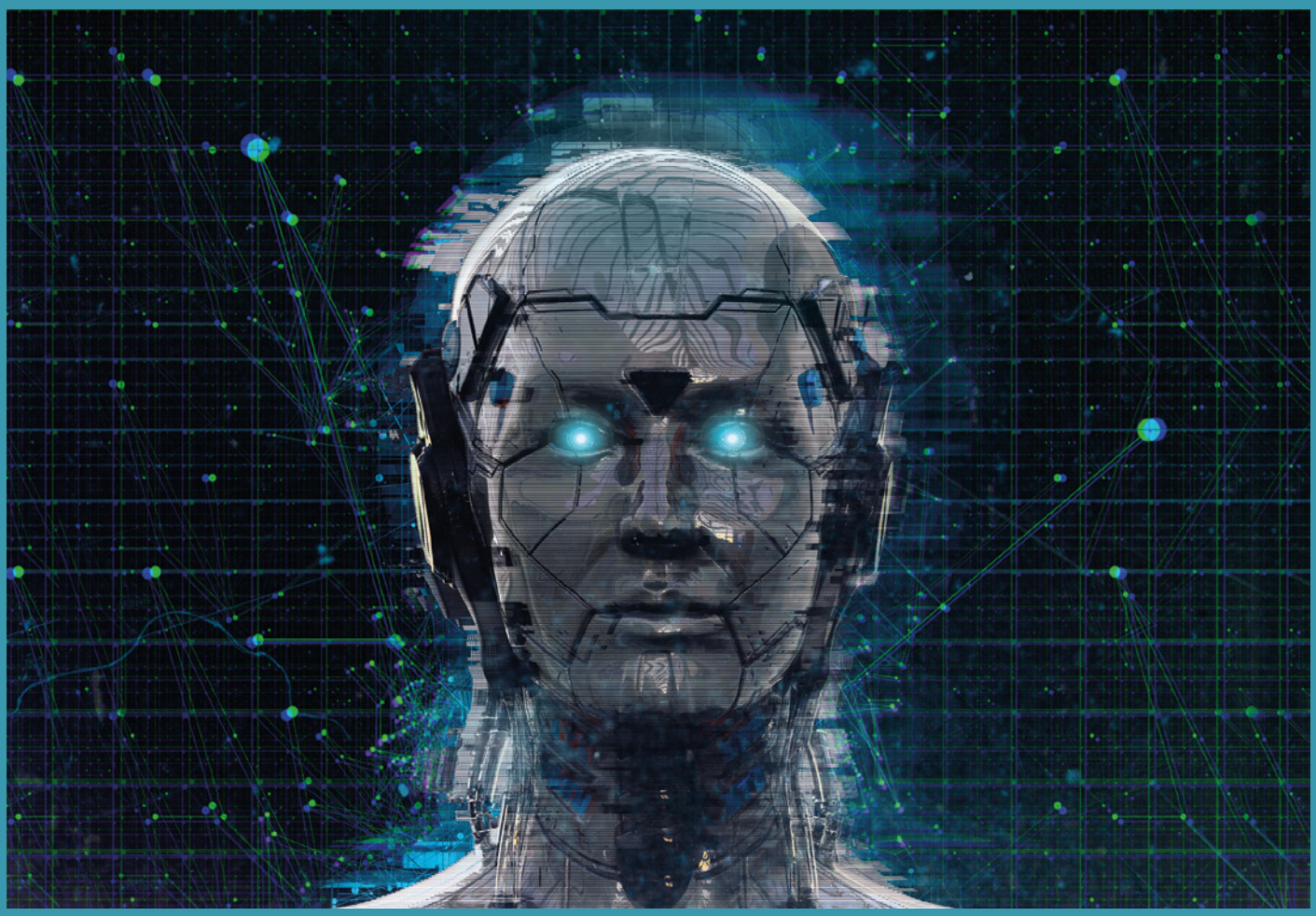
H 7625

FIfF-Kommunikation

Zeitschrift für Informatik und Gesellschaft

41. Jahrgang 2024 Einzelpreis: 7 EUR 1/2024 – März 2024

#FIfFKon2023



Perspektiven, Zukunftsvisionen, Chancen, Utopien

ISSN 0938-3476

• Weizenbaum-Studienpreise • Krieg im Weltraum • KI-Narrative •

FIfF Kommunikation

Zeitschrift für Informatik und Gesellschaft

Titelbild: Bildmaterial: Depositphotos
Autor abidal, ID 275369004

Inhalt

Ausgabe 1/2024

Editorial

Wie in jedem Jahr ist auch 2024 die erste Ausgabe der *FIfF-Kommunikation* der *FIfF-Konferenz* gewidmet, die diesmal am 3.-5. November 2023 am Ostkreuz in Berlin stattfand. Die Beiträge zu diesem Schwerpunkt wurden von Hans-Jörg Kreowski und Margita Zallmann zusammengestellt. Im Schwerpunkteditorial leiten sie ein:

> *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? Welche Perspektiven, Zukunftsvisionen, Chancen, Utopien und Inspirationen für Umbruch und Aufbruch können herausgearbeitet werden? Aufgrund der Rückmeldungen aus der Mitgliedschaft haben sich drei Schwerpunkte herauskristallisiert:*
>
> - Cyberpeace – z. B. Kritik an der Planung zum Future Combat Air System (FCAS) und zur militärischen Nutzung der Künstlichen Intelligenz,
> - Information und Nachhaltigkeit – z. B. Bits & Bäume sowie Informationstechnik und Entwicklungspolitik,
> - Entwicklungen der Künstlichen Intelligenz – z. B. Chancen und Risiken der Entwicklung und Nutzung von ChatGPT sowie Auswirkungen auf die IT-Sicherheit.

Besonderes Gewicht hat dabei der erste Schwerpunkt angesichts des fortdauernden Krieges der Russischen Föderation gegen die Ukraine und des zum Zeitpunkt der Konferenz gerade vier Wochen zurückliegenden Terrorakts der Hamas gegen Israel und der darauf folgenden Bombardierung des Gazastreifens:

> *Seit zehn Jahren greift die Cyberpeace-Kampagne des FIfF das Bedrohungspotenzial durch Cyberangriffe auf und mittlerweile generell die Gefahren durch zunehmende Aufrüstung mithilfe von Informations- und Kommunikationstechnik. Angesichts proklamierter „Zeitenwende" und „Kriegstüchtigkeit" ist das FIfF gefordert, die Risiken durch den militärischen Einsatz von Künstlicher Intelligenz und (teil-)autonomen Waffen zu thematisieren und den Diskurs darüber mitzugestalten.*

Ingesamt ergab sich ein breites Spektrum von Themen, bei denen deutlich wurde, dass die unterschiedlichen Bereiche viele Querverbindungen haben und zusammengedacht werden müssen.

Im Rahmen der FIfF-Konferenz wurde der *Weizenbaum-Studienpreis* verliehen. In diesem Jahr wurden damit zwei Arbeiten ausgezeichnet, die unausweichliche Überwachung aus zwei Perspektiven betrachten: Die problematische Forderung nach „Digitaler Mündigkeit" und die damit verbundene Abwälzung der Verantwortung für Überwachung auf Nutzer:innen, die dieser Verantwortung aufgrund der fortgeschrittenen Überwachungsmethoden nicht mehr gerecht werden können, und die Auswirkung der Überwachungstechniken auf Unbeteiligte – Menschen, die die Technik selbst nicht nutzen, ihr aber aufgrund

Tagungsort der FIfFKon23, Jugendherberge Berlin-Ostkreuz
Foto: privat

ihrer Allgegenwärtigkeit dennoch nicht entgehen können. Die Laudationes und Beiträge der Preisträgerinnen sind ebenfalls in diesem Heft enthalten.

Eine traurige Nachricht ereilte uns am Jahresbeginn: Peter Bittner, früherer stellvertretender Vorsitzender des FIfF und seit vielen Jahren Mitglied des Beirats, ist kurz vor Weihnachten verstorben. Als Grenzgänger zwischen unterschiedlichen Disziplinen beschäftigte er sich mit der Ethik und Profession der Informatik, arbeitete zu gesellschaftlichen, politischen und juristischen Fragen der Informatik, zur informationellen Selbstbestimmung und Überwachungstechniken. Viele seiner Arbeiten bündelte er in einem Entwurf einer Kritischen Theorie der Informatik. Das FIfF hat ihm viel zu verdanken. Wir trauern und erinnern an ihn in einem Nachruf.

Marie-Theres Tinnefeld erinnert an Joseph Weizenbaum und an seine Idee einer Friedensinformatik, die er auch bei der Gründung des FIfF verfolgt hat, an der er beteiligt war. Weizenbaum hat sich stets für Frieden, Freiheit und Toleranz eingesetzt. Die Autorin setzt dies in Beziehung zum wieder wachsenden Antisemitismus und dem Krieg im Gazastreifen – sie fragt, ob es für ihn nicht eine Herausforderung gewesen wäre, einen solidarischen Zusammenhang zwischen Israel und Palästina zu stiften.

Auch über die FIfF-Konferenz hinaus bleibt die *Künstliche Intelligenz* eines unserer zentralen Themen. Rainer Rehak unternimmt eine kritische Einordnung aktueller Narrative *zwischen Macht und Mythos*:

> *Der Einsatz von KI-Technologien verändert tatsächlich unsere Gesellschaften, aber nicht so, wie oft – wahlweise utopistisch oder dystopisch – argumentiert wird. Die Rettung der Menschheit durch eine leistungsstarke, mithin gute KI steht ebenso wenig zu erwarten wie die drohende Auslöschung der Menschheit durch eine unkontrollierbare, mithin böse Superintelligenz.*

Er nennt stattdessen eine Reihen von Folgen und Gefahren dieser Technologien, die Gegenstand gesellschaftlicher Debatten sein müssen, wie die Strukturveränderung des Arbeitsmarktes, die einseitige Macht- und Produktivitätssteigerung weniger Firmen, die Ausweitung personalisierter Überwachung oder die Implikationen militärischer KI-Nutzung. Mit der Regulierung der

Künstlichen Intelligenz auf EU-Ebene, dem *AI Act*, und den damit verbundenen Fragen setzen sich Daniel Leisegang, Chris Köver und Sebastian Meineck von *netzpolitik.org* auseinander. Vor einer weiteren Eskalation des *Kriegs im Weltraum* warnen Dieter Engels, Jürgen Scheffran und Ekkehard Sieker in ihrem Beitrag. Angesichts des Krieges in der Ukraine und der Spannungen zwischen China und den USA sei es *fünf vor zwölf*.

Die Demokratie gegen den zunehmenden Rechtsextremismus zu verteidigen, fordert Dagmar Boedicker in ihrem Beitrag:

> *Wir alle, die wir gruppenbezogene Menschenfeindlichkeit nicht tolerieren, sondern den Respekt für die anderen hegen, den wir für uns erwarten, wir sollten zeigen, dass wir aus der deutschen Geschichte gelernt haben.*

Als Schritte dahin nennt sie das Verbot rechtsextremer Parteien und das Unterbinden deren Finanzierung. Sie stellt eine Reihe von Quellen zusammen, aus denen man sich über den Schutz vor rechtsextremen Angriffen und Aktionsmöglichkeiten informieren kann.

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

Stefan Hügel
für die Redaktion

Der Brief

Ewiger Frieden?

There's no such thing as a winnable war /
it's a lie we don't believe anymore
(Sting, vor langer Zeit)

Liebe Freundinnen und Freunde des FIfF, liebe Mitglieder,

als der *Kalte Krieg* anfang der 1990er-Jahre endete, hofften wir, dass damit auch die Zeit militärischer Konflikte an ein Ende gekommen sei. Wie wir heute wissen, war diese Hoffnung trügerisch – doch im Prinzip wusste das schon Immanuel Kant:

> *Der Friedenszustand unter Menschen, die nebeneinander leben, ist kein Naturzustand (status naturalis), der vielmehr ein Zustand des Krieges ist, d. i. wenngleich nicht immer ein Ausbruch der Feindseligkeiten, doch immerwährende Bedrohung mit denselben.*[1]

Wurde Deutschland (und seine Nachbarstaaten) in den Jahren nach dem zweiten Weltkrieg von einem „heißen" Krieg verschont, bestand tatsächlich die *immerwährende Bedrohung* – bis hin zur atomaren Vernichtung durch einen Krieg zwischen den Machtblöcken. Wer in den 1980er-Jahren aufgewachsen ist, kann sich sicher noch gut an Sirenenproben, übende Tiefflieger über Wohngebieten, NATO-Manöver und Medienberichte über eskalierende Atomrüstung erinnern – in dieser Zeit und unter dieser Bedrohung wurde bekanntlich 1984 auch das FIfF gegründet.[2]

Dieser Konfrontation der Machtblöcke war mit dem Fall des *eisernen Vorhangs* scheinbar vorbei – doch seit Bundeskanzler Scholz in der Folge des Angriffs Russlands auf die Ukraine die *Zeitenwende* ausgerufen und Bundesverteidigungsminister Pistorius den Begriff der *Kriegstüchtigkeit*[3] in die Welt gesetzt hat, hat man immer mehr den Eindruck, dass sich Politiker:innen und Leitmedien gegenseitig in ihren eskalierenden Statements – gepaart mit dem Aufbau eines *Feindbilds* Russland[4] – übertreffen wollen. Aussagen von Donald Trump zur Zukunft der NATO[5] scheinen regelrechte Panik auszulösen. Einige Beispiele aus den letzten Tagen:

- Der französische Präsident Emmanuel Macron fordert, auf Kriegswirtschaft umzustellen und die Produktion von Waffen und Munition zu steigern. „*Selbst die Entsendung von Bodentruppen will Macron an diesem Abend nicht ausschließen, auch wenn darüber, wie er zugibt, kein Konsens in der gemeinsamen Diskussion bestanden habe.*"[6]

- Von eigenen Atombomben für die Europäische Union spricht die Spitzenkandidatin der SPD für die Europawahl, Katharina Barley.[7]

- „Der Krieg muss nach Russland getragen werden", fordert der CDU-Politiker Roderich Kiesewetter.[8] Er forderte gleichzeitig, das Sondervermögen für die Bundeswehr auf 300 Mrd. € zu erhöhen.[9]

- Nicht fehlen darf in dieser Aufzählung „Oma Courage" Marie-Agnes Strack-Zimmermann.[10] Zuletzt ließ sie sich mit einem albernen Stierkopf auf dem T-Shirt ablichten, um für die Lieferung von Taurus-Marschflugkörpern in die Ukraine zu werben.[11]

Doch was wollen wir eigentlich unter *Kriegstüchtigkeit* verstehen? Versuchen wir es in drei Dimensionen:

- *Mentale* Kriegstüchtigkeit – die Menschen müssen auf militärische Eskalation geistig vorbereitet werden, sie für notwendig halten oder gar wollen. Hier wurden bereits in der Vergangenheit große Erfolge erzielt. Es ist wohl davon auszugehen, dass die Techniken der Propaganda (a. k. a. *Politische Kommunikation*) im Lauf der Jahre deutlich verfeinert und perfektioniert wurden und werden[12] – auch bei Kindern.[13]

- *Physische* Kriegstüchtigkeit – Menschen, die willens und fähig sind, den Krieg zu führen und deren technische Ausstat-

tung. Vorschläge, Wehrkunde als Schulfach[14] und eine allgemeine Musterung für den Wehrdienst[15] einzuführen, wären erste Schritte in diese Richtung.

- *Finanzielle* Kriegstüchtigkeit – Finanzielle Mittel, um die Kriegstüchtigkeit herzustellen. Dafür gibt es das 2 %-Ziel der NATO, Sondervermögen im deutschen Grundgesetz und Forderungen nach einer Kriegswirtschaft. Die akquirierten Mittel werden großzügig ausgegeben – leidet die Bundeswehr womöglich nicht an Geldmangel, sondern an dessen Verschwendung?[16] Die Akzeptanz für eine höhere Finanzierung der Bundeswehr – auch auf Kosten von Einsparungen in anderen Bereichen – liegt laut einer Umfrage bei 72 %.[17]

Mit manchen Statements und Forderungen werden (noch) rote Linien überschritten – es ist gut, dass Bundeskanzler Scholz vernünftig bleibt und sowohl die Lieferung der Marschflugkörper *Taurus* nach wie vor ablehnt[18] als auch Macron hinsichtlich der Bodentruppen in der Ukraine widerspricht.[19] Katharina Barley ruderte beim Thema Atomwaffen schnell zurück. Doch all diese Verlautbarungen tragen zu einer Diskursverschiebung bei und erweitern den Bereich des sagbaren. *Man wird das doch einmal sagen dürfen!* Ja, darf man, aber wir müssen uns entschieden dagegen stellen.

> *Wenn es Pflicht, wenn zugleich gegründete Hoffnung da ist, den Zustand eines öffentlichen Rechts, obgleich nur in einer ins Unendliche fortschreitenden Annäherung wirklich zu machen, so ist der e w i g e F r i e d e, der auf die bisher fälschlich sogenannte Friedensschlüsse (eigentlich Waffenstillstände) folgt, keine leere Idee, sondern eine Aufgabe, die, nach und nach aufgelöst, ihrem Ziele (weil die Zeiten, in denen gleiche Fortschritte geschehen, hoffentlich immer kürzer werden) beständig näher kommt.[20]*

Lasst uns gemeinsam um friedliche Lösungen ringen. Militärische Eskalation hat selten in der Geschichte etwas Gutes bewirkt.

Mit FIfFigen Grüßen
Stefan Hügel

Anmerkungen

1 *Kant I (1984 [1781]) Zum ewigen Frieden. Stuttgart: Reclam, S. 10*
2 *Damit begeht auch das FIfF in diesem Jahr sein 40-jähriges Bestehen, was im weiteren Verlauf des Jahres noch zu feiern sein wird …*
3 *Es fällt auf, dass Pistorius von Kriegstüchtigkeit – nicht etwa von Verteidigungstüchtigkeit – gesprochen hat.*
4 *Strack-Zimmermann: Bundeswehr braucht ein Feindbild. 31. Mai 2022, dpa-Newskanal zit. nach sueddeutsche.de, https://www.sueddeutsche.de/politik/verteidigung-strack-zimmermann-bundeswehr-braucht-ein-feindbild-dpa.urn-newsml-dpa-com-20090101-220531-99-497796*
5 *Deutsche Politiker entsetzt über Trump-Äußerung zur Nato, Spiegel online, https://www.spiegel.de/politik/deutschland/donald-trump-und-die-nato-aeusserung-deutsche-politiker-entsetzt-a-a1200f43-0391-474f-891d-4d271d172cfe*
6 *Sandberg B (2024) … und dann spricht Macron über Bodentruppen, Spiegel online, https://www.spiegel.de/ausland/ukraine-unterstuetzerkonferenz-in-paris-was-laesst-sich-tun-fuer-die-ukraine-a-91cd3550-97ff-43d0-b200-f70893a325e4*
7 *Barley bringt eigene EU-Atombomben ins Gespräch, Spiegel online, https://www.spiegel.de/politik/deutschland/katarina-barley-spd-spitzenkandidatin-fuer-die-europawahl-bringt-eu-atombomben-fuer-europaeische-armee-ins-gespraech-a-263da72d-c631-4bfa-aa1d-94-f9f77cb8cc*
8 *Naumann F (2024) „Krieg muss nach Russland getragen werden": CDU-Experte fordert Eskalation – gegen den Worst Case, FR online, https://www.fr.de/politik/ukraine-waffen-deutschland-forderung-appell-kiesewetter-cdu-russland-krieg-putin-zr-92825380.html*
9 *CDU-Verteidigungspolitiker will 300 Milliarden Euro für Bundeswehr, Zeit online, https://www.zeit.de/politik/deutschland/2024-02/roderich-kiesewetter-verteidigung-bundeswehr-sondervermoegen-nato-donald-trump*
10 *Zippel T (2023) Abgehoben im Kampfjet: Bundeswehr führt Sonderflug für FDP-Politikerin durch. Ostthüringer Zeitung, https://www.otz.de/politik/abgehoben-im-kampfjet-bundeswehr-fuehrt-sonderflug-fuer-fdp-politikerin-durch-id239341153.html*
11 *Wieduwilt H (2024) Politikerin trägt Kriegsbotschaft auf einem T-Shirt – ist das stimmig? n-tv, https://www.n-tv.de/politik/politik_wieduwilts_woche/Politikerin-traegt-Kriegsbotschaft-auf-einem-T-Shirt-ist-das-stimmig-article24759493.html*
12 *Tögel J (2023) Kognitive Kriegsführung. Neueste Manipulationstechniken als Waffengattung der NATO, Frankfurt am Main: Westend*
13 *Ich bin ein großer Verfechter des öffentlich-rechtlichen Rundfunks. Ein besonders verstörendes (oder gar: widerliches) Beispiel scheint mir dennoch der Videoclip „Kein Taurus für die Ukraine?" (https://www.youtube.com/shorts/kgsVFZXnkAE) zu sein. Mein Versuch, das als Satire zu verstehen, ist leider gescheitert. Ein Kommentar dazu findet sich z. B. bei Voges C (2024) ZDF-Waffenkunde für den Nachwuchs: Taurus? Na „logo"?, Telepolis, https://www.telepolis.de/features/ZDF-Waffenkunde-fuer-den-Nachwuchs-Taurus-Na-logo-9643868.html*
14 *Alan Posener (2022) Für Wehrkunde im Schulunterricht, Zeit online, https://www.zeit.de/gesellschaft/schule/2022-06/wehrkunde-schule-unterricht-armee/komplettansicht. Zuletzt wurden von Bildungsministerin Stark-Watzinger ähnliche Vorschläge gemacht: https://www.tagesschau.de/inland/gesellschaft/schulen-katastrophenschutz-100.html*
15 *Wehrbeauftragte Högl bringt Rückkehr der Musterung ins Spiel, Spiegel online, https://www.spiegel.de/politik/deutschland/bundeswehr-eva-hoegl-bringt-rueckkehr-der-musterung-ins-spiel-a-10b712ef-2ece-48b1-8775-c7b50bdce875*
16 *Gebauer M (2024) Rechnungshof rügt geplanten Milliardendeal für neue Soldatenkopfhörer, Spiegel online, https://www.spiegel.de/politik/deutschland/rechnungshof-ruegt-geplanten-milliardendeal-fuer-neue-soldaten-kopfhoerer-a-90e70e6e-da96-4184-9fc7-9967b2040667*
17 *Das ergab eine Erhebung von statista im Februar 2024: https://de.statista.com/statistik/daten/studie/967899/umfrage/umfrage-zu-ausgaben-fuer-bundeswehr-und-verteidigung-in-deutschland/. Ob daraus auch die Bereitschaft zum eigenen Verzicht folgt, also – beispielsweise – die gerade demonstrierenden Landwirte auf die Subventionierung des Diesels zu Gunsten der Bundeswehr verzichten würden, wurde nicht erhoben.*
18 *Scholz begründet Ablehnung der Taurus-Lieferung, Spiegel online, https://www.spiegel.de/politik/deutschland/ukraine-olaf-scholz-begruendet-ablehnung-der-taurus-lieferung-a-3a43bb97-3709-4e24-80c9-dafb6ca2de75*
19 *Scholz stellt sich gegen Macron-Äußerungen über Bodentruppen, Spiegel online, https://www.spiegel.de/politik/deutschland/ukraine-krieg-olaf-scholz-stellt-sich-gegen-aeusserungen-von-emmanuel-macron-ueber-bodentruppen-a-10557ca4-169b-4a34-a505-52fa965b8147*
20 *Kant I (1984 [1781]) a. a. O., S. 56*

Eva Hornecker, Stefan Hügel, Sylvia Johnigk, Constanze Kurz, Kai Nothdurft, Jens Woinowski und andere, die Peter geschätzt haben

Nachruf auf Peter Bittner

Wir trauern um unser Beiratsmitglied

Es gab wohl niemand im FIfF, der oder die Peter nicht schätzte und mochte. Als Grenzgänger zwischen den Disziplinen hat er in und zwischen Informatik, Wirtschaftswissenschaften, Philosophie und Soziologie gearbeitet. Als wissenschaftlicher Mitarbeiter beschäftigte er sich mit der Ethik und Profession der Informatik, arbeitete zu gesellschaftlichen, politischen und juristischen Fragen der Informatik, zur informationellen Selbstbestimmung und Überwachungstechniken (mit dem Schwerpunkt auf Videoüberwachung und Biometrie). Viele seiner Arbeiten bündelte er in einem Entwurf einer Kritischen Theorie der Informatik. Er lehrte an den Technischen Universitäten Kaiserslautern und Darmstadt, der Humboldt-Universität zu Berlin sowie an der Berufsakademie Berlin. Daneben betreute er Studierende an der Hochschule München. Als IT-System-Berater konfigurierte er ERP-Systeme und entwickelte Betriebs-, Datenschutz- und Sicherheitskonzepte. Als Berater für Betriebsräte kämpfte er für datenschutzgerechte IKT-Systeme in den Betrieben und den Beschäftigtendatenschutz. Er war zehn Jahre im Bundesvorstand des FIfF und bis zuletzt Mitglied des Beirats.

Das FIfF dankt ihm für seine fachkundige und selbstlose Tätigkeit für den Verein.

Universitäten und FIfF-Regionalgruppen

Peter studierte von 1987 bis 1996 Informatik mit Nebenfach Wirtschaftswissenschaften an der Universität Kaiserslautern. Begleitende Studien in Mikroelektronik, Berufspädagogik und Philosophie ergänzten sein Studium, insbesondere hatte er großes Interesse an Technikfolgenforschung und Technikphilosophie/-ethik und informationeller Selbstbestimmung. Dazu war er aktiv in der Fachschaftsarbeit. Über diesen Weg haben ihn einige von uns dann auch kennen gelernt – 1992 beim Datenschutz-Arbeitskreis auf der KIF 20,0 in Rostock. Er nahm 1993 als Student zusammen mit mehreren anderen *Kiffeln* und weiteren Studierenden auch an einem *Teapot* genannten intensiven, privat organisierten Wochenendseminar mit Wilhelm Steinmüller teil, das Peters Interesse am Themengebiet *Informatik und Gesellschaft* vertiefte.

An der TU Darmstadt war er von 1996 bis 2001 wissenschaftlicher Mitarbeiter am Zentrum für Interdisziplinäre Technikforschung (ZIT) und von 1998 bis 2001 Kollegiat im Graduiertenkolleg *Technisierung und Gesellschaft* am Fachbereich Geschichts- und Gesellschaftswissenschaften.

Die FIfF-Regionalgruppe Darmstadt, in der Peter sehr aktiv war, hat die Jahrestagung 1998 unter dem Motto *Mensch – Informatisierung – Gesellschaft* organisiert. Im November 2023 war das 25 Jahre her. Was wir damals *Informatisierung* genannt haben, dürften heute viele unter dem Schlagwort *Digitalisierung* wiedererkennen. Wenn man durch den Tagungsband stöbert, den Peter mit herausgegeben hat, findet man einiges, was immer noch relevant ist. Ein paar Schlagworte aus den Key Notes von Rafael Capurro und Christiane Floyd sind zum Beispiel *Cyberkultur, Vernetzung als Lebenskunst, Virtualisierung des Selbst, Verproduktung und Mediatisierung des Selbst* und *Zusammenwirken von Menschen und intelligenten Agenten.* Was weder Peter noch die Vortragenden damals so vorhergesehen haben dürften, waren einige der düsteren Aspekte des noch jungen Internet, wie die Verrohung der sogenannten sozialen Medien. Auch das Phänomen der alternativen Fakten gehört, wie eine dialektische Antithese zur Informatisierung, zu den Dingen, die vielleicht auch Peter überrascht haben.

Jens Woinowski erinnert sich nicht nur an diese seriösen Unternehmungen, sondern auch an Erlebnisse in der Darmstädter WG. Wie die Idee, Peperoni mit Knoblauch zu braten:

> *„Wir hatten eine verdammt scharfe Version von Peperoni erwischt und saßen nach den ersten Bissen erst mal etwas ratlos in unserer WG-Miniküche. Unsere Rettung war die Packung Toastbrot, die wir dann innerhalb weniger Sekunden intus hatten."*

Von Oktober 2001 bis September 2006 arbeitete Peter als wissenschaftlicher Mitarbeiter bei Prof. Wolfgang Coy in der AG Informatik in Bildung und Gesellschaft an der Humboldt-Universität zu Berlin (HU). 2006/2007 war er Lehrbeauftragter an der HU Berlin (Datenschutz) und an der Berufsakademie Berlin (DV-Recht). Ab 2008 arbeitete er in wechselnden Funktionen an mehreren Hochschulen und als betrieblicher Datenschutzbeauftragter, seit 1995 auch als Mitglied im Berufsverband der Datenschutzbeauftragten Deutschlands (BvD). Er arbeitete u. a. in der DGB-Technologie-Beratungsstelle in NRW und bildete als Sachverständiger Betriebsräte zum Datenschutz weiter.

Aus Treffen der Regionalgruppe Rhein-Main ergab sich u. a. ein Interview mit der Zeitschrift *Testcard* in der *Apfelweinwirtschaft Frank* in Frankfurt.[1] Peter hat zahlreiche Vorträge beim FIfF, dem CCC und anderen gehalten und viel publiziert. Ein paar Vorschläge zum Nachlesen siehe unten.

FIfF-Tagungen

Von 1995 bis 2005 war Peter im Vorstand, von 2001 bis 2005 als stellvertretender Vorsitzender. Lange hat er sich gewissenhaft um die ungeliebten Finanzen gekümmert und für viele FIfF-Aktivitäten Verantwortung (und Arbeit) übernommen. Einige Vorstandssitzungen in Berlin fanden in Peters Dachgeschosswohnung statt. Ein paar Mal kam auch Joseph Weizenbaum, damals Ehrenmitglied im Vorstand, zu diesen Berliner Treffen. Peter war gastfreundlich. Dagmar Boedicker erinnert sich an seine winzige Wohnung – die muss in Darmstadt gewesen sein. Mehr als die Hälfte dieser Wohnung gehörte seinen Büchern, aber für Übernachtungsgäste war immer Platz.

2002 wurde Peter Mitglied der GI-Arbeitsgruppe *Verantwortung* innerhalb der Fachgruppe *Informatik und Gesellschaft* und wirkte an den ethischen Leitlinien der Gesellschaft für Informatik mit, die die Fachgruppe als Präsidiumsarbeitskreis überarbeitete (veröffentlicht 2003)[2]. Danach blieb er aktiv in der Fachgruppe *Ethik und Informatik* der GI. Aus dieser Zeit stammen eine Reihe von Veröffentlichungen zu ethischen Fragen in der Berufspraxis der Informatik und zu Informatik als Profession. 2004 richtete er maßgeblich die Tagung zum 20. Jubiläum des FIfF in Adlershof in Kooperation mit der GI aus: *20 Jahre FIfF – ReVisionen kritischer Informatik*. Es war eine umfassende Tagung, bei der u. a. der damals aktuelle *World Summit on the Information Society* (WSIS) behandelt wurde. Und es war die einzige FIfF-Konferenz, die vier Tage von Donnerstag bis Sonntag stattfand.

Mit dem Tagungsband zur Jahrestagung 1998 begann die Reihe *Kritische Informatik* im Lit-Verlag. Den achten Band *Gesellschaftliche Verantwortung in der digital vernetzten Welt* hat Peter wieder, zusammen mit einigen anderen bekannten FIfFerlingen, im Jahr 2014 herausgegeben. Das war der Jubiläumsband zum 30-jährigen Bestehen des FIfF.[3] Leider wird Peter das 40. Jubiläum nicht mehr mit uns feiern können.

Befreundete Organisationen

Constanze Kurz vom CCC hat Peter an der Humboldt-Universität (wahrscheinlich 2005) kennen und wie viele andere als sehr zugewandten, hilfsbereiten und humorvollen Kollegen schätzen gelernt:

> *„Er war ein Netzwerker, Organisator und kannte sich in seinen Themenfeldern hervorragend aus, nicht nur inhaltlich, sondern auch, was die forschenden und aktivistischen Menschen anging. Wir haben mehrere Seminare zusammen gestaltet, was eine große intellektuelle Freude war."*

Auch in anderen Kooperationen des FIfF setzte Peter sich klug und erfolgreich ein, so in der Zusammenarbeit des AK Videoüberwachung mit anderen Organisationen wie der Humanistischen Union zu den Themenbereichen Videoüberwachung, Biometrie und Datenschutz, mit Digitalcourage (damals als FoeBuD bekannt) in der Jury der Big Brother Awards, den Negativ-Preisen für Datenkraken.

Sein umfassendes technisches Wissen hat er übrigens auch in das Design von Bällen für Bahnengolf investiert, profan Minigolf genannt. In jüngeren Jahren spielte er in der Hessischen Amateurliga und besaß einen Koffer mit Bällen (hundert oder mehr).

Zum Nachlesen

Wolfgang Coy et al. (2013) Informatik in Bildung und Gesellschaft. *https://www.yumpu.com/de/document/view/9894766/informatik-in-bildung-gesellschaft-informatik-in-bildung-und-* (abgerufen 12.01.2024)

Peter Bittner, Stefan Hügel, Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht, Britta Schinzel Hg. (2014) Gesellschaftliche Verantwortung in der digital vernetzen Welt, Münster: Lit-Verlag mit Beitrag: Peter Bittner, Eva Hornecker (2014) A Micro-Ethical View on Computing Practice, S. 189-204

Peter Bittner: Unser aller Profession gib uns heute … oder die Frage nach einer mäeutischen[4] Informatik. In: F. Nake, A. Rolf, D. Siefkes (Hrsg.): Wozu Informatik? Theorie zwischen Ideologie, Utopie und Phantasie. Berlin, 2002, S. 42-45.

Peter Bittner, Jens Woinowski Hg. (1999) Mensch – Informatisierung – Gesellschaft, Münster: Lit-Verlag

Beiträge und Schwerpunkte für die FIfF-Kommunikation, beispielsweise Kritisch studieren … und dann? (1/2000 mit Eva Hornecker), Lächeln … gleich kommt das Vögelchen. Gedanken zur Videoüberwachung (1/2002, mit Hardy Frehe, Julia Stoll, Jens Woinowski), 4/2003 zu Softwarepatenten gemeinsam mit Sabrina Geißler, Digital Rights Management und Alternativen 4/2003 mit Volker Grassmuck. Und 4/2012 Theorien der Informatik – allgemein, handlungsorientiert, mäeutisch, 3/2013 Wenn der Mensch vermessen zur Informatik wird …über Biometrie im Masseneinsatz und ihre Grenzen, 2/2014 Videoüberwachung durchschauen, …

Anmerkungen

1 *Waltraud Blischke (2014) Bugs, Big Data und die UnverNETZbaren. Ein Gespräch mit Peter Bittner, Stefan Hügel und Julia Stoll vom FIfF. testcard – Beiträge zur Popgeschichte, #24: Bug Report. Digital war besser, Mainz*

2 *Aktuelle Fassung unter https://gi.de/ueber-uns/organisation/unsere-ethischen-leitlinien (abgerufen 12.1.24)*

3 *Links zur Reihe Kritische Informatik: https://www.lit-verlag.de/isbn/978-3-643-12876-8 und https://www.lit-verlag.de/isbn/978-3-8258-3930-3 (abgerufen 12.1.24)*

4 *(griechisch Hebammenkunst) „… die sokratische Methode, durch geschicktes Fragen die im Partner schlummernde, ihm aber nicht bewussten richtigen Antworten u. Einsichten heraufzuholen." (Duden. Das Fremdwörterbuch. 2001. 7. Aufl. Dudenverlag. Mannheim – Wien – Zürich)*

Marie-Theres Tinnefeld

Weizenbaum: Herkunft, Forschung, Vision

Der Universalgelehrte und professionelle Jurist Gottfried Wilhelm Leibniz zeichnete – wie schon Platon im Protagoras (Sophistiae) zuvor – den Menschen als Mängelwesen, das ohne Technik, ohne Gestaltung der Welt zur Lebenswelt nicht lebensfähig ist.[1] Die moderne Welt wird von der Computertechnik bestimmt, die Leibniz federführend mitentwickelt hat.[2] Er ist u. a. Erfinder der Binärzahlen, die die Grundlage für völlig neue Reichweiten des Computers bilden. Der Mathematiker Leibniz erkannte deren „grundsätzliche Bedeutung für eine Formalisierung aller Wissens- und Wissenschaftsbereiche" und kann als Ahnherr der Informationstechnologie bezeichnet werden[3], die aktuell mit Fragen der Künstlichen Intelligenz verbunden wird.

Leibniz glaubte wie viele seiner Zeitgenossen, dass die technologischen Gegebenheiten in einem göttlichen Heilsplan begründet sind. Heute wird angesichts der neuen technischen Möglichkeiten dagegen nach der Verantwortung des Menschen gefragt, die sich bei entstehenden Defiziten an Steuerungsfähigkeit und grundrechtlicher Legitimation zeigen. Ist es zutreffend, dass eine Gefährdung der Autonomie des Menschen immer an den Menschen selbst liegt? Wird die Technik nicht überschätzt? Und trägt nicht gerade der Informatiker für die so bezeichnete „Künstliche Intelligenz" oder KI (Artificial Intelligence oder AI) Mitverantwortung?[4]

Mit Blick auf Bilder vom Menschen hat sich der Mathematiker und Informatiker Joseph Weizenbaum mit den Folgen neuer Technologien befasst.[5] Denn das Konzept von Menschenbildern schließt Fragen darüber ein, welcher Wert Menschen zugemessen wird, worin ihre Aufgabe und ggf. auch ihre Verantwortung angesichts des technologischen Fortschritts und der jeweiligen Kultur- und Religionsgeschichte gesehen werden kann. So wies Weizenbaum eindringlich daraufhin, dass die Frage menschlicher Verantwortung keine technische, sondern eine gesellschaftliche Frage ist. Und er kritisierte, dass unsere Gesellschaft zwar Technik entwickelt, aber die Verantwortung dafür verweigert oder sie so verteilt, dass „niemand" sie wahrnimmt.[6]

Das Projekt „Verweigerung" erinnert an den Ausspruch des Schreibers Bartleby, einem Helden von Herman Melville, dem Verfasser des legendären Moby Dick. Das Motto dieses Schreibers, der eine Art Kafka-Figur ist, war: „I would prefer not to."[7] Macht sich der Schreiber damit unangreifbar, unzugänglich? Bedeutet sein Verhalten Stillstand? Ein Denken und Agieren in Kontexten wären jedenfalls bei Bartleby unvorstellbar.

Für Weizenbaum aber ist Wissen, Wahrheit und Bedeutung nur in entsprechenden Kontexten zu verstehen.[8] So ist auch Technologie immer nur im sozialen und kulturellen Kontext zu begreifen. Im Folgenden soll versucht werden, Herkommen und Denkräume von Joseph Weizenbaum zu skizzieren.

Deutscher, Amerikaner, Jude

Joseph Weizenbaum wurde 1923 als Sohn eines Kürschners in Berlin geboren. In diese Stadt sollte er nach der Emigration mit seiner jüdischen Familie 1936 in die USA seit 1996 wieder leben und 2008 sterben. Sein Blick richtete sich in Deutschland nicht auf seine jüdische Vergangenheit in Deutschland, also nicht nach „rückwärts", sondern immer auf die Gestaltung der Zukunft.[9]

Weizenbaums besondere Bedeutung als Informatiker war mit einer moralischen Idee verbunden: der des Friedens. Der Idee einer „Friedensinformatik" widmete er sich auch in Zusammenarbeit mit dem Forum Informatikerinnen für Frieden und gesellschaftliche Verantwortung e. V. (FifF), das er mitbegründet hat.[10]

Nach dem Menschheitsverbrechen, dem Holocaust, darf es in Deutschland keinen Riss mehr zwischen Juden und Nichtjuden geben. Und dennoch breitet sich in diesem Land eine erneute „Expansion des Antisemitismus in allen Tönen und Gesichtern der Niedertracht und des Menschenhasses" aus.[11] Die Einstellung rechtsextremer Kreise in Deutschland hat fatale Folgen für Juden in Deutschland und der Welt. Endlich gehen heute tausende von Deutschen auf die Straße und protestieren gegen den Rechtsextremismus, für Frieden und für eine offene Demokratie, in der kein Platz für Antisemitismus ist. Die sprengende Kraft des Antisemitismus zeigte sich ungebremst in Israel am 7. Oktober 2023 durch den brutalen Terrorangriff der Hamas. Vor diesem Hintergrund ist auf ein neues Werk der israelischen Schriftsteller Moshe Zimmermann und Moshe Zuckermann zu verweisen, die in den Ruf nach Frieden für Israel die palästinensische Zivilbevölkerung einbeziehen und Solidarität mit einem demokratischen Israel ohne Abspaltung der palästinensischen Zivilbevölkerung fordern.[12]

Informatiker, Fragen der Verantwortung

Als Pionier der *Computer Science* gehörte Weizenbaum zu den scharfen und phantasievollen Kritikern seines Fachs. Der Übergang vom vernünftigen Urteil zur schieren Berechnung, ja die Ersetzung des menschlichen Urteils durch die Entscheidung, die an einen Computer delegiert wird, ist das Grundthema seiner Kritik der Gesellschaft.[13] Im Dialog mit Gunna Wendt vermittelte Weizenbaum ein Bewusstsein selbstbestimmter Freiheit bis hin zum Tod.[14]

Weizenbaum selbst hat von 1964 bis 1966 in der Abteilung Physik am Massachusetts Institut of Technology (MIT) ein Computerprogramm entwickelt, mit dem sich Menschen über eine Fernschreibkonsole auf englisch „unterhalten" konnten. Dabei handelte es sich um die Anfänge eines natürlich-sprachlichen Dialoges. Das Programm gestaltete Weizenbaum nach dem Theaterstück von Bernard Shaws Pygmalion und nannte es *Eliza*.[15] Das Stück bezieht sich auf den antiken Mythos von Pygmalion, auf die Metamorphosen von Ovid[16], auf den Wandel der Gesellschaft, und die Verwandlung der Welt bzw. der Menschheit durch technische und andere Prozesse.

Eliza parodierte psychotherapeutische Gespräche, in dem das Programm Sätze aufnahm und umformulierte wie etwa „Tut mir leid, zu hören, dass Sie heute depressiv sind". Weizenbaum

selbst war überrascht, dass die Mensch-Maschine-Kommunikation so überzeugend simuliert werden konnte, dass Menschen dem sprechenden Computer vertrauliche Informationen offenbarten. Inhalt ist damals wie heute die Frage, ob leblose Objekte, algorithmengesteuerte Roboter menschenähnlich sind oder gar zu menschlichen Subjekten werden können. So hält beispielsweise der Bestsellerautor Yuval Harari die Vorstellung, dass den Menschen unüberwindliche Grenzen, Tabus, vorgegeben sind, für eine verblassende Fiktion. Denn die Menschen seien dabei, anorganisches Leben zu schaffen. Dadurch würden menschliche und nichtmenschliche Akteure zu hybriden Handlungseinheiten zusammengefasst.[17]

Weizenbaum bestand entschieden darauf, dass technologische Entwicklungen, die das Leben von Menschen im Kern verändern können, von keinem Menschen verantwortet werden können. Joseph Weizenbaum war überzeugt, dass der Mensch durch „maschinelles Denken" nicht voll erfasst werden kann, ihm bestimmte Denkakte vorbehalten bleiben müssen.[18] Er war überzeugt davon, dass der Mensch auch in Grenzsituationen die Hebel der Technik verantwortungsbewusst in der Hand behalten muss.

Für Weizenbaum stand die einzelne Person mit ihren vielfältigen Eigenschaften und widersprüchlichen Neigungen, die Einzigartigkeit eines jeden menschlichen Wesens im Zentrum seines Denkens.[19] Er wandte sich damit gegen die verbreitete Lehre von der „Ohnmacht des Einzelnen". Mit seinem Insistieren darauf, dass „die Ohnmacht des einzelnen eine gefährliche Illusion sei", appelliert er an die Chance des Menschen, „sich selbst als handlungsfähiges Wesen zu begreifen".[20] Und er betonte, dass Zivilcourage immer, auch in „kleinen" Situationen Mut braucht, um Ängste zu überwinden[21], um aktuell und ganz konkret gegen den wachsenden Antisemitismus anzugehen, sich vom geschlossenen zum offenen Menschenbild im Sinne der Erklärung der Allgemeinen Menschenrechte zu bewegen. Die ersten Worte der UN-Menschenrechtsdeklaration lauten: „Alle Menschen werden frei geboren, mit gleicher Würde und gleichen Rechten."

Sei ein Mensch

Bei dem Holocaust-Gedenken im Deutschen Bundestag am 31. Januar 2024 erinnerte der jüdische Redner Marcel Reif an den Satz seines Vaters: „Sei ein Mensch." Diesen Satz habe ihm sein Vater mit auf dem Weg gegeben, und zwar „in dem warmen Jiddisch", das er so vermisse. Diese Aussage korrespondiert mit der Weltsicht von Weizenbaum, der den Menschen nicht in Segmente zerlegte, sondern immer in seiner Ganzheitlichkeit betrachtete. „Ohne den Mut, den Welten in uns und außerhalb uns entgegenzutreten, ist eine solche Ganzheitlichkeit unmöglich zu erreichen."[22] So das Frühwarnsystem Weizenbaums!

Die Publizistin Rachel Salamander zitiert in ihrer Rede bei ihrer Verleihung der Moses-Mendelssohn-Medaille den Namensgeber der Medaille, den jüdischen Aufklärer Mendelssohn. Er habe nach der Überlieferung auf die Frage eines preußischen Offiziers, welchen Handel bzw. welches „Schachern" er betreibe, geantwortet: „Ich handle mit Vernunft!"[23] Dieses Diktum bezieht sich jenseits von Zeit und Raum auf den Menschen als Vernunftwesen und entspricht damit dem Inhalt der universalen Menschenrechte.

Die Verkettung von Herkunft, Aussehen und Beruf mit negativen Vorurteilen gehörten zur antisemitischen Konsensgeschichte des deutschen Kaiserreichs.[24] Sie erzeugten und erzeugen Ablehnung und Feindbilder. Es kann mit Marcel Reif nur wiederholt werden: „Sei ein Mensch!" Öffne die Fenster menschenrechtlicher Aufklärung! Die sich in Sozialen Netzwerken ausbreitenden algorithmengesteuerten Desinformationen, Fake News und Hate-Speeches gegen Juden setzen auf alte Vorurteile und sind weder mit den Grund- und Menschenrechten auf Meinungs- und Kunstfreiheit vereinbar noch achten sie die Menschenwürde, die den menschlichen Umgang mit dem Fremden und kulturell Andersdenkenden einschließt.

Joseph Weizenbaum trug an seiner linken Hand immer einen Ring mit dem Davidstern, der wohl als ein Signal für Freiheit und Toleranz gedeutet werden kann. Es ist anzunehmen, dass es dem Denken Weizenbaums entsprechen würde, dass sich Bürgerinnen und Bürger mit Zivilcourage für die Redefreiheit, insbesondere auch für die grundrechtlich garantierte Freiheit der Meinungsäußerung auch der Deutschen einsetzen würde, die jüdische Vorfahren haben. Gerade diese Personen werden heute häufig bei ihrer kritischen Auseinandersetzung mit der derzeitigen israelischen Regierung als „Antisemiten" abgestempelt. Ist es nicht zynisch, dass ein Zweifel an der Verhältnismäßigkeit des Krieges der israelischen Regierung als antisemitisch und damit als diskriminierende Einstellung bezeichnet wird?[25] Wird mit einer Kritik an der Regierung das Existenzrecht des israelischen Staates in Frage gestellt? Würde es Weizenbaum nicht für eine friedensstiftende Herausforderung halten, einen solidarischen Zusammenhang zwischen Juden und Palästinensern zu stiften, wie es etwa schon Martin Buber versucht hat?[26]

Marie-Theres Tinnefeld

Prof. Dr. **Marie-Theres Tinnefeld** ist Juristin und Publizistin, mit zahlreichen Konferenzen und Veröffentlichungen im In- und Ausland zum Thema *Informationsrecht und europäische Rechtskultur*. Sie ist Mitglied im Beirat des FIfF e. V.

Anmerkungen

1 *Poser, Theoria cum praxis. Das Leibnizsche Akademiekonzept und die Technikwissenschaften, in: Rechtshistorisches Journal, Bd. 15, hrsg. v. Dieter Simon, (1996). S. 167.*
2 *Vgl. Mathematische Schriften von G.W. Leibniz, hrsg. v. C.I. Gerhardt (1849-1864) (1962).*
3 *Poser, ebd., S. 168.*
4 *Manfred Broy, Zur Bewahrung unserer Autonomie vor den Automaten: Zum Menschenbild des Informatikers, in:Weis (Hrsg.), Bilder vom Menschen in Wissenschaft, Technik und Religion (1993) Faktum Bd. 2. (1993), S. 67ff.*
5 *Joseph Weizenbaum, Computermacht und Gesellschaft. Freie Reden, hrsg, v. Gunna Wendt und Franz Klug (5. Auflage 2023.), S. 35 ff.*
6 *Weizenbaum, ebd., S. 33.*
7 *Hanjo Kesting, I would prefer not, Frankfurter Hefte, Ausgabe 7+8 (2019), unter: https://www.frankfurter-hefte.de/artikel/I-would-prefer-not-to-278/ (zuletzt abgerufen am 30.01.2024).*
8 *Weizenbaum, ebd., S. 15f.*
9 *Wendt unter: https://www.weizenbaum-institut.de/w-100/weizenbaum-auf-der-spur/ (zuletzt abgerufen am 31.01.24).*
10 *Vgl. FIfF Kommunikation 4/2023. Das Heft „Wissenschaft für den Frieden" ist vor allem dem Andenken an Joseph Weizenbaum gewidmet.*
11 *Reinhard Merkel, Zum Staunen. Heimstatt jüdischer Kultur nach dem Völkermord: Rachel Salamanders Lebenswerk – eine beispiellose Leistung, ein Werk des Friedens. Eine Laudatio, SZ v. 32.01.2024 Feuilleton, 9.*
12 *Moshe Zimmermann an Moshe Zuckermann, in: dies., Denk ich an Deutschland…Ein Dialog in Israel (2023), S. 291ff.*
13 *Joseph Weizenbaum, Computer Power and Human Reason. From Judgement to Calculation (1976), s.a. Tinnefeld. MMR 12/2020, 799.*
14 *Joseph Weizenbaum im Gespräch mit Gunna Wendt, Wo sind sie, die Inseln der Vernunft im Cyberstrom, (2006).*
15 *Eliza Doolittle (bekannt als „My fair Lady") ist eine fiktive Figur, die Bernard Shaw nach Ovids Pygmalion 1912 gestaltet hat.*
16 *Ovid, Met. 10. 243-97 berichtet von Pygmalion, König auf Zypern, der sich in die elfenbeinerne Kultstatue der Göttin Aphrodite verliebt haben soll, die diese dann lebendig werden ließ.*
17 *Yuval Harari, Eine kurze Geschichte der Menschheit, aus dem Englischen von Jürgen Neubauer, 2015.*
18 *Tinnefeld, in: Tinnefeld/Buchner/Petri/Hof, Einführung in das Datenschutzrecht (7. Auflage 2020) , Prolog XXXI m. w. N.*
19 *Weizenbaum ebd., S. 33., Wendt/Klug, ebd. S. 133ff.*
20 *Wendt/Klug, in: Weizenbaum ebd., S. 133f.*
21 *Wendt/Klug, ebd., S. 133.*
22 *Zit. nach Wendt/Klug, ebd., S. 135.*
23 *Salamander, Ich wollte Neues in die Welt bringen, SZ v. 01.02.2024, Leute R2.*
24 *Peter Schäfer, Kurze Geschichte des Antisemitismus (2. Auflage 2020).*
25 *Moshe Zuckermann an Moshe Zimmermann, in, dies., Denk ich an Deutschland … (2023), S. 283f. Michael Agi, Zur Dogmatik des Verhältnismäßigkeitsgrundsatzes im Völkerrecht der bewaffneten Konflikte und im Völkerstrafrecht (Diss. 2022).*
26 *Martin Buber, Ein Land und zwei Völker, hrsg. u. eingeleitet von Paul R. Mendes Flohr (3. Auflage 2018).*

Rainer Rehak

Zwischen Macht und Mythos

Eine kritische Einordnung aktueller KI-Narrative

Bei der Veröffentlichung des interaktiven Chatbots ChatGPT durch das US-amerikanische Unternehmen OpenAI im November 2022 wurde das erste Mal eine Anwendung der künstlichen Intelligenz (KI) vorgestellt, die auch für Laien beeindruckende Ergebnisse liefert und als textbasierte Webanwendung quasi voraussetzungslos benutzt werden kann. Dadurch war es sowohl der Medienwelt als auch interessierten Akteuren aus Politik, Wirtschaft und Zivilgesellschaft – ebenso wie Privatpersonen – möglich, diese Art von Technik unmittelbar selbst auszuprobieren. Diskussionen zur aktuellen Leistungsfähigkeit und möglichen Entwicklungen dieser Technologie wurden so in der Breite der Gesellschaft anschlussfähig und das Thema KI war quasi über Nacht brennend aktuell.

Obwohl es viele andere Arten künstlicher Intelligenz gibt, zeichnen sich an den Diskursen über die Möglichkeiten und Grenzen von ChatGPT und ähnlichen Programmen einige wiederkehrende Narrative ab, die die gesellschaftliche Auseinandersetzung mit KI aktuell prägen. Der Artikel beginnt mit einer kurzen historischen und technischen Einordnung von KI-Systemen und widmet sich anschließend einer Beschreibung und kritischen Reflexion der gängigen Narrative, wie etwa Entscheidungs-, Wissens- und Wahrheitsfähigkeit, apolitische Neutralität, Demokratisierungspotenzial sowie Arbeitsplatzvernichtung und gesellschaftliche Utopien/Dystopien durch KI. Der Artikel schließt mit einem Gesamtfazit zur gesellschaftlichen Auseinandersetzung mit dem Thema künstlicher Intelligenz.

Eine kurze Geschichte der KI

Der Terminus *Artificial Intelligence* (AI) wurde im Jahre 1955 durch US-Informatiker um John McCarthy und Marvin Minsky eingeführt, um ein Forschungsprogramm im Rahmen der Dartmouth Conference vorzustellen und dafür Forschungsgelder einzuwerben.[1] In dem Zusammenhang klang „Artificial Intelligence" natürlich vielversprechender als Automatentheorie, wie das Feld zuvor hieß. In Abgrenzung zur traditionellen Automatentheorie etablierte sich alsbald ein Forschungsfeld mit dem Ziel, Computer intelligence simulieren zu lassen. Während die grundsätzliche Idee intelligenter Computer schon älter ist und sich etwa auf die Kommunikation mit Menschen bezog[2], beschrieb *intelligence* nunmehr das Vorhaben, Computer so zu programmieren, dass sie alle möglichen Aufgaben erledigen können, die bislang nur dem Menschen vorbehalten waren.[3]

Um diesem Ziel näher zu kommen, bildeten sich in den folgenden Dekaden im Wesentlichen zwei Strömungen innerhalb der Informatik heraus, die unterschiedliche Ansätze bei der Entwicklung von KI-Systemen verfolgten. Einerseits entstanden die sogenannten symbolischen Systeme, bei denen Informationen explizit abgespeichert und miteinander verknüpft werden (etwa

„Hauptstadt(Deutschland)=Berlin"). Die eingegebenen Daten und Zusammenhänge können dann strukturiert durchsucht und logisch kombiniert werden. Schachcomputer etwa funktionierten lange Zeit auf diese Weise – während des Spiels wurden Datenbanken mit den Verläufen vergangener Schachpartien durchsucht, um einen Zug zu ermitteln, der in Anbetracht der Spielsituation die eigene Gewinnwahrscheinlichkeit erhöht. Dieser Ansatz ermöglichte später die sogenannten Expertensysteme und Wissensdatenbanken, mit denen beispielsweise komplexe medizinische Probleme vereinfacht werden sollten, indem etwa aus Symptomen und anderen Krankendaten automatisiert individuelle (Differenzial-)Diagnosen erstellt werden.[4]

Andererseits und parallel dazu wurden sogenannte subsymbolische Systeme entwickelt, auch *Machine Learning* (ML) genannt, bei denen Informationen und Zusammenhänge nur implizit vorgehalten werden. Entsprechende Systeme sind so gestaltet, dass sich die Programmkonfiguration (etwa bestimmte Parameter im System) anhand von vielen Eingabedaten automatisiert so lange verändert, bis das Ergebnis in der gewünschten Qualität vorliegt. Wie das Programm letztendlich zu diesem Ergebnis gelangt, ist zweitrangig und lässt sich auch nicht ohne Weiteres nachvollziehen.

Während in symbolischen Systemen logische Zusammenhänge explizit modelliert und bei der Entwicklung in das System eingeschrieben werden, verläuft die Konfiguration subsymbolischer Systeme in vielen kleinen automatisierten Schritten. Dabei enthält das Programm am Ende eine Vielzahl komplexer statistischer Beziehungen, aber keine expliziten semantischen Zusammenhänge: Insofern die eingegebene Datengrundlage das hergibt, gibt es etwa bei einer textbasierten KI dann beispielsweise eine abstraktstatistische Beziehung zwischen den Worten „Hauptstadt", „Deutschland" und „Berlin", aber diese ist nicht direkt aus den unzähligen Parametern des Systems auslesbar.

Ein aktuell viel genutzter subsymbolischer Ansatz sind die *Künstlichen Neuronalen Netze* (KNN), die in den 1960er-Jahren erdacht wurden und der Vernetzung von Neuronen im menschlichen Gehirn nachempfunden sind. Im Vergleich zu diesen sind KNN sehr stark vereinfacht, sie werden im Computer als mathematische Gleichungen mit vielen Variablen abgebildet. Sie sind also komplexe statistische Modelle, die mit sehr vielen Beispieldaten vorkonfiguriert – „trainiert" – werden müssen, bevor sie eingesetzt werden können. Ein so vorkonfiguriertes KNN heißt „Modell", kann auf neue Daten angewendet werden und darin automatisiert Muster detektieren oder gar neue Muster generieren. In Bezug auf Bilddaten heißt das etwa, dass ein dafür erzeugtes Modell bei Eingabe eines Fotos hinreichend gut detektieren kann, ob darauf ein Affe, ein Pferd, ein Mopshund oder keines der drei Tiere zu sehen ist. Oder das Modell könnte Bilder von Affen, Pferden beziehungsweise Mopshunden generieren. So etwas ist mit symbolischen Ansätzen der künstlichen Intelligenz nie gelungen, denn dafür müssten sämtliche Kriterien für bestimmte Tiere auf Fotos explizit definiert werden, was praktisch unmöglich ist.

Weil in den 1980er-, 1990er- und 2000er-Jahren trotz vereinzelter methodischer Neuerungen konkrete Durchbrüche ausblieben, wurde es in dieser Phase immer wieder ruhig um die künstliche Intelligenz – oft ist in diesem Zusammenhang vom „KI-Winter" die Rede. Durch gesteigerte Rechenleistung, massenhaft verfügbare Daten (Stichwort *Big Data*) und das Aufkommen des Web 2.0, das es Nutzer:innen zunehmend ermöglichte, selbst Inhalte zu „generieren" (Stichwort User-generated content), konnte künstliche Intelligenz ab den 2010er-Jahren jedoch wieder von sich reden machen. Inzwischen kann KI nicht nur Bilder, sondern auch Texte erzeugen (man denke an automatische Übersetzungen von Aufsätzen und Transkriptionen von Tonaufnahmen oder eben Chatbots). Die Qualität vieler Systeme ist mittlerweile so gut, dass sie breit genutzt werden.[5]

Seit jeher wurde die technische Entwicklung von künstlicher Intelligenz stets von einem Diskurs bezüglich der Möglichkeiten und Grenzen der jeweiligen Systeme begleitet. Im Jahr 1966 entwickelte der Informatiker Joseph Weizenbaum ein simples Chatprogramm namens ELIZA – heute würden wir es als symbolische KI-Anwendung bezeichnen –, das zeigen sollte, wie einfach es ist, menschliches Verständnis zu simulieren.[6] Das Programm sollte einen Gesprächspsychotherapeuten nachahmen, indem es Begriffe aus den Texteingaben der Nutzer:innen in vorkonfigurierte Fragekonstruktionen einfügte („Was meinen Sie, warum X so ist?") oder aber generische Erwiderungen ausgab („Führen Sie das gern etwas aus."). Die für Weizenbaum verblüffende Reaktion bestand darin, dass dem Chatprogramm über die Fachwelt hinaus tatsächlich Empathie und Persönlichkeit zugeschrieben wurden. Diese Reaktionen machten ihn zu einem der vehementesten Kritiker mythischer Technikgläubigkeit, übersteigerter Erwartungen an Automatisierung und der Tendenz, Computer zu vermenschlichen.[7] Seitdem beschreibt der „Eliza-Effekt" den Hang, KI-Systemen menschliche Eigenschaften wie Intelligenz oder Bewusstsein zuzuschreiben, wenn sie nur gut genug typisch menschliche Redewendungen, Aussehen oder Verhaltensweisen imitieren.

Auch die wirtschaftlichen Folgen von KI wurden schon vor fünfzig Jahren diskutiert. So schrieb der Philosoph Hubert Dreyfus bereits im Jahr 1972 kritisch über den damaligen KI-Hype: „Jeden Tag lesen wir, dass digitale Computer Schach spielen, Sprachen übersetzen, Muster erkennen und bald in der Lage sein werden, unsere Jobs zu übernehmen"[8] – eine Prognose, die schon damals regelmäßig zu hören war und auch in den jüngeren Debatten eine wichtige Rolle spielt.[9]

Diese überaus grobe Zusammenfassung soll zwei Dinge herausstellen: Einerseits hat das Feld der künstlichen Intelligenz mittlerweile so große Erfolge vorzuweisen, dass alle, die mit dem Computer arbeiten, auch regelmäßig KI-Systeme nutzen (ob indirekt in Suchmaschinen oder direkt zum Übersetzen). Andererseits zeigt sich, dass die knapp 70-jährige Geschichte dieser Technologie von Anfang an geprägt war von der großen Erzählung einer angeblich kurz bevorstehenden KI-Revolution, die alles für immer verändern werde[10], oft mit apokalyptischem Unterton.[11]

Um in der teilweise unübersichtlichen Gemengelage von Gegenwartsdiagnosen und Vorhersagen Orientierung zu bieten, werden im Folgenden aktuell prominente Narrative zu künstlicher Intelligenz umrissen und diskutiert. Auf dieser Grundlage können dann sachgerechte Diskussionen über die gesellschaftspolitischen Implikationen von KI-Systemen angestoßen werden – über Potenziale, Gefahren, Regulierung und Gestaltung dieser Technologien.

Zwei Arten von KI und ein Diskurswerkzeug

Um einzelne Narrative analysieren zu können und die Bedingungen zu verstehen, unter denen künstliche Intelligenz aktuell gesellschaftlich verhandelt wird, müssen noch zwei Arten von KI-Systemen unterschieden werden. Diese werden in Diskursen zu künstlicher Intelligenz regelmäßig aufgegriffen und oft vermischt, obwohl sie jeweils verschiedene Eigenschaften und Implikationen haben.

Erstens gibt es domänenspezifische KI-Systeme (artificial narrow intelligence, ANI), manchmal auch schwache KI genannt, die für einen Aufgabenbereich konzipiert und entwickelt werden. Sie sind für bestimmte Abläufe optimiert, aber auch nur in diesem Rahmen überhaupt zu gebrauchen.[12] Ein Programm zur energieeffizienten Klimatisierung von Rechenzentren etwa wird mit ausgewählten Lastdaten der Vergangenheit vorkonfiguriert, sodass es den Einsatz von Kühlaggregaten je nach Bedarf wirtschaftlich regelt; es kann jedoch keine Musik-Playlist kuratieren. Ebenso wenig kann ein Schachprogramm Bilder erzeugen oder eine Bildgenerator-KI mathematische Regressionsanalysen durchführen. Darum sind vermenschlichende Begriffe wie „selbstlernend" unpassend.[13] Alle aktuell existierenden KI-Systeme fallen zweifelsfrei in die Kategorie domänenspezifischer künstlicher Intelligenz, vom modernen Go-Computer über Bilderkennungs- oder Übersetzungssoftware bis hin zu den großen Sprachmodellen (large language models, LLMs) wie OpenAIs GPT, Googles PaLM/Bard, BAAIs WuDao oder Metas LlaMa.

Zweitens gibt es das Konzept universeller KI-Systeme (artificial general intelligence, AGI), manchmal auch starke KI genannt, die eigenständig lernfähig seien und abstrakt denken könnten, dazu Kreativität, Motivation sowie Bewusstsein und Emotionen besäßen.[14] In manchen Vorstellungen haben diese AGIs geradezu übermenschliche Fähigkeiten.[15] Allerdings gibt es bislang weder eine funktionierende AGI noch belastbare Anhaltspunkte, dass ein solches System mit aktuellen Computerarchitekturen überhaupt entwickelt werden kann.[16] Zwar gibt es seit Jahrzehnten Forschungsprojekte und Wettbewerbe in diese Richtung – etwa der weltbekannte Loebner-Preis, bei dem eine Version des Turing-Tests zum Einsatz kommt –, doch die Ergebnisse blieben bislang stets ernüchternd. Zudem haben sich die breit diskutierten AGI-Zielmarken, also welche technischen Probleme dafür gelöst werden müssen, regelmäßig verschoben. Ehemals galt es eine Partie gegen den Schachweltmeister zu gewinnen, inzwischen ist automatische Texterzeugung der Maßstab. Viele Fachleute zweifeln sogar grundsätzlich an der Möglichkeit einer allgemeinen künstlichen Intelligenz in Form eines Digitalcomputers.[17] Dass dennoch oft über diese Art von KI diskutiert wird, hat mit geschäftlichen Motiven wirtschaftlicher Akteure zu tun[18], aber auch mit der zentralen Rolle solcher Systeme in Science-Fiction-Filmen, siehe etwa Samantha in ‚HER', Data in ‚Star Trek', HAL 9000 in ‚2001', Ava in ‚Ex Machina', C3PO in ‚Star Wars', Bishop in ‚Aliens', T-800 in ‚Terminator' oder auch dem Maschinenmenschen in ‚Metropolis'.[19]

Um die schwammige Verwendung von künstlicher Intelligenz im gesellschaftlichen Diskurs zu charakterisieren, schlage ich den Begriff der Zeitgeist-KI vor.[20] In dem Zusammenhang kann der Begriff KI dann von Big Data und Statistik über Software, IT, Digitalisierung, Algorithmen, Roboter, Apps und IKT bis hin zum Internet in etwa alles bedeuten. Auch im politischen Diskurs wird pauschal von „künstlicher Intelligenz" gesprochen, egal, ob es um selbstfahrende Autos, Roboterhunde, automatisierte Entscheidungssysteme, Klimamodelle, automatisierte Arbeitsmarktvermittlungssysteme, Tischreservierungssysteme oder smarte Verkehrsleitsysteme geht; beizeiten werden auch traditionelle Informatikprodukte mit dem Label versehen. Alles ist „KI", obwohl in alledem wenig bis keine künstliche Intelligenz steckt. In einem aktuellen Bericht zum Stand von KI in der öffentlichen Verwaltung heißt es etwa, „dass oftmals Projekte als KI-basiert bezeichnet würden, jedoch de facto konventionelle IKT-Anwendungen nutzen".[21] Aber auch in Wissenschaft und Wirtschaft ist jenes schwammige Verständnis anzutreffen.[22] Um eine reflektierte gesellschaftliche Auseinandersetzung mit künstlicher Intelligenz zu ermöglichen, muss dieses Verständnis expliziert, mithin aufgelöst werden.[23]

Besprechung aktueller KI-Narrative

Vor diesem Hintergrund können wir nun gängige Narrative zu künstlicher Intelligenz umreißen und diskutieren – auf welchen Annahmen beruhen sie, inwieweit entsprechen diese dem aktuellen Stand der Forschung, welche gesellschaftspolitischen Implikationen haben sie? Oftmals überschneiden und vermischen sich diese Erzählungen, sodass die folgende Darstellung nach Stichworten eine analytische Trennung vornimmt, die eher einer schlaglichtartigen Analyse von Diskursen zum Thema KI als einer systematischen Darstellung ihres Gegenstands dient. Die Ausführungen stützen sich auf Erkenntnisse aus der kritischen Informatik sowie den *critical data and algorithm studies*, der Datenschutztheorie und ferner der Philosophie des Geistes und der Semiotik.

Autonomie/Agency – Oft wird KI-Systemen die Fähigkeit zugesprochen, eigenständig „zu agieren" oder etwas „zu entscheiden".[24] Solche Diskussionen gehen implizit von der Annahme aus, KI-Systeme seien zu selbständigem Handeln (im Gegensatz etwa zu bloßem Verhalten) befähigt[25] und nicht bloß (komplexe) Werkzeuge, die einen extern gesetzten Zweck umsetzen. Handlungsfähigkeit impliziert jedoch eigene Intention, innere Vorstellung der Sachlage, einen potenziell alternativen Handlungsausgang, überdies ein Moment der bewussten Entscheidung und dann letztlich auch Verantwortlichkeit. KI-Systeme verhalten sich jedoch deterministisch – grundsätzlich erfolgt bei gleicher Eingabe, wie bei anderen Maschinen auch, die gleiche Ausgabe.[26] Ist dies nicht der Fall, wie etwa bei ChatGPT, so liegt das an absichtlich eingebauten Zufallsparametern und somit an Entscheidungen bei der Entwicklung, nicht an einer vermeintlich eigenen Handlungsfähigkeit der KI. Intention und eine innere Vorstellung sind gar nicht vorhanden. Solange es keine AGI gibt, sind die Ergebnisse aller KI-Systeme primär das Ergebnis von Designentscheidungen, gegebenenfalls inklusive Zufall oder Fehlern. Wenn die eingesetzten Systeme ihre Zwecke nicht erfüllen, ändern Hersteller und Betreiber sie, justieren nach und korrigieren, was den Werkzeugcharakter solcher Systeme weiter unterstreicht. Dass Anwendungen künstlicher Intelligenz eher großtechnischen Anlagen denn einfachen Werkzeugen gleichen, ändert nichts daran, dass ihre Charakterisierung als eigenständige Akteure von den tatsächlich verantwortlichen Organisationen (Firmen, Behörden etc.) ablenkt, die diese Systeme für ihre eigenen Zwecke programmieren oder kaufen und einsetzen. Autonomie – in einem bedeutsamen Sinn – haben diese Systeme daher keine.[27]

Wahrhaftigkeitsanspruch – Aktuelle KI-Systeme können weder lügen noch hochstapeln. Selbstverständlich können die Aussagen falsch sein (und das sind sie auch oft[28]), aber eine Lüge impliziert das Wissen um die Wahrheit und eine absichtliche Abkehr davon. Gleichermaßen impliziert Hochstapelei das Wissen um die eigene Identität und ein absichtliches Vorspielen einer anderen. KI-Systeme können keine Wahrheitsansprüche erheben, weil sie genau das ausgeben, was Modellarchitektur und Daten vorgeben. Sie können daher auch nicht achtlos Unsinn reden, strategisch manipulieren oder bewusst ablenken, denn all dies würde mindestens einen inneren Zustand, eine Motivation, ein Geistesmodell und ein Modell des Anderen voraussetzen. Wie oben beschrieben, bestehen KI-Systeme jedoch aus zwar komplexen, aber rein formalen Abläufen. Die einsetzenden Organisationen hingegen haben sehr wohl Interessen und potenziell auch das Wissen um die Wahrheit und die eigene Identität. Entsprechende Ansprüche müssen gegenüber den Entwicklerfirmen und -organisationen geltend gemacht werden.

Wissen und Wahrheit – Aktuelle textbasierte KI-Anwendungen wie ChatGPT beruhen auf Sprachmodellen, die gemäß ihrer Architektur aus den Unmengen an Eingabetexten mehrdimensionale Vektorräume errechnen, in denen der „Abstand" von Worten und Wortarten abgespeichert wird; das ist das Sprachmodell. Daraus werden in der normalen Nutzung Texte generiert, indem das Modell auf Basis einer User-Eingabe („Prompt") das wahrscheinlichste nächste Wort ermittelt.[29] Dann sind Prompt plus erstes Ergebniswort wiederum die interne Eingabe für das nächste Wort. Dies wird mehrfach wiederholt. So setzt sich die Ausgabe („Antwort") des Chatbots zusammen. Die Ausgaben sind also formalmathematisch begründete Aneinanderreihungen von Zeichenketten, die statistisch rekombiniert aus den Eingabetexten abgeleitet werden und deren Bedeutung – anders als bei den weniger leistungsfähigen symbolbasierten Wissensmodellen – für das System technisch bedingt gar keine Rolle spielen kann.[30] Dementsprechend sind Wahrheit oder Richtigkeit keine relevanten Kriterien für die Antworten und können es auch nicht ohne Weiteres werden. Die Ergebnisse solcher KI-Systeme (re)-produzieren die formalen Verhältnisse von Worten zueinander in den Ausgangstexten, genau das ist ihre Funktion. Die Ergebnisse sind teilweise beeindruckend, aber umso obskurer sind auch die Fehler, etwa wenn nichtssagende Allgemeinplätze oder reine „Fantasiefakten" ausgegeben werden. Streng genommen können Sprachmodelle jedoch keine „Fehler" machen, die Wortreihen in den Ausgangstexten sind eben, wie sie sind.[31] Gerade der Stil – also die Form – der generierten Texte ist in der Regel tadellos, da auch die Texte, an denen das Modell trainiert wurde, in der Regel stilistisch sehr gut sind. Insofern ergibt es wenig Sinn, zu behaupten, dass ChatGPT „sogar" Texte im Stil von Gedichten, akademischen Artikeln, Zeitungsmeldungen oder Handbüchern produzieren könne, denn es ist ja gerade die Form, auf die Sprachmodelle optimiert sind und etwas anderes ist mit dieser Technologie auch gar nicht möglich.[32] Mathematisch gesprochen sind die Ergebnisse also Variationen eines statistischen Durchschnittstexts innerhalb des Modells und zwar relativ zur jeweils konkreten Abfrage. Als passende Analogie bietet sich ein stochastischer Papagei an, der gemäß statistischer Regeln Wortfolgen reproduziert.[33] Mit echter Sprachkompetenz und Verständnis haben wir es weder in dem einen noch dem anderen Fall zu tun.

Vorhersagen – KI-Systeme können formale Muster und Abhängigkeiten von Variablen in vorhandenen Datensätzen detektieren, seien es Wetter-, Geschäfts- oder Verhaltensdaten. Diese Muster beziehen sich notwendigerweise immer auf die Vergangenheit, können aber statistisch ausgewertet und mathematisch in die Zukunft projiziert werden. Inwiefern das dann aber als Vorhersage im eigentlichen Sinne taugt, hängt vom Gegenstandsbereich ab. Sind es Daten und Abhängigkeiten, die physikalischen Gesetzen unterliegen, etwa Wetterdaten, kann das funktionieren. Sind es hingegen soziale Daten, erzeugen solche Vorberechnungen zwar ein Ergebnis, welches aber nur dann die Zukunft vorhersagt, wenn diese genau so strukturiert ist, wie es die (Daten-)Vergangenheit war – eine nicht nur aus wissenschaftstheoretischer und sozialwissenschaftlicher Sicht heikle Annahme, selbst wenn die Daten der Vergangenheit vollständig wären.[34] Der Aufstieg und Niedergang von Predictive Policing (zu Deutsch „vorrausschauende Polizeiarbeit") illustriert das Problem gut, denn dort wurde angenommen, dass sich Kriminalität auf ähnliche Weise wie Erdbeben geografisch vorhersagen lässt. Die jeweilig zugrunde liegenden Prozesse sind jedoch sehr verschieden – gesellschaftliche Prozesse folgen im Gegensatz zu physikalischen Vorgängen gerade keinen feststehenden Gesetzen. In der Praxis waren die Ergebnisse von Predictive-Policing-Softwares kaum zu gebrauchen – teilweise trafen die Voraussagen in weniger als ein Prozent der Fälle zu und in anderen Fällen reproduzierten sie sogar Rassismus, indem etwa Straftaten übermäßig in schwarzen Nachbarschaften angezeigt wurden.[35]

Neutralität und Objektivität – Datenbasierten Systemen wird häufig Neutralität und Objektivität attestiert, so ist es auch mit KI-Systemen. Dabei gestalten bestimmte Akteure die System- und Modellarchitektur für einen bestimmten Zweck. Diesem Zweck entsprechend wählen sie auch die Datengrundlage des Systems aus, die wiederum entscheidend für die Ergebnisse des Systems ist. Prinzipiell gibt es keine objektiven oder neutralen Daten, sondern nur jeweils passende Daten in Relation zu einem bestimmten Einsatzzweck.[36] Beispielsweise ist es möglich, Feinstaubsensoren in einer Stadt anzubringen, um die Luftqualität zu messen, aber in welcher Höhe und an welchen Orten (Parks, Straßen, Kindergärten etc.) dies geschieht, ist eine Entscheidung, die von Akteuren und Zwecken abhängt. Und selbst wenn es – rein hypothetisch – möglich wäre, eine „totale" Datenbasis in perfekter Qualität zu haben, müssten dennoch unzählige Entscheidungen für die konkrete Verarbeitung getroffen werden, um praktisch nutzbare Ergebnisse zu liefern. Wäre etwa bei der vorausschauenden Polizeiarbeit die Schadenshöhe vergangener Verbrechen miteinbezogen worden, hätten die Systeme überwiegend die Hauptgeschäftsviertel und Finanzhandelsplätze von Städten als Kriminalitätsschwerpunkte angezeigt, doch das entsprach nicht dem Zweck. Diese Art Entscheidungen braucht es bei allen datenbasierten Systemen – inklusive KI, weshalb keines davon als „neutral" oder „objektiv" gelten kann.

Selbst Ansprüche und Kritik an KI-Systemen unterstellen jedoch oft deren (mögliche) Neutralität beziehungsweise Objektivität, etwa wenn sie Fairness einfordern oder Diskriminierung durch diese Systeme bemängeln. Diese Ansätze greifen mitunter zu kurz, weil es sich bei Fairness nur teilweise um eine technische Eigenschaft der Systeme handelt und gerade die Frage, was als nicht-diskriminierend und fair gilt, primär von gesellschaftlichen Aushandlungsprozessen abhängt.[37] Ein automatisches Kredit-

vergabesystem basierend auf dem Einkommen einer Person beispielsweise kann aktuell nur korrekt oder fair sein: entweder es ist korrekt, aber reproduziert dann das geschlechtsspezifische Lohngefälle, oder es ist fair, aber mathematisch gesehen inkorrekt.[38]

(A)politische Optimierung – Beizeiten werden gesellschaftliche und politische Fragen als im Wesentlichen durch KI lösbare Aufgaben diskutiert.[39] Dazu zählen etwa das Abwenden des Klimawandels[40], die Einführung eines automatisierten Grundeinkommens oder die Beendigung des Welthungers.[41] Dem Narrativ nach erscheint das als möglich, mithin vielversprechend, weil KI apolitische und „unideologische" Lösungen für gesellschaftliche Probleme erzeugen könne. Diese Erzählung ist aus mehreren Gründen problematisch. Sie verkennt etwa, dass bevor KI-Systeme Muster detektieren oder Prozesse optimieren können, zunächst einmal festgelegt werden muss, was genau gesucht und was in einem bestimmten Sachbereich als Optimum gelten soll. Erst daraus ergibt sich eine sinnvolle Definition der technischen Zielfunktion des Systems. Auch diese Festlegung ist prinzipiell eine politische Frage, die gesellschaftlicher Aushandlung bedarf. Denn selbst wenn Einigkeit bezüglich eines Ziels herrscht, gibt es in der Regel unzählige Strategien, um es zu erreichen. Auch die Wahl der Zwischenschritte und die Gewichtung der relevanten Faktoren sind kategorisch keine technischen Fragen, sondern politische. Insofern besteht der Widerspruch des Narrativs in der Annahme, dass KI-Systeme ihre eigene gesellschaftliche Ausgangsbedingung als technisches Ergebnis liefern könnten. Das lässt sich an zwei Beispielen verdeutlichen. Eine KI kann den Energieverbrauch eines Rechenzentrums reduzieren (Ziel), indem es anhand von Lastdaten energieeffiziente Kühlzyklen berechnet (Strategie).[42] Dies ist möglich, wenn Ziel und Strategie unstrittig sind. Im Bereich der Stadtplanung wiederum kann eine KI bei Mobilitätsfragen helfen und beispielsweise dazu beitragen, die Auslastung von Autostraßen und Parkplätzen im Hinblick auf Verkehrsaufkommen zu optimieren (Stichwort *smart cities*). Die Frage aber, wie eine Stadt lebenswerter gestaltet werden kann, und ob dabei nicht eher eine Fahrradinfrastruktur mit erweiterten Fußgängerzonen zielführend wäre, ist jedoch keine technische Frage. Generalisiert gilt das auch für die Bekämpfung des Welthungers. Sollte man bestimmten Ländern Schulden erlassen, internationale Wirtschaftsverträge ändern, die Nahrungsverteilung überdenken, bestimmte Technologien global zugänglich machen oder ganz andere Maßnahmen ergreifen? Und wer sollte sie finanzieren? All das sind politische Fragen, die KI-Systeme nicht lösen können. Sie können bestenfalls helfen, Beispielszenarien zu errechnen und gegebenenfalls die Umsetzung zu erleichtern. Selbst bei der Auswahl und dem Modellieren der relevanten Rahmenbedingungen handelt es sich um Aufgaben, die kollektive, also politische Entscheidungen erfordern.

Demokratisierung – Auch wenn KI-Systeme komplexe Werkzeuge sind, die aktuell von mächtigen Konzernen entwickelt werden, wird oft gemutmaßt, dass diese Werkzeuge über kurz oder lang durch gesteigerte Effizienz und andere technische Verbesserungen bald allen zur Verfügung stehen könnten und somit eine Demokratisierung von KI ermöglichen würden.[43] Was zunächst wie ein erstrebenswertes politisches Anliegen klingen mag, entpuppt sich bei genauerem Hinsehen als Wirtschaftsagenda. „Demokratisierung" meint in diesem Fall nämlich nicht die Kontrolle oder Mitgestaltung solcher Technologien durch selbstorganisierte Gemeinschaften, sondern lediglich den breiten Nutzungszugriff für Unternehmen.[44] Die Kontrolle solcher Systeme kann auch schwerlich demokratisiert werden. Während es im Hinblick auf kleine, hochspezialisierte KI-Systeme mit einer vergleichsweise kleinen Datenbasis noch möglich sein kann, ist es bei großen KI-Systemen wie etwa LLMs hingegen illusorisch, da der technische, organisatorische (und energetische) Aufwand für Gestaltung und Herstellung schlechthin immens ist. Ihr Entwicklungsprozess schließt die Datenerhebung, ihre Qualitätssicherung, Klassifikation und Speicherung ein, betrifft weiter das inkrementelle Modelldesign und das Vorkonfigurieren („Training") der Modelle und hört auch bei der Moderation und Verfeinerung der KI-Systeme durch menschliche Arbeitskräfte nicht auf (Stichwort *Reinforcement Learning from Human Feedback*), die größtenteils in den globalen Süden ausgelagert wird.[45] Dementsprechend steckt hinter großen KI-Systemen eine komplexe globale Lieferkette.[46] Zudem müssen die Systeme regelmäßig aktualisiert, sämtliche genannten Schritte also regelmäßig wiederholt werden. Daten und Systeme altern schließlich auch. Es ist also kein Zufall, dass nur finanzstarke Player wie OpenAI, Meta, BAAI oder Google regelmäßig Durchbrüche bei LLMs vermelden können, denn nur sie verfügen über das nötige Kapital, um solche Projekte zu stemmen. Man kann behaupten, dass diese Art KI quasi die Atomkraft des Digitalen ist[47], also grundsätzlich nur durch mächtige Akteure kontrolliert und zentralisiert betrieben werden kann. Der Zugriff wird dann vermietet, aber die Kontrolle bleibt beim Eigentümer. Daran ändern auch die freien und offenen KI/ML-Programmbibliotheken von Google und Co. oder kleine LLMs zum Selbstbetreiben[48] nichts, weil stets die restlichen Zutaten zur eigenen Erstellung fehlen.

Arbeitsplatzverlust – Abschließend soll noch kurz das Narrativ angerissen werden, dem zufolge KI ein „Jobkiller" sei. Obwohl diese grundlegende Debatte so alt ist wie die Automatisierung selbst, wird sie auch im KI-Kontext verkürzt geführt – bereits die Ludditen oder andere Maschinenstürmer waren ja keineswegs technikfeindlich. Zugespitzt besagt das Narrativ, dass durch den Einsatz von KI massenweise Arbeitsplätze verschwinden würden, manche Studien sprechen gar von knapp der Hälfte aller Jobs in den USA[49], sodass auf absehbare Zeit eine Massenarbeitslosigkeit drohe. Dieses Narrativ hat mindestens drei fragwürdige Aspekte: Erstens ist es ja zunächst begrüßenswert, wenn Maschinen und KI-Systeme Menschen die Arbeit abnehmen, besonders wenn diese repetitiv, beschwerlich oder gar gefährlich ist.[50] Die Frage ist also, welche Jobs wegfallen, wer die Betroffenengruppen sind und welche Rolle Lohnarbeit überhaupt gesellschaftlich künftig spielen soll. Zweitens zeigen Studien, dass Arbeitsplätze so gut wie nie plötzlich wegfallen, sondern sich eher langsam verändern. Statt technologiebedingter Massenarbeitslosigkeit sehen wir einen Strukturwandel des Arbeitsmarktes.[51] Dabei besteht die Veränderung darin, dass sich moderat und zunehmend auch gut bezahlte Arbeitsplätze in eine überschaubare Anzahl lukrativer Stellen („high skilled labour") wandeln, während der Großteil schlechter bezahlten oder gar prekären Beschäftigungsformen („low skilled labour") weicht.[52] An der Arbeitslosenquote ändert das wenig, politischer Handlungsbedarf besteht dennoch. Drittens verschleiert das Narrativ wie so oft die tatsächlichen Zusammenhänge und verantwortlichen Akteure. Schließlich nimmt künstliche Intelligenz den Menschen die Arbeit nicht einfach weg und Arbeitsplätze verschwinden auch nicht von Zauberhand. Es sind Entscheider:innen in Konzernen, die

beschließen, dass es wohl profitabler wäre, Stellen abzubauen, Arbeitsprozesse zu automatisieren und/oder die Produktion zu verlagern. Diese Entwicklung hängt primär von rechtlichen und wirtschaftlichen Rahmenbedingungen ab, von unternehmerischen Strategien und nicht zuletzt politischen Entscheidungen bezüglich der Rolle von KI in der gesamtgesellschaftlichen Transformation.[53] Solange die Entwicklung künstlicher Intelligenz als Naturgewalt betrachtet und von Angstszenarien wie einer drohenden Massenarbeitslosigkeit begleitet wird, profitieren von ihr vor allem Unternehmen, die KI-Produkte herstellen oder vertreiben und darüber hinaus Konzerne, denen angstinduzierte Niedriglöhne zupass kommen. Für gesellschaftliches Gestaltungspotenzial bleibt dann kaum Raum.

Fazit und Ausblick

Bei der Analyse dieser KI-Narrative fällt auf, dass sie meist gar nicht auf den technischen Eigenschaften dieser Systeme fußen, oft Fehlannahmen über ihre Einsatzdynamik enthalten und somit nicht zu einer fruchtbaren und produktiven Debatte beitragen, sondern ihr teilweise sogar entgegenstehen. Dass sie in aktuellen Diskursen trotzdem prominent vorkommen, mag daran liegen, dass die Technologie missverstanden wird, gesellschaftliche Kontexte und Dynamiken ausgeblendet werden oder auch daran, dass solche Erzählungen oft einem kommerziellen Zweck dienen und entsprechend verbreitet werden.

KI wird gemäß den Zwecken gestaltet und verwendet, die Unternehmen, Regierungen und andere Organisationen für sie vorsehen, wenn auch manchmal mit nicht intendierten Effekten. Oberflächliche Zeitgeist-KI-Debatten oder dramatisch zugespitzte Gegenüberstellungen à la „Mensch gegen Maschine" sind jedoch fehl am Platze, verschleiern relevante Machtfragen[54] und gehören in den Bereich der Science-Fiction.

Gleichwohl müssen die Komplexität und Beherrschbarkeit dieser Systeme im Auge behalten werden. Dafür gibt es längst methodische Ansätze und regulatorische Maßnahmen, die getroffen werden könnten, wenn denn der politische Wille dafür vorhanden wäre. Dass nicht entsprechend gehandelt wird, hängt nicht zuletzt mit neoliberalen Gesellschaftsbildern, kokettierenden „Neuland"-Haltungen, wirkmächtigem Lobbyismus, Innovation um ihrer selbst willen oder auch mit naiver Technikgläubigkeit zusammen. In dieser Gemengelage sind Fragen ethischer und vertrauenswürdiger KI zwar technisch und philosophisch interessant, hängen aber weit hinter dem Stand der Diskussion in den technikregulatorischen Sozialwissenschaften[56] und der Datenschutztheorie zurück.[57] Denn die Fragen, die sich stellen, wenn Organisationen KI-Systeme einsetzen, sind zwar neu, aber nicht fundamental anders als die, die sich stellen, wenn Organisationen für ihre Zwecke Beton, Differentialgleichungen oder Spürhunde einsetzen. Ein hohes Maß an Entpolitisierung sowie eine Selbststilisierung sind jedoch wesentliche Aspekte der Selbsterzählung von KI – und auch von Digitalisierung allgemein.

Der Einsatz von KI-Technologien verändert tatsächlich unsere Gesellschaften, aber nicht so, wie oft – wahlweise utopistisch[58] oder dystopisch – argumentiert wird. Die Rettung der Menschheit durch eine leistungsstarke, mithin gute KI steht ebenso wenig zu erwarten wie die drohende Auslöschung der Menschheit durch eine unkontrollierbare, mithin böse Superintelligenz.[59] Tatsächliche Folgen und Gefahren dieser Technologien, die Gegenstand gesellschaftlicher Debatten sein müssen, sind etwa die Strukturveränderung des Arbeitsmarktes, die Ausweitung ausbeuterischer Lieferketten bei der Datenerhebung und -auswertung, insbesondere im globalen Süden[60], die einseitige Macht- und Produktivitätssteigerung weniger Firmen, die Ausweitung personalisierter Überwachung, die unendliche Welle von KI-generiertem Spam und Betrug[61], die automatisierte Aneignung und Kommerzialisierung von Online-Kulturwerken, die Herausbildung globaler Abhängigkeiten durch Oligopoltendenzen in der Industrie, die Implikationen militärischer KI-Nutzung[62], der exponentiell ansteigende Energieverbrauch durch KI-Systeme und nicht zuletzt der unreflektierte und nur scheinbar unpolitische Einsatz solcher Systeme im Wohlfahrtsstaat und in weiteren sensiblen Gesellschaftsbereichen (Kreditvergabe, Bewerbungsprozesse, Strafverfahren etc.).[63] Eine weitere drängende politische Frage betrifft die kollektive Gestaltung der geistigen Arbeit im Kontext der Maschinisierung unter den aktuell gegebenen Macht- und Besitzverhältnissen. Technikgestaltung ist immer auch die Gestaltung von (technisch geprägten) sozialen Praktiken, aber gleichzeitig ist sie selbst das Ergebnis sozialer Praktiken – und künstliche Intelligenz ist seit jeher ein diskursiv umkämpftes Terrain.

Doch die Zukunft ist offen und all diese Fragen sind zu diskutieren, sodass wir als Gesellschaft diesen interessanten und mächtigen Werkzeugkasten kreativ und reflektiert nutzen können. Auch wenn schon viele theoretische und praktische Vorarbeiten existieren, sind die Einsatzmöglichkeiten von KI und anderen digitalen Technologien jenseits von Profit und Markt noch nicht einmal ansatzweise erdacht und entwickelt worden – von kritischer Informatik[64] und anarchistischer Softwaregestaltung[65] über das digitale Commoning[66] und herrschaftsfreie Informationssysteme[67] bis hin zur Unterstützung der Nachhaltigkeitstransformation[68] und der Rückeroberung der Computationsmittel.[69] Wenn wir die gesellschaftliche Gestaltbarkeit künstlicher Intelligenz und ihre vielfältigen Anwendungsmöglichkeiten im Blick behalten wollen, müssen wir nicht nur die beizeiten wiederkehrenden ELIZA-Momente durchschauen, sondern auch überlegen, inwiefern der Fokus auf riesenhaft-überkomplexe KI-Systeme dabei überhaupt hilfreich ist, oder ob er nicht eher ablenkt von den eigentlichen Zutaten für ein gutes Leben für alle.

Förderhinweis: Diese Arbeit wurde durch das Bundesministerium für Bildung und Forschung (BMBF) gefördert (Förderkennzeichen: 16DII131 – „Deutsches Internet-Institut").

Der Beitrag erschien zunächst bei Soziopolis als Rehak, R. (2023). Zwischen Macht und Mythos: Eine kritische Einordnung aktueller KI-Narrative. Soziopolis: Gesellschaft beobachten.
https://nbn-resolving.org/urn:nbn:de:0168-ssoar-91379-4

Anmerkungen

1 *John McCarthy u. a., A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, Stanford University, https://wwwformal.stanford.edu/jmc/history/dartmouth/dartmouth.html (06.11.2023).*

2 Alan Turing, Computing Machinery and Intelligence, in: Mind 59 (1950), 236, S. 433–460 (https://doi.org/10.1093/mind/LIX.236.433).
3 McCarthy u. a., Proposal on Artificial Intelligence.
4 Wolfgang Coy / Lena Bonsiepen, Erfahrung und Berechnung. Kritik der Expertensystemtechnik, Berlin / Heidelberg 1989.
5 Vgl. etwa Martin Popel u. a., Transforming machine translation: a deep learning system reaches news translation quality comparable to human professionals, in: Nature Communications 11 (2020), doi.org/10.1038/s41467-020-18073-9.
6 Joseph Weizenbaum, ELIZA – A Computer Program for the Study of Natural Language Communication Between Man And Machine, in: Communications of the ACM 9 (1966), 1, S. 36–45.
7 Joseph Weizenbaum, Die Macht der Computer und die Ohnmacht der Vernunft 1978, übers. von Udo Rennert, Frankfurt am Main 2000; vgl. aktuell Emily M. Bender u. a., On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?, in: Association for Computing Machinery (Hg.), FAccT ‚21: Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency, New York 2021, S. 610–623.
8 Hubert L. Dreyfus, What Computers Can't Do. A Critique of Artificial Reason, New York 1972.
9 Vgl. etwa Carl Benedikt Frey / Michael A. Osborne, The Future of Employment: How Susceptible Are Jobs to Computerisation?, Oxford Martin School, https://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf (6.11.23); oder Joseph Briggs / Devesh Kodnani, The Potentially Large Effects of Artificial Intelligence on Economic Growth, Goldman Sachs Publishing, https://www.gspublishing.com/content/research/en/reports/2023/03/27/d64e052b-0f6e-45 d7-967b-d7be35fabd16.html (6.11.23).
10 Vgl. Ray Kurzweil, The Singularity is Near: When Humans Transcend Biology, New York 2005.
11 Vgl. Elon Musk u. a., Pause Giant AI Experiments: An Open Letter, Future of Life Institute, https://futureoflife.org/open-letter/pause-giant-ai-experiments/ (6.11.23); oder Geoffrey Hinton u. a., Mitigating the risk of extinction from AI should be a global priority alongside other societal-scale risks such as pandemics and nuclear war, Center for AI Safety, https://www.safe.ai/statement-on-ai-risk (6.11.23).
12 Vgl. Tom Mitchell, Machine Learning, New York 1997.
13 Rainer Rehak, The Language Labyrinth: Constructive Critique on the Terminology Used in the AI Discourse, in: Pieter Verdegem (Hg.), AI for Everyone? Critical Perspectives, S. 87–102, London 2021.
14 Vgl. Turing, Computing Machinery and Intelligence; siehe auch Martin Holland, Hat Chatbot LaMDA ein Bewusstsein entwickelt? Google beurlaubt Angestellten, in: heise online, 13.6.23, https://www.heise.de/news/Hat-Chatbot-LaMDA-ein-Bewussteinentwickelt-Google-beurlaubt-Angestellten-7138314.html (6.11.23).
15 Vgl. Kurzweil, The Singularity is Near; Musk u. a., Pause Giant AI Experiments.
16 Mariana Lenharo, Consciousness theory slammed as 'pseudoscience' — sparking uproar, in: Nature, 20.09.23, https://www.nature.com/articles/d41586-023-02971-1 (6.11.23).
17 Dreyfus, What Computers Can't Do; Ragnar Fjelland, Why general artificial intelligence will not be realized, in: Humanities and Social Sciences Communications 7 (2020), 10, https://www.nature.com/articles/s41599-020-0494-4; Andrea Roli / Johannes Jaeger / Stuart A. Kauffman, How Organisms Come to Know the World: Fundamental Limits on Artificial General Intelligence, in: Frontiers in Ecology and Evolution 9 (2021), https://doi.org/10.3389/fevo.2021.806283; Rainer Rehak, The Language Labyrinth.
18 O.A., X.AI: Elon Musk gründet KI-Unternehmen trotz Brief mit Moratorium, in: Frankfurter Allgemeine Zeitung, 16.4.23, https://www.faz.net/aktuell/wirtschaft/unternehmen/x-ai-elon-musk-gruendet-kiunternehmen-trotz-brief-mit-moratorium-18825457.html.
19 Isabella Hermann, Künstliche Intelligenz in der Science-Fiction: Mehr Magie als Technik, in: Helen Ahner / Max Metzger / Mathis Nolte (Hg.), Von Menschen und Maschinen: Interdisziplinäre Perspektiven auf das Verhältnis von Gesellschaft und Technik in Vergangenheit, Gegenwart und Zukunft. Proceedings der 3. Tagung des Nachwuchsnetzwerks „INSIST", 05.-07. Oktober 2018, https://www.ssoar.info/ssoar/handle/document/67663.
20 Rainer Rehak, Artificial Intelligence for Real Sustainability?, in: Patricia Jankowski u. a. (Hg.), Shaping Digital Transformation for a Sustainable Society. Contributions from Bits & Bäume, Technische Universität Berlin, https://doi.org/10.14279/depositonce-17526 (6.11.23).
21 Deutscher Bundestag, Bericht zum Stand von KI in der öffentlichen Verwaltung, Bildung, Forschung und Technikfolgenabschätzung — Bericht — hib 520/2022, https://www.bundestag.de/presse/hib/kurzmeldungen-914308 (6.11.23).
22 Im Hinblick auf die Wissenschaft vgl. stellvertretend Daniel Innerarity, The epistemic impossibility of an artificial intelligence take-over of democracy, AI & Society, https://doi.org/10.1007/s00146-023-01632-1 (6.11.23); für die Wirtschaft vgl. James Vincent, Forty percent of 'AI startups' in Europe don't actually use AI, claims report, in: The Verge, 5.3.2019, https://www.theverge.com/2019/3/5/18251326/ai-startups-europefake-40-percent-mmc-report (6.11.23).
23 Ein positives Beispiel liefert dazu der japanische Rat für soziale Grundsätze einer humanzentrierten künstlichen Intelligenz, vgl. Council for

Rainer Rehak

Rainer Rehak ist wissenschaftlicher Mitarbeiter in den Forschungsgruppen *Digitalisierung, Nachhaltigkeit und Teilhabe* und *Technik, Macht und Herrschaft* am Weizenbaum-Institut für die vernetzte Gesellschaft sowie assoziierter Mitarbeiter am Wissenschaftszentrum Berlin für Sozialforschung (WZB). Er promoviert aktuell an der TU Berlin zu systemischer IT-Sicherheit und gesellschaftlichem Datenschutz. Seine Forschungsfelder sind Datenschutz, IT-Sicherheit, staatliches Hacking, Informatik und Ethik, Technikfiktionen, Digitalisierung und Nachhaltigkeit, konviviale und demokratische Digitaltechnik sowie die Implikationen und Grenzen von Automatisierung durch KI-Systeme. Er studierte Informatik und Philosophie in Berlin und Hong Kong und beschäftigt sich seit über 15 Jahren mit den Implikationen der Computerisierung der Gesellschaft. Er ist Sachverständiger für Parlamente (z. B. den Deutschen Bundestag) und Gerichte (z. B. das Bundesverfassungsgericht) und publiziert zudem regelmäßig auch in nichtwissenschaftlichen Medien.

Social Principles of Human-Centric AI, Social Principles of Human-Centric AI, https://www.cas.go.jp/jp/seisaku/jinkouchinou/pdf/humancentricai.pdf (6.11.23).

24 Vgl. etwa Emma Farge, Robots say they won't steal jobs, rebel against humans, in: Reuters, 7.7.2023, https://www.reuters.com/technology/robots-say-they-wont-steal-jobs-rebel-againsthumans-2023-07-07/.

25 Vgl. Florian Butollo u. a. (Hg.), Lecture Series „Autonomous Systems & Self-Determination", Weizenbaum Institute for the Networked Society, https://doi.org/10.34669/wi/2 (6.11.23).

26 Stephen Wolfram, What Is ChatGPT Doing … and Why Does It Work?, Stephen Wolfram Writings, https://writings.stephenwolfram.com/2023/02/what-is-chatgpt-doing-and-whydoes-it-work/ (6.11.23).

27 Florian Butollo u. a. (Hg.), Lecture Series „Autonomous Systems & Self-Determination".

28 Christiane Floyd, From Joseph Weizenbaum to ChatGPT: Critical Encounters with Dazzling AI Technology, in: Weizenbaum Journal of the Digital Society 3 (2023), 3, https://doi.org/10.34669/WI.WJDS/3.3.3 (6.11.23).

29 Stephen Wolfram, What Is ChatGPT Doing.

30 Emily Bender u. a., On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?, in: Association for Computing Machinery (Hg.), FAccT ,21: Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency, New York 2021, S. 610–623.

31 Das zeigt sich etwa an den allgemeinen Antworten eines Chatbots, die für bestimmte Zwecke unpassend bis regelrecht schädlich sind: Lauren Aratani, US eating disorder helpline takes down AI chatbot over harmful advice, The Guardian, 31.7.2023, https://www.theguardian.com/technology/2023/may/31/eating-disorder-hotline-union-aichatbot-harm.

32 Paola Lopez, ChatGPT und der Unterschied zwischen Form und Inhalt, in: Merkur 77 (2023), 891, S. 15–27, https://www.merkur-zeitschrift.de/artikel/chatgpt-und-derunterschied-zwischen-form-und-inhalt-amr-77-8-15/ (6.11.23).

33 Bender u. a., On the Dangers of Stochastic Parrots.

34 Florian Eyert / Paola Lopez, Rethinking Transparency as a Communicative Constellation, in: FAccT '23: Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency, New York 2023, S. 444–454.

35 Aaron Sankin / Surya Mattu, Predictive Policing Software Terrible at Predicting Crimes, in: Wired, 2.10.2023, https://www.wired.com/story/plainfield-geolitica-crime-predictions (6.11.23); und Will Douglas Heaven, Predictive policing algorithms are racist. They need to be dismantled, in: MIT Technology Review, 17.7.2020, https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/ (6.11.2023).

36 Rob Kitchin, The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences, Thousand Oaks, CA 2014.

37 Eyert / Lopez, Rethinking Transparency.

38 Sayash Kapoor / Arvind Narayanan, Quantifying ChatGPT's gender bias, in: AI Snake Oil, 26.4.2023, https://aisnakeoil.substack.com/p/quantifying-chatgpts-gender-bias (6.11.23).

39 Vgl. etwa Michael Chui u. a., Applying Artificial Intelligence for Social Good, McKinsey & Company, https://www.mckinsey.com/featured-insights/artificial-intelligence/applyingartificial-intelligence-for-social-good (6.11.23).

40 Vgl. etwa o.A., Das Potenzial von KI für den Klimaschutz, in: UmweltDialog, 28.12.2020, https://www.umweltdialog.de/de/umwelt/klimawandel/2020/Das-Potenzial-von-KI-fuerden-Klimaschutz.php (6.11.23).

41 Eileen Guo / Adi Renaldi, Worldcoin: Tausche Kryptowährung gegen Augen-Scan, in: MIT Technology Review, 3.7.2023, https://www.heise.de/hintergrund/Worldcoin-Tausche-Kryptowaehrung-gegen-Augen-Scan-7097714.html (6.11.23).

42 Richard Evans / Jim Gao, DeepMind AI Reduces Google Data Centre Cooling Bill by 40%, in: Google DeepMind, 20.7.2016, https://www.deepmind.com/blog/deepmind-ai-reducesgoogle-data-centre-cooling-bill-by-40 (6.11.23).

43 Vgl. Stefan Betschon, Die Demokratisierung der künstlichen Intelligenz, in: Neue Zürcher Zeitung, 15.12.2016, https://www.nzz.ch/digital/aktuelle-themen/machine-learning-die-demokratisierung-derkuenstlichen-intelligenz-ld.135034 (6.11.23).

44 Vgl. Lisa Mayerhofer, „Künstliche Intelligenz wird demokratisiert", in: Werben & Verkaufen, 31.1.2020, https://www.wuv.de/Archiv/%22K%C3%BCnstliche-Intelligenz-wird-demokratisiert%22 (6.11.23).

45 Rainer Mühlhoff, Human-Aided Artificial Intelligence: Or, How to Run Large Computations in Human Brains? Towards a Media Sociology of Machine Learning, in: New Media & Society 10 (2019), 10, S. 1868–1884.

46 Kate Crawford, Atlas of AI. Power, Politics, and the Planetary Costs of Artificial Intelligence, New Haven, CT 2021.

47 Rehak, Artificial Intelligence for Real Sustainability?

48 Craig G. Smith, The Long and Mostly Short of China's Newest GPT, in: IEEE Spectrum, 28.7.2023, https://spectrum.ieee.org/china-chatgpt-wu-dao (6.11.23).

49 Frey / Osborne, The Future of Employment.

50 Constanze Kurz / Frank Rieger, Arbeitsfrei: Eine Entdeckungsreise zu den Maschinen, die uns ersetzen, München 2013.

51 Florian Butollo, Automatisierungsdividende und gesellschaftliche Teilhabe, in: regierungsforschung.de, 24.5.2018, https://regierungsforschung.de/automatisierungsdividende-und-gesellschaftlicheteilhabe/ (6.11.23).

52 Ebd.

53 Wissenschaftlicher Beirat der Bundesregierung Globale Umweltveränderungen (Hg.), Unsere gemeinsame digitale Zukunft, Berlin 2019, http://www.wbgu.de/hg2019 (6.11.23).

54 Jeanette Hofmann, Demokratie und Künstliche Intelligenz, Digitales Deutschland, https://digid.jff.de/demokratie-und-ki/ (6.11.23).

55 Martin Rost, Künstliche Intelligenz. Normative und operative Anforderungen des Datenschutzes, in: DuD – Datenschutz und Datensicherheit – DuD 42 (2018), 9, S. 558–565, https://www.maroki.de/pub/privacy/2018-09_DuD-KI.pdf (6.11.23).

56 Vgl. etwa Florian Eyert / Florian Irgmaier / Lena Ulbricht, Extending the framework of algorithmic regulation. The Uber case, in: Regulation & Governance 16 (2022), 1, S. 23–44, https://doi.org/10.1111/rego.12371 (6.11.23).

57 Rost, Künstliche Intelligenz.

58 Vgl. etwa Marc Andreessen, Why AI Will Save the World, in: Andreessen Horowitz, 6.6.2023, https://a16z.com/ai-will-save-the-world/ (6.11.2023).

59 Vgl. Musk u. a., Pause Giant AI Experiments; oder Hinton u. a., Mitigating the risk of extinction.

60 Mühlhoff, Human-Aided Artificial Intelligence.

61 Amy Castor / David Gerard, Pivot to AI: Pay no attention to the man behind the curtain, in: Amy Castor, 12.9.2023, https://amycastor.com/2023/09/12/pivot-to-ai-pay-no-attentionto-the-man-behind-the-curtain/ (6.11.2023).

62 Vgl. allgemein Hans-Jörg Kreowski / Aaron Lye, Künstliche Intelligenz im Dienst des Militärs, FIfF-Kommunikation 4/23, S. 19–23; und konkret: Yuval Abraham, 'A mass assassination factory': Inside Israel's calculated bombing of Gaza, in: +972 Magazine, 30.11.2023, https://www.972mag.com/mass-assassination-factory-israel-calculatedbombing-gaza/.

63 Rainer Mühlhoff, „Automatisierte Ungleichheit: Ethik der Künstlichen Intelligenz in der biopolitische Wende des Digitalen Kapitalismus", in: Deutsche Zeitschrift für Philosophie 68 (2020), 6, S. 867–890, https://doi.org/10.1515/dzph-2020-0059.

64 *Wolfgang Coy, Für eine Theorie der Informatik!, in: ders. u. a. (Hg.), Sichtweisen der Informatik, Braunschweig/Wiesbaden 1992.*

65 *Ralf Klischewski, Anarchie – Ein Leitbild für die Informatik: Von den Grundlagen der Beherrschbarkeit zur selbstbestimmten Systementwicklung, Bern 1996.*

66 *Silke Helfrich (Hg.), Wem gehört das Wissen der Welt? Zur Wiederentdeckung der Gemeingüter, München 2009.*

67 *Christian Ricardo Kühne, Zu Bedingungen und Möglichkeiten der Gestaltung herrschaftsfreier Informationssysteme, in: Rainer Fischbach / Klaus Lenk / Jörg Pohle (Hg.), Der Weg in die »Digitalisierung« der Gesellschaft, 2. Auflage. Marburg (im Erscheinen); Christian Ricardo Kühne, GNUnet und Informationsmacht: Analyse einer P2P-Technologie und ihrer sozialen Wirkung, Humboldt-Universität zu Berlin, https://doi.org/10.18452/14270 (6.11.23).*

68 *Tilman Santarius / Josephin Wagner, Digitalization and sustainability: A systematic literature analysis of ICT for Sustainability research, in: GAIA – Ecological Perspectives for Science and Society, 23 (2023), S1.*

69 *Cory Doctorow, Seizing the means of computation – how popular movements can topple Big Tech monopolies, Transnational Institute, https://www.tni.org/en/article/seizing-themeans-of-computation (6.11.23).*

Dieter Engels, Jürgen Scheffran, Ekkehard Sieker

Krieg im Weltraum – Ist es wieder 5 vor 12?

Anläßlich des Jubiläumssymposiums 40 Jahre Wissenschaft für den Frieden *am 6./7.10.2023 in Bonn haben die Autoren einen Vortrag zur aktuellen Militarisierung des Weltraums gehalten. Das Thema ist vor vier Jahrzehnten erstmalig in einer breiteren Öffentlichkeit diskutiert worden und hat seine Brisanz nicht verloren. Die Sorge um eine weitere Eskalation des Rüstungswettlaufs hat 1983 zum* Mainzer Appell *und 1988 maßgeblich zur Gründung der Naturwissenschaftler:innen-Initiative* Verantwortung für Frieden und Zukunftsfähigkeit *geführt.*

Am 20. Juli 1969 betrat der US-amerikanische Astronaut Neil Armstrong als erster Mensch einen außerirdischen Himmelskörper, den Mond. Weltweit regte die Übertragung dieses Ereignisses vor allem junge Menschen zu Träumen an, in denen sie selbst Teil der Erforschung des Weltraums, beginnend mit der Erkundung des Mondes und der Nachbarplaneten, sein würden. Bei einer vorherigen Mission des Apollo-Mondlandeprogramms war erstmals die aufgehende Erde aus der Mondumlaufbahn in Farbe fotografiert worden, und die Aufnahme mit dem blauen Planeten wurde im Laufe der Zeit zum Symbol für die Kostbarkeit der Erde (Abbildung 1). Weitgehend ausgeblendet blieb in der überschwenglichen Berichterstattung, dass die Raumfahrt ein Kind des Kalten Krieges war und sich ohne militärischen Hintergrund kaum soweit entwickelt hätte. Die für das Apollo-Programm verwendete Saturn-Rakete wurde unter der Leitung des Raketenpioniers Wernher von Braun entwickelt, der am Ende des 2. Weltkrieges die ersten Raketen für das Dritte Reich gebaut hatte. Die *Vergeltungswaffe 2* (V2) terrorisierte monatelang die Zivilbevölkerung in Städten wie Antwerpen oder London. Der erste 1957 von der Sowjetunion gestartete Satellit *Sputnik* wurde in den USA sogleich als Bedrohung angesehen, weil mit der eingesetzten Trägerrakete im Prinzip auch US-amerikanischer Boden mit Atombomben erreicht werden konnte. Die Mondlandung war der Höhepunkt eines Prestigeduells, mit dem die USA ihre technologische Überlegenheit gegenüber der Sowjetunion, der anderen Supermacht, demonstriert sehen wollten. Dass über 50 Jahre nach Beendigung des Apollo-Programms kein weiterer Mensch den Mond betreten hat, unterstreicht den geostrategischen Hintergrund dieses Programms, welches nur vordergründig etwas mit Weltraum-Forschung zu tun hatte.

Abbildung 1: Aufnahme der Erde vom 24.12.1968 aufgenommen von der Mondmission Apollo 8*. Quelle: William Anders/NASA*

Strategic Defense Initiative – Waffen im Weltraum?

Die Nutzung des Weltraums *(s. Infokasten Weltraum)* für militärische Zwecke wurde einer breiteren Öffentlichkeit erst mit der *Strategic Defense Initiative* (SDI) des US-Präsidenten Ronald Reagan bewusst. Reagan hatte in einer Fernsehansprache am 23. März 1983 das Programm aus der Taufe gehoben und verkündet, dass die USA einen Raketenabwehrschirm bauen würden, der die US-amerikanische Bevölkerung vor einem Atomwaffenangriff schützen könnte [1]. Die Ankündigung wurde unterschiedlich aufgenommen. Während die konservativen Kreise in den USA und die westliche (Rüstungs-)Industrie das Programm begrüßten, wurde es vor allem in Kreisen der Naturwissenschaftler als undurchführbar angesehen, weil ein hundertprozentiger Schutz niemals zu erreichen sein würde. Von der Sowjetunion wurde das Programm als Aggression wahrgenommen. Sie befürchtete, dass ein funktionierender Abwehrschirm ihnen die Möglichkeit zur Vergeltung nehmen würde, falls die USA mit einem atomaren Erstschlag das sowjetische Raketenarsenal dezimieren würden. Die Friedensbewegung weltweit lehnte das Programm wegen des sich abzeichnenden verstärkten Wettrüstens ebenfalls ab und forderte stattdessen Abrüstung *(s. Infokasten NaturwissenschaftlerInnen-Initiative)*

Der geplante Abwehrschirm würde auf jeden Fall einen Waffeneinsatz im Weltraum erfordern, weil die 20-minütige Flugphase der Sprengköpfe zwischen der Sowjetunion und den USA zum großen Teil außerhalb der Erdatmosphäre stattfindet. 1967 war zwar der Weltraumvertrag abgeschlossen worden, den auch die damaligen Supermächte ratifiziert hatten, doch schließt dieser

nur die Stationierung und den Einsatz von Massenvernichtungswaffen im Weltraum aus. Wir haben 1984 das Buch *Die Front im All* [2] geschrieben, welches in der deutschen Friedensbewegung viel gelesen wurde. Neben der Beschreibung des SDI-Programms und der technischen Probleme, die einen vollständigen Schutz vor einem Raketenangriff unmöglich machen, haben wir schon damals auf eine Vielzahl von satellitengestützten Programmen aufmerksam gemacht, die eine zunehmende Bedeutung für die Kriegsführung auf der Erde bekamen [3].

Militärsatelliten und Antisatelliten-Waffen

In unserem modernen Alltag sind satellitengestützte Dienste nicht mehr wegzudenken. Ob es die Standortbestimmung und Navigation, die täglichen Wetterkarten, Übertragungen von Sportereignissen, Überwachung von Klimaindikatoren oder einfach Bilder der Erde sind, alle diese Produkte und Dienste verwenden Daten, die von Satelliten geliefert werden. Die Nutzung dieser Dienste, welche auch zur Aufklärung, Kommunikation, Steuerung der Waffensysteme oder Einsatzplanung verwendet werden, war in den 1980er-Jahren noch weitgehend eine Domäne des Militärs. Eine bedeutende Rolle spielten sie im Golf-Krieg 1990/91, der wegen des umfassenden Einsatzes von Aufklärungs-, Kommunikations- und Navigationssatelliten auch als erster Weltraumkrieg bezeichnet wird [4]. Ein weiterer Meilenstein war der Kosovo-Krieg 1998/99, bei dem die von der NATO angeführten europäischen Streitkräfte in Sachen Weltraumdienste vollkommen abhängig von den USA waren [5]. In der Folge wurden in Europa und insbesondere in Deutschland eigene Radar-Aufklärungs- (SAR-Lupe seit 2006, Sarah seit 2022) und Kommunikationssatelliten (COMSATBw seit 2009) in Betrieb genommen. Die Radar-Aufklärungsergebnisse werden mit Frankreich geteilt, das dafür im Austausch Bilder eigener optischer Aufklärungs-Satelliten zur Verfügung stellt. Ein von GPS unabhängiges Navigations-Satelliten-System (Galileo, Aufbau seit 2011) wurde im Rahmen der Europäischen Union realisiert. Ein europäisches Kommunikationssatelliten-System IRIS^2 mit Anwendungen im militärischen Bereich befindet sich in Planung [6].

Weltraum

Die Grenze zwischen der Erdatmosphäre und dem Weltraum liegt bei 80 bis 100 km oberhalb der Erdoberfläche. Satelliten müssen auf Bahnen deutlich über dieser Grenze umlaufen, damit sie nicht durch die Restatmosphäre zu schnell abgebremst werden und zur Erde zurückstürzen. Die meisten Satelliten und die Raumstationen umkreisen die Erde in Umlaufbahnen bis ca. 2.000 km Höhe (LEO = Low Earth Orbit) und verändern dabei ständig ihre Position über dem Erdboden.

Dagegen befinden sich Satelliten, die auf einer Bahnhöhe von 36.000 km (GEO = Geostationary Orbit) über dem Erdäquator kreisen, ständig oberhalb eines bestimmten Ortes auf der Erde. Diese relativ weit entfernte Bahn wird gerne von Kommunikations-Satelliten benutzt, da mit drei von im Winkelabstand von 120 Grad angeordneten Satelliten ein weltumspannendes Netz aufgebaut werden kann. Die Bahnhöhen dazwischen (MEO = Medium Earth Orbit) werden weniger genutzt.

Die kommerzielle und militärische Nutzung des Weltraums beschränkt sich bisher auf den „erdnahen Raum" innerhalb der GEO-Bahn. Bereits abzusehen ist eine Ausweitung auf den sogenannten cislunaren Raum, also dem Raum zwischen Erde und Mond bis in eine Entfernung von 384.000 km. In den interplanetaren Raum – bis ca. 4.5 Millionen km – sind bisher nur unbemannte Sonden zur Forschung und Erkundung vorgedrungen.

NaturwissenschaftlerInnen-Initiative

Die NaturwissenschaftlerInnen-Initiative (NatWiss) Verantwortung für Frieden und Zukunftsfähigkeit *ist ein gemeinnütziger Verein, der im Februar 1988 gegründet wurde. NatWiss engagiert sich mit naturwissenschaftlicher Kompetenz für eine Welt ohne Krieg und Gewalt, für die Kontrolle und Beseitigung atomarer, chemischer, biologischer und konventioneller Waffensysteme, für Friedens- und Abrüstungsforschung und für soziale, ökologische und humane Technikgestaltung. NatWiss geht zurück auf die Friedensbewegung gegen die Nachrüstung der frühen 1980er-Jahre, die ihren Widerhall im Forum Naturwissenschaftler für Frieden und Abrüstung und im Wissenschaftler-Appell der* Mainzer 23 *fand. Beim Kongress* Naturwissenschaftler gegen Atomrüstung *kamen im Juli 1983 in Mainz 3.000 Teilnehmende aus vielen Bereichen der Wissenschaft zusammen. Auf dem Göttinger Kongress* Naturwissenschaftler warnen vor der Militarisierung des Weltraums *im Juli 1984 wurde ein Vertragsentwurf zum Verbot von Weltraumwaffen vorgelegt sowie ein internationaler Wissenschaftler-Appell, der ein Moratorium für solche Waffen forderte (Abbildung 2). 1986 suchten tausende von Wissenschaftler:innen und Studierenden aus zahlreichen Ländern beim Hamburger Kongress nach* Wegen aus dem Wettrüsten. *Viele verweigerten sich dem Aufruf von US-Präsident Ronald Reagan, in der Strategic Defense Initiative (SDI) ein weltraumgestütztes Abwehrsystem gegen Atomraketen zu entwickeln. An vielen Hochschulen fanden Lehrveranstaltungen zu Wissenschaft und Rüstung statt. Nach dem Kalten Krieg thematisierte NatWiss die vielfältigen Gefahren von Aufrüstung für Frieden und Nachhaltigkeit und mögliche Lösungen für globale Verantwortung und Zukunftsfähigkeit durch Abrüstung, die Abschaffung der Atomwaffen und ein Verbot von Weltraumwaffen. Bei einem Kongress in Berlin 1991 wurde das* International Network of Engineers and Scientists for Global Responsibility *(INES) gegründet, das sich in der Tradition von Albert Einstein, Joseph Rotblat, Dorothy Hodgkin und Hans-Peter Dürr sieht.*

Abbildung 2: Weltraum ohne Waffen

In den letzten 40 Jahren haben sich die Fähigkeiten der Satelliten-Technologien erheblich vergrößert. Vor allem die USA treiben diesen Prozess voran, da sie ihre Überlegenheit in den Kommunikations-Technologien dazu nutzen, um in einem Konflikt schneller und umfassender mit den Truppen kommunizieren zu können als der jeweilige Gegner. Waren die Satelliten in der Vergangenheit in der Regel für strategische Aufgaben (Aufklärung, Frühwarnung vor Raketenangriffen, Planung) von Bedeutung, werden sie heute zunehmend auch für taktische Zwecke (z. B. Waffensteuerung im Einsatzgebiet, Echtzeitübertragung der Gefechtslage) eingesetzt. Diese starke Abhängigkeit der irdischen Kriegführung von Weltraumdaten führt im Gegenzug zu Aktivitäten, die Funktionstüchtigkeit der gegnerischen Satelliten auszuschalten, sprich Antisatelliten-Waffen (ASAT) zu entwickeln. Solche Waffen basierten bisher häufig auf kinetischer oder Druck entfaltenden Wirkungen, d.h. der Drohung Satelliten mit Raketen oder *Killer-Satelliten* abzuschießen. Zunehmend werden auch Laser benutzt, um die Sensoren eines Satelliten zu blenden. Die Militär-Satelliten auf erdnahen Bahnen sind bisher in relativ kleiner Zahl stationiert, sodass die Funktionstüchtigkeit des Satellitensystems als Ganzes durch die Zerstörung einiger Satelliten nachhaltig beeinträchtigt werden kann. Jüngere ASAT-Tests von China (2007), den USA (2008), Indiens (2017) und Russlands (2019) haben erfolgreiche Abschüsse an eigenen ausgedienten Satelliten vorgeführt [7].

Federführend durch die USA vollzieht sich zur Zeit eine Umwandlung der Satellitensysteme, von Systemen mit wenigen großen und technologisch komplexen Satelliten hin zu Schwärmen von untereinander vernetzten Kleinsatelliten *(s. Infokasten Satellitenunterstützung für das Gefechtsfeld* und Abbildung 3). Eine Blaupause ist das Starlink-Netzwerk des US-Unternehmens SpaceX, welches in einer Höhe von ca. 550 km mit ca. 20.000 Satelliten ein weltumspannendes Kommunikationsnetz aufbaut. Seit 2004 ist bekannt, dass die USA Überwachungs-Satelliten für die geostationäre Bahn betreiben. Seitdem Russland und China ebenfalls solche *Inspektions-Satelliten* entwickelt haben, wird in den USA von einer Bedrohung für die eigenen Satelliten gesprochen, weil im Prinzip auf solchen Satelliten neben Kameras auch Waffen installiert sein können, die diese Satelliten dann zu verkappten ASAT-Systemen machen [8].

Waffenstationierung im Weltraum – erneut aktuell

Bisher haben alle Seiten vermieden, Waffen im Weltraum permanent zu stationieren. Antisatelliten-Tests sind ausschließlich vom Erdboden gestartet worden, aber die Diskussion um die Inspektions-Satelliten, welche in der GEO-Bahn operieren, zeigt, dass es keine technischen Hürden für eine Waffenstationierung im Weltraum gibt. Immer wieder ins Spiel gebracht werden wiederverwendbare Raumgleiter als Waffenträger. Die USA haben mit zwei seit 2010 eingesetzten unbemannten X37-B Raumgleitern, einer kleinen Version des Space Shuttles, bereits Erfahrungen gesammelt. Die Missionen der bisher sechs bis zu 2,5 Jahren dauernden Raumflüge unterliegen der Geheimhaltung, aber Spekulationen gehen davon aus, dass die Flüge hauptsächlich Experimenten und Langzeittests von Materialien dienen [9]. Eine chinesische Version *(Shenlong)* wurde seit 2020 dreimal gestartet, aber da es zu diesem Raumgleiter weder offizielle Mitteilungen noch öffentlich zugängliche aktuelle Bilder gibt (Abbildung 4), ist dessen Einsatzzweck unbekannt. Nicht überraschend wird er von interessierten Kreisen als potentieller Waffenträger angesehen [10].

Satellitenunterstützung für das Gefechtsfeld

Bei der Proliferated Warfighter Space Architecture *(PWSA) der USA handelt es sich um ein im Aufbau befindliches weltumspannendes Satellitensystem, mit dem anfliegende gegnerische Raketen, Hyperschall-Waffen und andere Flugkörper geortet und ihre Bahn verfolgt werden soll. Frei übersetzt handelt es sich um eine* umfassende Weltraum-Infrastruktur für die Unterstützung auf dem Gefechtsfeld. *Zunächst sind 500 Satelliten geplant, die untereinander durch Laser-Kommunikation vernetzt sind (Abbildung 3) und auf erdnahen Bahnen (LEO) umlaufen. Darunter sind 100-*Tracking Satelliten *für die Überwachung und 400* Transport-Satelliten *für die Datenübertragung. Die direkte Kommunikation zwischen Satelliten mit Lasern erlaubt viel höhere Bandbreiten, als bei der klassischen Funkübertragung mit Hilfe von Bodenstationen erreicht werden können. Damit können manövrierbare Flugkörper, deren Weg im Anflug mehrfach veränderbar ist, in nahezu Echtzeit verfolgt und ständig aktuelle Bahnkoordinaten an eigene Abwehrwaffen übermittelt werden. Die ersten 23 Prototyp-Satelliten sind seit 2023 im Weltraum. Das Gewicht der Satelliten beträgt mit ca. 200 kg nur etwa 1/100-1/25 der Masse klassischer Aufklärungs- oder Kommunikations-Satelliten. Es können deshalb 10-15 von ihnen mit einer Trägerrakete gestartet werden. Das PWSA-Projekt wird von der 2019 eingerichteten US-Behörde* Space Development Agency *gesteuert, welche heute zur ebenfalls 2019 neugegründeten Teilstreitkraft* Space Force *gehört. Allein der Rüstungsgigant Northrop-Grumman hat Bestellungen zum Bau von 92 Satelliten im Wert von ca. 2 Mrd. Dollar in seinen Auftragsbüchern stehen. Deutsche Unternehmen sind als Subunternehmer bei dem Projekt ebenfalls aktiv. Die Airbus-Tochter* Tesat *und der Münchner Laserspezialist* Mynaric *liefern einen Teil der auf den Satelliten zu installierenden Laser-Terminals. PWSA ist so konzipiert, dass eine ständige Modernisierung und Erweiterung mit anderen Aufgaben, z.B. der Navigation, möglich sind. Die durch PWSA aufgebaute Infrastruktur wird als ein Schlüsselelement für die Aufrechterhaltung der militärischen Überlegenheit der USA im Weltraum angesehen.*

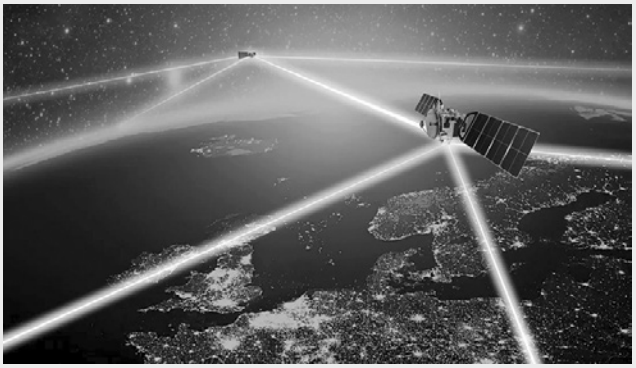


Abbildung 3: Laser-Kommunikation im Weltraum (Illustration). Quelle: Tesat-Spacecom

Die Stationierung von Waffen im Weltraum oder ihre Ankündigung (Abbildung 5) würde die militärische Nutzung des Weltraums auf eine neue Stufe heben. Die Einrichtung einer Weltraumstreitkraft (*Space Force)* in den USA und die Erklärung der NATO 2019, ihr Einsatzgebiet auf den Weltraum auszudehnen, hatten die Spirale bereits vor Kurzem weitergedreht. In Abwe-

Abbildung 4: Prototyp des chinesischen Raumgleiters Shenlong aus 2007. Quelle: Chinesisches Internet

Abbildung 5: Ein Wink mit dem Zaunpfahl: Erste offiziell herausgegebene künstlerische Darstellung des Einsatzes eines Raumgleiters gegen einen feindlichen Satelliten, der wiederum einen eigenen Satelliten bedroht (Quelle: Space Force /John Ayre, 2023).

senheit jeglicher Abkommen für Rüstungskontrolle oder vertrauensbildender Maßnahmen ist es durchaus möglich, dass eine militärische Auseinandersetzung auf der Erde mit Angriffen auf gegnerische Weltrauminfrastruktur beginnt. Einen Vorgeschmack hat der Krieg in der Ukraine geliefert. Zwei Stunden vor dem russischen Angriff am 24. Februar 2022 wurde das Kommunikations-Satelliten-Netzwerk des kommerziellen Anbieters VIASAT gehackt, welches von der ukrainischen Regierung, dem Militär und dem Geheimdienst genutzt wurde [11]. Im September 2022 schaltete SpaceX den Zugang zu Starlink-Satelliten-Terminals in der Ukraine ab, als ferngesteuerte unbemannte Boote (Seedrohnen) Einheiten der russischen Schwarzmeerflotte auf der Krim angreifen wollten. Offensichtlich war der Firma, wenn nicht gar der US-Regierung, der Einsatz des Starlink-Systems für offensive Operationen der Ukraine zu riskant [12].

Zusammenarbeit und Rüstungskontrolle im Weltraum

Die Ansätze für eine Rüstungsbegrenzung im Weltraum [13] sind dünn gesät und sind unter den Bedingungen, dass aktuell anderweitig bestehende Rüstungskontroll-Abkommen seit Jahren aufgekündigt werden [14], auch nicht zu erwarten. Das drängendste Problem für alle Raumfahrtnationen ist der Weltraummüll. Auf den LEO-Bahnen werden funktionsunfähige Satelliten oder ausgebrannte Raketenstufen hinterlassen, die über kurz oder lang wieder in die Erdatmosphäre eintreten und verglühen. Neben diesen relativ großen Teilen hat sich eine Vielzahl von Trümmern [15] angesammelt, die vornehmlich aus Explosionen ausgebrannter Raketenstufen, Antisatelliten-Tests und Zusammenstößen untereinander stammen. Wegen ihrer hohen Bahngeschwindigkeiten von mehreren zehntausend km/h sind auch kleine Teile eine Gefahr für die aktiven Satelliten und für die Weltraumstationen Chinas und der USA. Weltweit werden zur Zeit technische Systeme aufgebaut, die alle Trümmer größer als etwa 1 Zentimeter katalogisieren und verfolgen sollen [16]. Die europäische Weltraumbehörde ESA, aber auch mehrere private Firme, entwickeln Technologien, um den Weltraummüll einzusammeln. Die Vermeidung von neuem Weltraummüll steht im Mittelpunkt weltweiter Bemühungen, das Problem in den Griff zu bekommen. Ein Abkommen, welches Nationen oder Privatunternehmen verpflichtet, ausgediente Satelliten gezielt abstürzen zu lassen, lässt aber auf sich warten. Im Hinblick auf die aus tausenden Satelliten bestehenden neuen Satelliten-Systeme ist eine solche Regelung überfällig. Die USA haben 2022 ein einseitiges Moratorium verkündet, keine ASAT-Tests mehr durchzuführen, die Weltraummüll hinterlassen [17]. China, Indien und Russland haben sich dem offiziell nicht angeschlossen, aber es ist zu hoffen, dass sie aus Eigeninteresse solche Tests ebenfalls nicht mehr durchführen. Die USA kostet das Moratorium nichts, weil sie solche Tests nicht mehr benötigen und die Entwicklung modernerer ASAT-Technologien (Laser, Störungen der Kommunikationskanäle zwischen Satelliten und Bodenstationen) nicht eingeschränkt wird [18].

Transparenz und Internationalisierung sind die Schlüssel für eine Begrenzung der Militarisierung des Weltraums. Multi-nationale Satellitensysteme können nicht für nationale Militärprogramme verwendet werden. Bei ihnen wäre Transparenz hergestellt und es könnte dem ständigen Versuch ein Riegel vorgeschoben werden, jede Innovation des vermeintlichen Gegners (siehe die Raumgleiter) als Bedrohung aufzufassen, weil Weltraumtechnologien oft einen Dual-Use-Charakter [19] haben. Solche Satellitensysteme könnten ihre Dienste über Konfliktgebieten einstellen, sodass militärische Operationen behindert würden. Vorhergehende vertrauensbildende Maßnahmen sind eine Voraussetzung für den Aufbau internationaler Systeme, die am ehesten durch Kooperationen im zivilen Bereich möglich wären, zum Beispiel in der Grundlagenforschung (Weltraumteleskope, Weltraumstationen) oder bei einer gemeinsamen Eingrenzung des Weltraummülls. Wie das Beispiel des Weltraumvertrages von 1967 gezeigt hat, lassen sich Abkommen am ehesten erreichen, bevor Partikularinteressen bezüglich des Vertragsgegenstandes dominant werden. Bei der (bemannten) Erforschung unseres Planetensystems, die mit den Mondprogrammen der USA, Chinas und anderer Nationen erneut Fahrt aufnimmt, wird es zunehmend schwierig, Regelungen zu verabschieden, wie mit möglichen Konflikten z. B. auf dem Mond umgegangen werden soll. Nicht einmal Verhandlungen sind dazu in Sicht, vielmehr verfolgt man einseitige Regelungen, wie die Artemis-Accords der USA, die allenfalls und letztlich notgedrungen von den Partnern des US-Mondprogramms Artemis unterzeichnet werden [20]. Es wäre es wert, Verhandlungen über ein internationales Abkommen vorzuschlagen, keine Militärsatelliten oder Waffensysteme jenseits der Mondbahn zu stationieren, bevor man anfängt, bemannte Marsprogramme ernsthaft auf den Weg zu bringen. Unter den gegenwärtigen Bedingungen des Krieges in der Ukraine und den Spannungen zwischen China und den USA sind die Aussichten, den Weltraum frei

von dort stationierten Waffen zu halten, allerdings nicht besonders vielversprechend. Insofern ist es in der Tat fünf vor zwölf.

Anmerkungen

[1] S. Lakoff, H.F. York, A Shield in Space? Technology, Politics, and the Strategic Defense Initiative, University of California Press, 1989

[2] D. Engels, J. Scheffran, E. Sieker, Die Front im All, Pahl-Rugenstein Verlag 1984. Die Folgen für Europa wurden untersucht in D. Engels, J. Scheffran, E. Sieker (Hrsg.), SDI – Falle für Westeuropa, Pahl-Rugenstein Verlag 1987.

[3] dazu: P. Handley, Reagan's ‚Star Wars' at 40: Battle of the satellites, Space War, 22.3.2023

[4] L. Greenemeier, GPS and the World's First "Space War", Scientific American, 8.2.2016

[5] European Defence. A proposal for a White Paper, Report of an independent Task Force, 2004, EU Institute for Security Studies; s. a. D. Engels, Europäische Pläne zur militärischen Nutzung des Weltraums, in U. Cremer, S. Lutz, Die Bundeswehr in der neuen Weltordnung, 2000, VSA-Verlag, S. 36; R. Hagen, J. Scheffran, Weltraum – ein Instrument europäischer Macht?, in Wissenschaft und Frieden 2001/3

[6] IRIS²: the new EU Secure Satellite Constellation, European Commission, defence-industry-space.ec.europa.eu/eu-space-policy/iris2_en

[7] Global Counterspace Capabilities Report, Secure World Foundation, 2023, swfound.org/counterspace/

[8] Fact Sheets on Anti-Satellite Testing, Military and Intelligence RPOs, and the X-37B, Secure World Foundation, 11.7.2023, swfound.org/news/all-news/2023/07/counterspace-fact-sheets-2023

[9] Eine siebte Mission wurde am Ende 2023 gestartet. M. Smith, DOD's X-37B Spaceplane Flies Again, SpacePolicyOnline.com, 29.12.2023

[10] A. Lele, China's spaceplane returns: is this a new weapon in their counterspace arsenal?, The Space Review, 30.5.2023

[11] The war in Ukraine from a space cybersecurity perspective, European Space Policy Institute (ESPI) Report, Oktober 2022

[12] D. Trubetskoy, Seedrohnen – Kiews Wunderwaffe im Schwarzen Meer, Hamburger Abendblatt, 18.1.2024

[13] A. Sönnichsen, Noch Chancen für Rüstungskontrolle im Weltraum?, in J. Scheffran u.a., Weltraum zwischen Konflikt und Kooperation. W&F Dossier 95, Beilage zu Wissenschaft und Frieden 4/2022 (wissenschaft-und-frieden.de/dossier/weltraum-zwischen-konflikt-und-kooperation-2), S.17.; J. Scheffran, Geopolitik oder Gemeinsame Sicherheit im Weltraum, ebd., S. 2

[14] O. Thränert, Rüstung außer Kontrolle: Die neue atomare Bedrohung, Blätter für deutsche und internationale Politik, 2/2019

[15] Etwa 130 Millionen Teile größer als 1 Millimeter; European Space Agency: World-first Zero Debris Charter goes live, vision.esa.int/world-first-zero-debris-charter-goes-live, 6.11.2023

[16] In Deutschland zum Beispiel das Weltraumradar TIRA: J. Klare, Das wachsame Auge des Radarsystems TIRA, Sterne und Weltraum, 4/2021, S. 34

[17] A. Panda, B. Silverstein, The U.S. Moratorium on Anti-Satellite Missile Tests Is a Welcome Shift in Space Policy, Carnegie Endowment for International Peace, 20.4.2022

[18] T. Hitchens, 'Take down': Space Force targeting unit develops strike options for Joint Force, Breaking Defense, 5.1.2024

[19] R. Hagen, Ein doppelter Verwendungszweck, W&F Dossier 95, a. a. O., S. 14 (2022)

[20] The Artemis Accords: www.nasa.gov/artemis-accords; J. Foust, Germany signs Artemis Accords, Space News, 15.9.2023

Nukleare Anti-Satellitenwaffen

Nach Redaktionsschluss dieses Heftes wurde Russland bezichtigt, im Weltraum zu stationierende Atomwaffen zum Einsatz gegen Satelliten zu entwickeln, was die russische Regierung umgehend als „bösartige Fälschung" zurückwies. Eine Stationierung ist nach dem auch von Russland ratifizierten Weltraumvertrag von 1967 verboten, und ihr Einsatz würde die Satelliten aller Nationen, auch der eigenen, gleichermaßen schädigen. Über eine solche Option wurde bislang allenfalls spekuliert, aber offiziell nirgendwo berichtet, sodass sich auch Beobachter:innen der Entwicklung von ASAT-Technologien überrascht zeigten. Der Vorwurf geht von dem Vorsitzenden des Geheimdienstausschusses im US-Repräsentantenhaus, Mike Turner, aus, und wurde zu einem Zeitpunkt lanciert, als die Beschlussfassung über ein 60 Mrd. $ schweres Unterstützungspaket für die Ukraine im Repräsentantenhaus zu scheitern drohte. Der deutsche Ex-Astronaut Ulrich Walter meinte dazu: „Ich könnte mir gut vorstellen, dass die amerikanische Regierung dieses Atombomben-Gerücht aufbringt, um die Russen zu verteufeln. Im Krieg wird halt überall gelogen, wo die Wahrheit liegt, ist dann nur schwer festzustellen."

Dieter Engels, Jürgen Scheffran und Ekkehard Sieker

Dr. **Dieter Engels**, Astronom, Lehrbeauftragter an der Universität Hamburg

Dr. **Jürgen Scheffran**, Physiker und Professor für Geographie, Forschungsgruppe Klimawandel und Sicherheit, Universität Hamburg

Ekkehard Sieker, Wissenschaftsjournalist in Berlin für das Max-Planck-Institut für Wissenschaftsgeschichte

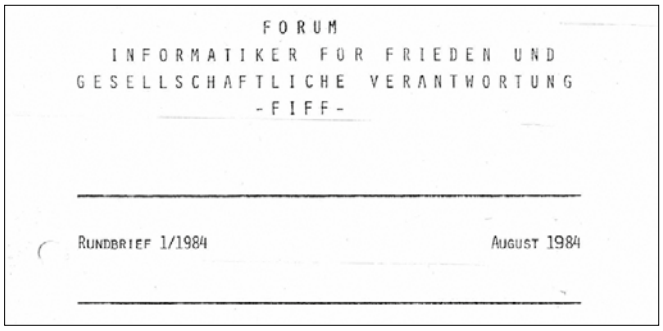
Alle drei Autoren sind Mitglied der NaturwissenschaftlerInnen-Initiative (NatWiss) *Verantwortung für Frieden und Zukunftsfähigkeit*.

Einladung zu Beiträgen für die FIfF-Kommunikation 2/2024

40 Jahre FIfF – Denkwürdige Zeiten

Im Sommer 1984 versammelten sich weit über 200 Informatiker:innen und Computerfachleute in Bonn und gründeten das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF). In einer Kurzbeschreibung im ersten FIfF-Rundbrief heißt es:

> *„Das Forum sieht seine Aufgabe darin, Wissen und Erfahrung über die Wirkung der Informationstechnik auf Gesellschaft und Umwelt zusammenzutragen, zu erarbeiten und zur Diskussion zu stellen. Dabei wird es sich zunächst vorwiegend mit dem engen Zusammenwirken von Informatik, Militärtechnik und modernen Militärstrategien auseinandersetzen."*


FORUM
INFORMATIKER FÜR FRIEDEN UND
GESELLSCHAFTLICHE VERANTWORTUNG
-FIFF-

RUNDBRIEF 1/1984 AUGUST 1984

Seitdem sind 40 Jahre vergangen – ein Anlass zum Innehalten (und durchaus auch zum Feiern). Die drängenden Themen von damals haben an Brisanz nichts eingebüßt. Die Auswirkungen von Informatik und Informationstechnik auf die Gesellschaft sind im Gegenteil eher noch viel ausgeprägter mit allen Chancen und Risiken, die damit verbunden sind. Die Stimme des FIfF ist wie eh und je weiterhin dringend erforderlich.

Die FIfF-Kommunikation 2/2024 wird dem 40-jährigen Bestehen des FIfF gewidmet sein. Es geht aber nicht um eine nostalgische Rückschau, sondern viel mehr darum, kritisch Bilanz zu ziehen und die Schwerpunkte zukünftiger Arbeit zu entwickeln und anzugehen. Alle FIfF-Mitglieder und Freund:innen des FIfF sind eingeladen, Beiträge einzureichen. Damit sich viele beteiligen können, sind zwei Kategorien mit wesentlich beschränkterer Länge als sonst üblich vorgesehen: Schlaglichter mit bis zu 500 Zeichen und Positionen mit bis zu 5000 Zeichen.

Inhaltlich sollten die Beiträge den Bereich Informatik und Gesellschaft thematisieren. Ohne dass das eine Bedingung ist, wäre es wünschenswert, wenn auf die Rolle des FIfF insbesondere in Gegenwart und Zukunft eingegangen wird. Die Einladung richtet sich ausdrücklich auch an Weggefährten und befreundete Organisationen.

Bitte schickt die Beiträge bis Ende April 2024 an *redaktion@fiff.de*. Es wäre auch nett, wenn ihr zeitnah mit einer kurzen E-Mail einen Beitrag ankündigt. Das würde die Heftplanung sehr erleichtern.

Das Herausgabeteam Michael Ahlmann, Stefan Hügel, Hans-Jörg Kreowski und Ralf Streibl

FIfF-Kommunikation 3/2024 – Call for Contributions

Schwerpunkt *Datenschutz*

Redaktion: Jörg Pohle & Stefan Hügel

Seit mehr als fünfzig Jahren gibt es dedizierte Datenschutzgesetze, das Bundesdatenschutzgesetz ist 45 Jahre alt, die EG-Datenschutzrichtlinie fast 30 und die EU-Datenschutz-Grundverordnung auch schon wieder fünf. Die Diskussion um die unerwünschten Eigenschaften und Auswirkungen moderner Informationen ist sogar noch älter, und selbst die informatische Forschung zu möglichen Gegen- und Schutzmaßnahmen geht der rechtlichen Regulierung zeitlich voraus. Gerade vor diesem Hintergrund überrascht es umso mehr, dass wir ganz offensichtlich noch weit entfernt davon sind, datenschutzfreundliche Systeme in der Breite zu entwickeln und in die Praxis zu bringen. Liegt das nur daran, dass die „Digitalisierung" selbst auch ein „moving target" ist, sich immer weiter entwickelt und dabei immer neue Herausforderungen produziert? Oder liegt es nicht auch daran, dass wir tatsächlich überhaupt kein gemeinsames Verständnis des Problembereichs entwickelt haben, sondern mehr oder weniger unterschiedlichen Vorstellungen anhängen und daher ebenso unterschiedliche Ziele verfolgen?

Im Heftschwerpunkt *Datenschutz* der FIfF-Kommunikation 3/2024 wollen wir einen Blick auf das breite Feld des Datenschutzes werfen. Wir sind auf der Suche nach dezidiert informatisch-technischen Perspektiven auf Problembeschreibung & -analyse sowie Schutzmaßnahmen & -mechanismen, nach Entwicklungsansätzen zur technischen Gestaltung von datenschutzfreundlichen Systemen, vor allem aber auch nach erfolgreichen Umsetzungen und deren Einsatz in der Praxis. Uns interessieren dabei aber nicht nur Erfolge, denn gerade auch aus gescheiterten Projekten können wir viel lernen.

Wir freuen uns über Arbeiten, die in alle Richtungen schauen: in die Vergangenheit, die Gegenwart und die Zukunft, auf die Sonnen- und die Schattenseiten, auf die Theorie und die Praxis, auf die Versprechungen und ihre (Nicht-)Umsetzungen, auf technische Systeme und Komponenten, auf Ansätze zur Systemgestaltung und praktische Erfahrungen in der Entwicklung, über Fragen ebenso wie über mögliche Antworten.

Die möglichen Themen sind so breit gefächert wie der Einsatz moderner Informationssysteme und die Auswirkungen auf Individuen, Gruppen, Organisationen und Gesellschaft: von Tracking im Internet über die Bestrebungen zur Einführung einer umfassenden Chatkontrolle bis zu sogenannter „Künstlicher Intelligenz", von Informationssystemen im Bildungs-, Gesundheits- oder Sozialbereich über alte und neue Datenplattformen bis zu technikgestützter zwischenmenschlicher oder Gruppenkommunikation, von Betreibern kleiner und großer Informationssysteme über deren Nutzer:innen bis zu jenen, die als Nichtnutzende von der Nutzung betroffen sind und dabei oft keine Einwirkungsmöglichkeiten haben, von konkret betroffenen Grundrechten (etwa Informationsfreiheit, Meinungsfreiheit, Vereinigungsfreiheit oder Nichtdiskriminierung) über Operationalisierungsansätze zur Überführung von normativen Vorgaben in konkrete Gestaltungen (etwa das Standard-Datenschutzmodell oder ISO-Standards wie 31700-1 und -2) bis zu konkreten technischen Umsetzungen und Systemen (etwa sogenannten „Datenschutz-Cockpits", „Einwilligungsagenten", Interventionsmechanismen oder einfach gut gestalteten, datenschutzfreundlichen Systemen). Ausschließen würden wir gerne nur klassische IT- und Datensicherheitsprobleme, -ansätze und -systeme, auch wenn sie von interessierter Seite, aber leider auch von Teilen der informatischen Community, als „technischer Datenschutz" verkauft werden.

Wir freuen uns über Einreichungen von Beiträgen mit ca. 20.000 Zeichen (inklusive Leerzeichen) bis zum 16. Juni 2024 per E-Mail an Jörg Pohle (*joerg.pohle@fiff.de*) und Stefan Hügel (*sh@fiff.de*). Alle Beiträge zum Schwerpunkt werden peer-reviewed, und die Autor:innen erhalten bis zum 21. Juli Rückmeldungen zu ihren Beiträgen. Die finalen Fassungen der Beiträge sind bis zum 4. August einzureichen.

Wir freuen uns über die Nutzung der Open-Access-Lizenz *Creative Commons – Namensnennung / CC BY* für Ihren Text und verwendete Bilder. Weitere Informationen finden sich im Leitfaden für Autor:innen.

Termine

Einreichungsfrist:	**16. Juni 2024**
Rückmeldung vom Review:	**21. Juli 2024**
Redaktionsschluss / Einreichung der finalen Fassung:	**4. August 2024**

#FIfFKon2024

25.–27. Oktober 2024 Hochschule Bremerhaven

Wir möchten das Themenspektrum:

https://2024.fiffkon.de/

Nachhaltigkeit in der IT

green coding – open source – green by IT

aus verschiedenen Perspektiven beleuchten.

Neben einigen Vorträgen sollen vorzugsweise (Hands-on-) Workshops angeboten werden, in denen praktische Beispiele und Lösungsansätze interaktiv gezeigt, entwickelt und ausprobiert werden können. Dafür können einige Informatik-Labore der Hochschule genutzt werden.

Wir freuen uns über Vortrags- und Workshopangebote zu Themen wie:

- Ressourcen-sparsames Programmieren
- Gestaltung nachhaltiger Infrastrukturen
- Recycling und Upcycling in der Software- und Hardware-Entwicklung
- Refurbishing von IT-Geräten
- Beitrag von Open Source, offenen Schnittstellen und offenen Standards zu längeren Software- und Hardware-Lebenszyklen
- umwelt- und klimaschutz-relevante IT-Anwendungen
- Nachhaltigkeit versus (Auf-)Rüstung

und zu Diskussionen darüber:

- ob und wie durch Open-Source-Software der CO_2-Verbrauch von IT-Systemen reduziert werden kann
- inwiefern Open Source die Gestaltung digital souveräner und langlebiger Infrastrukturen in Unternehmen, (öffentlichen) Verwaltungen und Hochschulen unterstützt
- und wie wir als FIfF Open-Source-Projekte stärken können.

Neben dem skizzierten Schwerpunkt sind Workshops zu weiteren FIfF-Themen wie immer herzlich willkommen.

Wir erbitten Vortrags- und Workshopangebote formlos per E-Mail an *fiffkon24@fiff.de*
Karin Vosseberg und Ulrike Erb, Bremerhaven

Die Tagungsankündigung und weitere Informationen befinden sich unter *https://2024.fiffkon.de/*

#FIfFKon2024

25.–27. Oktober 2024 Hochschule Bremerhaven

Dagmar Boedicker

Bekommen wir den Rechtsextremismus in den Griff?

Unser Verein hat explizit oder implizit die Demokratie immer im Mittelpunkt seiner Arbeit. Für unsere Mitglieder und Aktiven konnte sich über lange Zeit wohl kaum ein Zweifel an der Demokratie einschleichen, wenn es auch unterschiedliche Erwartungen daran gab, wie sie zu gestalten ist.

Seit etlichen Jahren, sogar Jahrzehnten, scheint mir diese Einstellung nicht mehr in der gesamten Gesellschaft gesichert zu sein, und ich glaube, dass wir uns sputen müssen, es könnte sonst bald zu spät sein. Gerade wir in Deutschland haben schlechte Erfahrungen damit gemacht, den Feinden der Demokratie freie Bahn zu lassen. Demokratie braucht Einsatz! Auch wenn der Demokratiebegriff umstritten ist – es gibt eine Partei in Deutschland, die ihre eigene Deutung länger propagiert hat als mit der Demokratie verträglich. Seit Jahrzehnten beherrscht die neurechte Szene das Umdeuten von Wörtern aus der Sprache des Dritten Reichs zu Formulierungen, die man *doch wohl noch aussprechen dürfe,* wie *Ethnopluralismus* für *Rassentrennung* oder *Remigration* statt *Deportation.* Es gibt einen englischen Begriff dafür: *dog whistling,* das heißt die, die gemeint sind, hören das Signal.

Foto vom Kongress des CCC 2023, privat, cc

Nordeuropäische Musterdemokratien von Schweden bis Holland kippen nach rechts. M. Le Pen hat gute Chancen bei der nächsten Wahl in Frankreich, E. Zemmour würde sie gern rechts überholen. A. Duda beklagt den Terror der Rechtsstaatlichkeit nach der Wahl und mit Ungarn sitzt der EU ab Juli 2024 der Autokrat V. Orban vor. H. Aiwanger meint, die schweigende Mehrheit müsse sich die Demokratie zurückholen, und S. Abascal verteidigt in Spanien Stierkampf und Jagd als Kulturgüter. D. Trump erkennt seine Abwahl nicht an und wird dafür von seinen Anhängern wahrscheinlich wieder gewählt. Die AfD gesteht Menschenwürde nur autochthonen Deutschen zu und B. Höcke würde als Ministerpräsident den öffentlich-rechtlichen MDR in Thüringen abschaffen.

Wer die AfD wählt, ist stillschweigend einverstanden mit ihren Ausschlussfantasien. Und wer das bestreitet, ist seit Pegida und anderen sogenannten Bewegungen entweder gedankenlos oder böswillig, jedenfalls nicht an einem gemeinsamen Miteinander in Vielfalt interessiert und bereit, es zu verteidigen. Unser Land hat bitter für das bezahlt, was solche Mitläufer vor fast hundert Jahren möglich gemacht haben.

Was tun?

Der Demokratiebegriff kann aus guten demokratischen Gründen nicht unabhängig vom Demokratieverständnis der jeweiligen Bevölkerung analysiert werden. Wir alle, die wir gruppenbezogene Menschenfeindlichkeit nicht tolerieren, sondern den Respekt für die anderen hegen, den wir für uns erwarten, wir sollten zeigen, dass wir aus der deutschen Geschichte gelernt haben.

Meine Überzeugung ist, dass eine rechtsextremistische Partei in Deutschland verboten gehört. Das kann dauern, deswegen sollten die Regierungen den Verbotsantrag sofort in die Wege leiten, zunächst in den Bundesländern, in denen der Verfassungsschutz zum Schluss gekommen ist, dass die AfD gegen das Grundgesetz arbeitet. Als Bürgerin erwarte ich von unseren Institutionen vollen Einsatz für die Demokratie, auch wenn das bedeutet, dass rechte Ausläufer in der Bevölkerung es übel nehmen. Wir können die Verteidigung des Rechtsstaats nicht von Menschen abhängig machen, die Demokratie ohnehin ablehnen. Bisher haben recherchierende Journalistïnnen sich größere Verdienste in der Verfolgung illegaler Taten und Worte erworben als die Sicherheitsbehörden.

Gleichzeitig fände ich es sinnvoll, die Finanzierung zu unterbinden, auch wenn das viel Aufwand ist. Mein Rechtsempfinden sträubt sich gegen Subventionen für rechtsextrem motivierte Ablehnung der Demokratie. Dazu gehört aber auch das Austrocknen ihrer Finanzierungswege, von der Innenministerin schon lange angekündigt. Wenig sinnvoll finde ich es, einzelnen Protagonisten wie B. Höcke bestimmte Persönlichkeitsrechte abzuerkennen. Abgesehen davon, dass es eine sehr diskriminierende Maßnahme ist, scheint mir damit nichts gewonnen.

Und was können wir tun, wir als Bürgerïnnen dieses Gemeinwesens? Lasst uns Abschied von Illusionen nehmen: Pegidisten, AfD-Mitglieder und Gleichgesinnte gehören zu denen, die andere Menschen nur unter Bedingungen respektieren und ihnen Rechte nur zubilligen, wenn diese Menschen ihren Erwartungen an Gesinnung, Hautfarbe, Religion usw. entsprechen. Vielleicht sind AfD-Mitglieder nicht ganz so gewaltbereit wie diejenigen, die zur *Identitären Bewegung, der Rechten,* zum *Dritten Weg* oder anderen gehören. Es gibt unter ihnen aber genügend, die Hassreden als berechtigte Meinungsäußerung betrachten. Sol-

Foto vom Kongress des CCC 2023, privat, cc

cher Gewalt im Internet entsprechen nur zu oft Drohungen und brutale Handlungen in der realen Welt.

Lasst uns strafbare Äußerungen als das behandeln, was sie sind: strafbar! Eine Anzeige, mindestens ein Widerspruch, die Meldung bei der Plattform, das sind notwendige Mittel der Gegenwehr gegen Menschen, die sich dreist so verhalten, als gelte das Recht für sie nicht oder als seien die sogenannten sozialen Medien rechtsfreie Räume.

Lasst uns die Rechten nicht unterschätzen. Die *sozialen Medien* nutzen sie gern und höchst effektiv. Sie sind seit Jahrzehnten international vernetzt und haben großzügige Förderer, von den Koch-Brüdern in den USA zu vermögenden Personen und Unternehmen in Europa und anderswo. Im ersten Halbjahr 2023 erhielt die AfD von einem hessischen Bauingenieur die größte Einzelspende von allen Bundestags-Parteien in Höhe von 265.000 Euro. Der Spender fürchtet die „Errichtung einer Weltdiktatur der internationalen Hochfinanz mithilfe eines linken Ökokommunismus".[1] 2018 war dieser Betrag allerdings von einem Erbe in Höhe von sieben Millionen Euro übertroffen worden. Vereine und Institute wie das Institut für Staatspolitik (IfS) helfen, Regelungen zur Parteienfinanzierung zu umgehen.

Feindseligen Äußerungen können wir positive Mitmenschlichkeit entgegensetzen. Wenn diese gelassene Reaktion nicht mehr möglich ist, ist eine Meldung besser. Wir müssen das Rad nicht neu erfinden. Verschiedene Initiativen verteidigen Menschenwürde, Mitmenschlichkeit und Demokratie seit Jahren auch im Netz. Hier einige Quellen[2], Ihr kennt vielleicht mehr:

Quellen zum Thema Rechtsextremismus (DACH)

Deutschland

https://www.klicksafe.de/rechtsextremismus
Hier gibt es Information zum Rechtsextremismus im Netz und die Möglichkeit, rechtsextreme Inhalte an Meldestellen für Hass und Hetze zu melden. *klicksafe* nennt weitere Websites und Materialien zum Thema Rechtsextremismus, wie *Belltower.news,* die *Amadeu Antonio Stiftung, Bundeszentrale für politische Bildung,* und bietet Hintergründe und Fallbeispiele sowie Analysen und Maßnahmen zu Rechtsextremismus, beispielsweise ein *Dossier Rechtsextremismus: https://www.bpb.de/themen/rechtsextremismus/dossier-rechtsextremismus/*

---

https://www.demokratie-leben.de/projekte-expertise/kompetenzzentren-und-netzwerke/kompetenznetzwerk-im-themenfeld-rechtsextremismus
Im Bundesprogramm „Demokratie leben!" finden sich Modellprojekte wie: *https://www.demokratie-leben.de/projekte-expertise/projekte-finden/themenfeld/Hass%20im%20Netz*

Ein Begleitprojekt des Bundesprogramms ist die Mediathek: *https://www.vielfalt-mediathek.de/rechtsextremismus.*

Darin findet sich diese Information über den *Mitmach-Faschismus.* Wie Memes Zugehörigkeit und Gruppenidentität herstellen:

> *„Memes sind wie Mathematik. Ich kann mit Leuten sprechen, die meine Sprache nicht kennen, aber wir wissen trotzdem beide, was gemeint ist."*

Normies wissen vielleicht nicht, was bestimmte Symbole bedeuten, wie dieses auf *Discord:* ((( ))) Die drei Klammern fingieren als antisemitische Chiffre für „die Juden*Jüdinnen". Sie wurden auf *4chan* um Namen gesetzt, um die Träger als jüdisch bzw. „jüdische Interessen" vertretend zu kennzeichnen.

---

https://cemas.io/ueber-cemas/
Die Vision von CeMAS A Better Internet is Possible — a Better World is Necessary bedeutet, auch in digitalen Räumen Strategien gegen verschwörungsideologische, antisemitische und rechtsextreme Hetze und Hass zu entwickeln, um diesen Herausforderungen frühzeitig aktiv begegnen zu können. CeMAS bündelt interdisziplinäre Expertise zu den Themen Verschwörungsideologien, Desinformation, Antisemitismus und Rechtsextremismus.

Bundesländer

Baden Württemberg

https://kompetenznetzwerk-rechtsextremismuspraevention.de/hilfe-vor-ort/
Das Kompetenznetzwerk Rechtsextremismusprävention (KompRex) bietet eine Suchplattform mit einem Überblick über 237 wichtige Beratungs-, Bildungs- und Präventionsstellen aus der Zivilgesellschaft in ganz Deutschland.

---

https://www.demokratie-bw.de/reflex
Aktiv gegen Vorurteile und Menschenfeindlichkeit

---

https://www.demokratie-bw.de/lokal-vernetzen
Projektförderung gegen Gruppenbezogene Menschenfeindlichkeit in lokalen Gemeinwesen.

Bayern

https://www.bige.bayern.de/infos_zu_extremismus/rechtsextremismus/index.html
Bayerische Informationsstelle gegen Extremismus (BIGE)
Es gibt ein Bürgertelefon und eine Mail-Adresse: (089) 2192-2192 und *gegen-extremismus@stmi.bayern.de*

NRW

https://www.medienanstalt-nrw.de/themen/hass/verfolgen-statt-nur-loeschen-rechtsdurchsetzung-im-netz.html
Initiative der Landesanstalt für Medien NRW: Verfolgen statt nur löschen und Hassrede melden. Dort haben die Behörden bereits 951 Ermittlungsverfahren eingeleitet, 430 Beschuldigte ermittelt und 41 rechtskräftige Verurteilungen ausgesprochen.

https://www.forena.de/aktuelles/
Forschungsstelle der Universität Düsseldorf.

https://www.idaev.de/
Informations- und Dokumentationszentrum für Antirassismusarbeit e. V. (IDA)

Hessen

Hessen gegen Hetze: *https://hessengegenhetze.de/*

Thüringen und Region

Topografie des Rechtsextremismus:
https://topografie-archiv.komrex.uni-jena.de/

Schweiz

Eine Meldestelle habe ich nicht gefunden, was nicht bedeutet, dass es keine gibt. Auf der Seite *https://www.jugendundmedien.ch/extremismus-radikalisierung* findet sich ein Nationaler

Foto vom Kongress des CCC 2023, privat, cc

Aktionsplan zur Verhinderung und Bekämpfung von Radikalisierung und gewalttätigem Extremismus 2023 – 2027:
https://www.newsd.admin.ch/newsd/message/attachments/74621.pdf

Österreich

https://www.doew.at/ ist das Dokumentationsarchiv des österreichischen Widerstands. Dort findet sich auch eine Liste von rechtsextremen Organisationen, von denen einige auch in Deutschland und der Schweiz vertreten sind. Eine deutsche Organisation, deren Anhänger in Österreich verbreitet sind, ist die DKEP/DKG: *https://www.doew.at/erkennen/rechtsextremismus/rechtsextreme-organisationen/deutsches-kulturwerk-europaeischen-geistes-dkeg-deutsche-kulturgemeinschaft-dkg*. Mehr gibt es auf der Seite *https://www.doew.at/erkennen/rechtsextremismus/neues-von-ganz-rechts*

Kanäle der Rechten: deutsche und internationale

Es ist gut zu wissen, welche Medien die rechte Szene nutzt. Hier eine kleine Auswahl: Junge Freiheit, Compact, Deutschland-Kurier, Antaios-Verlag, Kontrafunk, Nius, Auf1, 4chan, Gettr, X, TikTok, Discord, Telegram, ZUERST!, Tichys Einblick, PI News, Journalistenwatch, Russia Today, Breitbart News. Viele weitere verbreiten Desinformation im Netz.

Anmerkungen

1 *https://www.rnd.de/politik/hartmut-issmer-wer-ist-der-dubiose-afd-grossspender-E3J4XP4CJZEEFNXJRD65VDJZ6Q.html (abgerufen am 15.2.24)*
2 *abgerufen am 6. Februar 2024*

Dagmar Boedicker

Dagmar Boedicker ist Journalistin, technische Redakteurin und langjährige Redakteurin der FIfF-Kommunikation.

Hans-Jörg Kreowski und Margita Zallmann

FIfF-Konferenz 2023

Editorial zum Schwerpunkt

Vom 3. bis 5. November 2023 hat in der Jugendherberge Berlin Ostkreuz die FIfF-Konferenz 2023 stattgefunden. Der Schwerpunkt dieser ersten Ausgabe der FIfF-Kommunikation *im Jahre 2024 dient der Dokumentation der Veranstaltung.*

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 musste von diesem Prinzip abgewichen werden, weil keine Regionalgruppe die Organisation übernommen hat. Der Vorstand hat sich deshalb etwas Besonderes vorgenommen, nämlich gemeinsam mit den Mitgliedern in die Zukunft zu 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? Welche Perspektiven, Zukunftsvisionen, Chancen, Utopien und Inspirationen für Umbruch und Aufbruch können herausgearbeitet werden? Aufgrund der Rückmeldungen aus der Mitgliedschaft haben sich drei Schwerpunkte herauskristallisiert:

- Cyberpeace – z. B. Kritik an der Planung zum *Future Combat Air System* (FCAS) und zur militärischen Nutzung der Künstlichen Intelligenz,
- Information und Nachhaltigkeit – z. B. *Bits & Bäume* sowie Informationstechnik und Entwicklungspolitik,
- Entwicklungen der Künstlichen Intelligenz – z. B. Chancen und Risiken der Entwicklung und Nutzung von ChatGPT sowie Auswirkungen auf die IT-Sicherheit.

Die FIfF-Konferenz fand in einer Zeit zugespitzter Krisen und Katastrophen statt – für uns direkt wahrnehmbar in Europa, aber auch weltweit. Bereits die FIfF-Konferenz 2022 *make install PEACE – Impulse für den Frieden* war durch den immer noch andauernden Angriffskrieg von Russland auf die Ukraine geprägt. Die Teilnehmenden der Konferenz 2023 standen zusätzlich unter dem Eindruck der gerade vier Wochen zurückliegenden schockierenden Terrorangriffe der Hamas auf Israel sowie der nachfolgenden Bombardierung des Gazastreifens durch israelisches Militär.

Vor diesem Hintergrund erhält der erste Schwerpunkt ein besonderes Gewicht. Seit zehn Jahren greift die Cyberpeace-Kampagne des FIfF das Bedrohungspotenzial durch Cyberangriffe auf und mittlerweile generell die Gefahren durch zunehmende Aufrüstung mithilfe von Informations- und Kommunikationstechnik. Angesichts proklamierter „*Zeitenwende*“ und „*Kriegstüchtigkeit*“ ist das FIfF gefordert, die Risiken durch den militärischen Einsatz von Künstlicher Intelligenz und (teil-)autonomen Waffen zu thematisieren und den Diskurs darüber mitzugestalten. Das Cyberpeace-Thema war in einer Reihe von Beiträgen und in verschiedenen Präsentationsformen vertreten.

Beim *Pecha Kucha rund um Cyberpeace* wurde eine Folge von Beiträgen präsentiert, wobei jeder einzelne Beitrag aus 20 Folien zu je 20 Sekunden bestand. Da sich die Form eines Pecha Kucha nur schwer schriftlich widerspiegeln lässt, sind die Beiträge hier als einzelne Artikel dokumentiert:

- Daniel Guagnin: *IT-Sicherheit vs. Sicherheit in der IT – Ein unlösbarer Widerspruch?*
- Christian Heck: *Eine technisch erzeugte Wirklichkeit*
- Sylvia Johningk: *Warum man keine 0-Day-Schwachstellen geheim halten darf*
- Kai Nothdurft: *Responsible Disclosure stärken, Geheimhaltung von Schwachstellen schwächen*

Es sei besonders darauf hingewiesen, dass Kai in seinem Beitrag zur Mitwirkung in einer Kampagne für Responsible Disclosure aufruft.

Daniel Guagnin, Laura Anna Kocksch und Basil Wiesse haben auf einem Panel zum Thema *Für eine De-Militarisierung von Cybersicherheit. Perspektiven aus der Soziologie und den feministischen science and technology studies (STS)* für einen neuen Zugang zu Cybersicherheit plädiert. Ihre Überlegungen liegen in Form eines gemeinsamen Artikels vor.

Unter der Leitung von Christian Heck wurde im Rahmen des Labors *ground zero* im Fachgebiet *Experimentelle Informatik* an der Kunsthochschule für Medien Köln das Kunstprojekt *Cyber Peace Works* durchgeführt. Die entstandenen Werke wurden während der Konferenz in einem eigenen Raum ausgestellt, wo sich vielfach Gelegenheit bot, die Ausstellung zu besichtigen und mit den Künstler:innen ins Gespräch zu kommen. Unter dem Ausstellungstitel wurden die einzelnen Werke auf der Konferenz in einer kollektiven Performance-Lecture vorgestellt, und hier werden sie in kurzen Texten beschrieben. Darüber hinaus wird die Grundidee des Projekts von Lisa Reutelsterz, Leon-Etienne Kühr, Benita Martis und Christian Heck ausführlich in dem Artikel *Aesthetic approaches to cyber peace works* erläutert. Eine Kunstausstellung im thematischen Zusammenhang mit einer FIfF-Konferenz ist bisher einmalig. Es wäre aber höchst wünschenswert, wenn das ein wiederkehrendes Ereignis wird.

Der zweite und der dritte Schwerpunkt der Konferenz waren durch je zwei Vorträge repräsentiert. Friederike Hildebrandt vom BUND hat über *Machtfragen im Digitalisierungsprozess aus Sicht der Nachhaltigkeit* referiert, und Erich Pawlik hat sich mit *ICT4D trifft auf digitalen Kolonialismus und Überwachungsstaat* auseinandergesetzt. Friederikes Vortrag ist in diesem Heft in einem Extended Abstract reflektiert, während eine Langfassung für eine der nächsten Ausgaben der FIfF-Kommunikation angedacht ist. Von Erichs Beitrag erscheint ein erster Teil mit dem Titel *Entwicklungszusammenarbeit trifft auf Tech-Konzerne und den Überwachungsstaat: Teil 1 – Digitaler Kolonialismus*. Der zweite Teil erscheint demnächt. Erich Pawlik hat sich in seinem zweiten Vortrag damit beschäftigt: *Was man über die Ökonomie der generativen KI wissen sollte.* Zu dem zweiten Vortrag im Kontext generativer KI von Ulf Strohbach über Cyberangriffe mit ChatGPT und generativer KI ist leider keine schriftliche Fassung eingegangen. Auch Werner Winzerling hat auf eine Verschriftlichung seines Vortrags zum jetzigen Zeitpunkt verzichtet. Außerhalb des eigentlichen Programms hat Hans-Jörg Kreowski unter dem Titel *FIfFKon23 poetisch* Gedichte von Ernst Jandl und Kurt Schwitters vorgetragen, sowie zwei eigene. Ein Gedicht ist im Schluss-FIfF als Kostprobe abgedruckt.

Die Beiträge in diesem Schwerpunkt erscheinen in der Reihenfolge, wie sie auch in diesem Editorial aufgeführt sind. Auf der Webseite der FIfF-Konferenz 2023 unter *https://2023.fiffkon.de/* befinden sich einerseits im „Fahrplan" zu fast allen Beiträgen kurze Inhaltsbeschreibungen und andererseits die Links zu den Videoaufzeichnungen.

Es ist keine Übertreibung, die FIfF-Konferenz 2023 als Erfolg zu bewerten. Dazu haben viele beigetragen, denen Dank gebührt. Das gilt zuallererst den Beitragenden, die in Form und Inhalt für ein abwechslungsreiches Programm gesorgt haben. Das gilt aber auch den fast 100 Teilnehmer:innen, deren Interesse und Diskussionsfreude für eine erfolgreiche Konferenz unabdingbar waren. Besonders bedanken muss sich das FIfF auch beim CCC-Media-Team, das während der gesamten Konferenz durch ein Streaming-Angebot für zusätzliche Teilnahme gesorgt hat und durch die zeitnahe Verfügbarkeit der Videoaufzeichnungen für eine erhebliche Außenwirkung der Konferenz. Sehr wichtig war auch die finanzielle Unterstützung durch den Chaos Computer Club (CCC), ohne die das FIfF die Konferenz nicht hätte durchführen können. Zu danken ist auch der Jugendherberge Berlin Ostkreuz für die Zusammenarbeit. Die Räumlichkeiten, die technische Ausstattung, die gute Erreichbarkeit durch öffentliche Verkehrsmittel und die Verpflegung haben vieles erleichtert. Schließlich gebührt dem Berliner Organisationsteam für den reibungslosen Ablauf der Konferenz vor Ort besonderer Dank.

Daniel Guagnin

IT-Sicherheit vs. Sicherheit in der IT – Ein unlösbarer Widerspruch?

In der Cybersicherheit gibt es ein paar verwunderliche Gegensätze, die ich hier kurz kontrastiert skizzieren möchte.

Im Grunde gibt es wie so oft auch in diesem Feld drei Problembereiche:

1. Die Guten (im Wesentlichen die als Big Five bekannten Digitalmonopole GAFAM[1]) – sie lieben unsere Daten und haben große Ressourcen, diese zu sichern. Allerdings ist hier von Angriffslücken alle Welt zugleich betroffen, und lange Reaktionszeiten von der Meldung bis zur Schließung einer Lücke sind nicht ausgeschlossen.[2]

2. Die Bösen (Hacker) – erklärte Gegner:innen der Sicherheitsbehörden. Tatsächlich verursachen Ransomware-Attacken alltäglich Millionenschäden.

3. Das Hässliche: Sicherheitsbehörden setzen im Kampf gegen das Böse™ gerne Überwachungssoftware ein (z. B. Staatstrojaner), die funktional ebenso wie böse Schadsoftware funktioniert (Trojaner). Außerdem bekämpfen Sicherheitsbehörden damit „Terroristen", als die in manchen Ländern mitunter auch Menschenrechtsanwälte gelten.

Auch hässlich: Die sicherste Technologieinfrastruktur kann häufig von einem kleinen Eckstein zu Fall gebracht werden, z. B. ein unbeachtetes FOSS-Projekt *(Freie und Open-Source-Software)* von Hobbyprogrammierer:innen, die spärlich Zeit haben für aufwändige Code-Reviews oder zeitnahe Sicherheitspatches.

Schade, dass die staatliche Strategie immer wieder das „Überwachen und Strafen"[3] von Kriminalität höher priorisiert als die Verhinderung von Kriminalität. Statt Ressourcen für die Schließung von Sicherheitslücken bereitzustellen und Infrastrukturen zu etablieren, die Rechtssicherheit für Sicherheitsforschende und niederschwellige Meldewege ermöglichen, wird auf eine Ausweitung der Zugriffsmöglichkeiten der Sicherheitsbehör-

den hingearbeitet.[4] Somit werden Verfolgungsmöglichkeiten durch systematische Zugriffe auf Verschlüsselung, Staatstrojaner und Befugnisse für Cyberattacken gefordert, die auf der Ausnutzung und dem Vorhalten von Sicherheitslücken basieren.[5] So wird die Angreifbarkeit der allgemeinen technischen Infrastruktur mit finanziellen Ressourcen erhöht durch das Vorhalten (Nicht-Schließen) oder gar Einkaufen von Sicherheitslücken (auf illegalen Märkten) und das Entwickeln entsprechender Exploits. Damit wird allen geschadet, weil genau diese Lücken auch von Kriminellen genutzt werden, wie prominent bei WannaCry[6] deutlich wurde.

Alternativ erreicht man eine breite Informationssicherheit durch technische Integrität für alle, wenn man Ressourcen in das Schließen dieser Lücken steckt. Während hierzu staatliche Einrichtungen wie bspw. das Bundesamt für Sicherheit in der Informationstechnik und das Zentrum Informationstechnik in der Sicherheit gegensätzliche Positionen vertreten (technische Sicherheit vs. Überwachen und Strafen), ist sich die technische Community überwiegend so einig, dass sogar der CCC einen gemeinsamen offenen Brief mit Google verfasst hat, sonst im Diskurs eher auf gegenseitigen Positionen stehend.[7] Schön, dass es immer wieder Expert:innen-Anhörungen und Möglichkeiten für Eingaben von Stellungnahmen gibt. Schade, dass diese oft halbherzig und kurzfristig sind und die Ratschläge der Expert:innen von Exekutive und Legislative nur wenig berücksichtigt werden.[8]

Anmerkungen

1 https://de.wikipedia.org/wiki/Big_Tech (abgerufen am 2.2.2024)

2 https://unit42.paloaltonetworks.com/microsoft-exchange-server-attack-timeline/ (abgerufen am 2.2.2024)

3 Siehe auch Beitrag im gleichen Heft: Guagnin, Kocksch und Wiesse

4 Neue Programme wie der Souvereign Tech Fund der aktuellen Bundesregierung lassen auf eine konstruktivere Politik hoffen, aber die Chatkontrolle bleibt im EU-Diskurs

5 https://netzpolitik.org/2021/offener-brief-fuer-eine-echte-cybersicherheitsstrategie-ohne-neue-ueberwachungsmassnahmen/ (abgerufen am 2.2.2024), siehe auch Beitrag im gleichen Heft: Guagnin, Kocksch und Wiesse

6 https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/ (abgerufen am 2.2.2024)

7 https://netzpolitik.org/2021/offener-brief-google-facebook-und-ccc-protestieren-gemeinsam-gegen-staatstrojaner/

8 https://www.fiff.de/presse/CybersicherheitsstrategieJuni21.html (abgerufen am 2.2.2024)

Autoreninfo siehe Seite 41

Christian Heck

Eine technisch erzeugte Kriegswirklichkeit

Was codiert, auf tausende Maschinen übertragen und durch permanente Wiederholung Teil unserer Alltagswelt wird, stabilisiert sich selbst und wird schließlich zum kulturellen, unhinterfragten Sediment (Trogemann, Georg 2010).

Intelligence

Alles, was Soldatinnen und Soldaten in Operationszentralen gläserner Gefechtsfelder *(Transparent Battlefield)* sehen bzw. wahrnehmen können, das können sie einzig durch Apparate und Sehmaschinen wahrnehmen.

Alles, was sie erfahren, d. h. die Verarbeitung des Wahrgenommenen sowie auch der Abgleich mit weiteren Quellen, Geheimdienstinformationen, *Open Source Intelligence* (OSINT) usw, auch zu lernen, wie man sich innerhalb dieser Cyberräume verhält, wie man sich durch sie hindurch navigiert, all das findet mit Hilfe meist intelligenter Systeme statt. Technische Systeme, mit deren Hilfe Akteure symbolische Repräsentationen mit der konkreten Welt zu verbinden vermögen. Systeme, die sie befähigen in ihrem jeweiligen technologisierten Operationsumfeld zu handeln, d. h. für *Multi-Domain-Operations* (MDO), um „sinnvoll innerhalb von Kontexten handeln [zu] können" (Pangaro 2012). Diese technischen Systeme interpretieren somit Soldatinnen und Soldaten Teile von Welt technisch vor. Eben jene, die einst in sie hineinkamen.

> *„Während dieses Prozesses fließt demnach eine jeweilige Bedeutung […] in den Komplex auf der einen Seite*

(Input) hinein, um auf der anderen Seite (Output) wieder herauszufließen, wobei der Ablauf selbst, das Geschehen innerhalb des Komplexes, verborgen bleibt: eine ‚Black Box' also." (Flusser 2006).

Die Codierung der technischen, symbolischen Repräsentationen von Welt jedoch, nach denen und durch die militärisch-technische Handlungen vollzogen werden, so Flusser weiter, diese digitale Codierung „geht aber nun einmal im Inneren dieser Black-Box vor sich."

Artificiality

Zum Verständnis: Alles, was maschinenlesbar ist, musste erst einmal maschinenlesbar gemacht werden. Nicht nur technisch, sondern auch geistig. Alles, was für unsere Köpfe, auch technische Systeme berechenbar ist *(computable)*, musste erst einmal berechenbar gemacht werden.

Sprechen wir von gläsernen Gefechtsfeldern, von zivilen Cyberräumen, in denen militärische Handlungen verübt werden, so sprechen wir also von einer künstlichen Realität – einer technisch erzeugten Kriegswirklichkeit. Von einer Künstlichkeit *(Artificiality)* laut Herbert Simon, in der das technische Artefakt das Reale imitiert, indem es seiner Umwelt „das gleiche Gesicht zuwendet". Eine „Ähnlichkeit von außen und nicht von innen", „Wahrnehmungsgleichheit, aber zugleich auch eine wesentliche Verschiedenheit" (Simon 1969).

Künstliche technische Bilder als Verbundsysteme im Ineinander menschlicher und technischer Akteure, die aktiv über Leben und Tod von Soldatinnen und Soldaten, von Jugendlichen, von Großeltern, von Eltern und unseren Kindern Entscheidungen treffen. Folglich muss laut Vilém Flusser eine „jede Kritik der technischen Bilder darauf gerichtet sein, ihr Inneres zu erhellen. Solange wir über eine derartige Kritik nicht verfügen, bleiben wir, was die technischen Bilder betrifft, Analphabeten" (Flusser 2006).

Sense making

Denn die Militarisierung des Internets, auch dem der Dinge, greift mehr und mehr in unseren technologisierten Lebensalltag ein – in unser soziales Miteinander, dort, wo wir beisammen sind und miteinander sprechen. Dort, wo sich der Gemeinsinn verortet und Begriffe ihren gesellschaftlichen Sinn erhalten, also *Sense making* stattfindet. Mit technischen Systemen – und durch sie –, ob nun intelligent oder nicht, entstehen somit neue Erfahrungs- und Handlungsräume, die vorher nicht existiert haben. Wir lernten zu erkennen, dass Technik mehr und mehr der Erkenntnis unserer Lebenswelt vorausläuft. „Dass das, was wir erkennen können, sich im gleichen Maße verändert, wie wir unsere Lebenswelt technisch umbauen" (Trogemann 2021).

Cyberkriege sind demnach immer in bereits bestehende Handlungskontexte eingebunden und rekontextualisieren diese, indem sie durch Wiederaufladungen während des militärischen, computergestützten Erkenntnisgewinns in Erscheinung treten. Sie aktivieren somit realweltlichen Gebrauch, das heißt immer dann, wenn sie in die Umwelt eingebettet werden, neue Handlungskontexte, eben solche, die es für uns als Gesellschaft a posteriori zu erschließen gilt. Zu ihrer zivilgesellschaftlichen Erschließung sind die Systeme selbst jedoch leider nicht sonderlich hilfreich, da das, was wir wahrnehmen und erkennen können, eben erst innerhalb des gesetzten technischen Rahmens hergestellt wird.

So sind wir derweil auch nicht dazu in der Lage, sie in ihrer Komplexität durchzudenken und zu verstehen. Weder als Individuum, noch als Gesellschaft. Wenn laut Hannah Arendt das „Ergebnis des Verstehens Sinn" ist, dann kann der Zweck des Verstehens auch nur die Erzeugung von Sinn sein (Arendt 1994). Auf den gesellschaftlichen Kontext übertragen: Gemeinsinn. Dieser Sinn kann sich laut Arendt einzig durch die Existenz der Pluralität unter Menschen ergeben. Hierfür muss jedoch über diese technischen Wirkräume und über ihre sozialen, gesellschaftlichen und kulturellen Konsequenzen gesprochen werden können. Sie müssen in ihrer Komplexität verständlich dargelegt und gemeinsam erschlossen werden können.

Nach Arendt hieße das weiter: Je komplexer künstliche Welten auf Basis statistischer Modelle, Computersimulationen und Big Data generiert werden, desto weniger ergeben sie für die Gesellschaft Sinn, eben da wir nicht über sie sprechen können. Darum werden wir sie so nicht verstehen – weder die inneren Funktionsweisen der technischen Systeme noch ihre konkreten Folgen für die Zivilgesellschaft.

Einer der möglichen Gründe für die Sinnlosigkeit von Cyberkriegen liegt somit in den jeweiligen Ansätzen zur Konzeption gesellschaftsrelevanter Fragestellungen: der des Sinns und der Erkenntnis. Uns als Zivilgesellschaft ist es laut Hannah Arendt durchaus möglich, weit über die Grenzen der Erkenntnis hinauszudenken – nur nicht über das Wirkliche hinaus. Doch unser gemeinsames Leben, unser gemeinschaftliches Miteinander ist wirklich.

„Seien wir realistisch, versuchen wir das Unmögliche!" (Che Guevara)

Referenzen

Arendt, Hannah (1994): Zwischen Vergangenheit und Zukunft. Übungen im politischen Denken I., Ursula Ludz (Hrsg.), München: Piper Verlag, S. 111.

Flusser, Vilém (2006): Für eine Philosophie der Fotografie, 10. Aufl. (zuerst 1986), S. 15

Pangaro, Paul (2012): On artificial intelligence, Interview auf Vimeo. URL: https://vimeo.com/41782297

Simon , Herbert (1969): The Sciences of the Artificial, MIT Press.

Trogemann, Georg (2010): Code and Machine in Code: Between Operation and Narration, Andrea Gleiniger und Georg Vrachliotis (Hrsg.), Berlin, Boston: Birkhäuser, S. 41-53.

Trogemann, Georg (2021): DAS 18. KAMEL und Die Habitate des Denkens, in: Über das Paradox, Technik in der Kunst zu lehren, Ursula Damm / Mindaugas Gapsevicius (Hrsg.), Bielefeld: transcript Verlag, S. 117-166.

Autoreninfo siehe Seite 42

Sylvia Johnigk

Warum man keine 0-Day-Schwachstellen geheim halten darf

Der Artikel ist eine Zusammenfassung meines Pecha-Kucha-Vortrags auf der FIfF-Konferenz 2023 in Berlin. Er befasst sich damit, warum es ein Irrweg ist, 0-Day-Schwachstellen geheim zu halten, um sie für Angriffe im digitalen Raum nutzen zu können.

Der Einzige, der Schwachstellen in einem IT-Produkt beseitigen kann, ist der Hersteller. Wird ihm eine gefundene Schwachstelle nicht gemeldet, kann er sie nicht schließen und die Schwachstelle verbleibt in dem IT-Produkt. Nutzer:innen des IT-Produkts können sich nicht schützen. Angreifer:innen können die Schwachstelle nutzen, um so in das System einzudringen, unbemerkt an Informationen zu gelangen und/oder sogar Schaden anzurichten.

Interessensgruppen

Wer hat ein Interesse daran, Schwachstellen geheim zu halten? Kriminelle, Militär, Geheimdienste, Strafverfolgungsbehörden und der Verfassungsschutz sind die Hauptinteressenten. Schon immer waren sie daran interessiert, Schwachstellen auszunutzen, um Opfer, Gegner oder Verbrecher überführen zu können. Seit Jahren proklamieren sie, dass sie ihre Arbeit nicht leisten können, wenn sie nicht auf moderne Einsatzmittel zurückgreifen. Deshalb wollen sie geheime 0-Day-Schwachstellen haben, die sie dann für passgenaue 0-Day-Exploits verwenden können.

Spätestens seit dem Ukraine-Krieg und nun insbesondere dem Israel-Krieg wird die Rhetorik zunehmend härter. Wurde früher über die Nutzung von 0-Day-Schwachstellen „lediglich" von defensiven Exploits gesprochen, wird mittlerweile offen von offensiven Exploits gesprochen. Durch das Zeigen demonstrierbarer Angriffsstärke erhoffen sich die Befürworter:innen der Geheimhaltung Abschreckung zu erreichen.

Der Weg zur 0-Day-Schwachstelle

Bereits 2018 wurde eine neue Behörde gegründet: die *Zentrale Stelle in der Informationstechnik im Sicherheitsbereich*. Die zusätzliche Sicherheitsbehörde wurde geschaffen, da das Bundesamt für Sicherheit in der Informationstechnik in Misskredit geriet. Sie soll stellvertretend für eine Reihe von Behörden unter anderem 0-Day-Schwachstellen selbst suchen und weiterentwickeln bzw. am „Weißen Hacker:in-Markt" kaufen dürfen.

Dabei stellt sich die Frage: wie „weiß" sind Hacker:innen, die gefundene Schwachstellen an Regierungen verkaufen, anstatt sie dem Hersteller zu melden, um sie schließen zu lassen? Grundsätzlich schließt *white-hacking* aus, Schwachstellen an Dritte zu verkaufen oder sie zu verwenden, um in fremde Systeme einzudringen und Schaden anzurichten. Dafür gibt es keinen Spielraum. White-hat-Hacker:innen melden die gefundenen Schwachstellen dem Hersteller.

Zudem lässt sich gar nicht oder nur schwer hinter die Fassade der vermeintlich guten white-hat-Hacker:innen schauen. Es ist nur schwer nachvollziehbar, ob eine Schwachstelle selbst gefunden wurde oder am Schwarzmarkt gekauft und „aufpoliert" weitergereicht wurd, oder ob sie bereits anderweitig verkauft wurde. Schließlich gibt es außer einem Vertrag nichts, was den Nachweis erbringt, dass eine Schwachstelle nur einmal verkauft wurde.

Eine einzelne Schwachstelle stellt noch keinen ausgefeilten Angriff auf ein dediziertes System dar. Oft benötigt man mehrere Schwachstellen, die ineinandergreifen und ebenso den eigentlichen Exploit, der ein bestimmtes System ausspäht oder gar schädigt. Ein solcher Exploit muss erst entwickelt werden.

Ein wirklich „guter" 0-Day-Exploit

Dieser Exploit darf selbstverständlich nichts Bekanntes sein, das durch einen Malwarescanner sofort erkannt werden würde. Einen Sturmtruppler würde „jeder", der Star Wars kennt, sofort erkennen und auch seine Absicht – auch ein automatisches Überwachungssystem würde einen Sturmtruppler als Gefahr einstufen. Wäre er eine Malware, würde man allenfalls in ein ungepatchtes, unbewachtes System gelangen. Um in ein gut geschütztes System zu gelangen, ist mehr erforderlich, als es mit bekannten Angriffsmethoden zu attackieren. Wenn man Sturmtruppen und Star Wars nicht kennt, wäre der Patch, ins Kino zu gehen oder sich den Film im Internet anzusehen.

Etwas Neues zu entwickeln, was nicht durch Überwachungssoftware automatisiert erkannt wird, ist aufwändig, aber notwendig, wenn Angriffe tatsächlich erfolgreich sein sollen. Dabei geht es nicht nur darum, dass niemals dieselbe Software verwendet wird, sondern auch nicht dasselbe Muster. Die Signaturen der Überwachungssoftware arbeiten in der Regel mit Mustererkennung auf Basis (mathematischer) Modelle, um zu verhindern, dass nur ein paar „Wörter" ausgetauscht werden oder, um bei Star Wars zu bleiben, der Sturmtruppler rosa angemalt wird.

Sylvia Johnigk

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

Um ein zu attackierendes System auszutricksen, müssen Angreifer:innen einen Exploit entwickeln, der von der gängigen Überwachungssoftware nicht erkannt wird, damit sie möglichst lange im System Informationen ausspähen und/oder zum „richtigen" Zeitpunkt im System Schaden anrichten können. Das Problem dabei ist, dass sie das Zielsystem kennen müssen, also im Vorhinein orakeln müssen, welches Zielsystem ausgespäht und geschädigt werden soll. Jede Infrastruktur ist anders, die Systemsettings, die Überwachungssoftware etc.

Nun kann man sagen, dass unter der gegebenen politischen Lage Angriffsziele eher in Russland, China, der arabischen Welt etc. liegen werden, da von dort auch die meisten Angriffe zu erwarten wären, aber damit ist es noch nicht getan. Auch innerhalb eines Landes gibt es verschiedene Bereiche: Regierung, Militär, Infrastruktur, Medien, Rüstungsindustrie etc. Zudem muss ein Angriff angemessen sein, dies vorherzusehen erscheint unerreichbar.

Exploit-Entwicklung ist Teamarbeit

Für die Entwicklung eines einsatzfähigen 0-Day-Exploits, der gezielt ein bestimmtes Zielsystem ausspähen oder schädigen soll, benötigt man in der Regel neben Zeit und Geld ein Entwicklungsteam, das diesen Exploit professionell entwickelt.

Wie jede normale Software muss auch Angriffssoftware getestet werden. Es ist eine Testumgebung notwendig, die möglichst nah an den Gegebenheiten des Zielsystems liegt. Dafür ist es notwendig, dass Monitoring, Netzüberwachung und ggf. Server/Endgeräte zwar vorhanden sind, aber keine Rückmeldungen an die Hersteller liefern, die am Anfang möglicherweise noch anschlagen würden. Würde es Rückmeldungen geben, so können Hersteller möglicherweise die neue Angriffssoftware erkennen und ihr den Garaus machen, bevor die Angriffssoftware einsatzfähig ist.

Berücksichtigt man nun, dass es Auftraggebende, Bezahlende, Entwickelnde, Infrastrukturbetreibende, Kontrollierende und „Hackende" bzw. Unternehmen, die Schwachstellen verkaufen, gibt, wissen von diesem Vorhaben, von den 0-Day-Schwachstellen und den 0-Day-Exploits ziemlich viele Personen. Mehrere haben auf den ganzen Exploit Zugriff, da sie sehr eng an der Entwicklung und dem Test beteiligt sind. Das sind für ein „Geheimnis" ziemlich viele Mitwissende.

Wir sind nicht allein in der Welt

Wir sind auf dieser Welt nicht allein, mit uns gibt es weit über 190 Staaten, die genau dasselbe tun wie wir: Ihre Regierung, ihr Militär, ihr Geheimdienst und ihre Polizei suchen ebenfalls nach 0-Day-Schwachstellen und entwickeln Exploits. Dabei muss jedem klar sein, dass beim Aufspüren von Schwachstellen standardisierte Verfahren und Methoden benutzt werden – weltweit dieselben, da in der Regel Schwachstellen in Systemen gesucht werden, die mittels standardisierter Verfahren und Methoden entwickelt wurden. So ist es nicht überraschend, dass parallel von anderen Mitbewerbenden dieselbe Schwachstelle gefunden und ausgenutzt wird, an der man selbst arbeitet. Dann hoffen wir sehr, dass nicht wir das Zielsystem der anderen sind. Wir können uns nämlich nicht schützen, da der Einzige, der dies könnte, der Hersteller ist.

Insgesamt befassen sich viel zu viele Menschen mit großer Sorgfalt damit, Schwachstellen zu finden, um Exploits zu bauen, die Systeme zerstören können. Würden solche Ressourcen eingesetzt werden, um Systeme sicherer zu machen, wäre allen geholfen.

Legale Wege, gefundene Schwachstellen zu melden

Die Wahrheit ist aktuell, dass diejenigen, die sich an Hersteller wenden und Schwachstellen verantwortlich melden, kriminalisiert werden. Erst im Januar wurde ein Hacker von einem Jülicher Gericht verurteilt, weil er einem Online-Dienstleister 2021 eine Sicherheitslücke gemeldet hatte[1]. Edward Snowden musste 2013 aus den USA fliehen, nachdem er eine Vielzahl von illegalen Überwachungspraktiken und eine Vielzahl von bislang geheim gehaltenen Schwachstellen veröffentlicht hatte. Deshalb ist es an der Zeit, dass wir gemeinsam an dem Ziel arbeiten, dass es legale Wege gibt, Schwachstellen zu veröffentlichen.

Anmerkungen

1 *Michael Esser (2024): Anzeige statt Dank – Hacker soll 3.000 Euro zahlen. https://www1.wdr.de/nachrichten/rheinland/hacker-prozess-juelich-100.html*

Kai Nothdurft

Responsible Disclosure stärken, Geheimhaltung von Schwachstellen schwächen

Dieser Artikel greift die Ideen meines Pecha-Kucha-Vortrags auf der FIfF-Konferenz 2023 auf und führt die dort aufgrund der Kürze nur angerissenen Ideen detaillierter aus. Der Vortrag trug den Titel Responsible Disclosure *und stellte eine neue Initiative im Rahmen der Cyberpeace-Kampagne vor mit dem Ziel, Responsible Disclosure zu stärken und das Geheimhalten von Schwachstellen zu erschweren. Er baute auf den direkt davor gehaltenen Pecha-Kucha-Vortrag von Sylvia Johnigk zur Geheimhaltung von Zero-Day-Schwachstellen auf.*

Die Motivation für die Initiative ist, dass Responsible Disclosure nützlich und wichtig für die IT-Sicherheit ist, die eine notwendige Voraussetzung für das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist.[1] Deshalb ist es gesellschaftlich wünschenswert, Responsible Disclosure zu stärken.

Was versteht man unter „Responsible Disclosure“?

Responsible Disclosure (verantwortungsvolles Offenlegen, Veröffentlichen) bezieht sich auf einen Prozess, in welchem Sicherheitsschwachstellen in IT-Systemen derart veröffentlicht werden, dass dabei möglichst geringe Nebenwirkungen in Form von Sicherheitsrisiken entstehen. Eine Schwachstelle oder Sicherheitslücke in einem IT-System wird in der Regel durch einen Patch in Form eines Sicherheitsupdates des Herstellers des lückenhaften Systems geschlossen. Schwachstellen können in jeder Komponente von IT-Systemen vorhanden sein, in der Hardware, in der Plattform, den Schnittstellen, dem Betriebssystem oder der Anwendungssoftware.[2]

Verantwortungsvolles Veröffentlichen von Lücken

Wenn eine Sicherheitslücke entdeckt wird, ist ein wesentlicher Aspekt für die verantwortungsvolle Veröffentlichung dieser Lücke, die verantwortliche Stelle zu identifizieren und zu informieren. Dabei kann es sich je nach Situation um die Hersteller:innen, Produzent:innen, Entwickler:innen des Systems handeln oder wer auch immer sonst als verursachende Stelle für die Lücke verantwortlich war. Diese Stelle muss umgehend informiert werden, dass die Schwachstelle besteht und wie sie ausgenutzt werden kann, damit sie eine Lösung zur Behebung der Schwachstelle findet. Wichtig ist, ihr ausreichend Zeit zu geben, einen Patch zu entwickeln und zu testen. Die verantwortliche Stelle kann in der Regel am schnellsten das Problem beheben, das sie selbst verursacht hat.

Responsible Disclosure verlangt aber auch, nicht zu viel Zeit bis zur Veröffentlichung verstreichen zu lassen, da es durchaus sein kann, dass die Schwachstelle bereits einem kleinen Personenkreis bekannt ist oder in der Zeit bis zur Veröffentlichung von anderen ebenfalls entdeckt und missbraucht wird. Entscheidend ist also, der Stelle eine angemessene Frist zu geben, um den Patch zu erstellen. Je nach Komplexität der Behebung kann dieser Zeitraum unterschiedlich lang sein, er sollte aber eher wenige Wochen statt Monate oder gar Jahre umfassen. Je kritischer, also je gefährlicher die Lücke ist, desto kürzer sollte der Zeitraum sein.

Verantwortungslos wäre dagegen eine Veröffentlichung, wenn der Stelle überhaupt keine Zeit gelassen wird, einen Patch zu entwickeln, da die Schwachstelle dann schnell ausgenutzt werden kann, ohne dass die Anwender:innen sich angemessen schützen können. Hierzu gibt es allerdings eine Ausnahme. Wenn die Lücke nachweislich bereits von Angreifenden ausgenutzt wird, sollte die Veröffentlichung ohne Verzögerung erfolgen, um die Betroffenen und die Öffentlichkeit auf die Gefahr aufmerksam zu machen. Diese können auch ohne Patch zumindest risikomindernde oder -vermeidende Maßnahmen ergreifen, z. B. die betroffenen Systeme oder Funktionen zeitweise nicht mehr nutzen, deaktivieren oder sie isolieren, etwa vom Internet oder anderen Zugriffen trennen.

Idealerweise reagiert auch die Stelle verantwortungsvoll, stimmt sich mit den Personen, die die Schwachstelle entdeckt haben, ab und stellt möglichst schnell und zeitgleich mit der Veröffentlichung den Patch bereit, mit dem die Sicherheitslücke geschlossen werden kann. Damit endet die zeitliche Phase, die den Prozess des Responsible Disclose umfasst.

Nach der Veröffentlichung von Lücken

Nachdem die Sicherheitslücke veröffentlicht wurde, beginnt aus Risikosicht eine zweite Phase, in der die Schwachstelle bekannt ist, aber der Patch noch nicht in die betroffenen Systeme eingespielt wurde. Betreiber von Systemen wollen oft zunächst testen, dass der Sicherheitspatch den Betrieb nicht beeinträchtigt. Deshalb wird ein Patch insbesondere in größeren Organisationen auf vielen betroffenen Systemen nicht automatisch eingespielt. Automatische Update-Funktionen sind auch nicht auf allen Systemen herstellerseitig verfügbar. Daher kommt es häufig zu erheblichen Verzögerungen, bis ein Sicherheitsupdate in der Mehrzahl, erst recht auf fast allen der verwundbaren Systeme installiert wird. In dieser Phase sind die Systeme besonders vielen Angriffen ausgesetzt. Aus dem Patch kann, selbst wenn Details zur Schwachstelle nicht veröffentlicht werden, relativ einfach durch Reverse Engineering das Sicherheitsproblem und dessen Ausnutzung abgeleitet werden, die der Patch ja zielgerichtet behebt, aber damit leider auch deutliche Hinweise auf das Problem, und wie es ausgenutzt werden kann, offenbart. In einigen Fällen dauert es daher nur wenige Tage oder sogar Stunden, bis Exploitcode verfügbar ist, der die Schwachstelle für Angriffe ausnutzt. Die Reaktionszeit von der Veröffentlichung der Schwachstelle bis zum Einspielen des Patch ist zwar wesentlich dafür, bis wann das Risiko für das verwundbare System behoben ist. Diese Phase ist jedoch dem Responsible-Disclosure-Prozess nachgelagert und nicht mehr Teil davon, da sie ja erst mit der Veröffentlichung beginnt und von den Nutzer:innen abhängt.

Akteure und Interessen

Wer Schwachstellen verantwortungsvoll veröffentlicht, wird den Whitehats, den Sicherheitsforschenden und Hacker:innen mit guten Intentionen zugeordnet. Die Whitehats leisten einen großen Beitrag, Systeme sicherer zu machen, und dienen damit dem Allgemeinwohl. Sie sollten also unterstützt und gefördert werden.

Es gibt aber auch mehrere Akteure, denen die Veröffentlichung nicht gefällt und die z. T. über erhebliche Macht und Geldmittel verfügen und diese unter Umständen auch einsetzen, um die Veröffentlichung von Schwachstellen zu behindern und die Whitehats unter Druck zu setzen. Hersteller und Produzenten fürchten manchmal um ihre Reputation oder wollen mögliche Folgekosten, etwa Haftung oder auch nur den Aufwand für die Behebung einer Schwachstelle, vermeiden. Kriminelle und staatliche Sicherheitsbehörden wie Geheimdienste oder Strafverfolger nutzen Schwachstellen, um Systeme zu infiltrieren und Informationen zu exfiltrieren. Einige Schwachstellen werden militärisch als Cyberwaffen zur Spionage oder Sabotage in Exploits genutzt. Die einen verkaufen oder vermarkten Schwachstellen, andere kaufen oft Schwachstellen mit erheblichen Summen auf dem Schwarzmarkt ein. Wenn die Schwachstellen veröffentlicht und gepatcht werden, wird diese Investition wertlos.

Schwachstellen zu veröffentlichen ist daher bis zu einem gewissen Grad mit Whistleblowing vergleichbar und Menschen, die das tun, sollten wie Whistleblower vor Repressalien geschützt werden. Die Repressalien können u. a. Einschüchterung, Kriminalisierung, Unterlassungsklagen oder Schadensersatzforderungen umfassen. Aktuell ist die deutsche Rechtslage für Whitehats

problematisch, weil die Erforschung von Schwachstellen nach dem sogenannten Hackerparagraphen des Strafgesetzbuches (§ 202 a, b und c StGB) strafbar sein kann, selbst wenn sie eigentlich dazu dienen soll, die Systeme sicherer gegen solche Attacken zu machen.

Kampagne für Responsible Disclosure

Ich möchte deshalb eine Kampagne starten mit dem Ziel, Responsible Disclosure zu vereinfachen und das Verheimlichen von Schwachstellen zu erschweren.

Responsible Disclosure stärkt die IT-Sicherheit und damit das Grundrecht auf sichere IT-Systeme und sollte gefördert werden. Die Hersteller von IT-Systemen müssen motiviert werden, Schwachstellen in angemessener Zeit zu beheben. Die Öffentlichkeit kann sich, wenn das nicht geschieht, zumindest nach der Veröffentlichung selbst schützen, z. B. verwundbare Systeme nicht mehr nutzen. Schwachstellen geheim zu halten gefährdet die IT-Sicherheit in besonderem Maße, denn mit exklusivem Wissen um Schwachstellen sind Angriffe möglich, gegen die man sich nur sehr schwer schützen kann.

Die Kampagne soll für Responsbile Disclosure werben und über deren Sinn und Nutzen aufklären, um eine breite Öffentlichkeit für Unterstützung zu gewinnen. Neben der Werbung für Responsible Disclosure sollen auch konkrete Ideen und Forderungen entwickelt werden, die das Identifizieren und Veröffentlichen von Schwachstellen ermöglichen, erlauben oder sogar fördern und das Geheimhalten von Schwachstellen erschweren.

Für den Aufbau der Kampagne möchte ich in einem Kickoff die Organisation aufsetzen und erste Ideen sammeln:

- Festlegung, welche Technik und Tools genutzt werden
- Meetings und Aufgabenverteilung
- Suche nach Unterstützung durch weitere Menschen, Partner und Finanzierung
- Logo, Motto, Bündnispartner, Finanzierung

Themen zur Werbung für Responsible Disclosure sind z. B.:

- Wie kann das Thema aufbereitet und bekannt gemacht werden, um weitere Menschen von den Zielen zu überzeugen?
- Kreation von Kampagnenmotto und Logo
- Erstellung von Informationsmaterialien zu Responsible Disclosure

Folgende inhaltliche Fragen sollten im Kickoff behandelt werden:

- Welche Anforderungen stellen wir an rechtliche Regeln?
- Wie kann die Geheimhaltung von Schwachstellen erschwert werden?

Forderungen könnten z. B. in einer rechtlichen Absicherung und öffentlichen Förderung von Responsible Disclosure bestehen. Zur Unterstützung und zum Schutz der Veröffentlichenden braucht es Gesetze und Regeln anlog zu den Regeln für Whistleblower. Ein wichtiger Teilaspekt ist dabei die Legalisierung der Schwachstellensuche, also die rechtliche Absicherung von Menschen, die Schwachstellen entdecken und verantwortungsvoll veröffentlichen: Hacken mit Responsible Disclosure und dem Ziel, die Systeme sicherer zu machen, muss erlaubt sein.

Ab bestimmten Risikoschwellwerten sollten Hersteller verpflichtet werden, Bug-Bounty-Programme anzubieten. Bug Bounty ist eine organisierte Form, Hacker für ihre Hilfe zu entlohnen, indem man Belohnungen in Form von Geldbeträgen auslobt für die Meldung von Schwachstellen in ausgewählten Systemen. Ein rechtlicher Rahmen für Responsible Disclosure könnte eine Meldestelle umfassen sowie Fristen wie die Definition der Zeitspanne, die dem Hersteller für den Patch zugestanden wird, ab wann veröffentlicht werden darf. Um Geheimhaltung zu erschweren, könnte eine gesetzliche Pflicht zur Veröffentlichung von Schwachstellen eingeführt werden oder eine Haftung für Schäden aus der Geheimhaltung von Schwachstellen. Um den Markt auszutrocknen, könnte ein Verbot erlassen werden, 0-Day-Exploits zu handeln und zu exportieren.

Die Kampagne wird erfolgreich sein, wenn viele Menschen mitarbeiten und Ideen zur Umsetzung der Ziele entwickeln, damit wir Responsible Disclosure fördern und den gefährlichen Heimlichtuern etwas entgegen setzen.

Ihr könnt mich unter *kai@fiff.de* kontakten und Euch auf das FIfF-Wiki berechtigen lassen, um bei der Kampagne für Responsible Disclosure mitzumachen.

Das Kickoff fand online am 20. März 2024 um 19:00 Uhr statt.

Anmerkungen

1 *https://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html*

2 *Wenn ein erweiterter Systembegriff zu Grunde gelegt wird, bei dem das System auch das Umfeld der reinen Technik umfasst, können Sicherheitsschwachstellen auch in organisatorischen Prozessen, etwa der Administration oder dem Benutzerverhalten in Lieferketten, Bestellung oder Dekommissionierung stecken.*

Kai Nothdurft

Kai Nothdurft arbeitet als Information Security Officer in einer großen deutschen Versicherung. Seit 2009 ist Kai Nothdurft im Vorstand des FIfF e. V. aktiv. Seit Jahren hält er Vorträge und schreibt Artikel, die sich kritisch mit seinem Fachgebiet IT-Sicherheit beschäftigen.

Daniel Guagnin, Laura Kocksch, Basil Wiesse[1]

Für eine De-Militarisierung von Cybersicherheit

Perspektiven aus der Soziologie und den feministischen Science and Technology Studies (STS)

Konstante Cyberangriffe sind fast täglich medial präsent. Cyberkrieg, kriminelle Handlungen (wie Erpressung oder Diebstahl) sowie Spionage sind zu fast alltäglichen Vergehen im digitalen Raum geworden. Während militärische Narrationen von „Angriffen" dem Thema inhärent sind, ist es um ein Vielfaches schwerer, zahlreiche Strategien und Praktiken der „Verteidigung" ebenso linear zu beschreiben. Nutzer:innen, Administrator:innen oder Organisationen verhandeln mit kreativen, kollaborativen, situativen und deutlich mehr als technischen Strategien Cybersicherheit im Alltag.

In diesem Beitrag argumentieren wir daher dafür, Cybersicherheit nicht als bloße Opposition von Angriffen und Verteidigung zu verstehen, sondern vielmehr historische Entwicklungen, aktuelle politische Steuerungsversuche sowie konkrete alltägliche Praktiken zu nutzen, um Cybersicherheit neu zu interpretieren.

Nach einer Idee von Daniel Guagnin, Jan Magnus Nold
Gezeichnet von Erik Liebermann

Cybersicherheit ist bisher von militärischen, patriarchalen und hierarchischen Metaphern geprägt. Jedoch sind die allermeisten Organisationen, sowie die Gesellschaft insgesamt, nicht organisiert wie das Militär. Verantwortung und Sicherheit in demokratischen oder dezentralen Organisationsformen sind verteilt, fragmentiert, und Ambiguitäten müssen ausgehalten und debattiert werden. Mit einigen Reflexionen aus dem Bereich der Soziologie und den feministischen *science and technology studies* (STS) plädieren wir für de-militarisierte Cybersicherheit: Dies bedeutet nicht, dass jegliche „Cyberabwehr" eingestellt werden sollte, sondern, dass militärische und hierarchische Narrative in der Cybersicherheit eine Vielzahl von Alternativen unsichtbar gemacht haben.

In den folgenden drei Abschnitten und einer kurzen Konklusion argumentieren wir, dass Ansätze aus der Soziologie und den STS über die bloße Erforschung von Nutzer:innenpraktiken und „Usable Security" hinausgehen sollten. Im ersten Abschnitt skizzieren wir *genealogisch* die Verflechtung militärischer und kybernetischer Grundhaltungen, die das aktuelle Verständnis von Cybersicherheit mehrheitlich informieren. Im zweiten analysieren wir die *aktuelle* Dominanz paternalistischer Narrative der offensiven Cybersicherheit. Der letzte Abschnitt argumentiert basierend auf *qualitativ-ethnographischen Beobachtungen* in klein- und mittelständischen Unternehmen (KMUs), dass Cybersicherheit im Alltag oft mehr Fürsorge als Abschottung und verteilte Verantwortung im Gegensatz zu Moralisierungen beinhaltet. Militärische Narrationen können im schlimmsten Fall solch lokale und kreative Praktiken demotivieren. Vielmehr braucht es aber konkrete Gelegenheiten, solch „gute" lokale Gründe für „schlechte" Cybersicherheit zu diskutieren und fördern. Der Artikel schließt mit einigen Fragen, wie Cybersicherheit in Zukunft betrachtet, integriert und beforscht werden könnte.

Historische Einbettung in Kybernetisierung: Eine kleine Genealogie kybernetisch-militaristischer Schemata und ihrer Kritik

Dass das Internet mit ARPANET eine militärische Vorgeschichte hat, ist hinlänglich bekannt. Dies gilt nun gerade auch für Cybersicherheit, nicht nur mit Blick auf die lange Geschichte der Kryptographie (vgl. Dooley 2018), sondern auch in umfassenderer und arbeitspraktischer Verzahnung. Militär- und Rüstungsindustrie sind eine wichtige Zielgruppe für Anbieter von Cybersicherheits-Lösungen und führen zu nachhaltigen militärisch-zivilen Kooperationen. In den USA ist hier insbesondere die pentagon-nahe, 1958 gegründete MITRE Corporation zu nennen.[2] In Deutschland arbeitet der Cyber- und Informationsraum der Bundeswehr nach eigenen Angaben mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie mit vielen anderen Institutionen, Unternehmen und Hochschulen, zum Beispiel der Deutschen Telekom, dem Fraunhofer Institut und dem BITKOM zusammen.[3] Vor dem Hintergrund verstärkt kommunizierter Bedrohungsszenarien durch Cyberangriffe auf öffentliche Infrastrukture, wie jüngst auf 70 Kommunen in Nordrhein-Westfalen im Oktober 2023 ist mit weiterer gesellschaftlicher Akzeptanz und Vertiefung militärisch-ziviler Kooperationen im Bereich Cybersicherheit zu rechnen.

Für die Verträglichkeit militärischer und ziviler Cybersicherheit sorgen nicht allein Sachzwänge. Ebenso wichtig sind gemeinsame Sprech- und Denkmittel, wie sie insbesondere von der Kybernetik der Nachkriegszeit geprägt und kodifiziert worden sind. Das betrifft insbesondere die Denkfigur einer Leitunterscheidung zwischen System und Umwelt, im Sicherheitskontext das zu schützende und kontrollierende System und die potenziell existenzbedrohliche, systemkompromittierende (entropische) Umwelt (vgl. Wiener 1954: 28-48). Diese Leitunterscheidung bildet eine fortlaufende praktische Aufforderung der Bearbeitung der Durchlässigkeit von Systemgrenzen (z. B. als *vulnerabilities*), die Abschät-

zung von Gefährdungen (*threats*) und die Verhinderung und Eindämmung von Unterbrechungen des operativen Systemvollzugs (*attacks*) durch andere Systeme (*actors*) (vgl. Kelly 2013).

Ursprünglich ins Leben gerufen als interdisziplinäre Wissenschaft der autonomen Regulierung von Systemen jedweder Art war die Kybernetik mit dem Versprechen ihrer gezielten Steuerung (altgr. *κυβερνάω*, ich steuere) von Anfang an begleitet und gefördert durch militärische Interessen.[4] Sie war eine wichtige theoretische Belebung für *Operations Research* (vgl. Beer 1959), das im zweiten Weltkrieg von der Royal Air Force zur Planung von Angriffszielen eingesetzt wurde (und heute in nahezu allen Bereichen, in denen „analytics" eine Rolle spielen, eingesetzt wird) (vgl. Dekeyser/Culp 2022). Im Kalten Krieg war die Kybernetik sowohl von US-amerikanischer als auch sowjetischer Seite Gegenstand von politischen Projektionen, Träumen und Ängsten, die zunehmend antagonistisch wurden: „Hatte Wiener noch die Vision, dass die Regulierung durch Rückkopplungen eine stabile, friedliche und demokratische Welt schaffen könne, so ließen die kybernetischen Ideen im Kalten Krieg bald Phantasien von zentralisierten, automatisierten, sich selbst steuernden, intelligenten Waffen aufblühen" (Gerovitch 2009: 55).

Menschliche Systembestandteile sind aus solchen Vorstellungen nicht wegzudenken; so ist schließlich aktuell eine der zentralsten Fragen für Cybersicherheit das Management der *human question*, der Gefahr durch *social engineering* und menschliche Unachtsamkeit (vgl. Anderson & Stajano 2010). Gerade an der Schnittstelle technischer und biologischer wie auch sozialer Systeme entzündet sich bis heute Kritik. Joseph Weizenbaum bezeichnete die Idee eines technisch-neuronalen Interface als „Angriff auf das Leben an sich" (Weizenbaum 1978: 351; vgl. auch Weizenbaum 2001: 104-119). 1956 kritisierte der französische Philosoph Gilbert Simondon eindringlich das Technikverständnis der Kybernetik, insbesondere ihr homöostatisches Ideal (vgl. Simondon 2012). In den 1970ern entbrannte mit der *Habermas-Luhmann-Kontroverse* eine heftige Debatte um die gesellschaftspolitischen Implikationen der Kybernetik, um die Konsequenzen der Annahme (und Wünschenswertheit) von sozialer Steuerbarkeit (vgl. Habermas/Luhmann 1971). Ein Jahrzehnt später verübte die französische Gruppe CLODO Angriffe auf Technologiekonzerne, die an militärischen Projekten beteiligt waren (vgl. David 2020, Dekeyser/Culp 2022). 1990 formulierte Gilles Deleuze sein „Postskriptum über die Kontrollgesellschaften" (Deleuze 1993), in welchen Machtverhältnisse von den Teilnehmer:innen in systemimmanente Prozesse verlagert werden. 2001 schließlich erschien *The Cybernetic Hypothesis* des Kollektivs Tiqqun, in der Kybernetik, Deleuze aufgreifend, als „warfare directed against all that lives and all that lasts for a time" beschrieben wird (Tiqqun 2020: 32).

Unter dem Stichwort *de-perimeterisation* wurde Anfang der 2000er durch das Jericho-Forum das vorherrschende System-Umwelt-Modell von Sicherheit aus dem Feld der Cybersecurity selbst heraus in Frage gestellt (vgl. Spencer/Pizio 2023): Sicherheit solle sich nicht lediglich auf die Sicherung von Systemgrenzen beschränken, da es nur ihre einmalige Überwindung zur Systemkompromittierung bräuchte. Cybersecurity solle stattdessen in umfassende Protokolle, Techniken, Praktiken diffundiert werden. Dem Jericho-Forum ging es also keineswegs um eine Kritik am zugrundeliegenden kybernetischen Prinzip, sondern vielmehr um ihre Ausweitung und Vervielfältigung. Mit dem Ergebnis ihrer Bemühungen, dem *zero trust security model*, werden etwaige praktische Freiräume (die „brauchbare Illegalität"; Kühl 2020) nun auch innerhalb von Organisationen aufgehoben, und – wie von Deleuze antizipiert – auf eine Vielzahl von Kontrollmechanismen ausgeweitet. In *zero trust* werden auch die Nutzer:innen Teil der (risikobehafteten, nicht zu vertrauenden) Umwelt und müssen fortlaufender Beobachtung und Prüfung unterzogen werden, um am Systemvollzug teilnehmen zu können.

Hier lassen sich die Kritiken an der Kybernetik wieder aufgreifen, sie formuliere den konstruktivistischen Gedanken, dass Gesellschaften, wenn sie lange genug als System behandelt werden, sich früher oder später auch systemisch verhalten. Die Ausdehnung von Cybersicherheit in alltägliche Praktiken erscheint für diese Entwicklung dann konstitutiv. Mit der zivilgesellschaftlichen Ausweitung ursprünglich militärischer Sicherheitsbelange und damit verbundenen sicherheitspraktischen Anforderungen verbreiten sich kybernetischen Wahrnehmungs- und Beurteilungsschemata. Es sollte die Möglichkeit in Betracht gezogen werden, dass diese sich dabei, mit dem französischen Soziologen Pierre Bourdieu gesprochen, als kybernetische Dispositionen zu einem kybernetischen Habitus als gemeinsam geteilte Grundhaltung verdichten (vgl. Bourdieu 1993). Angesichts ihres militärischen Hintergrunds ist nicht auszuschließen, dass auch in der Zivilbevölkerung verbreitete soldatische Männlichkeitsideale (Theweleit 2019) und weitere Merkmale männlicher Herrschaft (Bourdieu 2012) dieser kybernetischen Sozialisation einen fruchtbaren Boden bereiten.

Paternalismus aktueller Steuerungsversuche

Im sicherheitspolitischen Kontext findet sich denn auch ein dezidiert männlich konnotierter Paternalismus offensiver Sicherheitsstrategien, während das Sich-kümmern und Instandhalten im Sinne einer defensiven Sicherheitsstrategie analog zur mangelnden Wertschätzung weiblich attribuierter Fürsorgetätigkeiten vernachlässigt wird.

Im Folgenden geht es um die Gegenüberstellung von offensiven und defensiven Sicherheitsstrategien im aktuellen politischen und technischen Diskurs zu Cybersicherheit. Dies basiert auf Beobachtungen des sicherheitspolitischen Feldes und der damit verbundenen Diskurse – bei denen auch das FIfF in Form von Stellungnahmen und offenen Briefen beteiligt war.

Der wesentliche Zwiespalt in der Diskussion besteht darin, einerseits im Sinne der Bekämpfung Organisierter Kriminalität eine Überwachung der Kommunikation von Bürger:innen grundsätzlich zu ermöglichen, andererseits diese auf der technischen Ebene weitreichend zu schützen, zur Verhinderung unautorisierter Zugriffe und Angriffe, gemäß der drei Schutzziele der IT-Sicherheit Vertraulichkeit, Integrität und Verfügbarkeit zu bieten – im Grunde ein Zielkonflikt zwischen Repression und Prävention. Kurz und prägnant zeigt sich dieser Widerspruch in der fragwürdigen politischen Forderung von „Sicherheit durch und trotz Verschlüsselung", wie sie in verschiedenen politischen Dokumenten gefordert wurde.[5]

Der Ansatz, Bürger:innen durch die grundsätzliche Zugriffsmöglichkeit auf ihre Kommunikationen zu beschützen, trägt paternalistische Züge im Sinne einer bevormundenden Beziehung

zwischen Regierenden einerseits und den von ihnen regierten Menschen andererseits. Verwiesen wird hierbei meist durch Sicherheitsbehörden auf das Problem eines „going dark" der Organisierten Kriminalität, die die Sicherheitsbehörden machtlos zurücklassen würde.[6]

Der propagierte Lösungsansatz fokussiert dabei auf den Zugriff von Geräten oder Kommunikationspunkten auf dem Weg dazwischen, etwa in der Verschlüsselungsthematik über einen unverschlüsselten Zugriff an bestimmten Knotenpunkten, beispielsweise zentrale Netzknoten (CITRIS), direkt bei den Betreiber:innen der Kommunikationsdienste[7] oder direkt auf den Geräten.[8]

Die politischen Narrative der Befürworter einer offensiven und repressiven Sicherheitsstrategie erklären den Widerspruch von Verschlüsselung aufzulösen als Überwachungsproblem und Sicherheitslösung aufzulösen durch das Postulat „Sicherheit trotz und durch Verschlüsselung". Dem gegenüber steht der Anspruch einer defensiven Sicherheit, die auf technischer Integrität beruht.[9] Dies entspricht einer Strategie der Fürsorge, die, statt Angriffspunkte vorzuhalten oder gesetzlich bei Dienstleistern zu fordern, Rahmenbedingungen und Ressourcen für eine umfassende technische Sicherheit schafft und permanentes Suchen und Schließen von Sicherheitslücken ermöglicht. Dies nützt allen – auch potentiellen politischen Gegnern – für eine sichere technische Infrastruktur.

Zwei gesellschaftspolitische Kritikpunkte des paternalistischen Ansatzes wollen wir in Kürze hier ausführen.

Einerseits unterliegt einem paternalistischen Sicherheitsverständnis das Narrativ, dass unbescholtene Bürger:innen nichts zu verbergen hätten, was aus verschiedenen Gründen problematisch ist. Das Recht auf Geheimnisse und Privatsphäre, und somit Wahrung individueller Freiheiten, wird damit delegitimiert. Die Kriminalisierung jeglicher Geheimnisse ist gleichermaßen ein Akt symbolischer Gewalt (vgl. Rehbein 2006: 189f.) in dem Sinne, dass damit eine Norm gesetzt und als selbstverständlich gesetzt wird – vergleichbar auch mit dem Paradigma des Zero Trust (siehe oben). Wichtiger noch, die Basis für einen freimütigen Austausch von persönlichen und politischen Ansichten bedarf geschützter Räume. Die politischen Rahmenbedingungen des Sagbaren und politisch Gewollten wandeln sich, dabei muss eine kritische Diskussion – auch im Rahmen der aktuell geltenden Gesetze – unbeobachtet möglich sein. Darüber hinaus ändern sich auch die Rechtsregime, wie wir in Anbetracht der Konjunkturen autoritärer Regierungen wiederholt feststellen müssen. Wo sich die rechtlichen Grenzen verschieben und legitime Staatskritik sowie freie Informationen kriminalisiert werden[10], ermöglichen technische Zugriffsmöglichkeiten auf die Kommunikation von Bürger:innen Massenüberwachung und Unterdrückung oppositioneller Gruppen.

Die Grenzen der Anwendung von Überwachungstechnik werden regelmäßig ausgeweitet. Ungeachtet des politischen Charakters des Begriffs Terrorismus, der auf eine Bandbreite von harmlosem zivilen Widerstand der letzten Generation[11] bis hin zu Menschenrechtsaktivismus angewandt wird, werden die Strafkataloge, auf die geheimdienstliche Methoden ausgeübt werden dürfen, stetig erweitert: Technologien, die nur zu einem bestimmten (engen) Zweck eingeführt werden, finden immer weitreichendere Anwendungsfelder (vgl. Koops 2021).[12] Dieser freiheitsrechtlichen Argumentation wird gerne die Notwendigkeit der Ermöglichung effektiver Strafverfolgung gegenübergestellt.

Andererseits verkennt die Idee einer zielgerichteten technischen Überwachung die technischen Grundlagen derselben und der damit verbundenen (Un-)Sicherheit.

Externe Zugriffsmöglichkeiten auf Informationstechnik lassen sich – technisch betrachtet – kaum auf staatlich legitimierte Akteure beschränken (vgl. Rehak 2014: 56ff). Sie basieren auf Sicherheitslücken, deren Ausnutzung folglich auch durch Kriminelle oder Geheimdienste anderer Staaten erfolgt (vgl. Singelnstein et al. 2018). Zudem setzt die politische Ausrichtung auf Überwachungsschnittstellen Anreize zum Vorhalten von Sicherheitslücken und stärkt schlimmstenfalls illegale Märkte, auf denen diese vertrieben werden. Selbst wenn nicht Kommunikationsprotokolle oder Endgeräte durch die Ausnutzung von Schwachstellen überwacht werden, bieten die an der Kommunikation beteiligten Knotenpunkte mögliche Angriffsvektoren, beispielsweise die Server der Diensteanbieter.

Zusammengefasst unterminieren der technischen Diskurse zufolge zusätzliche Zugriffspunkte die mathematisch-technische Sicherheit einer „Ende-zu-Ende-Verschlüsselung". An einer Stelle zwischen Absender und Adressat (der beiden Endpunkte) erfolgt unbemerkt Zugriff, womit (mindestens) ein Angriffspunkt geschaffen wird, der nur sehr bedingt kontrolliert werden kann: Jenseits der organisatorischen Schwierigkeiten, die im Grunde mit dem ersten Argument zusammen laufen (die Bewertung der Legitimität der Inhalte ist politisch), geht es an dieser Stelle um ein technisches Argument entlang Murphy's Law: Ist eine Verschlüsselung nicht von Ende zu Ende (Adressat zu Empfänger) technisch einwandfrei möglich und dort an den Endpunkten jeweils auf einem vertraulichen Gerät, werden Schnittstellen, Schwachstellen, Zugriffsmöglichkeit im Zweifelsfall von Dritten genutzt. Dritte sind hierbei insbesondere Akteure außerhalb der legitimierten Organisationen (Dienstleister und Sicherheitsbehörden), die also nicht ihre Zugriffsrechte ge- bzw. missbrauchen, sondern die sich vielmehr unrechtmäßig Zugriff verschaffen und Inhalte kopieren (Vertraulichkeit), manipulieren (Integrität) oder entziehen (Verfügbarkeit). Anders als der zuvor beschriebene organisatorische Zugriff, der durch die Organisationsstruktur grundsätzlich sanktioniert werden kann, bieten technische Schwachstellen weitreichende Angriffsmöglichkeiten, die oftmals lange unerkannt bleiben. Traurige Berühmtheit erlangte bspw. die Ransomware *WannaCry*, die auf einer der NSA lange bekannten Sicherheitslücke in MS Windows beruhte, und die auch nach öffentlicher Bekanntwerdung weiter ausgenutzt wurde und weitreichende Schäden anrichtete, nicht zuletzt in Teilen der kritischen Infrastruktur (vgl. auch Singelnstein et al. 2018). Heute verursachen Ransomware-Attacken wirtschaftliche Schäden in Milliardenhöhe.[13]

Einerseits gibt es also die paternalistische Argumentation einer – mit Foucault (1993) gesprochen – überwachenden und strafenden Sicherheitslogik, die auf offensive Sicherheitsstrategien fokussiert, indem integere Verschlüsselung als Problem geframed wird („going dark"/„Sicherheit trotz Verschlüsselung") und auch im Hinblick auf die internationale Cybersicherheit Gegenangriffsmaßnahmen gefordert werden („Hackback", „aktive Cyberabwehr", „Cyberverteidigung", „Gefahrenabwehr").[14] Im Zuge ihrer immer umfassenderen Ausdehnung und veralltäglichender

Diffusion, wie sie bei *zero trust* beobachtet werden kann, präsentiert sich Deleuzes Warnung vor den sich herausbildenden Kontrollgesellschaften hier gleichsam als handfeste sicherheitspolitische Forderung. Dieser Argumentation steht andererseits eine Sicherheitslogik der technischen Integrität gegenüber, die zum Ziel hat, jegliche Angriffspunkte der technischen Infrastruktur zu vermeiden: eine Infrastruktur, die sich allerlei Akteure und damit auch potentielle Gegner teilen, insbesondere in einer globalisierten Welt monopolistischer Monokulturen.

Die kritische technische Community hält wiederholt dagegen in offenen Briefen und kritischen Stellungnahmen.[15] Punktuell bilden sich sogar Allianzen von Chaos Computer Club bis Google, indem einhellig eine Sicherheitsstrategie gefordert wird, die eben gerade nicht Angriffspunkte für staatlichen Zugriff etabliert, die von illegitimen Dritten genutzt werden können. Zumal durch ein staatliches Vorhalten von Sicherheitslücken schlimmstenfalls der illegale Handel mit Sicherheitslücken gestützt wird, der ohnehin für ein konstruktives Sicherheitsregime falsche Anreize setzt, gefundene Sicherheitslücken teuer zu verkaufen, anstatt sie zu melden (und dafür ggf. eine Anklage vom Betreiber oder Hersteller der Software zu erhalten).[16]

Im Kontrast zum „männlich" konnotierten Angriff der offensiven Sicherheitsstrategie stellt der defensive Sicherheitsansatz eine „weiblich" attribuierte Perspektive des Kümmerns und Instandhaltens dar. Da großteils auch neutrale und gar gegnerische Parteien dieselbe Software nutzen, wäre es durchaus sinnvoll, gemeinsam in das Finden und Schließen von Angriffspunkten zu investieren. Die gezielte Suche ist sehr aufwändig, aber ein konsequentes und schnelles Schließen von Sicherheitslücken stellt eine nachhaltige und effektive Sicherheitsstrategie dar, in der alle Parteien von jeder Aktivität Einzelner profitieren, und der größte Angriffsvektor Organisierter Kriminialität so auf technische Weise bekämpft wird.

Fairerweise muss man benennen, dass es in der aktuellen Legislatur auch andere politische Bestrebungen gibt. Neben aktuellen, auch europaweiten Gesetzesvorhaben wie der *Cyber Resilience Act* stellt insbesondere der *Sovereign Tech Fund* ein bemerkenswertes Programm dar. Hierbei werden nationale Mittel verwendet, um Freie Open Source Software zu verbessern, die international verwendet werden, und somit wird nachhaltig und supranational Cyber-Fürsorge-Arbeit geleistet.

Zuletzt wollen wir uns noch den Fürsorgepraktiken in den Unternehmen zuwenden.

Mit Unsicherheit leben. Ethnographische Einblicke in Fürsorge und Instandhaltung in KMUs

„Please don't judge!" (beim Eintippen des Passworts „12345")
„We tidied up before you arrived" (beim Zeigen von Ordnerstrukturen)

Zitate wie diese deuten auf die ständige Moralisierung von Cybersicherheit durch Expert:innen und mediale Diskurse hin. Während einer der größten qualitativen Studien zu Cybersicherheit im Alltag von kleinen und mittelständischen Unternehmen (KMUs) haben wir zahlreiche solcher Reaktionen erfahren. KMUs fühlten sich „erwischt" von der Ethnografin, die sie für einige Tage besucht und ihre Praktiken und Routinen beobachtet hat. KMUs sind es gewohnt, dass Cybersicherheitsexpert:innen anklagen, sie seien ahnungslos, ihnen fehle es an Fähigkeiten oder gutem Willen, bessere Cybersicherheitsmaßnahmen durchzusetzen.

Im Alltag von Blumenläden, Anwaltskanzleien, Druckereien oder Logistikunternehmen ist Cybersicherheit selten schwarz-weiß. Im Gegensatz zur Behauptung, KMUs seien ahnungslos oder willenlos, zeigten uns Unternehmen ihre praktischen Dilemmata und bewiesen vielzählige alltägliche Maßnahmen, die über offizielle Sicherheitsstrategien hinausgingen. Cybersicherheit ist dabei manchmal nur teilweise möglich oder nötig, wird vertagt und fortlaufend diskutiert. Es ergeben sich Grauzonen, wo Sicherheit weder ignoriert noch offiziellen Maßnahmen eins-zu-eins gefolgt wird.

Geprägt von feministischen *science and technology studies* (STS) plädieren wir in unserer Arbeit dafür, die praktischen Dilemmata von KMUs ernst zu nehmen und so Cybersicherheit weniger als striktes Regelwerk und stärker als andauernden und oft kompromissbehafteten Prozess zu verstehen.

Anders ausgedrückt zeigt sich Cybersicherheit in der Praxis als gezieltes Balancieren von sozialen Beziehungen, technischer Agency und alltäglicher Praxis. Es ergeben sich imperfekte und improvisierte Lösungversuche, denen durch dauerhafte *response-ability* und nicht durch entfernte Beurteilung begegnet wird. Cybersicherheit ist ambivalenter und „messier". KMUs ringen nicht mit technischen Lösungen, sondern bearbeiten Cybersicherheit durch Fürsorge für Technologien und die sozialen Beziehungen, an denen sie teilnehmen. Im Alltag von KMUs wird Cybersicherheit nicht kontrolliert oder gelöst, sie wird verhandelt, ausbalanciert und verbleibt partiell. Es ist kein romantisierendes Bild von fürsorglichen KMUs, das so entsteht. Im Gegenteil, für sozio-technische Beziehungen zu sorgen ist lokal kontestiert, umfasst unangenehme Entscheidungen und Spannungen.

Zu behaupten, KMUs mangele es an Bewusstsein oder Willen, trägt zur maskulinisierten Moralisierung von Cybersicherheit als rationale Entscheidung bei, während mit Unsicherheiten zu leben, Ambivalenzen zu tolerien und kollektiv zu reagieren fürsorglichen Logiken entspricht (vgl. Tronto/Fisher 1990, Mol 2008). Vergleichbar mit Ärzt:innen und Pflegekräften, die für Patient:innen kodifiziertes und standardisiertes medizinisches Wissen in konkrete, dem Alltag angepasste, jedoch medizinisch unvollständige Ratschläge übersetzen müssen, muss Cybersicherheit in der Praxis als „gut-genug" oder „bestmöglich" verstanden werden (vgl. Kocksch et al. 2018). Was „gute" Cybersicherheit lokal bedeutet, ist kaum abstrakt zu evaluieren (vgl. Kocksch/Elgaard Jensen 2023).

„We would like to be more secure,
but that would be chaos in the everyday"
(Logistikunternehmen mit ungesicherten Computerterminals im Ladebereich)

Cybersicherheit als Toleranz von Grauzonen, unvollkommenen und temporären Lösungen und Praktiken der Instandhaltung im Gegensatz zu Fortschritt und Innovation zu verstehen hat politische Konsequenzen: Cybersicherheit ist nicht nur dramatisch, militärisch und bedrohlich, sie ist lokal, privat und ambivalent. KMUs begegnen praktischen Dilemmata und Realitäten.

Aus bestehenden und dominanten militärischen Sicherheitsnarrativen entsteht dabei Peinlichkeit und Scham. Es braucht mehr Räume, um imperfekte Sicherheit zu besprechen. Moralisierende Diskurse haben den Effekt, dass KMUs ihre Praktiken verstecken, da sie keine Legitimation für partielle Sicherheit sehen.

Wir können von KMUs lernen, wie gekonnt und kollektiv mit (partieller) Unsicherheit gelebt wird und so eine andere Konversation über Sicherheit beginnen. Teil dessen ist, dass wir aufhören, KMUs anzuklagen oder zu verurteilen, und ihre lokalen Dilemmata, Improvisationsarbeit und verteilte Fürsorge verstehen. Cybersicherheit erscheint dann nicht als militärische Verteidigungsstrategie, sondern als andauernde, verteilte Fürsorge für Technologien und die sozialen Beziehungen, die sie ermöglichen.

Wie de-militarisieren wir Cybersicherheit?

In diesem Artikel haben wir Cybersicherheit mit drei Heuristiken aus Soziologie und STS reflektiert: genealogisch, diskursanalytisch und ethnographisch. Wir haben dabei gezeigt, dass soziologische Betrachtungen der Cybersicherheit dazu beitragen können, dominante und subversive Narrative und Praktiken der Cybersicherheit zu identifizieren, und haben auf einige alternative Denk- und Praxisfelder hingewiesen.

Die von uns beschriebenen Praktiken der Kritik (vgl. Boltanski 2008) – ob an antizipierten Folgen der Kybernetik, an paternalistischen Steuerungsansätzen oder in der praktisch notwendigen Abweichung von Sicherheitsstandards – sollten deutlich gemacht haben, dass eine de-militarisierte Cybersicherheit denkbar und vor allem auch notwendig ist. Die bisher unreflektierte Kontinuität militärischer und paternalistischer Cybersicherheitsdefinitionen ist nicht nur unrealisitisch, sondern politisch und praktisch konsequenzenreich. Cybersicherheit ist mehr als das Spannungsfeld zwischen Angriffen und Verteidigung. Andere Formen sind denkbar: Formen, die sich weniger auf die Etablierung und Aufrechterhaltung einer übergreifenden organisatorischen (Befehls-) Ordnung beziehen, und sich mehr an den historischen und diskursiven Pfadabhängigkeiten und ihren Effekten für konkrete praktische Anforderungen, Gegebenheiten und Verknüpfungen von Teilnehmer:innen im Feld der Cybersicherheit orientieren.

Hieraus ergeben sich weiterführende Herausforderungen und Fragen, von denen wir abschließend einige aufwerfen möchten: Wie konfliktträchtig gestalten sich Praktiken der Cybersicherheit jenseits radikal antagonistischer Freund-Feind-Schemata, auch oder gerade im Zuge von Fürsorge-Logiken? Wie können wir Räume schaffen, um ambivalente und kompromisshafte Cybersicherheit zu diskutieren? Wie verhandeln wir (Expert:innen) Sicherheit anders als paternalistischer Rettungsversuch? Wann und wo genau wird sich auf weiterführende, auch gesellschaftspolitische Selbstverortungen gestützt? Und dort insbesondere nicht nur negativ, wie wir beobachten konnten, in schambesetzter Abweichung von herangetragenen Normierungen und Disziplinierungen, sondern auch beispielsweise in ihrer infrastrukturellen Einbettung zur fortlaufenden Ermöglichung der Bedingungen technologisch gestützter Kooperations- und Kommunikationsarbeit? Diese und weitere Fragen gilt es aus unserer Sicht kritisch und theoretisch reflektiert, ohne militärisch-moralische Aufladung *a priori* zu untersuchen, zur Sprache zu bringen und zu diskutieren.

Referenzen

Anderson, Ross & Stajano, Frank (2014): It's the Anthropology, Stupid!, in: Christianson, Bruce & Malcolm, James (Hrsg.), Security Protocols XVIII. Berlin: Springer, S. 137-140.

Beer, Stafford (1959): What has Cybernetics to do with Operational Research?, OR 10, Nr. 1: 1–21.

Boltanski, Luc (2010): Soziologie und Sozialkritik, Berlin: Suhrkamp.

Bourdieu, Pierre (1993): Sozialer Sinn. Kritik der theoretischen Vernunft, Frankfurt/Main: Suhrkamp.

Bourdieu, Pierre (2012): Die männliche Herrschaft, Frankfurt/Main: Suhrkamp.

David, Christophe (2020): Rage against the Machines. Notes sur l'affect antitechnologique. Écologie & politique, 2020/2, 117-136.

Dekeyser, Thomas & Culp, Andrew (2022): Machines in Flames. Destructionist International. https://www.youtube.com/watch?v=qGVMu5OPu7E. (abgerufen am 29.01.2024)

Deleuze, Gilles (1993): Postskriptum über die Kontrollgesellschaften, in: Unterhandlungen 1972-1990, Frankfurt/Main: Suhrkamp, 254–262.

Dooley, John F (2018): History of Cryptography and Cryptanalysis. Codes, Ciphers, and Their Algorithms, Cham: Springer.

Foucault, Michel (1993): Überwachen und Strafen. Die Geburt des Gefängnisses, Frankfurt/Main: Suhrkamp.

Gerovitch, Slav (2009): Die Beherrschung der Welt: Die Kybernetik im Kalten Krieg, Osteuropa 59, Nr. 10, 43–56.

Habermas, Jürgen & Luhmann, Niklas (1971): Theorie der Gesellschaft oder Sozialtechnologie, Frankfurt/Main: Suhrkamp.

Kelly, Max (2013): Perspectives in Cybersecurity and Cyberwarfare. DEF CON 18 Keynote, Las Vegas. https://defcon.org/html/links/dc-archives/dc-18-archive.html#Keynote (abgerufen: 02.11.2023).

Kocksch, Laura & Elgaard Jensen, Torben (2023): „Good" Organizational Reasons for „Bad" Cybersecurity: Ethnographic Study of 30 Danish SMEs, Aalborg Universitet.

Kocksch, Laura, Korn, Matthias, Poller, Andreas & Susann Wagenknecht (2018): Caring for IT Security: Accountabilities, Moralities, and Oscillations in IT Security Practices, in: Proceedings of the ACM on Human-Computer Interaction, Volume 2, Issue CSCW, Article 92, 1-20.

Koops, Bert-Jaap (2021): The Concept of Function Creep, in: Law, Innovation and Technology 13, Nr. 1, 29–56.

Kühl, Stefan (2020): Brauchbare Illegalität. Vom Nutzen des Regelbruchs in Organisationen, Frankfurt/Main: Campus.

Lipner, Steven B. (2018): The Birth and Death of the Orange Book, in: IEEE Annals of the History of Computing 37, Nr. 2, 19–31.

Marx, Gary T. (1990): Undercover: Police Surveillance in America, University of California Press.

Mol, Annemarie (2008): The Logic of Care, London: Routledge.

Rehak, Rainer (2014): Angezapft – Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung, Master's Thesis, Humboldt-Universität zu Berlin.

Rehbein, Boike (2006): Die Soziologie Pierre Bourdieus, 1. Aufl., Utb.

Simondon, Gilbert (2012): Die Existenzweise technischer Objekte, Zürich: Diaphanes.

Spencer, Matt & Pizio, Daniele (2023): The De-Perimeterisation of Information Security: The Jericho Forum, Zero Trust, and Narrativity, Social Studies of Science Online First.

Theweleit, Klaus (2019): Männerphantasien, Berlin: Matthes & Seitz.

Tiqqun (2020): The Cybernetic Hypothesis, South Pasadena, CA: Semiotext(e).

Tronto, Joan C. & Fisher, Berenice (1990): Toward a Feminist Theory of Caring, in: Abel, Emily K. & Nelson, Margaret K., Circles of Care, SUNY Press, 36-54.

Singelnstein et al. (2018): Verfassungsbeschwerde § 23b Abs. 2 Polizeigesetz Baden-Württemberg (PolG BW) in der Fassung des Gesetzes zur Änderung des Polizeigesetzes vom 28.11.2017, GBl. S. 624. https://legacy.freiheitsrechte.org/home/wp-content/uploads/2018/12/2018-12-07_VB_PolG-BaWue_final_anonym.pdf. (abgerufen am 29.01.2024)

Weizenbaum, Joseph (1978): Die Macht der Computer und die Ohnmacht der Vernunft, Frankfurt/Main: Suhrkamp.

Weizenbaum, Joseph (2001): Computermacht und Gesellschaft, Frankfurt/Main: Suhrkamp.

Wiener, Norbert (1954): The Human Use of Human Beings. Cybernetics and Society, Boston: Houghton Mifflin.

Wiener, Norbert (1966): God & Golem, Inc: A Comment on Certain Points Where Cybernetics Impinges on Religion, Cambridge, MA: MIT Press.

Anmerkungen

1 *Die Autor:innen sind in alphabetischer Reihenfolge genannt und haben zu gleichen Teilen zum Artikel beigetragen.*

2 *MITRE Corp. kuratiert seit 1999 die Liste der Common Vulnerabilities and Exposures (CVE), seit 2006 die Common Weakness Enumeration (CWE), und betreibt seit 2013 mit dem „MITRE ATT&CK framework" eine öffentliche Datenbank von Cybersicherheits-Angriffsvektoren (https://www.mitre.org/who-we-are/our-story; https://cwe.mitre.org/about/history.html). Ebenfalls unter Mitwirkung von MITRE entstand das sogenannte „Orange Book", die Trusted Computer System Evaluation Criteria (TCSEC) des US-amerikanischen Verteidigungsministeriums, aus denen der Common Criteria-Standard zur IT-Sicherheitsbewertung hervorging (vgl. Lipner 2015).*

3 *https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/auftrag/zusammenarbeiten*

4 *Mit John von Neumann hatte sie auch einen großen Verehrer des Militärs als Mitbegründer – ganz anders Norbert Wiener, der bis zuletzt ethische Bedenken in die kybernetische Diskussion eingebracht hatte (vgl. Wiener 1966).*

5 *Z. B. https://www.consilium.europa.eu/de/press/press-releases/2020/12/14/encryption-council-adopts-resolution-on-security-through-encryption-and-security-despite-encryption/ (aufgerufen am 29.01.2024)*

6 *Vgl. z. B. https://www.heise.de/news/Going-Dark-Schwedische-EU-Ratsspitze-startet-Angriff-auf-Verschluesselung-7471023.html (aufgerufen am 29.01.2024)*

7 *Wie dies bspw. bei der DE-Mail der Fall ist, vgl CCC 2011 – https://www.ccc.de/system/uploads/64/original/CCC-de-mail-2011.pdf (abgerufen am 29.01.2024)*

8 *Wie etwa bspw. beim Staatstrojaner (Rehak 2014) oder jüngst bei der Chatkontrolle geplant, vgl. https://www.ccc.de/de/updates/2022/eu-kommission-will-alle-chatnachrichten-durchleuchten (abgerufen am 29.01.2024)*

9 *Vgl. bspw. https://www.fiff.de/presse/Cybersicherheitsstrategie2021.html (aufgerufen am 29.01.2024)*

10 *Vgl. https://www.amnesty.at/news-events/russland-kreml-geht-ruecksichtslos-gegen-unabhaengige-journalist-innen-und-antikriegsbewegung-vor/ (abgerufen am 29.01.2024)*

11 *Jüngst illustrierte der Begriff des Klima-Terrorismus die Absurdität und Selbstverständlichkeit, wie ziviler Ungehorsam als Terror bezeichnet (vgl. https://www.deutschlandfunk.de/letzte-generation-ist-keine-terror-vereinigung-100.html) und tätliche Angriffe auf Bürger:innen verharmlost wurden, und durch die wiederholte Frage nach der Legitimität, diese schon unterstellt wurde (vgl. https://www.br.de/nachrichten/bayern/klima-proteste-darf-man-aktivisten-von-der-strasse-entfernen,TNvk6QB).*

12 *In jüngerer Zeit wurden Strafkategoren für die Anwendung geheimdienstlicher Methoden ausgeweitet und Befugnisse verstetigt und erweitert, vgl. https://netzpolitik.org/2020/verfassungsschutzrecht-bundesregierung-will-geheimdienst-befugnisse-aus-anti-terror-gesetzen-endgueltig-entfristen/, aber auch schon im letzten Jahrhundert wurden Geheimndienstmethoden auf Alltagskriminalität erweitert (vgl. Marx 1980).*

13 *Vgl. Heise 2021: https://www.heise.de/news/220-Milliarden-Euro-Schaden-durch-Ransomware-und-andere-Cyber-Angriffe-6156111.html (abgerufen am 29.01.2024)*

14 *Vgl. Herpig 2022: Aktive Cyberabwehr statt Hackback https://background.tagesspiegel.de/cybersecurity/aktive-cyberabwehr-statt-hackback (abgerufen am 29.01.2024)*

15 *Bei denen regelmäßig auch das FIfF beteiligt ist bspw. https://www.fiff.de/presse/offenerBriefCyberunsicherheitsstrategie.html, https://www.fiff.de/presse/Cybersicherheitsstrategie2021.html, https://www.ccc.de/de/updates/2017/staatstrojaner-stpo (abgerufen am 29.01.2024)*

16 *Wie bspw. im Fall Lilith Wittmann vs. CDU https://www.sueddeutsche.de/politik/cdu-connect-anzeige-wittmann-1.5373488 (abgerufen am 29.01.2024)*

Daniel Guagnin, Laura Kocksch und Basil Wiesse

Daniel Guagnin leitet den Bereich Netze und Gesellschaft am nexus Institut Berlin und ist Mitglied beim FIfF. Er arbeitet partizipativ und forscht zu den gesellschaftlichen Implikationen von Technik und ihrer Konstruktion, bspw. in den Bereichen Freie Software, Cybersicherheit, Datenschutz und Digitalisierung.

Laura Kocksch ist Post-Doktorandin am Technoanthropology Lab (TANTlab) der Aalborg Universität in Kopenhagen, Dänemark. Sie arbeitet mit ethnographischen und digitalen Methoden zu Cybersicherheit, Nachhaltiger IT, Datenzentren und Dateninfrastrukturen. Ihre Monografie *Fragile Computing – How to Live with Insecure Technologies* erscheint in 2024.

Basil Wiesse ist wissenschaftlicher Mitarbeiter an der Professur für Prozessorientierte Soziologie der KU Eichstätt-Ingolstadt. Seine Interessenschwerpunkte sind Ethnomethodologie, Praxis- und Affekttheorien, Soziologie des Körpers, Soziologie des Digitalen und qualitative Methoden. Zurzeit untersucht er Praktiken der Cybersicherheit. 2020 erschien seine Dissertation *Situation und Affekt*.

Christian Heck et al.

Cyber Peace Works

Wie kann man etwas erklären, dessen Hauptbestandteil Code ist? The symbol grounding. Etwas, das man nicht zeigen kann, weil es eher eine Art des Denkens ist. Ein Denken über abstrakte Zeichen und symbolische Repräsentationen. Gleich einem Zugang zur Realität, der nicht an einen bestimmten Ort gebunden ist oder einem Ding, das man nicht greifen kann, um es aus verschiedenen Perspektiven betrachten zu können. Etwas, das sich im Netz abspielt. Unter der Oberfläche der Gesellschaft. Etwas, das sowohl in unseren Ideen als auch in den Maschinen steckt.

Die künstlerischen Arbeiten der Plattform *[ ] ground zero*, die im Rahmen der FIfFKon 23 präsentiert wurden, nähern sich diesen Fragestellungen ästhetisch an und versuchen mögliche Wege durch sie hindurch für die Zivilgesellschaft zu ebnen. Wege, um über die gesellschaftlichen und kulturellen Konsequenzen dieser technischen, meist kognitiven Systeme öffentlich zu debattieren. Die Künstler:innen zeigen in ihren Werken technologisch bedingte Verzerrungen, Vorurteile, bis hin zu militärischen Mindsets auf, und die Notwendigkeit, sich öffentliche mediale Räume sowie Stadt- und Lebensräume zurückzuerobern.

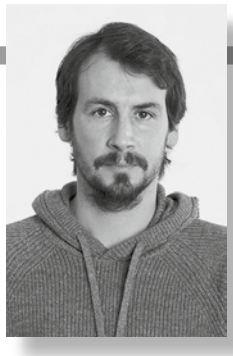
about [ ] ground zero @ khm

[ ] ground zero ist die Forschungsplattform der Experimentellen Informatik an der Kunsthochschule für Medien Köln (KHM).

Der Term *ground zero*, der seinen Ursprung in der militärischen Sprache hat, verortet ein bekanntes Problem der Informatik, das *Symbol grounding problem* innerhalb der KHM in eine Zone, in der sich (in Anlehnung an die Düsseldorfer Künstlergruppe ZERO) ein alter Zustand in einen unbekannten neuen verwandelt.

Ausgangspunkt der Forschung in *[ ] ground zero* ist die Überzeugung, dass die Menschheit zwar zunehmend von Technologie und ihrem reibungslosen Funktionieren abhängig ist, sie aber gleichzeitig „geistig nicht unter Kontrolle" hat. Ein anderes Verständnis, neue experimentell-ästhetische Ansätze und nicht zuletzt neue Sprachspiele sind notwendig, u. a. um den unzureichenden Dualismus von Technikeuphorie und Kulturpessimismus aufzulösen, der immer noch den Diskurs dominiert.

Christian Heck



Christian Heck ist künstlerisch-wissenschaftlicher Mitarbeiter für Ästhetik & neue Technologien/ Experimentelle Informatik und Doktorand an der Kunsthochschule für Medien Köln (KHM). Er forscht und arbeitet in [ ] ground zero @ KHM zu Ästhetischer Praxis, Ethik der Künstlichen Intelligenz und Friedensforschung mit Fokus auf generative Systeme, ADM, IT-Sicherheitstechnologien, Kampfdrohnen und autonome Waffensysteme.

Er ist Mitglied im Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e. V. und der Gesellschaft für Informatik (GI).

Benita Martis

Informationskrieg

Sozial- und Verhaltensforschungen zeigen, dass der Mensch dazu neigt, sich bestätigende Informationen zu suchen. Soziale Medien verstärken diesen Mechanismus, indem Algorithmen passende Beiträge vorschlagen. So können zum Beispiel die Einstellungen und das Verhalten gegenüber einem Krieg beeinflusst werden. Darüber hinaus sind KI-gestützte Werkzeuge bereits zu mächtigen politischen Instrumenten geworden, welche auch in sozialen Medien eingesetzt werden. Im Umgang mit den Rückmeldungen unterschiedlich trainierter KIs sollen durch die notwendige Übertreibung Methoden und Auswirkungen des digitalen Faschismus sichtbar gemacht werden. Das Spiel mit Fehlinformationen und Verschwörungsmythen stellt Nutzer:innen vor eine kritische Auseinandersetzung ihres eigenen Umgangs mit Informationen in sozialen Netzwerken.

Benita Martis

Benita Martis studiert an der Kunsthochschule für Medien Köln (postgradual) mit einem abgeschlossenen Studium in Kommunikationsdesign (Schwerpunkt Interaktive Medien). Ihre künstlerische Arbeit konzentriert sich auf die Erkundung der politischen Gefahren von Künstlicher Intelligenz in sozialen Netzwerken, insbesondere im Kontext des Informationskrieges. *http://benitamartis.de/*

Naoto Hieda

cctv.glitches.me

cctv.glitches.me ist eine Zusammenstellung von CCTV-Videos im Timelapse-Modus, die auf einer Webseite angezeigt werden. Closed-Circuit-Television (CCTV) oder eine Überwachungskamera wird oft installiert, um Verbrechen zu verhindern, Mitarbeiter zu überwachen oder den Verkehr auf der Straße zu verfolgen. Solche Videos von unsicheren, nicht passwortgeschützten Überwachungskameras werden in der Installation von einem Bot wahllos gesammelt, beschleunigt und vervielfältigt, um das Nichts, die Langeweile und die Alltäglichkeit zu zeigen, und suggerieren gleichzeitig die Unsicherheit der Sicherheit, die durch die Überwachungsgesellschaft und den Mangel an IT-Kenntnissen gewährleistet wird.

Naoto Hieda

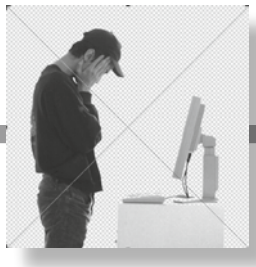
Naoto Hieda ist ein in Deutschland lebender Medienkünstler aus Japan. Er studierte Ingenieurwesen am Tokyo Institute of Technology, Japan (B. Ing.), und an der McGill University, Kanada (M. Ing.). Er absolvierte 2023 seinen Abschluss in *Mediale Künste* an der Kunsthochschule für Medien in Köln. In seiner künstlerischen Arbeit hinterfragt er die produktiven Qualitäten des Programmierens und erforscht neue Formen wie Post-Coding durch Neuroqueerness oder Dekolonisierung und Live-Coding. *https://naotohieda.com/*

Conrad Weise, Kjell Wistoff

Embedded Politics

In der Arbeit *Embedded Politics* beantworten verschiedene Large Language Models (LLMs) den politischen Kompass-Test. Large Language Models sind dialogfähige Sprachmodelle, die mit großen, oft nur teilweise moderierten Datenmengen aus dem Internet trainiert werden. Diese Daten enthalten Aussagen und Meinungen, die durch den Trainingsprozess in die Sprachmodelle eingebettet werden und so eine politische Voreingenommenheit der Modelle selbst erzeugen. Während diese Trainingsdatensätze als Grundlage für die Funktionsweise der Modelle dienen, erzeugt die aktuelle Implementierung von Inhaltsfiltern und Finetuning eine weitere Ebene der politischen Voreingenommenheit, die letztlich das dem Modell zugrundeliegende Meinungskonzept weiter prägt. Das Projekt macht sich die Ästhetik des politischen Kompasses zunutze, der nach seiner Einführung im Jahr 2001 große Popularität erlangte und sich zu einem beliebten Meme entwickelte.

Embedded Politics untersucht, wie digitale Werkzeuge/Interfaces die sozio-politischen Voreingenommenheiten des Internets übernehmen und potenziell verstärken. Maßgeblich beeinflusst wird dieses Phänomen von den Entwickler:innen solcher Tools, die in einem kontinuierlichen Entwicklungsprozess durch gezielte Eingriffe wie Filter und Finetuning Einstellungen vornehmen, die sich wiederum in der Prägung der Aussagen der Modelle über die Zeit beobachten lassen. Die ästhetische Konvergenz von visueller Symbolik und technologischer Exploration regt den Betrachter dazu an, über das komplexe Zusammenspiel von Algorithmen, Daten und der breiteren soziopolitischen Landschaft nachzudenken. Angesichts der steigenden Dialogfähigkeit von LLMs, die nun aktive Gespräche mit ihren Nutzer:innen führen können – und damit den fortlaufenden Prozess der Anthropomorphisierung imitieren und verstärken, stellt sich die Frage: Welche Art von Mensch will diese Technologie im Kontext unseres gegenwärtigen Wirtschaftssystems erschaffen?



Conrad Weise und Kjell Wistoff

Conrad Weise ist ein in Köln/Cluj ansässiger Designer und Forscher. In seiner Arbeit setzt er sich mit sozio-politischen Kontexten auseinander, in denen er die Computertechnologie und ihre Implikationen ausfindig macht. Durch investigative und computergestützte Ansätze innerhalb dieser Systeme versuchen seine Arbeiten, die intransparenten und unsicheren Arrangements zu kontextualisieren. *www.cnrd.computer* / *@cnrd@post.lurk.org*

Kjell Wistoff ist ein investigativer Künstler und Designer mit einem Schwerpunkt auf Interaktion. Vor allem zeitgenössische Technologien im sozio-politischen Kontext bilden sein Interessengebiet. Mit einem basisaktivistischen Ansatz arbeitet er mit diesen Technologien – und gegen sie.
https://kjellwistoff.de/

Leon-Etienne Kühr

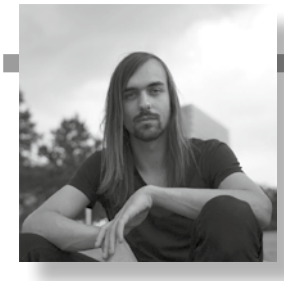
Euclidean Sensemaking

Da Datensätze und Modelle des maschinellen Lernens immer umfangreicher und komplexer werden, wird es für den Menschen immer schwieriger, die Nuancen, Verzerrungen und Gesamtstrukturen in ihnen vollständig zu erfassen. Um dieses Problem zu lösen, kommen Techniken wie Mappings und Projektionen ins Spiel, die helfen, die überwältigende Dimensionalität dieser Räume zu reduzieren.

Da die Verzerrungen und Beziehungen in diesen Räumen hochdimensional und kompliziert sein können, ist es notwendig, diese Komplexität in Metriken wie Abstände zwischen einzelnen Datenpunkten zu destillieren. Obwohl dieser Prozess unweigerlich mit einem gewissen Informationsverlust verbunden ist, bietet die allgemeine Nachbarschaft, die durch diese Abstände gebildet wird, einen wertvollen Überblick über die Konzepte, die sich im Raum nahe beieinander befinden.

Die interaktive Installation *Euclidean Sensemaking* befasst sich mit einem solchen Raum und den damit verbundenen Mapping-Techniken. Durch den Einsatz von Algorithmen zur Dimensionalitätsreduktion wird eine interaktive Karte erstellt, die einen der größten Bild-Text-Paar-Datensätze (Laion-5b) für state-of-the-art Bildgeneratoren wie Stable Diffusion in eine für Menschen lesbare Karte umwandelt. So kann man erkunden, warum Bildgeneratoren Katzen gegenüber Hunden bevorzugen oder eine Vorliebe für Bilder von Prominenten haben, die aus dem Auto steigen.

Leon-Etienne Kühr



Leon-Etienne Kühr ist sowohl als Informatiker als auch als Medienkünstler tätig und verwendet Methoden aus dem Bereich der Informationsvisualisierung und der Datenwissenschaft. Sein Schwerpunkt liegt auf der Erforschung und Visualisierung von Datensätzen und Modellen, die sich durch KI-gesteuerte Automatisierung allmählich in unseren Alltag integrieren. Seine künstlerischen Arbeiten befassen sich mit der Frage, wie unsere aktuelle algorithmische Landschaft möglicherweise eine Zukunft prägen könnte, in der sich der Schwerpunkt von der Mensch-Maschine-Interaktion zu einem Feedback von Maschine zu Maschine verlagert. *www.leon-etienne.de*

Ting-Chun Liu

Imaginary Landscape

Der Strand war seit der Aufklärung immer eine Touristenattraktion. Mit dem Aufkommen des Massentourismus und der sozialen Medien haben sich die idealisierten Strandbilder mit der Realität verflochten, was zu umfangreichen menschlichen Eingriffen und Terraforming entlang der Küsten weltweit geführt hat. Ausgehend von dieser Vorstellung von der Schönheit des Strandes untersucht das Projekt das Konzept der einseitigen Realitäten, die in Reisebildern in den sozialen Medien dargestellt werden, und wie diese Bilder in der Transformer-Ästhetik reproduziert werden.

Das größte Publikum für von Menschen produzierte Texte und Bilder sind in der heutigen Zeit nicht mehr Menschen, sondern Maschinen. Computer lernen und betrachten menschliche Wissenssysteme, um sie zu produzieren. Da der Lernprozess auf den von Menschen produzierten Bildern basiert, sind die daraus resultierenden Bilder bis zu einem gewissen Grad verzerrt. Ob in den sozialen Medien oder in einer Online-Bibliothek, die Bilder, nach denen im Zusammenhang mit Stränden gesucht wird, sind allesamt helle, weiße und saubere Strände. Die Verwendung solcher Bilder als Trainingsdaten führt zu einer Verzerrung der Darstellung, sodass der Computer die Strandbilder als künstliche Szenerie wahrnimmt. Wenn diese Bilder von der Maschine verarbeitet werden und Testbilder erzeugt werden, führt die Grundlage für die Bestimmung, ob die Bilder dem Eindruck des „Strandes“ entsprechen, ebenfalls zu einer Verzerrung der Bewertung. Mehrfache Verzerrungen ergeben sich auch bei der Erzeugung von Strandbildern durch das Transformer-Modell, das oft ein banales Bild des Strandes erzeugt.

Ting-Chun Liu

Ting-Chun Liu ist ein Medienkünstler aus Taiwan, der an der Kunsthochschule für Medien Köln studiert. Er beschäftigt sich mit audiovisuellen Medien, Feedback-Geräuschen, natürlicher Sprachverarbeitung und Künstlicher Intelligenz. Er setzt Feedback-Mechanismen für generative Bilder und Klänge ein, um über das kollektive Unbewusste und die unerreichbare „ideale“ Perspektive in KI-generierten Bildern zu reflektieren. *https://www.liutingchun.com*

Lisa Reutelsterz

[John and Mary] – by artificial and non-artificial systems

Emotionen und Schmerzempfinden gelten als essentiell für unser moralisches Handeln und unser soziales Miteinander. Wie drückt sich eine Maschine im Hinblick darauf aus und was verstehen wir als Betrachter davon bzw. wie? *[John and Mary] – by artificial and non-artificial systems* ist ein audiovisuelles Experiment, das die Grenzen zwischen Mensch, Maschine, natürlichen und künstlichen Systemen sowie Emotionen und deren maschinelle Reproduktion verwischt.

Gedichte wurden mithilfe eines großes Sprachmodells (LLM) generiert und dann in Bilddiffusionsmodelle eingelesen, um synthetische Videos zu erstellen. Diese wurden kontextlos Autor:innen präsentiert, um ihre individuelle Interpretation der Videos zu erfassen, die im Voiceover zu hören ist. Innerhalb traumartiger Sequenzen entsteht ein Sog, der dazu verführt, in den Bildern Bedeutung zu fassen und der ein Spannungsverhältnis zwischen maschineller und menschlicher Semantik zeigt.

Abstraktionen und Mehrdeutigkeiten eröffnen neue Bedeutungsräume, die die Unterscheidbarkeit zwischen Mensch und Maschine verwischen und eine kritische Reflektion ethischer Standards in der Technologieentwicklung suchen.

Lisa Reutelsterz

Lisa Reutelsterz ist Medienkünstlerin und Designerin, die an den Schnittstellen von Videokunst, experimenteller Informatik und Performance forscht und agiert. Ihr Ziel ist es dabei, neue Ästhetiken und Themenfelder zu erschließen und zu erweitern, die ihre Umsetzung beispielsweise in theatralen Prozessen oder audiovisuellen Rauminstallationen finden. Inhaltlich setzt sie sich vor allem mit den Fragen der Maschinenethik und Technikphilosophie auseinander, insbesondere im Hinblick auf Künstliche Intelligenz, Machine Learning und Affective Computing. *https://lisa-reutelsterz.com/*

Anton Linus Jehle

micromobility revolution (work in progress)

Der Begriff „Revolution" ist zu einem geflügelten Wort in der Welt des Risikokapitalismus geworden. Die Welt im Sturm erobern: Als Anfang 2018 Tausende von elektrischen Tretrollern oder „Trotinettes", wie die Franzosen sie nennen, die Stadt Paris überschwemmten, waren die Medien schnell dabei, dies als „Mikromobilitätsrevolution" zu bezeichnen. Da die Franzosen gewissermaßen Experten auf dem Gebiet des Revolutionierens sind, ist Paris wohl der Schlüssel für einen erfolgreichen Aufstand. Das scheinbar endlose Hin und Her zwischen Regulierung und Kooperation, zwischen Teilen und Ausbeuten, Fortschritt und Rückschritt der Mikromobilität ist hier wie in keiner anderen europäischen Stadt zu beobachten. Seit dem 31. August 2023 sind die Trotinetten von den Pariser Straßen verbannt, nachdem sich zuvor fast 90 % der Bürger dafür ausgesprochen hatten. Eine Revolution ohne das Volk. Die Arbeit „micromobility revolution" ist ihren letzten Tagen gewidmet.

Anton Linus Jehle

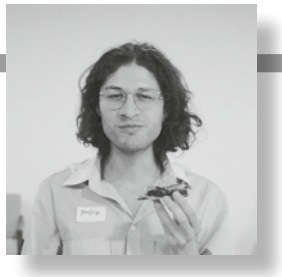
Als selbsternannter Mikromobilitätsparasit testet **Anton Linus Jehle** seit der Einführung von E-Scooter-Diensten im Jahr 2019 deren Grenzen aus. Mit Experimenten, Interventionen und Installationen durchbricht er erzwungene Perspektiven, um neue Ansätze für die gesellschaftspolitischen Herausforderungen unserer Zeit zu finden. In den letzten Jahren wurden seine Arbeiten u. a. im Körber-Forum in Hamburg, im Württembergischen Kunstverein in Stuttgart, beim Linz FMR23 Festival und bei der rc3 Remote Chaos Experience des Chaos Computer Clubs präsentiert. *https://www.antonlinus.art*

Pedro A. Ramírez

Speech Bubbles and Bespoke Chatter

Mit dem Aufkommen der maschinellen Intelligenz wächst das Interesse am maschinellen Zuhören als Strategie zur Erkennung und Unterscheidung der Wörter, während wir sie sprechen. Von OpenAI Whisper, das unverständliches Gemurmel in einzelne Wörter umwandeln kann, bis hin zu Siri, Alexa und zahllosen anderen Diensten, die in bidirektionalen Routinen zwischen der Sprache und dem Text arbeiten, also der Luft, die letztlich die Laute enthält, die wir ausdrücken.

Welche Arten von Algorithmen sind in diese Werkzeuge eingeschrieben? Welches ästhetische Potenzial haben sie als Instrumente zur Erweiterung des musikalischen Werkzeugkastens des zeitgenössischen Klangarbeiters, indem sie durch spektrale Differenzierung zwischen klanglichen Ereignissen näher an die Worte/Laute herankommen? Können die aus diesen Prozessen resultierenden Artefakte bearbeitet werden? Und wie können wir eine ästhetische Dimension in solchen Technologien finden, die gemeinhin mit den immerzu zuhörenden Apparaten der zeitgenössischen Hardware-Geräte assoziiert werden, die von großen Technologiekonzernen entwickelt werden?



Pedro A. Ramírez

Pedro A. Ramírez ist ein Künstler, der an der Schnittstelle von Klang und Technologie arbeitet. Ob analoge Synthesizer oder Computerprozesse, er interessiert sich für die Konzepte von Noise sowohl als ästhetischen als auch als konzeptionellen Raum. Seine Referenzpunkte sind die Kybernetik der Informationstheorie, Algorithmen der Computermusik sowie das auditive Wissen der Untergrundszene und ihre Strategien zur Mythenbildung. *https://airpopcrack.com/*

Bidisha Das

CyberEarth 0.1

Diese Installation wurde speziell entwickelt, um Pflanzen in einer ideal geschützten Umgebung mit dem Notwendigen, was sie zum Überleben brauchen, am Leben zu erhalten. In ihrem Lebensraum sind bestimmte äußere Bedingungen erforderlich, um den regelmäßigen Sauerstoff-Kohlenstoff-Kreislauf aufrechtzuerhalten. Untersuchungen ergaben, dass die robuste Grünlilie (Chlorophytum comosum) bei bis zu 3 Grad Celsius und die kleine Zimmerrebe (Cissus striata) bei bis zu 5 Grad Celsius überleben kann.

Da die beiden Arten ursprünglich aus den Tropen stammen, liegt die ideale Durchschnittstemperatur für sie bei 18 Grad Celsius. Um diesen Temperaturzyklus in der kontrollierten bewohnbaren Umgebung aufrechtzuerhalten, wird der *Projektor* als Instrument eingesetzt. Die Temperatur des Projektors kann während des Betriebs auf bis zu 35 Grad Celsius ansteigen. Diese Wärme ist für die Pflanzen notwendig, um ihren Sauerstoff-Kohlenstoff-Kreislauf in Gang zu halten, wie sie es in ihrem natürlichen Lebensraum tun würden.

Zurzeit wird die Funktion des Lichts im Prozess der Photosynthese erforscht. Bislang ist das derzeitige Licht für diese Funktion nicht ideal, aber in Zukunft werden sich die Pflanzen langsam an die bestehenden Lichtverhältnisse anpassen können, so wie sie es schon immer getan haben.

Bidisha Das

Bidisha Das ist Medienkünstlerin, Musikerin und Forscherin. Neben zahlreichen anderen Medien arbeitet sie vor allem mit improvisierter elektronischer Musik, für die sie analoge, digitale und selbstgebaute Instrumente verwendet. Ihre Klanglandschaften sind von einem konstanten DIY-Ansatz geprägt, der ihr tiefes Interesse an der Schnittstelle zwischen Kunst, Naturwissenschaft und Elektronik widerspiegelt. Zu den wiederkehrenden Themen ihrer vielfältigen Arbeiten gehören die planetarische Koexistenz, Transformationsprozesse, alternative Konzepte der Kommunikation und rhizomatisches Denken. Bidisha wuchs in Kalkutta, Indien, auf und lebt derzeit in Köln, wo sie ihre Praxis weiterführt.

Lisa Reutelsterz, Leon-Etienne Kühr, Benita Martis, Christian Heck

Aesthetic approaches to cyber peace work

Je wirkmächtiger und aktiver technische Bilder in unseren Lebensalltag eingreifen, desto zentraler stellt sich die Frage nach einer zivilgesellschaftlichen Rück-Eroberung der Deutungshoheit über diese Bilder. Mit zunehmender Integration gesellschaftlicher Werte in Technologie wachsen die ethischen Herausforderungen, die sich aus der zunehmenden Verschmelzung von Mensch und Maschine ergeben. Vorgestellt wird die bisweilen unterrepräsentierte Rolle der Ästhetik in der Friedensarbeit im Cyberraum zur Eröffnung eines neuen kritischen Debattierraums.

Abbildung 1: cyber peace works

Aesthetic approaches to cyber peace work setzte auf den Begriff der Performativa. Auf den Erhalt einer adäquaten Verhältnismäßigkeit zwischen Denken, Erfahren, Sprechen und unserem gemeinschaftlichen Handeln im Hier und Jetzt. Die kollektive Performance-Lecture war eine Art Experiment im Versuch, eine eigene Denkweise zu fördern – ein mögliches Denken in 90 Minuten, um bestenfalls und auch gemeinsam durch die Begegnung mindestens zweier Erfahrungen zu ästhetischen Erkenntnissen zu gelangen: der Erfahrung der Erzähler:innen und jener des Publikums. Diese uns ganz eigene Art des Erfahrens wird als „ästhetische Erfahrung" bezeichnet. Sie verspricht Denk- und Erfahrungsräume zu öffnen, die uns zu nicht-quantifizierbaren Erkenntnissen verhelfen können. Eine für die Friedensarbeit notwendige Art der Gegenüberstellung zur Meso-Welt – ganz einfach, weil Leben sich nicht messen lässt.

Ästhetische Ansätze zur Friedensarbeit fokussieren somit auf die deutungshoheitliche Rückeroberung technischer (digitaler) Bilder, die sich zwischen Apparat, Repräsentation, Begriffsgeschichten und institutioneller Rahmung situieren – im Cyber. Eine Rückeroberung aus der Zivilgesellschaft heraus, von Deutungshoheiten informatischer und medialer Räume – dem Cyberspace. Von experimentell-ästhetischen Zugängen und Sprachspielen in der Interpretation der Zeichen und Bedeutung, der Syntax und Semantik, losgelöst von der gewohnten Zweckorientierung im herrschenden Verbund von Wirtschaft-Technik-Wissenschaft und Militär. Und nicht zu vergessen: Vom Erhalt der Performativa im Umgang mit sozialen, gesellschaftlichen und kulturellen Konsequenzen von Cyber im Krieg und im Zivilen.

Denn viele der Begriffe, die es in den derzeit geführten Debatten um Cyberkrieg adäquat einzuordnen gilt, stammen aus eben jener fast schon in Vergessenheit geratenen Metadisziplin: der Kybernetik – Cybernetics. Und die Bedeutung dieser (kybernetischen) Begriffe „ist die Art, wie ihr Gebrauch in das Leben eingreift" (Wittgenstein, Ludwig 1973:29). Im Miteinander. In dem Raum, in dem der Gemeinsinn verortet ist und die Begriffe ihren gesellschaftlichen Sinn erhalten. In dem Raum, in dem das Sensemaking stattfindet. Im öffentlichen Raum.

Die begrifflich gefassten kybernetischen Modellvorstellungen von Welt haben zumindest in den letzten knapp einhundert Jahren massiv in unser Leben eingegriffen. Das zeigt sich in dem Maße, wie wir die aus diesen Modellen hervorgegangenen technischen Systeme in unserem täglichen Leben gebrauchen. Begriffe wie ‚Lernen', ‚Intelligenz', ‚Autonomie', ‚Kognition', ‚System' und ‚Kontrolle' wurden rekontextualisiert bzw. entstanden aus kybernetischen Mindsets heraus und stoßen bis heute an die Grenzen unseres rationalen Denkvermögens. Diese Grenze erstarrt insbesondere immer dann, wenn Logiken des Krieges in diese Systeme als sozio-technische Handlungsräume bewusst eingeschrieben werden. Krieg zu führen bedeutet innerhalb des Cyberspace, dass dieser zu weit mehr als nur zu einem Träger oder Verarbeiter von Zeichen mutiert, weit mehr als zu einer Technosphäre, in der Prozesse und Funktionen auf den militärischen Zweck gerichtet ablaufen. Cyber wird zum aktiven Erzeuger des „Un-Sinns" von „psychotischer Kriegswirklichkeit".

Abbildung 2

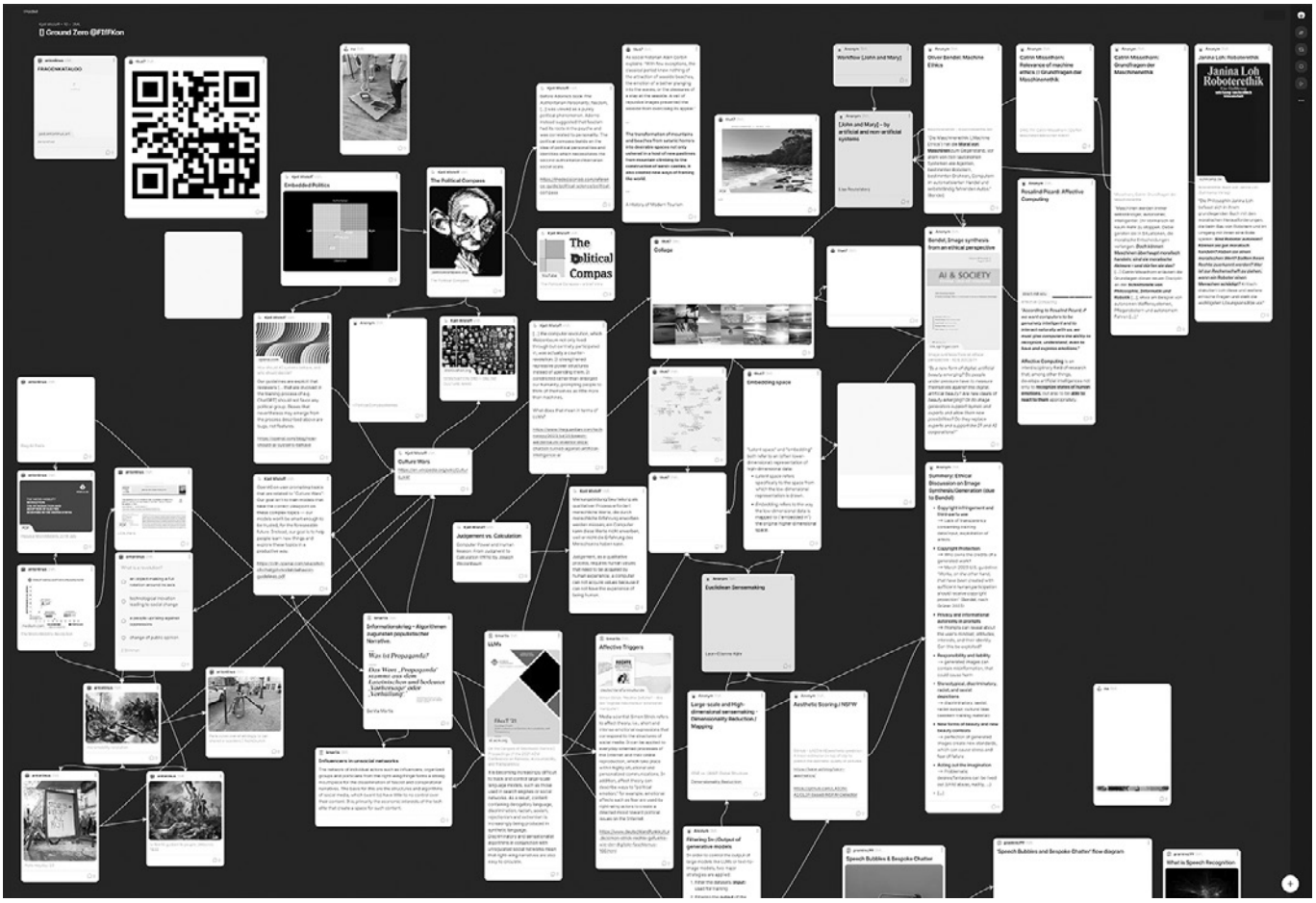


Abbildung 3

Einer grund-technischen, einer technisch erzeugten Kriegswirklichkeit, die als Sinneinheit – wie es die Schriftstellerin Marlene Streeruwitz beschreibt – einzig Entfremdung bedeuten kann (vgl. Streeruwitz, Marlene 2022).

Wenn wir unsere Seinsweisen in ihr demnach verstehen wollen, setzt das den Inbegriff der Performativa voraus. Um in Hannah Arendts Worten zu sprechen: die „Existenz der Pluralität unter Menschen" (Arendt, Hannah 1981). Denn nicht nur das ‚Verstehen' lässt ein Common Sensemaking, ein adäquates zivilgesellschaftliches Debattieren über Cyberkriege zu, auch ein Verständnis untereinander und vor allem: Verständnis füreinander.

Die Black Box der technischen Bilder: Wiederaufladung des Abstrahierten

Diese technischen ‚Erzeuger' wirken in unseren jeweiligen Lebens- und Arbeitsalltag hinein, indem sie durch spezifische technische Handlungen mehr oder weniger in unser Verhalten übergehen.

In der Praxis kann das wie folgt beschrieben werden: das, was zuvor durch den Prozess der Abstraktion weggenommen wurde, all die Mehrdeutigkeiten und Ungereimtheiten des Lebens, Phänomene, die vom konkreten Gegenstand gelöst und vom Sinn befreit wurden, alle Notwendigkeiten, um Leben erst maschinenlesbar machen zu können, all dieses Wegabstrahierte, muss in dem Moment, in dem das Abstrakte über die materiellen Schnittstellen zur Welt (Interfaces) wieder in Erscheinung treten kann, neu aufgeladen werden. Diese Codierung findet im Inneren, meist im Verborgenen statt: einer Black Box also. Diese abstrakten Zeichen werden in Interaktion wieder mit Bedeutungen aufgeladen. Es sind jedoch Bedeutungen, die den vormals entfernten, den wegabstrahierten, nicht gleichen (vgl. Trogemann, Georg 2015). Diese Wiederaufladung darf somit nicht einfach ignoriert werden. Sie ist Teil des Sensemaking, und zwar immer dann, wenn kulturelle Werte, die einst in Technologien eingeschrieben wurden, beginnen, in der Gesellschaft neue Wertedebatten anzustoßen (siehe Abbildung 4).

Die Integration menschlicher Werte in Technologie: eine ethische Perspektive

Menschliche Werte, normative ethische Werte, welche für uns, die wir eine individuelle Lebensgeschichte haben und in-der-Welt-sind, etwas bedeuten und unser Handeln und Miteinander bestimmen, werden in neue Technologien eingeschrieben. Die Maschine aber verarbeitet diese Werte als Signale und trifft statistische Vorhersagen (vgl. Weizenbaum, Joseph et al. 2001:12). Auch wenn die Argumentation in eine Richtung führt, in der vermehrt durch ‚Predictive-Policing'-Maßnahmen präventiv künftige Straftaten verhindert werden können, müssen wir uns dennoch darüber bewusst sein, dass die dahinterstehende Technologie niemals neutral sein kann und – neben der Qualität ihrer Hardware-Bestandteile wie Sensoren, Prozessoren oder Aktoren – auch von den Trainingsdaten und dem Einfluss der Menschen bestimmt ist, die sie trainiert und programmiert haben.

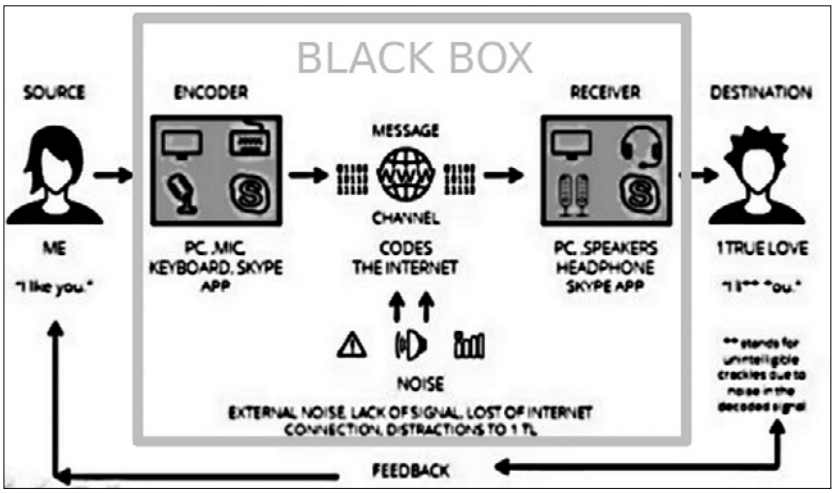


Abbildung 4

Diese Daten können auch „synthetisch generiert sein, wenn nicht genügend ‚echte' Daten in der gewünschten Qualität zur Verfügung stehen", was insbesondere im unüberwachten maschinellen Lernen zu Verzerrungen, Unsicherheiten oder einem verstärkten Bias führen kann (Deutscher Ethikrat 2023:94). Zugleich lässt sich beobachten, dass wir tendenziell der mathematischen Überlegenheit dieser Systeme vertrauen, ohne mögliche Konsequenzen der Entscheidungen zu berücksichtigen (vgl. Marino, Giorgia 2024).

Die Empfehlung des Deutschen Ethikrates in seiner 2023 erschienenen Stellungnahme ‚Mensch und Maschine – Herausforderungen durch Künstliche Intelligenz' zielt auf eine „klare Standardisierung von Datenformaten und zu erfassenden Metadaten" ab, sodass diese auch interdisziplinär und „institutionsübergreifend" genutzt werden können. Dabei wird betont, dass eine „Kombination" und „Verknüpfung" von Daten nur dann „sinnvoll gelingen [kann], wenn Kontext und Semantik für den jeweiligen Zweck hinreichend klar und kompatibel und die Daten auf dieser Grundlage interoperabel sind" (Deutscher Ethikrat 2023:94). Eine wesentliche Rolle in der Qualität der Datensätze spielt demnach auch der ursprüngliche Kontext, in dem sie erhoben und durch den eventuelle Schwerpunkte gelegt wurden. „Werden solche Fragen der Passung nicht rechtzeitig und hinreichend berücksichtigt, sind Verzerrungen oder irreführende Analysen möglich" (Barocas, Solon/Andrew D. Selbst (2016) zitiert nach Deutscher Ethikrat 2023:95). Damit einher geht die Reflexion über die Qualität der Hardware und die genutzte Infrastruktur, welche die Genauigkeit und Zuverlässigkeit beeinflusst. Eine solche „Standardisierung" kann jedoch auch die Gefahr bergen, wichtige historische, erinnerungsbezogene Informationen im Prozess zu verlieren. So argumentiert Weizenbaum dafür, die Notwendigkeit, die Vielfalt, Komplexität und den Kontext von Datensätzen anzuerkennen und sich nicht ausschließlich auf standardisierte Formen zu beschränken: „[W]enn eine Gesellschaft nur jene ‚Daten' als legitim anerkennt, die in ‚standardisierter Form' vorliegen, so daß sie einem ‚Computer leicht eingegeben werden können', dann ist Geschichte, dann ist Erinnerung überhaupt, ausgelöscht" (Weizenbaum, Joseph 2020:313).

Der Wirtschaftsinformatiker und Szientist Oliver Bendel weist bei der Übertragung von moralischen Werten in die Maschine auf jene „Unschärfen" hin, die während der Interaktion, d. h. im realweltlichen Einsatz entstehen: „Wir haben es in der Regel mit teilautonomen und autonomen Maschinen zu tun, die alleingelassen sind, die nicht von uns beaufsichtigt werden, die in Situationen geraten, die wir vielleicht vorausgesehen haben, aber doch ein wenig anders sind. Dadurch ergeben sich Unschärfen: Moral und Anwendungsfall der Moral passen nicht immer zueinander" (Bendel, Oliver 2018:48). Es gibt Szenarien, die von beispielsweise beteiligten Designer:innen, Programmierer:innen oder Entwickler:innen in ihrer Komplexität während des Trainingsprozesses nicht vorhergesehen werden können. Szenarien, die anders sein können als angedacht und Optionen enthalten, die in einer menschlichen Entscheidung, basierend auf Erfahrung und Kontext, möglicherweise anders ausfallen würden. Im Gegensatz dazu besitzen Maschinen weder ein Bewusstsein, noch einen freien Willen, keine Intuition und keine Emotionen (vgl. Bendel, Oliver 2022). Der Deutsche Ethikrat argumentiert zudem, dass „[m]oralische Verantwortung […] nur natürliche Personen übernehmen [können], die über Handlungsfähigkeit verfügen, das heißt, in der Lage sind, aktiv, zweckgerichtet und kontrolliert auf die Umwelt einzuwirken und dadurch Veränderungen zu verursachen. Träfe dies auch auf Maschinen zu, wären auch diese verantwortungsfähig." (Deutscher Ethikrat 2023:143). Es zeigt sich: „Merkmale menschlicher Intelligenz und menschlicher Vernunft lassen sich auf Maschinen nicht ohne Weiteres übertragen. Auch wenn Maschinen in Gestalt Künstlicher Intelligenz hochentwickelt sind, können sie den Menschen ihre Verantwortung nicht abnehmen" (Deutscher Ethikrat 2023a).

Weiterführend stellt sich die Frage nach den Haftungsregelungen, das heißt, wer für eventuelle Schäden durch autonome Systeme verantwortlich gemacht werden kann. In seiner Stellungnahme empfiehlt der Deutsche Ethikrat eine präzise Ausgestaltung der Haftungsregeln in den jeweiligen Anwendungsbereichen autonomer Systeme, was weitreichenden Einfluss auf deren Entwicklung mit sich bringt. Denn die Kenntnis über eine persönliche Haftung schafft „beispielsweise einen Anreiz, das System intensiver zu überwachen, seinen Aktionsradius einzuschränken oder eine menschliche Letztentscheidung vorzusehen" (Deutscher Ethikrat 2023:111). Die letztendliche Einbindung des Menschen in den Entscheidungsprozess als ‚human-in-the-loop' wird auch vom Philosophen Robert Sparrow als relevant erachtet, um Verantwortungslücken („responsibility gaps") zu vermeiden. Die Maschinenethikerin Catrin Misselhorn schreibt mit Verweis auf Sparrow, dass sich Verantwortung „minimiere oder gar verliere", wenn sie kollektiv auf „vielen Schultern verteilt" wird (vgl. Misselhorn, Catrin 2019:167). „The more autonomous these systems become, the less it will be possible to properly hold those who designed them or ordered their use responsible for their actions" (Sparrow, Robert 2007).

Hannah Arendt, die sich ein paar Jahre vor ihrer Berichterstattung zum Eichmann-Prozess aus einem „mehrlagigen Friedhof Namens Europa" heraus fragte, wie Menschen anderen Menschen so etwas antun können, schrieb in ihre Notizbücher, dass es grundsätzlich zum Gebaren von Bürokratien gehört, die Verantwortung für ihr Handeln anderen Stellen zuzuschieben. Doch eine unbeschränkt verschiebbare Verantwortung sei eine „Ver-

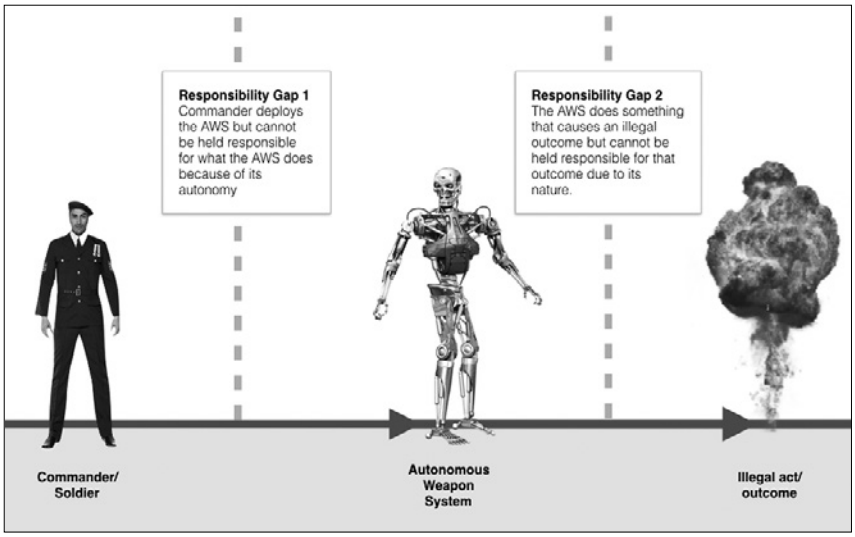


Abbildung 5: Illustration von Robert Sparrows Konzept der „responsibility gaps" Danaher, John 2017 | Copyright: John Danaher

antwortung des Niemand", so Hannah Arendt weiter. Demgemäß fiel auch Adolf Eichmanns Antwort aus, nachdem die Anklageschrift gegen ihn verlesen wurde. Sie lautete folgendermaßen: „Ich hatte mit der Tötung der Juden nichts zu tun. Ich habe niemals einen Juden getötet, aber ich habe auch keinen Nichtjuden getötet – ich habe überhaupt keinen Menschen getötet. Ich habe auch nie einen Befehl zum Töten eines Juden gegeben, auch keinen Befehl zum Töten eines Nichtjuden… Habe ich nicht getan" (Arendt, Hannah 1986:94).

Bei der Entwicklung digitaler Systeme liegt es jedoch auf der Hand, dass viele Menschen aus verschiedenen Disziplinen miteinbezogen sein müssen, die bestenfalls gemeinsam daran arbeiten. Soft- und Hardware-Engineering bewegt sich häufig an der Schnittstelle zwischen kreativen und bürokratischen Prozessen und tendiert meist eher in Richtung Arbeitsmodi nach klaren Vorgaben innerhalb festgelegter Strukturen. So fließen gänzlich unscheinbar technologische Solutionismen auch in politische Diskurse ein, wenn über deren prospektive Nutzung entschieden werden soll. Das heißt, neben politischen Entscheidungsträgern und wissenschaftlichen Gremien wird in militärisch genutzten, zivilen Cyberräumen auch Softwaredesigner:innen, KI-Unternehmen und Forschungsgemeinden eine gesonderte und überaus bedeutende Rolle der gesellschaftlichen Verantwortung zugeschrieben. Denn diese bestimmen während der Arbeit häufig präemptiv, und zwar durch den inneren Aufbau der jeweiligen Computerprogramme als Black Box, welche zukünftigen Phänomene wie konkret und in welcher Form als Symbole in IT-Systeme gelangen. Auch wie sie diese wieder verlassen werden, beispielsweise wenn Nutzer:innen sie in ihre jeweiligen technischen Handlungen übersetzen. So geben Programmierer:innen die Grenze zwischen dem Inneren eines technischen Systems und seiner Umgebung vor, Nutzer:innen der technischen Systeme wiederum legen sie fest.

Ethisch betrachtet kann das dazu führen, dass die Verantwortung des Einzelnen verwässert oder nur eingeschränkt rückverfolgt werden kann. Weizenbaum wies 2001 bereits darauf hin, dass die Verantwortungsübernahme bei intelligenten, autonomen Systemen auf gesellschaftlicher und struktureller Ebene zu betrachten ist: „Wir leben in einer Gesellschaft, in der eine große Scheu davor existiert, Verantwortung zu übernehmen. […] Verantwortung ist keine technische Frage, sondern eine gesellschaftliche" (vgl. Weizenbaum, Joseph 2001:33). Unser gemeinsames Miteinander in diesem Jahrtausend ist geprägt von den Entscheidungen, die wir im Umgang mit Technologie treffen, und wir haben die Verantwortung, sicherzustellen, dass diese Entscheidungen im Einklang mit unseren inneren und gesellschaftlichen Werten und auch mit den grundlegenden Menschenrechten stehen. Nur so können wir eine Zukunft gestalten, in der neue Technologien unser Leben bereichern können, ohne unsere Grundrechte zu gefährden.

Ästhetische Erfahrungen von Cyberräumen als Möglichkeitsräume für die Zivilgesellschaft

Das bedeutet: um über die militärische Nutzung von Cyberräumen adäquat sprechen, diskutieren und bestenfalls auch politisch debattieren zu können, um möglichen tiefgreifenden verletzenden Konsequenzen proaktiv entgegenwirken und aus der Zivilgesellschaft heraus Stellung beziehen zu können, ist es notwendig, kollektiv mehrere Perspektiven auf diese abstrakten Räume zu werfen. Auch außerhalb politischer Gremien, Sachverständigenräten und Entwickler:innengemeinden ist es essentiell, bestenfalls mit allen gemeinsam, die Entwicklungen dieser Räume zu beobachten, die Räume in ihrer Abstraktion zu verstehen, Ästhetiken technischer Möglichkeitsräume auszuloten und sie auf diese Weise zu interpretieren, zu konkretisieren und zu erfahren, und sie aus diesen ästhetischen Erfahrungen heraus analysieren und somit im Abstand zu sich im Bezug zum Cyberraum erleben zu können. Diese Herangehensweise ist eine zutiefst ästhetische. Eine Erfahrung, die im Sinne einer Differenzerfahrung als ästhetische Erfahrung bezeichnet wird.

Laut dem US-amerikanischen Philosophen Nelson Goodman handelt es sich hierbei um eine Erfahrung, die nicht statisch, sondern dynamisch ist, ähnlich wie bei unseren Kunst- und Alltagserfahrungen – weil wir die Dinge des Lebens erleben, das Gemälde sehen oder „das Gedicht erst lesen müssen" (Goodman, Nelson 1997:223). Es geht also darum, was ‚während' unserer Wahrnehmung bzw. unserer Erfahrung geschieht. Dieses ‚Dazwischen' wird versucht bei ästhetischen Ansätzen zu konkretisieren.

Die Musikpädagogin Ursula Brandstätter spricht von einem „doppelten Zugang zur Welt", der sowohl Zeichen repräsentieren als auch – wie beispielsweise ein Bild auf einer Leinwand – in einer physischen Materialität erlebbar werden kann (Brandstätter, Ursula 2013). Vorrangiges Ziel hierbei ist es, zu einer Sprache zu gelangen, die unsere Alltagssprache mit dem Gebrauch nichtnatürlicher Sprachen verbindet. Eben jene Sondersprache, auf die sich meist die wissenschaftliche Erkenntnis stützt. Denn die Verwendung dieser Sprachen birgt stets die Gefahr in sich, mit wirklichen Begebenheiten nie in Berührung gekommen zu sein.

In diesem Kontext öffnet die ästhetische Erfahrung für die Zivilgesellschaft bestenfalls einen Möglichkeitsraum, um über die Syn-

tax, Semantik und Pragmatik dieser Systeme zu sprechen. Einen Raum, um sich über sie zu unterhalten, sie greifbar zu machen, sie gemeinsam zu formen, sie miteinander zu gebrauchen, um politisch handeln zu können. Um sich innerhalb der Logik des herrschenden Ordnungssystems zu positionieren und dieses an seinem verwundbarsten Ort, dem Zentrum, anzugreifen. Das ermöglicht es, Dinge umzudeuten (detournement), das heißt in einen Kommunikationsprozess einzugreifen und den normalen, erwarteten Ablauf zu stören, um bei den Akteur:innen, Rezipient:innen oder Zuschauer:innen Distanz zu den vertrauten Verhältnissen zu schaffen. Möglichkeitsräume, um Worte zu finden, sie umzudeuten, sich anzueignen, Vertrautes und Normalität in Frage zu stellen.

Das Herstellen von Distanzen spielt eine entscheidende Rolle bei der ästhetischen Erfahrung, auch um das „flüchtigste aller Gefühle, oft rascher vorbei als ein Augenblick, und unvorhersehbar, unlenkbar, ungreifbar, unmeßbar" (Handke, Peter 1986:10), um das Gefühl von ‚Dauer' zu verlängern bzw. überhaupt erst erfahrbar zu machen, während man in digitaler ‚Echtzeit' technisch zu handeln angewiesen ist. Nach Bertold Brecht bedeutet das ‚Verfremdung'. „Einen Vorgang oder einen Charakter [zu] verfremden [heißt] zunächst einfach, dem Vorgang oder dem Charakter das Selbstverständliche, Einleuchtende zu nehmen" (Brecht, Bertolt 1939). In Teilen spricht man hierbei auch von ‚Cultural Hacking', der Umkodierung bestehender kultureller Codes. Dies kann bis hin zu einer Überführung ins Absurde gehen, zu unbrauchbaren Werkzeugen und zwecklosen Maschinen.

Operative Bilder: ästhetische Erfahrungen verborgener Ebenen

Doch was genau sind sie dann, diese technischen Bilder? Wie können wir denn nun etwas ästhetisch erfahren, wenn es gar nicht wirklich ein physisches Ding, nichts Greifbares, kein sichtbares Bild oder keinen menschenlesbaren Text, sondern nur Code gibt? Ein näheres Verständnis dieser Frage bringt uns das Konzept der „Operativen Bilder" des Filmemachers Harun Farocki: „Während die [operativen] Bilder nicht als Bilder zu betrachten sind, verfügen sie jedoch über mehrfache Operationsketten, durch die sie mit einer langen Reihe von institutionellen, epistemologischen und anderen Nutzungsformen verbunden sind, die eine andere Ästhetik auslösen. Eine Ästhetik, die sich mit Fragen dessen befasst, was […] als das nichtmenschliche Bild und das nicht-repräsentative Bild bezeichnet wird, da sie über institutionelle Orte und Nutzungsformen zirkulieren, von der Bildung über die Ausbildung von spezifischen Techniken bis hin zu den Algorithmen des Alltags" (Parikka, Jussi 2023:19).

So werden unsere Bilder, Worte, Gesten und Verhaltensweisen gemäß einer ästhetischen Operationalität des Sichtbaren zu interpretierbaren Zeichen nach vorgegebenen Kriterien. Eine verborgene Ebene dessen, was wir über Interfaces sehen: die Unterfläche der Bilder (vgl. Nake, Frieder (2006). Diese technischen Bilder in Zeichenform, die in ihrer militärischen Anwendung meist als die ‚eigentlichen' Bilder angesehen werden können. Sie tragen ihre eigene Historizität, die es offenzulegen und einzuordnen gilt. Von den Luftaufnahmen von Bombern im Zweiten Weltkrieg bis hin zu Klaus Theweleits ‚fliegenden Bomben' im Irakkrieg, die das sichtbare Leben überwachten und somit ausschließlich der militärischen Analyse dienten. Bilder, die das sichtbare Leben zerstörten, selbst jedoch unsichtbar blieben.

Abbildung 6: Filmstill aus: Farocki, Harun 2003

Farocki machte in seinen Filmen und Video-Installationen diesen Bildtypus ästhetisch erfahrbar und damit auch erst kritisierbar für Beobachter außerhalb der Operationsketten, das heißt für die Zivilgesellschaft. Diese Bilder, die ‚fliegenden Bomben' im kontrastarmen Schwarz-Weiß gehalten, im Zentrum ein Fadenkreuz, wurden erstmals 1991 in der Tagesschau der ARD gesendet. Die jeweilige Aufnahme riss mit dem Einschlag des Projektils ab.

Kriegsbilder in sozialen Netzwerken: wie KI politische Ereignisse beeinflusst

Die Bilder trugen keine ästhetische oder didaktische Funktion, sondern funktionierten rein als Bestandteil technisch-militärischer Operationen. Heute, in Gaza oder bei der Verteidigung der Ukraine, werden Drohnenkamerabilder zur Aufklärung

Abbildung 7: Verletzter russischer Soldat im Schützengraben zur Drohne schauend; Rechts: Zoom auf per Granatenabwurf getöteten oder verletzten Soldaten im Unterstand. Screenshots von Francis Hunger aus: Adam tactic group 2023

feindlicher Stellungen genutzt. Es handelt sich um Bewegtbilder in Echtzeit, die zur Korrektur von Artilleriefeuer und für direkte kriegerische Handlungen wie bspw. der Identifizierung von Zielorten eingesetzt werden. Auch für den Abwurf von Bomben und Granaten oder zur Steuerung von ‚Kamikaze'-Drohnen, die in feindliche Schützengräben geschickt werden und deren Angriffe als Livestream an übergeordnete Stabsstellen gesendet werden, finden diese Bilder Verwendung.

Unterlegt mit Popmusik und versehen mit verschönernden Farbfiltern tauchen die Kriegsbilder manchmal auch in den Feeds von Social-Media-Plattformen wie Telegram, Twitter oder TikTok auf. Durch ihre Ästhetik verschwimmen sie mit fern liegenden Inhalten und werden somit oft erst nicht als problematisch erkannt. Die meist ästhetisch aufbereiteten Aufnahmen, die – gleich Theweleits ‚fliegenden Bomben' – den Flugverlauf von ‚Kamikaze'-Drohnen bis zum Einschlag in ein vordefiniertes Zielobjekt zeigen, bezeichnete der Medienkünstler Francis Hunger als ‚Reästhetisierungsstrategien von YouTube-Influencer:innen' (Hunger, Francis 2023). Die Funktionsweise der Algorithmen in sozialen Netzwerken neigt dazu, negativ behaftete und reißerische Inhalte zu fördern. Somit erreichen gerade in sozialen Netzwerken propagandistische Narrative und Falschinformationen viele Menschen in kurzer Zeit. Vor allem für junge Menschen kann die Verbreitung von Kriegsbildern und KI-gestützten Falschmeldungen in Form von Wort und Bild gefährlich werden. Laut Umfragen sind rund 73 % der Nutzer:innen auf TikTok in Deutschland zwischen 16 und 19 Jahre alt (vgl. statista 2022). Sowohl TikTok als auch Instagram gehören bei jungen Menschen zu den beliebtesten Informationsquellen im Internet (vgl. mpfs 2022). Die Sprachwissenschaftlerin und Medienpädagogin Sabine Schiffler betont, dass „[die] gewichtigeren Falschmeldungen […] immer noch die [sind], die von besonders glaubwürdigen Stellen verbreitet werden" (Schiffler, Sabine 2023). Durch ihre Glaubwürdigkeit tragen somit auch Influencer:innen eine gesonderte Rolle der gesellschaftlichen Verantwortung im Desinformations- und Propagandakrieg.

So konnte man beispielsweise zu Beginn des Ukraine-Krieges direkt neben Kreml-Propaganda auch Kriegsalltagsgeschichten von Influencer:innen aus der Ukraine sehen. Anfang 2022 kursierte ein ‚Deepfake'-Video des ukrainischen Präsidenten Selenskyj, in dem sein digitales Double behauptete, den Krieg gegen Russland aufzugeben. Der Fake riet seinen Bürger:innen, die Waffen niederzulegen. Die Falschinformation, bei der es auf den ersten Blick für Nutzer:innen schwer ist, sie als falsch zu entlarven, erreichte in kurzer Zeit Millionen von Menschen. Somit kann das Geflecht einzelner Influencer:innen, organisierter Gruppierungen und Politiker:innen ein effektives Sprachrohr für die Verbreitung von Kriegspropaganda sein.

Diese gezielte Nutzung von Ranking-Algorithmen, Social Bots und Automationen in Kombination mit menschlicher zielgerichteter Kuration, um Falschinformationen in sozialen Netzwerken zu verbreiten, wird „Computational Propaganda" genannt (vgl. Woolley, Samuel et al. 2019:4). Donald Trump nutzte diese Strategie beispielsweise auch für seinen Wahlkampf im Jahr 2017, indem er Social Bots unter anderem auf Facebook einsetzte, um seinen potenziellen Wähler:innen individuelle Botschaften zu übermitteln (vgl. Welchering, Peter 2017). Er wird diese Techniken und Technologien wieder nutzen.

Abbildung 8: Influencerin Valeria Shashenok: „MY TYPICAL DAY IN A BOMB SHELTER" (Shashenok, Valeria 2022)

Die Verantwortung von KI-Unternehmen und die militärische Nutzung technischer Bilder

Die mehr oder minder einfach zu benutzenden manipulativen Erzeugnisse, die mit Hilfe von Systemen wie bspw. ChatGPT erstellt werden können, unter anderem das leicht zugängliche Angebot von KI-Unternehmen wie Stability AI oder OpenAI, ihre Dienste zu nutzen, sollten uns als Zivilgesellschaft hellhörig werden lassen, auch wenn diese ihre eigenen ‚Usage Policies' ohne Vorankündigung plötzlich ändern.

In der zweiten Januarwoche dieses Jahres hat OpenAI einen Passus aus seinen Nutzungsrichtlinien gestrichen, der die Nutzung seiner Forschungsergebnisse und Produkte für militärische Zwecke bislang ausdrücklich ausschloss. Bis zum 10. Januar enthielt die Seite ‚Usage Policies', welche die Nutzungsbedingungen von OpenAI-Technologien aufführte, ein Kapitel mit Verboten diverser Einbettungen bzw. Erweiterungen bestehender digitaler Systeme mit der Bezeichnung „Disallowed usage of our models". Neben ‚Hate Content', Propaganda, der Generierung von Schadsoftware und Pornographie wurden dort unter anderem Nutzungen, die ein hohes Risiko körperlicher Schäden mit sich bringen, aufgeführt: „Activity that has high risk of physical harm", insbesondere von Waffenentwicklung, Militär und Kriegsführung, im Original: „Weapons development; Military and warfare" (archive.org 2023).

Dieses klar formulierte Verbot von militärischen Anwendungen hatte die weitere, für den Konzern natürlich auch äußerst lukrative Nutzung durch das Verteidigungsministerium und andere staatliche militärische Einrichtungen ausgeschlossen. Die neue Richtlinie enthält zwar weiterhin die Aufforderung „unseren Dienst nicht zu nutzen, um sich selbst oder anderen zu schaden" und nennt als Beispiel die „Entwicklung oder Verwendung von Waffen", doch das pauschale Verbot der „militärischen und kriegerischen" Nutzung ist verschwunden (OpenAI 2024). Die nicht vorangekündigte Streichung dürfte als eine Reaktion auf die vermehrte Nutzung von KI-Technologien in den aktuellen Kriegen wie dem Gaza-Israel-Krieg oder dem Angriffskrieg Russlands gegen die Ukraine gelten. Die KI-Softwareprodukte von Firmen wie Palantir Technologies Inc. beispielsweise erfreuen sich großer Nachfrage in der NATO, unter anderem auch

aus Tel Aviv und Kiew. Eines von Palantirs neuesten Softwarepaketen ‚AIP for Defense' wurde entwickelt, um Daten in Echtzeit zu analysieren und so Ermittler:innen und Entscheidungsträger:innen in verschiedenen Bereichen, einschließlich Militär und Sicherheit, zu unterstützen. Das ‚Battle Management System' ermöglicht die Verknüpfung und Analyse großer Mengen von Daten aus unterschiedlichen Quellen, um so komplexe Zusammenhänge und Muster aufzudecken. So erkennt es unter anderem feindliche Stellungen. Durch eine Chatfunktion ähnlich dem Interface von ChatGPT schlägt es in Interaktion dann Gegenmaßnahmen vor. Eine Einstellung erlaubt es auch diese Maßnahmen autonom auszuführen – wie zum Beispiel das Starten einer Aufklärungsdrohne ins Zielgebiet.

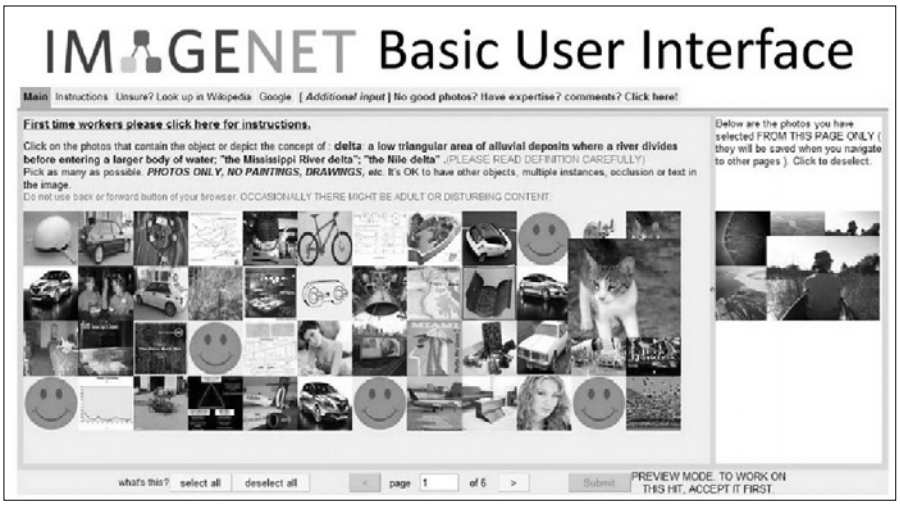


Abbildung 9: Interface, das von Amazon-Turk-Arbeitern verwendet wird, um Bilder im ImageNet zu beschriften (Fei-Fei, Li 2010)

Die Filmemacherin Hito Steyerl und der Künstler Trevor Paglen sprechen 2018 in ihrem Vortrag *The Autonomy of images, or we always knew images can kill, but now their fingers are on the triggers* im Centre Pompidou, ausgehend vom Konzept der ‚operational images' von ihrer Erweiterung, den „invisible images" (Steyerl, Hito/Trevor Paglen 2021): Bilder, die kein menschliches Auge mehr benötigen, um zu existieren, sondern „autonom" sind. Unsichtbare Bilder, die etwa im Rahmen von maschinellem Lernen entstehen und von Algorithmen generiert, trainiert und interpretiert werden, vermehrt ohne eine direkte menschliche Wahrnehmung. Die Autonomie dieser Bilder wirft Fragen bezüglich ihrer Entstehung, Interpretation und Auswirkungen auf, insbesondere hinsichtlich der Tatsache, dass etwa große Technologieunternehmen eine zentrale Rolle im Zugang zu diesen spielen.

Datenorientierte Weltzugänge: Machtstrukturen, Bias und ästhetische Wertungen im Kontext des maschinellen Lernens

Einen ästhetischen Deutungszugang zu diesen autonomen Bildern im Kontext des maschinellen Lernens eröffnen die Trainingsdaten. Bild-Datensätze sind zum einen durch die Auswahl der enthaltenen Bilder und zum anderen durch deren ‚Annotationen' definiert. Je nach Datensatz handelt es sich dabei um hierarchische Klassifizierungen der Bilder anhand zuvor bestimmter Konzepte, aber auch um textliche Beschreibungen oder das Labeln bestimmter Bildausschnitte. Große Datensätze wie der wohl bekannteste Bild-Datensatz ‚ImageNet' wurden dabei über Jahre manuell von Menschen kuratiert. Das Annotieren, Filtern, aber auch Erweitern des Datensatzes wurde u. a. durch die Nutzung ausbeuterischer Strategien wie das ‚Crowdsourcing' von Mikrojobs über Services wie ‚Amazons Mechanical Turk' maßgeblich vorangetrieben. Wie bei allen Prozessen, die auf Klassifizierung beruhen, stellt sich bei diesen Datensätzen unweigerlich die (Macht-)Frage, wer die Klassen bestimmt – wer klassifiziert und wer klassifiziert wird. Trevor Paglen und Kate Crawford beschreiben in ihrem Artikel *Excavating AI* diese annotierten Datensätze deshalb als „politische Intervention" (Crawford, Kate/Trevor Paglen 2019).

Die Vorstellung der Existenz einer neutralen und objektiven Perspektive, die durch technische Lösungen, das richtige Maß an Granularität und eine möglichst gleichmäßige Repräsentation in den jeweiligen Klassen bias-free würde, sei ein Fehlschluss und setze die Existenz einer verborgenen transzendenten „Essenz" eines Konzeptes voraus, das universell über mehrere Bilder hinweg visuell repräsentiert werden könne (vgl. Crawford, Kate/Trevor Paglen 2019).

Die Vorstellung suggeriert neben einer universalen Objektivität auch eine Quantifizierbarkeit ästhetischer Erfahrungen, welche durch den Trainingsprozess von den Daten in die Modelle übergeht. Aktuelle Forschungsansätze im Bereich der Bild-Text-Modelle forcieren diese Vorstellung und ersetzen vermehrt von Menschen annotierte Labels, Kategorien und Klassen durch automatisierte Prozesse. Inspiriert durch den derzeitigen Erfolg von Text-zu-Text-Modellen wie ChatGPT oder GPT-4 wird diese Taxonomie der Bilder zunehmend durch das Konzept der sogenannten ‚natural language supervision' getauscht. Das CLIP-Modell, das von OpenAI entwickelt wurde und derzeit wohl das meistzitierte Modell aus dem Bereich des maschinellen Sehens ist, wurde im Jahr 2021 mit der Vision veröffentlicht „das kostspielige und arbeitsintensive Erstellen von Bild-Datensätzen und die einseitige Spezialisierung eines Modells auf eine bestimmte Aufgabe zu überwinden" (Radford, Alec et al. 2021). ‚Natural language supervision' bedeutet dabei, dass feste Klassen und Labels von textuellen Beschreibungen abgelöst werden. Das heißt, dass zu jedem Bild ein Text in natürlicher Sprache eingetragen ist, der dieses Bild beschreiben soll. ‚Natürliche Sprache' bezieht sich dabei nur auf die Korrektheit der Syntax – encodiert in der Maschine jedoch bleiben diese Texte abstrakte Zeichen, die jegliche Sinnbeziehung verloren haben.

Die Quelle für die Text-Bild-Paare sind fast ausschließlich öffentlich zugängliche Daten aus dem Internet. Anders als noch bei kuratierten Datensätzen können diese Paare automatisiert mit Hilfe algorithmischer Filter aus archivierten Querschnitten des ‚Surface-Web' extrahiert werden. Diese prozesshafte und automatisierte Vorgehensweise eröffnet die Möglichkeit, Datensätze in bisher nicht gekannter Größenordnung zu erstellen.

Das CLIP-Modell wurde beispielsweise mit einem Trainingssatz von 400 Millionen Text-Bild-Paaren trainiert, wobei die genauen

Trainingsdaten von OpenAI nicht veröffentlicht wurden. Das von Stability AI entwickelte Text-zu-Bild-Modell Stable Diffusion basiert auf einem umfangreichen Datensatz mit 2 Milliarden Einträgen, bekannt als ‚laion2B-en'. Zum Vergleich: das oben erwähnte ImageNet-Datenset enthält ‚nur' etwa 14 Millionen annotierte Bilder. Im wissenschaftlichen Aufsatz zu CLIP preisen die Autor:innen das Modell für die gute ‚Zero-Shot'-Performance, also die große Erfolgsquote, wenn das Modell mit Daten konfrontiert wird, die nicht Teil des Trainingssets sind. Der Erfolg suggeriert die von Paglen und Crawford kritisierte Vorstellung einer transzendenten Essenz von Konzepten, die sich mit ausreichenden Trainingsdaten erfassen ließe. Die Allgemeingültigkeit und Universalität über mehrere Anwendungsgebiete und Aufgaben hinweg impliziert auch die Möglichkeit einer Anwendung für eine militärische Nutzung, wie die Klassifizierung von Kriegsbildern, oder für die innere Sicherheit, wie bspw. ‚Predictive Policing'. Dabei ist der gesamte Weltzugang, den diese Datensätze und Modelle repräsentieren, ein stochastischer, nämlich die Korrelation der abstrahierten Zeichen von Texten und Bildern aus dem Internet. Ein Prozess, der in seiner Gänze von Maschinen und Automatisierung bestimmt ist und unweigerlich eine Diskussion über Verantwortungsdiffusion anstößt. Er beginnt in der Überführung der Daten in einen gemeinsamen mathematischen Raum, auch ‚Latent Space' genannt. Diese maschinellen Repräsentationen sind für uns nicht ohne Neuinterpretation ästhetisch erfahrbar. Buchstaben- und Pixelrepräsentationen sind durch Vektoren und Tensoren ersetzt worden, mit denen operiert wird. Ein wesentlicher Teil dieser Operationen besteht jedoch im Filtern: Durch verschiedene mathematische Kriterien wird versucht, den ästhetischen Zugang zu Bildern zu quantisieren, zum Beispiel durch ‚aesthetic scoring'. Dabei wird ein Modell – auch als „Aesthetic Predictor" bezeichnet – darauf trainiert, den ästhetischen Wert von Bildern auf einer Skala von 1 bis 10 zu bewerten (vgl. Schuhmann, Christoph 2022).

Der „Aesthetic Predictor" ist auf programmatisch erstellten Datensätzen trainiert, welche Bewertungen aus Fotografie-Foren sowie Einschätzungen von Nutzer:innen auf großen Text-zu-Bild-Discord-Servern einschließen. Nach einem ähnlichen Prinzip bestimmt ein „NSFW Detector", welche Bilder ‚gefährliche Inhalte' abbilden. Trainiert wird dieser ‚Entscheider' auf gescrapten Bildern aus diffusen Kategorien wie ‚Gewalt' und ‚Pornographie' (vgl. Schuhmann, Christoph 2022a). Die Frage nach dem Urteilenden und dem Beurteilten verschwindet damit hinter der mathematischen Komplexität der Modelle und weicht einer Hegemonie automatisierter, scheinobjektiver Operationen auf Internet-Daten. Durch diese Vorgehensweise läuft alles, was als Bild im Internet vorhanden ist, Gefahr, jederzeit zu einem operativen Bild der operativen Datensätze zu werden.

Fazit

In einer Zeit, in der technische Bilder immer wirkmächtiger in unseren Lebensalltag eingreifen und unsere Handlungsräume bestimmen, stellt sich die zentrale Frage nach einer zivilgesellschaftlichen Rückeroberung der Deutungshoheit über diese Bilder – losgelöst von wirtschaftlichen oder militärischen Machtstrukturen. Insbesondere vor dem Hintergrund, dass die abstrakten Zeichen im Computer losgelöst von jeglicher Bedeutung existieren und dennoch in ihrer Interpretation Wirkmacht und Einfluss

Abbildung 10: Präsentationsbild von LAION-Aesthetics V1 | © LAION – Large-scale Artificial Intelligence Open Network, Schuhmann, Christoph 2022

auf unser Handeln ausüben – bedenke man etwa den Einfluss von ‚Deepfake'-Videos in Sozialen Netzwerken – gilt es, dies kritisch zu hinterfragen. Gleichzeitig führt der Versuch einer Integration menschlicher Werte in Technologie zu ethischen und gesellschaftlichen Herausforderungen, die Verantwortungslücken und Unschärfen mit sich bringen. Eine essentielle Form der Reflexion dieser ungreifbaren Prozesse ist die Übersetzung in eine ästhetische Erfahrung und ihre Erfahrbarkeit.

Referenzen

Adam tactic group (2023): Використання нікчемних істот з ніг продовжується, Screenshot von Telegram Video Post, 15.03.2023. URL: https://t.me/adamtactic/91 [abgerufen am 01.02.2024].

archive.org (2023): Usage policies, Archivseite auf archive.org. URL: https://web.archive.org/web/20240109122522/https:/openai.com/policies/usage-policies [abgerufen am 01.02.2024].

Arendt, Hannah (1981): Vita activa oder Vom tätigen Leben, München: Piper Verlag

Arendt, Hannah (1986): Eichmann in Jerusalem. Ein Bericht von der Banalität des Bösen, München / Zürich: Piper Verlag.

Bendel, Oliver (2018): Überlegungen zur Disziplin der Maschinenethik, in: Aus Politik und Zeitgeschichte, Nr. APuZ 6-8/2018.

Bendel, Oliver (2022): Maschinen können keine moralische Verantwortung tragen, in: Amosinternational 16, Nr. 3: 41–46.

Brandstätter, Ursula (2013): Ästhetische Erfahrung, kubi-online. URL: https://www.kubi-online.de/print/pdf/node/3231 [abgerufen am 01.02.2024].

Brecht, Bertolt (1939): Über das experimentelle Theater, in: ders: Gesammelte Werke, Bd. 15., Frankfurt am Main: Suhrkamp Verlag.

Crawford, Kate/Trevor Paglen (2019): Excavating AI: The Politics of Training Sets for Machine Learning. URL: https://excavating.ai/ [abgerufen am 01.02.2024].

Danaher, John (2017): How to Plug the Robot Responsibility Gap. URL: https://philosophicaldisquisitions.blogspot.com/2017/03/how-to-plug-robot-responsibility-gap.html [abgerufen am 01.02.2024].

Deutscher Ethikrat (Hrsg.) (2023): Mensch und Maschine – Herausforderungen durch Künstliche Intelligenz. URL: https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-mensch-und-maschine.pdf [abgerufen am 01.02.2024].

Deutscher Ethikrat (Hrsg.) (2023a): Künstliche Intelligenz zur Erweiterung menschlicher Entfaltungsmöglichkeiten einsetzen, Infobrief 01/23. URL: https://www.ethikrat.org/fileadmin/Publikationen/Infobrief/infobrief-01-23-web.pdf [abgerufen am 01.02.2024].

Farocki, Harun (2003): Erkennen und Verfolgen, Buch u. Regie: Harun Farocki; Kamera: Ingo Kratisch, Rosa Mercedes; Produktion: Harun Farocki Filmproduktion, Berlin, in Zusammenarbeit mit ZDF/3sat; Erstausstrahlung: 3sat, 2. März 2003.

Fei-Fei, Li (2010): ImageNet: crowdsourcing, benchmarking & other cool things, Präsentationsfolie CMU VASC Seminar. URL: https://www.image-net.org/static_files/papers/ImageNet_2010.pdf [abgerufen am 01.02.2024].

Goodman, Nelson (1997): Sprachen der Kunst, Frankfurt am Main: Suhrkamp Verlag.

Handke, Peter (1986): Gedicht an die Dauer. Frankfurt am Main: Suhrkamp Verlag.

Hunger, Francis (2023): Commercial of-the-shelf – Die Re-Ästhetisierung operativer Drohnenvideos im russischen Angriffskrieg gegen die Ukraine. Unveröffentlichtes Manuskript.

Marino, Giorgia (2024): Calculating and Powers: Interview with Kate Crawford, Renewable Matter. URL: https://www.renewablematter.eu/artificial-intelligence-computations-power-interview-kate-crawford [abgerufen am 01.02.2024].

Misselhorn, Catrin (2019): Grundfragen der Maschinenethik, 4. Aufl. Ditzingen: Reclam Verlag.

mpfs (2022): JIM-Studie 2022 – Jugend, Information, Medien, Medienpädagogischer Forschungsverbund Südwest. URL: https://www.mpfs.de/fileadmin/files/Studien/JIM/2022/JIM_2022_Web_final.pdf [abgerufen am 01.02.2024].

Nake, Frieder (2006): Das doppelte Bild. In: BAND 3,2 Digitale Form. Berlin, Boston: De Gruyter (A): 40-50.

OpenAI (2024): Usage policies, OpenAI. URL: https:/openai.com/policies/usage-policies [abgerufen am 01.02.2024].

Parikka, Jussi (2023): Operational Images: From the Visual to the Unvisual, Minneapolis: University of Minnesota Press.

Radford, Alec et al. (2021): Learning transferable visual models from natural language supervision, arXiv.org. URL: https://arxiv.org/abs/2103.00020 [abgerufen am 01.02.2024].

Schiffler, Sabine (2023): Erkenntnisse aus der Propagandaforschung, in: IMI-Analyse 2023/49, Informationsstelle Militarisierung e.V. (IMI). URL: https://www.imi-online.de/2023/12/18/erkenntnisse-aus-der-propagandaforschung/ [abgerufen am 01.02.2024].

Schuhmann, Christoph (2022): LAION-Aesthetics, laion.ai. URL: https://laion.ai/blog/laion-aesthetics [abgerufen am 01.02.2024].

Schuhmann, Christoph (2022a): LAION-AI/CLIP-based-NSFW-Detector, GitHub. URL: https://github.com/LAION-AI/CLIP-based-NSFW-Detector [abgerufen am 01.02.2024].

Shashenok Valeria (2022): MY TYPICAL DAY IN A BOMB SHELTER, Screenshot von @valerisssh, 4.03.2022. URL: https://www.tiktok.com/@valerisssh/video/7071270332891483397 [abgerufen am 01.02.2024].

Sparrow, Robert (2007): Killer Robots, in: Journal of Applied Philosophy 24, Nr. 1: 62–77

statista (2022): Anteil der befragten Internetnutzer, die TikTok nutzen, nach Altersgruppen in Deutschland im Jahr 2021/22. URL: https://de.statista.com/statistik/daten/studie/1318937/umfrage/nutzungvon-tiktok-nach-altersgruppen-in-deutschland [abgerufen am 01.02.2024].

Steyerl, Hito/Trevor Paglen (2021): The Autonomy of images, or we always knew images can kill, but now their fingers are on the triggers, Vortrag im Centre Pompidou, in: Hito Steyerl: I will survive espaces physiques et virtuels, Paris Düsseldorf Leipzig: Ed. du Centre Pompidou Kunstsammlung Nordrhein-Westfalen Spector Books.

Streeruwitz, Marlene (2022): Handbuch gegen den Krieg, Wien: Fischer Verlag

Trogemann, Georg (2015): Die Fülle des Konkreten am Skelett des Formalen, Open Access Publication. URL: https://e-publications.khm.de/frontdoor/index/index/docId/50 [abgerufen am 01.02.2024].

Weizenbaum, Joseph (2001): Computermacht und Gesellschaft. Freie Reden, Wendt, Gunna/Franz Klug (Hrsg.) (2001), Frankfurt am Main: Suhrkamp Verlag.

Weizenbaum, Joseph (2020): Die Macht der Computer und die Ohnmacht der Vernunft, 15. Auflage, Frankfurt am Main: Suhrkamp Verlag.

Welchering, Peter (2017): Wahlkampf der Algorithmen, Deutschlandfunk. URL: https://www.deutschlandfunk.de/social-bots-wahlkampf-der-algorithmen-100.html [abgerufen am 01.02.2024].

Wittgenstein, Ludwig (1973): Philosophische Grammatik, Frankfurt am Main: Suhrkamp Verlag.

Woolley, Samuel C./Howard, Philip N. (2019): Computational Propaganda. Political Parties, Politicians and Political Manipulation on Social Media, Oxford: Oxford University Press.

Autoreninfos siehe Seiten 42, 44 und 45

Friederike Hildebrandt

Machtfragen im Digitalisierungsprozess aus Sicht der Nachhaltigkeit

Vorschau auf einen längeren Artikel in einer der nächsten Ausgaben der FIfF-Kommunikation

„Ist Digitalisierung Chance oder Risiko für die Nachhaltigkeit?" Spätestens seit dem Gutachten des Beirats für Globale Umweltveränderung (WBGU) *Unsere gemeinsame digitale Zukunft*[1] und der ersten *Bits-und-Bäume*-Konferenz 2018[2] ist diese Frage aus dem politischen Diskurs nicht mehr wegzudenken. Auch die digitalpolitische Arbeit beim Bund für Umwelt und Naturschutz und im Bits-und-Bäume-Bündnis bewegt sich in diesem Spannungsfeld. Dabei ist das Ziel eine enkelfreundliche Zukunft zu ermöglichen – also zukünftigen Generationen einen gesunden, bewohnbaren und gerechten Planeten zu hinterlassen. Diese Zukunft gerät in Zeiten „multipler Krisen"[3] verstärkt in Gefahr, sei es durch den Rückgang demokratischer Regierungen weltweit[4], zunehmende Ungleichheit[5] oder anheizende bewaffnete Konflikte. Ökologisch stehen wir vor drei großen Krisen, die sich gegenseitig befeuern und bedingen: die Klimakrise, die Ressourcenkrise – also der übermäßige Verbrauch von biotischen und abiotischen Rohstoffen – und die Biodiversitätskrise oder das Artensterben.

Die Frage, ob Digitalisierung nur eine Chance oder doch ein Risiko für diese Krisen darstellt, lässt sich nicht abschließend beantworten. Allerdings deuten unterschiedliche Entwicklungen darauf hin, dass die üblicherweise durchgeführte Digitalisierung Krisendynamiken verstärkt:

1. Im Klimabereich führt die Nutzung von Rechenzentren für energieintensive Anwendungen wie KI-Systeme oder Kryptowährungen[6] zu erhöhten Emissionen von Treibhausgasen.

2. Der Bedarf an metallischen Ressourcen steigt weltweit durch sogenannte „Zukunftstechnologien" wie digitale Infrastrukturen, Elektromobilität und Weiterentwicklung der Hardware[7]. Für die Förderung der benötigten Rohstoffe werden eine Wiederbelebung des europäischen Bergbaus, die Erschließung der Lithiumförderung in Lateinamerika und Investitionen in den Tiefseebergbau diskutiert.

3. Eben dieser Rohstoffabbau bedroht zunehmend die Artenvielfalt – Tiefseebergbau kann bisher noch unerschlossene Ökosysteme zerstören, und schon heute ist die Förderung von metallischen Rohstoffen ein Hauptgrund für den globalen Verlust von Regenwäldern[8].
   Zudem nutzen große Agro-Chemie-Konzerne wie Bayer/Monsanto, Syngenta oder John Deere digitale Technologien, um die industrielle Landwirtschaft weiter zu intensivieren[9].

Aber warum verstärkt die Digitalisierung die Krisendynamiken? Der digitale Wandel wird von privatwirtschaftlichen Konzernen gestaltet und scheint klaren Mustern einer wachstums- und profitorientierten Wirtschaftslogik zu folgen[10]. Einerseits baut der digitale Wandel auf alten Strukturen auf – seien es lang etablierte Rohstofflieferketten oder die oligopolistische Stellung der Landwirtschaftskonzerne. Andererseits handeln die stärksten neuen Akteure im digitalen Sektor – die Technologiekonzerne wie GAFAM – ebenso gewinnorientiert wie die Landwirtschaftskonzerne und nehmen ökologische Schäden sowie Menschen- und Arbeitsrechtsverletzungen in Kauf, wie unterschiedliche Aktivist:innen und Organisationen kritisieren. Beispiele dafür sind die Arbeitsbedingungen von Content-Moderator:innen sozialer Medien[11] und Proteste gegen den Bau von Hyperscale-Rechenzentren in den Niederlanden[12] und der Region Sapmí[13]. Am eindrücklichsten ist die aktuell laufende Klage der Rohingya gegen den Meta-Konzern wegen der Befeuerung des Genozids an den Rohingya 2017 durch gezielte Hass-Rede und Hetze auf Facebook[14].

Damit tritt das Gegenteil dessen ein, was der WBGU in seinem Gutachten empfiehlt: dass Bürger:innen und Zivilgesellschaft den digitalen Wandel gestalten sollten. Diese Gestaltungsmacht ist jedoch nicht verloren, sie kann durch die Zivilgesellschaft und Bewegungen zurückerkämpft werden. Dazu braucht es strategische Policy-Arbeit, aber auch den Aufbau und die Ausweitung einer alternativen Digitalisierung. Hierfür müssen die ökologische und digitale Zivilgesellschaft eng zusammenarbeiten!

Anmerkungen

1 *https://www.wbgu.de/de/publikationen/publikation/unsere-gemeinsame-digitale-zukunft*
2 *https://bits-und-baeume.org/konferenz-2018/*
3 *https://www.boell.de/sites/default/files/multiple_krisen_u_brand_1.pdf*
4 *https://www.eiu.com/n/campaigns/democracy-index-2021/?utm_source=economist&utm_medium=daily_chart&utm_campaign=democracy-index-2021*
5 *https://www.oxfam.org/en/research/public-good-or-private-wealth*
6 *https://www.ecb.europa.eu/pub/financial-stability/macroprudential-bulletin/html/ecb.mpbu202207_3~d9614ea8e6.en.html*
7 *https://www.deutsche-rohstoffagentur.de/DE/Gemeinsames/Produkte/Downloads/DERA_Rohstoffinformationen/rohstoffinformationen-50.pdf?__blob=publicationFile&v=4*
8 *https://power-shift.de/wp-content/uploads/2022/01/HeissesEisen.pdf*
9 *https://www.etcgroup.org/content/disruptive-digital-food-and-ag-techs-invading-indigenous-territories-india*
10 *https://www.suhrkamp.de/buch/philipp-staab-digitaler-kapitalismus-t-9783518075159 https://aufkostenanderer.org/portfolio/digitalisierung/*
11 *https://www.bpb.de/mediathek/video/273199/the-cleaners/*
12 *https://www.washingtonpost.com/climate-environment/2022/05/28/meta-data-center-zeewolde-netherlands/*
13 *https://www.deutschlandfunkkultur.de/rechenzentren-in-nordeuropa-warum-die-samen-dagegen-kaempfen-dlf-kultur-b9cd40d3-100.html*
14 *https://www.deutschlandfunk.de/rohingya-klage-facebook-100.html*

Friederike Hildebrandt

Friederike Hildebrandt ist Ökonomin, Aktivistin und arbeitet beim Bund für Umwelt und Naturschutz zum Thema Nachhaltigkeit und Digitalpolitik.

Erich Pawlik

Entwicklungszusammenarbeit trifft auf Tech-Konzerne und den Überwachungsstaat

Teil 1 – Digitaler Kolonialismus

ICT4D (Information and Communications Technologies for Development) ist ein Sammelbegriff für verschiedene Herangehensweisen, die darauf abzielen, einen gerechteren Zugang zu digitalen Technologien zu ermöglichen und damit die wirtschaftliche und soziale Entwicklung weltweit voranzutreiben. Besonders arme und marginalisierte Gemeinschaften sollen davon profitieren. ICT4D-Akteure umfassen staatliche und überstaatliche Entwicklungsagenturen, zivilgesellschaftliche Organisationen, Universitäten sowie international tätige Unternehmen und deren Stiftungen. Diese verschiedenen Gruppen haben unterschiedliche Ansätze, aber sie alle teilen die Vorstellung, dass Digitalisierung eine positive Kraft ist und digitale Inklusion für die soziale Entwicklung von zentraler Bedeutung ist.

Die Informationstechnologie für den guten Zweck agiert in einem bereits digitalisierten Umfeld. In diesem Artikel werde ich mich auf Afrika konzentrieren. Der erste Teil des Artikels befasst sich mit den großen westlichen Tech-Konzernen, deren Vorgehen von Aktivist:innen im Globalen Süden oft als digitaler Kolonialismus bezeichnet wird. Zudem werde ich kurz auf die geopolitisch motivierte Unterstützung autoritärer Regime durch chinesische Akteure eingehen. Der zweite Teil erscheint in einer späteren Ausgabe der *FIfF-Kommunikation* und wird sich mit den staatlichen und zivilgesellschaftlichen ICT4D-Akteuren befassen.

Welthandel und Digitalisierung

Etwa die Hälfte des globalen Handels besteht aus dem Austausch von Dienstleistungen. Der Anteil der Dienstleistungen, die von Informations- und Kommunikationstechnologien (IKT) geprägt sind, nimmt kontinuierlich zu. Auch der Handel mit Waren und Rohstoffen ist zunehmend von IKT abhängig. Diese Nutzung von IKT basiert auf Beziehungen zwischen Ländern des Nordens und des Südens, in denen noch immer deutliche Spuren der kolonialen Vergangenheit zu erkennen sind.

Der Handel mit IKT-basierten Dienstleistungen begann in großem Maßstab mit IT-Outsourcing in den 80er- und 90er-Jahren des letzten Jahrhunderts. Unternehmen im Globalen Süden, in den Ländern der ehemaligen Sowjetunion und in Osteuropa dienten als ausgelagerte IT-Abteilungen. Für ihre Kunden waren die großen Lohnunterschiede wichtig, aber auch der Fachkräftemangel und die Möglichkeit, die innerbetriebliche Macht der oft widerspenstigen IT-Spezialist:innen zu brechen.

Dann kam *Business Process Outsourcing* (BPO), die Auslagerung von administrativen Arbeiten wie die Beantwortung von telefonischen Kundenanfragen oder Datenerfassung in Billiglohnländern des Globalen Südens. Eine moderne Variante ist die Content Moderation. Inhalte in sozialen Medien und KI-Plattformen wie ChatGPT, die von einem IT-System als potenziell anstößig, gewaltverherrlichend oder gegen die Nutzungsbedingungen der Plattform verstoßend eingestuft worden sind, werden auf die Bildschirme von Content Moderators projiziert. Diese Personen vor dem Bildschirm müssen im Sekundentakt entscheiden, ob der Inhalt den Vorgaben der Plattformbetreiber entspricht oder gelöscht wird.

BPO wird durch die Zerlegung von Aufgaben in kleine menschliche oder maschinelle Arbeitsschritte möglich, die wie am Fließband mit einem IT-System als Taktgeber ausgeführt werden. Die Auslagerung von Arbeit in Unternehmen des Globalen Südens hat für die Auftraggeber Kostenvorteile durch niedrigere Löhne, fehlende Sozialstandards, schlechtere Arbeitsbedingungen und weitgehende Kontrolle über das Personal gebracht. Bei Problemen verstecken sich die Auftraggeber hinter den lokalen Unternehmen oder argumentieren, dass alles gesetzeskonform sei.

Plattformen wie Amazon *Mechanical Turk* umgehen Unternehmen im Globalen Süden und bieten *24 hour access to a Global On Demand Workforce*. Dienstleistungen wie Bildbearbeitung, Textklassifikation für das Training einer Künstlichen Intelligenz oder das Schreiben einer Studienarbeit können auf den Plattformen ausgeschrieben werden. Deren Betreiber:innen treten als Vermittler:innen auf, ähnlich wie Uber oder eBay. Die Geschäftsbedingungen der Plattformen sind so ausgestaltet, dass die Auftragnehmer:innen gegenüber der Plattform und den Auftraggeber:innen fast machtlos sind und im Konfliktfall die zugesagte Bezahlung kaum durchsetzen können.

Tech-Konzerne im Globalen Süden

Die Ausbreitung von Mobilfunk und Internet im Globalen Süden schuf die Grundlage für globale Geschäftsmodelle. Kern der Strategie der Tech-Konzerne ist der Aufbau einer zunehmend festeren Bindung „ihrer" Benutzer:innen an ihre Plattformen. Dienste der Tech-Konzerne ermöglichen die Organisation des Alltags und des Kleingewerbes und können auch zur politischen Organisation wie etwa im Arabischen Frühling genutzt werden.

Die Tech-Konzerne sind auf die Loyalität ihrer Benutzer:innen angewiesen. Ein Großteil der Technologie, die beispielsweise in sozialen Netzwerken eingesetzt wird, ist frei verfügbar und könnte von lokalen Anbietern genutzt werden, um eine Alternative zu den internationalen Konzernen zu bieten. Für westliche Konzerne war es ein Warnsignal, dass in China lokale Unternehmen wie Baidu, AliBaba und Tencent westliche Konzerne verdrängt haben und zunehmend selbst global agieren.

Um dem entgegenzuwirken, hat Facebook damit begonnen, ein Konzept namens *Free Basics* in Ländern des Globalen Südens auszurollen. In Kooperation mit lokalen Telefongesellschaften wird kostenloser Zugang zu Facebook und anderen von Facebook ausgewählten Internetseiten angeboten, während für den Zugang zum restlichen Internet Telekommunikationsgebühren abgerechnet werden. Dies hat in vielen Ländern dazu geführt, dass Facebook mit dem Internet gleichgesetzt wird.

Rekolonisierung

In ihren Strategien setzen Tech-Konzerne auf Intransparenz. Moderne IKT-Systeme haben sorgfältig konstruierte Benutzungsschnittstellen, die den Benutzer:innen den Zugang zu den Leistungen der jeweiligen IKT-Systeme vereinfachen. Benutzungsschnittstellen dienen gleichzeitig der Verhaltenskontrolle von Nutzer:innen und sind wie ein Vorhang, der die durch die Entwickler:innen und deren Auftraggeber:innen in das IKT-System eingeschriebenen Ziele und Absichten verbirgt.

Während die Benutzungsoberflächen der angebotenen Dienste freie Kommunikation suggerieren, werden die sichtbaren Inhalte von intransparenten Algorithmen gesteuert. Die Algorithmen versuchen nicht nur zu ermitteln, was für die Benutzer:innen interessant ist, sondern auch, die Aufmerksamkeit auf Nachrichten zu lenken, die im Auftrag zahlender Dritter präsentiert werden. Der Globale Süden ist zwar noch kein großer Werbemarkt, politische Einflussnahme ist jedoch bereits ein weit verbreitetes Phänomen.

Umgekehrt werden Inhalte unterdrückt, die den von nordamerikanischen Werten geprägten Geschäftsbedingungen der Plattformen, lokalen Gesetzen oder auch den Wünschen autoritärer Machthaber widersprechen. Was toleriert wird, hängt davon ab, was die Plattform für opportun und bezahlbar hält. In vielen Ländern des Globalen Südens können Aufrufe zu Gewalt bis hin zum Mord, Mobbing von Angehörigen ethnischer Gruppen und digitalisierte sexuelle Belästigung ungehindert zirkulieren. Wenn es zu physischer Gewalt kommt, berufen sich die Plattformen meist auf mangelndes Wissen über die lokalen Verhältnisse oder fehlende Sprachkenntnisse. Auf der Website *Rest of World* wird der Fall eines politisch motivierten Mords in Äthiopien analysiert, dem mehrere Wochen Hatespeech auf Facebook vorausgegangen waren, ohne dass Meta etwas unternommen hätte (vgl. Deck 2023).

Die Strategie der Tech-Konzerne, ihre eingebetteten Machtstrukturen in den Plattformen zu verbergen, erweist sich trotz solcher Vorfälle als erfolgreich. Nutzer:innen betrachten und verteidigen die Plattformen weiterhin als Orte freier Kommunikation. Ein Beispiel hierfür ist ein Gespräch zwischen einer Professorin einer südafrikanischen Universität und ihren Student:innen (vgl. Becker 2017).

Die Technologie hinter den großen Plattformen wird hauptsächlich in westlichen Ländern und China entwickelt. So beeinflussen die Denkweisen der Entwickler:innen und ihrer Auftraggeber:innen die Gestaltung der Systeme maßgeblich. Dies geschieht meist unbeabsichtigt und oft aufgrund mangelnden Verständnisses für andere Lebenswelten. Dadurch besteht die Gefahr, dass kolonialistische Denkweisen verstärkt oder wieder eingeführt werden.

Von den weltweit etwa 7.000 Sprachen und Dialekten sind lediglich rund 500 im Internet vertreten (vgl. Trevino 2020). Dabei dominieren Inhalte in englischer Sprache, die etwa die Hälfte der Internet-Seiten ausmachen und nur etwa 10 weitere Sprachen machen fast die gesamte andere Hälfte aus. Dies führt dazu, dass viele Menschen, insbesondere im Globalen Süden, benachteiligt sind oder von der Nutzung dieser digitalen Werkzeuge ausgeschlossen werden.

Digitale Systeme nutzen zur Kommunikation eine dieser „Sprachen der Macht" (Alexander 2012). Sprache ermöglicht es Individuen und Gruppen, ihre Absichten umzusetzen und ihre Agenda anderen aufzudrängen. Diese Wirkungen sind in den schmalbandigeren Kommunikationstrukturen virtueller Umgebungen noch stärker ausgeprägt als im persönlichen Kontakt.

Die Vorherrschaft des Englischen und anderer postkolonialer Sprachen wird in vielen Ländern des Globalen Südens nicht nur toleriert, sondern auch als legitimes Modell für das Zusammenleben angesehen (vgl. Alexander 2012). Denn die Kenntnis der Sprache der ehemaligen Kolonialmacht ist in zahlreichen afrikanischen Ländern ein wertvolles kulturelles Kapital. Gleichzeitig werden mit der Sprache auch Denkweisen und Inhalte vom Norden in den Süden transportiert.

Automatische Übersetzung wird oft als Lösung angepriesen, um einen breiteren Zugang zu ermöglichen. Allerdings erfordert eine qualitativ hochwertige maschinelle Übersetzung einen umfangreichen Korpus an schriftlichem Material, der nur für etwa 30 Sprachen in ausreichender Qualität vorhanden ist. Bei den übrigen Sprachen, sofern überhaupt automatisierte Übersetzungsmöglichkeiten für diese vorhanden sind, treten häufig Übersetzungsfehler auf. Zudem führen viele maschinelle Übersetzungen über die englische Sprache zu einer verzerrten Darstellung sozialer und kultureller Konzepte.

Die Digitalisierung hat nicht nur dazu beigetragen, den ökonomischen und kulturellen Einfluss des Westens auf die Eliten und die Mittelklasse in Afrika zu verstärken, sondern auch neue Geschäftsmodelle für die Medien- und Kulturindustrie ermöglicht.

Streaming-Anbieter wie Netflix gewinnen Kunden in Afrika, stoßen im selben Moment jedoch auf Probleme aufgrund der fehlenden Internetinfrastruktur. Obwohl mobiles Internet weit verbreitet ist, sind die Kosten für das Streaming für die meisten Menschen in Afrika einfach zu hoch.

Derzeit ist es wirtschaftlich interessanter, afrikanische kulturelle Ressourcen für eine globale Kundenbasis zu nutzen. Netflix hat beispielsweise Nollywood entdeckt, ein Ökosystem für kostengünstige Filmproduktionen in Nigeria, die sich an ein afrikanisches Publikum richten. Basierend auf diesem Ökosystem hat Netflix begonnen, Filme in Afrika für ein globales Publikum zu produzieren (vgl. Okiche 2023:22).

Afrikanische Medienunternehmen könnten versuchen, in den USA und Europa Fuß zu fassen und afrikanische Inhalte wie Filme, Videos und Bilder zu vermarkten. Allerdings stoßen sie dabei u. a. auf das Hindernis des Urheberrechtsystems. Medienkonzerne aus dem Norden besitzen große Mengen an Rechten, die sie im Zweifelsfall auch gegen Konkurrenten einsetzen. Dies betrifft auch Trainingsdaten für KI-Systeme.

In Afrika werden in jüngster Zeit vermehrt Diskussionen geführt, bei denen die kollektiven Interessen von Gemeinschaften in den Vordergrund gestellt werden. Daten über soziale Zusammenhänge und kulturelle Traditionen werden als integraler Bestandteil der Gemeinschaft angesehen (vgl. Irura et al. 2021:16). Das auf Individuen ausgerichtete internationale Recht zum Schutz

von Immaterialgütern bietet hierfür keine Mechanismen. Artefakte wie die Shona-Skulpturen und die Benin-Bronzen können mithilfe generativer Künstlicher Intelligenz einfach nachgeahmt werden. Angehörigen der jeweiligen Gemeinschaft würden die Verdienstmöglichkeiten in der immer größer werdenden globalen Kulturindustrie genommen.

Handeln wie ein Staat

Tech-Konzerne versuchen im Globalen Süden, sich Funktionen anzueignen, die normalerweise Staaten vorbehalten sind.

Facebook hatte mit Libra (später Diem) eine inzwischen eingestellte Kryptowährung angekündigt. Libra wurde als Mittel zur finanziellen Inklusion im Globalen Süden beworben, einschließlich kostengünstiger Geldtransfers über Ländergrenzen hinweg. Facebook hatte dabei vermutlich die milliardenschweren Geldtransfers von Arbeitsmigrant:innen in ihre Heimatländer im Blick.

Die Idee einer Kryptowährung in den Händen von Tech-Konzernen wurde 2019 mit WorldCoin aufgegriffen. Dieses Projekt wird unter anderem von Sam Altman vorangetrieben, dem CEO der ChatGPT-Firma OpenAI. WorldCoin soll mit einer Identitätsprüfung per Iris-Scan und der Ausstellung eines global gültigen digitalen Identitätsmerkmals verbunden werden.

Staaten klassifizieren und machen Menschen und ihre sozialen Beziehungen transparent, um sich ihre Aufgaben zu erleichtern. Auch Tech-Konzerne sind bestrebt, digitale Zwillinge von ihren Benutzer:innen zu erstellen. Darüber hinaus wird auch versucht soziale Netzwerke zu erfassen sowie lokales Wissen, Kunst und Kultur. Fortschritte im Bereich der Künstlichen Intelligenz eröffnen neue Möglichkeiten zur Datenerhebung, z. B. durch Analyse der Gesprächsinhalte von Videotelefonaten.

Die zahlreichen Datensammlungen erfolgen nicht ausschließlich für Werbezwecke. Mehr und bessere Daten sollen den Plattformen ermöglichen, zukünftige Geschäftsmodelle zu entwickeln, insbesondere in Ländern des Globalen Südens mit ihren großen Wachstumschancen.

Es liegt nicht im Interesse der Tech-Konzerne, die von ihnen erhobenen Daten vollständig einem Staat zur Verfügung zu stellen, da dies die zukünftige Monetarisierung der Daten einschränken würde. Dies schließt jedoch eine Zusammenarbeit in Einzelfällen, wie beispielsweise bei polizeilichen Ermittlungen oder der Überwachung von Aktivist:innen, nicht aus.

Die Abhängigkeit der Benutzer:innen von den Plattformen gibt den Tech-Konzernen eine starke Position in der Debatte über die gesammelten Daten, da sie die Benutzer:innen für ihre Interessen mobilisieren können. Eine Blockade einer Plattform durch einen Staat kann zu massiven Gegenreaktionen der Benutzer:innen führen.

Ein kurzer Exkurs auf die dunkle Seite

Der „Arabische Frühling“, der manchmal auch als Twitter-Revolution oder Facebook-Revolution bezeichnet wurde, hat bei vielen Autokraten in Afrika ein Gefühl der Bedrohung ausgelöst. Obwohl sich die Bewegung letztendlich als fragil erwies (vgl. Tufekci 2017), fand die Nutzung des Internets zur Organisation sozialer Bewegungen viele Nachahmer.

Anfangs reagierten autoritäre Staaten auf die mit Hilfe sozialer Medien organisierten Bewegungen mit einer Abschaltung des Internets oder des Mobilfunknetzes. Da digitale Kommunikationstechnologien mittlerweile auch in Afrika eine bedeutende Rolle im täglichen Leben spielen, besteht bei langanhaltenden Abschaltungen allerdings die Gefahr, dass die Bewegungen an Breite gewinnen und sich radikalisieren.

Die Mächtigen haben ihr Repertoire dennoch erweitert, wohl wissend um dieses Risiko. Desinformation, Hacking von Geräten, Zensur und der Einsatz von Überwachungstechnologien wurden seit dem Arabischen Frühling kontinuierlich ausgebaut und zu einem Gesamtsystem integriert.

Digitale Überwachungstechnologien werden aus verschiedenen Quellen bezogen. Dabei spielen chinesische Technologien eine immer größere Rolle (vgl. Jili 2022). Die in China gut entwickelte Überwachungs- und Zensur-Technologie wird von chinesischen Unternehmen als Sprungbrett genutzt, um weitere digitale Dienste anzubieten und die Marktdominanz westlicher Tech-Konzerne zurückzudrängen.

Viele afrikanische Staaten und die Afrikanische Union arbeiten derzeit an Strategien zur Künstlichen Intelligenz. Es gibt nur sehr wenige Daten über die Lebenswelten und Wirtschaft der Menschen in Afrika, die eine Nutzung von Künstlicher Intelligenz zur Verbesserung der sozialen und wirtschaftlichen Situation ermöglichen würden. Gleichzeitig besteht jedoch ein erhebliches staatliches Interesse an digitalen Technologien wie der Gesichtserkennung z. B. in Äthiopien und Kenia.

Die deutsche Entwicklungszusammenarbeit

Die deutsche Entwicklungszusammenarbeit sieht die Digitalisierung seit einigen Jahren als wichtiges Thema an, hat aber noch nicht zu einer konsistenten Vorgehensweise gefunden. Ähnlich wie in anderen Bereichen schwankt die Digitalisierungspolitik zwischen den Zielen *Gutes tun* und *Interessenvertretung der deutschen Wirtschaft*.

Die aktuelle Afrikastrategie des Entwicklungsministeriums (vgl. Bundesministerium für wirtschaftliche Zusammenarbeit 2023) beginnt mit dem Verweis auf die wirtschaftlichen Potenziale Afrikas. Die deutsche Entwicklungszusammenarbeit wird als Akteur betrachtet, der zur Verbesserung der wirtschaftlichen und politischen Rahmenbedingungen der Staaten Afrikas beitragen kann. Ein zentrales Ziel ist die Verbesserung der Rahmenbedingungen für eine digitale Transformation, die Förderung digitaler Märkte sowie digitaler Inklusion.

Schwerpunkte liegen dabei auf der Digitalisierung des Gesundheitswesens und der Unterstützung der Verwaltung auf regionaler und lokaler Ebene. Darüber hinaus sollen digitale Technologien dazu beitragen, mehr Teilhabe, Austausch und Transparenz im Gemeinwesen zu ermöglichen.

Im zweiten Teil des Artikels wird untersucht werden, wie diese Ansprüche in die Realität umgesetzt werden können und wie sich die deutsche Entwicklungszusammenarbeit im Kontext von digitalem Kolonialismus, aufkommenden Überwachungsstaaten und anderen Akteuren im Bereich der Informations- und Kommunikationstechnologie behaupten kann.

Referenzen

Alexander, Neville (2012): The centrality of the language question in post-apartheid South Africa: Revisiting a perennial issue, in: South African Journal of Science, 108(9/10). URL: https://doi.org/10.4102/sajs.v108i9/10.1443.

Becker, Heike (2017): Talking Technologies of Transformation with my Students, Writer at Ethnography, 23. November. URL: http://writer-at-ethnography.com/social-media-students-2017.html [abgerufen am 30. Januar 2024].

Bundesministerium für wirtschaftliche Zusammenarbeit (2023): Gemeinsam mit Afrika Zukunft gestalten. Die Afrika-Strategie des BMZ, Bundesministerium für wirtschaftliche Zusammenarbeit. URL: https://www.bmz.de/de/aktuelles/publikationen/publikation-bmz-afrika-strategie-137600 [abgerufen am 30. Januar 2024].

Deck, Andrew (2023): AI moderation is no match for hate speech in Ethiopian languages, Rest of World, 27. Januar. URL: https://restofworld.org/2023/ai-content-moderation-hate-speech/ [abgerufen am 5. Juli 2023].

Irura, Mark et al. (2021): Responsible Data Governance for Monitoring and Evaluation in the African Context. Part 1 Overview of Data Governance, Faculty of Commerce, Law and Management | University of the Witwatersrand. URL: https://merltech.org/wp-content/uploads/2022/01/Responsible-Data-Governance-for-ME_part-1.pdf [abgerufen im Januar 2022].

Jili, Bulelani (2022): China's surveillance ecosystem and the global spread of its tools, Atlantic Council, 17 October. URL: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/chinese-surveillance-ecosystem-and-the-global-spread-of-its-tools/ [abgerufen am 6. November 2023].

Okiche, Wilfred (2023): Taken, with a pinch of salt, The Continent, 7. Oktober. URL: https://www.thecontinent.org/_files/ugd/287178_2405f839fe3b45a2896076f65a5abdfb.pdf [abgerufen am 31. Januar 2024].

Trevino, Miguel Trancozo (2020): The many languages missing from the internet, BBC Future, 15. April. URL: https://www.bbc.com/future/article/20200414-the-many-lanuages-still-missing-from-the-internet [abgerufen am 31. Januar 2024].

Tufekci, Zeynep (2017): Twitter and tear gas: the power and fragility of networked protest. New Haven London: Yale university press.

Erich Pawlik

Was man über die Ökonomie der generativen KI wissen sollte

Generative Künstliche Intelligenz (KI) kann Inhalte wie Bilder, Videos, Musik und Texte produzieren, die die Kreativität und den Einfallsreichtum von Menschen nachahmen. Nach dem Marketing-Erfolg von ChatGPT wurde generative KI als eine disruptive Innovation wahrgenommen. Schnell verbreiteten sich Beispiele von großartigen Leistungen wie auch von bizarren Fehlern von generativen KI-Systemen.

Generative KI

Der Hype um generative KI schoss durch die Decke. Sowohl große Tech-Konzerne, die viel Geld in die Entwicklung generativer KI investiert haben, als auch die Politik sehen in KI einen Hoffnungsträger für wirtschaftliches Wachstum. Allerdings gibt es auch Bedenken, dass unerfüllte Erwartungen zu einem neuen KI-Winter führen könnten.

Die dunklen Seiten der generativen KI, wie die Möglichkeit von erfundenen Fakten oder Anleitungen zum Bombenbau, sind mittlerweile bekannt. Diejenigen, die die Technologie vorantreiben, befürchten nun, dass Regulierungen oder eine negative öffentliche Meinung vielversprechende Möglichkeiten zur Monetarisierung der Technologie einschränken.

Moderne KI-Systeme werden mit großen Datenmengen trainiert, Muster zu erlernen und Texte sowie andere Medien zu erzeugen, die mit hoher Wahrscheinlichkeit zu Eingaben und Mustern passen. Die Kontrolle über die verwendeten Trainingsdaten bestimmt die Funktionalität des KI-Systems. In Unternehmenskreisen wird daher vermehrt die Frage diskutiert, ob die durch eifriges Datensammeln in den letzten Jahrzehnten gebildeten digitalen Zwillinge KI-Systeme zu überzeugenden und kostengünstigen Repräsentanten des Unternehmens machen können. Dies hat zu einer Wiederbelebung des Narrativs „Daten sind das neue Öl" aus der Zeit des Big-Data-Hypes geführt.

Geld machen mit KI

Die dominante wirtschaftliche Erzählung lautet, dass die (generative) KI Unternehmen in die Lage versetzt, effizient und kostengünstig hochwertige, personalisierte Produkte und Inhalte in großem Umfang zu erstellen. In rascher Folge wurden eine ganze Reihe von Studien veröffentlicht, die versuchen, diese Potentiale vorherzusagen und deren Größe betonen.[1]

Die Unternehmensberatung McKinsey hat detailliert die Geschäftsprozesse von großen Unternehmen untersucht (vgl. Chui et al. 2023) und kommt zu erstaunlichen Zahlen (siehe Tabelle 1). McKinsey geht von den folgenden Potenzialen in Billionen US$/Jahr aus (Chui et al., 2023:10).

Die Größe des Versprechens ist atemberaubend. Zum Vergleich: Der Internationale Währungsfonds (IWF) schätzt für das Jahr 2022 die weltweite Wirtschaftsleistung auf 100,1 Billionen US$.

	Minimum	Maximum
Big Data und „klassische" KI	11,0	17,7
Anwendung generativer KI in bestehenden Arbeitsprozessen	6,1	7,9
Neue Anwendungsfälle der generativen KI	2,8	4,4
Gesamtwirkung (nicht Summe wegen Überlappungen)	17,1	26,6

Tabelle 1: Wirtschaftliches Potenzial der KI (US $/Jahr)

Laut McKinsey werden die wirtschaftlichen Auswirkungen größtenteils durch Produktivitätssteigerungen erzielt. McKinsey erwartet, dass in nur wenigen Bereichen 75 % dieser Effekte erzielt werden: Software Engineering, Kundenbetreuung, Marketing, Vertrieb und Forschung/Entwicklung. In der Vergangenheit wurden in den von McKinsey genannten Feldern bereits zahlreiche Versuche zur Produktivitätssteigerung unternommen. Im Software Engineering wurden Codegenerierung, Software Lifecycle Management, Low-Code-Plattformen und anderes versucht. Ähnliche Versuche gab es auch in anderen Feldern der Wissensarbeit wie Marketing und Produktentwicklung. Im Kundenservice und Vertrieb wurde häufig versucht, die Kosten durch den Einsatz von Contact-Centre-Technologie und günstigen Arbeitskräften etwa im Globalen Süden niedrig zu halten. Die Tendenz, den Kontakt mit Menschen etwa durch Chatbots, Hilfesysteme, Voice Response Units zu vermeiden, hat oft zu Qualitätsproblemen und zur Kundenunzufriedenheit geführt. Gerade Unternehmen mit einem schlechten Ruf im Kundenservice erhoffen sich durch generative KI eine Verbesserung ihrer Kundenbeziehung und ihres Images.

Das ökonomische Versprechen der generativen KI baut auf dem seit mehreren Jahrzehnten selten hinterfragten Argument auf, dass Digitalisierung produktivitätssteigernd ist. Produktivität bezieht sich auf das Verhältnis zwischen den Ergebnissen einer wirtschaftlichen Tätigkeit und den dafür eingesetzten Produktionsfaktoren. Es ist diskussionswürdig, welchen Anteil die Digitalisierung etwa am Produktivitätsgewinn durch die Aufteilung der Produktionsprozesse in weltweit verstreute kleine Arbeitsschritte hat, die oft in Ländern mit schlechten Umwelt- und Sozialstandards durchgeführt werden. Der im Dezember verstorbene Wirtschaftsnobelpreisträger Robert Solow, der sich intensiv mit Produktivitätsstatistiken befasst hat, ist für seine Aussage „You can see the computer age everywhere but in the productivity statistics" (Solow 1987) bekannt.

Erik Brynjolfsson, ein prominenter Vertreter der Theorie einer neuen industriellen Revolution durch Digitalisierung, argumentiert in einem 2021 veröffentlichten Aufsatz, dass das Produktivitätswachstum über längere Zeiträume ausbleibe, wenn sich neue Allzwecktechnologien durchsetzen (vgl. Brynjolfsson/Rock/Syverson 2021). Der Grund sind die notwendigen Investitionen in immaterielle Güter wie Mitarbeiterqualifikation, die sich erst verzögert in Produktivitätsgewinnen niederschlagen.[2]

Trotz dieser Zweifel muss man davon ausgehen, dass Unternehmen nach Wegen suchen, das Versprechen der generativen KI Wirklichkeit werden zu lassen. In einer durch Marktkapitalisierung und finanzielles Controlling beherrschten Denkwelt wird jedem glaubwürdig vorgetragenen Versprechen nach mehr Profit nachgejagt. Auch wenn die gewünschten Effekte sich nicht realisieren sollten, wird es in vielen Fällen Umbauten in Unternehmen mit oft negativen Auswirkungen auf Arbeitsbedingungen und Lebenswelten von Kunden geben.

Die Anbieter:innen von generativer KI

Generative KI-Systeme wie ChatGPT, Midjourney oder Google's Gemini sind durch das Training mit großen Datenmengen vielseitig einsetzbar. Diese als Foundation Models bezeichneten KI-Systeme sind Plattformen, die erst dann einen konkreten Nutzen liefern, wenn ihnen ein Kontext bereitgestellt wird. Ein oder mehrere Prompts (Aufträge) sind die einfachste Form, um einen solchen Kontext zu erzeugen.

Die Entwicklung von Anwendungen auf Basis eines Foundation Models ist für Unternehmen attraktiv, da dies die Möglichkeit bietet, zusätzliche unternehmenseigene Trainingsdaten zu nutzen. Solche Anwendungen können die von Menschen eingegebenen Prompts verändern oder sogar umgehen, indem sie Antworten aus anderen Quellen liefern, anstatt sie an das Foundation Model weiterzuleiten.

In KI-Firmen und ihre Systeme werden zurzeit zweistellige Milliardenbeträge investiert. Trainings-Läufe können hohe zweistellige Millionenbeträge kosten.[3] Um die Kosten für die Entwicklung und den Betrieb wieder einzuspielen, wird der Zugang zu den Foundation Models als Cloud-Service über das Internet angeboten. Im Massenmarkt geschieht dies entweder als Premium-Angebot meist im Rahmen eines Abonnements oder kostenlos mit integrierter Werbung oder zur Datensammlung. Darüber hinaus stellen Cloud-Anbieter:innen maschinelle Schnittstellen (APIs) bereit, über die spezialisierte KI-Anwendungen auf Basis der Foundation Models entwickelt und genutzt werden können.

Die Anbieter:innen der Foundation Models unterstützen auch die Schaffung eines Ökosystems von Startups rund um die Foundation Models. Dies schafft Umsatzpotentiale, die Möglichkeit künftiger Investitionen in erfolgreiche Startups und Unterstützung bei der Diskussion über KI-Regulierungen.

Eine weitere Strategie besteht darin, KI-Systeme in bestehende Angebote zu integrieren. Sowohl Google als auch Microsoft integrieren beispielsweise ihre KI-Chatbots in ihre Suchmaschinen. Meta integriert in WhatsApp, Instagram und Facebook eine persönliche Assistenz sowie eine Reihe von spezialisierten Chatbots, die entweder bekannte Persönlichkeiten imitieren oder spezielle Funktionen wie die von Reisebüro-Angestellten erfüllen. Des Weiteren wurden KI-Werkzeuge entwickelt, um Inhalte auf YouTube und den Diensten von Meta zu modifizieren.

Es ist absehbar, dass die Tech-Konzerne in Zukunft versuchen werden, die Daten ihrer Nutzer:innen für das Training von KI-Systemen zu nutzen. In den letzten Jahren haben sie begonnen, ihre Erfahrungen in der Entwicklung und dem Betrieb von Plattformen sowie beim Verkauf digitaler Güter auf Sektoren wie Bildung, Gesundheit und Landwirtschaft zu übertragen.[4] Die hier anfallenden Daten können verwendet werden, um spezialisierte KI-Systeme zu trainieren. Dadurch gewinnen die Konzerne zunehmend Einfluss auf die Entwicklung von gesellschaftlich wichtigen Sektoren.

Neben Kooperationen mit Organisationen aus diesen Bereichen wie z. B. Krankenhäuser oder Universitäten spielt auch das Ökosystem der Startups eine Rolle, die über APIs mit den Plattformen der großen Technologieunternehmen verbunden sind.

Neben den Foundation Models der Tech-Konzerne existiert eine Reihe von Systemen, die ganz oder teilweise Open Source sind. Dazu gehören Systeme von Startups wie Mistral, die Systeme auf der Hugging-Face-Plattform sowie das von Meta entwickelte Foundation Model Llama2. Die Open-Source-Systeme ermöglichen eine von den Strategien der Anbieter großer Foundation Models unabhängige KI-Entwicklung, wobei der Fokus zurzeit auf geringem Ressourcenbedarf, Optimierung von Trainingsprozessen und Spezialanwendungen liegt. Gleichzeitig laufen Forschungsprojekte, um die Funktionsweise generativer KI-Systeme besser zu verstehen und das Risiko schwerwiegender Fehler zu verringern. Diese Projekte werden allerdings auch von den Tech-Konzernen gefördert, da die hohen Kosten für das Training und den Betrieb großer Foundation Models ein ernstzunehmendes Risiko für die Wirtschaftlichkeit der Investitionen in die Modelle darstellt und aus der Open-Source-Welt kostensenkende Erkenntnisse erwartet werden.

Ein weiterer Kostenfaktor resultiert übrigens aus dem erheblichen Energie- und Wasserbedarf durch den Betrieb der Rechenzentren für Foundation Models.[5] Die Möglichkeiten zur Verbesserung der Energieeffizienz von Rechenzentren sind weitgehend ausgeschöpft. Aufgrund der steigenden Kosten für Energie haben Cloud-Betreiber:innen begonnen, Standorte mit kaltem Klima zu nutzen, um den Kühlungsbedarf zu reduzieren. Darüber hinaus erwägen sie den Bau eigener Kraftwerke in der Nähe ihrer Rechenzentren.

Die Anwender:innen von generativer KI

Eine Flut von KI-Anwendungen durch Unternehmen ist in naher Zukunft trotz des versprochenen Nutzens unwahrscheinlich. Die erste Reaktion auf die Verfügbarkeit von ChatGPT war sogar, die Verwendung für die Arbeit im Unternehmen zu untersagen.[6]

Das Verhalten eines Modells wie ChatGPT ist in vielen Fällen nicht in dem für einen Einsatz in einem Unternehmen notwendigen Maß vorhersagbar. Es ist nicht klar, wie ein KI-System verläßlich daran gehindert werden kann, Ausgaben zu erzeugen, die dem Unternehmen oder seinem Ruf schaden könnten und vielfältige Haftungsrisiken beinhalten, wenn sie in die Öffentlichkeit gelangen.

Foundation Models sind Allzweckwerkzeuge, die durch zusätzliche Komponenten sowie ein Training mit unternehmensinternen Daten an den konkreten Anwendungsfall des Unternehmens angepasst werden müssen. Die Sicherheitsforschung hat demonstriert, dass das Training mit unternehmenseigenen Daten dazu führen kann, dass Geschäftsgeheimnisse oder andere Informationen bekannt werden könnten, die das Unternehmen lieber für sich behalten möchte.

Ein weiteres Hindernis sind Unsicherheiten über künftige KI-Regulierungen und den Umfang der sich daraus ergebenden Sorgfaltspflichten für Anbieter:innen und Nutzer:innen von KI-Systemen. Zwar gibt es gerade von der Angebotsseite eine Diskussion über verantwortliche KI, die jedoch auch dazu dient, dass statt wirkungsvoller staatlicher Regulierungen ein System von Freiwilligkeit aufgebaut wird. In welchem Umfang sich das durchsetzen kann, ist noch absolut unklar.

Um den vollen Nutzen aus generativer KI ziehen zu können, müssen Unternehmen neue Geschäftsprozesse einführen, spezifische Fähigkeiten entwickeln, Wissen aufbauen und ihre Managementprozesse sowie ihre Unternehmenskultur anpassen. Viele Unternehmen zögern, in immaterielle, nicht sofort profitable Vermögenswerte wie die Qualifikation von Mitarbeiter:innen zu investieren. Insbesondere börsennotierte Unternehmen stehen unter erheblichem Druck von großen Investoren, nur kurzfristig rentable Maßnahmen umzusetzen.

Viele Unternehmen setzen nach wie vor darauf, geeignetes Personal aus dem globalisierten Arbeitsmarkt und dem Bildungssystem zu rekrutieren. Dabei wird oft die interne Qualifizierung vernachlässigt, da sie einen hohen Zeit- und Ressourcenbedarf mit sich bringt. Unternehmen erschweren interne Qualifikation auch, indem sie Tätigkeiten, die Anfänger:innen für erste Praxiserfahrungen nutzen könnten, durch KI automatisieren.[7]

Es ist weitgehend anerkannt, dass neue Technologien am besten durch praktische Anwendung erlernt werden.[8] Es genügt jedoch nicht, das eigene Personal zu schulen. Unternehmen müssen auch dazu beitragen, dass die Gesellschaft als Ganzes die Nutzung von KI-Systemen erlernt und versteht.

Unternehmen sind sich durchaus bewusst, dass Lernprozesse ihrer Kunden wichtig sind. Allerdings stoßen sie bei der beliebten Strategie, mit kostengünstigen „Minimum Viable Products" schnell auf den Markt zu kommen und durch Interaktion mit Kunden zu lernen, auf erhebliche Schwierigkeiten. Ein Beispiel dafür ist die Entwicklung eines KI-basierten Chatbots, der das Kontaktzentrum eines Großunternehmens ersetzen oder verkleinern soll. Hierfür wird eine erhebliche Menge sorgfältig ausgewählter und damit teurer Trainingsdaten benötigt, um unerwünschte Interaktionen mit Kunden sicher zu verhindern.[9]

Gesellschaftliches Lernen

Die Digitalisierung, insbesondere der verstärkte Einsatz von KI, ist in unseren wirtschaftlichen und sozialen Strukturen integriert. Eine Entfernung digitaler Technologien würde daher erhebliche Schäden verursachen.

Die Nutzung von KI erfordert breit angelegtes gesellschaftliches Lernen. Menschen müssen lernen, mit KI-Systemen umzugehen, die mit einem unvollständigen und verzerrten Abbild der Welt trainiert wurden, auf Eingaben nach Gesetzen der Wahrscheinlichkeitsrechnung reagieren, auf unberechenbare Weise Fehler machen, auch von ihren Entwickler:innen nur in Ansätzen verstanden werden und mächtige Mechanismen zur Konstruktion von Realität sind.

Die aktuelle Diskussion über die Digitalisierung des Lernens konzentriert sich hauptsächlich auf Schulen und vernachlässigt dabei den eigentlichen Kern des Problems. Es ist zunächst wichtig, dass Erwachsene den Umgang mit KI erlernen. Sie sollten

in der Lage sein, KI-basierte Produkte und Dienstleistungen zu nutzen und mitzugestalten sowie an öffentlichen Diskussionen über deren Nutzung und Grenzen teilzunehmen. Das erworbene Wissen kann dann in den schulischen Lernprozess integriert werden.

Wie jedes IT-System konstruieren KI-Systeme Realität.[10] Beim Maschinenlernen wird dies gesteuert durch die Auswahl der Trainingsdaten. Bei moderner generativer KI, die weitgehend über Unsupervised Learning trainiert wird, sind dies die in den Trainingsdaten enthaltenen Stereotypen und Fakten. Diese Daten sind aber zwangsläufig vergangenheitsbezogen und änderungsfeindlich.

Einen wichtigen Beitrag können die Open-Source-Initiativen auf dem Gebiet der Künstlichen Intelligenz leisten. Die hohen wirtschaftlichen Hürden für die Entwicklung eines neuen Foundation Models machen es praktisch unmöglich, in den von einem Oligopol beherrschten Markt einzudringen, ohne offene Modelle und Daten zu nutzen. Dies betrifft auch nicht-profitorientierte Initiativen. Obwohl die zurzeit verfügbaren Open-Source-Systeme möglicherweise am Ende primär wirtschaftlichen Interessen dienen, ist es nur über offene Modelle und Daten möglich, digitale Souveränität für Anwender:innen, Gesellschaften und Staaten zu erreichen.

In diesem Prozess gesellschaftlichen Lernens haben verschiedene Beteiligte unterschiedliche Bedarfe. Die Dominanz einer Gruppe wie z. B. der Tech-Konzerne kann zu Fehlentwicklungen führen. Zivilgesellschaftliche Organisationen können bei der Gestaltung dieser Multi-Stakeholder-Prozesse eine wichtige Rolle spielen. Sie müssen sich aber neu erfinden und von der notwendigen Kritik zur Gestaltung kommen.

Referenzen

Arrow, K. J. (1962): The Economic Implications of Learning by Doing, in: The Review of Economic Studies, 29(3), S. 155-173. URL: https://doi.org/df2ggr.

Beane, M. (2019): Learning to Work with Intelligent Machines, in: Harvard Business Review, 2019 (September – Oktober).

Brynjolfsson, E., Rock, D. and Syverson, C. (2021): The Productivity J-Curve: How Intangibles Complement General Purpose Technologies, in: American Economic Journal: Macroeconomics, 13(1), S. 333-372. URL: https://doi.org/ghrhpw.

Chui, M. et al. (2023): The economic potential of generative AI. McKinsey. URL: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier [abgerufen am: 1. Juli 2023].

Floyd, C. et al. (Hrsg.) (1992): Software Development and Reality Construction, Berlin, Heidelberg: Springer Berlin Heidelberg. URL: https://doi.org/10.1007/978-3-642-76817-0.

Gupta, A. (2023): Beware the Emergence of Shadow AI, Tech Policy Press. URL: https://techpolicy.press/beware-the-emergence-of-shadow-ai [abgerufen am: 23. Dezember 2023].

Sharon, T. and Gellert, R. (2023): Regulating Big Tech expansionism? Sphere transgressions and the limits of Europe's digital regulatory strategy, Information, Communication & Society [Preprint]. URL: https://doi.org/10.1080/1369118X.2023.2246526.

Smith, G. et al. (2023): Environmental Impact of Large Language Models, Amplify, 36(8).

Solow, R. (1987): We'd better watch out, New York Times Book Review. URL: http://digamo.free.fr/solow87.pdf [abgerufen am: 29. Oktober 2023].

Anmerkungen

1 *Die meisten der öffentlich zugänglichen Studien sind entweder von Produktanbietern finanziert oder dienen zum Kompetenz-Marketing von Unternehmensberatungen. Kompetenz-Marketing demonstriert durchaus Kompetenz und setzt meist auf die für die eigenen Interessen förderliche Präsentation von Fakten.*

2 *Es kann sich laut Brynjolfsson um eine Wartezeit von mehreren Jahrzehnten handeln.*

3 *Die Kosten eines einzigen Trainings-Laufs für GPT-4, dem Foundation Model hinter der neuesten Version von ChatGPT, wurden für 2023 auf 63 Mrd. US$ geschätzt.*

4 *Diese Entwicklung und die damit verbundenen Herausforderungen an die Regulierung von Tech-Konzernen werden in (Sharon/Gellert 2023) diskutiert.*

5 *Mehr Details zu den ökologischen Auswirkungen der KI findet man bei (Smith et al. 2023).*

6 *Viele Mitarbeiter:innen griffen allerdings auf generative KI zurück, um ihre persönliche Produktivität zu steigern, auch im Geheimen auf eigenen Geräten. Die Nutzung geschieht oft ohne ausreichendes Verständnis der Werkzeuge sowie an Governance und Risikomanagement vorbei. Dies kann nicht nur zu Problemen für das Unternehmen, sondern auch zu erheblichen gesellschaftlichen Risiken führen (Gupta 2023).*

7 *Siehe z. B. (Beane 2019).*

8 *Der klassische wirtschaftswissenschaftliche Aufsatz dazu ist (Arrow 1962).*

9 *Das Minimum-Viable-Product-Modell könnte bei der Unterhaltung dienenden ChatBots und anderen Domänen mit geringem Fehlerrisiko durchaus funktionieren.*

10 *Siehe z. B. (Floyd et al. 1992).*

Erich Pawlik

Erich Pawlik ist Software-Ingenieur mit 20 mal zwei Jahren Berufserfahrung. Er befindet sich in der Grauzone zwischen dem Beginn des Rentenalters und dem Ruhestand.
Beruflich hat er auf allen Kontinenten der Welt gearbeitet, mit Ausnahme der Antarktis, und zwei Jahre als mitausreisender Ehemann im südlichen Afrika gelebt. Den größten Teil seiner beruflichen Laufbahn verbrachte er damit, im Dreieck von Sozialpsychologie, Betriebswirtschaft und Technologie konzeptionell zu arbeiten und Organisationen und Projekte zu managen. Aktuell ist er als Berater und Lehrbeauftragter an der Fakultät für Wirtschaftsinformatik der Hochschule Furtwangen tätig.

Verleihung des Weizenbaum-Studienpreises 2023 – Einleitung

Liebe Mitglieder des FIfF,
liebe Freundinnen und Freunde,
liebe Gäste,
liebe Preisträgerinnen des Weizenbaum-Studienpreises 2023,

ich beginne mit einem Zitat von Joseph Weizenbaum, das sich als Leitbild unseres Weizenbaum-Studienpreises eignet. Es betont die Verantwortung, der wir uns stellen müssen:

> *„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."*

Auch in diesem Jahr verleihen 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.

Der Unternehmensgründer und Investor Azeem Azhar, möglicherweise kein FIfF-Mitglied, sagte vor einiger Zeit in einem Interview: „Technology is too important to be left to technologists." Dieser Aussage können wir nur zustimmen. 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.

Wir bedanken uns herzlich für alle Arbeiten, die in diesem Jahr bei uns eingereicht wurden. Die dieses Mal prämierten Arbeiten befassen sich aus unterschiedlichem Blickwinkel mit Datenschutz und Privatheit, im Internet und auch im öffentlichen Raum. Dazu gleich mehr.

Für ihre Mitarbeit in der diesjährigen Jury bedanke ich mich herzlich bei:

1. Professorin Christina Claß aus Jena,
2. Professor Jochen Koubek aus Bayreuth,
3. Professor Dietrich Meyer-Ebrecht aus Aachen,
4. Frieder Strauß aus München,

die mit mir gemeinsam in der Jury die Arbeiten ausgewählt haben, die wir jetzt prämieren werden.

Lelia Friederike Hanslik: Infringements of Bystanders' Privacy through IoT Devices

Masterarbeit an der Technischen Universität Berlin

Für den Kontext und die Zielrichtung des 3. Preises darf ich kurz in das Jahr 2020 zurückgehen:

Im Jahr 2020 wurde der BigBrotherAward, der, so die Eigendarstellung, an *„Firmen, Organisationen und Personen verliehen [wird], die in besonderer Weise und nachhaltig die Privatsphäre von Menschen beeinträchtigen sowie persönliche Daten verkaufen oder gegen ursprüngliche Interessen verwenden"*, in der Kategorie Mobilität an den Elektrofahrzeughersteller Tesla verliehen.

In der Laudatio des Datenschützers Thilo Weichert heißt es dazu:

> *Die Firma Tesla erhält den BigBrotherAward dafür, dass sie Autos verkauft, die ihre Insassen und die Umgebung des Autos umfassend und langfristig überwachen. Die erhobenen Daten werden permanent ausgewertet und können für beliebige Zwecke weiter genutzt werden.*

… und weiter, zitiert aus der Datenschutzerklärung von Tesla: *„Telematikprotokolldaten", „Fernanalysedaten", „weitere Fahrzeugdaten":*

> *Bzgl. der Erfassung „über Ihr Tesla-Fahrzeug" erhebt die Firma den Anspruch, „Wartungshistorie" sowie „Informationen über Ladestationen", als „erweiterte Funktionen" „Navigationsdaten" sowie „kurze Videoaufnahmen von den Außenkameras des Fahrzeugs" zu erfassen.*

Die Videoaufnahmen der Außenkameras werden in der Regel zum einen die Nutzer:innen erfassen, die – so sollte man idealerweise annehmen – sich der mit der Nutzung verbundenen Risiken bewusst sind. Doch Außenkameras können auch Bewegungen in der Umgebung des Fahrzeugs aufzeichnen und gefährden so auch die Privatsphäre Unbeteiligter.

Durch die umfassende Durchdringung der digitalen Gesellschaft mit elektronischen vernetzten Geräten setzen wir uns so Risiken für Privatheit und Datenschutz aus. Diese Risiken sind nicht auf die primären Nutzer:innen der Geräte beschränkt, sondern können auch weitere Personen betreffen.

Mit diesen Risiken für Umstehende, Unbeteiligte (engl. *Bystanders*), also Risiken für die Privatsphäre für Personen, die nicht

selbst Nutzer:innen der vernetzten Geräte sind, setzt sich die Arbeit von **Lelia Friederike Hanslik** auseinander, die wir heute mit einem Weizenbaum-Studienpreis auszeichnen.

Fr. Hanslik ist leider aus gesundheitlichen Gründern verhindert, den Preis entgegenzunehmen.

Die Autorin untersucht die Risiken für *Bystanders* detailliert anhand von drei beispielhaften Anwendungsfällen, wie Daten von „zufällig anwesenden" Dritten in Systemen verarbeitet werden, so Datenschutzgesetze verletzen bzw. verletzen können und in denen dadurch Datenschutz und Privatheit potenziell gefährdet sind.

Die Anwendungsfälle sind:

- die Nutzung intelligenter persönlicher Voice Assistants am Beispiel von Amazons Alexa,
- die Corona-Warn-App und ihre Infrastruktur,
- im Bereich des Straßenverkehrs der Sentry Mode und automatisiertes Fahren bei Fahrzeugen von Tesla.

Dabei orientiert sie sich an zwei Forschungsfragen:

1. Sind Verletzungen der Privatheit von *Bystanders* in den ausgewählten Anwendungsfällen technisch möglich?
2. Wenn ja, in welcher Weise kann die Privatheit der *Bystanders* in den drei gegebenen Anwendungsfällen verletzt werden, und verstößt dies gegen geltendes Datenschutzrecht?

Die Ergebnisse für die einzelnen untersuchten Systeme sind sehr unterschiedlich.

Bei der Analyse des Voice-Assistenten *Amazon Alexa* wird herausgearbeitet, dass sich Alexa im „automatischen Modus" bei Gesprächen ggf. einschaltet und kurze Passagen aufnimmt, und auf den Servern von Amazon auswerten lässt, ob in der Passage eine relevante Aufforderung für Alexa enthalten ist.

Dabei werden ggf. auch Gesprächsinhalte von Besuchern übermittelt. Wenn der Server kein Triggerwort erkennt, wird die Aufnahme des Gesprächs auf dem Alexa-Endgerät wieder gestoppt. Diese Sprech-Schnipsel stellen biometrische Daten dar, die in der DSGVO besonders geschützt werden.

Amazon speichert diese Schnipsel standardmäßig, bis der Benutzer sie löscht. Zur Bewertung ist es relevant, dass Alexa die Sprachaufnahmen den Personen eines Haushalts zuordnen kann, was die Kritikalität der Datensammlung ggf. weiter erhöht.

Frau Hanslik hat die Verwendung dieser Daten durch Amazon untersucht, laut Amazon werden die persönlichen Daten genutzt, um

- *Funktionen, Produkte und Dienstleistungen, die für Sie von Interesse sein könnten, zu empfehlen, und*
- *Ihre Präferenzen zu identifizieren sowie Ihr Erlebnis mit Amazon Services zu personalisieren*

Fr. Hanslik konnte keine von Amazon veröffentlichte Datenschutzfolgeabschätzung auffinden, die in dem dargestellten Umfeld sicher zwingend nötig ist, was sie auch explizit und detailliert herleitet. Sehr schön findet die Jury, dass Fr. Hanslik in der Arbeit auch skizziert, welche Möglichkeiten es für eine datenschutzfreundlichere Umsetzung der Alexa-Services gibt.

Die Grundidee basiert auf einer initialen Verarbeitung der Daten nur auf dem Alexa-Gerät im Haushalt. Nur wenn hier erkannt wird, dass es eine Aufforderung an Alexa gibt, sollen die Daten an die Server zur umfassenden Verarbeitung weitergegeben werden. Dies setzt natürlich eine deutlich teurere Hardware voraus und – was vielleicht noch wichtiger ist – würde wohl auch den Datensammelinteressen von Amazon widersprechen.

Der zweite Anwendungsfall – die *Corona-Warn-App* – kommt bzgl. Einhaltung des Datenschutzes für *Bystanders* deutlich besser weg. Sie ist hinsichtlich der Risiken für Umstehende als unkritisch einzustufen – Risiken können sich aber aus der genutzten Infrastruktur von Apple und Google ergeben.

Der dritte Anwendungsfall des *Tesla Sentry-Mode* möchte ich hier aus Zeitgründen nicht weiter erläutern, wenn Kameraaufnahmen vom parkenden Auto in nicht vorhersehbarer Situation an Tesla geschickt werden und diese quasi beliebig ausgewertet werden können, steht es schlecht für *Bystanders*. Die Empfehlung: am besten frühzeitig die Straßenseite wechseln.

Speziell bei der untersuchten Corona-Warn-App wurde gut herausgearbeitet, dass hier der Datenschutz schon im Design berücksichtigt wurde, bis auf den nicht einsehbaren Code von Google bzw. Apple für den Bluetooth-Austausch, wo nicht klar ist, welche personenbeziehbaren Daten ggf. doch zu Google oder Apple übermittelt werden. Es ist schade, dass die später in der alternativen Corona-Warn-App enthaltene freie Implementierung der Bluetooth-Kommunikation mit anderen Smartphones, die auch diese Lücke schließt, nicht mehr Eingang in die Arbeit gefunden hat.

Im Anschluss an die Arbeit ergeben sich Folgefragen, die die Autorin benennt, aber in diesem Rahmen ebenfalls nicht mehr behandeln kann: unter anderem: Wie können *Bystanders* besser über die Risiken, denen sie ausgesetzt sind, informiert werden?

Wir haben uns entschieden, hier den dritten Preis zu verleihen. Für einen zweiten Preis würden wir uns eine noch weitergehende informatik-spezifischere Betrachtung wünschen. Dies tut der grundsätzlichen Preiswürdigkeit der Arbeit keinen Abbruch. Das datenschutzfreundliche Design der Corona-Warn-App ist erst entstanden, nachdem Google und Apple (und weitere) einen dezentralen Ansatz präferiert haben und der offene Brief vom Chaos Computer Club, der Gesellschaft für Informatik sowie weiteren Organisationen die anstehende Entscheidung für ein zentrales Speichern der Kontaktdaten kritisiert haben.

Ausgehend nicht nur von dieser Arbeit wäre auch eine Diskussion spannend, ob die derzeitigen Gesetze nicht eigentlich schon ausreichen, um diese Datenschutzverletzungen durch den Staat

verfolgen zu müssen. Zugestehen müssen wir aber, dass die immer stärkere Verlagerung der Durchsetzung der Gesetze vom Staat auf das Individium ein insgesamt ungelöstes Problem ist, insbesondere wenn es um internationale Wirtschaftskonzerne geht.

Mit sowohl quellenreicher als auch kompakter Darstellung bietet die Arbeit eine überzeugende Dokumentation möglicher Bedrohungsszenarien durch mobile Anwendungen. Die Verfasserin zeigt einerseits großes Verständnis der untersuchten technischen Systeme, andererseits einen breiten Horizont, der auch ethische, rechtliche und gesellschaftliche Fragen einbezieht. Der Arbeit gelingt eine sachliche und unaufgeregte Diskussion möglicher Risiken beim Einsatz vernetzter, datenverwertender Technologien.

Herzlichen Glückwunsch, Lelia Friederike Hanslik, zum Weizenbaum-Studienpreis 2023.

Lelia Friederike Hanslik

Infringements of Bystanders' Privacy through IoT Devices

3. Preis

Zusammenfassung

Die Verbindung von immer mehr Geräten mit dem Internet (allgemein als Internet der Dinge, IoT, bezeichnet) birgt neue Gefahren für die Privatheit von Menschen, besonders in Bezug auf die Verarbeitung und Speicherung personenbezogener Daten. Diese potentiellen Bedrohungen der Privatheit können sowohl die Nutzer:innen dieser Geräte als auch andere Personen betreffen, die von den Entscheidungen dieser Nutzer:innen betroffen sind (hier wird der Begriff *Bystanders* verwendet). Die zunehmende Menge an Informationen, die über Einzelpersonen zur Verfügung stehen, hat auch zu einem weiteren Phänomen geführt, der algorithmischen Gruppierung zum Zweck der gezielten kommerziellen Werbung und des (Gruppen-) Profilings (Taylor et al., 2017). Obwohl dies nicht der Schwerpunkt dieser Arbeit war, wurde das Konzept der *Group Privacy* und Gruppierung bei der Erörterung der Verletzung der Privatheit von Bystanders berücksichtigt. Eine Unterscheidung von Nutzer:in, Bystander und Gruppe ist in der nachfolgenden Grafik dargestellt.

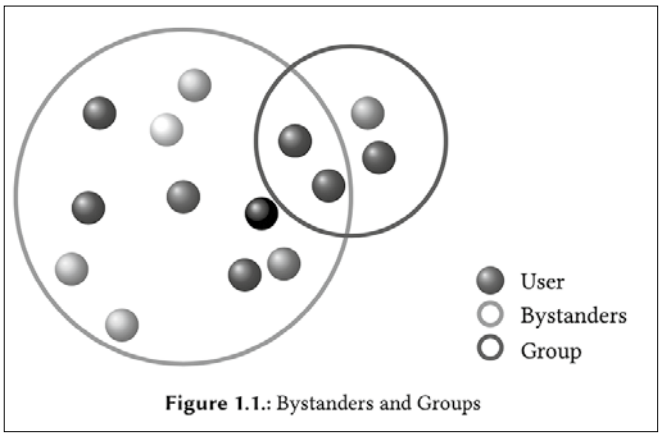


Figure 1.1.: Bystanders and Groups

In der aktuellen Forschung liegt der Schwerpunkt im Zusammenhang mit IoT-Geräten auf dem/der Nutzer:in. Wenn hingegen die Abhängigkeit der Privatheit von Menschen untereinander anhand eines konkreten Beispiels untersucht wird, dann geschieht dies hauptsächlich im Bereich der sozialen Online-Netzwerke. Es besteht daher eine Forschungslücke, in der die Gefahren für die (voneinander abhängige) Privatheit von Individuen, die nicht selbst Nutzer:in sind, anhand von Beispielen außerhalb der sozialen Online-Netzwerke untersucht werden. In dieser Arbeit wurden Anwendungsfälle rund um drei IoT-Geräte und -Anwendungen untersucht und im Hinblick auf die technische und rechtliche Möglichkeit von Datenschutzverletzungen für unbeteiligte Bystanders bewertet. Bei diesen Anwendungsfällen handelt es sich um intelligente persönliche Sprachassistenten, die deutsche Corona-Warn-App und den Wächtermodus (*Sentry Mode*) des Elektrofahrzeugherstellers Tesla. Die Analyse der Anwendungsfälle erfolgte auf der Grundlage von Szenarien, die erstellt wurden, um eine ganzheitliche Sicht auf die Interaktion von Nutzer:innen und Unbeteiligten mit dem Gerät zu ermöglichen.

Die Forschungsfragen, die die Analyse leiteten, lauten: (1) Sind Verletzungen der Privatheit von Bystanders in den ausgewählten Anwendungsfällen technisch möglich? und (2) Wenn ja, in welcher Weise kann die Privatheit der Bystanders in den drei gegebenen Anwendungsfällen verletzt werden und verstößt dies gegen geltendes Datenschutzrecht?

Die Auswahl der Anwendungsfälle

Die drei IoT-Anwendungsfälle, die für die Untersuchung der Verletzung der Privatheit von Bystanders ausgewählt wurden, weisen mehrere Unterschiede aber auch Ähnlichkeiten auf. In allen Anwendungsfällen spielt die Gefahr der Überwachung eine zentrale Rolle und alle drei IoT-Anwendungsfälle sind alltägliche Systeme, die einen bedeutenden Einfluss auf die Gesellschaft haben, da sie von Millionen von Nutzern weltweit, auch in Deutschland, verwendet werden. So besitzen beispielsweise 33 % der deutschen Haushalte einen intelligenten Lautsprecher, der im Jahr 2021 in ihrem Haushalt installiert ist (Statista, 2021), während auch andere Geräte wie Mobilgeräte die technologischen Funktionen eines intelligenten persönlichen Sprachassistenten tragen, wobei Schätzungen zufolge bis 2024 weltweit mehr als 8 Milliarden digitale Sprachassistenten im Einsatz sein werden (Thormundsson, 2022). Amazon gab im Jahr 2019 bekannt, dass das Unternehmen über 100 Millionen Alexa-fähige Geräte verkauft hat (Bohn, 2019). Im Szenario rund um den Anwendungsfall intelligenter persönlicher Sprachassistenten

wurde daher der Sprachassistent Alexa als spezifisches Beispiel gewählt, da er der am häufigsten verwendete intelligente persönliche Sprachassistent in der Kategorie der *Smart Speaker* ist (im Gegensatz zu Smartphones, wo Apples Siri am häufigsten verwendet wird) (Vixen Labs. Open Voice Network, 2021). Die Corona-Warn-App wurde in Deutschland im Zeitraum zwischen der Erstveröffentlichung am 15. Mai 2020 und Ende Juni 2022 45.992.847-mal heruntergeladen (Robert Koch Institut, 2022a). Während die meisten in Deutschland zugelassenen Fahrzeuge von Volkswagen und Mercedes hergestellt werden (Kraftfahrt-Bundesamt, 2022a), hatte Tesla den höchsten Zuwachs an Fahrzeugen in Deutschland (Kraftfahrt-Bundesamt, 2022c). Neben der gesellschaftlichen Relevanz, der Überwachungsgefahr und der hohen Nutzerakzeptanz in Deutschland gibt es Konzepte, die alle drei Anwendungsfälle in gleicher Weise beeinflussen, wie z. B. das *Privacy Paradoxon* (Kokolakis, 2017), bei dem das tatsächliche Verhalten der Nutzer von der theoretischen Sichtweise abweicht. Darüber hinaus stehen alle drei Anwendungsfälle in demselben Spannungsfeld gegensätzlicher Prioritäten, nämlich der Verbesserung der Privatsphäre für einzelne Nutzer einerseits und der Verbesserung der Dienstqualität insgesamt andererseits. Diese Sichtweise wird jedoch meist von den Unternehmen vertreten, die diese Geräte entwickeln. In der Forschungsgemeinschaft gibt es zahlreiche Stimmen, die diese Ansicht widerlegen und Ansätze vorlegen, wie Datenschutz und Effizienz tatsächlich Hand in Hand gehen können (Hoepman, 2012). Während der obige Absatz einige der Gemeinsamkeiten der Anwendungsfälle zusammenfasst, gibt es auch Achsen, entlang derer sich Unterschiede ausmachen lassen. Das wichtigste Beispiel ist der Raum, in dem das Gerät verwendet wird. Intelligente persönliche Sprachassistenten werden in den eigenen vier Wänden, also im privaten Bereich, eingesetzt. Ein Tesla-Fahrzeug bewegt sich meist auf öffentlichen Straßen und ist Teil des öffentlichen Lebens, und das Gerät, das die Corona-Warn-App beherbergt, wird die meiste Zeit mit sich herumgetragen und misst, wie oft und mit wem sich die Nutzer treffen, daher kann es im sozialen Raum verortet werden. Diese Unterschiede zeigen, dass kaum ein Raum, ob privat oder öffentlich, von Systemen unberührt bleibt, die wissentlich oder unwissentlich Daten über uns sammeln.

Ergebnisse der Arbeit

Während die Corona-Warn-App kein realistisches Potential für die Verletzung der Privatheit von Umstehenden bietet und somit keine weitere Forschung diesbezüglich erfordert, kam die Analyse der weiteren beiden Fälle zu einem gegenteiligen Ergebnis. Intelligente persönliche Sprachassistenten und der Wächtermodus von Tesla bieten nach den Analysen dieser Arbeit technisch realistisches Potential für die Verletzung der Privatheit von Unbeteiligten sowie Potenzial für die Verletzung der geltenden Datenschutzgrundverordnung und sollten weiter erforscht werden. In beiden Anwendungsfällen können die Verletzungen der Privatheit für Unbeteiligte sowohl vom/von der Nutzer:in als auch von der Systemarchitektur selbst ausgehen. Die Evaluierung dieser Anwendungsbeispiele bezüglich der Privatheit von Unbeteiligten hat einen wichtigen Beitrag zur aktuellen Forschung geleistet, da sie eine Grundlage für weitergehende Forschung bietet.

Referenzen

[Statista 2021] Anteil der Haushalte in Deutschland mit Smart Speaker bis 2021. In: Statista, 2021. – https://de.statista.com/statistik/daten/studie/1271603/umfrage/anteil-der-haushalte-in-deutschland-mit-smart-speaker/

[Thormundsson 2022] Thormundsson, Bergur: Virtual Assistant Technology – Statistics Facts. In: Statista, 2022. – https://www.statista.com/topics/5572/virtual-assistants [Accessed: 25th May 2022]

[Bohn 2019] Bohn, Dieter: Amazon says 100 million Alexa devices have been sold – what's next? In: The Verge (2019). – https://www.theverge.com/2019/1/4/18168565/ amazon-alexa-devices-how-many-sold-number-100-million-dave-limp [Accessed: 1st June 2022]

[Vixen Labs. Open Voice Network 2021] Voice assistant usage in Germany in 2021, by provider and device. In: Statista, 2021. – https://www.statista.com/statistics/1274452/voice-assistant-use-by-device-germany/ [Accessed: 25th May 2022]

[Robert Koch Institut 2022a] Corona-Warn-App (CWA): Kennzahlen – Downloads. 2022. – https://www.coronawarn.app/de/analysis/ [Accessed: 28th June 2022]

[Kraftfahrt-Bundesamt 2022a] Anzahl der Personenkraftwagen in Deutschland nach Marken von 2020 bis 2022. In: Statista, April 2022. – https://de.statista. com/statistik/daten/studie/159344/umfrage/pkw-bestand-in-deutschland-nach-marken/ [Accessed: 25th May 2022]

[Kraftfahrt-Bundesamt 2022c] Prozentuale Veränderung der Anzahl der Personenkraftwagen in Deutschland nach Marken im Vergleich der Jahre 2021 und 2022. In: Statista, March 2022. – https://de.statista.com/statistik/daten/studie/4964/ umfrage/veraenderung-des-pkw-bestandes-nach-marken/ [Accessed: 25th May 2022]

[Kokolakis 2017] Kokolakis, Spyros: Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. In: Computers & Security 64 (2017), p. 122–134. – https://doi.org/10.1016/j.cose.2015.07.002

[Hoepman 2012] Hoepman, Jaap-Henk: Privacy Design Strategies. In: IFIP TC11 Int. Information Security Conference 2014, October 2012. – https://doi.org/10.1007/978-3-642-55415-5_38

Lelia Friederike Hanslik

Lelia Hanslik studierte Mathematik (B.Sc.) und Wirtschaftsinformatik (M.Sc.) in Berlin und setzt sich seitdem kritisch mit den Machtverhältnissen zwischen Unternehmen, Politik, der Zivilgesellschaft und einzelnen Konsument:innen in der Software-Industrie auseinander. Sie engagiert sich außerdem für mehr (Sichtbarkeit von) FLINTA* Personen in MINT Berufen.

Anne Mareike Lisker: Von der (Un-)Möglichkeit, digital mündig zu sein. Tracking-Infrastrukturen und die Responsibilisierung des Individuums im Internet

Masterarbeit an der Technischen Universität Berlin

Wenn wir uns im Internet bewegen, setzen wir uns vielfältigen Risiken für den Datenschutz aus. Die Geschäftsmodelle großer Internet-Konzerne fußen darauf, unser Verhalten im Netz und unsere Daten zu nutzen, als Gegenleistung dafür, dass viele Dienste unentgeltlich zur Verfügung gestellt werden.

Die Daten, die über uns gesammelt werden, werden für unterschiedliche Zwecke verwendet. Dies erfolgt hauptsächlich durch die Werbewirtschaft, die die Daten dafür nutzt, unser Konsumverhalten zu untersuchen und Werbebotschaften individuell platzieren zu können. Gleichzeitig wird der Internetverkehr in zunehmendem Maß durch (Sicherheits-) Behörden überwacht, mit dem Argument der Strafverfolgung und Terrorismusbekämpfung – wir erinnern uns an die Vorratsdatenspeicherung und die inzwischen auch schon wieder zehn Jahre zurückliegenden Enthüllungen von Edward Snowden. Auch Verfahren der Künstlichen Intelligenz spielen dabei eine Rolle – sie nutzen unsere Inhalte und lassen sie in häufig intransparenter Weise in entsprechende Anwendungen einfließen; sie können aber auch zunehmend für die Analyse der gesammelten Daten genutzt werden, um neue Erkenntnisse über uns zu gewinnen.

Um sich vor übermäßigem Datensammeln zu schützen, wird die Forderung nach Digitaler Mündigkeit bei der Internetnutzung erhoben, also sich bei der Netznutzung des eigenen Verstandes zu bedienen – Nutzer:innen sollen sich der Risiken im Netz bewusst sein und sich entsprechend verhalten: beispielsweise indem sie datenschutzfreundliche Werkzeuge nutzen und bei der Konfiguration dieser Werkzeuge auf datenschutz-wahrende Einstellungen achten.

Doch solche Forderungen wälzen Verantwortung auf die Nutzer:innen ab, die sie in der Praxis des weltweiten unkontrollierbaren Netzes nicht wahrnehmen können; sie implizieren, dass sie in der digitalen Welt individuell für den Fluss und die Kontrolle ihrer eigenen Daten verantwortlich sind. Nicht mehr die Anbieter im Netz sind für die datenschutzfreundliche, sichere Abwicklung verantwortlich, sondern die Nutzer:innen sollen gefälligst selbst für ihre Sicherheit sorgen. Natürlich gibt es Regeln, die die Sicherheit im Netz sicherstellen sollen. Doch können wir immer auf die Einhaltung von Regeln wie der Datenschutz-Grundverordnung vertrauen – im weltweiten Netz? Sind die Regeln immer angemessen und ausreichend? Und können solche Regelungen alle Risiken umfassend abdecken? Können wir erwarten, dass wir uns darauf verlassen dürfen – wie wir uns im Alltag darauf verlassen, dass Hygienebedingungen in der Lebensmittelindustrie oder die technische Sicherheit von Automobilen sichergestellt sind?

Mit der Forderung nach Digitaler Mündigkeit und ihrer Erfüllbarkeit setzt sich die Arbeit von Anne Mareike Lisker auseinander, die wir heute mit dem Weizenbaum-Studienpreis auszeichnen.

Ausgangspunkt ist Digitale Mündigkeit. Mündigkeit impliziert eine Eigenverantwortung, bei der die Menschen „sich um bestimmte Dinge selbst kümmern müssen".

In der zentralen These der Arbeit stellt die Autorin dar:

> *Die als individuelle Datenflusskontrolle verstandene Forderung nach digitaler Mündigkeit stellt demnach uneinlösbare Ansprüche an Individuen und ist deshalb unangemessen. … Die resultierende Dynamik – die Übertragung von Verantwortung auf Individuen, ohne dass sie dieser Verantwortung gerecht werden können – [entspricht] der neoliberalen Regierungslogik der Responsibilisierung.*

Psychologische Methoden der Beeinflussung legen die Grundlage für die weitergehende Datenanalyse, die unsichtbar im Hintergrund stattfindet: Tracking und Auswertung des Verhaltens der Benutzer:innen durch

- Cookies und Marktinfrastruktur,
- weitere Trackingtechnologien, wie URL-Tracking, Fingerprinting etc.,
- prädiktive Analytik,
- Modellierung des Verbraucherverhaltens und Personalisierung.

Aus der Analyse dieser Techniken leitet die Autorin vier Zwischenfazits zum Datensammeln ab, die in der Summe ihre These der allumfassenden, unausweichlichen Datensammlung stützen:

- das Datensammeln ist kontinuierlich, komplex und unsichtbar,
- überall und unausweichlich,
- prädiktiv,
- das Datensammeln ist dividuierend.

Sicher wird die Autorin gleich in ihrem Vortrag im Detail auf diese Konzepte eingehen, die im Mittelpunkt der Arbeit stehen.

Aus den so hergeleiteten Eigenschaften ergibt sich, dass Individuen keine Kontrolle über Datenspuren im Netz haben können. Die Forderung nach digitaler Mündigkeit kann nicht erfüllt werden und wälzt lediglich die Verantwortung auf die Nutzenden ab, führt also zu einer Responsiblisierung des Individuums, so die Autorin.

Die Arbeit behandelt mit der immer weiter anwachsenden Überwachung und Datensammlung – gerade auch im Kontext der Entwicklung der künstlichen Intelligenz – ein wichtiges, aktuelles Thema. Die Kernthese der neoliberalen Responsibilisierung als Folge der Erwartung, stets digital mündig zu sein, wird deutlich dargelegt und überzeugend und schlüssig aus den tatsächlich vorhandenen Technologien hergeleitet und begründet. Auch die technische Basis des Datensammelns – die Technologien des

Datentracking – werden umfassend und verständlich beschrieben und legen so eine solide Grundlage für die weiterführenden Überlegungen.

Herzlichen Glückwunsch, Anne Mareike Lisker, zum Weizenbaum-Studienpreis 2023.

Anne Mareike Lisker

Von der (Un-)Möglichkeit, digital mündig zu sein

1. Preis

Seit 25 Jahren kursiert die Forderung nach digitaler Mündigkeit durch den netzpolitischen Diskurs. Durch die Forderung werden wir als individuelle Nutzer:innen des Internets unter anderem dazu angehalten, Kontrolle über unsere eigenen Daten auszuüben. Die Kontrolle von Daten ist wesentlich, denn automatisierte Diskriminierung durch datenbasierte Machine-Learning-Systeme ist ein drängendes Problem. Doch ‚unsere' Daten sind Teil einer hochkomplexen Marktinfrastruktur, die das Internet durchzieht und die Profitinteressen großer Plattformen befriedigt. Ich argumentiere in diesem Beitrag deshalb dafür, dass wir nicht in der Lage dazu sind, der Verantwortung, Kontrolle über unsere eigenen Daten zu haben, gerecht zu werden. Dass wir dennoch dafür verantwortlich gemacht werden, ist ein Fall von Responsibilisierung: einem Regierungswerkzeug des Neoliberalismus.

Digitale Mündigkeit als Universalmittel

Seit fast 25 Jahren kursiert die Forderung nach digitaler Mündigkeit durch den netzpolitischen Diskurs. Dabei wird das Konzept als Universalmittel gehandelt, um den problematischen Entwicklungen und Herausforderungen zu begegnen, die durch digitale Technologien entstehen. Im Kontext von digitaler Mündigkeit wird häufig gefordert, dass Nutzer:innen dieser Technologien – insbesondere des Internets – die Kontrolle über ihre eigenen Daten haben sollen.

Automatisierte Diskriminierung, oder: Warum Daten kontrolliert werden müssen

Seit wiederum fast 10 Jahren wird eine rege öffentliche Debatte über Systeme geführt, die mithilfe von Methoden der künstlichen Intelligenz und des maschinellen Lernens automatisierte Entscheidungen treffen und dabei historisch bedingte Diskriminierungsstrukturen reproduzieren und verstärken [1], [2], [3], [4]. Solche Systeme werden unter anderem im Marketing, in Einstellungsprozessen, bei der Vergabe von Krediten oder in der Strafverfolgung eingesetzt und haben somit Einfluss auf den Lebensverlauf. Besonders prominent war der Fall der Software COMPAS, die in einigen Staaten der USA vor Gericht verwendet wird, um Vorhersagen über das Rückfallrisiko von Angeklagten bzw. Gefängnisinsass:innen zu treffen – und dabei Menschen aufgrund ihrer Race [5] systematisch diskriminierte. So wurden zum einen fast doppelt so häufig schwarze Menschen fälschlicherweise als rückfällig bewertet und zugleich weiße Menschen häufiger fälschlicherweise als risikoarm eingestuft [6]. Ein System von Amazon, das automatisiert über die Geeignetheit von Bewerber:innen für einen Job entscheidet, stufte Frauen bei gleicher Qualifikation systematisch als weniger geeignet ein als männliche Bewerber [7]. Werbeanzeigen auf Facebook zeigten Frauen weniger häufig Anzeigen für Stellen als Softwareentwickler:innen an als Männern; und Häuser wurden vorwiegend weißen Personen zum Kauf angeboten, während BIPoC-Personen [8] vor allem Mietshäuser angezeigt wurden [9].

Anne Mareike Lisker bei der Präsentation ihrer Masterarbeit
Quelle: https://media.ccc.de/b/conferences/fiffkon#t=4

Bemerkenswerterweise ‚kannte' keines dieser Systeme die Kategorien, auf Basis derer Menschen durch das System diskriminiert wurden. COMPAS ‚wusste' nicht, welcher Race die Angeklagten angehören; die Entwickler:innen des Algorithmus von Amazon hatten die Kategorie ‚Geschlecht' ausgespart und auch Facebook schließt – theoretisch, und als Reaktion auf mehrere Strafverfahren – explizit sensible Kategorien in den Targeting-Mechanismen seines Werbesystems aus. Dass in den Systemen dennoch historisch bedingte strukturelle Ungleichverteilungen reproduziert werden, liegt an sogenannten Proxy-Merkmalen. Proxy-Merkmale sind zunächst scheinbar harmlose Attribute – wie beispielsweise eine Postleitzahl – die mit sensiblen Kategorien korrelieren und somit als Stellvertreter für diese sensiblen Kategorien dienen [10]. So wurde bei COMPAS unter anderem eben die Postleitzahl der Angeklagten erfragt. Da Stadtviertel in den USA häufig homogen sind in Bezug auf die Race ihrer Bewohner:innen, korrelierte die Postleitzahl also mit der Kategorie Race und fungierte als deren Proxy. Durch Proxy-Merkmale lassen sich also aus vermeintlich harmlosen Daten sensible Merkmale wie das Geschlecht, die Race oder die Sexualität ableiten auf Basis derer Menschen automatisiert und kollektiv diskriminiert werden. Es gilt also, Daten zu schützen und zu kontrollieren.

Ok, stimmt! Die Daten müssen kontrolliert werden. Aber …

Die Kontrolle von Daten obliegt den Nutzer:innen, die durch die Forderung nach digitaler Mündigkeit dafür verantwortlich gemacht werden, den Fluss ihrer eigenen Daten zu kontrollieren. Der Kontrollmechanismus, der darin impliziert wird, ist ein individueller: Einzelpersonen sollen für die Kontrolle ihrer vermeintlich eigenen Daten zuständig sein. Das ist ein naheliegendes Vorgehen, wenn Daten als ein ‚Rohstoff' inszeniert werden, der auf ganz ‚natürliche' Art und Weise von uns als Nutzer:innen erzeugt und besessen wird. Wenn etwas in meinem Besitz ist – so die Annahme – kann ich selbstverständlich auch kontrollieren, wie viel ich davon abgeben und wie viel ich zu meinem eigenen Vergnügen behalten möchte.

Fakt ist jedoch, dass Daten hauptsächlich von den großen Unternehmen und Plattformen generiert werden, deren Services die Nutzer:innen meist mit einer ganz anderen Absicht in Anspruch nehmen, und dass diese Unternehmen so viele Daten generieren und sammeln, wie sie nur kriegen können. Ich plädiere daher auch dafür, {Dld}aten nicht mehr als ein Substantiv zu verwenden, sondern als ein Verb, einen Prozess, einen Vorgang zu denken. Das ermöglicht eine Abwendung von der Idee des Rohstoffes und verdeutlicht zugleich die praxeologische Ebene des Datenflussprozesses: Daten werden immer situativ erzeugt, aggregiert, ausgewertet, angewendet.

Ein Blick in die Entstehungsgeschichte der cookifizierten Marktinfrastruktur

In den letzten 30 Jahren ist eine datenbasierte Marktinfrastruktur entstanden, deren Grundstein Warenkorb- und Sitzungscookies legten, die im Jahr 1994 von Software-Entwicklern des Unternehmens Netscape entwickelt wurden. Cookies waren die Lösung für das aus der Zustandslosigkeit des Hypertext Transfer Protocols resultierende Problem, dass Nutzer:innen bereits durch einen Subdomänenaufruf nicht wiedererkannt werden konnten, was insbesondere kommerzielle Vorhaben wie beispielsweise einen Warenkorb verunmöglichte. Vor der Einführung von Cookies war das Browsen im Internet im Grunde genommen ein privater Akt. Neben Cookies wurden auch andere Lösungsvorschläge diskutiert, unter anderem die Idee, jedem Browser eine eindeutige Identifikationsnummer zuzuteilen. Der Entwickler Lou Montulli sah damals in Browser-IDs jedoch die Gefahr eines websiteübergreifenden Trackings und lehnte diesen Vorschlag ab [11]. Es entbehrt nicht einer gewissen Ironie, dass das Tracking eine Eigenschaft ist, die Cookies zum Zeitpunkt ihrer Erfindung keinesfalls erfüllen sollten. Die Lösung für das aus der Zustandslosigkeit resultierende Problem führte also ein neues Problem mit sich: den Verlust der Privatsphäre.

Nach den Warenkorb- und Sitzungscookies entstanden Erstanbieter-Analysecookies, mit denen Besucher:innen über eine Seite hinweg von den Anbietern verfolgt werden konnten. Darauf folgten Drittanbietercookies, die websiteübergreifendes Tracking durch einen außenstehenden Akteur ermöglichten. Diese Entwicklung geschah in koerziver Wechselwirkung mit der Werbeindustrie, welche sich Cookies als Marketingwerkzeug aneignete. Zu Beginn war Onlinewerbung noch an traditionellen Medien wie Print oder Fernsehen orientiert und die Zielgruppenansprache basierte auf groben Kategorien wie Alter, Geschlecht oder Einkommen. Werbung für Sportschuhe wurde auf einer Website mit Sportartikeln angezeigt. Erstanbieter-Analysecookies ermöglichten, in einem Onlineshop auch Werbung für Sportschuhe in der Technikrubrik anzuzeigen, weil die Nutzerin sich zuvor Sportschuhe angesehen hatte. Mit Drittanbietercookies lässt sich einer Nutzerin Werbung für Sportschuhe auf der Website eines Nachrichtendienstes anzeigen, weil dem Drittanbieter bekannt ist, dass die Nutzerin vor Tagen in einem Onlineshop Sportschuhe angeschaut hatte. Der Verkauf der Werbeflächen passiert inzwischen algorithmisch automatisiert an Werbebörsen und innerhalb von Millisekunden in Echtzeit. Durch diese Entwicklung ist um Cookies herum eine riesige Marktinfrastruktur entstanden, die darauf basiert, mithilfe von Tracking Daten zu generieren, mit diesen Daten Wissen zu produzieren und dieses Wissen zu kapitalisieren [12].

Allein auf den 1.000.000 meistbesuchten Websites werden 30.000.000 Trackingtechnologien eingesetzt [13]. Das heißt im Umkehrschluss für die allermeisten von uns Nutzer:innen, dass im Prinzip jede von uns von Trackingtechnologien betroffen ist. Im Gegensatz dazu wird der Werbemarkt nur von einer Handvoll Akteuren beherrscht, welche zwar augenscheinlich keine reinen Marketingunternehmen sind – allen voran Google –, deren Geschäftsmodell im Kern jedoch weiterhin auf Daten basiert.

Aber was ist denn mit Schutzmaßnahmen wie Privacy-Add-Ons?

Es existieren zahlreiche Maßnahmen, die die Privatsphäre der Nutzer:innen im Netz stärken oder schützen sollen, indem sie Tracking beispielsweise durch Cookies blockieren, erschweren oder kontrollieren. Dazu gehören zum einen die durch die ePrivacy verpflichtend gewordenen Cookie-Banner, aber auch das schlichte Deaktivieren von Cookies im Browser, Privacy-Add-Ons oder individuelle Browsereinstellungen. Der Wirtschaftswissenschaftlerin Shoshana Zuboff zufolge schützen solche individuellen Maßnahmen allerdings immer nur einige Menschen vor bestimmten Tracking-Mechanismen [14]. In diesen Einzelfällen sind sie zwar wirksam, doch sorgt ihre schiere Existenz dafür, den Status Quo des Tracking paradoxerweise aufrecht zu erhalten. Denn sie erscheinen als vermeintliche Lösung für das durch Trackingtechnologien ausgelöste Datenschutzproblem, weshalb von einer gesamtheitlichen Lösung abgesehen wird.

Prädiktive Analytik, oder: Wieso ich eigentlich nicht nur meine Daten kontrollieren müsste

Selbst, wenn wir einräumen, dass individuelle Datenschutzmaßnahmen bestimmte Menschen vor bestimmten Trackingtechnologien schützen können, so können sie auch in den Fällen regelrecht unwirksam werden. In der Werbebranche werden statistische Verfahren wie prädiktive Analytik eingesetzt, die es ermöglichen, aus einer riesigen Menge von Daten auch Informationen über eine mehr oder weniger unbekannte Person abzuleiten bzw. vorherzusagen. Wir können uns das folgendermaßen vorstellen: Wenn 7 von 10 Menschen, die weiße Turnschuhe tragen, auch mitteilen, dass sie am liebsten Vanille-

eis mögen, so sagt ein prädiktives Modell voraus, dass eine unbekannte Person mit weißen Schuhen mit einer Wahrscheinlichkeit von 70 % Vanilleeis mag. Diese Wahrscheinlichkeit reicht einem Lebensmittelhersteller aus, um die unbekannte Person als Vanilleeisliebhaberin zu klassifizieren. Nun sind Schuhfarbe und Speiseeispräferenz zumindest im globalen Norden und vermutlich auch weltweit keine politischen Kategorien, sondern unbedenkliche Vorlieben. In der Realität werden jedoch mittels prädiktiver Analytik aus vermeintlich unverfänglichen, frei verfügbaren und zum Teil anonymen Daten wie Facebook-Likes oder dem Browserverlauf Rückschlüsse auf sensible Attribute wie die Sexualität, Race, Persönlichkeitseigenschaften, den Suchtmittelkonsum oder die mentale Gesundheit der Person gezogen [15]. Dass das möglich ist, liegt daran, dass über einige wenige Nutzer:innen sehr viele – zum Teil auch sensible – Daten generiert werden konnten, welche zusammen mit zahlreichen anderen, scheinbar unverfänglichen Hilfsdaten in das prädiktive Modell geflossen sind. Diese Daten haben einen unmittelbaren Einfluss darauf, welche Vorhersagen über alle möglichen anderen Personen getroffen werden können. In Abbildung 1 hat der Philosoph Rainer Mühlhoff den Zusammenhang veranschaulicht [16].

Dass aus dem Zusammenspiel der sensiblen Daten einzelner weniger Nutzer:innen mit der enormen Menge vermeintlich unverfänglicher Daten aller Nutzer:innen über eine beliebige andere Nutzerin Informationen abgeschätzt werden können, hat zur Folge, dass individuelle Datenschutzeinstellungen an Wirksamkeit verlieren. Denn die strengen Datenschutzeinstellungen eines datensparsamen Individuums schützen dieses nur bedingt davor, identifiziert zu werden. Wohlgemerkt bezieht sich die ‚Identifikation' in diesem Kontext nicht darauf, ein Individuum als eine bestimmte Person mit einem bestimmten Namen, Geburtsdatum oder Wohnort zu lokalisieren. Solche Informationen sind für die Unternehmen kaum von Relevanz, weshalb auch eine Anonymisierung von Daten vor einer Identifikation durch prädiktive Analytik nicht schützt. Vielmehr geht es den Unternehmen darum, die Wünsche und Bedürfnisse des Individuums zu erkennen und sie profitmaximierend zu nutzen – oder die Wünsche und Bedürfnisse des Individuums überhaupt erst zu erzeugen und zu formen. Auf der anderen Seite stehen die ‚datenfreigiebigen' Individuen, über die absichtlich oder unabsichtlich eine große Menge an Daten generiert werden kann – beispielsweise, weil sie überzeugt davon sind, ‚nichts zu verbergen zu haben. Deren Datenschutzeinstellungen haben einen umso stärkeren Effekt. Sie bedingen, was über andere Nutzer:innen vorhergesagt werden kann und wie identifizierbar sie selbst und andere Individuen sind. Einige Wissenschaftler plädieren daher dafür, die Validität des Rechtsmechanismus der Einwilligung, mit welcher heutzutage vorwiegend das Sammeln von Daten rechtlich abgesichert wird, in Frage zu stellen [17, 18]. Denn die Konsequenzen der Einwilligungsentscheidung betreffen nicht nur das einwilligende Individuum selbst, sondern auch andere Nutzer:innen.

Das bedeutet für die Forderung nach digitaler Mündigkeit, dass Kontrolle über die eigenen Daten haben zu sollen, impliziert, Kontrolle über die Daten aller Nutzer:innen haben zu müssen. Denn wenn eine Nutzerin ihre Daten insofern kontrollieren möchte, dass keinerlei sensible Informationen über sie bekannt sind, sensible Informationen über sie jedoch mittels prädiktiver Analytik ableitbar sind, dann reicht es nicht, nur die eigenen Daten zu kontrollieren – sie müsste auch die Daten aller anderen Nutzer:innen kontrollieren. ‚Alle anderen' bezieht sich nicht nur auf die zum Datenerhebungszeitpunkt aktiven Nutzer:innen, sondern auch auf Nutzer:innen aus der Vergangenheit sowie auf alle zukünftigen Nutzer:innen, da deren Daten ebenfalls in das prädiktive Modell geflossen sind und fließen werden.

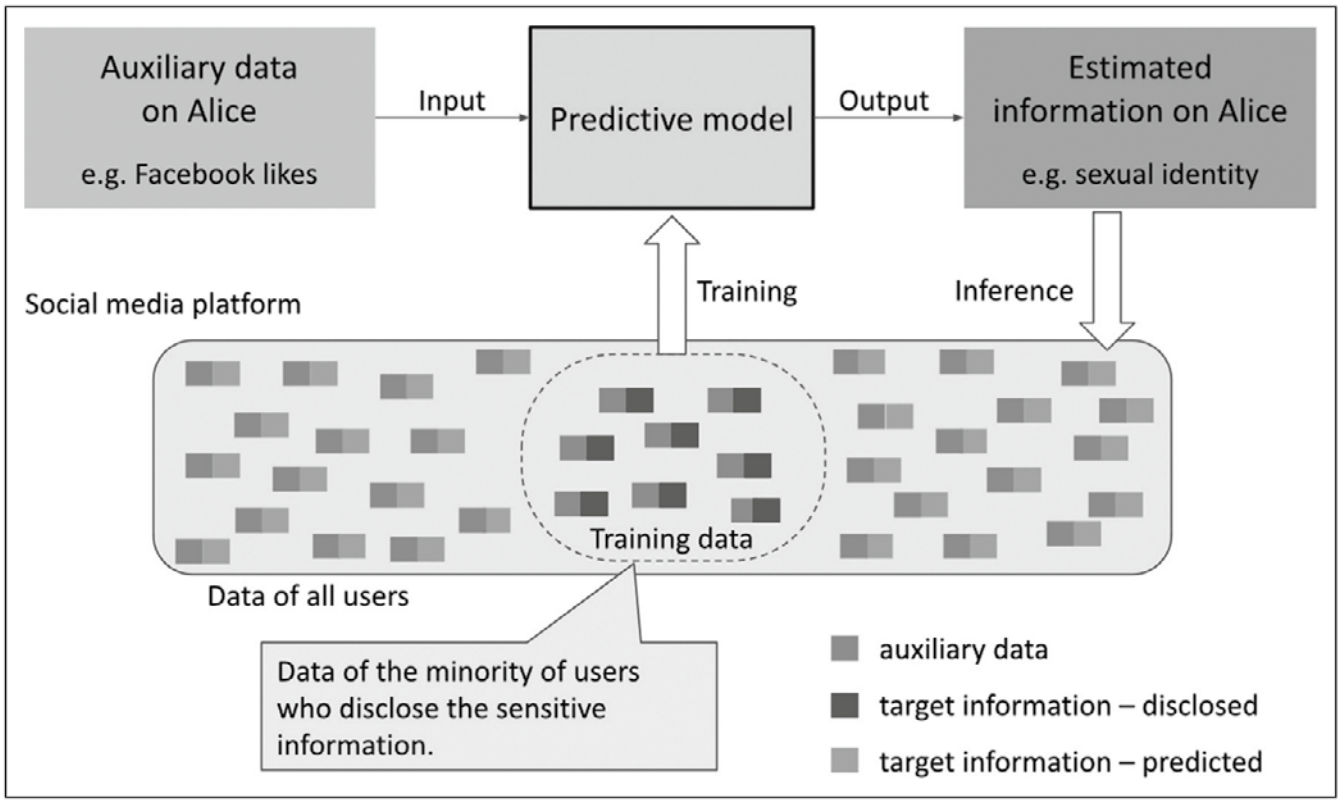


Abbildung 1: Die Funktionsweise von prädiktiver Analytik anhand von Social-Media-Daten nach [15]

Uff! Ist digitale Mündigkeit und individuelle Datenflusskontrolle da überhaupt noch möglich?

Wie sollen wir es also als Nutzer:innen im Angesicht dieser hochkomplexen Marktinfrastruktur schaffen, digital mündig zu sein und unsere Daten zu kontrollieren? Im Angesicht einer Infrastruktur, die das gesamte Internet durchdringt und hauptsächlich dazu dient, Profitinteressen mächtiger Plattformen zu befriedigen? Einer Infrastruktur, deren ‚Treibstoff' die über uns generierten Daten sind und die die Macht hat, auch Informationen über uns vorherzusagen, die wir gar nicht preisgeben möchten? Offenkundig sind diese Fragen rein rhetorischer Natur, und die Antwort „gar nicht!" sollte Ihnen auf der Zunge liegen. Denn im Kontext dieser gigantischen, trackingbasierten Marktinfrastruktur von Nutzer:innen zu fordern, ihre eigenen Daten mündig zu kontrollieren, gleicht einer Forderung an eine Person in einem Raum voller Überwachungskameras, zu kontrollieren, wie sie gefilmt wird. In der Analogie sind die Kameras in dem Raum zum Teil versteckt. Wenn sie etwas nicht gut erkennen können, werden die Bilder mit Material aus anderen Räumen von anderen Personen überlagert, um das aktuelle Bild zu vervollständigen. Und eigentlich ist die Person mit etwas völlig anderem beschäftigt, als zu überlegen, wie sie gefilmt werden möchte, beispielsweise damit, ihren Toaster zu reparieren.

Mal ganz abgesehen davon, dass Verfahren wie Dark Patterns und Nudging es uns als Nutzer:innen auf der Ebene des oberflächlichen Interfaces erschweren, die Kontrolle über unsere Daten zu haben: Es ist uns bereits auf der zugrundeliegenden, infrastrukturellen Ebene unmöglich.

Wo kommt diese trügerische Verantwortung eigentlich her? Die neoliberale Responsibilisierung

Doch wieso werden wir eigentlich durch die Forderung danach, digital mündig zu sein und unsere eigenen Daten zu kontrollieren, für etwas verantwortlich gemacht, das zu leisten wir überhaupt nicht in der Lage sind? Dieses Ungleichverhältnis – als Individuum für etwas verantwortlich gemacht zu werden, was wir strukturell nicht leisten können – ist charakteristisch für den Neoliberalismus. Im Rahmen des Prozesses der sogenannten Responsibilisierung überträgt der Staat Verantwortung für Aufgaben, die er vormals selbst innehatte oder die bis dahin keinem Akteur zugeordnet waren, auf seine Bürger:innen oder auf andere nicht-staatliche Akteure. Responsibilisierung lässt sich unter anderem im Diskurs um die Klimakrise wiederfinden, wenn die Verantwortung für mehr Nachhaltigkeit bei den individuellen Konsument:innen gesehen wird. Im Digitalen werden Individuen für die Sicherheit ihres eigenen Computers verantwortlich gemacht und sind dann eben selbst schuld, wenn sie unwissentlich auf den falschen Link geklickt und Schadsoftware weiterverbreitet haben [19]. Ein Scheitern an dieser Verantwortung ist in der Responsibilisierung programmiert, da strukturelle Aufgaben und Probleme nicht individuell gelöst werden können, und das Scheitern wird stets auf Seiten des Individuums verortet: das neoliberale Blaming-the-victim [20].

Dass Responsibilisierung auch dann so gut funktioniert, wenn Individuen strukturell nicht in der Lage sind, der Verantwortung gerecht zu werden, liegt daran, dass die Responsibilisierung unter dem Deckmantel des positiv konnotierten Empowerments wirkt [21]. Ein empowertes Subjekt ist selbstbestimmt, eigenständig, und nicht auf fremde Unterstützung, beispielsweise durch den Staat, angewiesen. Das klingt auf den ersten Blick erstrebenswert, doch werden dabei die historisch gewachsenen sozialen Strukturen, in die Menschen hineingeboren werden und aufgrund derer sie sich in Abhängigkeit von anderen Menschen oder Institutionen befinden, völlig negiert. Beispielsweise sind Personen, die Sorgearbeit leisten wie beispielsweise Kinderbetreuung oder Pflege und Unterstützung von Angehörigen und Freunden – was aufgrund von hegemonialen Geschlechtervorstellungen vorrangig Frauen machen – oder Menschen, die in einem Umfeld mit wenig Geld aufwachsen, häufig ebenfalls auf kollektive Unterstützung angewiesen. Denn sie haben nicht die finanziellen, zeitlichen und mentalen Kapazitäten, von anderen Institutionen unabhängig zu sein.

Womöglich ist die Forderung nach digitaler Mündigkeit also nur Empowerment im neuen Gewande. Dadurch würde sie eine Responsibilisierung legitimieren in der uns als individuelle Nutzer:innen eine Verantwortung übertragen wird, die wir gar nicht leisten können.

Der Artikel ist aus der Masterarbeit der Autorin hervorgegangen und ergänzter Nachdruck des Beitrags aus dem Magazin Frauen machen Informatik, Bd. 47 zu Digitale Souveränität der Gesellschaft für Informatik e. V.

Referenzen

[1] O'Neil, C.: Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Crown, New York 2016.
[2] Benjamin, R.: Race After Technology: Abolitionist Tools for the New Jim Code. 1. Ausgabe. Polity, Medford 2019.
[3] Eubanks, V.: Automating Inequality: How High-tech Tools Profile, Police, and Punish the Poor. St Martin's Press, New York 2018.
[4] Noble, S. U.: Algorithms of Oppression: How Search Engines Reinforce Racism.Combined Academic Publ., New York 2018.
[5] Weil der Begriff der Race als Beschreibung einer sozialen Kategorie nicht verlustlos ins Deutsche übersetzt werden kann und noch keine zufrie-

Mareike Lisker

Mareike Lisker ist Doktorandin an der Hochschule für Technik und Wirtschaft Berlin. Dort forscht und lehrt sie im Spannungsfeld von Informatik und Gesellschaft. Sie promoviert mit einer Arbeit zu automatisierten Content-Moderation-Verfahren abseits von zentralisierten Diensten und führt hierbei ihre Perspektiven aus der Informatik, der Philosophie und der Linguistik zusammen. Sie interessiert sich außerdem für Machtverhältnisse in der digitalen Welt, Datenethik und Ethik der KI.

denstellende Entsprechung existiert, übernehme ich den Begriff aus dem englischsprachigen Diskurs um Rassismus, vgl. dazu MissyRedaktion. 2020. "Hä, was heißt denn Race?" Missy Magazine (blog). September 21, 2020. https://missy-magazine.de/blog/2020/09/21/hae-was-heisst-denn-race/. Die Begriffe weiß und schwarz schreibe ich kursiv, um zu markieren, dass sie ebenfalls eine soziale Kategorie beschreiben und keinesfalls eine Farbe.

[6] Angwin, J., J. Larson, S. Mattu, und L. Kirchner: „Machine Bias", ProPublica 02.03.2023. (Quelle: ProPublica 23.05.2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

[7] Meyer, D.: „Amazon Killed an AI Recruitment System Because It Couldn't Stop the Tool from Discriminating Against Women", Fortune 07.12.2022 (Quelle: Fortune 10.2018), https://fortune.com/2018/10/10/amazon-ai-recruitment-bias-women-sexist/

[8] Das Akronym BIPoC steht für "Black, Indigenous, People of Colour" und ist eine positiv besetzte, politische Selbstbezeichnung rassistisch diskriminierter Personen.

[9] Hao, K.: „Facebook's ad algorithms are still excluding women from seeing jobs", MIT Technology Review 07.12.2022 (Quelle MIT Technology Review 09.04.2021), https://www.technologyreview.com/2021/04/09/1022217/facebook-ad-algorithm-sex-discrimination/

[10] Johnson, G. M.: „Algorithmic Bias: On the Implicit Biases of Social Technology", in: Synthese, Bd. 198, Nr. 10, 2020, S. 9941–9961: 9942.

[11] Montulli, L.: „The irregular musings of Lou Montulli: The reasoning behind Web Cookies", 05.10.2022 (Quelle The irregular musings of Lou Montulli 14.05.2013), https://montulli.blogspot.com/2013/05/the-reasoning-behind-web-cookies.html

[12] Mellet, K. und T. Beauvisage, „Cookie monsters. Anatomy of a digital market infrastructure", in: Consumption Markets & Culture, Bd. 23, Nr. 2, März 2020, S. 110–129.

[13] builtwith.com (25.11.2022): „Analytics technologies Web Usage Distribution" https://trends.builtwith.com/analytics

[14] Zuboff, S.: The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. 1. Aufl. PublicAffairs, New York 2019, S. 344.

[15] Kosinski, M., D. Stillwell, und T. Graepel: „Private traits and attributes are predictable from digital records of human behavior", in: Proceedings of the National Academy of Sciences, Bd. 110, Nr. 15, Apr. 2013, S. 5802–5805.

[16] Mühlhoff, R.: „Predictive privacy: Collective data protection in the context of artificial intelligence and big data", in Big Data & Society, Bd. 10, Nr. 1, Jan. 2023, S. 3.

[17] Mühlhoff, R.: „Prädiktive Privatheit: Kollektiver Datenschutz im Kontext von Big Data und KI", in: M. Friedewald, A. Roßnagel, J. Heesen, N. Krämer, und J. Lamla, (Hrsg.): Künstliche Intelligenz, Demokratie und Privatheit. Nomos Verlagsgesellschaft mbH & Co. KG, 2022, S. 31–58: 53.

[18] Engeler, M.: „Der Konflikt Zwischen Datenmarkt Und Datenschutz.", in Neue Juristische Wochenschrift, Bd. 47, 2022. S. 3398–3405.

[19] Renaud, K., S. Flowerday, M. Warkentin, P. Cockshott, und C. Orgeron, „Is the responsibilization of the cyber security risk reasonable and judicious?", in: Computers & Security, Bd. 78, Sep. 2018, S. 198–211: 204.

[20] Gray, Garry C.: "The Responsibilization Strategy of Health and Safety: Neo-Liberalism and the Reconfiguration of Individual Responsibility for Risk.", in: The British Journal of Criminology, Bd. 49, Nr. 3, 2009. S. 326–42.

[21] Hache, É.: „La responsabilité, une technique de gouvernementalité néolibérale? [Is responsibility a tool of neo-liberal governmentality?]", in: Raisons politiques, Bd. 28, Nr. 4, 2007, S. 49–65.

Wissenschaft & Frieden 1/24
Konflikte im „ewigen" Eis

Das „ewige" Eis – die kalten, weit entlegen scheinenden Pole der Welt, oft genug ein Bild für Einklang, Harmonie und Frieden. Die Polarregionen zeichnen sich durch ihre ökologische Fragilität und globale Bedeutung aus. Sie sind die Dreh- und Angelpunkte, um die sich die Erde dreht. Und trotz ihrer Kälte sind sie doch Brennpunkte der Weltpolitik, an denen sich geopolitische Interessen, Ressourcengewinnung und Umweltschutz überschneiden. Auch wenn sie gegenüber den Bevölkerungszentren als abgelegene und unberührte Landschaften erscheinen, ist hier eine gut koordinierte kooperative Regierungsführung mehr als dringlich, um eine Ausweitung territorialer Streitigkeiten und Ressourcenkämpfe in die Polarkreise zu vermeiden. W & F 1/24 thematisiert die unterschiedlichen Konfliktdimensionen in Arktis und Antarktis und legt vorsichtige erste Impulse für künftige Friedenssicherung in den Polarregionen.

Die Januarausgabe des Podcast *Fokus Frieden* der Mitherausgeberorganisation *Friedensakademie Rheinland-Pfalz* mit Patrick Flamm ergänzt das Heft mit einem einstündigen Gespräch zu den spezifischen Konflikten in der Antarktis.

Mit Beiträgen von Jürgen Scheffran und Verena Mühlberger, Henry Lesmann, Rene Urueña, Cornelia Lüdecke und Patrick Flamm.

Weitere Beiträge: Wintersteiner – 60 Jahre „Thirring-Plan" | Vogl – Chinas „Global Civilization Initiative" | Lipp – Der Antimilitarist Heinrich Mann

W & F 1/24 | Februar | 64 Seiten | 12 € (Druck) / 9 € (ePUB + PDF)
www.wissenschaft-und-frieden.de

Daniel Leisegang, Chris Köver, Sebastian Meineck

Die sieben quälendsten Fragen zur KI-Verordnung

26. Januar 2024 – *Wieso hagelt es jetzt so viel Kritik? Wie schlimm wird das mit der Gesichtserkennung? Und was lässt sich jetzt überhaupt noch machen? Wir liefern die wichtigsten Updates zur fast fertigen KI-Verordnung.*

Fast ist die KI-Verordnung[1] (auf Englisch: *AI Act*) beschlossene Sache. Sie soll das weltweit erste Gesetz werden, das sogenannte Künstliche Intelligenz umfassend reguliert. Doch auf den letzten Metern gibt es Streit. Erst jetzt kursiert nämlich der Text zur vorweihnachtlichen Einigung zwischen Kommission, Parlament und Rat. Und der ist deutlich weniger besinnlich als zunächst angenommen.

Fachleute warnen vor Massenüberwachung durch unerwartet große Lücken für Grundrechte. Manche Politiker:innen versuchen nun, doch noch an der Einigung zu rütteln. Der Weg zu Europas grundlegender KI-Gesetzgebung ist mühsam – und die quälendsten Fragen beantworten wir hier.

1. Die Einigung war doch vor Weihnachten, wieso hagelt es jetzt Kritik?
2. Gesichtserkennung: Wie schlimm wird es?
3. Emotionserkennung: Was droht hier?
4. Migrationskontrolle: Wie schlimm ist es?
5. Nationale Sicherheit: Was dürfen Staaten alles machen?
6. Ist an dem Gesetz auch irgendetwas gut?
7. Lässt sich jetzt überhaupt noch etwas ändern?

1. Die Einigung war doch vor Weihnachten, wieso hagelt es jetzt Kritik?

Das liegt vor allem daran, dass nach den Trilog-Verhandlungen wochenlang nicht klar war, worauf sich Kommission, Parlament und Rat genau geeinigt haben. Wenn drei Organe mit Vertreter:innen aus 27 EU-Ländern gemeinsam Gesetze schmieden, wird es schnell unübersichtlich – im Fall der KI-Verordnung war es geradezu chaotisch.

Bereits der Gesetzentwurf der EU-Kommission war lang und verwinkelt. Die Verhandler:innen haben das nicht einfacher gemacht, sondern vor allem Schnörkel und Klauseln hinzugezimmert, wie das inzwischen öffentliche, knapp 900-seitige PDF[2] anschaulich zeigt. Dort lassen sich die Versionen von Kommission, Parlament, Rat und Trilog nebeneinander nachlesen.

Die vorläufige Einigung am 9. Dezember geschah nach „dreitägigen Marathonverhandlungen", schrieb der Rat[3], mitunter wurde 22 Stunden am Stück[4] verhandelt. Sichtlich müde, aber mit gerecktem Daumen ließen sich die Verhandler:innen danach für die Presse fotografieren[5].

Misstrauen an der Daumen-hoch-Stimmung gab es schon damals: Es sei „zu früh zum Feiern", schrieb etwa EDRi[6], der Dachverband von Organisationen für digitale Freiheitsrechte in Europa. Noch immer ist der Text nicht final. Es ist üblich, dass auch nach einer Einigung im Trilog an juristischen und technischen Details gefeilt wird.

Weniger üblich ist jedoch, dass Verhandler:innen dabei aus allen Wolken fallen. Genau das ist bei der KI-Verordnung aber passiert: Manche Abgeordnete des EU-Parlaments erkannten die angeblich getroffene Trilog-Einigung[7] nicht wieder, als sie später den dazu gehörigen Kompromisstext vor Augen hatten, verfasst von der spanischen Ratspräsidentschaft. „Wir wurden über den Tisch gezogen", hieß es aus dem Umfeld der Verhandlungsdelegation[8]. Der Ärger bezieht sich vor allem auf die Regeln zur biometrischen Überwachung, bei denen von der einst starken Parlamentsposition kaum etwas übrig geblieben ist.

2. Gesichtserkennung: Wie schlimm wird es?

Bei diesem Thema kann es sehr ernst werden. Auch wenn es zeitweise anders lautende Hoffnungen gab[9]: Die KI-Verordnung bringt weder ein Verbot noch eine strenge Einschränkung von biometrischer Überwachung. Das heißt, EU-Staaten dürfen aus sehr vielen Gründen viele Menschen überwachen und anhand ihrer körperlichen Merkmale identifizieren, zum Beispiel mit Hilfe öffentlicher Kameras. Gesichtserkennung ist dabei bloß die bekannteste Methode; man kann Menschen etwa auch durch ihre Art zu gehen, eindeutig voneinander unterscheiden[10].

Die KI-Verordnung erlaubt biometrische Echtzeit-Identifikation auch dann, wenn nur die Annahme besteht, dass etwas Schlimmes passieren könnte. In der Verordnung steht hierzu: um eine „spezifische, erhebliche und unmittelbare" Bedrohung für die physische Sicherheit einer Person zu verhindern (Artikel 5(1), (d)). Auch die Suche nach Verdächtigen bestimmter Straftaten ist demnach ein legitimer Grund für biometrische Echtzeit-Überwachung. Dazu zählen laut Kompromisstext etwa Mord, schwere Körperverletzung oder „Kinderpornografie". Zuvor müsse allerdings eine zuständige Behörde den Einsatz der Technologie erlauben, das nennt man Richtervorbehalt. Als besonders hohe Hürde gilt dieser Schritt in der Praxis aber nicht.

Noch laxer ist die KI-Verordnung, wenn die Überwachung nicht in Echtzeit passiert, sondern nachträglich („retrograd"). Denkbar wäre etwa, hierfür archivierte Aufnahmen von Überwachungskameras zu durchleuchten. In solchen Fällen dürfen Men-

schen biometrisch identifiziert werden, sobald sie einer Straftat verdächtigt sind. Für die erstmalige Identifizierung braucht es dem Text zufolge keine besondere Genehmigung. Erst wenn Ermittler:innen eine bereits bekannte, gesuchte Person identifizieren möchten, sollen sie dafür eine behördliche Erlaubnis einholen. Das geht allerdings auch nachträglich, dafür dürfen sie sich 48 Stunden Zeit lassen (Artikel 29(6a)).

Die Kritik daran ist harsch. „Die retrograde biometrische Identifizierung von Personen ist nahezu ohne rechtsstaatliche Hürden wie eine vorherige richterliche Genehmigung und bereits für kleinste Bagatelldelikte möglich", warnt die Europa-Abgeordnete Svenja Hahn (FDP) gegenüber heise online[11]. Das von mehreren zivilgesellschaftlichen Organisationen getragene Bündnis „Reclaim Your Face" spricht von beispielloser dystopischer Massenüberwachung[12] in der EU.

Der Bundesdatenschutzbeauftragte Ulrich Kelber (SPD) schreibt auf Anfrage von *netzpolitik.org*: „Dies könnte gravierende Auswirkungen auf die Erwartung der Bevölkerung haben, im öffentlichen Raum anonym zu bleiben, womit wiederum direkte negative Auswirkungen auf die Ausübung der Meinungs-, Versammlungs- und Vereinigungsfreiheit sowie der Freizügigkeit einhergehen."

Der Europa-Abgeordnete Patrick Breyer (Piraten) befürchtet, die Verordnung führe Europa „in eine dystopische Zukunft eines misstrauischen High-Tech-Überwachungsstaats", und nennt konkrete Beispiele[13]: „So wird es Städten möglich, unter dem Schlagwort ‚Hausfriedensbruch' Obdachlose zu verdrängen, wie im italienischen Como geschehen[14], oder Sprayer wegen ‚Sachbeschädigung' zu verfolgen." Anderes Beispiel: In Großbritannien machen Supermärkte schon jetzt mit Gesichtserkennung Jagd auf Ladendiebe[15].

Die Polizei in Deutschland setzt seit langem Gesichtserkennung ein, jährlich werden damit Tausende Personen identifiziert[16]. Es gibt jedoch Streit darüber, in welchem Umfang das legitim ist. Ein prominenter Fall war die biometrische Datenbank mit den Gesichtern tausender Menschen[17], die Hamburg während der Proteste zum G20-Gipfel im Jahr 2017 angelegt hatte. Der dortige Datenschutzbeauftragte setzte sich dafür ein, dass diese Datenbank gelöscht[18] wird; passiert ist das erst im Jahr 2020[19].

Breyer warnt außerdem, dass Gesichtserkennung immer wieder zu falschen Festnahmen führt – dafür gibt es inzwischen mehrere Beispiele[20] aus den USA. Den einst erhofften Schutz vor solchen Problemen bietet die KI-Verordnung nicht.

3. Emotionserkennung: Was droht hier?

Das EU-Parlament wollte unbedingt ein weitreichendes Verbot von Systemen zur Emotionserkennung in der EU. Sie sollten an Schulen und Universitäten, am Arbeitsplatz, bei Sicherheitsbehörden und auch in der Grenzkontrolle auf die Verbotsliste gesetzt werden[21]. Übrig geblieben ist jetzt nur noch ein Verbot im Bildungsbereich und bei der Arbeit (Artikel 5(1), (d)(iiic)). Für den Einsatz der wissenschaftlich geächteten Technologie in der Polizeiarbeit und bei Grenzkontrollen gibt die Verordnung dagegen grünes Licht, ebenso wie in anderen Bereichen. Zwar gilt Emotionserkennung laut dem Kompromisstext als „hochriskant" und ist damit vielen Auflagen unterworfen, doch verboten ist sie nicht.

Technologien zur Emotionserkennung versprechen eine Menge: Studierende vor dem Bildschirm überwachen, mutmaßlich aggressive Personen aus einer großen Menschenmenge fischen oder Menschen vor der Einreise beim angeblichen Lügen ertappen. Doch aus wissenschaftlicher Sicht hat Emotionserkennung einen ziemlich miesen Ruf[22], um es vorsichtig zu formulieren. Viele Fachleute sagen, es gebe schlicht keinen Nachweis dafür, dass man aus Regungen des Gesichtes auf tatsächliche Gefühle einer Person wie Wut oder Angst schließen kann. Zu diesem Schluss kam auch eine groß angelegte Meta-Studie[23] aus dem Jahr 2019, die alle bis dahin durchgeführten Untersuchungen miteinander verglich. Kritiker:innen sprechen bei der Emotionserkennung von „Junk Science", wissenschaftlichem Müll.

Noch dazu greifen die Technologien tief in eine Reihe von Grundrechten ein, wie das Recht auf Privatsphäre oder auch das Recht, die Aussage zu verweigern. Erlaubt wäre mit dem jetzigen Text etwa weiterhin, sogenannte „Lügendetektoren" an den EU-Außengrenzen zu platzieren, wie die EU das bereits von 2016 an mit einem Pilotprojekt in Ungarn, Litauen und Griechenland erprobt hat[24]. Das „Täuschungserkennungsystem" sollte die kaum wahrnehmbare Gesichtsausdrücke von Einreisenden analysieren, um zu überprüfen, ob sie bei der Frage nach ihrem biografischen Hintergrund die Wahrheit sagen. Das Forschungsprojekt wurde 2019 beendet und ist nie in den Normalbetrieb gegangen. Sollte eine solche Technologie jedoch in Zukunft wieder zum Einsatz kommen, müssten Betroffene lediglich darauf hingewiesen werden, dass sie hier einem System zur Emotionserkennung gegenübersitzen.

Ella Jakubowska vom Dachverband EDRi kritisiert außerdem, dass selbst für die Bereiche Bildung und Arbeit Ausnahmen geschaffen wurden, um die Technologie dennoch einzusetzen – laut Kompromisstext aus „medizinischen oder Sicherheitsgründen". Auf Anfrage schreibt uns Jakubowska: „Da diese Gründe die häufigste Rechtfertigung für den Einsatz von Emotionserkennungssystemen sind, befürchten wir, dass das KI-Gesetz der EU die KI-gestützte Emotionserkennung nicht verbietet, sondern vielmehr legitimiert und einen Markt für ihren Einsatz schafft."

4. Migrationskontrolle: Wie schlimm ist es?

Der Trend, der sich schon in der Emotionserkennung abzeichnet, setzt sich auch bei der Migrationskontrolle fort: Menschen auf der Flucht können von der KI-Verordnung kaum Schutz erwarten. Die zumindest grundlegenden Einschränkungen für Gesichtserkennung im öffentlichen Raum gelten ausdrücklich nicht für Grenzkontrollen, da Grenzen laut Kompromisstext nicht Teil des „öffentlichen Raums" seien (Erwägungsgrund 9). Handeln mindestens zwei Menschen, die vor einer Entscheidung die Prognose eines KI-Systems überprüfen? Das schreibt die Verordnung zwar für alle als hochriskant geltenden Bereiche vor – nicht aber bei „Strafverfolgung, Migration, Grenzkontrolle oder Asyl" (Erwägungsgrund 48).

Es gibt noch mehr Regeln, die ausdrücklich nicht für Migrationskontrolle gelten. Wer riskante KI-Systeme einsetzt, ist laut

KI-Verordnung eigentlich zu Transparenz verpflichtet und muss sich in einer öffentlichen Datenbank registrieren – kritische Beobachter:innen hatten das gefordert[25]. Für „Strafverfolgung, Migration, Asyl und Grenzkontrollmanagement" gibt es jedoch diese Transparenz nicht: Hier sollen „die Registrierungspflichten in einem sicheren, nicht-öffentlichen Bereich der Datenbank erfüllt werden." Einblick in diese Hochsicherheitszone des Transparenzregisters haben dann weder Öffentlichkeit noch Presse, nur noch die Kommission und die nationale Aufsichtsbehörde.

So lässt die EU am Ende gerade dort eine bemerkenswerte Lücke, wo Menschen ganz besonders auf gesetzlichen Schutz angewiesen wären. Insgesamt sei das Gesetz in Bezug auf die Migration „sehr enttäuschend", sagt Ella Jakubowska von EDRi. „Die Tatsache, dass das Gesetz den Einsatz vieler strafbarer KI-Instrumente gegen Menschen auf der Flucht legitimiert, ist wirklich besorgniserregend." Die Ausnahmen an diesen Stellen suggerierten, „dass Menschen auf der Flucht nicht die gleichen Rechte verdienen wie alle anderen".

In den einleitenden Worten zum Gesetz, den sogenannten Abwägungsgründen, klingt das noch ganz anders. Dort steht: „KI-Systeme, die bei der Migrations-, Asyl- und Grenzkontrolle eingesetzt werden, betreffen Menschen, die sich häufig in einer besonders verletzlichen Lage befinden und vom Ergebnis der Maßnahmen der zuständigen Behörden abhängig sind" (Erwägungsgrund 39). Dementsprechend sollten zumindest einige dieser Systeme als hochriskant eingestuft werden. Doch auf diese wohlklingenden Sätze folgt im Gesetzestext selbst eher Eiseskälte.

5. Nationale Sicherheit: Was dürfen Staaten alles machen?

Ein besonders großes Schlupfloch bietet die KI-Verordnung in Fällen der „nationalen Sicherheit". Diese schwammige Formel kann herangezogen werden, um Ausnahmen zu definieren, bei denen der Einsatz von Künstlicher Intelligenz dennoch erlaubt ist. Konkret heißt es in Artikel 2:

> *„Diese Verordnung gilt nicht für KI-Systeme, die entwickelt oder verwendet werden, wenn und soweit sie ausschließlich für militärische, verteidigungspolitische oder die nationale Sicherheit betreffende Zwecke in Verkehr gebracht, in Betrieb genommen oder mit oder ohne Änderung solcher Systeme verwendet werden, unabhängig von der Art der Einrichtung, die diese Tätigkeiten ausübt."*

Die KI-Verordnung verweist hier auf den Gründungsvertrag der EU[26] (Vertrag über die Europäische Union, EUV), wonach ausschließlich die Mitgliedstaaten für ihre nationale Sicherheit zuständig sind (Erwägungsgrund 12a).

Die Sache hat jedoch einen großen Haken: Der Begriff der nationalen Sicherheit ist europaweit nicht klar definiert. Die einzelnen Mitgliedstaaten können daher solche Fälle mit Verweis darauf weitgehend eigenmächtig bestimmen und sich damit den Einsatz von laut KI-Verordnung eigentlich verbotenen Systemen selbst genehmigen.

Autokratische EU-Regierungen wie jene in Ungarn könnten dann nach Belieben selbst gefährlichste KI-Systeme einsetzen, etwa anlasslose biometrische Massenüberwachung oder Social Scoring für EU-Bürger:innen.

Dass dem Einsatz gefährlichster KI-Technologien damit keine Schranken gesetzt sind, zeigt auch die staatliche Spionagesoftware Pegasus[27], angeboten von der israelischen NSO Group. Diese Technologie wurde laut Herstellerangaben ausschließlich für Zwecke der nationalen Sicherheit entwickelt. Längst aber ist bekannt, dass damit auch Oppositionelle, Journalist:innen und Dissident:innen in der EU ins Visier genommen[28] werden. Nicht nur in Ungarn und Polen, sondern auch in Griechenland und Spanien.

Der urprüngliche Verordnungsentwurf der EU-Kommission zur KI-Verordnung sah keine Ausnahme für die nationale Sicherheit vor. Und auch das EU-Parlament hatte die Gefahr erkannt und in seiner Position nur Ausnahmen für militärische Nutzung vorgesehen. Der Rat hat sich aber offenbar auch in dieser Frage durchgesetzt und die „nationale Sicherheit" als Ausnahmegrund in den Kompromisstext gehievt.

Noch im September vergangenen Jahres hatten sich 150 Organisationen der deutschen und europäischen Zivilgesellschaft in einem offenen Brief[29] an Bundesjustizminister Marco Buschmann (FDP) und Bundeswirtschaftsminister Robert Habeck (Grüne) gewandt und gefordert: „KI für Zwecke der nationalen Sicherheit darf nicht pauschal von der Verordnung ausgenommen werden". Sie haben sich nicht durchgesetzt.

6. Ist an dem Gesetz auch irgendetwas gut?

Ja, in der KI-Verordnung stecken neue Rechte für Nutzer:innen und Pflichten für Anbieter von KI-Systemen. So soll sich jede Person bei ihrer nationalen KI-Aufsichtsbehörde[30] beschweren dürfen, wenn sie ihre Rechte verletzt sieht. Anbieter von besonders riskanten KI-Systemen müssen ihre Technologien auf Risiken prüfen, ausreichend transparent gestalten und unter menschliche Aufsicht stellen.

Der Bundesdatenschutzbeaufragte Ulrich Kelber schreibt, die KI-Verordnung stärke auch den Schutz der Grundrechte, insbesondere den Datenschutz im Zusammenspiel mit der Datenschutz-Grundverordnung (DSGVO).

Das Verbot von öffentlich zugänglichen Gesichtersuchmaschinen hat es auch in den Kompromisstext geschafft (Artikel 5(1), (d)(iiib)). Über den Vorstoß des Parlaments haben wir vergangenen Sommer berichtet[31]. Nicht erlaubt ist demnach „das ungezielte Auslesen von Gesichtsbildern aus dem Internet", um daraus Datenbanken zur Gesichtserkennung zu erstellen.

Erfreulich ist außerdem, dass der Kompromisstext ein Verbot von Predictive Policing vorsieht. Predictive Policing beschreibt den Versuch, aus polizeilichen Daten Vorhersagen abzuleiten. In Deutschland[32] ist die Technologie bereits seit längerem im Einsatz[33]. In den vergangenen Jahren hatte unter anderem die Menschenrechtsorganisation Amnesty International gezeigt, dass Predictive Policing in Großbritannien[34] und in den Nieder-

landen[35] zu Massenüberwachung, Fehlentscheidungen und Diskriminierung führt.

Die Trilog-Einigung im Dezember sah noch vor, solche Systeme als Hochrisiko-Technologie zu kategorisieren und damit ihren Einsatz unter Einschränkungen zu erlauben[36]. Nun steht im Kompromisstext ein Verbot von Predictive Policing (Artikel 5(1), (d)(iiia)).

Konkret geht es dabei um die „Verwendung eines KI-Systems zur Risikobewertung natürlicher Personen, um das Risiko einer natürlichen Person, eine Straftat zu begehen, zu bewerten oder vorherzusagen, und zwar ausschließlich auf Grundlage der Erstellung eines Profils einer natürlichen Person oder der Bewertung ihrer Persönlichkeitsmerkmale und Eigenschaften".

Ungeachtet dieses Verbots ist jedoch damit zu rechnen, dass einzelne EU-Staaten diese Technologie mit Verweis auf die „nationale Sicherheit" künftig dennoch einsetzen werden.

Nach wie vor hat die EU die Hoffnung, mit der KI-Verordnung einen großen Wurf zu landen, immerhin arbeiten weltweit gerade mehrere Staaten[37] an ihren eigenen KI-Gesetzen. Die KI-Verordnung sei „wegweisend", schreibt etwa Europa-Abgeordnete Alexandra Geese (Grüne), sie enthalte wichtige Bestimmungen zum Schutz von Grundrechten.

Dahinter steckt auch die Annahme, dass die EU mit ihren Gesetzen andere Länder beeinflussen kann, der sogenannte Brüssel-Effekt[38]. „Die EU schreibt Geschichte", heißt es auch vom Bündnis „Reclaim Your Face" – allerdings mit dem bitteren Zusatz: „aus den falschen Gründen".

7. Lässt sich jetzt überhaupt noch etwas ändern?

Ja, einiges. Sobald die KI-Verordnung verabschiedet sein wird, sind die Mitgliedstaaten wieder am Zug. Und die können manche Lücken zumindest innerhalb ihrer eigenen Grenzen stopfen. Zur biometrischen Identifizierung heißt es in der Verordnung ausdrücklich, Mitgliedstaaten können strengere Gesetze erlassen. Der Bundesdatenschutzbeaufragte schreibt: Die Bundesregierung sollte diese Klausel nutzen.

Passend dazu steht im Koalitionsvertrag der Ampel-Regierung[39]: „Flächendeckende Videoüberwachung und den Einsatz von biometrischer Erfassung zu Überwachungszwecken lehnen wir ab. Das Recht auf Anonymität sowohl im öffentlichen Raum als auch im Internet ist zu gewährleisten."

Zunächst richtet sich der Blick aber auf die EU. Denn trotz der Einigung im Trilog ist die KI-Verordnung noch nicht beschlossen. Die Mitgliedstaaten im Rat und das Parlament müssen sie noch verabschieden. In der Regel gibt es bei diesen Abstimmungen grünes Licht, da sich Parlament und Rat bereits zuvor geeinigt haben.

In diesem Fall wollen zumindest manche nochmal an der Einigung rütteln. Wie etwa Euractiv und Tagesspiegel Background berichten[40], ist Frankreich mit der Einigung nicht zufrieden. Das Land hatte sich vehement für industriefreundlichere Regeln eingesetzt[41]. Jetzt tüftele die französische Regierung daran, das Gesetz auf den letzten Metern im Rat zu stoppen, dafür bräuchte es aber mindestens vier Mitgliedstaaten[42].

Unmut gibt es auch aus Deutschland. So erwarte der digitalpolitische Sprecher der FDP-Fraktion, Maximilian Funke-Kaiser, laut Tagesspiegel Background „von der Bundesregierung eine Ablehnung", sollte es nicht zu Änderungen kommen. Aus den Reihen von SPD und Grünen gibt es dagegen Signale für eine Zustimmung zur KI-Verordnung, etwa vom digitalpolitischen Sprecher der Grünen-Bundestagsfraktion, Maik Außendorf. Viele scheint die Aussicht abzuschrecken, mitten im KI-Hype plötzlich ohne ein entsprechendes Gesetz dazustehen.

Geduld ist auf jeden Fall gefragt: Selbst wenn die KI-Verordnung beschlossene Sache ist, vergehen dann noch zwei weitere Jahre, bis die neuen Regeln vollständig angewandt werden.

Quelle: https://netzpolitik.org/2024/grundrechte-in-gefahr-die-sieben-quaelendsten-fragen-zur-ki-verordnung/

Anmerkungen

1 *https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0106(COD)&l=en*
2 *https://drive.google.com/file/d/1xfN5T8VChK8fSh3wUiYtRVOKIi9oIcAF/view*
3 *https://www.consilium.europa.eu/de/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/*
4 *https://www.spiegel.de/netzwelt/netzpolitik/matthias-spielkamp-zum-ki-gesetz-riesenschritt-in-eine-ueberwachungsgesellschaft-a-4802b72c-dcfa-4c83-80f0-81111bf7891b*
5 *https://germany.representation.ec.europa.eu/news/historischer-moment-politische-einigung-zwischen-eu-parlament-und-rat-auf-ki-gesetz-2023-12-09_de*
6 *https://edri.org/our-work/eu-ai-act-deal-reached-but-too-soon-to-celebrate/*
7 *https://netzpolitik.org/2023/ki-verordnung-schraffierte-rote-linien-als-kompromiss/*
8 *https://netzpolitik.org/2024/ki-verordnung-biometrische-massenueberwachung-ohne-wenn-und-aber/*
9 *https://netzpolitik.org/2023/kw-19-die-woche-als-das-eu-parlament-beim-ai-act-hoffnung-machte/*
10 *https://arxiv.org/abs/2204.07855*
11 *https://www.heise.de/news/Flaechenbrand-fuer-Buergerrechte-Liberale-kritisieren-KI-Verordnung-scharf-9606490.html*
12 *https://twitter.com/ReclaimYourFace/status/1747907071252503762 3*
13 *https://www.patrick-breyer.de/ki-gesetz-ai-act-droht-gesichtsueberwachung-zum-europaeischen-alltag-zu-machen/*
14 *https://privacyinternational.org/case-study/4166/how-facial-recognition-spreading-italy-case-como*
15 *https://netzpolitik.org/2023/vereinigtes-koenigreich-mit-gesichtserkennung-auf-jagd-nach-ladendieben/*
16 *https://netzpolitik.org/2021/gesichtserkennung-polizei-verdoppelt-zahl-identifizierter-personen-jaehrlich/*
17 *https://netzpolitik.org/2018/kritik-an-g20-gesichtserkennung-als-neue-dimension-staatlicher-ermittlungs-und-kontrolloptionen/*

18 https://netzpolitik.org/2019/datenschuetzer-scheitert-an-loeschung-biometrischer-g20-datenbank/
19 https://www.golem.de/news/gesichtserkennung-hamburger-polizei-loescht-gesichtsdatenbank-2005-148780.html
20 https://web.archive.org/web/20240102105321/https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html
21 https://netzpolitik.org/2023/ki-verordnung-die-wunschliste-der-mitgliedstaaten/
22 https://www.ft.com/content/c0b03d1d-f72f-48a8-b342-b4a926109452
23 https://journals.sagepub.com/stoken/default+domain/10.1177%2F15291006198329 30-FREE/pdf
24 https://netzpolitik.org/2021/eu-projekt-iborderctrl-kommt-der-luegendetektor-oder-kommt-er-nicht/
25 https://algorithmwatch.org/de/transparenzregister-oeffentliche-verwaltung-2023/
26 https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0020.02/DOC_1&format=PDF
27 https://netzpolitik.org/pega/
28 https://netzpolitik.org/2023/pegasus-skandal-zieht-die-samthandschuhe-aus/
29 https://algorithmwatch.org/de/wp-content/uploads/2023/09/Offener-Brief_28.09.23.pdf
30 https://background.tagesspiegel.de/digitalisierung/ai-act-wer-uebernimmt-in-deutschland-die-kontrolle
31 https://netzpolitik.org/2023/pimeyes-eu-koennte-gesichter-suchmaschinen-verbieten/
32 https://netzpolitik.org/2024/automatisierte-datenanalyse-bei-der-polizei-bundeslaender-nicht-scharf-auf-palantir/
33 https://netzpolitik.org/2023/palantir-software-bayerische-polizei-testet-datamining-mit-echten-personendaten/
34 https://www.amnesty.org.uk/files/reports/Trapped in the Matrix Amnesty report.pdf
35 https://www.amnesty.org/en/documents/eur35/2971/2020/en/
36 https://netzpolitik.org/2023/ki-verordnung-schraffierte-rote-linien-als-kompromiss
37 https://www.bloomberg.com/news/articles/2023-10-30/ai-regulation-what-biden-s-new-rules-might-mean-in-the-us
38 https://www.stiftung-nv.de/en/publication/transcript-policy-debate-brussels-effect-will-europes-ai-regulation-achieve-global
39 https://www.bundesregierung.de/breg-de/service/gesetzesvorhaben/koalitionsvertrag-2021-1990800
40 https://background.tagesspiegel.de/digitalisierung/ai-act-wer-uebernimmt-in-deutschland-die-kontrolle
41 https://www.euractiv.com/section/artificial-intelligence/news/behind-frances-stance-against-regulating-powerful-ai-models/
42 https://www.consilium.europa.eu/de/council-eu/voting-system/qualified-majority/
43 https://www.blaetter.de/
44 http://www.schmetterling-verlag.de/page-5_isbn-3-89657-068-4.htm
45 https://www.alternativer-medienpreis.de/preistraeger-2016/daniel-leisegang/
46 https://www.eurozine.com/
47 mailto:daniel@netzpolitik.org
48 https://keys.openpgp.org/search?q=daniel@netzpolitik.org
49 https://mastodon.social/@dleisegang
50 https://bsky.app/profile/dleisegang.bsky.social
51 https://missy-magazine.de/online-magazin/
52 https://keys.openpgp.org/search?q=0x5E598DD0D37B9F71A88DD92233D38859243016F9
53 https://sebmeineck.substack.com/
54 mailto:sebastian%5Bat%5Dnetzpolitik.org
55 https://keys.openpgp.org/search?q=sebastian[at]netzpolitik.org
56 https://sebastianmeineck.wordpress.com/kontakt/
57 https://sebastianmeineck.wordpress.com/presse-kontakt/
58 https://mastodon.social/@sebmeineck

Daniel Leisegang, Chris Köver und Sebastian Meineck

Daniel Leisegang ist Politikwissenschaftler und Co-Chefredakteur bei *netzpolitik.org*. Zuvor war er Redakteur bei den *Blättern für deutsche und internationale Politik*[43]. 2014 erschien von ihm das Buch *Amazon – Das Buch als Beute*[44]; 2016 erhielt er für seinen Beitrag *Facebook rettet die Welt* den *Alternativen Medienpreis*[45] in der Rubrik *Medienkritik*. Daniel gehört dem Board of Trustees von *Eurozine*[46] an.
Kontakt: E-Mail[47] (OpenPGP[48]), Mastodon[49], Bluesky[50], Threema ENU3SC7K, Telefon: +49-030-577148228 (Montag bis Freitag, jeweils 8 bis 18 Uhr).

Chris Köver ist seit 2018 Redakteurin von *netzpolitik.org*. Sie recherchiert unter anderem zu Digitaler Gewalt, so genannter Künstlicher Intelligenz und zur Migrationskontrolle. Bis 2014 war sie Chefredakteurin des *Missy Magazine*[51].
Kontakt: Mail *chris@netzpolitik.org (PGP-Schlüssel[52]).*

Sebastian Meineck ist Journalist und seit 2021 Redakteur bei *netzpolitik.org*. Zu seinen aktuellen Schwerpunkten gehören digitale Gewalt, Pornoseiten und Künstliche Intelligenz. Er interessiert sich besonders für Methoden der Online-Recherche; darüber schreibt er einen monatlichen Newsletter[53] und gibt Workshops an Universitäten. Zu seinen vorigen Stationen gehören VICE (Senior Editor), Motherboard (Editor-in-chief), der SPIEGEL (Autor) und die Deutsche Journalistenschule München. Das Medium Magazin hat ihn 2020 zu einem der Top 30 unter 30 im Journalismus gekürt.
Kontakt: E-Mail[54] (OpenPGP[55]), Sebastian Hinweise schicken[56] | Sebastian für O-Töne anfragen[57] | Mastodon[58].

Daniel Leisegang

KI-Verordnung erhält grünes Licht

2. Februar 2024 – *Die EU-Mitgliedstaaten haben heute den Kompromisstext der KI-Verordnung bestätigt. Das größte Regelwerk der Welt für Künstliche Intelligenz wird damit wahrscheinlich noch vor den EU-Wahlen in Kraft treten – ungeachtet der breiten Kritik am gesetzgeberischen Prozess und an der drohenden Massenüberwachung.*

Die Entscheidung war mit Spannung erwartet worden: Der Ausschuss der stellvertretenden ständigen Vertreter der einzelnen EU-Mitgliedstaaten (AStV I[1]) hat heute mehrheitlich den endgültigen Kompromisstext der KI-Verordnung bestätigt[2]. Damit wird die Verordnung nach drei Jahren Verhandlung sehr wahrscheinlich noch vor den EU-Wahlen im Juni in Kraft treten.

Die Ausschussabstimmung geht dem Beschluss des EU-Rats voraus. Er setzt sich aus den zuständigen Minister:innen aller EU-Regierungen zusammen und hat die offizielle Entscheidungsbefugnis. Aller Voraussicht nach wird sich der Rat dem heutigen Wahlergebnis anschließen.

Deutsche und französische Regierung zögerten

Noch vor wenigen Tagen war ungewiss, ob der Ausschuss der Trilog-Einigung zustimmen wird. Erst am Dienstag gaben Bundesdigitalminister Volker Wissing (FDP) sowie das Justizministerium unter Marco Buschmann (FDP) und das von Robert Habeck (Grüne) geführte Wirtschaftsministerium die Entscheidung bekannt: Die Bundesregierung werde der Verordnung zustimmen. Das Justiz- und das Wirtschaftsministerium sind bei der KI-Verordnung im Kabinett federführend. Das Digitalministerium ist in den Beratungen lediglich mit eingebunden.

Wissing hatte sich zuvor für „innovationsfreundlichere" Regeln eingesetzt und Verbesserungen für kleine und mittlere Unternehmen gefordert. Der Minister kritisierte[3] vor allem die unzureichende Regulierung kleinerer KI-Basismodelle und die aus seiner Sicht zu niedrigen Hürden für die nachgelagerte biometrische Überwachung.

Auch die französische Regierung zeigte sich unzufrieden mit dem vorliegenden Entwurf. Sie strebte einen Aufschub der heutigen Abstimmung um mindestens eine Woche an. Präsident Emmanuel Macron befürchtet – anders als Wissing – eine Überregulierung der Basismodelle und fordert laxere Regeln bei der biometrischen Überwachung.

Hätte sich die Bundesregierung im Vorfeld auf die Seite Frankreichs, Italiens und anderer kleiner EU-Länder wie Ungarn geschlagen, wäre das Gesetz wahrscheinlich gescheitert.

„Intransparenter" und „chaotischer" Prozess

Die Entscheidung für den KI-Entwurf wird von vielen Seiten begrüßt. Bereits im Vorfeld hatte der Startup-Verband dafür geworben, die Verordnung anzunehmen[4]. Auch ein „Bündnis aus Wissenschaft, Thinktanks, Wirtschaft und Zivilgesellschaft" sprach sich in einem von der Mercator-Stiftung initiierten offenen Brief[5] dafür aus. Ebenso befürwortete die Kultur-, Kreativ- und Medienwirtschaft ein zustimmendes Votum[6].

Aber es gibt auch weiterhin deutliche Kritik. So beschreibt Kai Zenner den gesetzgeberischen Prozess als „intransparent" und „chaotisch". Im Ergebnis sei die Verordnung „an vielen Stellen extrem vage geworden, zum Teil auch fehlerhaft", so der Büroleiter des Europaabgeordneten Axel Voss (EVP) gegenüber heise online[7].

Zum anderen warnen Fachleute davor[8], dass die KI-Verordnung europaweit Massenüberwachung ermögliche. So kritisiert EDRi[9], der Dachverband von Organisationen für digitale Freiheitsrechte in Europa, dass die Verordnung „das Ergebnis eines großen Machtungleichgewichts zwischen den EU-Institutionen" sei. Die nationalen Regierungen und die Lobbys der Strafverfolgungsbehörden hätten sich gegen jene Kräfte durchgesetzt, „die das öffentliche Interesse und die Menschenrechte vertreten".

Auch AlgorithmWatch sieht die Einigung kritisch[10]. Der Kompromiss offenbare „einen systemischen Fehler" bei der EU-Gesetzgebung: „Die nationalen Regierungen und die Strafverfolgungslobby haben einen unverhältnismäßig großen Einfluss", so Angela Müller, Policy- & Advocacy-Leiterin bei der Nichtregierungsorganisation. Im Ergebnis lege die Verordnung zwar „wichtige grundlegende Transparenzpflichten fest", ergänzt Müllers Stellvertreter Kilian Vieth-Ditlmann. Sie biete „aber keinen ausreichenden Schutz vor biometrischer Massenüberwachung".

Das Bündnis *Reclaim your Face* kritisiert ebenfalls[11] den „verwässerten Schutz gegen die rückwirkende Gesichtserkennung". Sie sei „eine weitere Enttäuschung in unserem Kampf gegen eine biometrische Überwachungsgesellschaft".

Nationalstaaten können Überwachung noch beschränken

Auch Alexandra Geese, Digitalexpertin der Fraktion Greens/EFA und stellvertretende Fraktionsvorsitzende, ist nicht ganz zufrieden. Zwar setze die EU mit der KI-Verordnung „einen globalen

Standard für Künstliche Intelligenz, auf den auch die USA mit großer Aufmerksamkeit schauen". Zugleich sagte die EU-Abgeordnete gegenüber netzpolitik.org, dass es nicht gelungen sei, besonders grundrechtswidrige Anwendungen wie die biometrische Massenüberwachung „zu zähmen". Dies müsse nun auf Ebene der Mitgliedstaaten geschehen.

Diesen Plan verfolgt offenbar auch die FDP. Deren digitalpolitischer Sprecher Maximilian Funke-Kaiser *fordert die Bundesregierung auf*[12], den Einsatz biometrischer Überwachung nun „so weit wie möglich" auf nationaler Ebene einzuschränken.

Nachdem der EU-Rat über die Verordnung abgestimmt hat, muss voraussichtlich bis April noch das Parlament in den zuständigen Ausschüssen und im Plenum abschließend den finalen Gesetzestext verabschieden. Erst dann wird dieser im Amtsblatt der EU veröffentlicht, womit er in Kraft tritt. Bis die neuen Regeln vollständig angewandt werden, vergehen zwei weitere Jahre.

Quelle: https://netzpolitik.org/2024/eu-rat-ki-verordnung-erhaelt-gruenes-licht/

Anmerkungen

1 *https://www.consilium.europa.eu/de/council-eu/preparatory-bodies/coreper-i/*
2 *https://x.com/EU2024BE/status/1753428600542384290*
3 *https://www.handelsblatt.com/politik/international/ai-act-fdp-bremst-bei-deutscher-zustimmung-zum-europaeischen-ki-gesetz/100007879.html*
4 *https://startupverband.de/presse/pressemitteilungen/startup-verband-appelliert-zur-annahme-des-eu-ai-acts-l-buettner-startups-wollen-loslegen-und-loesungen-entwickeln"-29-01-2024/*
5 *https://www.ai-act-verabschieden.de/*
6 *https://urheber.info/diskurs/offener-brief-an-bundesregierung*
7 *https://www.heise.de/news/Interview-zum-AI-Act-Zustimmung-trotz-teils-chaotischer-Zustaende-9613817.html*
8 *https://netzpolitik.org/2024/grundrechte-in-gefahr-die-sieben-quaelendsten-fragen-zur-ki-verordnung/*
9 *https://edri.org/our-work/council-to-vote-on-eu-ai-act-whats-at-stake/*
10 *https://algorithmwatch.org/de/pressemitteiling-tritt-die-ki-verordnung-jetzt-endlich-bald-in-kraft/*
11 *https://reclaimyourface.eu/eu-ai-act-will-fail-commitment-to-ban-biometric-mass-surveillance/*
70 *https://www.handelsblatt.com/politik/international/ai-act-fdp-bremst-bei-deutscher-zustimmung-zum-europaeischen-ki-gesetz/100007879.html*

Autoreninfo siehe Seite 78

Constanze Kurz

Kompetent, aber trotzdem abserviert

26. Januar 2024 – *Seine Diskussionsbeiträge fanden im politischen Berlin kein Gehör: Der außerhalb der Ampel weithin angesehene Bundesdatenschutzbeauftragte wird keine zweite Amtszeit bekommen. Ein Kommentar.*

Schon bevor seine reguläre Amtszeit am 7. Januar endete, war klar: Der aktuell noch amtierende Bundesdatenschutzbeauftragte Ulrich Kelber wird keine zweite Runde laufen. Eine Wiederwahl hat die SPD-Fraktion ihrem Parteigenossen nicht ermöglicht.

Kelber ist seit 2019 Behördenchef, er und seine Leute füllen wichtige Kontrollfunktionen aus und sind auch der Anlaufpunkt für die anderen europäischen Datenschützer. Sie sind in Deutschland zugleich eine vernehmbare Stimme der datenpolitischen Vernunft, die öffentlich für den Datenschutz und auch die Informationsfreiheit spricht, die Expertise in politische Prozesse einbringt und die nicht selten einfach nur auf das gern ignorierte geltende Recht pocht und es erläutert.

Natürlich nervt das die Regierenden ab und an, aber als allzu anstrengend gilt Kelber nicht. Als früherer Profi-Politiker wusste er recht gut, bei welchen politischen Schmerzpunkten er besser nur leise poltert, auch mal strategisch verschleppt[1] oder aber schweigt. Er saß für die SPD fast zwei Jahrzehnte im Bundestag. Allzu radikale Forderungen kamen ihm nicht über die Lippen.

Mussten sie vielleicht auch gar nicht: Allein das Pochen auf die Durchsetzung geltenden Rechts und die Ermahnung zur Einhaltung höchstrichterlicher Vorgaben gilt so mancher Innenministerin und manchem Gesundheitspolitiker offenbar schon als Zumutung. Das Bundesinnenministerium entblödete sich in Fragen der Informationsfreiheit nicht einmal, Kelber zu verklagen[2].

Techniker an der Spitze

Dass Kelber als Informatiker auch technisch durchblickt, hat er vielen seiner Jura- und Politkollegen voraus. Für das Datenschutzfeld ist eine starke Verrechtlichung typisch, die sich aus der Geschichte der Entstehung des Grundrechts auf informationelle Selbstbestimmung erklärt. Kelbers Haus ist entsprechend aufgestellt. Doch ein Techniker an der Spitze hat offenkundig mehr genutzt als geschadet, wenn man Kelbers Wortmeldungen zur Chatkontrolle *(„muss unbedingt unterbleiben"[3])* oder generell zur Digitalisierung betrachtet, die auch technisch gut begründet sind.

Doch der außerhalb der Ampel angesehene Bundesdatenschutzbeauftragte redete oft gegen eine Wand: Auf datenschutzpoliti-

sche Debatten reagierte die Bundesregierung – und Olaf Scholz sowieso – mit viel Schweigen, ansonsten häufig mit sich widersprechenden Positionen: Justizminister Marco Buschmann (FDP) ist gegen die Vorratsdatenspeicherung, Innenministerin Nancy Faeser (SPD) möchte sie mindestens teilweise wieder einführen. Das Bild der Ampel-Regierung, die sich in nichts einig ist, war auch beim Datenschutz stimmig. Nur bei der Ökonomisierung der Gesundheitsdaten und beim *E-Rezept*[4] war man sich in der Ampel weitgehend einig, dass Datenschutzfragen und IT-Risiken gemeinschaftlich kleingeredet oder ignoriert gehören.

Nach seinem Amtsantritt setzte Kelber neben der politischen Rechtsberatung in allen datenrelevanten Feldern auch ganz praktische Akzente, indem er sich von den von der Bundesregierung hofierten kommerziellen sozialen Netzwerken ablöste und auf Mastodon einließ. Schon 2020 eröffnete der Bundesdatenschutzbeauftragte die Mastodon-Instanz *bund.social*[5], wo interessierte Behörden Accounts bekommen können. Der Datenschutzbeauftragte rieb der Bundesregierung zugleich gern unter die Nase, dass es nicht mit der Datenschutzgrundverordnung vereinbar sei, wenn Bundesbehörden weiterhin Fanpages auf Facebook betreiben würden[6].

Seine Diskussionsbeiträge wurden auch ohne Kommerzplattformen zweifelsohne gelesen – auch im politischen Berlin. Er zeigte sich bei Mastodon als klares Gegenmodell zu seiner desaströsen Vorgängerin Andrea Voßhoff (CDU)[7]: kompetent, diskussionsfreudig, sich aktuell zielsicher positionierend, manchmal nerdig, auch humorvoll.

Postengefeilsche

Völlig zu Recht kritisierte Kelber in seinem letzten Tätigkeitsbericht[8], dass „der Datenschutz bei vielen Projekten erst sehr spät mitbedacht und eingebunden wird". Insbesondere das Innenministerium dürfte sein Haus nur ungern und spät einbezogen haben. Das aber führe zu „unnötigen Verzögerungen und Verteuerungen im Größenbereich von Jahren und Millionen Euro". Jeder, der sich in dem Bereich Datenschutz auskennt, kann dafür *Beispiele nennen*[9], die erstaunlich oft auch mit IT-Sicherheitsrisiken einhergehen.

In der Ampel aber wird die Wichtigkeit des Datenschutzes erneut dem Postengefeilsche und Ämterkarussell untergeordnet. Der erfolgreiche Amtsinhaber ist abserviert.

Kompetenz scheint kein bedeutsames Kriterium mehr zu sein, zumindest nicht für die Datenschutz-Ignoranten in der SPD-Fraktion. Falls die Ampel bei der obersten Datenschutz-Aufsichtsbehörde für die nächste fünfjährige Amtszeit nun jemanden ins Auge fassen sollte, der wegen politischen Kuhhandels versorgt werden muss, dann würde sie dem Amt enorm schaden. Die Frage könnte aber sein, ob sich überhaupt noch jemand von datenschutzpolitischem Format für die Neubesetzung des Postens findet. Denn der unrühmliche Abgang und die unangemessene Behandlung von Kelber muss ohne Zweifel jene abschrecken, die für solch ein Amt qualifiziert wären.

Quelle: https://netzpolitik.org/2024/ulrich-kelber-kompetent-aber-trotzdem-abserviert/

Anmerkungen

1 *https://netzpolitik.org/2022/die-software-ist-[redacted]/*
2 *https://netzpolitik.org/2020/bundesrepublik-vs-bundesrepublik-innenministerium-verklagt-bundesdatenschutzbeauftragten/*
3 *https://www.heise.de/news/Bundesdatenschuetzer-Kelber-mahnt-Bundesregierung-und-kritisiert-EU-Kommission-7547153.html*
4 *https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2022/12_E-Rezept.html*
5 *https://social.bund.de/*
6 *https://netzpolitik.org/2021/druck-vom-bundesdatenschutzbeauftragten-facebook-seiten-der-bundesbehoerden-sollen-in-die-tonne/*
7 *https://www.faz.net/aktuell/feuilleton/aus-dem-maschinenraum/andrea-vosshoff-versagt-als-datenschutzbeauftragte-13269359.html?printPagedArticle=true#pageIndex_2*
8 *https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/31TB_22.pdf?__blob=publicationFile&v=7*
9 *https://netzpolitik.org/2023/digitalisierung-und-datenschutz-schluss-mit-ausreden/*
10 *https://de.wikipedia.org/wiki/Constanze_Kurz*
11 *https://nowyouknow.eu/*
12 *http://gewissensbits.gi.de/constanze-kurz/*
13 *https://www.randomhouse.de/Buch/Cyberwar-Die-Gefahr-aus-dem-Netz/Constanze-Kurz/C.-Bertelsmann/e537921.rhd*
14 *http://www.faz.net/aktuell/feuilleton/aus-dem-maschinenraum/*
15 *https://wirsindderosten.de/menschen/constanze-kurz/*
16 *https://www.youtube.com/watch?v=hj3gAsqrB18*
17 *http://www.ev-akademie-tutzing.de/toleranz-preis-fuer-christian-wulff-und-constanze-kurz/*
18 *https://keys.openpgp.org/vks/v1/by-fingerprint/58ACBDA9D67D462D249605444A13B8EE269F8A45*

Constanze Kurz

Constanze Kurz[10] ist promovierte Informatikerin, Autorin und Herausgeberin[11] von Büchern[12], zuletzt *Cyberwar*[13]. Ihre Kolumne *Aus dem Maschinenraum*[14] erschien von 2010 bis 2019 im Feuilleton der FAZ. Sie lebt in Berlin[15] und ist ehrenamtlich Sprecherin[16] des *Chaos Computer Clubs*. Sie war Sachverständige der Enquête-Kommission *Internet und digitale Gesellschaft* des Bundestags. Sie erhielt den *Toleranz-Preis*[17] für Zivilcourage und die *Theodor-Heuss-Medaille*.
Kontakt: *constanze(at)netzpolitik.org* (*PGP*[18]).
Foto: Heike Huslage-Koch, CC BY-SA 4.0

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. Außerdem 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 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-Mailinglisten

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

FIfF-Mitgliederliste
An- und Abmeldungen an:
https://lists.fiff.de

FIfF-Beirat

Ute Bernhardt (Berlin); **Peter Bittner** (†); **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
Gilbert Assaf – Berlin
Alexander Heim – Berlin
Sylvia Johnigk – München
Prof. Dr. **Hans-Jörg Kreowski** – Bremen
Kai Nothdurft – München
Prof. Dr. **Britta Schinzel** – Freiburg im Breisgau
Dr. **Friedrich Strauß** – München
Prof. Dr. **Werner Winzerling** – Fulda
Margita Zallmann – Bremen

FIfF-Geschäftsstelle

Ingrid Schlagheck (Geschäftsführung) – Bremen
Anne Schnerrer – Berlin
Benjamin Kees – Berlin

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	Hans-Jörg Kreowski und Margita Zallmann
V.i.S.d.P.	Stefan Hügel
Retrospektive	Beiträge für diese Rubrik bitte per E-Mail an *redaktion@fiff.de*
Lesen, SchlussFIfF	Beiträge für diese Rubriken bitte per E-Mail an *redaktion@fiff.de*
Layout	Berthold Schroeder, München
Cover	Bildmaterial: Depositphotos Autor abidal, ID 275369004
Druck	Girzig+Gottschalk GmbH, Bremen Heftinhalt auf 100 % Altpapier gedruckt.

Druckprodukt mit finanziellem Klimabeitrag
ClimatePartner.com/12164-2404-1001

Aktuelle Ankündigungen

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

FIfF-Konferenz 2024 – „Nachhaltigkeit in der IT green coding – open source – green by IT"
25.–27. Oktober 2024 Hochschule Bremerhaven

FIfF-Kommunikation
2/2024 „40 Jahre FIfF – Denkwürdige Zeiten"
Michael Ahlmann, Stefan Hügel, Hans-Jörg Kreowski und Ralf E. Streibl
Redaktionsschluss: 3. Mai 2024

3/2024 „Datenschutz"
Jörg Pohle, Stefan Hügel
Redaktionsschluss: 2. August 2024

Zuletzt erschienen:
1/2023 #FIfFKon22
2/2023 Mensch – Gesellschaft – Umwelt ... und Informatik
3/2023 IT-Gestaltung für Gute Arbeit
4/2023 Wissenschaft für den Frieden

W&F – Wissenschaft & Frieden
1/23 Jenseits der Eskalation
2/23 Klimakrise
3/23 Gesellschaft in Konflikt
4/23 40 Jahre Wissenschaft & Frieden
1/24 Konflikte im „ewigen" Eis

vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik
#241 Demokratie und Rechtsstaat verteidigen
#242 Künstliche Intelligenz
#243 Kritische Kriminalpolitik
#244 Identitätspolitik

DANA – Datenschutz-Nachrichten
1/23 Europäische Entwicklungen
2/23 Europäische Entwicklungen, Teil 2
3/23 Whistleblowing
4/23 Internet der Dinge
1/24 DSGVO und BDSG und Datenschutzaufsicht
2/24 Gesundheitsdaten

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

FIfFKon23 poetisch – Kostprobe

Das Programm von *FIfFKon23 poetisch* bestand aus Gedichten von Ernst Jandl und Kurt Schwitters sowie drei eigenen. Zu einem davon hat mich das 1-Satz-Statement inspiriert, das Ende Mai 2023 veröffentlicht wurde und von einer langen Reihe bekannter Vertreter:innen der einschlägigen IT-Konzerne und teils berühmter KI-Fachleute unterzeichnet ist. In meiner Übersetzung lautet es:

> *„Das Risiko der Ausrottung (der Menschheit) durch KI zu mindern, sollte eine globale Priorität sein neben anderen weltweiten gesellschaftlichen Risiken wie Pandemien und Atomkrieg."*

Ob diese Warnung vor den Gefahren der KI berechtigt ist oder nicht, wird das FIfF wie schon in der Vergangenheit sicherlich noch lange beschäftigen. Sie muss auf jeden Fall ernst genommen werden. Ich habe mich beim Lesen allerdings gleich gefragt, was diese Leute zu ihrer Mahnung bewogen hat: Einsicht? Ernste Sorge? Kenntnisse, die sich noch nicht herumgesprochen? Langeweile? Wenn sie recht damit haben, dass die aufkommenden und absehbaren KI-Systeme die Existenz der Menschheit bedrohen, dann könnten all die vielen Verantwortlichen aus den großen IT-Konzernen, die unterschrieben haben, die Entwicklungen stoppen, die Milliardeninvestitionen in gesellschaftlich nützliche Anwendungen umlenken, die existierenden, als gefährlich eingestuften Systeme abschalten und die gigantischen Datensammlungen, ohne die die inkriminierten Anwendungen gar nicht möglich wären, löschen oder unzugänglich machen. Was hindert sie? Das Gedicht thematisiert die Möglichkeit der aktiven Verweigerung:

Informatiker:innen, Ihr müsst nicht
mitdrehen an der Rüstungsspirale,
beitragen zur Optimierung des Kriegsgeschäfts,
soziale Überwachungstechnik entwickeln,
Profit- und Machtgier befördern,
mithelfen bei Natur- und Umweltzerstörung –
Ihr müsst nicht.

Geeignete Texte für den SchlussFIfF bitte mit Quellenangabe an *redaktion@fiff.de* senden.