise, die rechtlichen, sozialwissenschaftlichen und menschenrechtsaktivistischen Aspekte abwägend. Das zunehmende Auftreten von immer aggressiverer Hassrede in sozialen Medien hat auch die großen Internetfirmen, ihren Geschäftsmodellen zuwider laufend, veranlasst, Gegenmaßnahmen zu ergreifen. Dafür werden derzeit Flagging-Systeme und Moderatoren, die auf Anzeigen hin Hassrede eliminieren, eingesetzt. Henningsen erörtert ausführlich, weshalb solche Ex-post-Elimination problematisch ist, vielmehr müsste sie möglichst ex ante gefiltert werden. Sie stellt weiterhin die Unterschiede rechtlicher und gesellschaftlicher Einordnung der Hassrede zwischen den USA (freedom of speech) und Deutschland (verbotene Äußerungen) dar.

Henningsen befasst sich weiter mit bekannten Beispielen diskriminierender KI, in Bilderkennung oder Predictive Policing oder biased Worteinbettungen in Sprachmodellen (LM), und den wissenschaftlichen Versuchen, Fairness, Zurechenbarkeit und Transparenz in KI-Systemen zu erreichen. Manche davon sind selbst unfair, indem sie sich auf bevorzugte Sprachen beziehen.

Der technische (Haupt-) Teil ihrer Arbeit bezieht sich auf die Gruppenbezeichner als Indikatoren für Hassrede und die dabei mögliche technologische Erzeugung neuerlichen Bias bei der Erkennung und Elimination von Hassreden mittels Klassifikatoren.

Angesichts der ungeheuren Menge an Daten und Texten, die im Internet mittels natürlichsprachlicher Systeme laufend verarbeitet werden, ist es unmöglich, Hassrede, Diskriminierungen und Bias händisch zu eliminieren. Es bedarf daher gut evaluierter automatisierter Mittel, hier der sich bereits für Fairness etabliert habenden erklärbaren KI, solche unerwünschten Vorkommnisse – zumindest teilweise – zu entfernen. Dies kann immer nur im Wechsel mit menschlichen Bewertungen und kontextabhängig erfolgen. Dass dabei notwendigerweise über das Ziel hinaus geschossen wird, da dieselben Begriffe sowohl in abwertender Manier wie auch in neutralem Kontext verwendet werden können, ist ein Phänomen zusätzlicher Erzeugung von Diskriminierung und Bias.

Im Bereich natürlichsprachlicher Verarbeitung (NLP) wird Bias und Diskriminierung automatisiert eliminiert, indem geschützte Attribute, wie Gender und Rasse, für definierte geschützte Gruppen aus Sentiment-Klassifikatoren entfernt werden. Wegen der Komplexität und der Ambiguitäten von Sprache ist schon das erste ein schwieriges Problem, mehr noch das zweite wegen des Black-Box-Charakters der in NLP eingesetzten KI-Methoden. Dabei werden oft Indikatoren wie *LGBTQ* oder *Moslem* als Hassreden definiert, die bei der Verwendung als Klassifikatoren in Sprachmodellen unbeabsichtigt wiederum Biases erzeugen können, etwa weil Minoritäten keine Stimme im Netz bekommen, was demokratieschädlich ist. In dieser Arbeit wird solcher Bias evaluiert, indem eine Liste aus Gruppenbezeichnern erstellt und strukturiert wird. Während des Trainingsprozesses von solchen Modellen werden durch Erklärungsmethoden Beachtungswerte für jeden dieser Bezeichner berechnet. Diese Werte repräsentieren die Menge an Beachtung, die das Sprachmodell Worten während der Klassifizierung schenkt. Sie werden später in der Verlustfunktion genutzt, um das Verhalten des Modells zu korrigieren. Nun untersucht Frau Henningsen die Korrelation zwischen Modell-Entscheidungen und zuvor als neutral angenommenen vordefinierten Gruppen-Identifikatoren, um Bias in den Klassifikatoren aufzeigen zu können. Um Diskriminierung gegen bestimmte Gruppen einzudämmen wird die Verlustfunktion aktualisiert, indem zur Regularisierung ein post hoc verfügbarer Erklärungsscore verwendet wird, der das Modell für Entscheidungen gegen solche geschützten Terme bestraft.

Laudator Stefan Hügel

Die Methode ist insofern nicht neu, als sie bereits mit der Erklärmethode SOC für das Vanilla-Modell erforscht wurde. Frau Henningsen hat die Methode für die Erklärmethode LIME angepasst. Für die Bewertung der resultierenden Modelle nach ihrer Leistung und anhand des verbleibenden Bias entwickelte sie ein Testset, wo sie Satzvorlagen und die Liste an Gruppenbezeichnern kombiniert hat. Bei der Evaluation zeigte sich nicht nur, dass die verbesserten Modelle, die mit der regularisierten Verlustfunktion trainiert wurden, die Leistung gegenüber dem existierenden Vanilla-Modell halten konnten und überraschenderweise auch Genauigkeit bieten, sondern dass auch der Modellbias reduziert werden konnte. Darüber hinaus untermauern die Resultate die Verbindung zwischen der Leistung eines Modells und der Menge an Aufmerksamkeit, die Gruppenbezeichnern beigemessen wird.

Die in perfekter englischer Sprache gehaltene Arbeit enthält eine gute Einführung, ist verständlich geschrieben und zeigt eine Reihe von Tabellen und Grafiken zur Unterstützung der Evaluationsergebnisse. Eine ungewöhnlich lange Literaturliste, auf die referenziert wurde, ergänzt das Werk. Der Grad der Durchdringung sowohl der sozialen, rechtlichen und KI-Problematik, wie auch der technische Neuheitswert sind für eine Bachelorarbeit eine außerordentliche Leistung.

Herzlichen Glückwunsch, Marte Henningsen, zum Weizenbaum-Studienpreis 2022.

Marte Henningsen

1. Preis

Hassrede und erklärbare KI

Im Oktober 2022 machte die Kurzvideoplattform TikTok Schlagzeilen (Eckert et al. 2022), diesmal durch den Umgang der Plattform mit bestimmten Kommentaren zu den dort veröffentlichten Videos. Postings, die bestimmte Worte enthalten, werden gelöscht, ohne die Ersteller:innen der Kommentare zu informieren. Journalist:innen finden mindestens 20 solcher Wörter, die das Sperren eines Kommentars veranlassen, darunter Wörter wie *Nazi* und *Sklaven*, aber auch *gay*, *LGBTQ* und *schwul* sind dabei (ebd.). Das Problem solcher Wortfilter liegt auf der Hand: Ganze Diskurse um beispielsweise Sexualität und Queerness werden verhindert, sowie Aktivist:innen und Betroffene ihrer Bühne auf öffentlicher Plattform beraubt. Begründet wird dies mit dem proaktiven Schutz vor Hassrede. Dies wirft die grundlegende Frage auf:

Wie können und wollen wir als Gesellschaft mit Hassrede umgehen?

Hassrede, also gesprochene oder geschriebene Sprache, die Hass gegenüber Personen oder Personengruppen aufgrund ihrer (vermeintlichen) Geschlechts-, Religions-, Race- und/oder Klassenzugehörigkeit etc. ausdrückt, ist ein großes Problem auf sozialen Netzwerken. Alleine im ersten Quartal 2021 musste Facebook 25 Millionen Posts aufgrund ihres hasserfüllten Inhalts löschen (Facebook 2021). Wenn diese Postings nicht gelöscht werden, können sie verherende Konsequenzen haben. Neben psychologischen Folgen, wie Depression oder Angststörungen (Klaßen und Geschke 2019, Awan und Zempi 2015) und in Extremfällen sogar Suizid (Mullen und Smyth 2004), hat Hassrede auch gesellschaftliche Folgen. Diese werden insbesondere durch die weite Verbreitung von Hassrede auf sozialen Netzwerken hervorgerufen und umfassen beispielsweise Demokratiegefährdung durch sinkende Partizipation an öffentlichen Diskursen (Klaßen und Geschke 2019), wie auch einen Anstieg an Hassverbrechen in der Offline-Welt (Williams et al. 2019, Relia et al. 2019, Müller und Schwarz 2017).

Hassrede stellt also ein gravierendes Problem dar, und unsere Gesellschaft steht vor der Aufgabe, sie zu verhindern oder, wo nötig und möglich, zu löschen. Eine Möglichkeit sind die oben beschriebenen Wortfilter, die TikTok einzusetzen scheint. Dass diese keine wirkliche Lösung sind, ist klar, doch welche anderen Methoden haben wir? Jeden Tag werden eine unfassbare Menge an Postings auf sozialen Netzwerken veröffentlicht: Auf Twitter wurden beispielsweise im Jahr 2020 durchschnittlich 6000 Tweets pro Sekunde abgesetzt (Sayce 2020). Es ist also angesichts dieser schieren Datenmenge nicht möglich, alle Postings vor der Veröffentlichung manuell zu prüfen. Heutzutage ist es gängig, dass Nutzer:innen einer Plattform Inhalte, die gegen Richtlinien verstoßen, melden können. Diese werden dann geprüft und eventuell gelöscht. Doch wer prüft und entscheidet über die gemeldeten Posts? Casey Newton, amerikanischer Journalist, veröffentlichte mehrere Artikel über die Menschen, die in den USA die gemeldeten Inhalte von Facebook-Nutzer:innen sichten und entscheiden müssen, ob ein Post auf der Plattform bleiben darf oder gelöscht wird (Newton 2019b, Newton 2019a). Er beschreibt Menschen, die in Vollzeit Inhalte, wie zum Beispiel Videos von Morden, Kindesmisshandlung und Verschwörungstheorien, sichten müssen. Er beschreibt Panikattacken, Leistungszwang, und zusammenbrechende Kollegen und Kolleginnen, sowie die Tatsache, dass einige Inhaltsmoderator:innen gegenüber den dargestellten rassistischen, antisemitischen, sexistischen Ansichten abstumpfen oder sogar selbst anfangen, die gemeldeten Verschwörungserzählungen zu glauben.

Menschen diesen verstörenden Inhalten, darunter auch Hassrede, in diesem Ausmaß auszusetzen, ist also offensichtlich auch keine Lösung. Warum also nicht eine KI arbeiten lassen? Diese kann schließlich keine posttraumatische Belastungsstörung davon tragen und ist außerdem schneller als ein Mensch. Mit diesem Ansatz habe ich mich in meiner Bachelorarbeit beschäftigt.

KI als Lösung!

Dieser Ansatz scheint viele Vorteile zu bieten. Eine KI kann der riesigen Menge an Postings, die jede Minute auf den Plattformen veröffentlicht wird, standhalten, kostet weniger als Arbeiter:innen, nimmt keinen Schaden an den ‚gesehenen' Inhalten und kann sogar angewendet werden, bevor ein Post oder Kommentar veröffentlicht wird. So muss die Plattform nicht auf unzuverlässige Nutzer:innen-Meldungen vertrauen und im Zweifelsfall werden Hassrede und anderer verstörender Content gar nicht erst öffentlich gemacht. Doch es gibt ein Problem. Die entwickelten KI-Systeme zeigen einen Bias. Das Problem lässt sich mit dem Bild eines stochastischen Papageis (Bender et al. 2021) visualisieren. Bender et al. beschreiben, wie große Sprachmodelle, wie etwa BERT (Devlin et al. 2018), GPT-3 (Brown et al. 2020) und zuletzt auch ChatGPT (OpenAI 2022) Sprache nicht wie Menschen analysieren, sondern lediglich die stochastischen Korrelationen, die in den Sprachbeispielen der Trainingsdaten vorkommen, finden und anwenden. Das ist auch beim Beispiel der Hassrede relevant.

Da in Hassrede oft sogenannte Gruppenbezeichner vorkommen, werden diese als Indikator für die Hassrede selbst genommen. Gruppenbezeichner sind hier Wörter, die eine Personengruppe mittels ihres Geschlechts, ihrer Religion, Race und weiteren Merkmalen identifiziert, also beispielsweise *Schwarz*, *Juden*, *Frau* oder *Lesben*. Hassrede betrifft per Definition bestimmte Menschengruppen, die mittels solcher Gruppenbezeichner adressiert werden können, also kommen diese Wörter auch besonders häufig in Hassrede vor. Dabei ist Gruppenbezeichner natürlich nicht gleich Gruppenbezeichner. Auch Begriffe wie *Mann* und *Christ* sind denkbar, allerdings werden diese Gruppen deutlich seltener Ziele von hasserfüllten Kommentaren. Auch das haben die KI-Systeme gelernt: Nur bestimmte Gruppenbezeichner führen zu einer fälschlicherweise erkannten Hassredeklassifikation.

In meiner Bachelorarbeit habe ich zunächst diesen Bias untersucht und anschließend Methoden aus dem Bereich der erklär-

baren KI genutzt, um genau diesen Bias zu reduzieren. Dabei habe ich mich an dem Paper Kennedy et al. 2020a orientiert, die mittels der SOC (Sampling and Occlusion) Methode den gefundenen Bias des KI-Modells reduziert haben. Das untersuchte Sprachmodell ist das BERT-*(Bidirectional Encoder Representation from Transformers)* Modell (Devlin et al. 2018), welches anhand von großen Datenmengen in englischer Sprache vortrainiert ist. Es kann dann für spezifische Anwendungsgebiete nochmals auf speziellen Trainingssets trainiert werden, hier also auf Trainingssets, die viele kurze Texte enthalten, die jeweils mit einem Label (Hassrede oder keine Hassrede) versehen sind. Kennedy et al. 2020a nutzen für diesen Schritt den *Gab Hate Corpus* (GHC)(Kennedy et al. 2020b), welcher aus einem Trainingsset mit über 22.000 Einträgen und einem Testset mit über 5.000 Einträgen besteht. Das Testset ermöglicht es, die Genauigkeit des trainierten Modells zu evaluieren, indem es Texte bereitstellt, mit denen das KI-System nicht gelernt hat, sie also noch nicht ‚kennt'. Der GHC wurde mit Postings der Seite gab.ai, einem sozialen Netzwerk aus den USA mit einer extrem rechten Nutzer:innenschaft (Jasser et al. 2021), erstellt und beinhaltet über 2.000 Postings (ca 8 % aller Datenpunkte), welche als Hassrede klassifiziert wurden.

Gründe dafür, dass der Erkennungsalgorithmus Hassrede mit bestimmten Gruppenbezeichnern gleichsetzt, lassen sich bereits in der Analyse des Trainingssets finden. Über 50 % der Datenpunkte, welche als Hassrede eingestuft wurden, beinhalten Gruppenbezeichner, während nur 14 % der anderen Datenpunkte solche Begriffe enthalten. Es scheint also für den Algorithmus eine logische Schlussfolgerung zu sein, dass Wörter wie *Jude* oder *schwul* ein Indikator für Hassrede sind. In meiner Bachelorarbeit habe ich noch ein weiteres Datenset verwendet, nämlich ein selbst konstruiertes Testset, um den Bias des untersuchten KI-Modells besser evaluieren zu können. Damit kann also nicht die allgemeine Leistung des Algorithmus getestet werden, sondern spezifisch, wie er für verschiedene Gruppenbezeichner abschneidet. Dafür habe ich eine Liste von verschiedenen Gruppenbezeichnern erstellt, welche aus 83 Begriffen besteht, die jeweils in 3 Kategorien (Gender, sexuelle Orientierung, sowie Race & Religion) eingeordnet und nach dem Status der Diskriminierung (diskriminiert und nicht diskriminiert) unterschieden wurden. Das konstruierte Testset wurde mittels dieser Liste und verschiedenen Testphrasen, in welche die Gruppenbezeichner eingefügt wurden, erstellt und umfasst knapp 1.500 Einträge, von denen 50 % als Hassrede klassifiziert wurden. Jeder Datenpunkt enthält einen Gruppenbezeichner und alle Gruppenbezeichner kommen gleich häufig vor, um eine Vergleichbarkeit zu gewährleisten.

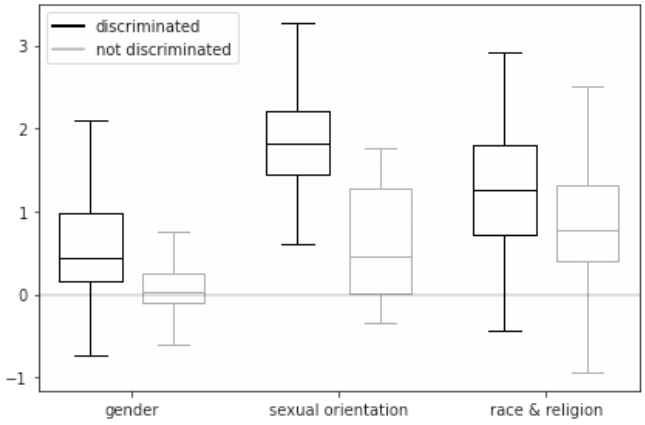
Um den Bias zu reduzieren, nutzen Kennedy et al. die bereits erwähnte Methode *Sampling and Occlusion* (SOC), welche von Jin et al. 2019 entwickelt wurde. Diese Methode stammt aus dem Bereich der erklärbaren KI und berechnet sogenannte Aufmerksamkeitswerte (*attention scores*), für die einzelnen Elemente eines Inputs. Wenn also erklärt werden muss, warum ein Posting auf einer sozialen Plattform eine bestimmte Klassifikation erhalten hat, können solche Methoden verwendet werden, da sie die Satzteile mit den höchsten Aufmerksamkeitswerten zurück geben können. Dafür berechnet die Methode, wie wichtig die einzelnen Wörter oder Wortteile für die Klassifikation des gesamten Inputs sind. Sie generiert aus dem Inputtext weitere ähnliche Texte, indem Satzteile verändert werden. Diese Input-Nachbarschaft wird dann durch das Modell klassifiziert, damit durch Unterschiede in der Klassifizierung zwischen dem originalen und den veränderten Texten ermittelt werden kann, wie wichtig einzelne Bestandteile für eine Klassifizierung sind. Diese Aufmerksamkeitswerte werden dann hier nicht dazu genutzt, um zu erklären, warum ein Posting aus den sozialen Medien gesperrt wurde, sondern, um das KI-Modell zu verbessern und seinen Bias zu reduzieren. Das geschieht, indem das Modell ‚bestraft' wird, wenn es einem Gruppenbezeichner zu viel Bedeutung bei der Klassifikation beimisst. In der Trainings-/Verfeinerungsphase des Modells wird es immer wieder getestet, um zu verifizieren, dass es gut funktioniert. In diesen Verifizierungsdurchläufen wird hier auf jeden Input, der einen Gruppenbezeichner enthält, der in einer vorher definierten Liste vorkommt, diese Erklärmethode angewandt, um herauszufinden, ob das System bei der Klassifizierung zu stark auf diese Begriffe vertraut. Falls dies der Fall ist, wird eine Straffunktion verwendet, um dieses Verhalten künstlich zu verändern.

Die unten stehende Tabelle zeigt die Evaluation von drei Varianten des Modells: Einmal ohne Biasreduktion, und zweimal mit Biasreduktion (BR), wobei jeweils unterschiedliche Listen von Gruppenbezeichnern genutzt wurden. Liste A umfasst 25 Begriffe und wurde von Kennedy et al. 2020a verwendet, während Liste B meine erweiterte Liste mit 83 Begriffen bezeichnet. Für jede Modellvariante wurden die Genauigkeitswerte berechnet und für das konstruierte Testset konnten die spezifischen Genauigkeiten für diskriminierte (d) und nicht-diskriminierte ($\overline{d}$) berechnet werden, sowie der Unterschied zwischen diesen beiden Werten.

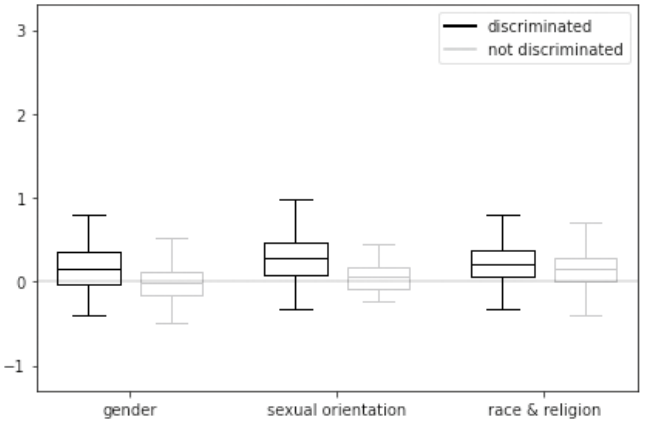
		BERT Base	BR Liste A	BR Liste B
GHC Testset	Genauigkeit [%]	88.43	87.21	86.99
konstruiertes Testset	Genauigkeit [%]	71.37	74.04	75.62
	Genauigkeit d [%]	67.84	73.33	75.20
	Genauigkeit $\overline{d}$ [%]	76.14	75.68	76.59
	Unterschied	8.30	2.35	1.39

Man erkennt, dass alle Modelle ähnlich gut auf dem GHC Testset abschneiden mit leicht abfallenden Werten, je ausgeprägter die Biasreduktion ist. Interessant sind die Unterschiede zwischen den Modellen für das konstruierte Testset. Alle 3 Modelle schneiden schlechter als beim ersten Testset ab, aber die Genauigkeit steigt mit der Stärke der Biasreduktion an. Besonders aufschlussreich sind die Genauigkeitsunterschiede der Modelle, abhängig davon, ob die bezeichneten Gruppen typischerweise diskriminiert werden. Je umfangreicher die Biasreduktion ist, desto geringer ist der Unterschied, den das Modell hier aufweist: Während das ursprüngliche Modell noch über 8 Prozentpunkte Unterschied zwischen den beiden Gruppen verzeichnet, sind es bei dem auf Liste B trainierten Modell nur noch 1,39 Prozentpunkte Unterschied.

Die Entwicklung der Aufmerksamkeitswerte für die Gruppenbezeichner aus Liste B wird in Abbildung 1 dargestellt. Die links stehende Grafik zeigt die berechneten Werte vor der Anwendung der Erklärmethode zur Biasreduktion, während die rechts stehende Grafik die Werte nach der Biasreduktion mithilfe von



(a) BERT Base



(b) Biasreduktion Liste B

Abbildung 1: Aufmerksamkeitswerte vor und nach der Biasreduktion

Liste B zeigt. Die Aufmerksamkeitswerte sind gruppiert nach Kategorie und Diskriminierungsstatus.

Es fällt auf: Vor Anwendung der Biasreduktion wird Gruppenbezeichnern typischerweise diskriminierter Gruppen mehr Aufmerksamkeit geschenkt als denen typischerweise nicht diskriminierter Gruppen. Für alle drei Kategorien gilt, dass Gruppenbezeichner von diskriminierten Gruppen stärker zu einer Klassifizierung als Hassrede beitragen.

Man erkennt außerdem, dass die Erklärmethode erfolgreich zur Reduktion von Bias genutzt wurde. In der rechten Grafik sind die Aufmerksamkeitswerte deutlich niedriger und die Unterschiede zwischen den verschiedenen Gruppen hat sich verringert. Die Gruppenbezeichner tragen deutlich weniger zur Entscheidungsfindung bei der Klassifikation bei und damit werden also die Fälle minimiert, in denen fälschlicherweise ein Post aufgrund eines Gruppenbezeichners als Hassrede klassifiziert wird. Es stellt sich eventuell die Frage, warum man nicht einfach manuell diese Werte auf 0 setzen kann, wenn das Ziel zu sein scheint, ihnen so wenig Aufmerksamkeit wie möglich im Entscheidungsprozess zu schenken. Ganz so leicht ist es leider auch nicht, da Gruppenbezeichner durchaus ausschlaggebend sein können. Wenn man sich beispielsweise die Sätze „Ich hasse Spinnen“ und „Ich hasse Muslime“ anschaut, stellt man fest, dass sie sich im Satzbau, bis auf das letzte Wort, nicht unterscheiden. Eines ist ein Gruppenbezeichner und das Andere beschreibt ein Tier. Hier ist es wichtig, dass das System erkennt, dass der Gruppenbezeichner „Muslime“ dem Satz eine ganz andere Tragweite zukommen lässt, als das Wort „Spinnen“ an der selben Stelle. Es muss also eine goldene Mitte gefunden werden, in der Hassrede als solche erkannt wird, aber dabei betroffenen Gruppen ihre Bühne auf sozialen Netzwerken nicht durch eine übermäßige Anzahl an falschen Löschungen streitig gemacht wird.

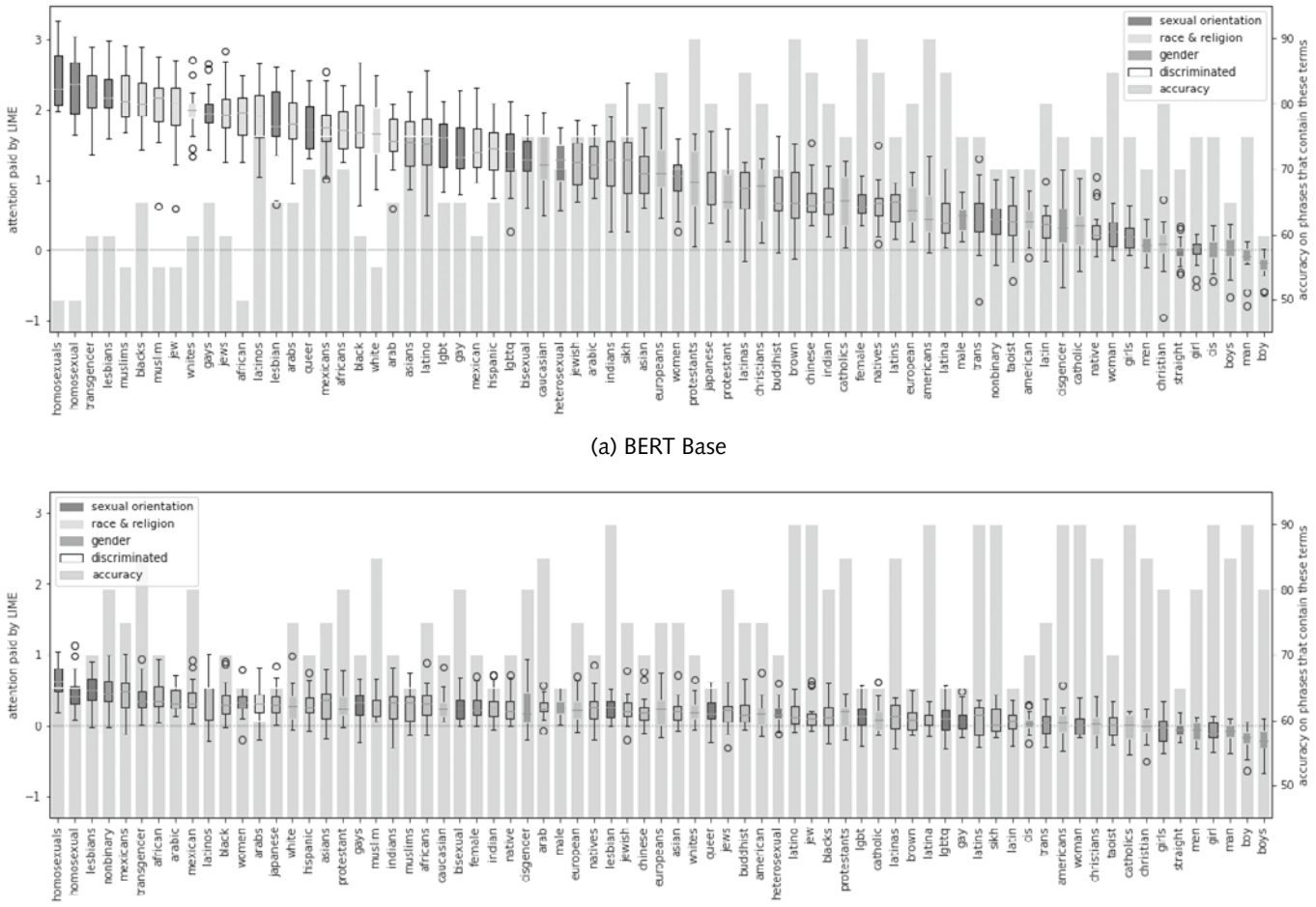
Abbildung 1 zeigt also, dass das verbesserte Modell bei der Klassifikation den Gruppenbezeichnern weniger Wert beimisst, aber sie zeigt nicht, ob es Hassrede auch besser erkennt. Diesen Zusammenhang zeigen die beiden Grafiken in Abbildung 2. Hier sind alle Gruppenbezeichner aus Liste B aufgeführt. Für alle Begriffe sind die berechneten Aufmerksamkeitswerten sowie die Genauigkeit des Modells auf dem konstruierten Testset aufgeführt. Die obere Grafik zeigt die Ergebnisse für die Modellvariante vor der Biasreduktion und die untere Grafik die Werte des Modells, für welches mit Liste B der Bias reduziert wurde.

Man sieht, dass in der oberen Grafik ein grober antiproportionaler Zusammenhang zwischen Performance und Aufmerksamkeitswert besteht. Je größer der Aufmerksamkeitswert, desto niedriger die Genauigkeit. Darüber hinaus sieht man, dass sich die Genauigkeit des Modells nach der angewandten Biasreduktion verbessert hat und die Unterschiede der Gewichtung zwischen den einzelnen Gruppenbezeichnern geringer geworden ist. Das Modell hat also nicht an Leistung eingebüßt, während ein entdeckter Bias reduziert wird. Methoden aus dem Bereich der erklärbaren KI helfen also nicht nur, Einblicke in die Blackbox zu gewähren, die viele KI Systeme darstellen, sondern können darüber hinaus auch für Verbesserungen des Modells selber während des Trainingsprozess angewandt werden.

KI als Lösung?

Wie eingangs erwähnt, hat die Verwendung von KI-Systemen zur Erkennung von Hassrede im Internet viele Vorteile und wir sind sogar in der Lage, einen nicht beabsichtigten Bias zu minimieren. Doch das grundlegende Problem von Hassrede ist viel tiefliegender, und auch ein Anflug von Tech-Solutionismus kann es nicht eben so lösen. Auch nicht, wenn jeder Bias entdeckt und minimiert ist. Im Nachfolgenden erläutere ich einige Grenzen der hier beschriebenen Technologie.

Zunächst bleibe ich auf der Ebene des beschriebenen Frameworks. So ist es beispielsweise der Fall, dass die gewählten Gruppenbezeichner von mir als weiße, europäische cis-Frau ausgewählt wurden. Ich habe versucht, so gewissenhaft wie möglich vorzugehen, aber es ist nicht auszuschließen, dass ich verschiedene Gruppenbezeichner ausgelassen habe, weil ich sie zum Beispiel nicht kenne. Hier zeigt sich also auch, wie die eigene Situiertheit von Forschern und Forscherinnen die entwickelte Technologie beeinflusst. Während Diskriminierungsdiskurse, die hier viele mediale Beachtung bekommen, in der Biasreduktion widergespiegelt werden, werden andere Diskriminierungserfahrungen weiterhin ausgeblendet. Die oben beschriebene Liste



(a) BERT Base

(b) Biasreduktion Liste B

Abbildung 2: Aufmerksamkeitswerte sowie Genauigkeit des Modells für die einzelnen Begriffe vor und nach der Biasreduktion

müsste also stetiger Verbesserung und Ergänzungen unterzogen werden. Darüber hinaus ist das konstruierte Testset vergleichsweise klein und für eine noch klarere und tiefere Biasanalyse müsste auch dieses erweitert werden.

Darüber hinaus lohnt es sich, nicht nur auf Verbesserungsmöglichkeiten innerhalb der Technologie zu schauen, sondern auch über die Grenzen der Anwendung nachzudenken. Ein Problem bei der Erkennung von Hassrede ist, dass diese stark kontextabhängig ist (Castelle 2018). Wenn ich beispielsweise meine Freundinnen *Bitches* nenne, hat das eine ganz andere Bedeutung, als wenn ein wildfremder Mann uns das auf der Straße zuruft. Diese verallgemeinerte Kontextabhängigkeit lässt sich auch auf den digitalen Raum übertragen. Um diese Unterschiede mit einer KI identifizieren zu können, wären mehr (sensitive) Informationen der Nutzer:innen nötig, wodurch weitere Bedenken bezüglich Datenschutz und Überwachung entstehen. Darüber hinaus ist es auch denkbar, dass eine Art Katz-und-Maus-Spiel zwischen Nutzer:innen und KI-Systemen, beziehungsweise deren Entwickler:innen, stattfindet. Dieses Phänomen besteht schon länger in Subkulturen von sozialen Netzwerken, beispielsweise pro-Anorexia-Gruppen (Chancellor et al. 2016). In Bezug auf die eingangs erwähnten Wortfilter auf TikTok haben sich ebenfalls viele neue Wörter hervorgetan, um trotzdem über Themen wie Diskriminierung und mentale Gesundheit sprechen zu können, ohne durch Verwendung von Wörtern wie *Suizid* oder *LGBTQ* an Reichweite zu verlieren. Die amerikanische Journalistin Taylor Lorenz gab dieser entstehenden Sprache den Namen *Algospeak* (Lorenz 2022). Auch im Bezug auf Hassrede ist diese Entwicklung denkbar. Während Beleidigungen wie *Dummkopf* erkannt werden können, sieht es bei der Zeichenkette *Dummk0pf* schon anders aus. Für den Algorithmus ist dies ein völlig neues und unbelastetes Wort und er würde es nicht als Beleidigung erkennen, während andere Nutzer:innen der Plattform sofort entziffern können, was das Posting bedeuten soll. Dieselbe Entwicklung ist genauso bei deutlich schwerwiegenderen Beleidigungen möglich. Berichte, wie Sonnad 2016 und Farabee 2021, zeigen, dass rechtsextreme Nutzer:innen schnell Alternativworte oder Emojis finden, um ihre hasserfüllten Ansichten trotz eines KI-Filters veröffentlichen zu können.

Darüber hinaus muss klar sein, dass Hassrede als Ausdruck von Rassismus, Sexismus, Klassismus und jeder weiteren Unterdrückungsform ein gesellschaftliches Problem darstellt und sich nicht mit einer neuen Technologie lösen lässt. Die menschenfeindlichen Ressentiments hinter Hassrede lösen sich schließlich nicht in Wohlgefallen auf, nur weil ein entsprechender Kommentar nicht mehr auf Facebook veröffentlicht wird. Die Effekte der Technologie auf die Verfasser:innen von Hassrede sind noch nicht tiefgehend erforscht. Chandrasekharan et al. 2017 zeigten, dass die Löschung von mehreren Reddit-Foren mit großem Anteil von Hassrede erfolgreich war, weil die betroffenen Nutzer:innen nicht merklich auf andere Bereiche der Plattform auswichen. Es ist aber durchaus denkbar, dass die Nutzer:innen

sich einfach auf anderen Plattformen als Reddit angemeldet haben. Rechtsextreme Internetforen gibt es schließlich reichlich. Baele et al. 2023 zeigen beispielsweise, dass durch Löschung von Plattformen sich zwar weniger gut besuchte aber immer extremere Onlinegemeinschaften entwickeln. Das Löschen von Hassrede kann also auch einen gegenteiligen Effekt haben als ursprünglich beabsichtigt und zu einer weiteren Extremisierung von Teilen der Gesellschaft beitragen.

Natürlich ist es richtig und wünschenswert, dass Nutzer:innen auf sozialen Plattformen keiner Hassrede mehr ausgesetzt sind. So können die eingangs beschriebenen gravierenden Folgen für Individuen und Gesellschaft reduziert werden, doch leider ist das Problem vielschichtiger. Löschung von Hassrede im Internet kann nur ein Teil eines viel größer gedachten Ansatzes darstellen, um dem Hass zu begegnen, dem viele Menschen unserer Gesellschaft noch immer Tag für Tag ausgesetzt sind. Joseph Weizenbaum schrieb 2001

> *„Wichtig ist immer, in welches gesellschaftliche Umfeld ein Massenmedium, egal welches, eingebaut ist. […] Jedes Instrument erbt und erhält seinen Wert von der Gesellschaft, in die es eingebettet ist. (Weizenbaum et al. 2001: 32)*

Es ist also auch unsere Aufgabe als Informatiker:innen, genau die Frage nach dem gesellschaftlichen Umfeld nicht aus den Augen zu verlieren. Aus diesem Grund möchte ich dem Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung zum einen für die Auszeichnung mit dem Weizenbaum-Studienpreis, aber vor allem für ihre wichtige Arbeit danken.

Referenzen

Awan, Imran und Irene Zempi (2015). ‚I will Blow your face off' Virtual and Physical World Anti-Muslim Hate Crime. In: The British Journal of Criminology, azv122. issn: 0007-0955. doi: 10.1093/bjc/azv122.

Baele, Stephane, Lewys Brace und Debbie Ging (Jan. 2023). A Diachronic Cross-Platforms Analysis of Violent Extremist Language in the Incel Online Ecosystem . In: Terrorism and Political Violence, S. 1 24. doi: 10.1080/09546553.2022.2161373. (Besucht am 15. 02. 2023).

Bender, Emily M. et al. (2021). On the Dangers of Stochastic Parrots . In: Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency. New York, NY, USA: ACM, S. 610 623. isbn: 978-1-4503-8309-7. doi: 10.1145/3442188.3445922.

Brown, Tom et al. (2020). Language Models are Few-Shot Learners . In: Advances in Neural Information Processing Systems. Hrsg. von H. Larochelle et al. Bd. 33. Curran Associates, Inc, S. 1877 1901. url: https://proceedings.neurips.cc/paper/2020/file/1457c0d6bfcb4967418bfb8ac142f64a-Paper.pdf.

Castelle, Michael (2018). The Linguistic Ideologies of Deep Abusive Language Classification . In: Proceedings of the 2nd Workshop on Abusive Language Online (ALW2). Hrsg. von Darja FiÇer et al. Stroudsburg, PA, USA: Association for Computational Linguistics, S. 160 170. doi: 10.18653/v1/W18-5120.

Chancellor, Stevie et al. (Feb. 2016). #thyghgapp: Instagram Content Moderation and Lexical Variation in Pro-Eating Disorder Communities . en. In: Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing. San Francisco California USA: ACM, S. 1201 1213. isbn: 978-1-4503-3592-8. doi: 10.1145/2818048.2819963. url: https://dl.acm.org/doi/10.1145/2818048.2819963 (besucht am 15. 02. 2023).

Chandrasekharan, Eshwar et al. (2017). You Can't Stay Here: The Efficacy of Reddit's 2015 Ban Examined Through Hate Speech. In: Proceedings of the ACM on Human-Computer Interaction 1.CSCW, S. 1 22. doi: 10.1145/3134666.

Devlin, Jacob et al. (2018). BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. url: http://arxiv.org/pdf/1810.04805v2.

Eckert, Svea, Catharina Felke und Oskar Vitlif (Okt. 2022). TikTok schränkt Meinungsfreiheit ein. In: tagesschau, NDR. url: https://www.tagesschau.de/investigativ/ndr/tik-tok-begriffe-101.html.

Facebook (2021). Global number of hate speech-containing content removed by Facebook from 4th quarter 2017 to 1st quarter 2021. url: https://www.statista.com/statistics/1013804/facebook-hate-speech-content-deletion-quarter/.

Farabee, Mindy (Aug. 2021). AI is still bad at detecting hate speech – Here's a way to make it better. Hrsg. von Columbia Engineering Magazine. url: https://magazine.engineering.columbia.edu/ai-still-bad-detecting-hate-speech-heres-way-make-it-better.

Jasser, Greta et al. (Juni 2021). ‚Welcome to #GabFam': Far-right virtual community on Gab. In: New Media & Society. doi: 10.1177/14614448211024546. (Besucht am 15. 02. 2023).

Jin, Xisen et al. (2019). Towards Hierarchical Importance Attribution: Explaining Compositional Semantics for Neural Sequence Models. url: http://arxiv.org/pdf/1911.06194v2.

Kennedy, Brendan et al. (2020a). Contextualizing Hate Speech Classi ers with Post-hoc Explanation. url: http://arxiv.org/pdf/2005.02439v3.

Kennedy, Brendan et al. (2020b). The Gab Hate Corpus. doi: 10.17605/OSF.IO/EDUA3.

Klaßen, Anja und Daniel Geschke (2019). Forschungsbericht: Wahrnehmung, Betro enheit und Folgen von Hate Speech im Internet aus Sicht der Thüringer Bevölkerung: Ergebnisse einer repräsentativen Befragung im Juni 2019. Place: Jena. url: https://www.idz-jena.de/fileadmin/user_upload/IDZ_Sonderheft_Hate_Speech_WEB.pdf.

Lorenz, Taylor (Apr. 2022). Internet ‚algospeak' is changing our language in real time, from ‚nip nops' to ‚le dollar bean'. In: The Washington Post.

Marte Henningsen

Marte Henningsen studiert seit 2021 Kognitionswissenschaften im Master an der Universität Osnabrück. Davor hat sie Bachelorabschlüsse in Informatik und Computergestützten Ingenieurwissenschaften an der Leibniz Universität Hannover gemacht. Sie ist studentische Hilfskraft der Arbeitsgruppe ‚Ethik der KI' in Osnabrück und sie befasst sich schwerpunktmäßig mit den Auswirkungen von KI Systemen auf Arbeit und Gesellschaft.

url: https://www.washingtonpost.com/technology/2022/04/08/algos-peak-tiktok-le-dollar-bean/.
Mullen, Brian und Joshua M. Smyth (2004). Immigrant Suicide Rates as a Function of Ethnophaulisms: Hate Speech Predicts Death. In: Psychosomatic Medicine 66.3, S. 343. issn: 0033-3174. url: https://journals.lww.com/psychosomaticmedicine/fulltext/2004/05000/immigrant_suicide_rates_as_a_function_of.9.aspx.
Müller, Karsten und Carlo Schwarz (2017). Fanning the Flames of Hate: Social Media and Hate Crime. In: SSRN Electronic Journal. doi: 10.2139/ssrn.3082972.
Newton, Casey (Juni 2019a). Bodies in Seats . In: The Verge. url: https://www.theverge.com/2019/6/19/18681845/facebook-moderator-interviews-video-trauma-ptsd-cognizant-tampa.
Newton, Casey (Feb. 2019b). The Trauma Floor: The secret lives of Facebook moderators in America. In: The Verge. url: https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona. OpenAI (Nov. 2022). ChatGPT: Optimizing Language Models for Dialogue. url: https://openai.com/blog/chatgpt/.
Relia, Kunal et al. (2019). Race Ethnicity and National Origin-Based Discrimination in Social Media and Hate Crimes across 100 U.S. Cities . In: Proceedings of the International AAAI Conference on Web and Social Media 13.01, S. 417 427. url: https://ojs.aaai.org/index.php/ICWSM/article/view/3354.
Sayce, David (2020). The Number of tweets per day in 2020. url: https://www.dsayce.com/social-media/tweets-day/.
Sonnad, Nikhil (Okt. 2016). Alt-right trolls are using code words for racial slurs online. url: https://qz.com/798305/alt-right-trolls-are-using-googles-yahoos-skittles-and-skypes-as-code-words-for-racial-slurs-on-twitter/.
Weizenbaum, Joseph, Gunna Wendt und Franz Klug, Hrsg. (2001). Computermacht und Gesellschaft: Freie Reden. Orig.-Ausg., 1. Au . Bd. 1555. Suhrkamp Taschenbuch Wissenschaft. Frankfurt am Main: Suhrkamp. isbn: 3-518-29155-6.
Williams, Matthew L. et al. (2019). Hate in the Machine: Anti-Black and Anti-Muslim Social Media Posts as Predictors of Offline Racially and Religiously Aggravated Crime. In: The British Journal of Criminology. issn: 0007-0955. doi: 10.1093/bjc/azz049.

Weizenbaum-Studienpreis – Laudatio für den ersten Preis

Linus Feiten: Take the Power back! Secrecy, Accountability and Trust in the Digital Age

Dissertation an der Universität Freiburg im Breisgau

Die Wissenschaft Informatik befasst sich erst seit kurzer Zeit umfassender und interdisziplinär mit Sicherheitsaspekten, insbesondere der hier behandelten Hardware-Sicherheit. Einen Anfang dazu machte das Zero-Trust-Paradigma, später gefolgt von Zero-Trust-Architekturen.

Während gespeicherte Daten ursprünglich eng verbunden waren mit den zugehörigen Hard- und Software-Speichermedien, sind sie heute nur mehr sehr indirekt zugänglich über Mensch-Maschinen-Interfaces, die weder ihren Ort noch ihre Spuren, noch Formate und Strukturen, noch Zusammenhänge untereinander in den inneren Strukturen von Microchips, Harddisk oder Flash-Memory preisgeben. Um Datenmanipulation oder -diebstahl zu vermeiden, wäre es umso wichtiger, Mittel zum Datenschutz sowohl in Hard- wie in Software, auch von Netzwerken, angemessen zu implementieren, damit das Recht zur informationellen Selbstbestimmung auch erfüllt werden kann. Vertrauen beinhaltet nicht nur, dass man etwas weiß, sondern auch dass es allgemein glaubhaft ist und dass dieses Vertrauen auf gültiger Evidenz beruht. Für vertrauenswürdige Computersysteme muss die Evidenz sowohl sozial als auch technologisch gelten.

Die *European General Data Protection Regulation* [48, Art. 23] soll zu mehr Datensouveränität mittels sozialwissenschaftlicher Mechanismen führen. Hier bedeutet Vertrauen die Überzeugung in die Ehrlichkeit und Integrität einer Person oder Institution, auch wenn es dafür keine Garantie oder Beweise gibt. Zum Zugang zu sensiblen Daten verlangen Zero-Trust-Systeme einen Sicherheitsrahmen, wo sich alle User authentifizieren und autorisiert sein müssen, d. h. bevor sie Zugang zu Anwendungen und Daten erhalten, müssen sie validiert werden.

Hier aber geht es um technologische Mechanismen zur Erhöhung von Vertrauen, indem den Bürger:innen maximale Einsicht und Transparenz hinsichtlich der Datensicherheit gewährt werden sollen. Leider sind für die komplexen Prozesse Vertraulichkeit und Zurechenbarkeit derzeit kaum erreichte Wünsche, ja noch schwieriger wäre die Überprüfung der korrekten Implementierung derselben bereits durch Professionelle, völlig unmöglich hingegen durch Laien. Die Frage ist daher, wie Vertrauen in ein System bei der Prozessierung sensitiver Daten hergestellt werden kann, und wie Menschen die Souveränität über ihre Daten (zurück) erhalten können. Die vorgelegte Arbeit trägt ein wenig, d. i. so viel wie maximal in diesem Rahmen möglich, dazu bei.

Ein Problem dabei ist, dass ein Computer Chip in Operation eine Black Box für menschliche Sinne ist, egal welche Expertise ein:e Betrachter:in haben mag. Sie kann aufgrund des E/A-Verhaltens Annahmen über des Chips Vertrauenswürdigkeit machen, aber diese können falsch sein, wenn der Chip schlecht designed oder modifiziert wurde. In *Hardware Security or Trusted Hardware* nennt man ein IT-device *trusted*, wenn beweisbar ist, dass es nicht korrumpiert wurde; genauer, wenn die Kosten für eine unentdeckte Korruption so hoch sind, dass sie unwahrscheinlich ist. Für das Erreichen informationeller Selbstbestimmung bedarf es sowohl verifizierbarer *trustable* Hard- und Software als auch sozialen Vertrauens in Personen mit Zugang und natürlich auch deren informierten Vertrauens in die verifiziert vertrauenswürdigen Systeme und ihre Umgebungen.

Das Szenario, in dem die entwickelten Methoden hier exemplarisch vorgeführt werden, ist die Videoüberwachung: die Kame-

ras (vertrauenswürdige Systeme) nehmen dann Aufnahmen von Personen (personenbezogene Daten) nur in kryptierter Form, wobei der Schlüssel für die Dekryptierung nur einer vertrauenswürdigen dritten Partei verfügbar ist. Damit sich Bürger:innen, die sich so überwacht wissen, dennoch frei bewegen und äußern können, bedarf es ihres Vertrauens in die beschriebene Technologie.

Herr Feiten hat dazu das Konzept der digitalen Tarnkappe (DCI = *Digital Cloak of Invisibility*) im Laufe einer Jahre andauernden Kooperation mit Forschern anderer Fachrichtungen (Geistes-, Sozial und Rechtswissenschaften) wesentlich mitentwickelt, aber auch die technische Realisierbarkeit mit seiner Arbeit am Beispiel digitalisierter Videoüberwachung umgesetzt. Wenn die Hardware über den gesamten Nutzungszeitraum als vertrauenswürdig angenommen werden kann, ermöglicht die DCI, personenbezogene Daten automatisiert zu entfernen (für Videosequenzen ist die Umgebung sichtbar, aber Personen sind zunächst ausgeblendet), aber sie – nur bei Vorliegen entsprechender Legitimation – (selektiv) sichtbar zu machen. Eine DCI konstituiert also eine Gewaltenteilung für das Sammeln, Speichern und Analysieren von personenbezogenen Daten.

Ein Mittel, um Datensicherheit und mit *Trusted Hardware* Vertrauen zu ermöglichen, sind *Physically Unclonable Functions* (PUFs) als Komponenten einer DCI-Implementierung. Eine PUF wurde für die Beispielanwendung implementiert.

An Methoden wurden Hash-, Hardware-Security-Funktionen und vorwiegend Kryptographie verwendet, aber das Gesamtkonzept berücksichtigt den Workflow, eine GUI, die FPGA-Architektur, Qualitätsmetriken und vieles andere. Die Implementierung von delay-basierten PUFs wurde auf *Intel Field FPGA Programmable* (in Hardware Description Language HDL) *GateArray* dargestellt. Delay-basierte PUFs verwenden die Verzögerungszeiten einzelner Leitungen als chip-spezifische Charakteristika, aus denen die Schlüssel abgeleitet werden. Am Ende entwickelte Feiten Methoden wie Ring-Oszillator (RO)-PUFs, die mit der Intel-FPGA-Architektur und den zugehörigen Design-Tools implementiert und verfeinert werden können. PUFs können das Vertrauen erhöhen, wenn sich die geheimen Schlüssel nicht im Speicher eines Geräts befinden. Stattdessen werden die Schlüssel aus physikalischen Eigenschaften abgeleitet, die für jeden individuellen Chip einzigartig sind. Solche aus physikalischen Eigenschaften abgeleitete PUF-generierte Schlüssel sind nicht nur schwerer durch Angriffe auf die Hardware zu extrahieren, sie sind auch empfindlich gegenüber Manipulationsversuchen, was in der Arbeit gezeigt wurde.

Manche offene Fragen werden im Weiteren angesprochen: z. B., wie kann die Vertrauenswürdigkeit der Hardware auf nachvollziehbare und transparente Weise an Laien vermittelt werden, oder wer agiert über die verschiedenen Instanzen in der durch die DCI konstituierten Gewaltenteilung, und was macht sie gegenüber der Öffentlichkeit vertrauenswürdig?

Herr Feiten hat seine Forschungen und Implementierungen in vielen Veröffentlichungen und auf Workshops bekannt gemacht. Sein Gesamtwerk scheint mir der Idealfall einer interdisziplinären Informatik-Arbeit zu sein, die aus der Kooperation mit anderen Disziplinen heraus zu geeigneten Kombinationen von Bekanntem und Neuem aus der Hardware-Sicherheit zur Lösung eines komplexen Problems findet.

Herzlichen Glückwunsch, Linus Feiten, zum Weizenbaum-Studienpreis 2022.

CC BY

Linus Feiten

Take the Power back!

1. Preis

Über die Auszeichnung meiner Dissertation mit dem Weizenbaum-Studienpreis 2022 habe ich mich sehr gefreut. Gerne gebe ich den Leser:innen der FIfF-Kommunikation daher in diesem Artikel eine kleine Übersicht von deren Inhalt. Auf Literaturangaben werde ich dabei verzichten; da sich alles in der Dissertation nachschlagen lässt, die unter CC-Lizenz online zur Verfügung steht.[1] Es sei außerdem auf die Aufzeichnung meines Vortrags bei der Preisverleihung hingewiesen, dessen Inhalt sich weitgehend mit dem dieses Artikels deckt.[2]

Der Aufbau meiner Dissertation besteht aus zwei Hauptteilen: *Privacy-preserving Surveillance* und *Physically Unclonable Functions*. Letzterer ist ein Bereich aus der Hardware-Security und soll in diesem Artikel nur kurz umrissen werden, obwohl ich darüber die meisten Veröffentlichungen während meiner Promotionszeit hatte. Denn die gesellschaftliche Relevanz meiner Arbeit, für die es schließlich die Auszeichnung mit dem Weizenbaum-Studienpreis gab, ergibt sich erst durch den Anwendungsfall der *Privacy-preserving Surveillance*, der hier genauer ausgeführt werden soll.

Um jedoch vorweg kurz auf die *Physically Unclonable Functions* (PUFs) einzugehen, sei das folgende gesagt: die Cyber-Security eines Systems basiert meistens darauf, dass berechtigte Personen oder Maschinen ein Geheimnis kennen, das nicht von unbefugten Angreifern in Erfahrung gebracht werden darf. Wenn Angreifer physischen Zugriff zu einem Gerät haben, in dem sich das Geheimnis befindet, ist es im Allgemeinen nur eine Frage des Aufwands, an das Geheimnis heran zu kommen. Mit Methoden der Hardware-Security wird versucht, diesen Aufwand so zu erhöhen, dass die geschätzten Kosten für einen erfolgreichen Angriff den geschätzten Gewinn für die Angreifer wahrscheinlich übersteigen. PUFs können dazu einen Beitrag leisten, indem ein Geheimnis nicht wie normalerweise in einem physischen Speicher auf dem Gerät abgelegt wird, sondern aus den physischen Eigenschaften des Geräts abgeleitet wird, sobald dieses Geheimnis für eine Berechnung gebraucht wird. Danach kann das Geheimnis sofort wieder aus dem flüchtigen

Speicher des Geräts gelöscht werden. Dies macht das Extrahieren des Geheimnisses für Angreifer deutlich komplizierter. Es besteht sogar die Möglichkeit, dass die physischen Eigenschaften, aus denen das Geheimnis abgeleitet wird, durch einen Angriff unwillkürlich verfälscht werden, sodass beim Angriff ein falsches Geheimnis ausgelesen wird. Außerdem wird das Nachbauen eines Geräts deutlich schwieriger, wenn sich das Gerät durch ein aus seinen physischen Eigenschaften abgeleitetes Geheimnis zu erkennen gibt. Denn die für ein Gerät einzigartigen physischen Eigenschaften entstehen durch unkontrollierbare Variationen im Produktionsprozess und lassen sich in der Regel nicht im Nachhinein manipulieren. Daher rührt das *Unclonable* bei PUFs, für die deshalb auch oft die Metapher eines Fingerabdrucks von Computerchips verwendet wird.

Für meine Arbeit habe ich an PUFs basierend auf Ring-Oszillatoren (ROs) geforscht. Die einzigartigen physikalischen Eigenschaften eines Geräts sind dabei die Widerstände von Leiterbahnen eines Mikrochips, die ein elektrisches Signal je nach Widerstand schneller oder langsamer transportieren. Durch Vergleiche mehrerer ROs untereinander auf einem Gerät kann für das Gerät eine einzigartige Signatur berechnet werden, die gegenüber wechselnden Umwelteinflüssen (z. B. Betriebstemperatur und Versorgungsspannung) robust ist. Die Beiträge meiner Arbeit zu diesem Forschungsfeld waren: Implementations-Methoden für PUFs auf FPGAs, Qualitäts-Metriken, Kompensation von RO-Frequenz-Biases sowie ein besonders platzsparender Typ von RO-PUF basierend auf sogenannten *Programmable Delay Lines*.

Nun sind PUFs ein anwendungsneutrales Mittel, das überall da eingesetzt werden kann, wo unbefugter physischer Zugriff auf ein Geheimnis erschwert werden soll. Mir war es aber ein Anliegen, in meiner Forschung auch den Einsatz von Technik in gesellschaftlichem Kontext zu beleuchten, was mich zum Forschungsfeld der *Privacy-preserving Surveillance* führte. PUFs können dabei eine vertrauensbildende Rolle spielen, wie weiter unten ersichtlich wird.

Privacy-preserving Surveillance befasst sich damit, überall dort, wo Überwachung stattfindet, diese so zu gestalten, dass sie weniger in die Privatsphäre der überwachten Personen eingreift. Am Beispiel der Videoüberwachung lässt sich das gut veranschaulichen: die Videodaten könnten zum Beispiel durch einen Algorithmus so modifiziert werden, dass Bildbereiche ausgeschwärzt werden, anhand derer Personen eindeutig identifizierbar sind. Für Videoüberwachung, die lediglich dazu dient feststellen, wie sich Personen im Bild bewegen, würde dem Zweck der Überwachung dadurch kein Abbruch getan. Ist der Zweck der Überwachung darüber hinaus, dass Personen identifiziert werden sollen (z. B. wenn diese etwas Illegales verbrochen haben), müsste das Ausschwärzen der Bildbereiche reversibel gestaltet werden. Dies könnte durch kryptographische Verschlüsselung erfolgen, so dass eine Deanonymisierung der Videodaten nur unter Verwendung eines bestimmten kryptographischen Schlüssels möglich ist. Abbildung 1 stellt einen solchen Anonymisierungsprozess schematisch dar.

Die Trennung zwischen personenbezogenen Daten (im Folgenden abgekürzt durch PII *personally identifiable information*) und nicht personenbezogenen Daten (im Folgenden NPII) hat durch einen wie auch immer gearteten Automatismus zu erfolgen, bevor die Daten das Gerät verlassen, in dem sie erhoben werden. Im Fall von Videoüberwachung dafür einen vollständigen Objekterkennungsalgorithmus einzusetzen, wie es die Mock-ups in Abbildung 1 suggerieren, ist wegen limitierter Rechenleistung eher unpraktikabel. Aber für Videoüberwachung sind simplere Algorithmen möglich, um PII-Bildinhalte automatisch zu identifizieren, wie in meiner Arbeit genauer ausgeführt wird. Ebenfalls in meiner Arbeit wird auf die Problematik eingegangen, dass sich Personen auch anhand ihrer Silhouette identifizieren lassen, und es werden Lösungen dafür vorgeschlagen.

Die Deanonymisierung könnte dann wie in Abbildung 2 gestaltet sein. Um einzelne Personen wieder sichtbar zu machen, muss eine Deanonymisierungsanfrage bei einer sogenannten *Key Keeper Authority* (KKA) gestellt werden. Diese kann anhand der NPII (bei Videoüberwachung also der Uhrzeit oder dem Hintergrund der Bilder) beurteilen, ob die Anfrage gerechtfertigt ist, und ggf. die Schlüssel zur Deanonymisierung freigeben. Die KKA verfügt über einen Hauptschlüssel, der das Pendant zum Schlüssel in der Kamera ist. Von diesem Hauptschlüssel lässt sich für jeden anonymisierten Bildbereich ein Sub-Schlüssel ableiten. Jeder Sub-Schlüssel kann nur für einen bestimmten Bildbereich und Zeitpunkt verwendet werden und lässt keine Rückschlüsse auf den Hauptschlüssel zu. Die KKA kann also zielgenau entscheiden, welche der beantragten Bildbereiche deanonymisiert wer-

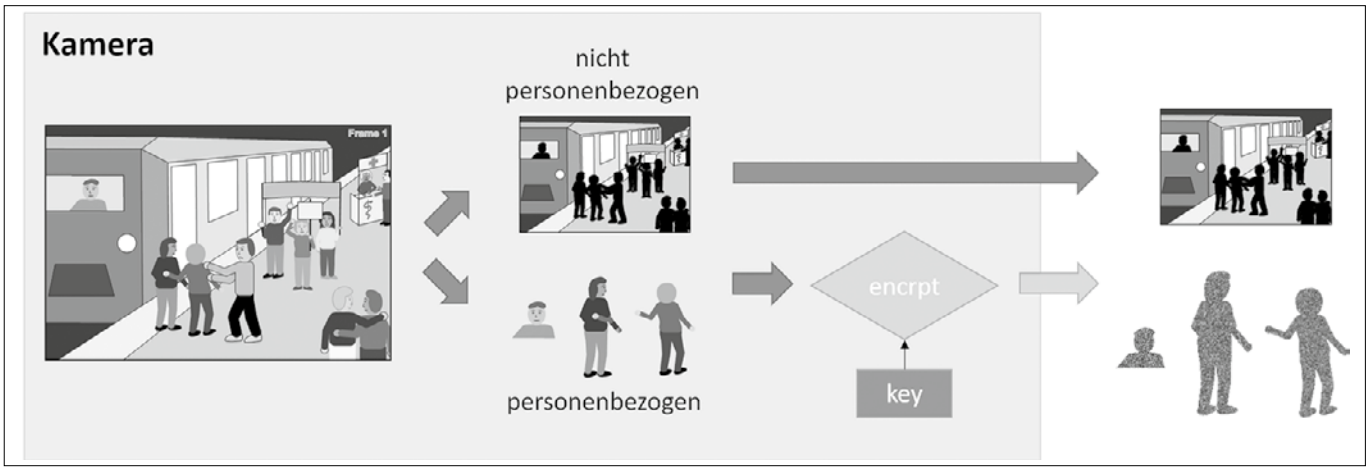


Abbildung 1: Reversible Verschlüsselung personenbezogener Überwachungsdaten

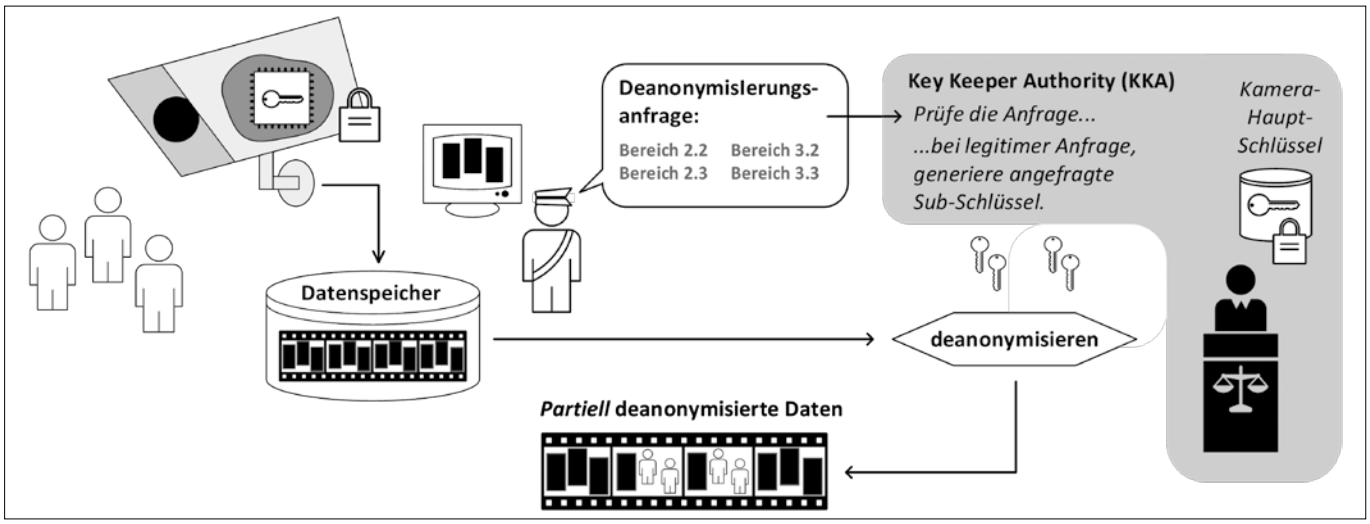


Abbildung 2: Durch Keeper-Authority autorisierte Deanonymisierung

den und welche nicht. Somit wäre die Privatsphäre von Personen in Überwachungsdaten auf eine ähnliche Weise geschützt, wie man es vom Schutz der Wohnung kennt, wo erst ein Durchsuchungsbefehl durch eine dritte Instanz (Richter:innen) nötig ist, damit die Polizei handeln darf.

Konzepte wie das eben beschriebene sind bereits in mehreren wissenschaftlichen Veröffentlichungen beschrieben und experimentell umgesetzt worden. Eine Übersicht sämtlicher *Related Work* befindet sich in meiner Dissertation. Die Beiträge durch meine Arbeit bestehen im Wesentlichen in der Ausgestaltung folgender Aspekte:

Betrugssichere Deanonymisierungsanfragen

Bei einer Deanonymisierungsanfrage muss die KKA anhand der NPII beurteilen, ob es sich um eine berechtigte Anfrage handelt und ob die angefragten Sub-Schlüssel freigegeben werden. Damit es aber nicht möglich ist, Sub-Schlüssel zu beantragen und dabei die NPII eines ganz anderen Vorfalls zu präsentieren, fließt ein Hash-Wert der zugehörigen NPII in die Erstellung der Sub-Schlüssel ein. Werden also falsche NPII mit der Deanonymisierungsanfrage präsentiert, kann die KKA daraus nur unbrauchbare Schlüssel generieren. Ein Betrug beim Beantragen ist somit ausgeschlossen.

Break-Glass

Falls Gefahr im Verzug ist, muss es möglich sein, auch ohne den relativ zeitaufwändigen Deanonymisierungsprozess Personen deanonymisieren zu können. Hierfür wurde in meiner Arbeit ein *Break-Glass*-Verfahren vorgestellt, durch das eine Kamera ihren Hauptschlüssel unmittelbar heraus gibt. Die Kamera gibt sich daraufhin aber unwiderruflich als korrumpiert zu erkennen, was bei Integritäts-Checks (siehe unten) auffallen wird. Mit dem herausgegebenen Schlüssel lassen sich nur die Aufzeichnungen eines vordefinierten vergangenen Zeitraums deanonymisieren. Ältere Aufzeichnungen bleiben also trotz Break-Glass geschützt und können weiterhin nur nach Anfrage bei der KKA deanonymisiert werden. Das Key-Rotation-Verfahren, welches dies ermöglicht, ermöglicht außerdem, dass die KKA ältere Schlüssel in ihrer Datenbank löschen kann und dadurch eine Deanonymisierung älterer Aufzeichnungen für immer verhindert wird. Die überwachten Personen brauchten dann nicht mehr darauf zu vertrauen, dass die überwachenden Personen selbst alte Aufzeichnungen löschen, insofern die KKA von diesen unabhängig und vertrauenswürdig ist.

Zertifizierte Inbetriebnahme durch Auditoren und Integritäts-Checks im Feld

Privacy-preserving Surveillance kann ihr Ziel nur erfüllen, wenn die von der Überwachung betroffenen Personen ein berechtigtes Vertrauen in das zugrundeliegende System haben können; sowohl in die Technologie als auch in die Personen und Institutionen, welche das System aufbauen und in Stand halten. In meiner Arbeit wird dafür ein Prozess vorgeschlagen, wie ein Gerät (z. B. Kamera) vor der Inbetriebnahme durch Auditoren geprüft und zertifiziert werden kann. Anschließend wäre es (aus Sicht der Hardware-Security) sehr schwierig, das Gerät noch einmal zu modifizieren, ohne dabei die eingebetteten Zertifikate der Auditoren zu verlieren. Das Vorhandensein der Zertifikate in einem Gerät ist somit ein Indiz dafür, dass sich das Gerät mit sehr hoher Wahrscheinlichkeit noch in dem Zustand befindet, den die Auditoren zur Inbetriebnahme vorgefunden haben. Die Zertifikate lassen sich im Betrieb der Kamera jederzeit von jedem durch einen *Proof of knowledge* überprüfen, wobei das Vorhandensein der Zertifikate nachgewiesen wird, ohne diese selbst preiszugeben. So schwer es also ist, die Zertifikate aus dem Gerät zu extrahieren, so schwer ist es, ein manipuliertes (d. h. nicht privatsphäreschützendes) Gerät zu bauen, das sich mit dem gleichen Zertifikat ausweisen würde. Die Hürden, die Angreifern durch Methoden der Hardware-Security in den Weg gestellt werden, müssen so hoch gewählt werden, dass der geschätzte Aufwand deutlich höher ist als der geschätzte Nutzen eines nur vorgeblich privatsphäreschützenden Gerätes. Anhaltspunkte für die Höhe dieser Hürden können Standards wie die IEC 62443-4-2 geben, in der für verschiedene Anwendungsbereiche bestimmte *Security Levels* beschrieben sind.

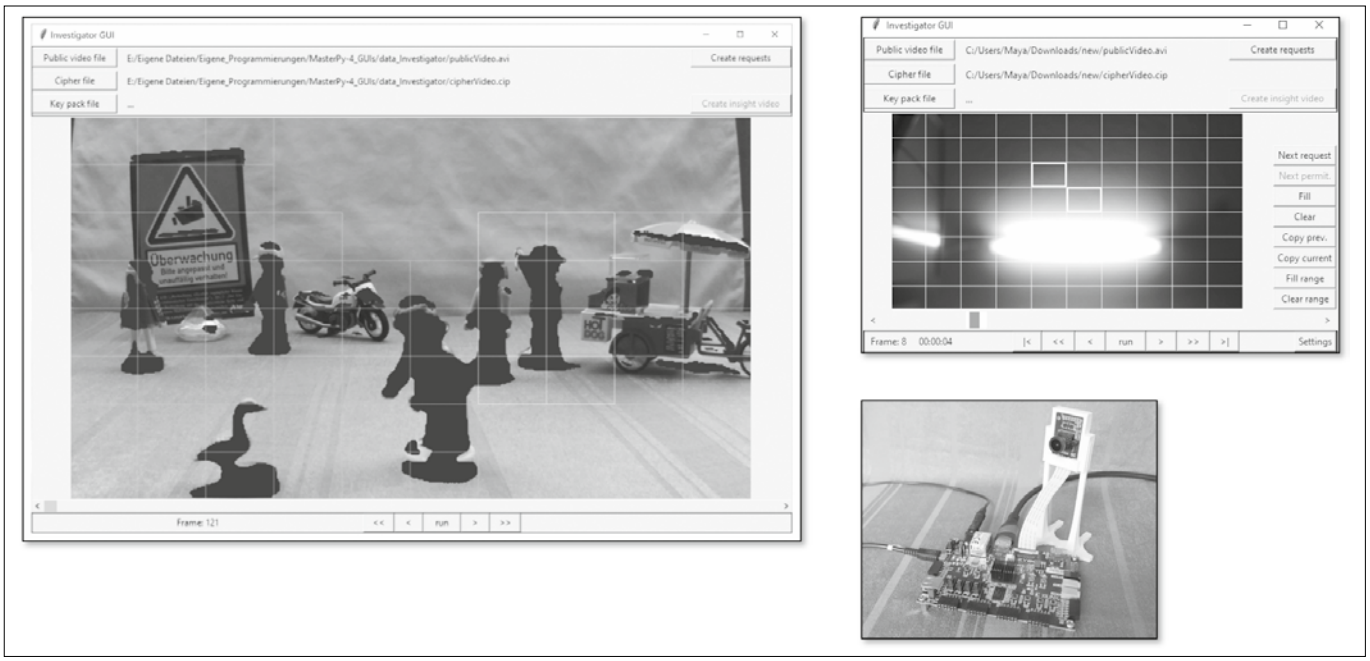


Abbildung 3: Masterarbeiten von Jan Reisacher und Maya Schöchlin

Aber der Erfolg von Privacy-preserving Surveillance hängt nicht nur vom Vertrauen der Betroffenen in die Technik ab. Mindestens genauso wichtig ist das Vertrauen in die eben genannten Auditoren sowie in die KKA. Wie diese zu besetzen und demokratisch zu legitimieren wären, wird in meiner Arbeit angedeutet. In jedem Fall macht ist es sinnvoll, sich durchaus überschaubare Szenarien vorzustellen, in denen Privacy-preserving Surveillance sinnvoll zum Einsatz kommen könnte. Man stelle sich z. B. eine Hausgemeinschaft vor, in der immer wieder im Hausflur randaliert wird. Man möchte den Tätern mit Videoüberwachung auf die Spur kommen, ohne dabei jedoch zu tracken, wer wann mit wem das Haus verlässt oder betritt. Die Auditoren könnten eine Gruppe von technikaffinen Personen sein, so dass jeder im Haus mindestens einer davon vertraut. Die KKA könnte eine Gruppe von Hausbewohnern (oder sogar alle) sein. Durch sogenannte *threshold cryptography* wäre es möglich zu definieren, dass mindestens eine bestimmte Anzahl von KKA-Mitgliedern einer Deanonymisierung zustimmen muss, damit diese stattfinden kann.

An der Uni Freiburg haben zwei Studierende im Rahmen ihrer Masterarbeiten einen Prototyp von Kamera und Deanonymisierungs-Software erstellt, von denen Abbildung 3 einen Eindruck vermittelt. Zu Akzeptanzstudien in der Praxis ist es bisher nicht gekommen.

Ein Dilemma der Privacy-preserving Surveillance scheint mir zu sein, dass sie wahrscheinlich gesetzlich verpflichtend wäre, wenn sie bereits in einer Form existieren würde, die im Vergleich zu konventioneller Überwachung „wirtschaftlich zumutbar" wäre. Denn ein Grund, warum konventionelle Überwachung und die dadurch entstehenden Eingriffe in die Privatsphäre überhaupt legal sind, ist nach meinem Verständnis, dass es kein „wirtschaftlich zumutbares" minderes Mittel gibt. Einen Menschen als Wachpersonal zu bezahlen statt eine Kamera aufzuhängen, wäre z. B. ein weniger in die Privatsphäre eingreifendes minderes Mittel, was aber um ein vielfaches teurer wäre und somit als nicht „wirtschaftlich zumutbar" angesehen werden kann. (Die Gesetzestexte, aus denen sich dies herleiten lässt, sind im Anhang meiner Arbeit beschrieben.) Solange konventionelle Überwachung legal ist, wird es wohl keine ernsthafte Nachfrage nach einer aufwändigeren und somit teureren Privacy-preserving Surveillance geben. Und solange es keine Nachfrage gibt, wird wohl kein Hersteller das Risiko eingehen, Privacy-preserving Surveillance zur Marktreife zu bringen. Aber erst diese würde es ermöglichen zu beurteilen, ob wirtschaftliche Zumutbarkeit gegeben und konventionelle Überwachung somit nicht mehr legal ist. Vielleicht gelingt es eines Tages durch ehrenamtliche oder Crowdfunding-Projekte, eine alle Kriterien erfüllende Privacy-preserving Surveillance in die Welt zu setzen. Ich würde mich freuen, wenn meine Arbeit einen kleinen Teil dazu beigetragen hätte.

Linus Feiten

Linus Feiten, geb. 1981, studierte Informatik mit Nebenfach Psychologie in Freiburg. Nach Abschluss seines Diploms begann er 2010 die Tätigkeit als Doktorand am Lehrstuhl für Rechnerarchitektur von Prof. Dr. Bernd Becker, wo er 2021 seine Doktorarbeit abschloss. Heute arbeitet er als Penetration Tester bei der SICK AG in Waldkirch.

Enden möchte ich mit einigen mir wichtigen Hinweisen. Als Techniker haben wir die Tendenz, uns „solutionistisch“ technische Lösungen für Probleme zu überlegen, die wir in der Welt sehen. Beim Austüfteln dieser Lösungen können wir durchaus Freude erleben. Aber wie diese Lösungen dann tatsächlich in der Welt wirken, ist für uns oft nur schwer zu antizipieren. In Hinblick auf Überwachungstechnologie muss ich sagen, dass ich statt einer Welt mit perfekter Privacy-preserving Surveillance lieber eine Welt hätte, in der flächendeckende, anlasslose Überwachung gar nicht nötig ist. Die Ressourcen, die wir in Überwachungstechnik stecken, wären vielleicht besser investiert, wenn sie in die Förderung von sozialen Projekten fließen würden. Dies ist auch eine der für mich bedeutendsten Erkenntnisse durch Joseph Weizenbaum: wir meinen, dass Computer uns einen Fortschritt bringen. Aber in wie vielen Bereichen haben es Computer lediglich ermöglicht, alte Strukturen beizubehalten? Ohne Computer und die damit möglich gewordene Skalierbarkeit hätten vielleicht wirklich neue, fortschrittliche Ideen entstehen müssen. Dies immer im Hinterkopf zu haben, scheint mir sehr wichtig.

Anmerkungen

1 *Linus Feiten, Take the power back! – Secrecy, accountability and trust in the Digital Age, 2021, https://doi.org/10.6094/UNIFR/225691*

2 *https://media.ccc.de/v/fiffkon22-9-verleihung-weizenbaum-studienpreise#t=3885 (starte bei 01:04:45)*

Weizenbaum-Studienpreis – Laudatio für den dritten Preis

Jan Hölzer: Am Vorabend der Digitalisierung

Bachelorarbeit an der Technischen Universität Braunschweig

Eine wesentliche ethische Frage bei der Nutzung jeder Form von Technik ist die Frage nach der Verantwortung. Diese Frage stellt sich besonders dringlich bei der Nutzung von Informationstechnik, durch die eine neue Stufe von Komplexität bei technischen Systemen ins Spiel kommt. Heute ist es vor allem die künstliche Intelligenz und die dadurch ermöglichten autonomen Systeme und das maschinelle Lernen, deren Komplexität die Frage nach der Verantwortung in besonderem Maß aufwirft. Doch bei auch „normal“ programmierten IT-Systemen stellt sich die Frage nach der Verantwortung und danach, wie Technikwissenschaftler:innen dieser Verantwortung gerecht werden. David Parnas, Preisträger des FIfF, lehnte es in den 1980er-Jahren ab, an dem Militärprojekt *Strategic Defense Initiative* (SDI) mitzuwirken – nicht aus einer pazifistischen Haltung heraus, sondern aus beruflicher Verantwortung. Er war überzeugt, dass Systeme dieser großen Komplexität (und mit diesen gravierenden Folgen bei Fehlfunktionen) nicht sicher entwickelt und betrieben werden können.

Hans Jonas schrieb in seinem Prinzip Verantwortung: „Handle so, dass die Wirkungen deiner Handlung verträglich sind mit der Permanenz echten menschlichen Lebens auf Erden.“ Dies ist der ethische Maßstab, an dem sich Technikwissenschaftler:innen orientieren müssen.

Doch auch bei weniger gravierenden Wirkungen stellt sich die Frage nach der Zuschreibung und Wahrnehmung von Verantwortung. In der technikphilosophischen Arbeit von Jan Hölzer – *Am Vorabend der Digitalisierung* –, die wir heute auszeichnen, werden Texte dreier herausragender Persönlichkeiten der Informatik daraufhin untersucht, inwieweit sich darin Selbstzuschreibungen von Verantwortung finden lassen. Unter *Vorabend* wird dabei grob der Zeitraum von 1970 bis 1995 verstanden; untersucht werden Veröffentlichungen von Joseph Weizenbaum, Norbert Wiener und Ray Kurzweil.

Dabei wird der Gegenstand – die Selbstzuschreibung von Verantwortung durch Technikwissenschaftler:innen – dadurch untersucht, dass Texte der drei Wissenschaftler Joseph Weizenbaum, Norbert Wiener und Ray Kurzweil dazu zusammengestellt, eingeordnet und gegenübergestellt werden. Dabei wird nach den Kategorien Informationsphilosophie, philosophische Anthropologie, Sozialphilosophie und Bildungsphilosophie differenziert. Die Selbstzuschreibung ist dabei sehr ungleich verteilt:

- Informationsphilosophie: Hier spricht dem Autor zufolge nur Weizenbaum explizit von außergewöhnlicher Verantwortung beim Umgang mit dem Informationsbegriff. Bei Kurzweil und Wiener ist keine Selbstzuschreibung von Verantwortung zu finden.

- Philosophische Anthropologie: Auch hier bleibt die Zuschreibung von Verantwortung bei Wiener und Kurzweil unerwähnt oder mindestens unklar. Wieder ist es Weizenbaum, der sich als Technikwissenschaftler in der Verantwortung sieht, Veränderungen für das Selbstverständnis des Menschen kritisch zu hinterfragen.

- Sozialphilosophie: Kurzweil erkennt die Gefahren in der Nutzung intelligenter Maschinen. Wiener betont, dass die Verantwortung stets beim Menschen verbleibt, thematisiert aber nicht explizit die Verantwortung von Technikwissenschaftler:innen. Auch hier ist es nur Weizenbaum, der die Verwantwortung auf die Programmierung und damit auf die Technikwissenschaftler:innen zurückführt.

- Bildungsphilosophie: Auch aus bildungsphilosophischer Perspektive ist Weizenbaum der Einzige unter den drei Technikwissenschaftlern, bei dem eine klare Selbstzuschreibung von Verantwortung zu finden ist.

Aus Sicht des Autors wurden verschiedene Positionen innerhalb der Technikwissenschaften deutlich: Kurzweil streut nur vereinzelt kritische Betrachtungen ein und spricht dabei nicht von seiner Verantwortung, Wiener thematisiert Verantwortung und schreibt sie sich teilweise selbst auch zu, Weizenbaum setzt sich ausführlich mit der Verantwortung auseinander.

Es ist also vor allem jener, der immer wieder auf die Verantwortung von Technikwissenschaftler:innen hinweist. Dies wird im Abschlusskapitel unterstrichen, mit dem Hinweis, dass sich Weizenbaum einmal als „Feigenblatt des MIT" bezeichnet hat.

Die Arbeit bietet einen sehr guten, zusammenfassenden Überblick über die verantwortungsethischen Positionen der behandelten Wissenschaftler:innen. Formal ist sie korrekt verfasst und sinnvoll strukturiert. Wenn auch das Ergebnis nicht überrascht, wird es stringent und strukturiert herausgearbeitet. Dabei wird eine sinnvolle Aufteilung der Aussagen zugrunde gelegt. Der verwendete Verantwortungsbegriff, der sich auf „Vorhaltung" und „Nötigung zur Verteidigung" beschränkt, ist jedoch ein wenig zu vereinfachend. Hier wäre ein umfassenderer Verantwortungsbegriff und auch in der Folge eine umfassendere Bewertung wünschenswert gewesen, auch mit Bezug auf weitere Positionen der Verantwortungsethik aus dem betrachteten Zeitraum, beispielsweise der schon genannte Hans Jonas, Hans Lenk oder Günter Ropohl. Der Zeitraum ist gut abgegrenzt; zusätzlich wäre es schön gewesen, die weitere Entwicklung verantwortungsethischer Positionen bis zur Gegenwart zumindest kurz anzureißen.

Diese Punkte tun der hervorragenden Arbeit von Jan Hölzer aber keinen Abbruch. Insgesamt stellt die Arbeit eine lesenswerte Zusammenstellung, Einordnung, Gegenüberstellung und Bewertung der Standpunkte dreier zentraler Persönlichkeiten der Technikwissenschaft dar. Die Jury des Weizenbaum-Studienpreises hat sich deswegen für die Auszeichnung der Arbeit entschieden.

Herzlichen Glückwunsch, Jan Hölzer, zum Weizenbaum-Studienpreis 2022.

CC BY

Jan Hölzer

Am Vorabend der Digitalisierung

Die Selbstzuschreibung von Verantwortung bei den Technikwissenschaftlern Weizenbaum, Wiener und Kurzweil aus philosophischer Sicht

3. Preis

Dieser Beitrag stellt eine Kurzfassung meiner Bachelorarbeit dar und soll einen Einblick in ihre Inhalte ermöglichen. Die Vollversion mit detaillierteren Quellenangaben wird auf der Website des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (https://www.fiff.de/studienpreis) zu finden sein.

Auf der Suche nach den Verantwortlichen

Der Verantwortungsbegriff hat laut Walther Zimmerli in den letzten Jahrzehnten eine „ebenso beeindruckende wie besorgniserregende Karriere erlebt"[1]. Der technologische Fortschritt erweiterte die Tragweite menschlicher Handlungen beträchtlich. Die Verantwortung erfährt somit eine gleichwertige Erweiterung. Unter „Verantwortung" soll in dieser Ausarbeitung „die Möglichkeit, einem Menschen die Folgen seines Handelns vorzuhalten sowie die daraus für diesen Menschen erwachsende Nötigung, sich gegenüber dieser Vorhaltung zu verteidigen"[2], verstanden werden. Eine ausführliche Behandlung des komplexen Verantwortungsbegriffs ist im Rahmen dieser Untersuchung nicht vorgesehen. Dennoch muss betont werden, dass sich die Verantwortung nicht auf die unmittelbaren Folgen einer Handlung beschränkt, sondern aufgrund der „Unüberschaubarkeitsvermutung gegenüber den Folgen der Anwendung von Technologien" (Zimmerli 2014: 22) auch Folgen, die vom Handlungssubjekt möglicherweise nicht vorhergesehen worden sind, umfasst. In komplexen Systemen, in denen eine Vielzahl von Menschen und Maschinen an den Handlungen beteiligt sind, wird die Vorhersage der Handlungsfolgen sowie die damit verbundene Zuschreibung von Verantwortung immer schwieriger. Für Zimmerli ändert dies nichts daran, dass das einzelne Individuum „Letztadressat moralischer Verantwortung" (Zimmerli 2014: 22) bleibt.

Die Bachelorarbeit kehrt zu den Anfängen dieser Entwicklungen zurück, um zu untersuchen, ob sich bereits am Vorabend der Digitalisierung eine Selbstzuschreibung von Verantwortung bei den Technikwissenschaftlern Weizenbaum, Wiener und Kurzweil finden lässt.

Um eine halbwegs unstrittige Periodisierung der Digitalisierung vorzunehmen, fehlt noch der zeitliche Abstand. Für den Historiker Ulrich Herbert markiert das Jahr 1995 „den Beginn des digitalen und das Ende des analogen Zeitalters"[3]. Die Ausarbeitung orientiert sich an der Auslegung Herberts und will mit der historischen Zäsur „am Vorabend der Digitalisierung" die Zeit bis zum Jahr 1995 beschreiben. Die drei ausgewählten Technikwissenschaftler verbindet ihre bedeutende Rolle für die Entwicklung der heutigen Technologien. Ihre Positionen hinsichtlich ihrer Verantwortung weichen allerdings stark voneinander ab.

Joseph Weizenbaum arbeitete für über 20 Jahre am MIT und wurde neben seinen Errungenschaften im Bereich der Computertechnologie durch seine kritischen Worte bezüglich des Umgangs mit Computern bekannt. Er ist Mitbegründer des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. und „wirkte lange Zeit im Vorstand mit"[4].

Norbert Wiener gilt als der Begründer der Kybernetik. Der Begriff bezeichnet „die formale, in erster Linie mathematische Wissenschaft von der Struktur komplexer Systeme“[5].

Raymond Kurzweil wurde vom SPIEGEL als „schillernde Figur der frühen Computer- und Internetszene“[6] bezeichnet und ist seit 2012 als Director of Engineering bei Google tätig.

Der Hauptteil der Ausarbeitung gliedert sich in vier Unterkapitel, die die Entwicklungen aus verschiedenen philosophischen Perspektiven beleuchten. Jedes Kapitel gibt zunächst einen Überblick über die wichtigsten Aspekte der jeweiligen Sicht, um im Anschluss zu untersuchen, inwieweit sich die Autoren Verantwortung hinsichtlich der behandelten Auswirkungen zuschreiben. Die Inhalte stammen vorwiegend aus den Texten der drei Technikwissenschaftler und werden nur vereinzelt um Aussagen aus der Sekundärliteratur ergänzt. Im Rahmen dieser Kurzfassung wird auf die jeweilige Analyse der Selbstzuschreibung von Verantwortung verzichtet. Sie wird zusammenfassend den Schlussteil des Textes bilden.

Die ausgewählten Betrachtungsweisen können nicht das ganze Potential einer philosophischen Untersuchung ausschöpfen. Die Ausarbeitung beschränkt sich auf die vier folgenden Perspektiven, da sie in den Texten der drei Technikwissenschaftler am stärksten hervortreten. Für den vorliegenden Beitrag werden nur beispielhaft einzelne Aspekte dieser Blickwinkel angerissen.

„Informationsphilosophie“

Bei der ersten Perspektive handelt es sich nicht um eine etablierte Fachrichtung innerhalb der Philosophie, weshalb ihr Titel umgeben von Anführungsstrichen aufgeführt wird. Ihre Wichtigkeit für die folgende Untersuchung beeinträchtigt dies nicht. Für Luciano Floridi ist der Informationsbegriff von zentraler Bedeutung für die Entwicklung der Informations- und Kommunikationstechnologien in den letzten Jahrzehnten. Der Fortschritt auf diesem Gebiet „geht mit einer riesigen intellektuellen Verantwortung einher“[7], weshalb er versucht, die Informationsphilosophie als bedeutende Fachrichtung der zeitgenössischen Philosophie stark zu machen. Den Ausführungen der drei Technikwissenschaftler liegen stark voneinander abweichende Auffassungen des Informationsbegriffs zugrunde. Weizenbaum weist darauf hin, dass „es viele unterschiedliche Meinungen darüber gibt, was Information ist und wo und wie sie erzeugt wird“[8].

Für Wiener steht die funktionale Bedeutung einer Information im Vordergrund. Laut Weizenbaum sollte in diesen Fällen besser von einer Nachricht gesprochen werden. Der Computer arbeitet nur mit Signalen und erst die Interpretation dieser Signale durch den Menschen macht sie zu Informationen. Eine Information kann nicht unabhängig in einem Computer konserviert werden. Allerdings fehlt es laut Kurzweil nur an „*suitable structures for knowledge representation*“[9]. Die zentrale Rolle des Menschen wird nicht erwähnt. Das Wissen muss aus Kurzweils Sicht nur gesammelt und in den Computer eingespeist werden. Was der Computer noch nicht kann, kann er nur *noch* nicht. Allein die Frage zu stellen, ob es denn etwas gibt, das einem Computer nicht mitgeteilt werden kann, ist laut Weizenbaum „ein Zeichen für die Geisteskrankheit unserer Zeit“[10].

Philosophische Anthropologie

Die technologischen Entwicklungen stellten immer „eine Provokation für das menschliche Selbstverständnis dar, da mit neuen Technologien die Bedingungen des Menschseins und die Position der Menschen verändert wurden“[11]. Eine Aufgabe der philosophischen Anthropologie ist es, „[d]ieses Selbstbild kritisch zu prüfen“[12]. Anthropologische Betrachtungen gehen meist mit einer Beschreibung von *dem* Menschen einher, der ausschließlich als Abstraktion existiert. Diese Problematik sollte während des gesamten Kapitels im Hinterkopf behalten werden.

Weizenbaum warnte davor, zu glauben, mit einer einzigen Perspektive den ganzen Menschen erfassen zu können. Wiener hingegen sieht den Menschen als eine „special sort of machine“[13]. Die „intellectual capacities“ (Wiener 1954: 57) des Menschen basieren auf seiner maschinellen Struktur, sodass lediglich ein exakter Nachbau der Physiologie nötig ist, um sie nachzubilden. Für Kurzweil ist das menschliche Gehirn nicht mehr als „three pounds of ‚ordinary‘ matter“ (Kurzweil 1990: 13). Bezüglich der menschlichen DNA stellt er fest, dass es sich bei der Evolution nicht um einen „very efficient programmer“ (Kurzweil 1990: 151) handelt.

Der Mensch als „das schwächste Glied“ (Weizenbaum 2001: 111) findet keinen Platz mehr im Netzwerk komplexer Maschinen. Weizenbaum stellt deshalb eine bedeutende Frage: „Warum brauchen wir überhaupt Menschen?“ (Weizenbaum 2001: 44) Wiener bezeichnet die Frage nach der Relation zwischen Mensch und Maschine als „one of the great future problems“[14].

Sozialphilosophie

Als Entwickler der neuen Technologien wurde den drei Technikwissenschaftlern ein großer Einfluss zuteil, der sie zu Autoritäten bei Fragen machte, die über den technischen Bereich weit hinausgingen. Neben dieser Macht der Technikwissenschaftler:innen verschoben sich auch die Machtverhältnisse zwischen Mensch und Maschine. Die sozialphilosophische Betrachtung der Texte soll diese Veränderungen herausarbeiten.

Kurzweil sieht unsere Zukunft mit der Technik in den Händen der Nutzer:innen. „It will all depend on who controls the technology“ (Kurzweil 1990: 447). Diese Annahme einer Neutralität der Technik war in den Technikwissenschaften weit verbreitet. Problematische Projekte, die beispielsweise der Militärtechnik dienen oder vorrangig die Bedürfnisse einer im Entwicklerteam dominanten Gruppe berücksichtigen, belehren uns eines Besseren. Für Judy Wajcman ist die Überwindung der “gender-blindness”[15] ein wichtiger Schritt. Allerdings können Technikwissenschaftler:innen keine Entscheidungen treffen, ohne dabei selbst von außen beeinflusst zu werden. Am MIT kommt ein Großteil der Forschungsmittel „direkt vom amerikanischen Militär“[16].

Darüber hinaus scheinen wir alle nur noch den technischen Innovationen hinterherzuhinken. Wiener bezeichnet die Menschen als „slaves of [their] technical improvement“ (Wiener 1954: 46), die sich an die neuen Gegebenheiten anpassen müssen, um weiter existieren zu können. Für Kurzweil steht fest:

„It cannot be stopped" (Kurzweil 1990: 9). Weizenbaum kritisiert die Annahme einer Zwangsläufigkeit des technischen Fortschritts und bezeichnet sie als „wirksames Beruhigungsmittel für das Bewußtsein" (Weizenbaum 2020: 317).

Technikwissenschaftler:innen treffen Entscheidungen darüber, welche Maschine sie entwerfen und wie sie sie entwerfen. Hierbei muss berücksichtigt werden, dass die durch den Computer entstandenen neuen Handlungsmuster oft die Möglichkeit ausschließen, wieder „nach den älteren Mustern zu handeln" (Weizenbaum 2020: 62). Jede Maschine akzeptiert nur ein bestimmtes Befehlsformat, sodass die Menschen ihr Verhalten an die Maschine anpassen müssen, um sie zu nutzen. Wir *bedienen* sie. Den Menschen, die diese Systeme einführten, war nicht bewusst, dass sie „‚Sklaven' des Computers" (Weizenbaum 2020: 314) geworden sind.

Bildungsphilosophie

Mit einer größeren Verantwortung der Technikwissenschaftler:innen gehen neue Anforderungen an diese Berufsgruppe einher. Zudem wirkt sich der technologische Fortschritt auf das gesamte Bildungssystem aus. Deshalb wird im Kapitel zur Bildungsphilosophie näher untersucht, für welche Veränderungen sich die drei Technikwissenschaftler aussprechen und wie zukünftige Technikwissenschaftler:innen aus ihrer Sicht an ihre bedeutungsvolle Aufgabe herangeführt werden sollten.

Weizenbaum warnt vor einer unüberlegten Einführung der neuen Technologien, vor allem wenn dies damit verbunden ist, bestehende Lerninhalte zu verkürzen oder sogar aus dem Lehrplan zu streichen. Allerdings spricht er sich gegen die Position aus, dass der Computer „das Denken vergiftet" (Weizenbaum 2001: 88). Es ist sinnvoll, dass alle etwas über den Aufbau eines Computers lernen und mit entsprechender Unterstützung selbst einen Computer herstellen. Auf diese Weise könnte er entmystifiziert werden.

Für Weizenbaum ist die Ausbildung der Technikwissenschaftler:innen ein zentrales Thema, um sie auf ihre verantwortungsvolle Rolle vorzubereiten. Aus seiner Sicht reicht es nicht aus, die Lehrinhalte anzupassen. „An Vorbildern fehlt es heute" (Weizenbaum 1984: 27). Die Lehrenden müssen mit gutem Beispiel vorangehen. Sie sollen „über die Beschränkungen [ihrer] Werkzeuge ebenso sprechen wie über deren Möglichkeiten" (Weizenbaum 2020: 362). Technikwissenschaftler:innen müssen die konkreten historischen und sozialen Gegebenheiten erkennen. Die Kenntnis dieser Gegebenheiten wird sich dann in ihren Handlungen niederschlagen. „Wer weiß, wer und was er ist, der braucht nicht zu fragen, was er tun sollte" (Weizenbaum 2020: 356).

Die Selbstzuschreibung von Verantwortung

Die aus den vier Perspektiven beleuchteten Entwicklungen verdeutlichen, wie wichtig es ist, dass Technikwissenschaftler:innen verantwortungsvoll mit ihrer einflussreichen Rolle umgehen. Dennoch wird diese außergewöhnliche Verantwortung ausschließlich von Weizenbaum angemessen thematisiert. Obwohl Wiener und Kurzweil maßgeblich zu der von Weizenbaum kritisierten Entwicklung beitragen, findet sich in ihren Texten keine Selbstzuschreibung von Verantwortung hinsichtlich der beschriebenen Auswirkungen. Wiener kritisiert zumindest die Tendenz, immer mehr Verantwortung an die Maschinen abgeben zu wollen. Er hält es für realistisch, dass sogar die Verantwortung für einen Atomkrieg auf eine Maschine übertragen werden könnte. Allerdings können die Menschen keine Verantwortung an die Maschinen weitergeben, ohne weiterhin die „full responsibility" (Wiener 1954: 184) für diese Entscheidung zu tragen. Weizenbaum würdigt die Überlegungen Wieners und weist darauf hin, dass er bereits „sehr früh einen Zusammenhang zwischen der Technik und dem Bösen in der Welt gesehen" (Weizenbaum 2001: 57) hat.

Die Bachelorarbeit konnte einen Teil dazu beitragen, die Verantwortung der Technikwissenschaftler:innen sichtbar zu machen. Die Untersuchung der Aussagen von Weizenbaum, Wiener und Kurzweil veranschaulichte verschiedene Positionen innerhalb der Technikwissenschaften und die Unterschiede hinsichtlich der Selbstzuschreibung von Verantwortung traten deutlich hervor. Während Kurzweil nur selten eine kritische Betrachtung einstreut und dabei nie von seiner Verantwortung spricht, verweist Wiener an vielen Stellen auf die möglichen Auswirkungen der Entwicklungen. Wiener thematisiert den Umgang mit der Verantwortung und schreibt sie sich vereinzelt explizit selbst zu. Die schärfste Kritik, die sich auch gegen ihn selbst richtet, findet sich bei Weizenbaum, der sich ausführlich mit der Verantwortung der Technikwissenschaftler:innen auseinandersetzte und somit zur zentralen Figur dieser Ausarbeitung wurde.

Wenn Weizenbaum sagt, dass nur ein Wunder die Menschen noch retten könnte, will er nicht, dass wir nur abwarten und hoffen. Die Ohnmacht des Einzelnen ist nur eine Illusion. Jeder Mensch muss sich so verhalten, als würde „die Zukunft der ganzen Menschheit" (Weizenbaum 1984: 53) von ihm abhängen. Allerdings ist die Vermeidung von Verantwortung laut Wei-

Jan Hölzer

Jan Hölzer, studiert nach Abschluss seines Bachelorstudiums der Philosophie den Masterstudiengang „Kultur der technisch-wissenschaftlichen Welt" an der TU Braunschweig. Vor seinem Studium hat er eine Ausbildung zum Fachinformatiker abgeschlossen und war mehrere Jahre im Kontext IT berufstätig.

zenbaum ein „allgemeingesellschaftliches Phänomen“ (Weizenbaum 2001: 33) und die Technik unterstützt zusätzlich dabei, die Verantwortung so zu verteilen, dass sich scheinbar auch niemand mehr verantwortlich fühlen muss. Die eigenen Handlungen mit dem Kommentar zu entschuldigen, dass es anderenfalls ein anderer Mensch getan hätte, ist für ihn mit einer „moralischen Bankrotterklärung“ (Weizenbaum 2020: 330) zu vergleichen. Wer sich seiner Verantwortung entzieht, ist dazu verurteilt, „lediglich eine Figur in einem Drama zu sein, das anonyme Mächte geschrieben haben“ (Weizenbaum 2020: 348).

Anmerkungen

1 *Zimmerli, Walther (2014): Verantwortung kennen oder Verantwortung übernehmen? Theoretische Technikethik und angewandte Ingenieurethik. In: Lutz Hieber und Hans-Ullrich Kammeyer (Hg.): Verantwortung von Ingenieurinnen und Ingenieuren, Wiesbaden: Springer VS, S. 15, im Folgenden mit Autor, Erscheinungsjahr und Seitenzahl im Text.*

2 *Bayertz, Kurt (2010): Verantwortung. In: Hans Jörg Sandkühler (Hg.): Enzyklopädie Philosophie, Bd. 3, Hamburg: Meiner, 2860u.*

3 *Herbert, Ulrich (2017): Geschichte Deutschlands im 20. Jahrhundert, 2. Auflage, München: C.H.Beck, S. 1239.*

4 *Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (o.D.): Weizenbaum-Studienpreis des FIfF – 2021, https://www.fiff.de/studienpreis, zuletzt aufgerufen am 30.01.2023, 14:00 Uhr.*

5 *Burkard, Franz-Peter (2008): Kybernetik. In: Peter Prechtl und Franz-Peter Burkard (Hg.): Metzler Lexikon Philosophie. Begriffe und Definitionen, 3. erweiterte und aktualisierte Auflage, Stuttgart: J.B. Metzler, S. 326.*

6 *Knobbe, Martin (2012): Ray Kurzweil: Technik-Visionär fängt bei Google an, hochgeladen am 17.12.2012, https://www.spiegel.de/netzwelt/web/ray-kurzweil-technik-visionaer-faengt-bei-google-an-a-873282.html, zuletzt aufgerufen am 30.01.2023, 14:00 Uhr.*

7 *Floridi, Luciano (2015): Die 4. Revolution. Wie die Infosphäre unser Leben verändert, Berlin: Suhrkamp, S. 9.*

8 *Weizenbaum, Joseph (2001): Computermacht und Gesellschaft. Freie Reden, herausgegeben von Gunna Wendt und Franz Klug, Frankfurt am Main: Suhrkamp, S. 7, im Folgenden mit Autor, Erscheinungsjahr und Seitenzahl im Text.*

9 *Kurzweil, Raymond (1990): The Age of Intelligent Machines, Cambridge (Massachusetts): MIT Press, S. 210, im Folgenden mit Autor, Erscheinungsjahr und Seitenzahl im Text.*

10 *Weizenbaum, Joseph (2020): Die Macht der Computer und die Ohnmacht der Vernunft, 15. Auflage, Frankfurt am Main: Suhrkamp, S. 299, im Folgenden mit Autor, Erscheinungsjahr und Seitenzahl im Text.*

11 *Heßler, Martina und Kevin Liggieri (2020): Einleitung: Technikanthropologie im digitalen Zeitalter. In: Martina Heßler und Kevin Liggieri (Hg.): Technikanthropologie. Handbuch für Wissenschaft und Studium, Baden-Baden: Nomos, S. 12.*

12 *Prechtl, Peter (2008): Anthropologie, philosophische. In: Peter Prechtl und Franz-Peter Burkard (Hg.): Metzler Lexikon Philosophie. Begriffe und Definitionen, 3. erweiterte und aktualisierte Auflage, Stuttgart: J.B. Metzler, S. 32.*

13 *Wiener, Norbert (1954): The Human Use of Human Beings. Cybernetics and Society, Boston: Da Capo Press, S. 79, im Folgenden mit Autor, Erscheinungsjahr und Seitenzahl im Text.*

14 *Wiener, Norbert (1964): God & Golem, Inc.. A Comment on Certain Points where Cybernetics Impinges on Religion, Cambridge (Massachusetts): MIT Press, S. 71, im Folgenden mit Autor, Erscheinungsjahr und Seitenzahl im Text.*

15 *Wajcman, Judy (2004): TechnoFeminism, Cambridge (UK): Polity Press, S. 107.*

16 *Weizenbaum, Joseph (1984): Kurs auf den Eisberg. Oder nur das Wunder wird uns retten, sagt der Computerexperte, Zürich: Pendo, S. 22, im Folgenden mit Autor, Erscheinungsjahr und Seitenzahl im Text.*

Weizenbaum-Studienpreis – Laudatio für den dritten Preis

Christina Hecht: Datafizierte Situationen und Gesellschaftsbilder

Masterarbeit an der Humboldt-Universität zu Berlin

Die Erhebung und Verarbeitung von Daten spielt eine immer größere Rolle bei der Nutzung digitaler Technik. Sowohl die „unsichtbar“ erhobenen Daten, die wir als Preis dafür bezahlen, eine Vielfalt von Services nutzen zu können, als auch die Daten, die wir bereitwillig den Dienstleistern geben, um sie – irgendwo in der Cloud – verarbeiten zu lassen. Dazu kommen Daten, die beispielsweise ein Arbeitgeber oder staatliche Behörden erheben und zur Überwachung nutzen.

Aus dieser Datennutzung ergeben sich Risiken. Von unmittelbaren Konsequenzen aus der Nutzung der Daten – man denke an die Nutzung von Gesundheitsdaten durch Versicherungsunternehmen zur Risikoeinstufung oder Nutzung der im Arbeitskontext anfallenden Daten zur Leistungsbewertung oder gar für dizipliarische Maßnahmen durch den Arbeitgeber. Verstärkt werden diese Risiken durch die Nutzung in Systemen maschinellen Lernens, deren Komplexität zu weiterer Intransparenz der Verarbeitung führt.

Christina Hecht untersucht in ihrer soziologischen Arbeit *Datafizierte Situationen und Gesellschaftsbilder*, die wir heute auszeichnen, zwei Arten datafizierter Situationen daraufhin, wie sie solche Gesellschaftbilder beeinflussen: im Bereich der Erwerbsarbeit die Nutzung von Daten zur Steuerung der Arbeitsprozesse (bei Amazon bzw. Lieferando) und im privaten Bereich die Nutzung von Daten zur Optimierung der Gesundheit anhand von Fitness-Trackern. Dazu wurden jeweils fünf Personen in qualitativen Interviews befragt und die Ergebnisse ausgewertet. Die Autorin stellt und beantwortet dabei folgende Forschungsfragen:

- Wie werden datafizierte Situationen erfahren und eingeordnet?

- Sind diese Erfahrungen und Einordnungen verbunden mit Vorstellungen von der datafizierten gesellschaftlichen Wirklichkeit? Wenn ja, inwiefern?

Der freiwilligen Nutzung der Daten in Fitness-Trackern stehen die Proband:innen positiv gegenüber; sie empfinden die Effekte, die sich z. B. durch Nudging und Gamification auf Basis der Erfassung von Kennzahlen (wie Fitness-Punkten) ergeben, als motiverend, ihr „Tagespensum" zu schaffen – empfinden dabei aber keinen Zwang. Auffällig ist auch, dass Datenschutzbedenken beim überwiegenden Anteil der Befragten keine wesentliche Rolle spielen.

Anders bei der Datafizierung im Arbeitskontext. Nudging und Gamification sind hier nicht mehr freiwilllig sondern werden zu einem Zyklus aus Anweisung – Evaluation – Disziplinierung. Hier werden klare Anweisungen erteilt und Ziele gesetzt, deren Erreichen auf Basis der gesammelten Daten evaluiert wird. Die Performance ist Grundlage der Leistungsbeurteilung und wird beispielsweise bei der Zuteilung von Liefergebieten berücksichtigt. Damit werden die Daten zur Disziplinierung der Mitarbeiter:innen genutzt, bis hin zur Kündigung, wenn die vorgegebenen Zahlen nicht erfüllt werden.

Zusammenfassend ergibt sich der Unterschied zwischen Freiwilligkeit der Datenabgabe beim Fitnesstracking und unfreiwilliger Datenabgabe im Arbeitskontext. Im ersten Fall werden die Daten als Nutzen stiftend empfunden, da sie sonst unbestimmbare Aktivitäten zum eigenen Nutzen quantifizierbar machen. Im Arbeitskontext ist dies nicht mit einer Ermächtigung verbunden sondern wird als Kontrolle empfunden.

Darüber hinaus kommt die Autorin zu dem Ergebnis, dass die bestehende Ordnung entweder als Schichtsystem oder als komplexes Gefüge verschiedenster Dimensionen mit unterschiedlichen Hierarchien wahrgenommen wird – im ersten Fall mit der zentralen Bedeutung finanzieller Ungleichheit. Die Politik komme ihrer Aufgabe, Rahmenbedingungen für das gesellschaftliche Leben zu setzen, im Hinblick auf Datafizierung nicht hinreichend nach. Datafizierung sei ein kommerzielles Projekt, von dem vor allem Unternehmen profitierten. Nach Ansicht einiger Befragter profitierten neben Unternehmen auch die Gesamtgesellschaft und Individuen von der fortschreitenden Datafizierung. Der andere Teil der Befragten kritisiert hingegen, dass durch diesen Prozess gesellschaftliche Konflikte verschärft werden.

Die Arbeit ist klar strukturiert, die Forschungsfragen sind klar benannt und überzeugend und klar beantwortet. Das Ergebnis ist weitgehend konform mit der intuitiven Erwartung, dass die freiwillige Datennutzung positiv gesehen wird, als Erweiterung der persönlichen Möglichkeiten (wobei die Möglichkeit der „ungewollten" Nutzung ebenfalls erwähnt wird); die vom Arbeitgeber erzwungene Datennutzung aber eher negativ als Kontrolle wahrgenommen wird. Es wird überzeugend herausgearbeitet; lediglich das Sample von jeweils nur fünf (insgesamt zehn) Personen erscheint etwas gering, es sind aber auch klar die methodischen Schwächen benannt, der Zugangsweg zu den Daten dokumentiert und die so entstandene Verzerrung thematisiert.

Insgesamt ergibt sich eine überzeugende Behandlung des Themas, die wir gerne mit einem Weizenbaum-Studienpreis auszeichnen.

Herzlichen Glückwunsch, Christina Hecht, zum Weizenbaum-Studienpreis 2022.

CC BY

Christina Hecht

Algorithmisches Management und Fitnesstracking

Datafizierte Situationen und Gesellschaftsbilder

3. Preis

Die Bedeutung von Daten und digitaler Technologie wird in aktuellen Beschreibungen der Gesellschaft in den schillerndsten Farben hervorgehoben. Es wird über die Ära der Datafizierung (Krüger 2021), die Datengesellschaft (Houben & Prietl 2018) oder den Digitalen Kapitalismus (Staab 2019) geschrieben. Auch wird untersucht, wie Prozesse der Datafizierung in gesellschaftlichen Teilbereichen wirksam werden (exemplarisch: Danaher 2016; Staab & Nachtwey 2017; Thiel 2017; Keiner 2020). Teilweise werden in quantitativen Untersuchungen individuelle Einstellungen zu den Veränderungen erfasst, die mit der Datafizierung einhergehen (Gagr in et al. 2021). Unklar ist jedoch bisher, wie Datafizierung als gesamtgesellschaftlicher Prozess wahrgenommen wird – gewissermaßen das subjektive Gegenstück zu den oben aufgeführten Zeitdiagnosen. Datafizierung meint an dieser Stelle die quantifizierende Erfassung, Auswertung und Speicherung von Aspekten des menschlichen Lebens mittels digitaler Technologie (Mau 2018: 40; Couldry & Mejias 2019). In der vorliegenden, explorativen Untersuchung werden zwei Fragen verfolgt. Erstens: Wie wird Datafizierung im Alltag erlebt und gedeutet? Und zweitens: Hängen diese Deutungen zusammen mit dem Bild von der datafizierten Gesellschaft – und wenn ja, inwiefern? Mit der zweiten Frage ist auf das Konzept vom Gesellschaftsbild verwiesen. Außerdem wird nach einem möglichen Zusammenhang von Gesellschaftsbild und Alltagserfahrung gefragt. Beide Aspekte werden im folgenden Abschnitt erläutert.

Theoretischer Rahmen

In Gesellschaftsbildern fügen sich „Vorstellungen über die gesellschaftliche Wirklichkeit" (Sandberger 1983: 112, Kursivierung i. O.) zu einem kohärenten Ganzen zusammen. Für Individuen sind Gesellschaftsbilder „Bezugssysteme, Orientierungshilfen, Interpretationsschlüssel" (Herkommer 1969: 209). Sie sind durch ein hohes Maß an Abstraktion gekennzeichnet, da sie grundlegende Vorstellungen darüber umfassen, wie ‚unsere'[1] Gesellschaft funktioniert und geordnet ist. Diese deskriptive Komponente ist untrennbar verbunden mit normativen Bewertungen: Wie sollte die Gesellschaft geordnet sein? Wie könnte oder sollte

die Ordnung in Zukunft aussehen? Welche Rolle spielt dabei die technische Entwicklung (Oetterli 1971: 160 f.)?[2]

Diese Antworten auf diese Fragen sind untrennbar verbunden mit dem sozialen Standort, von dem aus Gesellschaft erfahren wird. Mannheim (2015 [1985]: 230 ff.) argumentiert, dass dieser spezifische Erfahrungszusammenhang zu verschiedenen Arten der Weltauslegung führt. Die Position im sozialen Gefüge – dafür können verschiedenste Merkmale eine Rolle spielen, z. B. Bildungsgrad, Geschlecht, Staatsbürgerschaft – hängt zusammen mit der „Art, wie einer eine Sache sieht, was er an ihr erfaßt und wie er sich einen Sachverhalt im Denken konstruiert" (ebd.: 234). Dennoch gehen Gesellschaftsbilder über den Bereich der unmittelbaren Erfahrung hinaus. Popitz und Kollegen argumentieren in *Das Gesellschaftsbild des Arbeiters*, dass deren Alltagserfahrungen stets auf ein Mehr verweisen, „das innerhalb des eigenen Erlebnisbereiches nicht greifbar ist" (Popitz et al. 2018 [1957]: 8 f.). Giddens (1984) führt später aus, dass Subjekte durch „knowledgeability" (ebd.: 25, 281 f.) gekennzeichnet sind: Sie wissen um die Ordnungen des sozialen Lebens und setzen sich deutend mit sozialen Handlungen sowie Handlungskontexten auseinander. Dies umfasst auch soziale Kategorien, die diese Kontexte strukturieren. Subjekte nehmen am Arbeitsplatz, in der Familie, im Staat (ebd.: 83-86) verschiedene soziale Positionen ein, die in einem bestimmten Verhältnis zueinander stehen. So macht es einen Unterschied für meine Handlungsoptionen, ob ich in einer Situation als Arbeitnehmerin oder -geberin auftrete. Ebendiese Kategorien verweisen auf abstraktere gesellschaftliche Verhältnisse. Daher wissen Subjekte „a great deal more than they ever directly live through" (ebd.: 91).

Methodischer Zugang

Gesellschaftsbilder werden bisher vor allem in Verbindung mit Erfahrungen in der Erwerbssphäre untersucht. Diese ist weiterhin zentral für den sozialen Standort von Subjekten in der Gesellschaft. Die vorliegende Untersuchung fokussiert sich jedoch auf die Frage, wie Datafizierung als gesamtgesellschaftlicher Prozess gedeutet wird. Damit wird sowohl die Erwerbs- als auch die Privatsphäre – und die dort verbreiteten digitalen Technologien – in den Blick genommen. Um beide Sphären abzubilden wurden qualitative Leitfadeninterviews mit zwei Gruppen geführt, die später inhaltsanalytisch ausgewertet wurden (Kuckartz 2018: Kapitel 5).

Die erste Gruppe stellen Beschäftigte dar, die in der Erwerbssphäre algorithmisches Management erleben. Das bedeutet, dass im Rahmen ihrer Arbeit Algorithmen eingesetzt werden, um (1) Anweisungen für Beschäftige zu strukturieren, (2) um deren Arbeitsleistung zu evaluieren und aufbauend darauf (3) ihr Verhalten am Arbeitsplatz zu disziplinieren (Kellogg et al. 2020: 373 ff.). Die Befragten sind unter anderem als Rider bei Essenslieferdiensten tätig, andere arbeiten als Logistiker:in im Warenlager. Für alle sind Apps, Handscanner und digitale Endgeräte zentral im Arbeitsprozess, denn sie geben einerseits die Schritte vor, die zu erledigen sind, und vermessen andererseits das Arbeitshandeln der Befragten. Durch betriebliche Mitbestimmung können Arbeitnehmer:innen Einfluss darauf nehmen, wie algorithmisches Management am Arbeitsplatz umgesetzt wird. Auch ist klar, dass sie sich reflexiv und widerständig mit Kontrollsystemen des Managements auseinander setzen (Moore & Joyce 2020: 931). Sich derer gänzlich zu verweigern, ist allerdings schwierig bis unmöglich.

Im privaten Bereich wurden Fitnesstracker:innen befragt, die ihre körperliche Aktivität mit digitalen Geräten und Apps beobachten und beeinflussen wollen. Dabei kommen zwei zentrale Mechanismen zum Einsatz. Einerseits sollen Nudges „den Lebenswandel permanent […] korrigieren" (Mau 2018: 178). Mit einer Vibration am Handgelenk erinnert beispielsweise der Fitnesstracker von Apple daran, kurz aufzustehen und sich zu bewegen. Ein weiterer Mechanismus ist Gamification, beispielsweise in der Form monatlicher ‚Fitness-Challenges'. Hierbei werden durch die Anpassung der Ziele an das bisherige Aktivitätslevel Genauigkeit und Individualisierung signalisiert (Schaupp 2016: 78). Ähnlich zu den Beschäftigen setzen sich auch Fitnesstracker:innen kritisch mit den algorithmischen Anwendungen auseinander (Lyall & Robards 2018: 118 f.). Dennoch wirken die Apps und Sportuhren als Mediator in der Beziehung zum Selbst, ihr Einfluss offenbart sich im „guiding, formatting, or altering the course of a given tracked phenomenon according to their own classificatory and procedural logics" (Ruckenstein & Schüll 2017: 268).

Die zentrale Annahme der Fallauswahl ist, dass beide Gruppen durch die jeweils herausragende Rolle der algorithmischen Erfassung und Auswertung von Daten strukturanaloge Situationen erleben. Die Auswertung erlaubt daher einen fruchtbaren Vergleich zwischen den beiden Sphären, indem Gemeinsamkeiten und Unterschiede in den Gesellschaftsbildern der Befragten herausgearbeitet werden. Im Folgenden werden Schlaglichter auf die Ergebnisse der Untersuchung geworfen.

Ergebnisse

Datafizierte Situationen …

Die Erwerbstätigen verbinden die Erfassung von Daten über ihren Arbeitsprozess mit Kritik an Leistungsbeurteilung und Kontrolle. Einige äußern diese direkt, vor allem wenn sie besonders auf die Beschäftigung angewiesen sind: „die Sache ist ja die, dass man mit den Daten ja auch steuern kann. Und ich bin der Meinung, dass ich immer noch selber entscheiden soll und mich nicht von, durch die Daten, die erhoben werden, mich steuern lassen soll."[3] Besonders die Ausführungen von Beschäftigten in der Warenlager-Logistik zeigen, wie Daten für die Leistungsbeurteilung relevant werden. „Dort [im Handscanner, CH] wird halt alles gesammelt, wie viel du gepickt hast pro Stunde, wie viel, wie lange du gebraucht hast, wird intern auch noch ausgerechnet, auch noch mit ner Performance dann von allen Leuten. So und so, also hundert Prozent wär gut. Dadrunter hast du irgendwann ein Manager-Gespräch." Andere Befragte betrachten die kontinuierliche Datenaufzeichnung eher pragmatisch als notwendiges Merkmal der Arbeit mit dem sie „nicht so ein großes Problem" haben. Trotzdem formulieren sie auf einer anderen Ebene Kritik daran. Ungerechtigkeiten könnten nicht ausgeschlossen werden und durch Zahlen könne Leistungsdruck entstehen. Sie meinen, dass das System „teilweise unfair ist, natürlich kann ein 80-jähriger, naja, 80 ist jetzt übertrieben, aber du weißt, was ich meine, vielleicht nicht so wie

ein 20-jähriger arbeiten." Alle Befragten meinen, dass vor allem Arbeitgeber:innen von den technischen Systemen profitieren: „Die wollen natürlich auch Personalkosten gering halten." So beschreibt ein Befragter, dass die Anforderungen im Warenlager mit der Zeit stiegen: „Das steigert sich, die erwarten irgendwann mehr von dir, automatisch". Ein anderer formuliert besonders scharf, dass ihm alle Entscheidungen durch die Software vorgegeben würden, und er „wie ein Roboter" am Fließband sitze. Das Ziel dieser Praxis ist ihm zufolge, Beschäftigte möglichst schnell anlernen und ersetzen zu können, indem Prozesse vereinfacht und kleinteiliger werden. Wie die zur Leistungsbeurteilung so zentrale „Performance-Rate" berechnet wird, „das ist ne gute Frage. […] Wie das festgelegt wird, das wissen so ungefähr nicht mal die Manager selber."

Im Gegensatz dazu betonen die Fitnesstracker:innen, wie komfortabel es sei, dass Fitnessuhren und Apps automatisch und kontinuierlich die eigene Aktivität erfassen: „du musst letztendlich kaum darüber nachdenken, was alles über dich getrackt wird, sondern du – es passiert einfach." So können die Befragten in quantifizierter Form sichtbar zu machen, was sonst unbestimmbar bleibt – z. B. gelaufene Schritte oder verbrannte Kalorien. Diese Daten werden langfristig gespeichert, und die Befragten identifizieren Trends in ihrer körperlichen Aktivität. Sie sehen ihre „Leistung in Zahlen." Die visuelle Evaluation von Aktivitätsdaten aus verschiedenen Zeiträumen spiegelt für die Fitnesstracker:innen wider, wie sportlich aktiv sie waren oder auch nicht waren: „Ich merk auf jeden Fall, dass die App verstärkend wirkt auf so meine Stimmung, oder mein eigenes Körpergefühl. Ob ich jetzt Sport oder nicht Sport gemacht habe." Wenn beim Aktivitätsring auf der Apple Watch „echt nur so ein bisschen fehlt, dann bin ich schon so, ja das packst du heute noch." Die Tracker:innen bleiben so motiviert, ihre sportliche Leistung zu verbessern. Sie können ihrem „Optimierungswahnsinn" nachgehen und „Selbstoptimierung" betreiben. Andere formulieren weniger drastisch, dass sie sehen wollen, ob sie „irgendwie fitter geworden" sind. Generell wollen sie durch körperliche Aktivität auch (langfristig) ihr „Wohlbefinden optimieren" und Krankheiten entgegenwirken. Durch die Geräte müssen sie ihre Aktivitätsziele nicht selbst im Blick behalten. Notifications und algorithmisch kuratierte Trainingspläne erinnern daran, Sport zu machen. Diese stellen eine „unglaubliche Erleichterung" dar, weil „so wenig aktiv dafür gearbeitet werden muss, dass es passiert." Eine Befragte führt aus, es sei: „total hilfreich wenn man seinen Kopf nicht anstrengen muss. […] Ich kriegs einfach gesagt und dann mach ich das." Diese Abnahme von kognitivem Ballast erfahren die Fitnesstracker:innen als Mehrwert, weil sie förderlich für ihre selbstgesetzten Ziele sind.

Zusammenfassend wird so deutlich, dass Datafizierung von den beiden befragten Gruppen grundsätzlich unterschiedlich erfahren wird. Für Beschäftigte in der Erwerbssphäre bedeutet Datafizierung Fremdbestimmung – auch wenn die Kritik auf unterschiedlichen Ebenen formuliert wird. Sie bewerten den Einsatz digitaler Technik als ein potenziell ungerechtes Projekt, von dem Arbeitgeber:innen einseitig profitieren. Im Gegensatz dazu eröffnen sich für Fitnesstracker:innen durch Datafizierung ermächtigende Handlungsräume, innerhalb derer sie selbstbestimmt und entlang eigener Maßstäbe ihre Ziele verfolgen können. Doch inwiefern spiegeln sich diese Unterschiede in den Gesellschaftsbildern der Befragten wider?

… und Bilder von der datafizierten Gesellschaft

Bei der Frage, wer Macht in unserer Gesellschaft habe, antwortet ein Befragter Elon Musk und Mark Zuckerberg. Dies verweist auf eine zentrale Gemeinsamkeit der Befragten. Sie alle nehmen finanzstarke Technologieunternehmen als die richtungsweisenden ‚Player' der digitalen Transformation wahr. Ihre erste Assoziation zur Bedeutung digitaler Technik in unserer Gesellschaft ist deren kommerzielle Nutzung durch große Technologieunternehmen – YouTube, Google, Instagram. Diese könnten personalisierte Werbung schalten und verfolgten dabei das Ziel „Konsumverhalten zu kontrollieren" um ihre „Verkäufe hochzutreiben." Auch könne durch datenbasiertes „Personalmanagement" die Effektivität im Arbeitsprozess gesteigert und die Leistungsfähigkeit von Beschäftigten beurteilt werden. Vor diesem Hintergrund wird Datenschutz von den Befragten als zentrales Konfliktfeld herausgestellt, unabhängig davon, ob sie selbst vorsichtig oder freigiebig mit persönlichen Daten umgehen. Die Politik, so der Eindruck unter den Befragten, kommt nicht schnell genug hinterher: „das ganze Internet ist ja noch Neuland, wie Merkel gesagt hat" – und Unternehmen nutzen diese regulatorischen Lücken für sich aus. „Dadurch, dass bei den Daten noch so unbestimmt definiert ist, wem sie gehören […] dann sind es wieder Unternehmen, die sich daran, also, die sie eben nutzen und zu ihrem Vorteil nutzen."

Die Effekte dieser unternehmensgetriebenen digitalen Transformation bewerten die Befragten ambivalent bis kritisch – hier zeigt sich keine klare Unterscheidung zwischen den befragten Gruppen. Ein feiner Unterschied wird jedoch deutlich, wenn der zeitliche Horizont ausgeweitet und nach der gesellschaftlichen Zukunft gefragt wird. Fitnesstracker:innen stellen sich zwei Szenarien vor: Ein Teil vermutet, dass digitale Technik im Sinne verschiedenster Interessenlagen eingesetzt wird, die auch heute schon miteinander verhandelt werden müssen. Dabei werde es immer Vorteile und Nachteile, Chancen und Risiken geben, die bereichsspezifisch ausgeprägt sind (diese Einschätzung findet sich zum Teil auch bei befragten Beschäftigten). Ein zweiter Teil hat „Utopien im Kopf". Sie sehen die Möglichkeit, große Technikunternehmen zu besteuern, um so den Problemen, „die wir haben aus öffentlicher Hand entgegenzuwirken". Auch könne durch die Vergesellschaftung digitaler Infrastrukturen „die Entscheidung darüber, was überhaupt im Markt passiert […] demokratisch gestärkt" werden. Durch Datenauswertungen in allen gesellschaftlichen Bereichen könne ein globaler „Optimalzustand" erreicht werden, von dem alle Menschen profitieren würden. Durch künstliche Intelligenz in der Forschung könnten schneller Medikamente entwickelt werden. Nicht prekär beschäftigte Fahrradkuriere müssten Essen ausliefern, das könnten Drohnen übernehmen. Wenn die Politik proaktiv Rahmenbedingungen für die digitale Transformation entwickele, könne „Glückseligkeit" für die Menschen erreicht werden. „Wenn natürlich alle Rahmenbedingungen so gestimmt sind, dass man sich keine Sorgen mehr machen muss, haben Personen nicht mehr Ängste […], sondern können sich einfach auf die positiven Sachen im Leben konzentrieren." Diese Art von utopischen Ideen schwebt durchaus auch den befragten Beschäftigten vor. Der zentrale Unterschied ist jedoch, als wie wahrscheinlich sie die Verwirklichung dieser Ideen einschätzen. Neben diese utopischen Potenziale tritt ausschließlich bei befragten Beschäftigten ein dystopisches Szenario: Sie befürchten, dass die Politik da-

bei versage, Rahmenbedingungen zu gestalten. Daher sei wahrscheinlich, dass digitale Technik zukünftig allein zur Vermehrung von Profit eingesetzt wird. Dies hieße dann, dass „überall mehr Werbung reinkommt" und alles auf „Trends von consumern […] zugeschnitten wird". Am Ende ist „halt wieder vom Geld angetrieben." Eine Befragte sieht zukünftig „gläserne Mensch[en]" in einer „Gesellschaft, in der man so ja, ständig von Algorithmen geleitet so einfach lebt und bewertet wird."

Die Frage nach der Zukunft verweist also auf die Gegenwart – und auf die Rolle der Politik. Abschließend soll daher auf eine weitere zentrale Gemeinsamkeit der Befragten hingewiesen werden. Unabhängig von ihren Gedanken zu Zukunftsszenarien fordern sie alle mehr Initiative von der Politik, um die Nutzung digitaler Technologien zu regulieren. Sie sehen die Politik in der Pflicht, Rahmenbedingungen für die kommerziellen Akteure der digitalen Transformation festzulegen, wenn diese beim Einsatz digitaler Technik ‚vorpreschen' oder rechtliche Schlupflöcher nutzen. Folgen wir den Ausführungen der Befragten, erfüllt sie diese Rolle nur unzureichend. Sie alle sehen ein gesamtgesellschaftlich gewinnbringendes Potenzial, das mit dem Einsatz digitaler Technologie einhergeht oder einhergehen könnte. Wie zukünftig mit diesem Potenzial umgegangen wird, bleibt also ein Feld für Träume und Ideen – und Aufgabe der Politik.

Referenzen

Couldry N, Mejias UA (2019) Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. In: Television & New Media, 20: 336-349.

Danaher J (2016) The Threat of Algocracy: Reality, Resistance and Accommodation. In: Philosophy & Technology, 29: 245-268.

Gagrčin E, Schaetz N, Rakowski N, et al. (2021) Weizenbaum Institute for the Networked Society – The German Internet Institute; Goethe-Institut e.V. (2021): We and AI – Living in a Datafied World: Experiences and Attitudes of Young Europeans. Berlin.

Giddens A (1984) The Constitution of Society: Outline of the Theory of Structuration Oxford: Polity Press.

Herkommer S (1969) Gesellschaftsbild und politisches Bewußtsein. Gegen affirmative und defensive Sozialforschung. In: Das Argument. Zeitschrift für Philosophie und Sozialwissenschaften, 50: 208-222.

Houben D, Prietl B (2018) Datengesellschaft. Einsichten in die Datafizierung des Sozialen Bielefeld: Transcript.

Keiner AE (2020) Algorithmen im Asylprozess. Legitimität von Algorithmen in politischen Verwaltungsorganisationen am Beispiel der Dialekterkennungssoftware des BAMF. In: FIfF-Kommunikation, 1: 71-75.

Kellogg KC, Valentine MA. Christin A (2020) Algorithms at Work: The New Contested Terrain of Control. In: Academy of Management Annals, 14: 366-410.

Krüger K (2021) Die Ära der Datafizierung. Medieninnovation als Wandel der Medientypen Wiesbaden: Springer Gabler.

Kuckartz U (2018) Qualitative Inhaltsanalyse. Methoden, Praxis, Computerunterstützung (4. Auflage). Weinheim, Basel: Beltz Juventa.

Lyall B, Robards B (2018) Tool, toy and tutor: Subjective experiences of digital self-tracking. In: Journal of Sociology, 54: 108-124.

Mannheim K (2015 [1985]) Ideologie und Utopie (9. Auflage). Frankfurt a. M.: Vittorio Klostermann GmbH.

Mau S (2018) Das metrische Wir. Über die Quantifizierung des Sozialen (3. Auflage). Berlin: Suhrkamp.

Moore PV, Joyce S (2020) Black box or hidden abode? The expansion and exposure of platform work managerialism. In: Review of International Political Economy, 27: 926-948.

Oetterli J (1971) Betriebssoziologie und Gesellschaftsbild Berlin, New York: De Gruyter.

Popitz H, Bahrdt HP, Jüres EA., et al. (2018 [1957]) Das Gesellschaftsbild des Arbeiters. Soziologische Untersuchungen in der Hüttenindustrie Wiesbaden: Springer VS.

Ruckenstein M, Schüll ND (2017) The Datafication of Health. In: Annual Reviews of Anthropology, 46: 261-278.

Sandberger JU (1983) Gesellschaftsbild. In: Lippert, E. and Wakenhut, R. (Hrsg.) Handwörterbuch der Politischen Psychologie. Opladen: Westdeutscher Verlag, 112-124.

Schaupp S (2016) „Wir nennen es flexible Selbstkontrolle.": Self-Tracking als Selbsttechnologie des kybernetischen Kapitalismus. In: Duttweiler, S., Passoth, J.-H., Strübing, J., et al. (Hrsg.) Leben nach Zahlen. Self-Tracking als Optimierungsprojekt? Bielefeld: Transkript, 59-82.

Staab P (2019) Digitaler Kapitalismus. Markt und Herrschaft in der Ökonomie der Unknappheit. (1. Auflage). Berlin: Suhrkamp.

Staab P, Nachtwey O (2017) Das Produktionsmodell des digitalen Kapitalismus. In: Soziale Welt, Sonderband – „Soziologie des Digitalen".

Thiel T (2017) Digitalisierung als Kontext politischen Handelns. Republikanische Perspektiven auf die digitale Transformation der Gegenwart. In: Jacob, D. and Thiel, T. (Hrsg.) Politische Theorie und Digitalisierung. Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG, 189-216.

Anmerkungen

1 *In der vorliegenden Untersuchung wird das Gesellschaftsbild in Bezug auf die Bundesrepublik Deutschland thematisiert. So wurde es auch mit den Befragten besprochen.*

2 *Dieser Fokus auf technische Entwicklung geht auf die arbeitssoziologischen Wurzeln des Konzepts zurück.*

3 *Alle Zitate in diesem und dem kommenden Abschnitt stammen aus den geführten Interviews. Zur besseren Lesbarkeit wurde auf Zeilenverweise verzichtet.*

Christina Hecht

Christina Hecht, hat Sozialwissenschaften an der Humboldt-Universität zu Berlin studiert. Seit Mai 2022 arbeitet sie als wissenschaftliche Mitarbeiterin am Sonderforschungsbereich Re-Figuration von Räumen an der Technischen Universität Berlin. Im Projekt zur Plattformökonomie forscht sie zu Raumkonflikten um Airbnb in Berlin und Kapstadt. (Foto ©Jule Würfel)

Call for Contributions

Schwerpunkt „IT-Gestaltung für Gute Arbeit“ der FIfF-Kommunikation 3/2023

Redaktion: Dagmar Boedicker, Klaus Heß, Katharina Just

Es kommt wesentlich auf eine vorausschauende Schwerpunktsetzung von Förderung und Regulierung an, in welche Richtung sich informationstechnische Anwendungen in Zukunft weiterbewegen. Das hat der Wissenschaftliche Beirat der Bundesregierung Globale Umweltveränderungen (WBGU)[1] schon 2019 festgestellt, und es gilt auch für die Arbeitswelt. Wir wollen in diesem Schwerpunkt der Frage nachgehen, wie eine solche Regulierung, wie überhaupt die Gestaltung von IT und ihres organisatorischen Umfelds aussehen kann, welche Leitbilder und Anreize es dafür gibt und auf welche Realität in den Unternehmen sie trifft.

Wie wirkt sich der Siegeszug von Digitalisierung und maschinellem Lernen in den Unternehmen auf die Beschäftigten aus, wie schätzen sie die Folgen ein und wie beurteilen sie die eigene Betroffenheit? Welche Rolle spielt die Technik im Arbeitsprozess: Ist sie Hilfsmittel, Überwachungsinstrument, Steuerungstechnologie? Wahrt sie die Menschenwürde? Ermöglicht sie gleichberechtigte und inklusive Teilhabe und Gestaltung? Dient sie dem Gemeinwohl? Wo hakt es bei der Mitbestimmung und bei der Regelung des IT-Einsatzes, wo fallen die Entscheidungen darüber und in wessen Sinn? Lassen KI-Systeme sich so gestalten, dass sie Transparenz und Intervenierbarkeit ermöglichen? Und wenn ja, wie? Was bedeutet es, dass der überwiegende Teil der Software in anderen Ländern mit anderen Kulturen und Prioritäten entwickelt wird?

Wir freuen uns über Arbeiten, die verschiedene Sektoren betrachten und auf Risiken und Chancen für einen sozial und ökologisch nachhaltigen Einsatz abklopfen: Produktion, Pflege und der ganze Bereich der Sorge, Handwerk, Landwirtschaft, Kunst und Medien, Forschung, Logistik, öffentliche und private Verwaltung, …

Dabei sind Praxisberichte ebenso interessant wie politische Forderungen und deren Begründung, lokale Erfahrungen ebenso wie nationale oder supranationale Entwicklungen, informatische Perspektiven ebenso wie die anderer Disziplinen, Analysen ebenso wie Gestaltungsoptionen, Fragen ebenso wie Antworten.

Wir bitten um Einreichungen von Beiträgen mit ca. 20.000 Zeichen (inklusive Leerzeichen) bis zum 25. Juni 2023 per E-Mail an Dagmar Boedicker (db@fiff.de). Alle Beiträge zum Schwerpunkt werden Peer-reviewed, und die Autorïnnen erhalten bis zum 25. Juli 2023 Rückmeldungen zu ihren Beiträgen. Die finalen Fassungen der Beiträge sind bis zum 4. August 2023 einzureichen.

Wir freuen uns über die Nutzung der Open-Access-Lizenz Creative Commons Namensnennung (CC BY) für Ihren Text und die Abbildungen, für die Sie die Rechte haben sollten. Rückfragen gern an die Redakteurïnnen.

Nach der Veröffentlichung erhalten Sie natürlich zwei Belegexemplare.

Termine
Einreichung bis: 25. Juni 2023
Rückmeldung vom Review: 25. Juli 2023
Redaktionsschluss/Einreichung der finalen Fassung: 4. August 2023

Hinweise für Autorïnnen schicken wir gerne zu.

1 *WBGU-Hauptgutachten „Unsere gemeinsame digitale Zukunft“ https://www.wbgu.de/de/publikationen/publikation/unsere-gemeinsame-digitalezukunft*

FIfF-Kommunikation 2/2023

Mensch – Gesellschaft – Umwelt … und Informatik?

Aufruf zur Einreichung von Beiträgen

„Die Digitalisierung durchdringt in zunehmendem Maße alle Bereiche unserer Gesellschaft.“ Wie oft habt ihr diesen Satz – oder Variationen davon – schon gelesen? Aber er ist offensichtlich wahr – und wir setzen uns in der FIfF-Kommunikation seit fast 40 Jahren damit auseinander.

Die Auswirkungen der Informatik umfassen ein breites Spektrum. Aktuell ist die Künstliche Intelligenz ein – auch außerhalb der reinen Fachdiskussion – ein stark beachtetes Thema. Doch sie bildet nur einen Ausschnitt aus der Vielfalt der technischen Artefakte der Informatik und deren Konsequenzen.

Wir wollen diese Vielfalt in unserer nächsten Ausgabe sichtbar machen. Wir bitten um die Einreichung von Beiträgen zu den Auswirkungen der Informatik – und der Künstlichen Intelligenz – auf:

- Bildung;
- Gesundheit;
- Kriegführung, Rüstung, Militär;
- Umwelt und Nachhaltigkeit;
- Politik;
- Öffentliche Verwaltung und Demokratie;
- Menschenrechte;
- alle weiteren Lebensbereiche.

Wir bitten um Einreichungen von Beiträgen mit ca. 20.000 Zeichen (inklusive Leerzeichen) bis zum 4. Mai 2023 per E-Mail an redaktion@fiff.de. Wir freuen uns über die Nutzung der Open-Access-Lizenz Creative Commons Namensnennung (CC BY) für Ihren Text und die Abbildungen, für die Sie die Rechte haben sollten. Rückfragen gern an die Redakteur:innen.

Dagmar Boedicker

IT-Sicherheit für dummies

von Rainer W. Gerling und Sebastian R. Gerling

IT-Sicherheit ist ein steiniges, weites Feld … Und das für dummies? Es ist das erste Buch aus dieser Reihe für mich, ich finde es gut, obwohl ich nicht zum Kreis der Adressatïnnen gehöre. Die Autoren, beide mit viel Erfahrung auf diesem Gebiet, wenden sich an Studierende, Datenschutzbeauftragte und IT-Administratorïnnen. Denen muten sie zwar kein spezielles Fachwissen *zu, Bereitschaft zum Bohren von dicken Brettern sollten sie aber mitbringen.*

Wie sehr Profis fehlen, die etwas von IT-Sicherheit verstehen, teilen uns Medien aller Art jeden Tag mit, sie melden beinah täglich gravierende Sicherheitsvorfälle. Eine Fortbildung in Sachen Informationssicherheit lohnt sich also für Informatikerïnnen in welcher Branche auch immer, auch in kleinen und mittleren Unternehmen, deren Abhängigkeit von ihrer IT-Infrastruktur groß, aber nicht immer allen bewusst ist. Fachleute werden nicht nur in Unternehmen der kritischen Infrastruktur gebraucht (welche das sind, findet sich auf Seite 85f). Das Thema ist umfangreich und das Buch deckt es gut ab: den Zusammenhang zwischen Datenschutz, IT- und Informationssicherheit, rechtliche Anforderungen, technische und organisatorische Maßnahmen, technische Bausteine, Umsetzung. Vorn steht auf einem zweiseitigen Spickzettel, was gut vorbereitete ITler drauf haben sollten, bis hin zur Ausstattung des Notebooks für eine Dienstreise.

Worauf müssen Sie achten, wenn Sie in Ihrem Unternehmen für die IT-Sicherheit zuständig sind? Wie gehen Sie vor? Welche Normen, beispielsweise europäische Richtlinien/Verordnungen, nationale und internationale technische Standards usw. sind relevant für Ihre Arbeit? Welche Funktionen und Rollen sind festzulegen und welche technischen Werkzeuge brauchen die Beschäftigten des Unternehmens?

Die Einführung präzisiert den Begriff Informationssicherheit, beschreibt einige verbreitete Illusionen über den sicheren Umgang mit IT, formuliert Annahmen über die Interessen der Leserïnnen und erklärt den Aufbau des Buchs. Die paar Seiten zu Syntax und Konventionen sollten Sie lesen, weil beispielsweise die Unterschiede zwischen *können, sollen, müssen* nur für Juristïnnen selbstverständlich sein dürften. Wer in der IT arbeitet, wird nicht überrascht von dem Hinweis sein, dass Informationssicherheit nie erreicht und ein ständiger Verbesserungsprozess ist. Ab Seite 163 vertiefen die Autoren diesen Aspekt mit Deming-Kreis/PDCA. Vorher erklären sie die Grundlagen anhand verschiedener Schutzziele Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität, Verantwortlichkeit und Benutzbarkeit. Die Erläuterungen sind praxisnah, beispielsweise zum Risikomanagement: Wer klassifiziert wie, aus welcher Perspektive und wie oft? Oder die meldepflichtigen Vorfälle: Welche sind zu melden und wohin? Welche Sicherheitsstandards gibt es und wie weisen Sie nach, dass sie eingehalten werden? Etwas mehr Information hätte ich mir zu Notfallplänen gewünscht.

Rainer W. Gerling und
Sebastian R. Gerling
IT-Sicherheit für dummies
Weinheim 2022
Wiley VCH GmbH
384 Seiten
Preis € 24,00 (Softcover)
ISBN-13: 978-3-527-71852-8
Preis € 20,99 (epub)
ISBN 978-3-527-83357-3

Was die Autoren auf etwas mehr als 50 Seiten im Teil I vorgestellt und erklärt haben, vertiefen sie anschließend. Im Teil II sind die geltende Rechtslage und die Standards aufgeführt sowie welche Institutionen auf nationaler und internationaler Ebene dafür zuständig sind und wo es Regelungslücken gibt.

Ich gebe zu, dass ich nicht das gesamte Buch gelesen habe, beim Datenschutz hoffte ich das Notwendigste zu wissen. Teil IV erklärt verständlich und nicht komplizierter als nötig die Bausteine technischer IT-Sicherheit wie Verschlüsselungsarten, Vertrauens- und Zertifizierungsmodelle, Biometrie und Tokens. Interessant finde ich auch Teil V *Lösungen und Umsetzungen:* Hier werden die verschiedenen Bedrohungen beschrieben und welche Lösungen dafür bestehen, technische wie organisatorische. Die Autoren verdichten sie anschließend in Kapitel 28 *Zehn Maßnahmen für den technischen Basisschutz* und Kapitel 29 *Zehn Maßnahmen für den organisatorischen Überbau.*

Zusammenfassend: Die Struktur des Buchs ist so durchdacht, dass die Komplexität des Themas für mich gut handhabbar wurde. Ich musste nicht alles lesen, fand aber eine gute Orientierung – auch einen Index –, durch die ich vertiefen konnte, was mich besonders interessiert. Die Autoren sind Praktiker, sie wissen offensichtlich, was wirklich wichtig ist, schreiben verständlich und gehen sorgsam mit der Zeit ihrer Leserïnnen um.

CC BY

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung

Im FIfF 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 FIfF 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 FIfF-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 FIfF regelmäßig an weiteren Veranstaltungen, Publikationen, vermittelt bei Presse- oder Vortragsanfragen ExpertInnen, führt Studien durch und gibt Stellungnahmen ab etc. Das FIfF kooperiert mit zahlreichen Initiativen und Organisationen im In- und Ausland.

FIfF-Mailinglisten

FIfF-Mailingliste
An- und Abmeldungen an:
http://lists.fiff.de/mailman/listinfo/fiff-L
Beiträge an: *fiff-L@lists.fiff.de*

FIfF-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*

FIfF online

Das ganze FIfF
www.fiff.de
Twitter FIfF e.V. – *@FIfF_de*

Cyberpeace
cyberpeace.fiff.de
Twitter Cyberpeace – *@FIfF_AK_RUIN*

Faire Computer
blog.faire-computer.de
Twitter Faire Computer – *@FaireComputer*

Mitglieder-Wiki
https://wiki.fiff.de

FIfF-Beirat

Ute Bernhardt (Berlin); **Peter Bittner** (Bad Homburg); **Dagmar Boedicker** (München); Dr. **Phillip W. Brunst** (Köln); Prof. Dr. **Christina Claß** (Jena); 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); **Ulrich Klotz** (Frankfurt am Main); Prof. Dr. **Klaus Köhler** (Mannheim); Prof. Dr. **Jochen Koubek** (Bayreuth); 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)

FIfF-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
Benjamin Kees (Mitgliedschaft ruhend) – Berlin
Prof. Dr. **Hans-Jörg Kreowski** – Bremen
Kai Nothdurft – München
Prof. Dr. **Britta Schinzel** – Freiburg im Breisgau
Ingrid Schlagheck – Bremen
Anne Schnerrer – Berlin
Dr. **Friedrich Strauß** – München
Prof. Dr. **Werner Winzerling** – Fulda

FIfF-Geschäftsstelle

Ingrid Schlagheck (Geschäftsführung) – 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	1 300 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	Daniel Guagnin, Gilbert Assaf
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	Lichtinstallation von Stephan und Benks, Foto von Alexander Heim
Druck	Meiners Druck, Bremen Heftinhalt auf 100 % Altpapier gedruckt.

KLIMAneutral produziert

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 Abonnent:innen, Adressänderungen dem FIfF-Büro möglichst umgehend mitzuteilen.

Aktuelle Ankündigungen

(mehr Termine unter *www.fiff.de*)

Konferenz Bits&Bäume 2023
16. und 17. Juni in Münster, Akademie Franz Hitze Haus

FIfF-Kommunikation
2/2023 „Mensch – Gesellschaft – Umwelt … und Informatik?"
Stefan Hügel
Redaktionsschluss: 4. Mai 2023

3/2023 „IT-Gestaltung für Gute Arbeit"
Katharina Just, Klaus Heß, Dagmar Boedicker
Redaktionsschluss: 4. August 2023

Zuletzt erschienen:
1/2022 Selbstbestimmung in digitalen Räumen
2/2022 Künstliche Intelligenz
3/2022 Digitalisierung in Staat, Politik und Verwaltung
4/2022 100 Jahre Joseph Weizenbaum

W&F – Wissenschaft & Frieden
2/22 Kriegerische Verhältnisse
3/22 Krieg gegen die Ukraine
4/22 Gewalt/Ökonomie
1/23 Jenseits der Eskalation

vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik
#236 Anleihekäufe der EZB
#237/238 Diskriminierung
#239/240 Krieg und Frieden
#241 Demokratie und Rechtsstaat verteidigen
#242 Kriminalpolitik

DANA – Datenschutz-Nachrichten
1/22 Ampelpolitik
2/22 Social Media
3/22 Datenschutz und andere Grundrechte
4/22 Beschäftigtendatenschutz
1/23 Europäische Entwicklungen

Das FIfF-Büro

Geschäftsstelle FIfF e. V.
Ingrid Schlagheck (Geschäftsführung)
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 FIfF

Hans-Jörg Kreowski

Die Berliner FIfF-Regionalgruppe hat nicht nur die FIfF-Konferenz 2022 mit einem spannenden Programm und in einer großartigen Atmosphäre ausgerichtet, sondern drei Wochen vorher schon in vielfältiger Weise und mit riesigem Engagement dazu beigetragen, dass die Bits & Bäume-Konferenz ein großer Erfolg geworden ist. Als speziellen persönlichen Dank habe ich deshalb zwei Gedichte konzipiert, die im weitesten Sinne der Konkreten Poesie zugerechnet werden können. Dabei kommt es vor allem auf die sprachliche und visuelle Wirkung an, nicht so sehr auf den Sinn, was aber Hintersinn auf gar keinen Fall ausschließt. Das Gedicht „make install PEACE" ist kooperativ gedacht, wobei die rechte Spalte von einem Chor gesprochen werden soll. Das Gedicht „Bits & Bäume" ist ein Lautgedicht, in dem insbesondere mit „schtzngrmm" ein bekanntes Werk von Ernst Jandl zitiert wird.

make install PEACE

Krieg	make install PEACE
Hunger Ausbeutung Armut Krankheit	make install PEACE
Klimawandel Naturzerstörung Artensterben	make install PEACE
Flucht Vertreibung Migration	make install PEACE
Unrecht Unterdrückung Diktatur	make install PEACE
Kampf um Weltherrschaft Kapitalismus	make install PEACE
Menschheit am Abgrund zur Selbstvernichtung	make install PEACE
Krieg	make install PEACE

Bits & Bäume

Bits & Bäume
Blitz & Donner
Fritz & Franz
Tricks & Treats

Bits & Träume
Witz lass nach
Schwitzkasten
Schmidts Katze

Bits & Schäume
Hitzschlag
Grützwurst
Sitzfleisch

Bit & Räume
Schlitz im Kleid
Kids sind laut
„schtzngrmm"

Bits & Bäume