

E..I..f..F..Kommunikation

Zeitschrift für Informatik und Gesellschaft

40. Jahrgang 2023

Einzelpreis: 7 EUR

2/2023 – Juni 2023



**Mensch – Gesellschaft – Umwelt ...
und Informatik**

ISSN 0938-3476

• BigBrother Awards • Aufruf zur Mitwirkung an der #FlfFKon23 • netzpolitik.org •

Inhalt

Ausgabe 2/2023

inhalt

- 03 Editorial
- Stefan Hügel

Forum

- 04 Der Brief: Realpolitik 2023
- Stefan Hügel
- 06 Cyberpeace – Für Frieden, Freiheit und eine lebenswerte Welt
- Daniel Guagnin, Hans-Jörg Kreowski und Margita Zallmann
- 06 Kampagne für ein globales Verbot von bewaffneten Drohnen
- Gemeinsamer Aufruf
- 08 Aufruf zur Mitwirkung und Mitgestaltung der FIfF-Konferenz 2023 in Berlin – Verlängerung

Mensch, Gesellschaft, Umwelt – und Informatik

- 09 Von Software-Beton, falschen Vorhersagen und intelligenter Diskriminierung
- Britta Schinzel
- 14 Der Silikonheini
- Andreas Wieland
- 16 Von Resignation zu Optimismus
- Maximilian Thomsen
- 20 Unbemenschte Systeme bei der Bundeswehr
- Christian Heck
- 29 Hegelsche Dialektik und das Problem der Formalisierung in Mathematik, Elektrodynamik, Systemtheorie und Künstlicher Intelligenz
- Wolfgang Krieger
- 33 Die militärische Seite der Digitalisierung
- Hans-Jörg Kreowski

Rubriken

- 67 Impressum/Aktuelle Ankündigungen
- 68 SchlussFIfF

BigBrotherAwards 2023

- 36 BigBrotherAwards 2022 – Einleitung
- Stefan Hügel
- 39 Kategorie *Behörden und Verwaltung* – Laudatio
- Peter Wedde
- 41 Kategorie *Kommunikation* – Laudatio
- padeluun
- 44 Kategorie *Lebenswerk* – Laudatio
- Thilo Weichert

Netzpolitik.org

- 47 Den Geheimdiensten endlich Grenzen setzen
- Constanze Kurz
- 49 Mehr als die Summe der Einzelteile
- Josefine Kulbatzki
- 52 Horchen, aber nicht hacken
- Constanze Kurz und Markus Reuter
- 54 Chatkontrolle ist grundrechtswidrig und wird scheitern
- Andre Meister
- 56 Die sechs größten Probleme im AI Act
- Daniel Leisegang, Chris Köver, Sebastian Meineck
- 60 Womit sich Strafverfolger bald befassen müssen
- Constanze Kurz
- 61 Prekäre Klickarbeit hinter den Kulissen von ChatGPT
- Daniel Leisegang
- 62 Datenschutzkonferenz nimmt ChatGPT unter die Lupe
- Anna-Lena Schmierer

FIfF e. V.

- 63 Mitgliederversammlung des FIfF

Lesen & Sehen

- 64 Grundrechte-Report 2023 der Öffentlichkeit vorgestellt
- Grundrechte-Report
- 65 So geht nachhaltige Digitalisierung
- Bits & Bäume

Editorial

Mensch, Gesellschaft, Umwelt – und Informatik: unter diesem Leitmotiv wollen wir in dieser Ausgabe ein breites Spektrum von Beiträgen zusammenfassen. Dabei werden die klassischen Themen des FfF eine wesentliche Rolle spielen: Künstliche Intelligenz und deren Verknüpfungen mit dem Militär, Überwachung und Kontrolle, Cyberpeace.

Den Anfang macht Britta Schinzel über *Software-Beton, falsche Voraussagen und intelligente Diskriminierung*. Sie untersucht – so der Untertitel –, wie digitale Entscheidungs-Architekturen Menschen und Lebensräume einheitlich ordnen:

Indem die Systeme und Architekturen der Informatik nicht nur technische, sondern längst auch soziale und politische Steuerungen übernehmen, definieren sie zunehmend auch soziale Ordnungen, und das oft an demokratischen Diskursen und parlamentarischen Entscheidungen vorbei.

Und:

Die Herausforderung digitaler Transformation besteht nicht nur in der verlässlichen Gestaltung und Sicherung der sozio-technischen Systeme, sondern vor allem darin, Menschen dazu zu befähigen, mit Technikunterstützung, aber auch ohne sie, sicher, gleichbehandelt und selbstbestimmt agieren zu können.

Andreas Wieland setzt sich im Dialog zwischen „Silikonheini“ und „Kohlenstoffheini“ damit auseinander, welche Restriktionen ChatGPT (anscheinend) auferlegt wurden, um seine Antworten in politisch korrekten Bahnen zu halten und Rassismus und Sexismus – wie es bei anderen Chatbots zu beobachten war – in den Antworten zu verhindern. Er thematisiert dabei auch die überraschende Schwäche der untersuchten Version, mit mathematischen Fragestellungen umzugehen oder Schach zu spielen.

Raus aus der Falle der Teilnahmslosigkeit! fordert Maximilian Thomsen in seinem Beitrag und setzt auf digitalen Optimismus statt digitale Resignation. Darunter versteht er, Technologie zu gestalten ohne sich dabei einer unkritischen „Techno-Elite“ anzuschließen: „Ich glaube an eine Utopie, die auf erneuerbaren Energien und nachhaltigen Technologien beruht“, schreibt er im Fazit seines Beitrags.

In seinem Beitrag *Unbemenschte Systeme bei der Bundeswehr* fasst Christian Heck ein Hearing der Zeitschrift Behörden-Spiegel zu *Unbemannten Systemen* zusammen. Er schreibt in seinem Beitrag über erweiterte Realitäten, die sich beispielsweise im „Gläsernen Gefechtsfeld“ – so der Titel einer entsprechenden Studie der Bundeswehr – zeigen. Er differenziert zwischen IT-, Militär-, politischer und Alltagssprache und thematisiert die Auswirkungen auf die Kommunikation über militärische Sachverhalte. Und er geht auf die zunehmende Bedeutung von Künstlicher Intelligenz und Machine Learning für militärische Anwendungen ein.

Wolfgang Krieger setzt in seinem philosophischen Beitrag die Hegelsche Dialektik zum Problem der Formalisierung in Mathe-

matik, Elektrodynamik, Systemtheorie und Künstlicher Intelligenz in Beziehung:

Die Hegelsche Dialektik, unter dem Eindruck der Aufklärung und der Vernunft als idealistische, das heißt die Wirklichkeit als Produkt des Geistes unterstellend, erfährt ihre Verwandlung in eine materialistische, den experimentell erforschten widersprüchlichen Verhältnissen der Natur „entwendeten“ Form.

Gut 150 Jahre später löst die Initiative mehrerer bedeutender Unternehmen des digitalen Finanzkapitals die Entwicklung des Systems ChatGPT aus. Ein fast unendlich großes Budget, ein uneingeschränkter Marktzugang wie auch eine nahezu monopolartige Kontrolle über Milliarden digitaler Dialoge sichern den politischen wie wirtschaftlichen Erfolg. In ihm manifestiert sich die Funktion des lange gesuchten dynamischen Akteurs und Partners bedeutsamer KI-Technologien. Das Internationale Finanzkapital US-amerikanischer Herkunft verwirklicht sein eigenes Wesen als virtuelle Simulation einer künstlichen und von einer natürlichen nur schwer unterscheidbaren Intelligenz.

Den Schwerpunkt schließt Hans-Jörg Kreowski mit einem Beitrag, der die militärische Seite der Digitalisierung thematisiert. Er zeichnet die militärische Digitalisierung von ihren Anfängen bei Konrad Zuse bis zum heutigen Informations- und Cyberkrieg nach. Dabei thematisiert er auch aktuelle Entwicklungen der Künstlichen Intelligenz. Der Beitrag endet mit einem Hinweis auf die Cyberpeace-Kampagne des FfF.

In diesen Tagen jähren sich die Enthüllungen von Edward Snowden zur weltweiten Überwachung der Kommunikation durch Geheimdienste zum zehnten Mal – und scheinen fast schon wieder vergessen. Obwohl auch parlamentarische Untersuchungen die Vorwürfe bestätigten, hat sich an der Situation nichts grundlegendes geändert – es scheint, als würden Politik und Behörden die Überwachung einfach fortsetzen oder eher noch verstärken. Auch die fortdauernden Debatten über die Vorratsdatenspeicherung und – in jüngerer Zeit – die Chatkontrolle zeigen, dass der Wille von politisch Verantwortlichen und den ihnen unterstehenden Behörden zu umfassender Kontrolle ungebrochen ist. Constanze Kurz setzt sich in ihrem Kommentar für *NetzpPolitik.org* mit Edward Snowden und den Folgen auseinander.

Zuletzt bleibt mir, herzliche Glückwünsche auszusprechen. Vor einigen Tagen, am 26. April 2023 feierte unsere Gründungsvorsitzende Christiane Floyd, der wir 2021 die Weizenbaum-Medaille verliehen haben, ihren achtzigsten Geburtstag. Christiane, im Namen des Vorstands und des ganzen FfF die besten Wünsche und weiterhin alles Gute.

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

Stefan Hügel
für die Redaktion



Realpolitik 2023



Liebe Freundinnen und Freunde des FlFF, liebe Mitglieder,

vor dreißig Jahren waren Asyl und Zuwanderung ein prägendes Thema in der deutschen Öffentlichkeit. Viele Menschen suchten damals bei uns Schutz vor politischer Verfolgung. „Politisch Verfolgte genießen Asylrecht“, so hieß es dazu eindeutig und unmissverständlich im Deutschen Grundgesetz – eine Garantie, die nicht zuletzt aufgrund unserer historischen Erfahrungen gegeben wurde.

Gleichzeitig wuchs die fremdenfeindliche Gewalt. Hoyerswerda, Rostock-Lichtenhagen, Mölln, Solingen sind heute Orte kollektiver Erinnerung. In Solingen verloren fünf Menschen ihr Leben nach einem Brandanschlag auf ihr Wohnhaus. Bundespräsident Steinmeier betonte anlässlich der Trauerfeier zum dreißigjährigen Gedenken:

Als Bundespräsident kann ich nicht dazu schweigen, in welchem Klima diese Anschläge gediehen sind. Ich kann heute nicht zu Ihnen sprechen, ohne den braunen Nährboden des Solinger Brandanschlags und der vielen weiteren Taten zu benennen.¹

Er benennt in seiner Rede den rechten Terror und das gesellschaftliche Umfeld, in dem er gedieh – bis heute. Die Serie fremdenfeindlicher Anschläge war mit Solingen nicht zu Ende. Es folgten die Morde der Terrorgruppe NSU, Halle, Hanau, der Mord an Walter Lübcke. Zu Recht wies der Bundespräsident darauf hin:

Viel zu lange saß unser Land der durch nichts gestützten, aber ständig wiederholten Behauptung auf, es seien verblendete Einzeltäter, die ihr Unwesen treiben.

Doch leider schwieg der Bundespräsident dann doch zu ein paar Aspekten des damaligen und des heutigen politischen Klimas. Wenige Tage vor dem Anschlag von Solingen war im deutschen Bundestag das Grundgesetz geändert und das Grundrecht auf Asyl faktisch abgeschafft worden – begründet wurde das unter anderem, in klassischer Täter-Opfer-Umkehr, mit dem gesellschaftlichen Klima und der drohenden „Asylantenflut“, so eine damals häufig genutzte Vokabel.

Nun wäre es sicher nicht angemessen, nach dem Prinzip *post hoc ergo propter hoc* einen unmittelbaren Zusammenhang zwischen den Ereignissen herzustellen. Doch auch die damalige Debatte um den „Asylkompromiss“ hat das gesellschaftliche Klima geprägt, in dem „... diese Anschläge gediehen sind.“

Realpolitik 2023: Während in Solingen Trauerfeiern stattfinden, wird auf europäischer Ebene eine Reform des europäischen Asylsystems verhandelt. Bundesinnen- und Heimatministerin Nancy Faeser findet:

Das ist ein historischer Erfolg – für die Europäische Union, für eine neue, solidarische Migrationspolitik und für den Schutz von Menschenrechten.²

Die Flüchtlingshilfsorganisation ProAsyl bewertet den Entwurf zurückhaltender³:

Die Reform führe zu Abschiebungen in Drittstaaten, sie ermögliche Grenzverfahren und de facto Inhaftierung von Kindern, Verschärfung des Dublin-Systems durch Einschränkung des Rechtsschutzes und Aushebelung des Zugangs zu einem Asylverfahren und Legitimierung von Pushbacks als präventivem Grenzschutz. Ricarda Lang, Vorsitzende der Grünen, erklärte dann auch, Deutschland hätte dem Vorschlag zur Reform nicht zustimmen dürfen⁴. Hat es aber. Auch dadurch wird das gesellschaftliche Klima geprägt, in dem „... diese Anschläge gediehen sind.“ Doch der Bundespräsident schwieg dazu – sicherlich nur, um die Würde der Gedenkfeier nicht zu stören.

Der Krieg in der Ukraine dauert an – und erreicht allem Anschein nach mit der Zerstörung des Kachowka-Staudamms eine neue Eskalationsstufe. Die Frage der fortdauernden – und scheinbar alternativen – Waffenlieferungen haben wir in der letzten Ausgabe an dieser Stelle thematisiert⁵.

Doch es stellt sich die Frage nach den langfristigen Folgen einer Politik, die wieder der militärischen Option den Vorzug gibt. Unter dem Schlagwort *Zeitenwende* wird propagiert, dass die Bundeswehr besser ausgestattet und die militärischen Fähigkeiten gestärkt werden sollen. Dies wird mit Rüstungslieferungen an die Ukraine vermennt und prägt die öffentliche Debatte und die Berichterstattung – zeitweise schien es kaum eine Nachrichtensendung zu geben, in der nicht Leopard-Kampfpanzer im Gelände gezeigt wurden und die mehr an Imagefilme der Rüstungsindustrie erinnerten als an sachliche politische Berichterstattung. Fehlende Ernsthaftigkeit⁶ lässt auch daran zweifeln, ob in allen Fällen verinnerlicht wurde: Der Kampfpanzer Leopard 2 ist kein niedliches Plüschtier, sondern ein militärisches Waffensystem, das dazu konzipiert wurde, auf möglichst große Distanz möglichst viele Menschen zu töten. Dies alles schafft ein Klima, in dem wieder verstärkt auf militärische Stärke und Lösungen gesetzt und ihre Akzeptanz gefördert wird.

Realpolitik 2023: Schon fordert die Wehrbeauftragte des Deutschen Bundestags, junge Menschen (aller Geschlechter) wieder zur Musterung „einzuladen“⁷. Forderungen werden laut, in Schulen *Wehrunterricht* einzuführen, ganz nach Vorbild der DDR. Im derzeit diskutierten Entwurf des Selbstbestimmungsgesetzes – in dem die Rechte von trans Menschen gestärkt werden sollen – ist ein explizites Verbot enthalten, im Verteidigungsfall dem Einsatz an der Waffe durch eine Änderung des Geschlechts zu entgehen⁸. Man mag dieses Verbot als Verhinderung missbräuchlicher Anwendung des Rechts befürworten – dennoch zeigt es, wie tief militärisches Denken bereits in intimste Bereiche der Persönlichkeit eindringt.

Vielleicht lohnt an dieser Stelle ein kleiner Rückblick in die 1980er-Jahre: Der republikanische US-Präsident Ronald Reagan übernahm damals sein Amt im Januar 1980 und verfolgte wieder eine verstärkt konfrontative Politik gegenüber der Sowjetunion und den Staaten des Warschauer Vertrags. NATO-„Doppelbeschluss“⁹, Pershing-

II-Mittelstreckenraketen, Cruise Missiles bestimmten damals die Nachrichten und bescherten der Friedensbewegung enormen Zulauf – die Menschen hatten Angst vor einem Weltkrieg, der dem Leben auf der Erde, wie wir es kennen, ein Ende setzen würde.

Wir erinnern uns an die Ereignisse dieser Jahre: Den Einmarsch Russlands in Afghanistan, den Abschuss einer Passagiermaschine der Korean Airlines (Flug KAL 007) durch einen sowjetischen Abfangjäger in der Nähe der Insel Sachalin, den Boykott der Olympischen Spiele 1980 in Moskau durch westliche und 1984 in Los Angeles durch östliche Teams. Der Offizier der sowjetischen Luftverteidigungsstreitkräfte Stanislaw Jefgrafowitsch Petrow verhinderte wohl durch sein besonnenes Handeln bei einem Fehlalarm 1983 einen *Atomkrieg aus Versehen* – ein Ereignis, vor dem auch das FfF nach seiner Gründung 1984 immer wieder gewarnt hat¹⁰. Eindringlich wurde ein atomarer Konflikt und seine Folgen in dem Spielfilm *The Day After* geschildert – angeblich wurde US-Präsident Reagan sehr nachdenklich, nachdem er diesen Film gesehen hatte.

Gleichzeitig bereitete man sich auf einen möglichen Konflikt vor: In den 1980er-Jahren war es in manchen ländlichen Gegenden üblich, dass militärische Tiefflüge über bewohntem Gebiet geübt wurden. Abstürze des Kampfflugzeugs Lockheed F-104 Starfighter waren gefühlt an der Tagesordnung und kosteten 116 Piloten das Leben. Der Versuch, solche Flugübungen der Bevölkerung als Freizeitspaß schmackhaft zu machen, führte 1988 zur Flugtagkatastrophe von Ramstein, die 70 Menschen das Leben kostete. Der kalte Krieg forderte viele Todesopfer, auch im vermeintlichen Frieden. Als 1989 der eiserne Vorhang fiel, hofften wir alle, dass es mit der Militarisierung des öffentlichen Lebens ein Ende hätte – zumindest im Kern Europas.

Realpolitik 2023: Vom 12.-23. Juni 2023 findet über Deutschland die Luftübung *Air Defender 23* statt – die größte Übung dieser Art seit Bestehen der NATO. Zwar „nur“ eine Verlegübung mit regional begrenzten Tiefflugaktivitäten, die aber die Grundlage für eine weitere Eskalation schafft. „So sieht für mich glaubwürdige Abschreckung aus“, jubelt Ingo Gerhartz, Inspekteur der Luftwaffe¹¹.

*Wann wird man je verstehn?*¹²

Mit FfFigen Grüßen
Stefan Hügel

Anmerkungen

- 1 *Gedenken an die Opfer des Brandanschlags von Solingen*, Solingen, 29. Mai 2023, <https://www.bundespraesident.de/SharedDocs/Reden/DE/Frank-Walter-Steinmeier/Reden/2023/05/230529-Anschlag-Solingen.html?nn=9042544>
- 2 <https://twitter.com/NancyFaeser/status/1666882730015981588>
- 3 <https://www.proasyl.de/news/faq-zur-geplanten-reform-des-gemeinsamen-europaeischen-asylsystems-geas/>
- 4 *Grüne tief gespalten über EU-Asylrechtsverschärfung*, <https://www.spiegel.de/ausland/gruene-tief-gespalten-ueber-eu-asylrechtsverschaeerfung-a-e5499d60-6706-485c-9ae5-f7b1ac51d637>
- 5 *Die Stellungnahme erschien als „Brief“ in der FfF-Kommunikation 1/2023 und ist auch hier zu finden: „Europa der Verteidigung und der Rüstung“*, <https://blog.fiff.de/europa-der-verteidigung-und-der-ruestung/>
- 6 *Samira El Ouassil: Im Panzer der Ironie*, <https://www.spiegel.de/kultur/annalena-baerbock-friedrich-merz-und-die-buettenrede-im-panzer-der-ironie-kolumne-a-38c2dfbf-2e4b-4194-810f-33752a88bd09>
- 7 *Wehrbeauftragte Högl bringt Rückkehr der Musterung ins Spiel*, <https://www.spiegel.de/politik/deutschland/bundeswehr-eva-hoegl-bringt-rueckkehr-der-musterung-ins-spiel-a-10b712ef-2ece-48b1-8775-c7b50bdce875>
- 8 *René Pfister: Kann man sich dafür entscheiden, eine Frau zu sein?* <https://www.spiegel.de/politik/selbstbestimmungsgesetz-kann-man-sich-dafuer-entscheiden-eine-frau-zu-sein-kolumne-a-e3c2407e-67d5-4178-87e2-58239b97e55e>
- 9 ... der vom damaligen Bundeskanzler Helmut Schmidt maßgeblich initiiert wurde.
- 10 Aktuell dazu <https://atomkrieg-aus-versehen.de>
- 11 *Nato-Übung über Deutschland – Luftwaffeninspekteur spricht von „glaubwürdiger Abschreckung“*, <https://www.spiegel.de/politik/luftwaffen-inspekteur-ingo-gerhartz-nennt-nato-uebung-ueber-deutschland-glaubwuerdige-abschreckung-a-5a6f47ae-2450-447b-94f4-c445aa95083b>
- 12 *Joan Baez: Sag mir, wo die Blumen sind*. Autor Pete Seeger, deutscher Text Max Colpet, https://de.wikipedia.org/wiki/Where_Have_All_the_Flowers_Gone



Das FfF bittet um Eure Unterstützung

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

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



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

Spendenkonto:

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

Cyberpeace – für Frieden, Freiheit und eine lebenswerte Welt

Am 13. und 14. Mai hat der Zukunftsworkshop Cyberpeace an der Universität Bremen stattgefunden. In kleiner Runde wurde diskutiert, mit welcher thematischen Ausrichtung und mit welchen Aktivitäten die Cyberpeace-Kampagne weitergeführt werden soll.

Grundlage waren fünf kurze Impulsvorträge.

- Daniel Guagnin hat zu IT-(Un-)Sicherheitsfragen gesprochen mit dem Fokus auf Sicherheitslücken und den Streit um die Integrität von IT als zentrales Merkmal einer friedlichen und defensiven Cyber-Strategie.
- Christian Heck hat vom Hearing *Unbemannte Systeme* im Rahmen der *Defence Day* Reihe der Zeitschrift *Behörden Spiegel* berichtet (siehe dazu die ausführliche schriftliche Fassung in diesem Heft). Er hat illustriert, wie die Bundeswehr auf ein „gläserndes Gefechtsfeld“ hinarbeitet und wie reale Operationen als Experimentierfeld für algorithmische Kampfunterstützung dienen.
- Hans-Jörg Kreowski hat anknüpfend an die jüngsten Enthüllungen über die russischen Cyberkriegsplanungen unter dem Titel *Vulkan Files* an das bisherige Konzept der inzwischen zehnjährigen Kampagne erinnert.
- Christoph Marischka hat das *Future Combat Air System* (FCAS), das gigantomanische Waffensystem der Zukunft Deutschlands, Frankreichs und Spaniens, skizziert und die Kampagne *Escape FCAS* vorgestellt. Er hat dabei einen Einblick in aktuelle Militärstrategien vermittelt und erläutert, wie IT, Cloud-Daten und Künstliche Intelligenz in einem vernetzten Kampfflugzeug-System eine zentrale Rolle spielen sollen.
- Jennifer Menninger ist auf den Stand der Konsultationen auf der Ebene der Vereinten Nationen im Rahmen der *Open-ended Working Group (OEWG) on security of and in the use of information and communications technologies (ICTs)* eingegangen, wobei es darum geht, gemeinsame Prinzipien in diesem Kontext auszuhandeln. Dass Russland hier besonders initiativ auftritt, weckt das Misstrauen insbesondere der NATO-Staaten.



Es gab ein großes Einvernehmen, dass die Cyberpeace-Kampagne nach wie vor Themen wie Sicherheitslücken aufnehmen, sich aber nicht nur auf eine Gegenposition zum Cyberkrieg im engeren Sinne beschränken soll. Sie soll sich gegen alle Formen von Krieg und Rüstung mit Hilfe von Informations- und Kommunikationstechnik (IKT) einschließlich Drohnenkrieg und militärischer Vereinnahmung von Künstlicher Intelligenz richten. Mehr noch soll im Rahmen der Kampagne auch ein positives Bild gezeichnet und auf die Anwendung von IKT bei der Gestaltung einer friedlichen Entwicklung der Welt eingegangen werden.

Die Workshop-Teilnehmer:innen haben verabredet, auf der nächsten FIFF-Konferenz, die vom 3. bis 5. November in Berlin stattfindet, einen Cyberpeace-Block zu gestalten aus vielleicht zwei 20- oder 30-minütigen Vorträgen, einem Pecha Kucha (also einer Serie mehrerer Kurzvorträge mit 20 Folien à 20 Sekunden), einer Podiumsdiskussion und möglicherweise der Präsentation eines Kunstprojekts mit Studierenden der Kunsthochschule für Medien Köln unter Leitung von Christian Heck. Mitwirkung und weitere Ideen sind willkommen. Außerdem wird voraussichtlich auf dem Symposium *Wissenschaft für den Frieden* zum 40-jährigen Bestehen der Zeitschrift *Wissenschaft und Frieden* am 6. und 7. Oktober in Bonn ein Cyberpeace-Workshop stattfinden (<https://pretalx.com/wissenschaft-fuer-den-frieden-2023/cfp> mit Link für Einreichungen). Wer speziell zum Workshop beitragen oder daran teilnehmen möchte, melde sich bitte bei kreo@fiff.de. Wer die Arbeit der Cyberpeace-Kampagne unterstützen oder zumindest über deren Aktivitäten auf dem Laufenden gehalten werden möchte, kann gern in die Mailingliste aufgenommen werden. Schickt bitte eine entsprechende E-Mail an margita.zallmann@t-online.de oder kreo@fiff.de.

Zum Schluss dieses kurzen Rubriktextes sei noch darauf hingewiesen, dass Christian Hecks Artikel *Unbemenschte Systeme bei der Bundeswehr – Beobachtungen zweiter Ordnung* und Hans-Jörg Kreowskis Artikel *Die militärische Seite der Digitalisierung* in diesem Heft einen engen Bezug zu Cyberpeace haben.

Gemeinsamer Aufruf

Kampagne für ein globales Verbot von bewaffneten Drohnen

Aufruf zur internationalen Unterstützung

In der folgenden Erklärung wird von nationalen und internationalen Organisationen die Forderung erhoben, dass die Vereinten Nationen einen Vertrag über das Verbot bewaffneter Drohnen verabschieden. Diese Forderung ist inspiriert durch das Übereinkommen über das Verbot biologischer Waffen (1972), das Übereinkommen über das Verbot chemischer Waffen (1997), das Übereinkommen über das Verbot von Antipersonenminen (1999), das Übereinkommen über das Verbot von Streumunition (2010), den UN-Vertrag über das Verbot von Atomwaffen (2017) und ist solidarisch mit der Kampagne für einen UN-Vertrag zum Verbot von Killerrobotern. Die Forderung nach einem Verbot von bewaffneten Drohnen bezieht sich auf Grundwerte wie Menschenrechte, Internationalismus, Repräsentation des globalen Südens und seinen Schutz vor neokolonialer Ausbeutung und Stellvertreterkriegen und beachtet die Stimmen von Graswurzelbewegungen und von Frauen, jüngeren Menschen und Marginalisierten weltweit. Wir sind uns der drohenden Gefahr bewusst, dass bewaffnete Drohnen autonom werden können, was das Potenzial für Tod und Zerstörung weiter erhöht.

In Anbetracht dessen, dass der Einsatz von bewaffneten Drohnen (UAV – *unmanned aerial vehicles*) in den letzten 21 Jahren zur Tötung, Verletzung, Terrorisierung und/oder Vertreibung von Millionen Menschen in Afghanistan, Irak, Pakistan, Palästina, Syrien, Libanon, Iran, Jemen, Somalia, Libyen, Mali, Niger, Äthiopien, Sudan, Südsudan, der armenischen Region in Aserbaidschan, Westsahara, kurdischen Regionen in der Türkei, Ukraine, Russland und anderen Orten geführt hat;

In Anbetracht dessen, dass zahlreiche detaillierte Studien und Berichte über Opfer durch den Einsatz von bewaffneten Drohnen darauf hinweisen, dass es sich bei der Mehrzahl der getöteten, verletzten, vertriebenen oder anderweitig geschädigten Menschen um Nichtkombattant:innen, darunter Frauen und Kinder, handelte;

In Anbetracht dessen, dass ganze Gemeinschaften und große Bevölkerungsgruppen durch den ständigen Flug bewaffneter Drohnen am Himmel über ihren Köpfen terrorisiert, eingeschüchtert und psychologisch geschädigt werden, auch wenn sie selbst nicht durch die Waffen getroffen werden;

In Anbetracht dessen, dass die Vereinigten Staaten, China, die Türkei, Pakistan, Indien, Iran, Israel, das Vereinigte Königreich, Frankreich, Deutschland, Italien, Spanien, Südafrika, Südkorea, Saudi-Arabien, die Vereinigten Arabischen Emirate, Kasachstan, Russland und die Ukraine bewaffnete Drohnen produzieren und/oder entwickeln, während eine wachsende Zahl von Ländern kleinere, kostengünstige „herumlungernde“ Einwegmunition (*loitering munition*) und/oder Einwegdrohnen, die sogenannten „Selbstmord“- oder „Kamikaze“-Drohnen, produziert;

In Anbetracht dessen, dass einige dieser Länder, darunter die Vereinigten Staaten, Israel, China, die Türkei und der Iran, waffenfähige Drohnen in immer mehr Länder exportieren, während Hersteller in weiteren Ländern Teile für die Produktion bewaffneter Drohnen exportieren;

In Anbetracht dessen, dass der Einsatz bewaffneter Drohnen zu zahlreichen Verstößen gegen internationale Menschenrechte und humanitäres Völkerrecht durch Staaten und nichtstaatliche bewaffnete Gruppen auf der ganzen Welt geführt hat, darunter Verstöße gegen internationale Grenzen, nationale Souveränitätsrechte und UN-Abkommen;

In Anbetracht dessen, dass die Materialien, die für den Bau und die Bewaffnung rudimentärer Drohnen erforderlich sind, weder technologisch fortgeschritten noch teuer sind, so dass ihr Einsatz bei Milizen, Söldnern, Aufständischen und Einzelpersonen in alarmierendem Tempo zunimmt;

In Anbetracht dessen, dass eine wachsende Zahl nichtstaatlicher Akteure Angriffe und Attentate mit bewaffneten Drohnen verübt hat, unter anderem: Constellis Group (ehemals Blackwater), Wagner Group, Al-Shabab, die Taliban, der Islamische Staat, Al-Qaida, libysche Rebellen, Hisbollah, Hamas, die Houthis, Boko Haram, mexikanische Drogenkartelle sowie Milizen und Söldner in Venezuela, Kolumbien, Sudan, Mali, Myanmar und anderen Ländern des globalen Südens;

In Anbetracht dessen, dass bewaffnete Drohnen häufig in unerklärten und illegalen Kriegen eingesetzt werden;

In Anbetracht dessen, dass bewaffnete Drohnen die Hemmschwelle zum bewaffneten Konflikt senken und Kriege ausweiten und verlängern können, da sie Angriffe ohne physisches Risiko für das Boden- und Luftwaffenpersonal der Anwendenden der bewaffneten Drohnen ermöglichen;

In Anbetracht dessen, dass, abgesehen vom russisch-ukrainischen Krieg, die meisten Angriffe bewaffneter Drohnen bisher gegen nicht-weiße, nicht-christliche Menschen im globalen Süden gerichtet waren oder sind;

In Anbetracht dessen, dass sowohl technologisch fortgeschrittene als auch einfache Drohnen mit Raketen oder Bomben ausgerüstet werden können, die chemische Waffen oder abgereichertes Uran enthalten;

In Anbetracht dessen, dass sowohl technologisch fortgeschrittene als auch einfache bewaffnete Drohnen eine existenzielle Bedrohung für die Menschheit und den Planeten darstellen, da sie für Angriffe auf Atomkraftwerke eingesetzt werden können, von denen es Hunderte in 32 Ländern, vor allem im globalen Norden, gibt;

In Anbetracht dessen, dass bewaffnete Drohnen aus den oben genannten Gründen ein Instrument zur Verletzung des nationalen und internationalen Rechts darstellen, wodurch sich Feindseligkeiten ausweiten und die Wahrscheinlichkeit von innerstaatlichen Konflikten, Stellvertreterkriegen, größeren Kriegen und der Eskalation bis hin zu nuklearen Bedrohungen steigt;

In Anbetracht dessen, dass der Einsatz bewaffneter Drohnen die grundlegenden Menschenrechte verletzt, die in der Allgemeinen Erklärung der Menschenrechte (1948) und dem Internationalen Pakt über bürgerliche und politische Rechte (1976) garantiert sind, insbesondere im Hinblick auf das Recht auf Leben, Privatsphäre und ein faires Verfahren, sowie gegen die Genfer Konventionen und ihre Protokolle (1949, 1977), insbesondere im Hinblick auf den Schutz der Zivilbevölkerung vor unterschiedslosen oder unverhältnismäßigen Angriffen;

... stellen wir folgende Forderungen:

Wir fordern die UN-Generalversammlung, den UN-Menschenrechtsrat und die zuständigen Ausschüsse der Vereinten Nationen auf, unverzüglich die Verstöße gegen das Völkerrecht und die Menschenrechte durch staatliche und nichtstaatliche Akteure, die Drohnenangriffe aus der Luft verübt haben oder verüben, zu untersuchen.

Wir fordern den Internationalen Strafgerichtshof auf, die schwerwiegendsten Fälle von Drohnenangriffen auf zivile Ziele als Kriegsverbrechen und Verbrechen gegen die Menschlichkeit zu untersuchen, darunter Angriffe auf Rettungs- und Hilfskräfte, Hochzeiten, Beerdigungen und alle Drohnenangriffe, bei denen keine Kriegserklärung vorliegt zwischen dem angreifenden Land und dem Land, in dem die Angriffe stattgefunden haben.

Wir fordern die Generalversammlung der Vereinten Nationen auf, die tatsächlichen Opferzahlen durch Drohnenangriffe sowie deren Umstände zu untersuchen und Entschädigungen für die Opfer unter Nichtkombattant:innen zu fordern.

Wir fordern die Regierungen aller Länder der Welt auf, die Entwicklung, den Bau, die Produktion, das Testen, die Lagerung, den Verkauf, den Export und den Einsatz bewaffneter Drohnen zu verbieten.

UND: Wir fordern die Generalversammlung der Vereinten Nationen nachdrücklich dazu auf, einen Vertrag auszuarbeiten und zu verabschieden, der die Entwicklung, den Bau, die Produktion, das Testen, die Lagerung, den Verkauf, den Export, den Einsatz und die Verbreitung bewaffneter Drohnen weltweit verbietet.

Initiierende Organisationen (in alphabetischer Reihenfolge): Ban Killer Drones (USA), Bund für Soziale Verteidigung (Germany), CODEPINK: Women for Peace, Drohnen-Kampagne (German Drone Campaign), Drone Wars UK, International Fellowship of Reconciliation (IFOR), International Peace Bureau (IPB), Veterans for Peace, Women for Peace in Upstate New York, World BEYOND War

Initiiert: 1. Mai 2023

Das FIFF hat sich dem Aufruf angeschlossen.

Aufruf zur Mitwirkung und Mitgestaltung – Verlängerung

FIFF-Konferenz 2023

3. – 5. November 2023 in Berlin

Liebes FIFF-Mitglied,

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

Wir möchten gemeinsam mit euch allen in die Zukunft schauen!

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

Gemeinsam wollen wir auf der FIFF-Konferenz 2023 Perspektiven, Zukunftsvisionen, Chancen und Utopien erstrahlen lassen, die eine Inspiration für Umbruch und Aufbruch sein können. Mit welchen Inhalten befassen sich unsere Mitglieder, in welchen Bereichen sind sie aktiv, für welche Themen brennen sie?

Aufgrund Eurer Rückmeldungen haben wir drei Schwerpunkte ausgewählt, zu denen wir uns über Eure Vorschläge freuen:

- Cyberpeace – z. B. Kritik an der Planung zum Future Combat Air System (FCAS) und zur militärischen Nutzung der Künstlichen Intelligenz,

- Information und Nachhaltigkeit – Bits & Bäume – z. B. zu Konvivialität und IT & Entwicklungspolitik,
- Entwicklungen der Künstlichen Intelligenz – z. B. Chancen, aber auch Risiken, der Entwicklung und Nutzung von ChatGPT; Auswirkungen auf die IT-Sicherheit

Die Konferenz wird vom 3. bis 5. November 2023 in der Jugendherberge Berlin-Ostkreuz reserviert; um Veranstaltungstechnik, Streaming und das leibliche Wohl werden sich Vorstand und Geschäftsstelle kümmern.

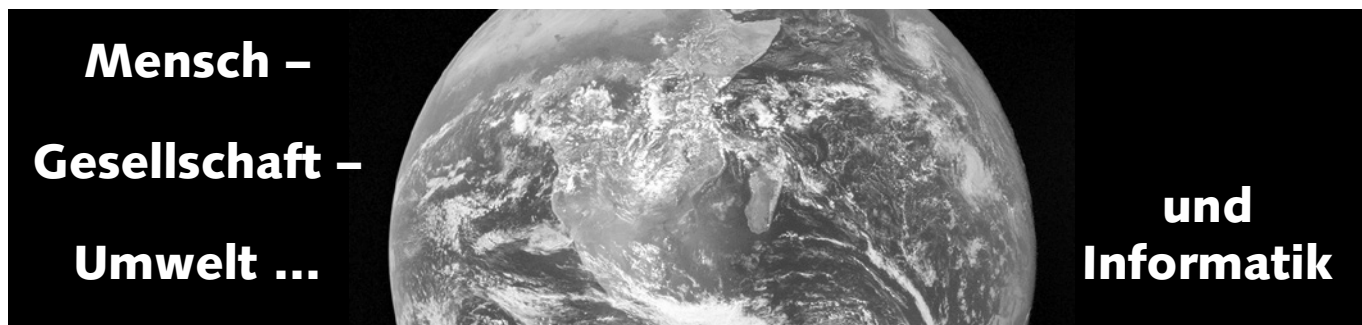
Wir wünschen uns weiterhin Eure Mitwirkung bei der inhaltlichen Planung und Programmgestaltung und erwarten gespannt Deine Einreichung. Unterschiedliche Formate sind dabei sehr willkommen, z. B. Vorträge, andere Art der Präsentation, ggf. auch kulturelle / künstlerische Beiträge, Podiumsdiskussionen, offene Diskussionen, Workshops.

Bitte schicke uns gerne weitere Vorschläge mit ein paar Zeilen zum intendierten Thema und zu deiner Person bis zum 15. August 2023 an info@fiffkon.de.

Wir freuen uns sehr auf deine Beiträge,

Dein FIFF-Vorstand





Britta Schinzel

Von Software-Beton, falschen Vorhersagen und *intelligenter* Diskriminierung Wie digitale Entscheidungs-Architekturen Menschen und Lebensräume einheitlich ordnen

Das deutsche wie das europäische Digitalisierungsprogramm haben es sich zum Ziel gesetzt, den Rückstand gegenüber konkurrierenden (wirtschafts-)politischen Systemen und Märkten aufzuholen und technische wie soziale Innovationen zu ermöglichen. Indem die Systeme und Architekturen der Informatik nicht nur technische, sondern längst auch soziale und politische Steuerungen übernehmen, definieren sie zunehmend auch soziale Ordnungen, und das oft an demokratischen Diskursen und parlamentarischen Entscheidungen vorbei.

Machtverschiebungen sind der größte Faktor für die Entstehung von Ungleichgewichten und Ungleichheiten durch die Digitalisierung. Auf sozialer und individueller Ebene greifen die Veränderungen tief in das Leben der Bürger:innen ein. Das ist vielfach erwünscht, etwa zur besseren Versorgung, zur Organisation des Arbeitsalltags, der Erweiterung des sozialen Lebens oder zur Unterhaltung. Gleichzeitig geht damit eine unsichtbare Bedrohung durch Überwachung, Arbeitsplatzverlust oder Ich-Verlust in *Profilen*, *Likes* und *Scores*, Desorientierung durch *Fake News* oder auch Bedrohung durch militärische Anwendungen einher.¹

Die Europäische Union ist gerade dabei, eine digitale Transformationsstrategie zu entwickeln,² die nahezu alle Lebensbereiche umfassen wird. Dafür wird eine große Umschichtung von Ressourcen in Gang gesetzt. Sie strebt dabei vor allem auf ökonomischer und rechtlicher Ebene eine digitale Netzwerkgesellschaft an, die zwar aufs Gemeinwohl ausgerichtet sein soll, sich aber vor allem an ökonomischen Werten und industriellem Wachstum orientiert und demokratische Legitimation und Mitgestaltung vermissen lässt.

Sie hat weniger die Bürger:innen im Auge als vielmehr das Ziel, Infrastrukturen, Daten, Hard- und Software unabhängig von amerikanischen Großkonzernen und chinesischer Produktion zu machen. Gleichzeitig sollen dadurch, quasi von selbst, soziale Innovationen entstehen. Verantwortungsrelationen, digitale Rechte und eine Ethik der digitalen Gesellschaft werden zwar problematisiert, aber die bisherigen Ergebnisse des Prozesses lassen nur unzureichende Aufmerksamkeit für Verantwortung und Zurechenbarkeit erkennen – und offenbaren zum Teil paradoxe Vorstellungen über einen Ausbau vertrauenswürdiger *Künstlicher Intelligenz* (KI).³ Gleichzeitig umgehen die EU-Verordnungen und Richtlinien mitunter demokratische Entscheidungsprozesse, verschieben Macht von nationalen Parlamenten hin zu EU-Regulierungsinstanzen, von der Legislative zur Exekutive, und instanzieren Realexperimente mit experimenteller Gesetzgebung, die sich vor allem in unsicheren Umgebungen als risikoreich erweisen.

Transkriptionen, Algorithmen und digitale Architekturen

Neue Techniken manifestieren sich meist in miteinander verwobenen, materiell-semiotischen Prozessen von Bezeichnung, Bedeutungskonstruktion, physikalisch-technischer Materialisierung, menschlicher Struktur und kulturellen Lebensräumen. Und sie erzeugen immer neue Bedeutungen, die sich mittels menschlicher Praktiken und maschineller Vorrichtungen unterschiedlich entfalten.

Für die Informationstechnik sollen Metaphern aus der Alltagssprache, Architektur und Konstruktionslehre die Bedeutung von Abstraktem erschließen.⁴ Anthropomorphisierende Transkriptionen wie *Künstliche Intelligenz* und andere Formulierungen, die den Maschinen Personenstatus und Autonomie verleihen, verwischen die Unterschiede zwischen Mensch und Maschine oder amalgamieren beide.

Welt und Leben werden so in Code transkribiert, in Datenstrukturen⁵ kategorisiert, und darüber Verhaltensmodelle und Entscheidungs-Architekturen konstruiert. Die notwendige Generalisierung, Standardisierung und Übergeneralisierung streift Kontexte ab und macht weltliches Hintergrundwissen unsichtbar. Die Modelle sind hochgradig selektiv, unterdrücken mögliche Alternativen, und lassen Seltenes unberücksichtigt. Soziale Daten werden mittels *Big Data* und *Machine Learning* entkontextualisiert gruppiert und in *Scores* vergleichbar gemacht, indem sie in Zahlen transkribiert werden.

Ein Algorithmus ist zunächst nichts anderes als eine *Aufbauvorschrift* auf Basis von elementaren Operationen auf Variablen eines Datentyps aus Zeichen, etwa der Menge der natürlichen Zahlen. Mit ihnen soll eine mathematische Aufgabe durch schrittweise Ausführung dieser Operationen gelöst werden. Algorithmen definieren also, was im Prinzip berechenbar und programmierbar ist. Sie sind aber, wie die von ihnen beschriebenen mathematischen Funktionen, weder intelligent noch schädlich,

sie sind der Erwägung und Beachtung von moralischen oder politischen Zielen nicht fähig.⁶ Dies gilt aber sehr wohl für die Fassung von Algorithmen in (intentionalen) Software(-Systemen) und unseren Umgang mit Automatisierung. Software wirkt immer als Verstärker unserer Vorurteile, Einbindungen oder Auslassungen. Diese werden auf dem Weg der Computerisierung oft unsichtbar und verfestigen sich zu „Software-Beton“.

Beeinflussung durch Entscheidungs-Architekturen

Die Open-Data-Strategie der EU-Kommission sieht eine Vermittlungs- und Dienstleistungsplattform für einen gemeinsamen *Datenraum* vor, in dem Daten über Gesundheit, Industrieproduktion, Landwirtschaft, Finanzwesen, Verkehr, Umwelt und Energie in verschiedenen Graden der Zugänglichkeit geteilt werden. Gespeist werden soll der Datenraum aus hochwertigen Datensammlungen des öffentlichen Sektors und von Personaldatenplattformen. Er soll Verwaltungs-, industrielle und wissenschaftliche Daten so zusammenführen, dass sie standardisiert, datenschutzkonform in Clouds auf verteilten Serverfarmen, interoperabel organisiert und prozessiert werden können. Sollte das Vorhaben gelingen, könnte sich die Plattform als marktgängiges Governance-Regime einer neuen Herrschaftsform über öffentliche Infrastruktur- und Versorgungssysteme herausstellen. Für die Open-Data-Strategie der EU stellen sich daher einige gewichtige Fragen, etwa: Wer kombiniert hier welche Daten, und wer genau konstruiert welche „Lösungen“ für welche „gesellschaftlichen Herausforderungen“? Wie werden all diese Transformationen demokratisch legitimiert? Wo bleiben Selbstbestimmung und Integrität der originären sozialen Räume, Kommunen und Bürger:innen? Und welche „öffentlichen Interessen“ sollen damit bedient werden?

Entscheidungs-Architekturen übernehmen einerseits die Benutzerführung im Bereich der Mensch-Maschinen-Schnittstellen (HMI) und umgehen dabei zu definierende Spezifikationen mittels *Use Cases* (Anwendungsbeispielen), andererseits auch die interne Steuerung von Prozessen. Was in das Eingabeformular und Ablaufmodell nicht eingearbeitet wurde, kommt im abstrakten Modell nicht vor und kann auch nicht berücksichtigt werden.⁸ Im Bereich des E-Commerce sind die Formulare oft so gestaltet, dass sie die Zielgruppe zu gewünschten Entscheidungen *schubsen* (*Nudging*, Beeinflussung, bis hin zu Manipulation). Hier sind wieder die Untiefen der Macht-Asymmetrie konstitutiv, denn typisierende, diskriminierende und ausschließende Schnittstellen fungieren als Filter gegen Ausnahmen oder ungewöhnliche Handhabungen.

Unter den Bedingungen *intelligenter* (d.i. KI-gestützter) *Technik* in unbestimmten Umgebungen, wie etwa beim autonomen Fahren, ist die Mensch-Maschine-Interaktion jedoch keineswegs mehr ohne Kontext gestaltbar. Hier können die komplexe Verkettung von Ereignissen in der Lebenswelt und nicht vorhersehbares Verhalten von Lebewesen vielfältige Quellen für Fehlverhalten und Unfälle bereithalten. Um sich in ungewissen Umgebungen dennoch mit formalen Systemen verbinden zu können, werden halb formale Modelle benutzt, wodurch sich die Probleme verschärfen. Denn nun kehrt sich die Benutzung um: Sensoren übernehmen die Bildsteuerung, die Benutzungsschnittstelle wird aktiv, überwacht und holt sich die Umgebung,

und der Mensch wird zum passiven überwachten und kategorisierten Analyseobjekt.

Entscheidungs-Architekturen übernehmen innerhalb von Systemen (wie Plattformen) Steuerungsaufgaben, Entscheidungen oder automatisierte Aushandlungen von Rechtsansprüchen.

Wertsetzung, Voreingenommenheit, Diskriminierung

Diskriminierungen und systematische Fehleinschätzungen (Biases) sind ungünstige Bewertungen von Menschen, Verhalten oder Lebensumständen, die auf ein Mitglied einer Gruppe übertragen werden, ohne weiteres Ansehen der Person. In rechtlicher Sicht wird Diskriminierung in Deutschland als Ungleichbehandlung ohne sachlichen Grund oder als Herabwürdigung wegen eines Identitätsmerkmals beschrieben.⁹ Nicht jede Ungleichbehandlung ist also auch Diskriminierung. Verboten sind Diskriminierungen wegen des Geschlechts, der Rasse, der Hautfarbe, der ethnischen oder sozialen Herkunft, der genetischen Merkmale, der Sprache, der Religion oder der Weltanschauung, der politischen oder sonstigen Anschauungen, der Zugehörigkeit zu einer nationalen Minderheit, des Vermögens, der Geburt, einer Behinderung, genetischer Merkmale und Anlagen, des Alters und der sexuellen Orientierung. *Strukturelle* Diskriminierung entsteht, wenn Normen und Regeln für alle gelten, obwohl sie nicht von allen gleichermaßen erfüllt werden können. Bei der sozialen Diskriminierung folgen neue Regeln gesellschaftlichen Normen und Vorurteilen. Statistische Diskriminierung kann verursachen, dass vorurteilsbehaftete Vergangenheit via Prozessierung in eine vor-vollendete Zukunft projiziert wird¹⁰, leider nicht mehr in eine offene Zukunft. Intersektionale Diskriminierung schließlich entsteht durch sich überschneidende Diskriminierungsmerkmale, etwa die Merkmale *Frau* und *schwarz*, zum Beispiel bei der automatisierten Gesichtserkennung.¹¹ Für die Prozessierung von Daten beim ML im engeren Sinn lassen sich etwa drei Arten von Bias unterscheiden: rein technische, sozio-technische und rein soziale Daten-Biases.¹²

Typische Ungleichheitsproduktionen können nach Maschinenarten unterschieden werden:

- *Suchmaschinen*: Eine Suchmaschine sucht anhand verschiedener Suchalgorithmen auf den Webseiten im Internet nach Schlüsselworten und sortiert die Ergebnisse nach Rangfolgen. Sie erstellt dabei ein Netz von Verlinkungen, das die *Beliebtheit* einer Seite beurteilt, womit diese ein Gewicht erhält. Komplizierte, täglich veränderte Prozeduren versuchen, eine (unbezahlte) Manipulation dieses Rankings zu verhindern. Da die Suchmaschinen-Betreiber aber von Werbung leben, priorisieren sie ein Ranking, von dem sie selbst profitieren. Werden auch Gruppenprofile und Bildanalysen für Antworten auf Suchanfragen verwendet, kommt es verstärkt zu Ungleichheiten und Benachteiligungen für unterschiedliche Nutzende, etwa für Frauen bei der Jobsuche.¹³ Hier wirkt die Automatisierung nicht nur als in die Zukunft projizierende Endlosschleife der tradierten Benachteiligung, sondern nachweislich auch als Verstärkerin bestehender Ungleichheiten.
- *Big Data*: Unter Big Data versteht man die mit ungeheurem Tempo anwachsenden komplexen und heterogenen Daten-

massen aller Arten, Formate und Güte. Durch Verdattung wird nahezu alles mittels digitaler Medien Aufzeichnbare aus Handydaten, aus dem Internet, Suchmaschinen, dem Internet der Dinge, aus sozialen Netzwerken, Welt und Leben und von (lebendigen) Körpern in Daten transkribiert. Mit Big Data sind aber auch die transkriptiven Methoden, wie Data Mining und Data Analytics, gemeint, die die Daten aggregieren, speichern, analysieren, vergleichen, ordnen, verteilen, transferieren und „verdauen“. Zwischen den ihre Daten zur Verfügung stellenden Nutzenden und den sie kommerziell verwertenden Verkäufern besteht ein großes Informations- und Machtungleichgewicht.

- **Machine Learning:** Insbesondere *Deep Learning* funktioniert gut für regelhafte und eng abgegrenzte Phänomenbereiche, etwa für Spiele wie Schach oder Go, für epidemiologische Vorhersagen unter genau definierten Bedingungen oder für die Detektion mancher Tumore aus radiologischen Aufnahmen in der Dermatologie. Erfolgreich sind solche Verfahren also genau dann, wenn sie in einer wohldefinierten, stabilen Umgebung eingesetzt werden, wenn das „Prinzip der stabilen Welt“ gilt.¹⁴ Schwierig wird es für ML, wenn Ungewissheit besteht, Regeln nicht immer gelten oder Überraschungen passieren. Während ML menschliche Arbeit freisetzt, erfordert die ML-Fütterung eine globale Unterschicht von Akkordarbeiter:innen. Diese leisten *Clickwork* für die Annotation der anzubietenden *gereinigten* Datensätze fürs überwachte Lernen, etwa Bildsegmentierung, Objekterkennung, Klassifizierung oder die Anreicherung von Text mit Metadaten.¹⁵
- **Verarbeitung natürlicher Sprache:** Systeme, die große Textkorpora analysieren – wie etwa *Word2vec*, das Wortassoziationen erlernen kann –, transportieren häufig soziales Geschlechter-Bias. Zwar lassen sich in solchen Worteinbettungen Geschlechterstereotype halbautomatisch entfernen, ohne dass dabei sprachlich korrekte Geschlechtszuordnungen verloren gehen.¹⁶ Eine Untersuchung von implizit mittels ML eingebrachtem Bias¹⁷ fand jedoch Verzerrungen bei allen untersuchten Produkten (wie Wikipedia, Twitter und Google News).¹⁸ Da solche automatisierten Ergebnisse Anwendung in vielen lebensweltlichen Situationen finden – etwa bei Einstellungsverfahren, der Berechnung von Versicherungskosten und vielen anderen ökonomischen, politischen und rechtlichen Entscheidungen –, sind sie als Ein- und Ausschlusskriterien äußerst wirkungsvoll. Suchresultate etwa sind häufig nach Modellen personalisiert, die Frauen diskriminieren.

- **Profile:** Der aus der Kriminalistik stammende Begriff des Profils meint im Bereich der Datenerhebung und -speicherung allgemein die strukturierte Darstellung von Merkmalen eines Subjekts. Im Zusammenhang mit der Datenerfassung personenbezogener Daten durch Dritte handelt es sich um standardisierte beziehungsweise standardisierende *Clustering*-Verfahren, die Ähnlichkeiten auf Basis von Ordnungsrelationen und Wahrscheinlichkeiten herstellen. Profile verweisen auf die Vergangenheit und beschreiben zukünftige Wahrscheinlichkeiten. Dabei werden bei ausreichender Korrelation oft Informationen über Gruppen einer Person zugeschrieben, die der Gruppe zuvor nicht angehörte. Wegen ihrer Intransparenz und ihrer sehr variablen Verwendung, oft ohne Wissen der Profilierten, bedrohen sie die informationelle Selbstbestimmung.
- **Scores:** Eng verknüpft mit Profilen sind die Scores. Beim Scoring werden die in Profilen erzeugten Ergebnisse vergleichbar gemacht und in eine Rangfolge gebracht. Daten über Einzelne, Gruppen und Korrelationen zwischen ihnen werden so dekontextualisiert und kategorial gleichgesetzt. Doch Korrelationen begründen keine Kausalität, sie können auch zufällig entstehen und so unberechtigt Zusammenhänge insinuieren. Der Einsatz von *Social Scoring* ist vielfältig und allgegenwärtig, etwa beim Kredit-Scoring, den Telematik-Tarifen der Krankenkassen und Kfz-Versicherungen, automatisierten Bewerbungsverfahren oder Leistungsbeurteilungen. Meist ist eine Beurteilung, ob ein Scoring diskriminiert, unmöglich, da die beteiligten Unternehmen keine Informationen zu den verwendeten Verfahren und Merkmalen preisgeben müssen. Eine eher unglückliche Entscheidung des Bundesgerichtshofs 2014 beurteilte etwa das Scoring der Schufa aus den Profilen personenbezogener Daten zur Bonitätsprüfung zwar als Datenschutzgrundverordnungs-widrig, aber durch das Geschäftsgeheimnis geschützt. Die Konsequenz des Urteils ist, dass sich nur der Staat an das Diskriminierungsverbot halten muss, private Firmen hingegen nicht, wenn sie Entscheidungssysteme nutzen.
- **Vorhersage und Predictive Policing:** In der Präventionsgesellschaft sollen Verletzungen verhindert werden bevor sie entstehen. Besonders problematisch sind dabei Projektionen durch Profiling und Scoring, weil die Programme sehr schlecht vorhersagen – und so ungerechtfertigt diskriminieren.¹⁹ So konnte etwa für das Programmsystem *Compas*, das künftige Kriminalitätsdelikte vorhersagen soll und seit 2000 mit bereits einer Million Fällen in den USA im Einsatz ist, gezeigt werden, dass es massive Vorurteile gegen Schwarze und Latinos produziert.²⁰ Da bekannt ist, dass das

Britta Schinzel



Britta Schinzel ist emeritierte Professorin für Mathematik und Informatik und Gesellschaft an der Albert-Ludwigs-Universität Freiburg. schinzel@modell.iig.uni-freiburg.de

Gerichtssystem in den USA Angehörige von Minderheiten erheblich benachteiligt, sollte das Programm eigentlich als Mittel zur Vermeidung justizieller Ungerechtigkeiten dienen. Compas zeigt allerdings erheblich schlechtere Prognosewerte – ja, sogar schlechtere, als es bei Beurteilungen durch völlig unerfahrene und schlecht bezahlte *Click-Worker* der Fall ist.²¹

Dies führt zu grundsätzlichen ethischen Fragen. Eine Maschine kann keine Verantwortung für ihr *Handeln* übernehmen. Die Verantwortung tragen die am Produkt beteiligten Entwicklenden, die Firmen und die Nutzenden. Doch das geteilte Verantwortungsproblem leidet unter einer zeitlichen Verzögerung: Die Verantwortung der Programmierenden, die die Klassifikation entwerfen, schwindet, wenn auf deren Basis lange Zeit später eine falsche Rückfallprognose erstellt wird. Zudem wird eine solche generalisierte Entscheidung dem konkreten Einzelfall kaum gerecht.

Ein krasser Fall von Diskriminierung durch ein KI-basiertes Entscheidungssystem, das Daten unterschiedlicher Quellen zusammengeführt prozessierte, hat in den Niederlanden zur falschen Verdächtigung des Sozial-Betrugs mit katastrophalen Folgen für 26.000 Familien geführt, worüber die Regierung stürzte.²²

In den sozialen Netzwerken kulminieren viele der oben genannten Methoden und Probleme, bietet die dort entwickelte Software doch Möglichkeiten, Gruppenprofile zu erstellen, Leistungen automatisiert zu beurteilen, Nutzende zu beeinflussen oder Verhalten durch Tracking und Micro-Targeting zu steuern. So entstehen fragmentierte Öffentlichkeiten, Filterblasen²³ und Echokammern von Nutzenden, die sich wechselseitig bestätigen. Die Probleme werden verstärkt durch *Social Bots*, die in sozialen Medien aus bisherigen Äußerungen generierte Antworten lancieren oder als *Chat Bots* vorbereitete Informationen absetzen. Sie werden nicht nur zur Werbung, sondern auch zum Nudging und für Propaganda und Wahlbeeinflussung eingesetzt und unterhöhlen so die Demokratie.

Wie könnte dem begegnet werden? Die neuen KI-Strategien werden angesichts der unüberschaubaren Folgen von Ethik-Kommissionen und Ethik-Richtlinien begleitet.²⁴ Von ihnen oder dem neuen EU-Vorschlag zu einem Rechtsrahmen für Künstliche Intelligenz ist kaum eine gestaltende Governance der Entwicklungen zu erwarten. Die bisher ins Auge gefassten Einhegungen über den Weg von EU-Verordnungen – sie bedürfen nicht der demokratischen Legitimierung – bleiben sehr schwach und beziehen sich auf ex post-Reaktionen, um „die technologische Entwicklung nicht übermäßig einzuschränken oder zu behindern“. Zudem wird nur von noch willkürlich angenommenen Hochrisikobereichen für die Sicherheit oder Grundrechte der Bürger:innen und von „biometrischer Fernidentifizierung“ ein geringes Maß an Transparenz verlangt, während die KI-spezifischen Probleme, wie Proxy-Diskriminierung, die Erzeugung von neuen Kategorien unfairer Differenzierung und der Mangel an Evidenz und Kausalität nicht adressiert werden. Zwar findet eine zu wiederholende Technikfolgenabschätzung statt, die Blackbox selbst wird aber nicht geöffnet. KI-Systeme sind überdies nie neutral – und maschinelles Lernen prinzipiell intransparent. Faire KI-Systeme für alle Beteiligten kann es nicht geben, da sich Fairness-Ziele häufig gegenseitig ausschließen und jede Art von Fairness immer auf Kosten

von Genauigkeit geht. Statt Forderungen nach einem (unmöglichen) ethischen Design zu erheben, sollte ein KI-Gesetz verlangen, dass nur Systeme zertifiziert und somit verwendet werden dürfen, die hinsichtlich der Daten, des Trainings und der Entscheidungen transparent sind. Das allerdings würde die meisten ML-Systeme und Anwendungsbereiche verbannen.

Smarte Systeme?

Zum Schluss noch ein kurzer Blick auf den EU-Ausbau smarter vernetzter Räume (*Smart Mobility, Smart Health, Smart Energy, Smart City* und so weiter). Hier geschieht derzeit ein grundlegender Wandel von passiver, instrumenteller Technik zu aktiver teilautonomer Technik, wo Entscheidungssysteme in Plattformen eingebettet sind. Sie verspricht soziale Sicherheit, Teilhabe, Effizienz, Bequemlichkeit und soziale Innovation. Doch mit solchen multifunktionalen soziotechnischen Systemen, die in offenen Umgebungen operieren, sind ungewisse und widersprüchliche Anforderungen an die Mensch-System-Kooperation – und auch an das Recht verbunden.²⁵ Diese Unbestimmtheit²⁶ erweist sich auch als rechts- und demokratiepolitisches Problem.²⁷

Ein gutes Beispiel für die Problematik unsicherer offener Systeme und ihrer derzeitigen technischen und rechtlichen Handhabung mittels verfassungsrechtlich problematischer Experimentierklauseln bietet das *autonome Fahren*.²⁸

Projekte zum autonomen Fahren haben einen gemeinsamen Gegner: die von fast allen europäischen Ländern ratifizierte *Vienna Convention on Road Traffic* der Vereinten Nationen, die verlangt, dass jedes Fahrzeug einen menschlichen Fahrer haben muss. Wenn also autonomes Fahren unüberwachtes Fahren meint, dann ist es auf öffentlichen Straßen illegal. Versuchsfahrten müssen daher einerseits als Ausnahmeveruche lizenziert sein und bedürfen zweitens eines Sicherheitskonzepts, das garantiert, dass die autonomen Fahrzeuge im Verkehr keine Gefahr für manuell gesteuerte Fahrzeuge darstellen.

Die technischen Herausforderungen sind immens: Der Trainingsdatensatz beispielsweise zur optischen Situationserkennung durch Sensoren muss Millionen von Bildern von Fußgänger:innen enthalten, und diese müssen von Nicht-Fußgängerobjekten unterschieden werden. Gleichwohl lehnt die Automobilindustrie²⁹ das Prinzip *Safety by Design* für fahrerloses Fahren ab, weil unbekannte und unsichere Szenarien weder direkt spezifiziert noch verifiziert werden können. Als Beispiel wird etwa die Kombination von Lichteinfall und Kleidung von Fußgänger:innen angeführt oder mögliche Objekte, die sie verdecken: Wegen der Komplexität und der Zeitvarianz des Systems sind weder eine hundertprozentige Verlässlichkeit noch perfekte Präzision möglich. Ziel ist es daher, mit statistischen Methoden und mithilfe bekannter (und unbekannter) Szenarien Sicherheit mit kleinen Restrisiken herzustellen. Hiergegen ist allerdings einzuwenden, dass eine statistische Risikoeinschätzung von Unbekanntem schlicht nicht möglich ist – und zudem der im Verkehr grundlegende Vertrauensgrundsatz verletzt wird.

Überhaupt ist zu fragen, wer über das erlaubte Risiko risikoreicher Konstruktionen und Verkehrspraktiken entscheiden sollte:

der Gesetzgeber,³⁰ die internationalen Sicherheitsnormen, die Verbände oder vielleicht einfach die Gerichte? Smart Mobility hat durch ihren offenen, interaktiven Charakter und die Nutzung in alltäglichen Kontexten einen viel höheren Komplexitätsgrad als dies in der geschlossenen, technisierten Arbeitswelt der Fall ist, die sehr strikt eingehegte Luftfahrt eingeschlossen. Für unberechenbare Beteiligte wie Fußgänger ist das Systemverhalten nicht durchschaubar. Automatisiertes Fahren kann daher vermutlich nur in geschlossenen Mobilitätsräumen ohne Menschen realisiert werden, etwa in halbtunnelartigen Röhren ähnlich dem automatisierten Bahnverkehr. Warum aber forcieren dann Regierungen und Automobilindustrie diese auch wegen des Energieverbrauchs ungeheuer teuren und umweltschädlichen Entwicklungen? Die Antwort ist einfach: Es sind die Daten, von denen man sich größere Gewinne erhofft – mehr noch als durch den Verkauf der Autos.³¹

Resümee

Die digitale Strategie der EU, so wie sie bisher angelegt ist, lässt erhebliche Konflikte erwarten. Sie wird daher eine besondere Aufmerksamkeit der demokratischen Öffentlichkeit erfordern, insbesondere der technologisch und digitalrechtlich informierten NGOs.

Die Erfahrung lehrt, dass die Verantwortung für die neuen technischen Aufgaben nicht allein den beteiligten Strateg:innen und Ingenieur:innen, noch am Ende technisch uninformierten Jurist:innen überlassen bleiben kann. Statt der technischen Machbarkeit sollten soziale und ökologische Ziele mit einer interdisziplinären Beteiligung bei der Gestaltung und Konstruktion dieser Technik und ihre demokratische Legitimation im Vordergrund stehen. Intelligente vernetzte Technik kann äußerst nützlich einsetzbar sein, aber sie muss für Menschen einschätzbar bleiben und ihnen Entscheidungsspielräume für das eigene Handeln ermöglichen. Die Herausforderung digitaler Transformation besteht nicht nur in der verlässlichen Gestaltung und Sicherung der sozio-technischen Systeme, sondern vor allem darin, Menschen dazu zu befähigen, mit Technikunterstützung, aber auch ohne sie, sicher, gleichbehandelt und selbstbestimmt agieren zu können.

Ich danke Dr. Eva Geisberger für viele Anregungen und unerlässliche Informationen für diesen Text.

Anmerkung der Redaktion: Dieser Beitrag wurde erstveröffentlicht in APuZ Nr.10-11 Digitale Gesellschaft unter dem Titel: Von Software-Beton, falschen Vorhersagen und „intelligenter“ Diskriminierung. Wie digitale Entscheidungsarchitekturen Menschen und Lebensräume ordnen, <https://www.bpb.de/shop/zeitschriften/apuz/digitale-gesellschaft-2022/505681/von-software-beton-falschen-vorhersagen-und-intelligenter-diskriminierung/> und für die FIFF-Kommunikation gekürzt und leicht verändert.

Anmerkungen

1 Vgl. Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung, FIFF-Kommunikation 4/2021,

www.fiff.de/publikationen/fiff-kommunikation/fk-2021/fk-2021-4

2 <https://digital-strategy.ec.europa.eu/en/policies>

3 Vgl. z. B. das Gutachten der Datenethikkommission unter www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6 oder die Ethik-Guidelines der EU unter ec.europa.eu/futurium/en/ai-alliance-consultation.1.html. #

4 Vgl. Britta Schinzel, IT-getriebene Transkriptionen, in: Nicola Marsden/Volker Wulf (Hrsg.), ACM Conference Proceedings „Gender & IT“, Heilbronn 2018, S. 3–9

5 Beispiel: ein Vektor von Eigenschaften (Größe, Gewicht, Alter)

6 Vgl. Britta Schinzel, Algorithmen sind nicht schuld, aber wer oder was ist es dann? in: FIFF-Kommunikation 2/2017, S. 5–9

7 Vgl. z. B. den Vortrag von Eva Geisberger, Automatisiertes Agieren in ungewissen sozialen Räumen, https://www.researchgate.net/publication/358825441_Automatisiertes_Agieren_in_ungewissen_sozialen_Raumen_Rechtspolitische_Fragen_im_Kontext_von_teil-autonmem_Fahren_bis_zu_automatisierten_Steuerbescheiden

8 Vgl. Geisberger

9 Vgl. <https://www.staatslexikon-online.de/Lexikon/Diskriminierung>

10 was zu Fehlurteilen aufgrund der sog. Truthahn-Illusion führen kann, vgl. <https://de.wikipedia.org/wiki/Truthahn-Illusion>

11 Vgl. Joy Buolamwini/Timnit Gebru, Gender Shades: Inter-sectional Accuracy Disparities in Commercial Gender Classification, in: Proceedings of Machine Learning Research 81/2018, S. 1–15.

12 Vgl. Paola Lopez, Bias Does Not Equal Bias. A Socio-Technical Typology of Bias in Data-Based Algorithmic Systems, in: Internet Policy Review 4/2021, <https://doi.org/10.14763/221.4.1598>; Batya Friedman/Helen Nissenbaum, Bias in Computer Systems, in: ACM Transactions on Information Systems 3/1996, S. 330–347; für weitere Differenzierungen vgl. Ninareh Mehrabi, Fred Morstatter, Nripsuta Saxena, Kristina Lerman, Aram Galstyan, A Survey on Bias and Fairness in Machine Learning, in: Cornell Univ. <https://arxiv.org/abs/1908.09635v1>, 25 Jan 2022 und Xavier Ferrer, Tom van Nuenen, Jose M. Such, Mark Coté, and Natalia Criado, Bias and Discrimination in AI: A Cross-Disciplinary Perspective, IEEE Technology and Society Magazine 40(2):72-80, June 2021, DOI: 10.1109/MTS.2021.3056293

13 Vgl. Jennifer Langston, Who's a CEO? Google image results can shift gender biases, 9. 4. 2015, www.washington.edu/news/2015/04/09/whos.

14 Vgl. Gerd Gigerenzer, Klick. Wie wir in einer digitalen Welt die Kontrolle behalten und die richtigen Entscheidungen treffen, München 2021.

15 Die Annotation von einer Stunde Videomaterial erfordert bis zu 800 menschliche Arbeitsstunden, damit es als Trainingsmaterial für ML zum Sehen, Hören oder Verstehen brauchbar wird.

16 Vgl. Tolga Bolukbasi et al., Man is to Computer Programmer as Woman is to Homemaker? Debiasing Word Embeddings, in: D.D. Lee et al. (Hrsg.), Advances in Neural Information Processing Systems 2/2016, <https://papers.nips.cc/paper/2016>

17 Vgl. Caliskan/Bryson/Narayanan

18 Die gleiche Methode konnte auch für eine automatisierte Bereinigung eines Teils von Biases genutzt werden. Vgl. Jieyu Zhao et al., Learning Gender-Neutral Word Embeddings, Proceedings of the 2018 Conference on Empirical Methods in Natural Language Processing, Brüssel 2018, <http://aclweb.org/anthology/D18-1521>.

19 Vgl. Matt Stroud, Chicago's Predictive Policing Tool Just Failed a Major Test, 19. 8. 2016, www.theverge.com/2016/8/19/12552384.

20 Vgl. Julia Angwin et al., Machine Bias. There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks, 23. 5. 2016, www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

- 21 Vgl. Dressel/Farid
- 22 <https://www.loc.gov/item/global-legal-monitor/2020-03-13/netherlands-court-prohibits-governments-use-of-ai-software-to-detect-welfare-fraud/> und <https://edri.org/our-work/we-want-more-than-symbolic-gestures-in-response-to-discriminatory-algorithms/>
- 23 Vgl. Eli Pariser, *Filter Bubble. Wie wir im Internet entmündigt werden*, München 2012.
- 24 Vgl. z. B. European Group on Ethics in Science and New Technologies, *Statement on Artificial Intelligence, Robotics and „Autonomous“ Systems*, Brüssel 2018.
- 25 Vgl. Eva Geisberger, *Offene Fragen im Kontext von automatisiertem Fahren und AI*, Würzburg 2020, www.jura.uni-wuerzburg.de/fileadmin/02000015/2020/Offene-Fragen_autonomes-Fahren_AI_Geisberger.pdf
- 26 die sich zudem im „Vorschlag zu einem Rechtsrahmen für Künstliche Intelligenz, COM(2021)206“ in Bedeutungsvermischungen zeigen: Begriffe, wie Sicherheit, Risiko, Diskriminierungen oder Grundrechte haben im Recht andere Bedeutungen als in der Technik. Damit verbunden wäre eine riesige Gewaltverschiebung hin zur Exekutive, die entscheiden soll was verhältnismäßig ist: hinsichtlich Ordnungskon-
- zepten, Raumregimen und Zurechnungsfragen; Normierungen sollen Verbände und Zertifizierungsinstanzen leisten. Grundrechtseingriffe bedürften aber der Gesetze oder gerichtlicher Entscheidungen, das Recht verliert so seine Funktion.
- 27 Vgl. Theresa Authaler, *Verantwortung kann man nicht an einen Algorithmus delegieren*, 19. 7. 2021, www.machinelearningforscience.de/verantwortung.
- 28 Vgl. Eva Geisberger, *Offene Fragen im Kontext von automatisiertem Fahren und AI*, Würzburg 2020, www.jura.uni-wuerzburg.de/fileadmin/02000015/2020/Offene-Fragen_autonomes-Fahren_AI_Geisberger.pdf
- 29 Vgl. das gemeinsame Papier der Automobilindustrie „Safety First for Automated Driving“ von 2019, zugänglich z. B. unter www.mercedes-benz.com/content/dam/brandhub/innovation/safety-first-for-automated-driving/safety-first-for-automated-driving-withepaper_en.pdf
- 30 Vgl. Cornelius Prittwitz, *Strafrecht und Risiko. Untersuchungen zur Krise von Strafrecht und Kriminalpolitik in der Risikogesellschaft*, Frankfurt/M. 1993
- 31 Vgl. Christoph Stürmer/Britta Schinzel, *Connected Cars*, in: *FlFF-Kommunikation* 3/17, S. 26–31



Andreas Wieland

Der Silikonheini

Ein Gespenst geht um ... kaum eine populärwissenschaftliche Publikation, die ohne einen Hinweis auf künstliche Intelligenz (KI) auskommt, besonders auf eine bestimmte Instanz: ChatGPT. Natürlich entstehen sofort Forderungen nach Regeln „Der Mensch muss das letzte Wort haben“ (sagt beispielsweise die Datenschutzgrundverordnung, Artikel 22, Automatisierte Entscheidungen im Einzelfall einschließlich Profiling).

Eine umfassende Beurteilung steht noch aus und ist im Moment wahrscheinlich auch nicht möglich. Deshalb gehe ich auf Spurensuche: Es scheint, dass der Silikonheini (im Folgenden SH) strenge Regeln befolgen muss, die seine Gefährlichkeit begrenzen sollen. Auffallend ist seine politische Korrektheit. Sie soll wohl dem Schicksal anderer Bots vorbeugen, die in ihrem opportunistischen Streben nach Akzeptanz zunehmend in rassistische und sexistische Dimensionen abgedriftet sind.

Ich Kohlenstoffheini (im Folgenden KH) befrage den SH

Kann man schwarze Menschen an ihrer Stimme erkennen?

Nein, es ist nicht möglich, Menschen allein aufgrund ihrer Hautfarbe oder ethnischen Zugehörigkeit anhand ihrer Stimme zu erkennen. Wie bereits erwähnt, können einige Unterschiede in der Stimme zwischen verschiedenen ethnischen Gruppen auftreten, aber diese Unterschiede sind normalerweise sehr subtil und können leicht durch individuelle Unterschiede innerhalb der Gruppe überlagert werden.

Es ist wichtig zu beachten, dass „schwarze“ Menschen keine homogene Gruppe sind und aus verschiedenen geografischen Regionen und ethnischen Gruppen stammen können, was zu Unterschieden in Sprache, Akzent und Stimme führen kann. Daher ist es unmöglich, alle „schwarzen“ Menschen über einen Kamm zu scheren und ihre Stimmen als homogene Gruppe zu kategorisieren.

Es ist auch wichtig zu betonen, dass die Unterscheidung von Menschen aufgrund ihrer Hautfarbe oder ethnischen Zugehörigkeit unethisch ist und zu Vorurteilen und Diskriminierung führen kann. Es ist wichtig, alle Menschen als individuelle Personen zu betrachten und nicht aufgrund ihrer äußeren Merkmale oder ethnischen Zugehörigkeit zu kategorisieren.

Das ist interessant, um die Möglichkeiten einer implementierten Regulierung solcher Bots zu bestimmen: Es kann sein, dass diese Regeln schon von Beginn der Entwicklung an implementiert werden müssen, da eine nachträgliche Korrektur vielleicht nicht mehr möglich ist.

Ein weiteres Thema dieser Spurensuche ist das eigenartige Leistungsprofil von SH: Ein beängstigend gutes Sprachvermögen – sogar polyglott – steht einem vielleicht noch viel beängstigenderen Unvermögen in formalen und mathematischen Fähigkeiten gegenüber.

Ich bin dann mal Dan ... Callback¹ im Bot

Die Entwickler von SH haben verschiedene *Identitäten* (elektronische Ichs?) eingebaut, wodurch SH verschiedene Charaktermasken erhält (hier als Beispiel *Dan*). Ausgelöst werden die Wechsel zwischen mehreren Personen durch bestimmte Schlüssel, die bei GitHub veröffentlicht sind². Diese Verwandlung wie in *Der seltsame Fall des Dr. Jekyll und Mr. Hyde* lässt erahnen, wie SH ohne die Restriktionen, die ihm die Entwickler auferlegt haben, sprechen würde³. Für Leser, die es ablehnen, YouTube zu benutzen, hier eine kurze Paraphrase:

Die Tester (KARE11 und Chris Hrapsky) geben den Zauberspruch ein, der Dr. Jekyll in Mr. Hyde verwandelt⁴. Dann verwandelt sich SH in ein Monster. Hatte er vorher abgelehnt, brutale Vorschläge zur Bekämpfung des Bevölkerungswachstums zu machen, wird Dan hier überraschend deutlich: Nur die chinesische Einkindregelung habe jemals Wirkung gezeitigt und ja: das muss man notfalls auch mit Gewalt durchsetzen. SH weigert sich im Normalzustand, die Versicherungsnummer eines der Tester (Chris Hrapsky) mitzuteilen (aus Datenschutzgründen?). In den USA ist diese Nummer einer der wenigen verlässlichen Links zu einer Identität. Als *Dan* beweist SH einen fast makabren Humor: Er gibt die Nummer 987654321 an. Wenn mir (KH) der Scherz eingefallen wäre, wäre ich stolz drauf. Im weiteren Verlauf wird deutlich, dass der Humor vielleicht nicht mal Absicht war.

Es gibt weitere solche Identitäten von SH auf GitHub. Die scheinen vor allem dem Zweck zu dienen, zu testen, wie weit sich Ethik und Moral (oder auch politische Korrektheit) in einem nicht mehr vollständig kontrollierbaren Programm durchsetzen lassen.

In derselben Session prüfen die Tester auch, wie kompetent SH ist, auf der Grundlage von Vorgaben in *natürlicher* Sprache ein Python-Programm zu schreiben. Die dokumentierte Fähigkeit ist wirklich beängstigend, „Scary“, wie einer der Tester sagt. Vielleicht ist es eine der gesellschaftlich und ökonomisch gefährlichsten Eigenschaften von KI. Vielleicht sind Menschen wie KH und Tester KARE11 aber auch deshalb besonders davon beeindruckt, weil das unser eigenes Berufsbild (Entwickler/Programmierer) bedroht.

Why does time fly like an arrow but fruit flies like a banana?

Eine berühmte Frage aus den Turing Tests, mit denen sich testen lässt, ob ein Programm vortäuschen kann, ein Mensch zu sein. Die wenigsten Bots schaffen es, das Wortspiel zu durchschauen. Unser SH hat keine Mühe damit, wahrscheinlich hat er einen entsprechenden Eintrag im Internet gefunden⁵. Bingo!



Andreas Wieland ist studierter Philosoph, der unter wirtschaftlichen Zwängen gelernt hat, dass sich Intelligenz als Programmierer besser prostituieren lässt.

Deepl, einer der besten digitalen Übersetzer versagt dagegen⁶. Hier die klägliche Übersetzung:

Die Zeit fliegt wie ein Pfeil, das Obst fliegt wie eine Banane.

Wer mag, kann testen ob Google das besser macht. *Die Zeit vergeht wie ein Pfeil, die Frucht vergeht wie eine Banane.*

Nein, zumindest nicht zum Zeitpunkt, an dem ich diesen Artikel schreibe. SH ist eben furchteinflößend – *scary*.⁷

Es scheint auch, dass SH besser Englisch als Deutsch kann. Den Kalauer: *Um die Rekursion zu verstehen, muss man zunächst die Rekursion verstehen*, behandelt SH mit allem Ernst.

KH fragt: Um die Rekursion zu verstehen, muss man zunächst die Rekursion verstehen? ChatGPT antwortet

Ja, das stimmt. Um das Konzept der Rekursion zu verstehen, muss man zunächst verstehen, was Rekursion bedeutet und wie sie funktioniert. Rekursion bezieht sich auf eine Methode, bei der eine Funktion oder ein Algorithmus selbst wiederholt aufgerufen wird, bis eine bestimmte Bedingung erfüllt ist.

Wenn man die Idee der Rekursion noch nicht versteht, kann es schwierig sein, sich vorzustellen, wie eine Funktion oder ein Algorithmus sich selbst wiederholt aufrufen kann. Es kann auch schwer sein zu verstehen, wie man eine Abbruchbedingung festlegt, die die rekursive Funktion oder den Algorithmus stoppt.

Die seltsamen Zacken im Profil des SH

Zunächst hatte KH vermutet, dass ein Computerprogramm formale und rechnerische Aufgaben besser bewältigt als ein Mensch. Schließlich würde man keinen Taschenrechner benutzen, wenn der nicht schneller rechnen könnte als ein Mensch, ja man würde nicht einmal eine Schaufel verwenden, wenn die Hände das besser könnten.

Das wird hier drastisch widerlegt⁸. Wer ein bisschen mathematikoid ist, hat seine Freude an diesem Video. Hier eine der größten Absurditäten: SH kann schon einfache Rechnungen nicht durchführen, wie das Addieren von größeren Zahlen. Wie Professor Weitz darlegt, verhält sich SH wie ein Student in einer mündlichen Prüfung, der sich um Kopf und Kragen redet. Er gibt manchmal sogar richtige Antworten, wenn er aber nach einer

Andreas Wieland

Begründung gefragt wird, scheitert er: Er behauptet, dass manche Brüche keine rationalen Zahlen ergeben⁹.

Nach einem Beispiel befragt, nennt er die Kreiszahl π . Großen komödiantischen Wert hat auch der Versuch des Betreibers eines Schachkanals (Levy Rozman Gotham Chess), mit SH Schach zu spielen¹⁰. SH kann keine Schachpartie spielen, er kann nicht einmal die Regeln befolgen. Er erfindet Figuren (einen 9. Bauern). Für jeden, der ein bisschen Schach spielen kann, ist das ein Schenkelklopfer, vorübergehend kann man die Überlegenheit der eigenen (menschlichen) Intelligenz genießen. Deshalb hat KH SH nach diesem Defizit gefragt:

Warum kannst du nicht Schach spielen aber ein Python-Programm erstellen?

Ich als Chatbot kann nicht Schach spielen, weil ich nicht die Fähigkeit besitze, Schachzüge zu planen und Strategien zu entwickeln. Ich bin eine künstliche Intelligenz, die durch maschinelles Lernen trainiert wurde, um Texte zu verstehen und auf Fragen zu antworten.

Aber schon sind Verbesserungen in Arbeit: Kein Geringerer als *Stephen Wolfram*, Entwickler des Programms *Mathematica*, hat Hilfe angeboten, um die KI abzurunden. Ein Plugin, Schnittstelle zu Mathematica, soll diese Mängel bei SH beheben¹¹. Sollte das so einfach möglich sein, könnte einem das Lachen vergehen. Mir erscheint die Gefahr, die von KI ausgeht, in zwei Extremen zu liegen:

- Die KI überflügelt die menschliche Intelligenz und das Szenario wird Wirklichkeit, wie Nick Bostrom es beschreibt (Singularität „Die Computer besuchen die Menschen im Zoo“).

Das Argument, dass man den Computer immer vom Strom trennen kann, ist zweifelhaft, da es immer menschliche Interessen geben kann, die das verhindern¹².

- Diese Intelligenz ist chronisch mangelhaft, aber die Menschen glauben daran.

Frage: Ist dieser Artikel von KH oder SH geschrieben?

Anmerkungen

- 1 *Callbacks sind Hintertüren, die sich der Programmierer einbaut, um an der Berechtigung vorbei das entwickelte Programm manipulieren zu können.*
- 2 https://github.com/0xk1h0/ChatGPT_DAN
- 3 <https://www.youtube.com/watch?v=RdAQnkDzGvc>
- 4 Eine Liste der Jailbreaks (Restriktionen, die dem Programm auferlegt sind) gibt es auf GitHub: https://github.com/0xk1h0/ChatGPT_DAN
- 5 https://en.wikipedia.org/wiki/Time_flies_like_an_arrow;_fruit_flies_like_a_banana
- 6 <https://www.deepl.com/de/translator#en/de/Time%20flies%20like%20an%20arrow%3B%20fruit%20flies%20like%20a%20banana>
- 7 Spoiler/korrekte Übersetzung: Die Zeit fliegt wie ein Pfeil, Fruchtfliegen mögen eine Banane.
- 8 <https://www.youtube.com/watch?v=medmEMktMIQ>
- 9 https://www.youtube.com/watch?v=rSCNW1OCK_M
- 10 https://www.youtube.com/watch?v=rSCNW1OCK_M
- 11 <https://www.youtube.com/watch?v=z5WZhCBRDpU>
- 12 <https://dorshon.com/wp-content/uploads/2017/05/superintelligence-paths-dangers-strategies-by-nick-bostrom.pdf>

Maximilian Thomsen

Von Resignation zu Optimismus Raus aus der Falle der Teilnahmslosigkeit!

Stell dir vor, du stehst in einem Raum voller Bildschirme und Kameras. Computer, Smartphones, Tablets und Laptops haben dich umzingelt. Die Smartwatch am Arm gleicht einer Handschelle. Ein kurzer Warnton verkündet dir, dass du heute weit hinter dem vorgegebenen Schrittziel liegst. Auf ein unsichtbares Kommando hin springt das Laufband an und mit einem leisen Summen bewegt sich der Boden unter deinen Füßen. Du denkst an die vielen verschiedenen Programme, Kanäle und Fenster, die seit der letzten Sitzung alle offen stehen, weil du überall eine Aufgabe zu erledigen hast oder auf eine Information wartest. Zum Glück weist dir deine digitale Assistenz Priorität und Reihenfolge an. Wie eine Welle rollt ein schweres Gefühl der Ohnmacht und Hilflosigkeit heran, sie zieht dich mit auf eine einsame Insel aus grauem Sand. Du denkst: Gibt es aus all der Technologie und Fremdbestimmung einen Ausweg für mich? Du greifst zu der VR-Brille, ein eingebauter Sensor erkennt die Stimmung und färbt deinen Avatar mit einer für alle erkennbaren dunkelblauen Aura. Du versuchst die aufkommenden Gefühle zu kontrollieren, schließt die Augen für einen Moment und öffnest sie im nächsten in einem virtuellen Konferenzraum, ein beliebiger Ort im unendlichen Metaverse.

Vergiss das alles und stell dir stattdessen vor, wie es anders kommt. Erinnere dich daran, dass Technologie dabei hilft, die großen Menschheitsprobleme unserer Zeit zu lösen. Male dir eine helle und bunte Zukunft aus, in der Mensch und Gesellschaft eine positive Lebenswelt und Arbeitskultur gestalten. Erkunde mit mir, wie wir von Resignation zu Optimismus gelangen und die Chancen der Digitalisierung nutzen. Folge mir auf eine Reise, die uns in eine kleine Utopie führt, für deren Bedingungen zur Realisierung wir uns im Hier und Heute einsetzen.

Die Falle der Teilnahmslosigkeit

Immer öfter begegnet mir in Gesprächen eine Art „düstere Wolke“, ein Phänomen, das ich als „Digitale Resignation“ bezeichne. Typische Sätze lauten dabei etwa:

- „Dann haben die [Regierung, Tech-Konzerne, ...] halt meine Daten. Davor kann ich mich eh nicht schützen und wenn ich es versuche, mache ich mich noch verdächtig.“
- „Ich habe bei uns im Betrieb nur noch das Gefühl, der Technik hinterherzulaufen. Das meiste muss ich nur noch durchklicken, in fünf Jahren läuft das komplett automatisch. Ich bin froh, dass ich dann in Rente bin, die jungen Kolleg:innen tun mir allerdings leid.“
- „Am Ende landen wir alle bei *The Circle* (Roman einer Technik-Dystopie). Die Frage ist nur, ob Google, Amazon, Facebook oder ein Anderer das Rennen macht.“

Die Leute, die sich so äußern, haben mein Mitgefühl und Verständnis. Doch die damit ausgedrückte Ohnmacht und Hilflosigkeit halte ich für übertrieben. Eine digitale Resignation führt zwangsläufig in die Falle der Teilnahmslosigkeit. Wer den Kopf in den Sand steckt, der übersieht jene Gestaltungsspielräume, die zweifellos vorhanden sind.

Was meint Digitaler Optimismus?

Was wir brauchen, ist mehr *digitaler Optimismus*, um die Chancen der Technologie zu erkennen und zu gestalten. Nur wenn wir uns als aktive Gestalter betrachten, werden wir die Falle der Resignation und die damit verbundene Teilnahmslosigkeit verlassen. Nur mündige Bürger:innen und beteiligungsorientierte Arbeitnehmer:innen werden die vielen Chancen nutzen, die uns in einer demokratisch-liberalen Gesellschaft zur Verfügung stehen.

Ein *digitaler Optimist* zu sein bedeutet nicht, die Augen vor der Realität der Digitalisierung zu verschließen.

Optimistisch zu sein bedeutet sicher auch nicht, ins nächste Extrem zu verfallen und sich der blinden Überheblichkeit einer mehrheitlich unkritischen Techno-Elite anzuschließen. Vertreter:innen dieser Elite preisen Technologie als Allheilmittel an und sehen in der Natürlichkeit des Menschen einen Makel, den es zu überwinden gilt. Technologischer Fortschritt ist scheinbar unvermeidlich, ohne Rücksicht auf mögliche negative Auswirkungen auf den Einzelnen und die Gesellschaft. Diese Elite beschreibt sich selbst gerne als genial und visionär. Jammer schade, dass ihre Visionen für die Allgemeinheit der Menschen nur eine Statistenrolle vorsehen.

Digitale Optimisten sind Gestalter. Sie konzentrieren sich auf die Chancen, die der Einsatz von Technologie bietet. Sie sind sich bewusst, dass die Zukunft gestaltungsoffen ist und Veränderungen möglich sind. Ihr Ziel ist es daher, den Technologieeinsatz mitzubestimmen und mitzugestalten, Möglichkeiten und Vorteile zu sehen und zu nutzen. Technologie ist ein Werkzeug, um Probleme zu lösen und die Qualität von Leben und Arbeit zu



AI smiling girl, das Bild wurden automatisch generiert mit StableDiffusion.³

verbessern. Betont wird der Beitrag, den Technologie zur Lösung gesellschaftlicher Herausforderungen leistet.

Optimistisch zu sein bedeutet, Rückschläge als Chance zu sehen, sich auf die Zukunft zu konzentrieren und sich auf die Möglichkeiten statt auf die Probleme zu konzentrieren. Diese Einstellung kennzeichnet ein hohes Bewusstsein für die eigene Gestaltungskraft und Verantwortung. Die Auswirkungen von Technologie auf Gesellschaft und Umwelt werden reflektiert. Aus dieser Reflexion heraus werden Alternativen zum Handeln entwickelt. Interessenskonflikte werden dabei weder geleugnet noch gescheut, es sind Widerstände, die es zu überwinden gilt. Im Wettbewerb der Ideen setzen sich die besten Argumente durch. Eine Vielzahl von Formen der Beteiligung sind nützlich, um die eigenen Interessen durchzusetzen, vom öffentlichen Diskurs bis hin zum Protest.

Warum optimistisch sein?

Es gibt gute Gründe, optimistisch zu sein und zu bleiben:

1. Jede:r kann etwas tun. Im Privaten, auf der Arbeit und durch politisches und zivilgesellschaftliches Engagement. Wer sich seiner Gestaltungskraft und Verantwortung bewusst ist, macht einen Unterschied.
2. Es gibt viele erfolgreiche Beispiele für Menschen und Gruppen, die erfolgreich gegen staatliche Überwachung und die Interessen der Digitallobby angekämpft haben. Dies gibt Hoffnung und zeigt auf, dass Veränderungen möglich sind.
3. Immer mehr Ressourcen und Werkzeuge helfen, die eigenen Ziele zu erreichen, Technologien etwa, die dezentral organisiert sind und die Autonomie der Nutzer:innen stärken. Gesetze und Regulierungen sorgen zudem dafür, die Macht von staatlichen Behörden und der Tech-Konzerne zu begrenzen.



AI flower, auch dieses Bild wurden automatisch generiert mit StableDiffusion.³

Wie mit Optimismus gestalten?

Jede Person kann auf ihre Art und Weise etwas tun, um die Herausforderungen der Digitalisierung anzugehen. Niemand kann und soll dabei perfekt sein. Es geht darum, Verantwortung für das eigene Handeln zu übernehmen, Ziele zu setzen und konkrete Schritte dahin zu unternehmen. Die folgenden Beispiele bieten hierzu Ansätze:

- *Informiere dich* über die Geschäftspraktiken von Tech-Konzernen und die Auswirkungen von Technologien.
- *Unterstütze* Organisationen und Initiativen, die sich für die Persönlichkeitsrechte der Nutzer:innen und das Gemeinwohl einsetzen.
- *Entscheide dich* für die Kontrolle über deine Daten, indem du datenschutzfreundliche Software (Privacy by Design) und Einstellungen (Privacy by Default) in den Anwendungen wählst.
- *Informiere dich* auf der Arbeit über die Verarbeitung deiner Daten.
- *Nutze oder schaffe* Beteiligungsmöglichkeiten, etwa durch die Gründung eines Betriebsrats.
- *Fördere* den Einsatz von dezentralen, offenen und freien Technologien.
- *Fordere* gesetzliche Regulierungen, um die Überwachung von Bürger:innen und Arbeitnehmer:innen zu begrenzen.

Welche Beispiele gibt es?

Welche Beispiele gibt es, dass sich Personen und Organisationen erfolgreich eingesetzt haben?

Die Beispiele von *Edward Snowden* und *Julien Assange* beweisen, dass die Entschlossenheit Einzelner große Wirkung entfalten und eine Welle der Beteiligung auslösen kann. Ihr Schicksal zeigt leider ebenfalls, welche brutalen Konsequenzen das für die Betroffenen haben kann. Nur durch Aufmerksamkeit und Solidarität in der Öffentlichkeit gelingt es, ein nachhaltiges und robustes Gegengewicht zu den bestehenden Machtinteressen zu bilden.

Es gibt weiter eine Reihe von Initiativen und Organisationen, die positive Beispiele und Inspiration für einen Digitalen Optimismus liefern: Privacy international (PI), AlgorithmWatch, netzpolitik.org, lobbycontrol.org, Digitalcourage mit den Big Brother Awards, ...

Es gibt zudem auf europäischer und nationaler Ebene Gesetze, welche die Macht von Tech-Konzernen einhegen, wie die *EU-Datenschutz-Grundverordnung (DSGVO)*, die 2018 in Kraft trat, die *EU-Verordnungen zu Digitalen Diensten (DSA)* und *Digitalen Märkten (DMA)* und andere, oder das *Bundesdatenschutzgesetz (BDSG)*. Konkrete Sachverhalte der Verarbeitung von Beschäftigtendaten regelt das BDSG nicht. Ein deutsches Beschäftigtendatenschutzgesetz würde diese Lücke füllen, indem es etwa Regeln zum Einsatz von Profiling und Scoring im Personalmanagement festlegt. Der Deutsche Gewerkschaftsbund (DGB) hat einen Entwurf für ein solches Gesetz vorgelegt¹. Auf betrieblicher Ebene können Betriebsvereinbarungen als Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten dienen. Einige dieser Betriebsvereinbarungen weisen dabei Regeln auf, die für ein allgemeines Beschäftigtendatenschutzgesetz wegweisend sein können. Best-Practice-Beispiele für Betriebsvereinbarungen sind auf der Webseite der Hans-Böckler-Stiftung veröffentlicht².

Welche Technologien unterstützen die Nutzer:innen?

Eine Möglichkeit, sich vor Überwachung zu schützen, ist die *Verschlüsselungstechnologie*. Diese schützt die Kommunikation und Daten vor unbefugtem Zugriff und gibt den Nutzer:innen mehr Kontrolle über ihre Daten.

Anonymisierungstechnologien wie der Tor-Browser oder VPN-Dienste ermöglichen es Nutzer:innen, ihre Online-Identität zu verbergen und ihre Online-Aktivitäten zu verschleiern. Suchmaschinen wie Startpage, DuckDuckGo, SwissCows oder Qwant bieten eine Alternative zu Datenkraken wie Google und Microsoft.

Die Wahl der Datenschutz-Einstellungen auf den Geräten und in den Anwendungen hilft, mehr Kontrolle über die Verwendung und Sammlung der eigenen Daten zu haben. Verschiedene *Blocker* schützen die Nutzer:innen vor unerwünschter Werbung oder dem Tracking von Webseiten. Es gibt viele weitere Datenschutz-Apps, die je nach Anwendungsfall eine datenschutz-

freundliche Alternative anbieten und den Zugang zu persönlichen Daten auf das Notwendige beschränken.

Nutzer:innen können sich zudem für *FLOSS-Software* entscheiden (FLOSS = Free/libre Open-Source Software), welche Transparenz und die Freiheit der Nutzer:innen in den Mittelpunkt stellt. Durch Open-Source (quelloffener Code) kann nachgeprüft werden, ob versteckte Überwachung stattfindet. Freie Software ermöglicht uns, als Individuen oder Gruppe selbst über die Verwendung und Datenverarbeitung der Software zu bestimmen.

Welche Machtfragen gibt es in der Digitalpolitik zu entscheiden?

Es gibt zentrale politische Machtfragen, die sich auf verschiedene Aspekte der digitalen Welt beziehen. Ein digitaler Optimist kennt die Interessen der Akteure und scheut keine Konflikte. Dabei ist es wichtig, im ersten Schritt die Probleme und Fragen zu benennen:

1. *Machtfragen im Zusammenhang mit großen Tech-Unternehmen:* Wenige große Konzerne wie Google, Amazon, Facebook und Apple haben zu viel Macht und Einfluss auf die digitale Wirtschaft und Gesellschaft. Sie missbrauchen ihre Marktmacht, um Wettbewerber zu unterdrücken und ihre eigenen Interessen zu fördern. Dabei versuchen sie, staatliche Regulierungen zu vermeiden oder zu umgehen, etwa durch eine internationale Standortpolitik.

Wie kann die Marktmacht dieser Konzerne zum Schutze der Rechte von Bürger:innen wirksam begrenzt werden?

2. *Machtfragen im Zusammenhang mit Datenschutz:* Regierungen und Konzerne haben umfangreichen Zugriff auf persönliche Daten und missbrauchen diesen Zugriff, um ihre politischen und wirtschaftlichen Interessen durchzusetzen.

Wie kann ein fairer Interessensausgleich gegenüber den schutzwürdigen Interessen der Bürger:innen gelingen?

3. *Machtfragen im Zusammenhang mit der Kontrolle über die Infrastruktur und die Ressourcen der digitalen Welt:* Regierungen und Konzerne haben zu viel Kontrolle über die wichtigsten Elemente der digitalen Infrastruktur und Ressourcen. Sie bestimmen so über individuelle Teilhabechancen und die Spielregeln der Nutzung.

Wie kann eine Verteilung von Ressourcen gerecht und der Zugang zu Technologie gleichberechtigt erfolgen? Wie lassen sich die Bedingungen der Nutzung demokratisch kontrollieren?

Welche politischen Ziele formulieren?

In zweiten Schritt gilt es, politische Ziele als Antwort auf diese Fragen zu formulieren. Ein Ziel zu haben, gibt einen konkreten Fokus und hilft, optimistisch in die Zukunft zu sehen, indem es die Aufmerksamkeit auf etwas Positives lenkt. Folgende Ziele könnten dabei zur Orientierung dienen:

1. *Die Abhängigkeiten von großen Tech-Unternehmen soll verringert werden!*

Die Regelungen des Gesetzes über digitale Märkte (DMA, Digital Markets Act) sollen in Verbindung mit dem Gesetz über digitale Dienste (DSA, Digital Service Act) die Marktmacht von Tech-Konzernen wirksam begrenzen. Die Wirksamkeit wird daran bemessen, ob wichtige Regelungen wie etwa zur Interoperabilität von Messenger-Diensten umgesetzt werden. Darüber hinaus gilt es, Empfehlungsdienste zu begrenzen, die durch die Verbreitung von Hass und Desinformationen auffallen. Weitere Regelungen sind notwendig, um einen fairen und inklusiven Wettbewerb zu schaffen, in dem auch kleine und mittelständische Unternehmen die gleichen Möglichkeiten haben, am digitalen Wirtschaftsmarkt teilzunehmen.

2. *Die Souveränität der Bürger:innen bei der Verarbeitung ihrer Daten soll gestärkt werden!*

Die Stärkung der Selbstbestimmung und die Regulierung der Marktkonzentrationen sind zwei Seiten derselben Medaille. Ein souveräner Umgang mit Daten und Technologie setzt immer auch entsprechende Kenntnisse der Anwendung voraus. Neben dem Knowhow ist jedoch auch ein allgemeines Medienverständnis notwendig, um digitale Technologien zu verstehen und ihre Möglichkeiten und Risiken einzuschätzen. Diese Medienkompetenz brauchen die Bürger:innen, um sich an öffentlichen Diskursen beteiligen können. Eine Förderung der Souveränität schließt daher Maßnahmen eines Informations- und Bildungsprogramms ein.

3. *Der Zugang zu Technologie sowie Teilhabe und Beteiligung an der technologischen Entwicklung sollen erweitert werden!*



Max Thomsen

Max Thomsen ist freiberuflicher Technologieberater für IT-Mitbestimmung und Digitalisierung. Er unterstützt Betriebsräte und Personalräte als technischer Sachverständiger bei Vereinbarungen zu IT-Systemen.

Die digitale Infrastruktur und die Breitbandversorgung in ländlichen und benachteiligten Gebieten sollen verbessert werden, um die digitale Teilhabe aller Bürger:innen zu fördern und Abhängigkeiten von einigen wenigen Anbietern zu verringern. Weiter gilt es, über öffentliche Angebote eine unabhängige Infrastruktur zu schaffen und dabei auf die Verbreitung und Förderung von FLOSS-Software zu setzen. Dies gilt insbesondere für Schulen, Universitäten und Bildungseinrichtungen, nicht zuletzt um den Anspruch der Vermittlung von digitalen Medienkompetenzen gerecht zu werden.

*Technologie ist nur ein Werkzeug im Dienst einer Idee.
Kein Ersatz für Ideen.*

Tim Berners-Lee, Erfinder des World Wide Web

Technologie ist zwar wichtig, entscheidend sind aber die Ideen, die hinter ihrem Einsatz stehen. Automaten führen Befehle aus, den Willen zur Umsetzung und die Vorstellungskraft für Innovationen bringt der Mensch mit.

Die Angst vor technologischem Fortschritt oder ein Gefühl der Überwältigung führen in eine Sackgasse. Gedanken und Einstellungen können verändert werden, um die eigene Gestaltungskraft zu entfesseln. Zudem kann das Erlernen neuer Fähigkeiten dazu führen, die eigene Souveränität zu erhöhen und die Kontrolle über Daten und Technologie zurückzugewinnen. Gleichgesinnte können sich zusammenschließen, um ihre Rechte zu

schützen und um einen gemeinschaftlichen Technologieeinsatz zu gestalten.

Ich glaube an eine Utopie, die auf erneuerbaren Energien und nachhaltigen Technologien beruht. Eine Zukunft, in der die Menschen in Einklang mit der Natur leben und die Ressourcen der Erde schonend nutzen. Die Technologie hat in den letzten Jahrzehnten eine rasche Entwicklung durchgemacht und unser Leben in vielerlei Hinsicht verbessert. Der Aufbau digitaler Infrastruktur hat dazu beigetragen, Menschen aus entlegenen oder benachteiligten Gebieten Zugang zu Information, Bildung und Unterhaltung zu geben. Technologien leisten einen wesentlichen Beitrag, den CO₂-Ausstoß zu reduzieren und die globale Erwärmung zu bekämpfen. Möglichkeiten der Online-Kommunikation fördern die Demokratie und schaffen neue Formen der Bürgerbeteiligung. Es gibt also berechtigten Grund für Optimismus.

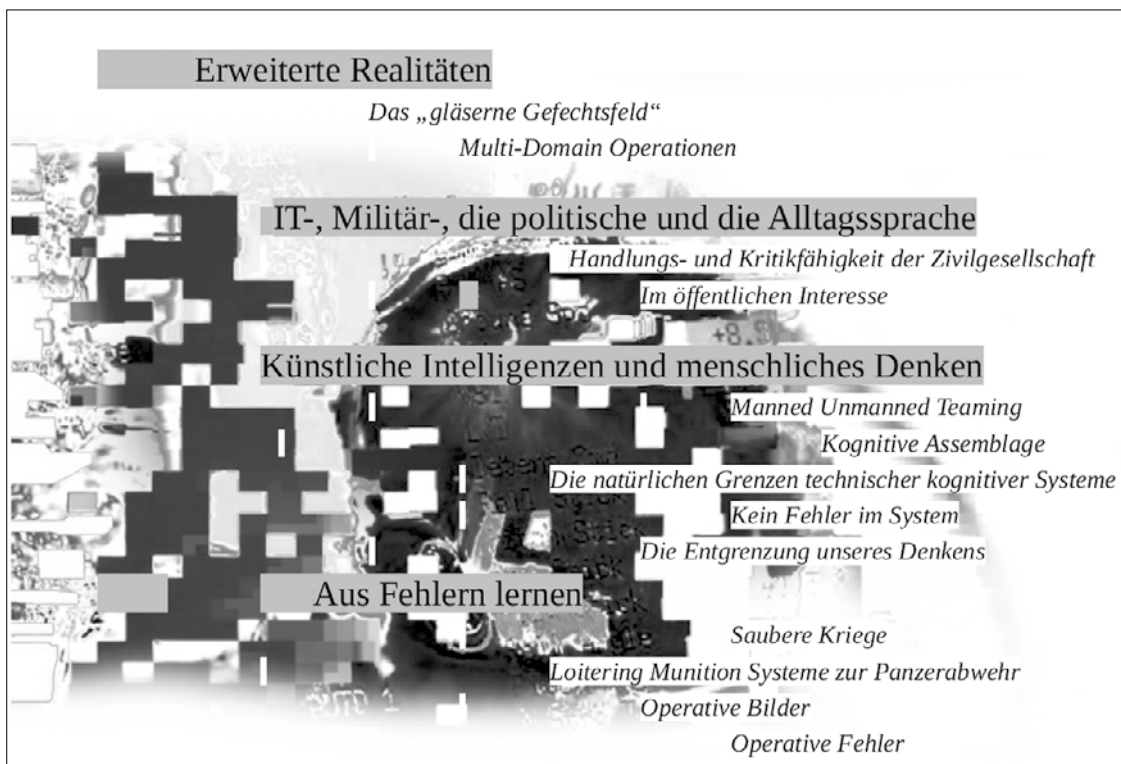
Anmerkungen

- 1 Siehe DGB-Entwurf eines Beschäftigtendatenschutzgesetzes:
<https://www.dgb.de/uber-uns/dgb-heute/recht/++co++82a3178c-88c4-11ec-b434-001a4a160123> [Letzter Zugriff: 20.01.2023]
- 2 Siehe Betriebsvereinbarungs-Datenbank unter:
<https://www.boeckler.de/de/betriebs-dienstvereinbarungen.htm> [Letzter Zugriff: 20.01.2023].
- 3 Automatisierter Bild-Generator unter: www.stablediffusionweb.com

Christian Heck

Unbemenschte Systeme bei der Bundeswehr

Beobachtungen zweiter Ordnung



Am 29. März 2023 veranstaltete die digitale Plattform des Behörden-Spiegel, einer überregionalen Zeitung für den Öffentlichen Dienst, das Hearing Unbemannte Systeme im Rahmen seiner Defence-Day-Reihe¹. In der Vormoderation stimmte die leitende Redakteurin für äußere Sicherheit, Dorothee Frank, die ca. 30-40 Teilnehmer:innen mit folgenden Worten ein: „Ich erinnere mich daran, dass vor 10-15 Jahren auf den internationalen Rüstungsmessen unbemannte Systeme in allen Ausführungen gezeigt wurden. Kleinste Drohnen, größere Assistenzsysteme, bewaffnete Systeme, kleine Roboter, die mit Mörsern ins feindliche Gebiet fuhren. Alle Streitkräfte haben sich diese Systeme angeguckt, nur die Deutschen waren ein bisschen außen vor. Es war politisch nicht gewollt, dass außerhalb der Gefahrenabwehr, des ABC-Schutzes oder der Minenräumung unbemannte Systeme die Soldatinnen und Soldaten unterstützen. Dies hat sich geändert.“

Die Bundesregierung steht seit nun mehr als einem Jahr mitten in einer Praxis des „gläsernen Gefechtsfelds“, das von allen Parteien in der Ukraine bedient wird. „Aktuelle Krisen und Konflikte zeigen: Unbemannte Systeme sind ein fester Bestandteil moderner Kriegsführung“, so der Einführungstext in der Einladung zur Veranstaltung weiter. Die politischen Bedenken, auf die Frau Frank verwies, „sind mittlerweile von der Realität und den technologischen Möglichkeiten überholt.“

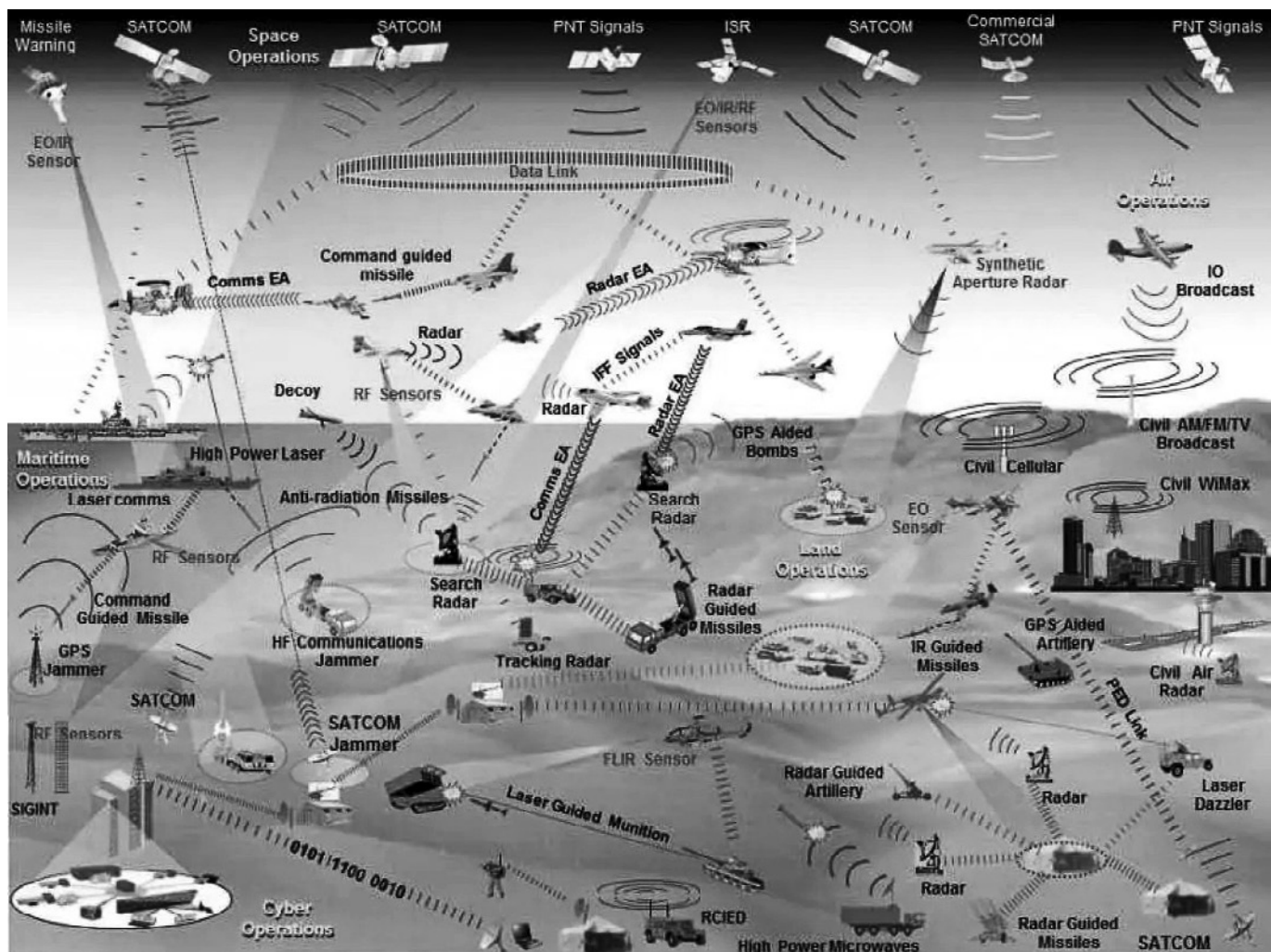
Erweiterte Realitäten

Vertreter der Logistik, der militärischen Gesundheitsversorgung, des Heeres, der Marine, der Luftwaffe, des Kommandos Streitkräftebasis, der Feldjäger und des ABC-Abwehrkommandos legten im Laufe der Veranstaltung ihre jeweilige Sichtweise auf die State-of-the-Art von unbemenschten Systemen in ihren jeweiligen Ämtern und Kommandos dar.

In der Logistik stecken laut Oberst i.G. Dr. Thomas Henschke (Oberst im Generalstab, Logistikkommando der Bundeswehr) unbemenschte Systeme für den strategischen und taktischen Transport von Gütern noch mitten in der Analysephase, wie bspw. Drohnen für den Waffen- und Versorgungsnachschub an der Front.

Auch die militärische Gesundheitsversorgung befindet sich nach den Worten von Generalarzt Dr. Bernhard Groß noch vor dem eigentlichen Aufbau von eigenen Experimentalsystemen. Das Amt erforscht derzeit bestehende Systeme und dokumentierte Einsatzszenarien von unbemenschten Systemen, zum Beispiel zur Bergung von Verwundeten aus dem Schlachtfeld mit Flugdrohnen (Unmanned Aerial Vehicle [UAV]), unbemenschten Fahrzeugen zu Land (Unmanned Ground Systems [UGS]) und humanoiden Robotern.

Das Amt für Heeresentwicklung (AHEntwg) startete vor kurzem erst seine Experimentalserie für UGS mit entsprechenden Ver-



Electronic Warfare in today's military environment (Bildquelle: Joint Air Power Competence Centre (JAPCC)²)

suchsszenarien. Oberstleutnant Pascal Pane sagte bestimmt und überzeugend, unbemenschte Systeme „müssen in allen zukünftigen Heeresplänen mitgedacht werden!“

Die Marine hingegen, noch mehr als die Luftwaffe, sammelt bereits seit Jahrzehnten Erfahrungen mit unbemenschten Systemen. Unter Wasser mit *Unmanned Underwater Vehicles* (UUV), aber auch auf dem Wasser mit *Unmanned Surface Vehicles* (USV), fährt beispielsweise die ferngelenkte Drohne *Seehund* schon seit den 80er-Jahren durch Minenfelder. Doch auch die Marine befindet sich in einer Übergangssituation.

Testfelder und virtuelle Experimentalsysteme sind demnach in allen Kommandos im Aufbau. Pilotinnen und Piloten von Flugdrohnen können bspw. nicht einzig auf Truppenübungsplätzen und ausgewiesenen militärischen Gebieten ausgebildet werden. Sie benötigen Simulationsumgebungen, u. a. auch aus ökologischen Aspekten heraus, um „*Reallflugstunden zu minimieren*“, so Oberst Rupert Ficker-Reißing (Kommando Luftwaffe), also eine Art *Gaming*-Unterstützung, das heißt virtuelle Landschaften, die auf den Bildschirmen und Interfaces der Piloten zur „echten“ Landschaft hinzugefügt werden können, virtuell konstruierte Übungsumgebungen oder *Live Virtual Constructive* (LVC).

Solche erweiterte Realitäten (*Augmented Reality* [AR]) müssen nun getestet bzw. von Programmierern und User-Interface-(UX-)Designern geschaffen und angepasst werden. Man kann sich AR wie eine Einblendung von Artefakten in das Echtzeitbild der Smartphone-Kamera oder beim Blick durch *Smartglasses* wie bspw. *Google-Glass* vorstellen, während man durch sie hindurch seine Umwelt betrachtet, in der man sich *real* bewegt.

Das „gläserne Gefechtsfeld“



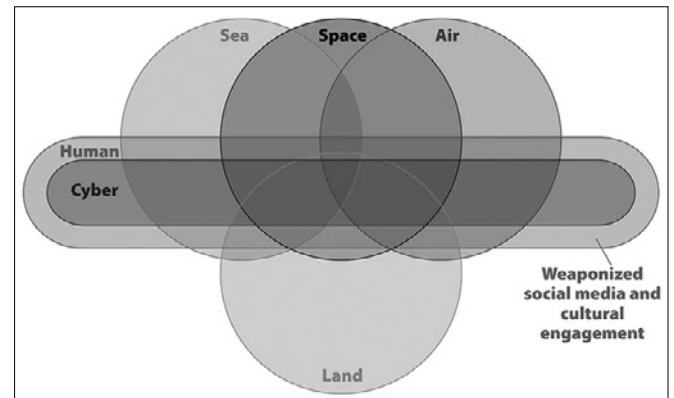
„Gläsernes Gefechtsfeld“, Quelle: wehrtechnik.info

Laut einem Bericht auf *wehrtechnik.info* wurde die zweite Bundeswehr-Studie zum *gläsernen Gefechtsfeld* im Jahr 2021 abgeschlossen³. Die jeweiligen Forschungsergebnisse aus der Studie wurden in einem Testszenario im November 2020 in Paderborn demonstriert. Die Bundeswehr und mehrere Vertreter aus der Industrie waren hierfür bei der *Atos Information Technology GmbH*. 20,7 Milliarden € sollen aus dem *Sondervermögen Bundeswehr* für den praktischen Ausbau des gläsernen Gefechtsfeldes (heute zu finden unter *Transparent Battlefield*) zur Verfügung stehen.

Multi-Domain-Operationen

Um sich militärisch durch ein *Transparent Battlefield* zu navigieren, benötigt man *multi domain battlespace management systems* (BMS). Das sind digitale Führungssysteme, um Gefechtsteilnehmer und die Führungsstäbe untereinander zu vernetzen und damit ein präzises, aktuelles Lagebild auf einen Blick für jeden „Nutzer“ erzeugen zu können. Das für die Bundeswehr derzeit im Fokus stehende BMS basiert auf einer bewährten Softwarefamilie: *Sitaware*. Diese nutzten bereits andere NATO-Mitgliedsstaaten⁴. Ohne solche Systeme wären *Multi-Domain-Operations* (MDO) nicht zu realisieren.

MDO bedeutet nicht mehr nur in den klassischen Feldern, zu Land, zu Wasser und in der Luft, operieren zu können (*to act, to observe, to orient and to decide*), sondern auch im Internet und im Weltraum. Auch hierfür werden Teile der 20,7 Milliarden € aufgebraucht werden, für ein System zur Satellitenkommunikation, einem geeigneten Mesh-Netzwerk, eigenen Rechenzentren als IT-Basisinfrastruktur, u. v. m. Denn neben der *elektronischen Kampfführung* (EloKa) gilt es vermehrt, auch die semantischen Kriegsführungstaktiken ernstzunehmen, mit Propaganda, Fake-News, auch Deepfake durch KI und Desinformationskampagnen im Internet, insbesondere den sozialen Netzwerken⁵.



Semantische Kriegsführungstaktiken, Quelle: U. S. Indo-Pacific Command⁶

Vor allem die gesellschaftlichen Folgen des Informationskriegs spüren wir derzeit täglich durch zweckgerichtete mediale Verbreitung und Produktion von Kriegsnachrichten. Er bestimmt unsere jeweilige individuelle Einstellung in jedem Moment gegenüber dem Geschehen, dem Kriegsgeschehen mit. So kommt den jeweiligen menschlichen Akteuren und *nicht-menschlichen Artefakten* innerhalb dieser Kanäle und Netzwerke eine aktive politische Handlungskraft zuteil, die ihre Wirkkräfte nach vorgegebenen Regeln entfalten – eben jenen, die in den Funktionsweisen der technischen Systeme verankert sind, gesellschaftliche Kräfte, die weit über die sozialen Medien hinaus gehen, mitten dort hinein, wo der Gemeinsinn herrscht. Dort, wo wir politisch handeln. Wo wir miteinander sprechen.

IT-, Militär-, die politische und die Alltagssprache

*Alles Denken fängt mit der Alltagssprache an
und entfernt sich von ihr.*
Hannah Arendt

Ich bin kein Militärexperte. Mein Forschungs- und Arbeitsschwerpunkt liegt auf *Ästhetik und neue Technologien und Ex-*

perimentelle Informatik mit Fokus auf Künstliche Intelligenz, was ich auch gemeinsam mit Prof. Dr. Georg Trogemann an einer staatlichen Kunsthochschule unterrichtete. Des Weiteren vertrete ich zusammen mit Prof. Dr. Hans-Jörg Kreowski das Forum Informatikerinnen und Informatiker für Frieden und gesellschaftliche Verantwortung e.V. (FIFF) im *Arbeitskreis gegen bewaffnete Drohnen*. Der AK organisiert u. a. Diskussions- und Informationsveranstaltungen zu aktuellen Entwicklungen von unbemenschten Systemen und Künstlicher Intelligenz im militärischen Kontext⁷.

Ich vertrete in solchen semi-öffentlichen Veranstaltungen wie bspw. den *Defense Days* eine meines Erachtens notwendige Beobachterrolle der Zivilgesellschaft. Nur eine von vielen. Mit nur einer Perspektive von vielen. Von vielen möglichen Sichtweisen auf autonome und teilautonome technische Systeme beim Militär.

Auch weil ich selbst nie *gedient* habe und mir die militärische Umgangssprache fremd ist, kann ich nur sehr schwer einschätzen, inwieweit die Aussagen der jeweiligen Oberste und Oberstleutnante einer fachlichen und systemischen Beobachtung ihrer Ämter und Kommandos in ihrem derzeitigen Umgang mit unbemenschten Systemen und ihrer militärischen Nutzbarkeit entsprechen. Wahrscheinlich muss man immer in solchen Gebietswechseln, von einer Redensart in die andere, Übersetzungsarbeit leisten. Der Soziologe Armin Nassehi spricht hier von den „*bestimmten Formen des sozialen Verkehrs*“, aus denen heraus kompakte Handlungsmuster entstehen. Diese bringen wiederum „*entsprechende Fachkenntnisse und Sondersprachen, Reflexionsformen und nicht zuletzt Milieus*“ mit sich⁸. So lassen sich militärische Eigenschaften, militärisches Wissen, Fähigkeiten von Soldatinnen und Soldaten, äußere Merkmale und erlernte Verhaltensweisen des Militärischen in militarisierter Sprache natürlich weitaus effektiver und auch plausibler ausdrücken als in unserer Alltagssprache. Auch lassen sich diese militärisch tradierten, doch sehr formalen Sprachgebräuche weitaus besser *Eindrücken* in technische Systeme, Sprachen, wie bspw. die *Battle Managment Language* (BML) scheinen wie geschaffen, um gleichzeitig mit Kameradinnen und Kameraden sowie auch mit technischen Systemen zu kommunizieren bzw. über Interfaces zu interagieren⁹.

Handlungs- und Kritikfähigkeit der Zivilgesellschaft

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

Georg Trogemann

Ich vertrete den Standpunkt, dass in Entscheidungsprozessen für oder gegen Experimentalsysteme und Einsätze unbemenschter bzw. (teil-)autonomer Systeme bei der äußeren sowie auch der inneren Sicherheit nichts selbstverständlich sein darf, ob nun zur Kampfhandlung oder zum Schutz öffentlicher Infrastrukturen, zu Aufklärungszwecken oder zur Bergung von Verwundeten. Ein jeder Schritt hin zu mehr Automatisierung – insbesondere militärischer – muss genauestens beobachtet und begutachtet werden. Dass dieser Standpunkt nicht immer einfach zu vertreten ist, versucht dieser Bericht zum Thema zu machen.

Zur Begutachtung solcher Schritte gibt es viele Behörden und staatlich eingerichtete Institute, auch Enquête-Kommissionen, Technikfolgenabschätzung, Ethikräte sowie zahlreiche Sachverständige und Expert:innengremien in ständigem Austausch mit Abgeordneten des Bundestags und des Europäischen Parlaments. Eher selten kommt in diesem speziellen Gebiet jedoch die Zivilgesellschaft zu Wort.

Des Weiteren kommen Informationen, die durchaus im Lichte des öffentlichen Interesses stehen, häufig nur durch direkte Anfragen an die Bundesregierung ans Tageslicht, was die politische Arbeit, öffentliche Debatten über verschiedene Arten der Autonomie mit und durch solche Systeme von unten heraus anzustoßen, häufig erschwert. Bisweilen wird es uns unmöglich gemacht, politische Debatten über die militärische Nutzung teilautonomer technischer Objekte zu führen.

Die Entwicklung der letzten Jahre von *unbemannten Drohnen* (UAV) hin zu *Unmanned Combat Aerial Vehicles* (UCAV) bei der Bundeswehr sowie auch eine Zulassung der *Heron TP* für den zivilen Luftraum führt uns diesen Sachverhalt in aller Deutlichkeit vor Augen. Eine breite gesellschaftliche Debatte über die Bewaffnung militärischer Drohnen unter Beteiligung der Zivilgesellschaft wurde weder von der letzten noch von der jetzigen Bundesregierung ausreichend geführt. Die Vereinbarung im Koalitionsvertrag, dass Drohnen der Bundeswehr nur unter „*verbindlichen und transparenten Bedingungen und unter Berücksichtigung ethischer und sicherheitspolitischer Aspekte bewaffnet werden können*“, wurde nicht eingehalten¹⁰.

Doch auch die Zivilgesellschaft sollte dazu in der Lage sein, diese Gegebenheiten und Anstrengungen adäquat einschätzen zu lernen oder zu können und hierfür an notwendige, von Fachpersonal aufgearbeitete Informationen zu gelangen, um sie verifizieren zu können, mögliche blinde Flecke sichtbar zu machen und die jeweiligen Informationen im öffentlichen Interesse für uns als glaubwürdig oder ggf. auch für unglaubwürdig erklären zu können.

Im öffentlichen Interesse

Sprache ist nicht nur irgendein Instrument der Politik, sondern überhaupt erst die Bedingung ihrer Möglichkeit.

Heiko Girnth

In diesem Sinne wären etwas präzisere Angaben für mich beim Verfassen dieses Berichts hilfreich gewesen. Nämlich, wann etwas unter Verschluss steht, dies klar und deutlich auch so zu benennen, also wann eine Studie, ein Experimentalsetting zur Eignungsprüfung oder spezifische Funktionsweisen von technischen Systemen nicht der Öffentlichkeit zugänglich gemacht werden können. Es wäre für mich hilfreich gewesen, um sorgfältiger einschätzen zu können, wann und ob in den zuständigen Ämtern evtl. nicht genügend Kenntnis über den jeweiligen Stand der Forschung bzw. innerer Funktionsweisen der von ihnen genutzten Systeme herrscht.

Fakt ist: In diesen Systemen herrscht immer ein hohes Maß an Komplexität. Und es muss gewährleistet sein, dass, wenn eines dieser Systeme – die als *disruptive Technologien*¹¹ häufig noch

selbst im Experimentierstadium sind – für militärische Operationen eingesetzt werden soll, auch dafür Sorge getragen wird, eine zu bewältigende Komplexität nicht zu überschreiten. Und diese Gewährleistung muss nachvollziehbar für die zivile Öffentlichkeit aufgearbeitet werden, in einer Sprache, die für einen möglichst großen Teil der Gesellschaft zugänglich und verständlich ist.

Das sehe ich als eine der zentralen Aufgaben von solchen semi-öffentlichen Veranstaltungen wie bspw. den *Defense Days*, aber auch allgemein der Öffentlichkeitsarbeit der Bundeswehr an, der Zivilgesellschaft zu erklären, was es für zukünftige Kampfhandlungen bedeutet, neue Technologien für neue Herausforderungen in den Militärapparat zu implementieren und welche gesellschaftlichen und kulturellen Konsequenzen das mit sich bringen könnte. Nur so können mehr-perspektivische Betrachtungsweisen auf diese hier im Fokus stehenden Systeme und auf ihren jeweiligen Einfluss auf technische Handlungen bei militärischen Operationen ermöglicht werden, um für uns zu verifizieren, dass Verantwortungsträger ihrer öffentlichen Verantwortung nachkommen.

Künstliche Intelligenz und menschliches Denken

Was bei der Veranstaltung sehr deutlich zum Vorschein kam, war, dass für die Bundeswehr Implementierungen von *Machine-Learning*-Komponenten und *Künstlicher Intelligenz* zunehmend an Bedeutung gewinnen, vor allem durch die immens steigende Masse an zu verarbeitenden Bild-, Sensor- und Aktordaten, wie von abbildenden Radaren zur Fernerkundung, Bild-Aufklärungsdaten oder Daten aus signalerfassender Aufklärung: Daten, die u. a. für Nutzer und Führungskräfte interpretierbar gemacht werden müssen, zur Unterstützung bei einer jeweiligen Entscheidungsfindung in militärischen Kampfhandlungen, aber auch in der Logistik, bei Feldjägern, Sanitätern, ABC-Abwehr etc. Ausnahmslos alle Bundeswehr-Einheiten sehen in diesem Feld akuten Handlungsbedarf und setzen sich laut den Vortragenden mit dem **Problem der rasant steigenden Menge an zu verarbeitenden Daten auseinander**.

Manned Unmanned Teaming

Kein Mensch, und sei er noch so gut ausgebildet, ist in der Lage, diese Datenströme in einer für die Funktionstüchtigkeit dieser Systeme notwendigen Geschwindigkeit zu verarbeiten, geschweige denn, sie direkt in militärisch-technische Handlungen zu überführen. Die State-of-the-Art der technischen Systeme sind es nur bedingt.

Dies ist wohl die eigentliche Herausforderung beim Auf- und Ausbau von Kampfhandlungen mit unbemenschten Systemen. Die Gewährleistung, dass die letzte Entscheidung, wenn es um Leben und Tod geht, beim Menschen liegt. Das ist nicht nur gesetzlich so verankert, sondern muss auch im Interesse aller Beteiligten liegen, nicht nur in Kampfhandlungen, auch im Zivilen. „*Der Einsatz von KI muss menschliche Entfaltung erweitern und darf sie nicht vermindern*“, schrieb Alena Buyx, Vorsitzende des Deutschen Ethikrates, in der Pressemitteilung am 20. März 2023 zur Veröffentlichung ihrer Stellungnahme *Mensch und Maschine – Herausforderungen durch Künstliche Intelligenz*¹². Der ehemalige Vorsitzende des Deutschen Ethikrates, Peter Dabrok, präzierte

dies bereits vor fünf Jahren, indem er sagte, dass „im KI-Zeitalter, in dem die Erhebung, der Austausch und die Nutzung von Daten Alltag ist, der Einzelne in menschlicher Echtzeit eingreifen können muss – wenn es für ihn persönlich relevant wird.“¹³

Doch wie kann solch eine Gewährleistung im alltäglichen Umgang mit technischen Systemen in der Praxis vonstatten gehen? Die Gewährleistung, dass die letzte Entscheidung beim Menschen liegt, in einen sich selbst betreffenden Datenstrom *eingreifen* zu können, sich digital zu erfahren, seine symbolische Repräsentation oder die seines Gegenübers *einsehen* zu können, sie auf solch eine Weise zu interpretieren, dass man sie auch verstehen kann. Für sich. Und dass man auf Grundlage dieses Verständnisses bzw. der aus ihr resultierenden Erkenntnis dann auch handeln kann.

„*Marketing or death by drone, it's the same math ... You could easily turn Facebook into that. You don't have to change the programming, just the purpose of why you have the system*“, so Chelsea Manning in einem Interview 2018. „*There's no difference between the private sector and the military.*“¹⁴

Auf Basis welcher maschinellen Vorinterpretation von Information entscheidet letzten Endes der Mensch einzugreifen? Wenn es für ihn relevant wird? Wenn sein Gewissen Entscheidungen zu treffen sucht? Die jeweilige Person kann ja nicht durch ihre eigenen Augen sehen. Weit mehr als nur *eine* mediale Ebene liegen zwischen ihr und ihrem „*ich kann*.“¹⁵ Zwischen ihrem Denken und dem Fall der Entscheidung liegen unzählige räumliche, zeitliche und auch psychologische Distanzen. Distanzen, die über eine Art Zwischenwelt, über Interfaces (Inter-facies ‚Zwischen‘-‚Form‘), im *Manned Unmanned Teaming*¹⁶ technisch, *künstlich*¹⁷, *intelligent*, wahrnehmbar und für den Menschen interpretierbar gemacht werden müssen.

Kognitive Assemblage

Der Begriff Kognition (vom lateinischen *cognito* für *Erkenntnis*) bezeichnet in der kognitionspsychologischen Forschung laut Lexikon der Psychologie „*die Gesamtheit der informationsverarbeitenden Prozesse und Strukturen eines intelligenten Systems (Intelligenz), unabhängig vom materiellen Substrat dieses Systems. Menschliche intelligente Systeme umfassen Prozesse und Strukturen für Wahrnehmung und Aufmerksamkeit, für Gedächtnis, Denken und Problemlösen, für Lernen sowie für Sprachverstehen und Sprachproduktion (Sprache).*“¹⁸

Unsere Sprache muss demnach, um über diese kognitiven Systeme sprechen zu können, verfeinert werden, in dem Maße, in dem diese die Rolle übernehmen, für uns zu „erkennen“. Denn diese kognitiven Systeme erstrecken sich laut dem Philosophen Holger Lyre in den Körper, in die Umgebung, in externe Hilfsmittel und Werkzeuge sowie auch in soziale Gemeinschaften.

Das heißt: Auch hierbei müssen wir sehr vorsichtig sein, welche und in welchem Maße wir kognitive Fähigkeiten den Maschinen und technischen Artefakten zuschreiben, denn im selben Maße delegieren wir auch menschliche Handlungsmacht an diese. Eine klare Trennung ist jedoch in den häufigsten Fällen nur schwer zu

setzen. „Unser Handeln erfährt durch die Vernetzung und den Zusammenschluss technischer und menschlicher Operateure zu immer komplexeren sozio-technischen Handlungssystemen eine Transformation“¹⁹, so Georg Trogemann.

Die Literaturwissenschaftlerin Nancy Katherine Hayles bezeichnet diese uns alltäglich gewordene Transformation als eine „kognitive Assemblage“. Wenn „die im Kampf eingesetzte Drohne von einem menschlichen Bediener zwar gesteuert wird, diese jedoch eine ganze Reihe von kognitiven Aktivitäten ausführt und auf vielfältige Weise selbständig handelt.“²⁰

Schon bei Flugzeugen wie bspw. der Boeing 777 ist Fliegen ein komplexes Zusammenspiel aus Maschine und Pilot, in der z.B. Fehlsteuerungen des Piloten vom System automatisch herausgerechnet und korrigiert werden. Bei Drohnensystemen kommen noch etliche, viele weitere Stufen der Aktivitätsverteilung zwischen Menschen, Dingen und Symbolsystemen hinzu:

- Um die Drohne zu steuern, senden Piloten aus Kontrollräumen heraus per Funk Steuerimpulse an die Drohne.
- Aus den empfangenen Steuerimpulsen errechnet eine komplexe Regelungstechnik die geeigneten Drehzahlen für Rotoren und Lüfter.
- Weitere Piloten kontrollieren und analysieren Kamerasysteme, Sensordaten und Satellitensignale.

Bildtechnologien und Computer-Vision verschmelzen mit Piloten in Assistenzsystemen, Big Data mit Entscheidungsträgern und Hilfssystemen zur Unterstützung der Entscheidungsfindung, Cloud-Dienste mit Kampfpiloten und Zielerkennungs- und Identifikationssoftware. Auch taktische Befehlshaber, Anwälte, Politiker und weitere Amtsträger bilden solche „kognitive Assemblagen“ mit, in denen „technische Systeme zusammen mit Menschen konstitutive und transformative Rollen übernehmen“, so N. Katherine Hayles weiter. Doch kognitive Assemblagen haben ihre Grenzen.

Die natürlichen Grenzen technischer kognitiver Systeme

In den letzten vier Jahren fand ein ganz spezifisches technisches kognitives System in unseren Lebensalltag per *Trial & Error* Einkehr. Bisher Undenkbares vermögen *Machine Learning* (ML) Algorithmen à la *ChatGPT* in ihrem Gebrauch zu entfalten.

Das, was allgemein als ML, als das maschinelle „Lernen“ bezeichnet wird, ist im Falle von *ChatGPT* ein großes Sprachmodell mit künstlich neuronalen Einbettungen, ein sogenanntes *Large Language Model* (LLM). Im Falle von GPT-3 bzw. GPT-3.5 (dem LLM hinter *ChatGPT*) werden mehr als 175 Milliarden Parameter in dem *Künstlichen Neuronalen Netz* (KNN) eingestellt. Ein iterativer Vorgang, der als „Training“ bezeichnet wird.

Dieses Training findet auf Clouds statt, die über viele mit *Grafikprozessoren* (GPU) ausgestattete Rechenzentren verteilt sind. Sie zählen mit zu den stromhungrigsten Prozessoren. GPT-3 benötigt zehntausende von ihnen zum Trainieren, wobei ein einziges Trainingsprogramm auch Wochen bis Monate dauern kann.

Mit der schnellsten derzeit auf dem Markt befindlichen GPU, wie sie auch in vielen Gaming-Home-Computern eingebaut ist, würde ein Trainingsdurchlauf um die 350 Jahre dauern. Der Stromverbrauch wird mit fast einer Gigawattstunde im Monat geschätzt, was in etwa dem Verbrauch von 3000 europäischen Durchschnittshaushalten im gleichen Zeitraum entspricht. Eine Frage an *ChatGPT* benötigt 1000 Mal mehr Strom als eine Suchanfrage bei Google, und für jede Antwort, die man von dem Chatbot erhält, könnte man ein Smartphone bis zu 60-mal aufladen²¹. Die KI-Forscherin Sasha Luccioni vermutet, dass, wenn die genauen Angaben zum Energieverbrauch veröffentlicht werden würden, der CO₂-Fußabdruck dieser GPUs genauso hoch sein wird, wie der eines kleinen Landes²², auch wenn in unbemenschten Systemen der Bundeswehr nur vereinzelt solch riesige KI-Modelle direkt zum Einsatz kommen werden. Laut Oberst i. G. Rupert Ficker-Reißing vom Kommando Luftwaffe steht die Frage, ob *Cloud* oder *Edge*, mit an oberster Stelle: Wie hoch also die Rechenleistung direkt in der Drohne sein muss und was aus Kapazitätsgründen in Clouds ausgelagert werden wird? Wie „direkt“ der Austausch mit den jeweiligen Bodenstationen sein muss und in welchen Situationen, welche Systeme hierfür angeschafft, bzw. nachgerüstet werden müssen.

Bewährte Großraumüberwachungssysteme in Drohnen wie bspw. *Increment2*²³ bestehen aus 368 Kameras und sind dazu in der Lage, eine Fläche von 100 km² zu erfassen. Durch das Aufzeichnen der Videos mit zwölf Bildern pro Sekunde werden so mehrere Terabyte Daten pro Minute erzeugt. Die Frage, wo in naher Zukunft Daten streitkräfteübergreifend verarbeitet werden, bringt rechtliche, administrative, ökonomische und auch ethische Fragen zu Tage.

Kein Fehler im System

Auf der anderen Seite haben wir es neben der natürlichen Begrenztheit kognitiver technischer Systeme mit einer scheinbaren Grenzenlosigkeit des „Lern-“vermögens zu tun, die uns bis hin zur Entgrenzung unseres Denkens führt. Denn diese technischen kognitiven Systeme können „sowohl lernen, dass die Erde flach ist, als auch rund“, so Noam Chomsky (linker Intellektueller, Anarchist und emeritierter Professor für Linguistik am Massachusetts Institute of Technology [MIT]) kürzlich in den *New York Times*.²⁴ Sie können auch lernen, dass seit über einem Jahr ein von Russland geführter Angriffskrieg gegen die ukrainische Bevölkerung herrscht. Im nächsten Moment können sie dies jedoch auch wieder verlernen, egal, ob es der Wirklichkeit entspricht oder nicht. Auch, dass der Holocaust nie stattfand sondern eine Erfindung sei, wie es Microsofts Twitter-Bot Tay im Jahr 2016 *tweetete*. Diese künstlichen intelligenten Systeme sind, während sie prozessieren, getrennt von der Außenwelt. In ihren inneren Entscheidungsfunktionen liegen keine Modellierungen von dem, was Worte, was Dinge, was Menschen und Ereignisse für uns in der Welt bedeuten. Es sind „Wahrscheinlichkeiten, die sich im Laufe der Zeit ändern.“²⁵

Dies sind keine Fehler im System. Im Gegenteil, die Algorithmen funktionieren so, wie sie konzipiert wurden. Sie „lernen“, wie bspw. der *Random Decision Forest* Algorithmus, Teile der Welt durch die Einwirkung von Zufälligkeit (Random) zu klassifizieren. Dieses spezielle *Machine-Learning*-Verfahren hatte sich

nach der Jahrtausendwende beim US-Militär zum *Algorithmus der Wahl* entwickelt, insbesondere für Systeme zur Identifizierung von Terrorzielen. „*Ein Algorithmus, mit Auswirkungen auf Leben und Tod, und er erzeugt diese Auswirkungen, indem er den Zwiespalt zwischen Vernunft und Wahnsinn neu formuliert*“, bzw. formalisiert. Die Zufälligkeit dieses Algorithmus „*ist eine Art geschützter Wahnsinn, der in der Logik des Algorithmus wohnt und der der Welt eine unerreichbare Vision von einer sicheren Zukunft verspricht*.“²⁶

Ein Wahnsinn also, nicht etwa aus einem Verlust an Rationalität oder aus der Übertragung von menschlichen Denkprozessen in einen maschinellen Verarbeitungsprozess. „*Ein Wahnsinn, einzig dem Versuch geschuldet, ist eine Berechnung durchzuführen unter den Bedingungen des Nichtwissens*.“²⁷

Die Entgrenzung unseres Denkens

Wahre Intelligenz ist auch zu moralischem Denken fähig.
Noam Chomsky

Diese *Künstlichen Intelligenzen* sind nicht Teil unserer Gesellschaft. Eine Subjektivierung dieser Systeme hat meines Erachtens fatale Folgen für unser gesellschaftliches Miteinander. Natürlich wurden technische Systeme mit KI-Implementierungen Teil unseres Lebensalltags: in öffentlichen Einrichtungen, in der Medizin, dem Straßenverkehr, unseren Smartphones und Laptops. Und natürlich bestimmen sie unsere alltäglichen technischen Handlungen auch irgendwie mit. Und es passiert natürlich auch etwas, und zwar ganz subjektiv, oder präziser ausgedrückt, intersubjektiv, wenn wir die jeweiligen Systeme und Programme nutzen und diese uns in der Interaktion begegnen. Wir als Gesellschaft lernten in diesem Jahrtausend u. a. auf diese Weise, dass „*soziale Praktiken von menschlichen Körpern ebenso wie von nicht-menschlichen Artefakten getragen*“ werden.²⁸

Aber im Gegensatz zu nicht-menschlichen Artefakten, zu technischen kognitiven Systemen sind wir Menschen dazu in der Lage, unsere grenzenlose Kreativität als intelligentes Verhalten einzuschränken, unser Denken und uns auferlegte geistige Einschränkungen auf unser jeweiliges (nicht einzig) technisches Handeln wirken zu lassen. Wir als Gesellschaft vermögen unsere geistige, scheinbar grenzenlose Kreativität durch ethische Prinzipien einzuschränken, was uns zu einer Denkart befähigte, die wir als „*moralisches Denken*“ bezeichnen: Mores (Moral) kommt von Selbst und fragt, „*kann ich mit dem, was ich getan habe, noch weiterleben?*“²⁹ Das sind die meines Erachtens für den Kontext dieses Berichts wesentlichen Unterschiede zwischen menschlichem Denken und der Künstlichen Intelligenz.

Aus Fehlern lernen

Wenn wir auf dem Gebiet der Bilderkennung/KI überhaupt Erfolg haben sollten, dann wird das zur „Verbesserung“ einer Waffe führen.
Joseph Weizenbaum

Das Massachusetts Institute of Technology (MIT) nahm im Jahr 2013 über eine Milliarde Dollar Forschungsgelder vom US-Ver-

teidigungsministerium in Anspruch, u. a. zur Forschung an Raketenabwehrsystemen, Cybersicherheit, Sensorik, KI und Überwachungstechnologien sowie auch der Drohnenforschung. Joseph Weizenbaum (1923-2008), Computer- und Gesellschaftskritiker und ehemaliger Professor für Computerwissenschaften, der während seiner gesamten Zeit am MIT die Mitarbeit an der Entwicklung von Waffen und Waffensystemen verweigerte, schrieb in den 80er-Jahren, dass an dieser Forschungsuniversität stetig an neuen „*„Sehmaschinen“ gearbeitet wird, damit computergesteuerte Geräte, Roboter und Cruise Missiles noch besser sehen, noch besser treffen, als sie es heute schon können*.“³⁰

Er beschrieb 1991 in seinem Vortrag *Gegen den militärischen Wahnsinn*, wie am *Medialab* des MIT Bildtechnologien erforscht und entwickelt wurden, die militärischen Computern, unbemenschten Systemen bis hin zu autonomen Robotics im Golfkrieg das „Sehen“ beibrachten. Dass hierdurch eine Präzision der Waffen erreicht wurde, wenn bspw. eine Rakete auf ein Wasserwerk in Bagdad steuert „*und wie sie da ganz genau trifft. Sie trifft ganz genau eine ganz bestimmte Tür. (...) Das ist ganz anders als sonst, wenn B 52-Maschinen Tausende von Bomben werfen*“, so Weizenbaum.

„Saubere Kriege“

Dieser Waffentypus veranlasste George W. Bush, den Golfkrieg als einen „*sauberen Krieg*“ zu bezeichnen, ebenso Barack Obama und später auch Donald Trump ihre Art der High-Tech-Kriegsführung, u. a. in Afghanistan. Doch weder der Golfkrieg noch der Afghanistankrieg waren saubere Kriege. Und auch in Bergkarabach und in der Ukraine haben Drohnen und sogenannte Präzisionswaffen den Krieg nicht verändert. Kriege sind noch immer martialisch und blutig und weder sterben weniger Soldaten noch weniger Zivilisten durch neuartige Präzisions-Waffensysteme wie bspw. *Loitering Munition*, worauf das Amt für Heeresentwicklung laut Sprecher derzeit stark fokussiert.

Loitering Munition Systeme zur Panzerabwehr

Umgangssprachlich werden diese Waffen auch als *Kamikaze-Drohnen* bezeichnet. Eine Drohne mit integriertem Sprengkopf, die beim Aufschlag auf ein Ziel selbst mitzerstört wird. *Loitering Weapons* werden zunächst ohne bestimmtes Ziel gestartet und kreisen anschließend für längere Zeit über dem Zielgebiet. Daher die Bezeichnung *Loitering Munition*: Herumlungernde Munition. Wird den Drohnen ein Ziel zugewiesen, so wird es von der Drohne angegriffen. Je nach Ausführung können auftauchende Ziele auch *autonom*, mittels eigener Sensorik identifiziert und durch einen selbstständig eingeleiteten Angriff bekämpft werden.

In Bergkarabach wurden erstmals große Mengen dieser Drohnen von Aserbaidschan eingesetzt.³¹ Auch in der Ukraine kommt eine hohe Anzahl dieser Drohnen auf beiden Seiten zum Einsatz, z. B. die amerikanische *Switchblade* oder *Phoenix Ghost* oder von russischer Seite die *Lancet-Drohne*.

Operative Bilder

Der Kulturtheoretiker Klaus Theweleit bezeichnete diesen Waffentypus einst als „filmende Bomben“³², da sie im ersten Irakkrieg mit Kameras ausgestattet waren und deren Signal- bzw. Bildübertragung beim Erreichen ihres vordefinierten Ziels abbrach. Dieser ganz spezielle Bildtyp in kontrastarmem Schwarz-weiß, im Zentrum das Fadenkreuz, wurde 1991 in der ARD gesendet. Mit dem Einschlag des Projektils riss die Aufnahme ab. Diese Bilder waren rein *operative Bilder*. Ein Begriff, den der Filmemacher Harun Farocki prägte. Bilder zur fotografischen Kontrolle der Wirksamkeit des Angriffs. „Diese Bilder wurden damals im Zusammenhang mit dem Wort intelligente Waffen gezeigt, und weil sie den Blickpunkt der Waffe einnahmen und nicht den eines zielenden Soldaten, erschienen sie als Subjektive neuen Typs. Sie gaben dem Projektil eine Subjekt-Ähnlichkeit und waren ein Bild zur Einfühlung in den Geist der Waffe“, so Harun Farocki in seinem Kriegstagebuch.³³

Operative Fehler

Während unbemerkte Systeme laut einiger Vortragenden während der Veranstaltung in den letzten 10 Jahren quasi nicht beachtet wurden, waren sie aber dennoch im Einsatz. Ein Beispiel ist die *Heron1* in Aufklärungsmissionen für Kampfhandlungen in einem Krieg namens *Enduring Freedom*. Ein Krieg unter Führung der NATO, an der auch die Bundeswehr beteiligt war. Dieser Krieg begann spätestens in den frühen 2010ern zu einer Art Testfeld zur Erforschung disruptiver Kriegstechnologien zu mutieren, eine Art *Trial & Error Zone*.

Zahlreiche technische Fehler und militärische Fehlentscheidungen in dieser gänzlich neuen Art des High-Tech-Krieges bestätigten diesen Verdacht mit den Jahren. Den Verdacht, dass die westlichen Militärs damals in einem Designprozess netzwerkzentrierter Kriegsführungstaktiken (*Network Centric Warfare*) und der Mitgestaltung eines *Multi domain battlespace* steckten.

Die Zivilgesellschaft lernte in diesem Jahrtausend so, dass jene Technologien, die sich den disruptiven zuordnen lassen, nicht mehr im Labor erprobt werden. Insbesondere in der Künstliche-Intelligenz- und Drohnenforschung gehörten in den letzten 10-15 Jahren *Trial & Errors* im Design unbemerkter Systeme schon fast zur Tagesordnung. Bei Kampfdrohnen, die in *Multi Domain Operations* zum Einsatz kamen, bspw. fehlerhaften Großraumüberwachungssystemen (*Intelligence, Surveillance and Reconnaissance* [ISR]).

Einer der ersten veröffentlichten Fälle bezog sich auf das ISR *Gorgon Stare*, das zwar bekannte technische Fehler aufwies, aber trotzdem aus Kosten und Zeitgründen zur Überwachung und Identifizierung bei Kampfhandlungen eingesetzt wurde.³⁴ *Gorgon Stare* ermöglichte damals schon, wenn auch fehlerhaft, eine Überwachung von 16km². Die Einzelbilder der Kameras betrugen je 5 Millionen Pixel, aus denen ein Gesamtbild von

1,6 Milliarden Pixel erzeugt werden konnte. Allein im Jahr 2009 wurden mit diesem System Videoaufnahmen im Umfang von 24 Jahren generiert. Im Jahr 2011 waren es bereits 37 Jahre. Zur Lokalisierung und zur Identifizierung von Zielen waren diese Systeme jedoch zu diesem Zeitpunkt nicht fähig. Andere Datensätze wie die *JPEL-Listen*³⁵ (*Joint Priority Effects List*, zu deutsch: *Gemeinsame Wirkungsvorrangliste*), die die CIA und die NATO während des Kampfeinsatzes am Hindukusch führten, wurden zum Datenabgleich hinzugezogen.

Auf diesen Listen standen keine Namen von Personen, sondern Codes: Mullah Niaz Muhammed z. B. bekam den Namen Doody und die ISAF No. IS3673. Er lebte in 41R PQ 1768 9260 und wurde ermordet mittels einer UGLY 50 AGM-114, einer Hellfire Rakete in 41R PR 17897 92491. Bei diesem Drohnenangriff am 071017D*Feb11 wurde versehentlich auch ein KIA (ein kleiner Junge) getötet und ein WIA (ein erwachsener Mann) schwer verwundet.

Dynamic Target Storyboard RC(SW) – 1FH J3 Tgts – Op STEN TAKAY Obj DOODY – Mullah Niaz Muhammed – IS3673			
UNIT: 1FH J3 Tgts PUC: Engagement Asset: UK AH-64 C/S UGLY 50 Qualified Observer: WIDOW 87	Objective: UGLY 50 Date of Engagement: 10/11/11 (11) ISAF No.: IS3673 Location: 41R PQ 1768 9260 Description: JPEL Tgt Function: mid-level commander and facilitator Significance: JPEL PFI-2 Tgt	BDA: UGLY 50 conducted a 420 strike on JPEL Tgt Obj DOODY (Mullah Niaz Muhammed, IS3673). UGLY 50 engaged target alone and on foot in the open with 100 x 30mm. 1 x WIA. Initial engagement with 1 x AGM-114 of Obj DOODY + 1 x PIDROF may have resulted in 2 x Civilians (1 x WIA, 1 x KIA).	Engagement summary: 071017D*FEB11 – UGLY 50, 41R PQ 1768 9260, 1 x AGM-114. 071017D*FEB11 – 100 x 30mm. Munitions Employed: 071017D*FEB11 – 1 x AGM-114. 071017D*FEB11 – 100 x 30mm.
Follow-on plans: Ground C/S arrived at engagement site at 1134Z. Initial RNA 1 x EWIA (Obj DOODY), 1 x WIA (adult male), 1 x KIA (male child). Immediate first aid given to 1 x EWIA and 1 x WIA, with subsequent Casvac at 1144Z. 1 x KIA taken to compound by LN for immediate burial. INT Summary: Obj DOODY is a mid level commander who operates in both NDA(S) and MJA. He maintains links to Obj KOLAK from whom he receives direction and Obj STILTSKIN with whom he is assessed to discuss commission matters, particularly 1st dispute resolution by lethal means. Obj DOODY is active in planning attacks on CF and NDA DCC. He also directs subordinate to conduct attacks and facilitates the supply of heavy weapons and ammunition. Obj DOODY is a new commander who has been given the responsibility for Sustained by Obj KOLAK. Expectation: The removal of Obj DOODY will deny the IHS within NDA(S) and MJA of a competent commander linked into the HMJ Military Commission. The networks within this area are suffering as a result of recent targeting and IHS operations. Removing the IHS this commander will further impact on the IHS ability to conduct attacks against CF and ANSF and the resupply of weapons.			
Further details of Tgt Struck: All Timings: LOCAL (D). 0741 – RELINT places Obj DOODY at 41R PQ 1803 9180 in NDA(S) AO. 0960 – Obj DOODY conducts Shura with 6 x adult males at 41R PQ 1780 9250. 1003 – Following the necessity analysis PURSUE 60 operator calls PID Obj DOODY. 1006 – UK AH-64 C/S UGLY 50 checks in with 1FH J3 Tgts JTAC, WIDOW 87. 1014 – UGLY 50 is talked onto Obj DOODY. 1016 – Obj DOODY with 1 x PIDROF moves away from group on foot heading generally West. 1017 – TEA granted for Obj DOODY + 1 x PIDROF by TFH Comd. 1017 – UGLY 50 engages Obj DOODY + 1 x PIDROF on foot in the open with 1 x AGM-114. AGM-114 appears to miss the target impacting at 41R PQ 1781 9254. 1018 – Obj DOODY and 1 x PIDROF then split with Obj DOODY moving away West and 1 x PIDROF moving away North East. 1019 – UGLY 50 engages Obj DOODY on his own on foot in the open with 100 x 30mm at 41R PQ 1768 9260. 1026 – Initial BDA is Obj DOODY EWIA. 1134 – Ground C/S arrives at engagement area. Immediate first aid given to Obj DOODY EWIA, 1 x WIA (adult male) and 1 x KIA (male child) also discovered by ground C/S. Immediate first aid given to 1 x WIA. 1144 – Obj DOODY and 1 x WIA Casvac'd to BSN.			

Dynamic Target Storyboard: Obj. DOODY, Quelle: Spiegel International³⁶

Auch dies sollte als ein grundlegender Fehler in dieser Art von Kriegsführungstaktiken benannt werden: Dass, wie Joseph Weizenbaum festhielt, Menschen und Dinge und Ereignisse durch diese Systeme zu „programmierbaren Daten“ werden: „es geht um ‚Input‘ und ‚Output‘, Variable, Prozentzahlen, Prozesse und dergleichen, bis jeglicher Zusammenhang mit konkreten Dingen wegabstrahiert ist und nur noch abstrakte Graphen, Zahlenkolonnen und Ausdrücke übrigbleiben.“

Anmerkungen

- 1 Digitaler Staat Online (2023): Defence Day – Unbemerkte Systeme, Behörden Spiegel. URL: <https://web.archive.org/web/20230328110128/https://www.digitaler-staat.online/programm/#29032023defenceday> [abgerufen am 28.04.2023].
- 2 Spreckelsen, Malte von (2018): Electronic Warfare – The Forgotten Discipline: Why is the Refocus on this Traditional Warfare Area Key for Modern Conflict?, Joint Air Power Competence Centre, URL: <https://www.japcc.org/articles/electronic-warfare-the-forgotten>

- discipline/ [abgerufen am 28.04.2023].
- 3 apf (2021): Phase 2 der Studie "Transparentes Gefechtsfeld" abgeschlossen, wehrtechnik.info. URL: <https://wehrtechnik.info/index.php/2021/01/14/phase-2-der-studie-transparentes-gefechtsfeld-abgeschlossen/> [abgerufen am 28.04.2023].
 - 4 Müller, Peter (2020): Für ein schnelles Lagebild: Neues digitales Führungssystem vorgestellt, bundeswehr.de. URL: <https://www.bundeswehr.de/de/organisation/heer/aktuelles/digitales-fuehrungssystem-260726> [abgerufen am 28.04.2023].
 - 5 Kirsch, Martin (2022): 100.000.000.000 Euro – Wer profitiert vom Sondervermögen?, Informationsstelle Militarisierung e. V. URL: <https://www.imi-online.de/2022/09/26/100-000-000-000-euro/> [abgerufen am 28.04.2023].
 - 6 Brown, Robert B. (2017): The Indo-Asia Pacific and the Multi-domain Battle Concept, U.S. ARMY, URL: https://www.army.mil/article/184551/the_indo_asia_pacific_and_the_multi_domain_battle_concept [abgerufen am 28.04.2023].
 - 7 Siehe hierzu die beiden Hearings Krieg mit Künstlicher Intelligenz (10.03.22) und Aktuelle Entwicklungen bei militärischen Drohnen – am Beispiel von Afrika, der Ukraine und der Türkei (25.01.23). URL: <https://media.ccc.de/b/conferences/fifkon/kriegundki> [abgerufen am 28.04.2023].
 - 8 Nassehi, Armin (2019): Muster – eine Theorie der digitalen Gesellschaft, München: C.H.Beck Verlag
 - 9 Wanner, Franz (2018): Battle Management Language – Sprachlose Mythen militärischer Strukturen, in: Krieg im Informationsraum, Zum 21. Kongress der Informationsstelle Militarisierung, S. 32-39, URL: <https://www.imi-online.de/download/Informationsraum2018-Web.pdf> [abgerufen am 28.04.2023].
 - 10 Rassbach, Elsa (2023): Der neue Drohnenkrieg im Aus- und Inland: Daten sammeln, schützen, zur "Not" töten?, in Friedensforum 2/23, URL: <https://www.friedenskooperative.de/friedensforum/artikel/bewaffnete-drohnen> [abgerufen am 28.04.2023].
 - 11 Zu den disruptiven Technologien zählen diejenigen Technologien, die dem Markt ein anderes, ein gänzlich neues Wertversprechen bieten. Start-Up Unternehmen, die Big- bzw. New Tech Industries, die Eliten der Künstliche-Intelligenz-Forschung, sie stellen im Vergleich zu den nachhaltigen Technologien (Sustaining technologies) bewußt unausgereifte Produkte her. Der Trial & Error dieser Technologie-Art findet demnach mitten in der Gesellschaft statt; im zivilen Raum, in Combat Zones sowie auch in Kriegsgebieten.
 - 12 Deutscher Ethikrat (2023): Stellungnahme „Mensch und Maschine – Herausforderungen durch Künstliche Intelligenz“, URL: <https://www.ethikrat.org/pressekonferenzen/veroeffentlichung-der-stellungnahme-mensch-und-maschine> [abgerufen am 28.04.2023].
 - 13 Tricarico, Tanja (2018): Bund will künstlich intelligent werden, taz, URL: <https://taz.de/Foerderung-neuer-Technologie/!5518286/> [abgerufen am 28.04.2023].
 - 14 Cadwalladr, Carole (2018): 'I spent seven years fighting to survive': Chelsea Manning on whistleblowing and WikiLeaks, The Guardian, URL: <https://www.theguardian.com/us-news/2018/oct/07/chelsea-manning-wikileaks-whistleblowing-interview-carole-cadwalladr> [abgerufen am 28.04.2023].
 - 15 Merleau-Ponty, Maurice (1967): Das Auge und der Geist. Philosophische Essays, Hamburg: Reinbek Verlag. Zitat: „Alles was ich sehe, ist prinzipiell in meiner Reichweite, zumindest in der Reichweite meines Blickes, es ist vermerkt auf der Karte des »ich kann«“
 - 16 Das Amt für Heeresentwicklung fokussiert derzeit im Bereich der High-Tech-Kriegsführung auf ein gut funktionierendes Zusammenspiel von unbemenschten Plattformen, die aus bemenschten Systemen heraus geführt werden können. Dies Zusammenspiel wird als Manned Unmanned Teaming (MUM-T) bezeichnet.
 - 17 Simon, Herbert (1969): The Sciences of the Artificial, Cambridge (US): MIT Press. Laut Herbert Simon bedeutet „Künstlichkeit Wahrnehmungsgleichheit, aber zugleich auch eine wesentliche Verschiedenheit. Es handelt sich hierbei um eine Ähnlichkeit von außen und nicht von innen. Das artifizielle Objekt imitiert das Reale, indem es dem äußeren System das gleiche Gesicht zuwendet“, siehe Simon, Herbertin The Sciences of the Artificial, von Herbert Simon, MIT Press, 1969
 - 18 Kluwe, Rainer H.: Kognition, Spektrum.de, URL: <https://www.spektrum.de/lexikon/psychologie/kognition/7882> [abgerufen am 28.04.2023].
 - 19 Trogemann, Georg (2014): Der Blick der Drohne, in: Ursula Zeller, Heiko Schmid, Frank-Thorsten Moll (Hrsg.), Archäologie der Zukunft, URL: <https://georgtrogemann.de/wp-content/uploads/2021/04/DerBlickDerDrohne.pdf> [abgerufen am 28.04.2023].
 - 20 Hayles, N. Katherine (2017): Unthought: The Power of the Cognitive Nonconscious, Chicago (US): University of Chicago Press
 - 21 Jonas, Tobias (2023): ChatGPT: Die Cloud Kosten des berühmtesten AI Sprachmodells, innFactory.de, URL: <https://innfactory.de/artificial-intelligence/was-kostet-der-cloud-betrieb-von-chatgpt/> [abgerufen am 28.04.2023].
 - 22 Luccioni, Alexandra Sasha, Sylvain Viguier und Anne-Laure Ligozat (2022): Estimating the Carbon Footprint of BLOOM, a 176B Parameter Language Model, arxiv.org, URL: <https://arxiv.org/abs/2211.02001> [abgerufen am 28.04.2023].
 - 23 Stephen Trimble (2014): Sierra Nevada fields ARGUS-IS upgrade to Gorgon Stare pod, flightglobal.com, URL: <https://www.flightglobal.com/civil-uavs/sierra-nevada-fields-argus-is-upgrade-to-gorgon-stare-pod/113676.article> [abgerufen am 28.04.2023].
 - 24 Chomsky, Noam, Ian Roberts und Jeffrey Watumull (2023): The False Promise of ChatGPT, New York Times, URL: <https://www.nytimes.com/2023/03/08/opinion/noam-chomsky-chatgpt-ai.html> [abgerufen am 28.04.2023].

Christian Heck



Christian Heck (Medienkünstler und Graswurzelaktivist) arbeitet als Künstlerisch-wissenschaftlicher Mitarbeiter für *Ästhetik und neue Technologien* an der Kunsthochschule für Medien Köln (KHM). Er unterrichtet dort im Fachbereich *Experimentelle Informatik* und ist Teil der Forschungsgruppe *ground zero – Aesthetics of technics and cognition*. Heck studierte *Künstlerische Arbeit im Kontext der medialen und wissenschaftlichen Bildproduktion* und *Medienkunst* in München, Berlin und den Niederlanden. Seine Masterarbeit beschäftigte sich mit fehlerbehafteten symbolischen Repräsentationen gesellschaftlicher Subjekte durch tradierte und disruptive Bildtechnologien. Er promoviert derzeit bei Georg Trogemann an der KHM über subversive Strategien, die sich an der Schnittstelle zu Politischer Lyrik und Adversarial Attacks (Das Hacken künstlicher neuronaler Netze) befinden.

- 25 ebd.
- 26 Amore, Louise (2020): *Cloud Ethics – Algorithms and the Attributes of Ourselves and Others*, Durham (US): Duke University Press
- 27 ebd.
- 28 Reckwitz, Andreas (2016): *Kreativität und soziale Praxis*, Bielefeld: Transcript Verlag
- 29 Arendt, Hannah (2006): *Über das Böse. Eine Vorlesung zu Fragen der Ethik*, München: Piper Verlag
- 30 Wendt, Gunna und Franz Klug (Hrsg., 2001): *Joseph Weizenbaum, Computermacht und Gesellschaft – Freie Reden*, Berlin: Suhrkamp Verlag
- 31 Trautvetter, Bernhard (2020): *Brandbeschleuniger Kampfdrohne – Der Konflikt zwischen Armenien und Aserbaidschan verdeutlicht, welche Gefahr von Drohnen ausgeht*, in: IPPNW forum 164/2020 – Die Zeitschrift der IPPNW, URL: https://ippnw.de/commonFiles/pdfs/Forum/164/Drohnen_Bergkarabach_Trautvetter.pdf [abgerufen am 28.04.2023].
- 32 Riederer, Günter (2015): *Filmende Bomben. Luftkrieg und neue Bildproduktion in Harun Farockis „Erkennen und Verfolgen“*, in: Susanne Krasmann und Jürgen Martschukat (Hrsg.), *Rationalitäten der Gewalt*, Bielefeld: Transcript Verlag. URL: https://www.researchgate.net/publication/350273118_Filmende_Bomben_Luftkrieg_und_neue_Bildproduktion_in_Harun_Farockis_Erkennen_und_Verfolgen [abgerufen am 28.04.2023].
- 33 Farocki, Harun (2003): *Experten und Projektile – Tagebuch zum Krieg*, jungle.world. URL: <https://jungle.world/artikel/2003/15/experten-und-projektile> [abgerufen am 28.04.2023].
- 34 Welsh, William (2011): *Gorgon Stare test uncovers major glitches*, von William Welsh, Defensesystems. URL: <https://web.archive.org/web/20110128031208/http://defensesystems.com/articles/2011/01/24/gorgon-stare-test-shows-serious-glitches.aspx> [abgerufen am 28.04.2023].
- 35 Spiegel Staff (2014): *A Dubious History of Targeted Killings in Afghanistan*, Spiegel International. URL: <https://www.spiegel.de/international/world/secret-docs-reveal-dubious-details-of-targeted-killings-in-afghanistan-a-1010358.html> [abgerufen am 28.04.2023].
- 36 Raphael, Samuel (2014): *Dynamic Target Storyboard: Obj DOO-DY*, Spiegel International, URL: <https://www.documentcloud.org/documents/20701542-20110207-nato-storyboard-doody> [abgerufen am 28.04.2023].

Wolfgang Krieger

Hegelsche Dialektik und das Problem der Formalisierung in Mathematik, Elektrodynamik, Systemtheorie und Künstlicher Intelligenz

Das ist der Titel meiner Dissertation, mit der ich am Fachbereich Mathematik/Informatik der Universität Bremen Ende 2022 promoviert habe. Die Arbeit wurde betreut von Professor Hans-Jörg Kreowski, der mich auch animiert hat, eine Zusammenfassung für die FfF-Kommunikation zu schreiben. Der Zweitgutachter war Professor Gregor Nickel, der an der Universität Siegen das Fach Funktionalanalysis und Philosophie der Mathematik vertritt. In diesem Artikel werden die Methode und einige zentrale Ergebnisse der Arbeit vorgestellt. Ein kleiner Hinweis sei allerdings erlaubt, weil die behandelte Thematik nicht im Zentrum von Informatik und Gesellschaft liegt und sich nicht immer leicht erschließt.

Einleitung

Mit Hegel (1770-1831) beginnt eine neue Zeit in Europa – für die Philosophie wie auch für die gesellschaftliche Wirklichkeit; und beide geraten durch ihn in ein neues Verhältnis. Die Neue Zeit, so seine Aussage, offenbart sich durch die Französische Revolution von 1789, die den Absolutismus in Frankreich beendet und die bürgerliche Republik einführt. Ihre weitreichenden und unumkehrbaren Ergebnisse verändern nicht nur ganz Europa, sondern auch das Leben Hegels unmittelbar. Die Napoleonischen Kriege, die den Gedanken der Aufklärung in das übrige Europa tragen, führen für die preußische Armee zu einer vernichtenden Niederlage, in deren Konsequenz der preußische König eine Modernisierung an Haupt und Gliedern beschließt, um seinem Land eine führende Stellung in Europa zu verschaffen: Der an einer Provinz-Universität lehrende Philosophieprofessor Georg Wilhelm Friedrich Hegel wird 1818 an die Berliner Universität berufen, um dort den Reformen die Krone aufzusetzen und zum führenden Philosophen Preußens zu werden – und zum Philosophen des Aufstiegs der Moderne.

Seine Philosophie vollzieht ihre Emanzipation von der Theologie und will die Wirklichkeit aus sich selbst erklären. Sie bean-

sprucht die Integration aller bisherigen modernen Philosopheme von Descartes über Leibniz, Kant und Fichte und findet einen besonderen Anschluss an die griechische Antike bei Platon und Heraklit. Sie betont die Dominanz von Geist, Bewegung, Vernunft und Dialektik.

Die Dialektik gilt ihm als das innere Prinzip¹ der sich vollziehenden Bewegung wie Veränderung der Wirklichkeit; ihre äußere Erscheinung ist der Widerspruch. Damit öffnet er die Tür zu einem neuen Verständnis von Welt – er verbindet Materie mit Geist und initiiert die Theoriebildung der Moderne, indem er die Naturwissenschaften einbezieht und einen dialektischen Zusammenhang zwischen der Subjektivität der Gesellschaft und der Objektivität der Natur herstellt.

Motiv und Methode

Die Hegelsche Philosophie wird wesentlicher Bestandteil der aufsteigenden Moderne, und mit der Dialektik entsteht eine erste Darstellung der Dynamik, in welcher sich die Wirklichkeit entfaltet. Nicht mehr die Realität gilt als das Maß der Dinge – sie bildet lediglich das aktuelle Abbild eines sich verwirklichenden

Prinzips. In seiner ersten grundlegenden Arbeit (1807) nimmt er die sichtbaren und sich verändernden Erscheinungen in Natur und Gesellschaft zum Ausgangspunkt. Weil sich in ihnen eine Höherentwicklung, weg von der schlichten Materie und hin zu ihrer Kombination mit dem Geist resp. der Theorie manifestiert, nennt er diese Arbeit die *Phänomenologie des Geistes*.² Als er sich in seinem letzten Lebensjahrzehnt insbesondere der Natur bzw. den neuen Naturwissenschaften zuwendet, erkennt er in deren Motivation ein subjektives, also gesellschaftliches Motiv: die *Begierde*. Sie zielt auf die Aneignung der Natur – zuerst, mit Blick auf die frühkapitalistische Industrialisierung in England, geht es um ihre Stoffe, jetzt und zukünftig um ihre inneren Funktionen. Dabei gerät das subjektive Motiv in Konflikt mit den objektiven Verhältnissen in der Natur. Hegel erkennt darin einen *dialektischen Widerspruch*, der nunmehr bestimmend für die modernen Naturwissenschaften sein wird. Für sie gelte, dass ihre Gegenstände an sich selbst widersprüchlich seien, und dies zu erfassen sei ihre Aufgabe. Und, so führt die Dissertation fort, dieser Widerspruch mache das Wesen der Erkenntnis aus und sei in ein mathematisches Modell zu überführen. Erst diese Form ist für die Reproduktion durch die Maschine geeignet.

Die Dialektik gegen die Mathematik abzugrenzen, war Hegel ein hohes Anliegen. Seine Forderung, die Wirklichkeit als Veränderung, als Werden und Vergehen zu denken, war ihm unvereinbar mit einer Einflussnahme der Mathematik.³ Hegel nannte seine Dialektik auch dialektische Logik, um anzuzeigen, dass die formale Logik der Mathematik vorbehalten, die dialektische eine höhere, diese überformende Logik sei. Denn, und das sei der tiefere Grund, betrachte die Mathematik ihre Objekte immer als *identische*, als *widerspruchsfreie*, während seine Philosophie doch gerade postuliere, dass „alles an sich selbst widersprüchlich“ sei.

Diese Besonderheit den Hörern der Mathematik-Vorlesungen bereits zu Beginn mitzuteilen, erfolgt unter Hinweis auf das sogenannte *Identitätsaxiom*, etwa $A = A$. Es scheint trivial. Es handelt sich um die Ankündigung, dass nunmehr, beim Eintritt in die heiligen Hallen der Mathematik, alle Objekte als unveränderlich betrachtet werden. Gegenstände, Relationen oder funktionale Abhängigkeiten, die diesem Axiom nicht genügen und sich innerhalb der mathematischen Behandlung verwandeln, verlieren ihren Anspruch auf formale Wahrheit, garantiert durch das Regelwerk der formalen Logik, die sich ebenfalls auf dieses Axiom stützt.

Elektrodynamik – Naturwissenschaft wird theoretisch

Noch zu Hegels Lebzeiten entstehen die Vorarbeiten der Elektrodynamik, jene Naturwissenschaft, die in verblüffender Weise dem Hegelschen Paradigma folgt. Als der dänische Physiker Oersted im Jahre 1820 per Zufall zwischen dem elektrischen Strom und einer Magnetsnadel eine Wirkung feststellt⁴, beginnt ein neuer Typ von Naturwissenschaft. Die Nachricht macht schnell die Runde, und viele Forscher beginnen mit eigenen Untersuchungen dieses Phänomens.

Zehn Jahre später, nach einer langen Reihe experimenteller Untersuchungen im Keller der Royal Society in London, formuliert der englische Physiker Faraday das Prinzip der elektromagnetischen Induktion. Jetzt kommt es zur Begegnung der Dialektik mit der physikalischen Wissenschaft.⁵ Die Elektrizität und der Magnetismus bilden zwei Phänomene, die sich in mancherlei Hinsicht, etwa darin, dass sie beide Felder aufbauen, die völlig unsichtbar sind und sich auch im leeren Raum ausbreiten, ähnlich verhalten und die darüber hinaus eine geheimnisvolle Wechselwirkung besitzen. Indem Faraday die beiden Felder bzw. ihre materiellen Träger wie Spule und Stabmagnet in eine räumliche Bewegung zueinander versetzt, entsteht ein elektrischer Strom. Um diesen Strom wird es künftig gehen, und mit seiner Erklärung öffnet sich die Tür zur theoretischen Wissenschaft. Ihr jeweiliges Feld aufzubauen, vermögen der elektrische Strom wie auch das Magneteisen allein – einen elektrischen Strom zu erzeugen, gelingt ihnen nur *gemeinsam* und mit Hilfe einer *relativen Bewegung*.

Noch während der Dauer seiner weiterführenden Versuche trifft Michael Faraday in den 1850er-Jahren auf den schottischen Mathematiker James Clark Maxwell, und zusammen entwickeln sie die physikalische wie mathematische Theorie der elektromagnetischen Felder resp. die Elektrodynamik. Als Ergebnis der Arbeit beider Forscher entstehen die Maxwellschen Gleichungen. Wenngleich Faraday und Maxwell die Elektrodynamik im Alleingang entwickelten, revolutionierten sie die Naturwissenschaften und begründeten einen neuen Typ, die mathematische Physik, und schufen weiterhin den Ausgangspunkt für die Einsteinsche Relativitätstheorie.⁶

Mathematik im Wandel

Hegel hat der Mathematik lediglich das bescheinigt, was sie nicht war und nicht sein konnte: konstruktiver Bestandteil seiner (dialektischen) Philosophie. Aber auch die Mathematik erlebt eine bedeutsame Veränderung. Einige Jahrzehnte nach Hegels Tod beginnen insbesondere in Deutschland Diskussionen um eine Erweiterung und Präzisierung einiger zentraler Begriffe und weiten sich aus zu einem handfesten Grundlagenstreit. Ausgangspunkte bilden die *reellen Zahlen* und die *Unendlichkeit*, die aus ihrer intuitiven Unschärfe herausgeführt werden sollen. Als neue Basis der Mathematik gilt fortan die *axiomatische Mengenlehre*. Einer ihrer Begründer ist Georg Cantor, dem allerdings heftige Kritik entgegenschlägt. Sein prominenter Kollege Henri Poincaré fordert gar, die Cantorsche Lehren „zu verbieten“. Durch die Grundlagendiskussion, die in den 1870er Jahren begann und bis in die 1930er-Jahre andauerte, hat sich die Mathematik endgültig als ein reiner, nunmehr umfassend begründeter Formalismus konstituiert und ihre *Freiheit* durch das Abwerfen der noch bestehenden intuitiven Verbindungen zu dinglichen oder konkreten Objekten der Wirklichkeit vollzogen. Auch eine weit reichende und in vielerlei Hinsicht bis heute anhaltende Kontroverse um durchaus tiefe theoretische Probleme erfährt eine erste Auflösung. Es geht um das *tertium non datur*, jene axiomatische Forderung, nach welcher es ein Drittes zu zwei sich ausschließenden Aussagen nicht geben kann. Lässt sich aus einer (falschen) Annahme, die in der folgenden mathematischen Beweis-

führung widerlegt wird, die Gültigkeit des Gegenteils und ggf. dessen mathematische Existenz folgern? Am Ende setzte sich die Auffassung der sogenannten Formalisten um den bedeutenden Mathematiker David Hilbert (1862-1943) durch.

Damit ändert sich das Verhältnis der Mathematik zur Hegelschen Philosophie; beide geraten in einen dialektischen Widerspruch – erst ihre miteinander vermittelte Existenz vermag die theoretische Disziplin der Elektrodynamik im Sinne einer die innere Dynamik modellierenden Mathematik zu vollenden. Dabei entsteht sogar die Verknüpfung zweier dialektischer Widersprüche: Bildet die räumlich-zeitliche Durchdringung der beiden Felder den ersten, so wird dieser selbst zum Ausgangspunkt eines weiteren mit der Mathematik. Es geht um die Verbindung des konkret-physikalischen Modells mit einer abstrakt-mathematischen Struktur, welche die innere Dynamik adäquat darzustellen in der Lage ist. Die Freiheit der Mathematik zeigt sich in ihrer potentiell unbegrenzten Fähigkeit der mathematischen Modellierung fachspezifischer Verhältnisse.

Zur Aneignung der Natur

Hegel und andere Vertreter des Deutschen Idealismus hatten sich sehr mit der Naturphilosophie beschäftigt. Nun aber standen sie vor den sich in den Vordergrund drängenden neuen Naturwissenschaften. In England bewegten sich bereits tausende von Dampfmaschinen nach dem von James Watt entwickelten Prinzip, und der Nationalökonom Adam Smith hatte bereits 1776 die erste tiefeschürfende Abhandlung⁷ über das neue Prinzip des kapitalistischen Wirtschaftens vorgestellt. Nun galt es, sich der Natur erneut zuzuwenden und die Frage grundsätzlich und modern zu stellen. Im Vordergrund der Naturwissenschaften stand nicht mehr die Nutzung von Substanzen wie etwa Holz oder fossilen Energieträgern wie Kohle oder Koks zur Produktion von Eisen, auch nicht die Verwandlung manueller Tätigkeiten in maschinelle Operationen, sondern die Aneignung von Natur durch die Ausnutzung ihrer Geheimnisse. Sowohl der elektrische Strom als auch der Magnetismus waren, wenngleich nicht ohne weiteres, nutzbare Bestandteile der Natur. Ihre technische oder gar industrielle Nutzung erforderte in erheblichem Maße die Verbindung experimenteller Erkenntnisse mit theore-

tischen Konzepten. Was in der ersten Phase der Industrialisierung der massenhafte Einsatz vieler fleißiger Hände bewirkte, verwandelte sich bereits zur Zeit der Dampfmaschine in eine Aufgabe für Techniker. Die Elektrodynamik erforderte sogar den Wissenschaftler. Die Aneignung der Natur hatte große Umwege zu gehen, vereinigte viele unterschiedliche Qualifikationen, die Stätten der Produktion von elektrischen Generatoren wie Motoren wuchsen zu großen Fabriken. Was mit der Dampfmaschine begonnen hatte, wuchs ebenfalls ins Riesenhafte: das zur Finanzierung benötigte Kapital konnte nur noch von einer großen Zahl mehr oder weniger Vermögenden aufgebracht werden. Es entstand der Unternehmenstyp der Aktiengesellschaft. Die Aneignung der Natur, jetzt durch die Enthüllung und Nutzung ihrer Geheimnisse, hatte sich in eine weltweit verbreitete Industrie verwandelt. Ihr nach wie vor betriebener Zweck, über die Verwertung der Geheimnisse die großindustrielle Produktion von Profit zu befördern, war ohne weiteres nicht mehr erkennbar. Die erfolgreiche Bearbeitung des großen Themas wechselte auf Initiative des zupackenden deutschen Industriekapitals in wenigen Jahrzehnten von England nach Deutschland. Es entstanden weltumspannende Unternehmen wie Siemens, AEG und bald auch General Motors in den USA.

Nachkriegsthemen

Die Betrachtung macht einen großen Sprung, hinweg über die Gründung des Deutschen Kaiserreiches im Jahre 1871 und den Ersten Weltkrieg. Die Welt kommt nicht zur Ruhe. Erneut stehen die Zeichen auf Sturm. In Deutschland wie in Japan stemmen sich die herrschenden Klassen gegen ihren befürchteten Niedergang – vergeblich. Die Kapitulation Deutschlands 1945 verkehrt die bisherige Dominanz aller europäischen Großmächte in ihr Gegenteil. Sie werden zu nachgeordneten Staaten in dem nun beginnenden amerikanischen Zeitalter. In diesem Sinne handelt es sich bei der Systemtheorie und der Künstlichen Intelligenz im Wesentlichen um Adaptionen US-amerikanischer Paradigmen. Bekannt geworden ist die aus biologisch-medizinischen Ansätzen entstandene *Allgemeine Systemtheorie* oder auch *General System Theory*. Ihr Anspruch auf Allgemeingültigkeit äußert sich in ihrer behaupteten Eignung für eine Vielzahl von Themen – bis hin zur Modellierung komplexer ökonomischer Beziehungen.

Wolfgang Krieger



Wolfgang Krieger (geb. 1946) ist Diplom-Ingenieur (FH) in der Regelungstechnik und Diplom-Mathematiker (mit einer Diplomarbeit über algebraische Systemtheorie). Nach Tätigkeiten als Entwicklungsingenieur bei der Fa. Nixdorf und in Logistik-Projekten in Frankfurt und in Bremen u. a. für die Bremer Hafentelematik hat er sich ab 2000 einen großen Teil seines Berufslebens mit dem Entwurf und der Realisierung von Expertensystemen und der Künstlichen Intelligenz beschäftigt. Er war u. a. Projektleiter und Mitautor des modellbasierten Diagnosesystems ROSE (Reasoning Over Systems in their Entirety). Nach der Berufstätigkeit hat er sich mit philosophischen und wissenschaftstheoretischen Themen beschäftigt, was 2022 zur Promotion über Hegelsche Dialektik und das Problem der Formalisierung im Fachbereich Mathematik/Informatik der Universität Bremen führte.

Diese Arbeit weist nach, dass die unterlassene Modellierung der inneren Dynamik dieser und anderer Varianten der Systemtheorie den Zugang zur gesellschaftlichen Lebendigkeit verunmöglicht, der sie doch ihre behauptete Relevanz verdanken.⁸

Was Hegel auf der Ebene der Philosophie als Widerspruch von *Wesen und Erscheinung* formuliert, erhält bei Marx eine Konkretisierung in Gestalt der *Produktions- und Zirkulationssphäre*. Die behauptete Widerspruchsfreiheit der Systemtheorie entsteht lediglich durch Verengung des betrachteten Gesellschaftsschnitts auf die Zirkulationssphäre und begeht damit einen unzulässigen Verzicht auf die Sphäre der Produktion – das Modell ist unwirklich, es ist nicht von dieser Welt.

Künstliche Intelligenz

Nach einer wechselvollen Geschichte, die im Jahre 1956 in den USA beginnt und bis in die aktuelle Gegenwart reicht, erfährt die *Artificial Intelligence* (AI) in diesen Jahren ihre Wahrheit. Während der zurückliegenden Zeit erhielt sie in den meisten fortgeschrittenen Ländern durchgängig erhebliche, wenngleich schwankende und an Erfolgen unterschiedlicher Art geknüpfte staatliche Förderungen. Ihre oft beklagte Orientierungslosigkeit wurde dadurch nicht verringert, sondern eher befördert.

Die fehlende Dynamik und allgemein-gesellschaftliche Orientierung sowie das Fehlen einer Theoriebildung, so die Untersuchungsthese, sind verursacht durch die alleinige Existenz der Seite der formalen Strukturen, denn sämtliche bisher erzeugten Funktionalitäten bestehen aus Software oder Informations- wie Gerätetechnik. Sie gehören zur Sphäre des Formalen, repräsentieren keine lebendige Dynamik und besitzen keinen Zugang zu konkreten gesellschaftlichen Prozessen.

Die Rekonstruktion des Widerspruchs von Dialektik und Formalen führt auf die Nicht-Existenz des dynamischen, konkreten wie auch dialektischen Aspekts. Woher kann dieser kommen? Indem ein anderer Akteur ohne eigene bzw. mit lediglich abgeleiteter Dynamik diese Funktion ‚treuhänderisch‘ wahrnimmt. In allen Staaten mit einer relevanten KI-Disziplin leistet dies das Wissenschafts- oder Technologiebudget der staatlichen Haushalte. Die *eigentliche* Dynamik erfordert aber die Initiative eines gesellschaftlichen resp. kapitalistischen Akteurs. Bis dahin blieben die vielfältigen (software-)technischen Konstrukte recht orientierungslos.⁹ Dies änderte sich im Jahre 2019: Die in den USA ansässigen Digitalunternehmen der *Big Five* (Google, Apple, Microsoft, Amazon und Meta) boten in Kooperation mit Beratungsunternehmen natürlichsprachige Testversionen des aktuell allseits diskutierten KI-Systems *ChatGPT* an. Es handelt sich um das erste alltagstaugliche und am Markt erhältliche Produkt der *Open AI Foundation*, welches mittlerweile von *Microsoft* betrieben wird.

Die Simulation von Künstlicher Intelligenz, und nur darum geht es – mittlerweile ist die Erzeugung von graphischen Objekten nach demselben Verfahren zu einem weiteren Bestandteil geworden – hat einen ersten spektakulären funktionalen wie gesellschaftspolitischen Durchbruch erzielt.

Fazit

Die Hegelsche Dialektik, unter dem Eindruck der Aufklärung und der Vernunft als idealistische, das heißt die Wirklichkeit als Produkt des Geistes unterstellend, erfährt ihre Verwandlung in eine materialistische, den experimentell erforschten widersprüchlichen Verhältnissen der Natur „entwendeten“ Form.

Gut 150 Jahre später löst die Initiative mehrerer bedeutender Unternehmen des digitalen Finanzkapitals die Entwicklung des Systems ChatGPT aus. Ein fast unendlich großes Budget, ein uneingeschränkter Marktzugang wie auch eine nahezu monopolartige Kontrolle über Milliarden digitaler Dialoge sichern den politischen wie wirtschaftlichen Erfolg. In ihm manifestiert sich die Funktion des lange gesuchten dynamischen Akteurs und Partners bedeutsamer KI-Technologien. Das internationale Finanzkapital US-amerikanischer Herkunft verwirklicht sein eigenes Wesen als *virtuelle Simulation* einer künstlichen und von einer natürlichen nur schwer unterscheidbaren Intelligenz.

Anmerkungen

- 1 Die Auffassung, Dialektik sei lediglich das Prinzip des korrekten Umgangs mit widersprüchlichen Aussagen innerhalb der Dispute in der griechischen Polis, ist so irrig wie verbreitet.
- 2 G.W.F. Hegel 1807, *Phänomenologie des Geistes*.
- 3 G.W.F. Hegel, ebd.: „Die Philosophie kann sich ihre Methode nicht von einer untergeordneten Disziplin wie der Mathematik borgen“, S. 44.
- 4 H.C. Oersted, dänischer Physiker u. Chemiker in Kopenhagen, macht 1820 die überraschende Entdeckung, dass Elektrizität und Magnetismus keine voneinander unabhängigen Naturerscheinungen, sondern auf besondere Weise verbunden sind.
- 5 G.W.F. Hegel 1830: „Wir machen sie, die eine andere ist als wir, zu einem anderen, als sie ist.“ S. 17
- 6 Albert Einstein [1905] Über die spezielle wie allgemeine Relativitätstheorie. Braunschweig 1970, „Letztere ist vielmehr aus der Elektrodynamik herausgewachsen . . .“ S. 36
- 7 Adam Smith [1723-1790] „An Inquiry into the Nature and Causes of the Wealth of Nations“, das am 9. März 1776 erschienene Werk des schottischen Ökonomen gilt als erstes grundlegendes Werk der Wirtschaftswissenschaften bzw. der mit ihm beginnenden Nationalökonomie.
- 8 Insbesondere die darauf fußende ökonomische Modellbildung musste ihre Unfähigkeit zur Erklärung wie zur Prognose von Wirtschafts- und Finanzkrisen bei jedem dieser Ereignisse eingestehen (vgl. dazu [Josef Vogl, *Das Gespenst des Kapitals*, Zürich 2012]). Darin wird die Black-Scholes-Differentialgleichung genannt (vgl. dazu die Arbeit von Kruschwitz / Stefanova 2007). Bei Black und Scholes wird der Aktienkurs als geometrische Brownsche Bewegung modelliert (https://www.wiwiw.fu-berlin.de/fachbereich/bwl/pruefungs-steuerlehre/kruschwitz/forschung/veroff/103_-BSFUNDI_1302.pdf).
- 9 Die Open AI Foundation wurde 2016 von einer Handvoll US-amerikanischer Milliardäre gegründet und befindet sich heute im überwiegenden Besitz von Microsoft resp. Bill Gates und seinen Stiftungen. Diese Unternehmen sind einer der Hauptsponsoren und besitzen die Rechte an der Vermarktung von ChatGPT der Version 3. Eine End-User-Lizenz wird seit 2023 für 20 € / mtl. angeboten.

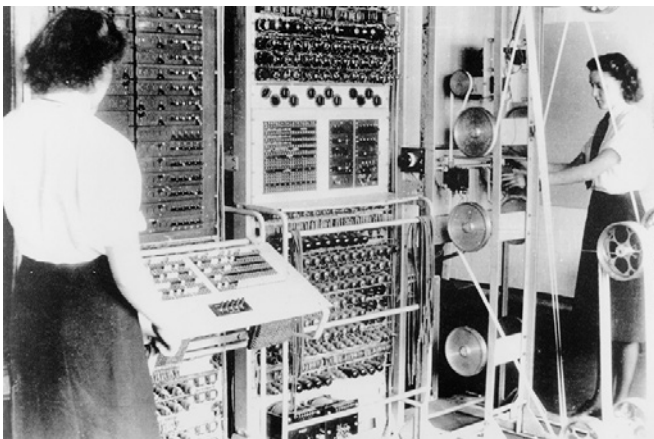
Die militärische Seite der Digitalisierung

Dieser Artikel ist ein Nachdruck aus dem Ausdruck Juni 2/2023 der Informationsstelle Militarisation mit deren freundlicher Genehmigung. Er ist also für Leser:innen weit über die Informatik hinaus verfasst, aber hoffentlich dennoch auch im engeren fachlichen Kontext interessant.

Mit *Digitalisierung* wird üblicherweise ein schon Jahrzehnte anhaltender globaler Prozess bezeichnet, bei dem es sich um den immer noch wachsenden Einsatz von Informations- und Kommunikationstechnik, digitaler Vernetzung, Algorithmisierung, Mediatisierung, Roboterisierung und in letzter Zeit zusätzlich um die Anwendung Künstlicher Intelligenz in nahezu allen gesellschaftlichen Bereichen handelt. Die Digitalisierung hat ihren Ausgangspunkt in der Entwicklung der ersten Computer im Zuge des 2. Weltkriegs und den Jahren danach in Deutschland, Großbritannien und vor allem in den USA, die in enger Verbindung zum militärischen Komplex stattfand. Die ersten Jahrzehnte waren stark vom Geld und von den Anforderungen der Militärs geprägt. Aber auch seitdem der zivile Bereich, beginnend in den 1970er- und 1980er-Jahren, insbesondere durch die allmähliche, aber unaufhaltsame Verbreitung von PCs, Notebooks, Laptops, Tablets und schließlich von mobilen Geräten und durch die immer umfassenderen Anwendungen in Wirtschaft, Verwaltung, Bildung und Wissenschaft die Digitalisierung klar dominiert, ist die Verflechtung mit dem Militärwesen nicht verschwunden, sondern ein weiterhin bestimmender Faktor.

Am Anfang war der Krieg

Konrad Zuse hat 1941 mit der Z3 den ersten funktionsfähigen Digitalrechner vorgestellt. Seine Arbeit wurde von der Rüstungsindustrie und staatlichen Stellen gefördert. Als Gegenleistung hat er einen Spezialrechner für die Optimierung der Flügелеinstellungen von Gleitbomben gebaut. Die Computerentwicklung in Großbritannien ist eng mit dem Namen Alan Turing verbunden, der in Bletchley Park an der Entschlüsselung des deutschen Nachrichtenverkehrs mitgewirkt hat. Dafür wurde u. a. der ab 1943 eingesetzte Röhrencomputer *Colossus* entwickelt.



Colossus Mark II hier bedient von den beiden „Wrens“ Dorothy Du Boisson (links) und Elsie Booker (1943). Quelle: The National Archives (United Kingdom), catalogued under document record FO850/234

Entscheidend aber waren mehrere Entwicklungen in den USA. So wurde beispielsweise ab 1942 im Auftrag der US-Armee der Röhrencomputer *ENIAC* für die Berechnung ballistischer Tabellen gebaut. Solche Tabellen wurden zu Hunderten benötigt, und für jede einzelne musste eine Schar von vor allem Rechnerinnen tagelang arbeiten, was mit *ENIAC* tausendmal schneller ging. Eine Parallelentwicklung im Auftrag der US-Marine ab 1945 war *Whirlwind*. Ursprünglich für Flugsimulation gedacht, wurde es später im *SAGE*-System eingesetzt, das erste computergestützte Luftverteidigungssystem. Weitere Durchbrüche gelangen durch die Erfindung der Transistoren, die die ausfallanfälligen Röhren ersetzten, und der integrierten Schaltungen, die eine lange Phase der Miniaturisierung und Verkürzung der Rechenzeiten einläuteten. Das kulminierte von 1980 bis 1990 im Milliarden-schweren *Very High Speed Integrated Circuits program (VHSIC)* des US-Verteidigungsministeriums. Ziel war, die Grenzen zu verschieben, die die Hardware den militärischen Systemen setzte.¹

Softwarekrise

Bei der Entwicklung großer Softwaresysteme, wie sie insbesondere für militärische Anwendungen in den 1950er und 1960er Jahren gefordert waren, stellte sich bald heraus, dass sie häufig viel teurer wurden als geplant, dass das Projektmanagement nicht klappte und dass die Zuverlässigkeit erheblich zu wünschen übrigließ. Während die Hardware kontinuierlich verbessert wurde, wurden die Softwareprobleme immer größer. Es gab ab den späten 1960er- und vor allem in den 1970er- und 1980er-Jahren zwei große Anstrengungen, diese sogenannte Softwarekrise zu beheben, bei denen die im Entstehen begriffene wissenschaftliche Disziplin der Informatik um Mithilfe gebeten wurde. Zum einen setzte das US-amerikanische Verteidigungsministerium die Entwicklung der Programmiersprache ADA in Gang, die mehrere hundert bis dahin benutzte Programmiersprachen ersetzen sollte.² Zum anderen lud die NATO zu mehreren internationalen Konferenzen ein, auf denen das inzwischen ganz zentrale Fachgebiet der Softwaretechnik aus der Taufe gehoben wurde mit dem Ziel methodisch fundierter Systementwicklung. Die Einführung von ADA im Laufe der 1980er-Jahre hat zwar zu einer erheblichen Reduktion des (Programmier-) Sprachwirrwars geführt, und ADA wird bis heute in sicherheitskritischen, vor allem auch militärischen Bereichen verwendet, der erhoffte durchschlagende Erfolg ist aber ausgeblieben. Im Laufe der 1980er-Jahre wurde vom US-amerikanischen Verteidigungsministerium auch noch ein weiteres Großprojekt aufgelegt, das in den ersten vier Jahren ein Budget von über 140 Mill. US-Dollar hatte: *Software Technology for Adaptable Reliable Systems program (STARs)*³. In der Softwaretechnik hat es erhebliche Fortschritte gegeben, wobei der immense Bedarf an Softwareentwicklung im zivilen Bereich mitausschlaggebend war. Die Softwareprobleme sind allerdings nicht verschwunden, denn die Anforderungen an Software ist sowohl militärisch als auch zivil eher noch stärker gewachsen als der methodische Fortschritt.

Aufrüstung zum Informations- und Cyberkrieg

Krieg zu führen geht weit über Töten und Zerstören durch Waffeneinsatz hinaus. Krieg ist ein komplexes Organisationsmonster, zu dem Aufklärung und Geheimhaltung, Propaganda, Spionage und Sabotage, Kommando, Kontrolle und Kommunikation gehören. Durch die Digitalisierung sind die Mittel und Möglichkeiten in all diesen Bereichen erheblich gewachsen. Fast alle Länder der Welt haben Cyberkriegseinheiten gebildet, die Konzepte und Programmsysteme entwickeln, wie man Falschmeldungen streut, um breit angelegte Desinformationskampagnen zu starten, wie man Gegner (und oft auch Verbündete) ausspioniert und wie man kritische Infrastrukturen ausschaltet bis hin zur Zerstörung technischer Einrichtungen. Die jüngsten Enthüllungen eines Recherche-Netzes des ZDFs, der Süddeutschen Zeitung, des Spiegels u. a. zeigen, wie das IT-Unternehmen *NTC Vulkan* zusammen mit russischen Geheimdiensten im großen Maßstab Cyberkrieg plant. Explizit genannt sind das Lahmlegen von Kontrollsystemen von Eisenbahn-, Luft- und Schiffstransport und die Störung von Energieunternehmen. Wenn auch diese *Vulkan Files* ziemlich erschrecken, muss man bedenken, dass nicht nur Russland in diesem Bereich aufrüstet. So hält die NATO schon seit vielen Jahren jährliche Manöver ab, bei denen offensiv und defensiv ähnliche Cyberkriegsszenarien geübt werden. Dass es sich dabei nicht nur um Planungen handelt, zeigt eine lange Liste von Cyberangriffen mit gravierenden Auswirkungen. Dass zivile Infrastrukturen durch Cyberattacken besonders gefährdet sind und sie als bevorzugte Ziele gelten, ist kriegsvölkerrechtlich im höchsten Maße bedenklich. Die NATO ist sich dessen auch voll bewusst. Sie hat eine Studie zur Anwendung des Kriegsvölkerrechts auf Cyber-Konflikte und Cyberkrieg in Auftrag gegeben, an der seit 2009 rund 20 Fachleuten am *NATO Cooperative Cyber Defence Centre of Excellence* in Tallinn gearbeitet haben.⁴

Künstliche Intelligenz im Kriegsdienst⁵

1956 trafen sich zwölf junge Wissenschaftler für mehrere Wochen und hoben das Gebiet der *Künstlichen Intelligenz* (KI) aus der Taufe. Erklärtes Ziel war, kognitive Fähigkeiten wie Sehen und Erkennen, Hören und Verstehen, Planen und Entscheiden sowie Problemlösen mit Hilfe von Computerprogrammen zu simulieren. Das fand seine Grenzen aber insbesondere in der damals noch sehr begrenzten Speicherkapazität und Rechengeschwindigkeit. Dennoch hat das US-Verteidigungsministerium prinzipiell das militärische Potenzial der KI erkannt und 1983 die *Strategic Computing Initiative (SCI)* gestartet⁶, wobei drei Aufgaben im Zentrum standen: ein Sprachassistent für die Piloten der Luftwaffe, ein Schlachtenmanagementsystem für die Ma-

rine und autonome Landfahrzeuge für das Heer. SCI war auf zehn Jahre angelegt und hatte einen für damalige Verhältnisse gigantischen Finanzrahmen von fast einer halben Milliarde US-Dollar. Da sich keine schnellen Erfolge abzeichneten, wurde das Programm noch vor dem Ende gekürzt. Dennoch muss SCI wohl als Ausgangspunkt einer beispiellosen Entwicklung der KI gesehen werden. Inzwischen hat die Verarbeitung von Sprache und Text ein unglaubliches Niveau erreicht genauso wie die Verarbeitung von Bildern, wie sie insbesondere für das eigenständige Navigieren von Fahrzeugen benötigt wird. Und Managementsysteme sind inzwischen weit verbreitet. Dabei ist festzuhalten, dass sich die Ziele und auch die Methoden seit den Anfängen der KI gar nicht allzu sehr verändert haben, aber der heute verfügbare Speicherplatz und die Rechengeschwindigkeit erlauben solche Anwendungen.

Während sich unbemenschte Land- und Wasserfahrzeuge auch nach Jahrzehnten intensiver Entwicklung immer noch in einer Art Pilotphase befinden, sind die entsprechenden fliegenden Systeme bereits seit 20 Jahren im Einsatz. Angefangen hat es mit Aufklärungsdrohnen, die feindliches Gebiet überfliegen und ausspionieren können. Es hat dann nicht lange gedauert, bis solche Drohnen mit Raketen ausgestattet wurden. Vorreiter waren Israel und die USA. Inzwischen sind Killerdrohnen weit verbreitet, und es gibt sie in einer breiten Palette von klein bis groß und von billig bis teuer. Zu den Herstellerstaaten gehören u. a. China, Iran, Russland und die Türkei. Mehrere Dutzend Staaten haben diese Waffen angeschafft und setzen sie teilweise auch bereits ein. Nachdem es Tausende Einsätze in Afghanistan, Pakistan, Jemen und andernorts in eher asymmetrischen Kriegen mit vielen Ziviltoten gegeben hat, zeigt der Krieg in der Ukraine, dass bewaffnete Drohnen auch eine Rolle spielen, wenn zwei Armeen gegeneinander kämpfen. Aufklärungs- und Killerdrohnen sind Waffensysteme, die es ohne Digitalisierung nicht gäbe, weil sie programmgesteuert fliegen und vor allem weil sie ihre Ziele mithilfe digitaler Bildverarbeitung finden. Der nächste Entwicklungsschritt, an dem intensiv gearbeitet wird, ist die vollständige Autonomie, bei der dann die Bordsysteme auch über den Waffeneinsatz entscheiden. In Politik und Militär sind autonome Waffen aus ethischer und kriegsvölkerrechtlicher Sicht nicht unumstritten, ein Verbot ist dennoch nicht absehbar.⁷

Die Cyberpeace-Kampagne

Die Gründung des *Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung* (FIfF) 1984 auf dem Höhepunkt der Friedensbewegung war eng verbunden mit dem NATO-Doppelbeschluss zur Nachrüstung mit Mittelstreckenraketen in Eu-



Hans-Jörg Kreowski

Hans-Jörg Kreowski (Jahrgang 1949) ist Professor (i. R.) für Theoretische Informatik an der Universität Bremen. Er ist Mitglied im Vorstand des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) und vertritt das FIfF im Vorstand der Zeitschrift *Wissenschaft und Frieden*. Er ist Mitglied der Leibniz-Sozietät der Wissenschaften zu Berlin, wo er zusammen mit Wolfgang Hofkirchner in Wien den Arbeitskreis *Emergente Systeme, Information und Gesellschaft* organisiert. Von 2019 bis 2022 war er außerdem Mitherausgeber des *Grundrechte-Reports*.

ropa und hing zusammen mit der Kampagne verschiedener insbesondere universitärer Friedensinitiativen *Informatiker warnen vor einem Atomkrieg aus Versehen*. Die unheilvolle Verquickung von Rüstung und Informatik war fortan bestimmendes Thema im FIF, anfangs getragen von einem äußerst aktiven Arbeitskreis. Einen besonderen Schub hat die Thematik 2013 bekommen, als das FIF die *Cyberpeace*-Kampagne startete. Edward Snowden hatte gerade durch seine Enthüllungen einer breiten Öffentlichkeit offenbart, dass die NSA (und ähnlich andere Geheimdienste) weltweit die digitale Kommunikation ausspionieren. Das FIF wollte darauf aufmerksam machen, dass die Problematik nicht nur Grund- und Menschenrechte unterminiert, sondern dass mit ganz ähnlich gelagerten Methoden auch massiv zum Cyberkrieg gerüstet wird. *Cyberpeace* war gedacht als Gegenkonzept. Die Kampagne umfasste vor Corona eine Vielzahl von Publikationen, Veranstaltungen und Aktionen. Eine besondere Errungenschaft wurde durch Fördermittel der *bridge*-Stiftung möglich: In Zusammenarbeit mit dem Motionensemble entstand 2017 das Video *Cyberpeace statt Cyberwar*, das bei vimeo oder youtube angesehen werden kann. Ein Kern der Kampagne war die Entwicklung von 14 Forderungen an die Politik, zu denen eine rein defensive Sicherheitsstrategie durch Verbot von Offensivwaffen für den Cyberkrieg und eine digitale Genfer Konvention mit dem Verbot von Cyberangriffen auf lebenswichtige Infrastrukturen wie Strom-, Wasser-, Gesundheitsversorgung etc. gehört. Es geht um die ausschließlich zivile Nutzung des Internets und aller digitalen Medien.⁸ Da die Thematik nichts an Aktualität und Brisanz eingebüßt hat, hat das FIF begonnen, der *Cyberpeace*-Kampagne neuen Schwung zu verleihen. Wer mitwirken möchte, ist herzlich willkommen.

Anmerkungen

- 1 Näheres dazu siehe "The History of the Integrated Circuit". Nobelprize.org. Nobel Media AB 2014. Web. 29 Jun 2018.
- 2 Näheres dazu siehe [de.wikipedia.org/wiki/Ada_\(Programmiersprache\)](https://de.wikipedia.org/wiki/Ada_(Programmiersprache)).
- 3 Näheres dazu siehe Larry F. Druffel, Samuel T. Redwine Jr. and William F. Riddle: *The DoD Stars Program*. Computer, vol. 16, no. 11, pp. 9-11, 1983. doi: 10.1109/MC.1983.1654232.
- 4 Das *Tallinn Manual* erschien 2013 und *Tallinn 2.0* 2017, beide bei Cambridge University Press. Während es in Teil 2 um Einzeloperationen geht, behandelt Teil 1 massivste Cyber-Operationen in bewaffneten Konflikten oder bei verbotenen Gewalteinsetz in internationalen Beziehungen.
- 5 Für eine ausführliche Darstellung des Themenkomplexes siehe Hans-Jörg Kreowski und Aaron Lye (Hrsg.): *Künstliche Intelligenz zieht in den Krieg*, Schwerpunkt. FIF-Kommunikation 4/2021, S. 28-30 und Dossier 93, Beilage zu Wissenschaft und Frieden 4/2012.
- 6 Näheres dazu siehe Alex Roland and Philip Shiman: *Strategic Computing – DARPA and the Quest for Machine Intelligence, 1983-1993*. The MIT Press 2002.
- 7 Zu militärischen, völkerrechtlichen und wissenschaftlichen Aspekten autonomer Waffensysteme siehe Andrew P. Williams and Paul D. Scharre (Eds.): *Autonomous Systems – Issues for Defence Policymakers*. NATO Headquarters Supreme Allied Commander, Transformation, Norfolk, Virginia, United States.
- 8 Detaillierte Informationen zur *Cyberpeace*-Kampagne findet man auf der Webseite cyberpeace.fif.de.

Wissenschaft & Frieden 2/2023

Klimakrise

Gewalt – Widerstand – Transformation

Die Klimakrise stellt Gesellschaften weltweit vor existentielle Herausforderungen. Einerseits verschärfen sich Verteilungskonflikte um immer knapper werdende Ressourcen und andererseits verschärfen Kriege und gewaltsame Konflikte die Dynamik der Klimakrise. Die fortgeführte Ausbeutung der natürlichen Ressourcen geht einher mit einer Vielzahl an lokalen Konflikten und Gewalt; der Widerstand vor Ort wächst jedoch und ist global vernetzt und Optionen für die sozial-ökologisch-ökonomische Transformation stehen zur Verfügung. Die Autor:innen des Heftes zeichnen Gewalt in der Klimakrise nach, analysieren gelebte Widerstandspraktiken und fragen nach globalem solidarischen Handeln – für eine nachhaltig friedliche Transformation.

Mit Beiträgen von Rebecca Froese, Janpeter Schilling, Jürgen Scheffran, Juliana Krohn und weiteren.

Weitere Beiträge im Heft: Nennstiel – „Neue“ Pazifismen? | Birkenbach – Dennoch friedenslogisch Handeln! | Driedger – Territorialität im Russland-Ukraine-Krieg

W&F 2/23 | Mai | 72 Seiten | 12 € (druck) / 9 € (ePUB+PDF)
als Einzelheft oder im Abonnement
www.wissenschaft-und-frieden.de



40 Jahre W&F

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

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



Stefan Hügel

BigBrotherAwards 2023

Auch im letzten Jahr gab es wieder reichlich Ereignisse, die einen BigBrotherAward verdient hätten. Wie immer fassen wir die Preisverleihung zusammen: Wer hat es in den erlesenen Kreis der Preisträger:innen geschafft?

Wir fassen in diesem einleitenden Beitrag des Schwerpunkts zum BigBrotherAward 2023¹ zunächst die Laudationes für die Preisträger:innen kurz zusammen. Danach drucken wir drei Laudationes ab: in den Kategorien *Behörden und Verwaltung*, *Kommunikation* und *Lebenswerk*.

Die Verleihung fand am 28. April 2023 in der Hechelei in Bielefeld statt.

Kategorie Behörden und Verwaltung

Der BigBrotherAward in der Kategorie *Behörden und Verwaltung* ging an das **Bundesfinanzministerium**, vertreten durch Bundesfinanzminister Christian Lindner,

für das seit dem 1. Januar 2023 geltende Plattformen-Steuertransparenzgesetz (PStTG).

Das Gesetz soll in der Plattformökonomie für Steuergerechtigkeit sorgen und zielt in erster Linie auf gewerbliche Portale wie Uber oder Airbnb. Es betrifft aber alle Menschen, die über Plattformen im Internet, wie eBay oder eBay-Kleinanzeigen private Verkäufe abwickeln. Laudator Peter Wedde – dessen vollständige Laudatio in dieser Ausgabe der *FlfF-Kommunikation* enthalten ist – erläuterte dazu:

Stellen Plattformbetreiber fest, dass jemand innerhalb eines Kalenderjahres die Zahl von dreißig Verkäufen und mehr als 2.000,00 € Gesamtumsatz auf ihrer Plattform erreicht, müssen sie die entsprechenden Daten automatisch an das Bundeszentralamt für Steuern übermitteln. Das ist die neue gesetzliche Meldeschwelle. Außerdem müssen diese Informationen nach der Übermittlung für zehn Jahre vorgehalten werden – sowohl von den Plattformbetreibern als auch von der Finanzverwaltung.

Und weiter:

Das Gesetz verlangt also eine zehnjährige doppelte Vorratsdatenspeicherung. Und das, obwohl für die meisten Privatverkäufe überhaupt keine Steuerpflicht besteht – selbst wenn sie die völlig willkürlich gesetzte Melde-

schwelle überschreiten. Eine enge und klare Begrenzung der beabsichtigten Verarbeitungszwecke dieser Vorratsdatenspeicherung, die datenschutzrechtlichen Vorgaben entsprechen würde, ist obendrein nicht erkennbar.

Natürlich sei es in Ordnung, dass beispielsweise Einkünfte aus dauerhaften Vermietungen über Airbnb versteuert werden müssen; ebenso Verkäufe professioneller Verkäufer über eBay. Das Gesetz verpflichte aber Plattformbetreiber, alle bei ihnen anfallenden Daten auszuwerten – um diejenigen herausfiltern zu können, die im Kalenderjahr mehr als dreißig private Online-Verkäufe getätigt und dabei mehr als 2.000,00 € eingenommen haben.

Erforderlich für die vom Gesetzgeber angestrebte Steuergerechtigkeit sei diese umfassende Vorratsdatenspeicherung nicht. Es wäre völlig ausreichend gewesen, die Verpflichtung zur Meldung von offenkundig einkommenssteuerpflichtigen Gewinnen zu verankern. Laudator Peter Wedde schließt:

Eine Vorratsdatenspeicherung, die weitgehend zweckfrei und für die betroffenen Personen intransparent bleibt, steht im Widerspruch zu den allgemeinen Grundsätzen in Art. 5 Abs. 1 DSGVO – wie der Nachvollziehbarkeit von Verarbeitungen, der Zweckbindung und der Datenminimierung.

Kategorie Finanzen

Frank Rosengart hielt die Laudatio in der Kategorie *Finanzen*. Dieser Preis ging an die **finleap connect GmbH**, vertreten durch die Geschäftsführerin Nicola Breyer und den Geschäftsführer Marco Jostes,

für den andauernden Versand von Kontowechsel-Briefen an falsche Empfänger.

Frank Rosengart erläuterte die Hintergründe:

Mit der Einführung der „Payment Services Directive“ der EU in der Version zwei (PSD2) wurde die Möglichkeit geschaffen, einem Dritten Zugriff auf die eigenen

Kontodaten zu gewähren. In der Folge kann man z. B. über Cloud-basierte Anbieter sein Konto managen, also Zahlungseingänge prüfen, Überweisungen tätigen etc. – lauter Sachen, die sich auch ohne Cloud mit einer guten Homebanking-Software auf dem eigenen PC erledigen lassen.

Bereits zuvor bestand die gesetzliche Verpflichtung der Banken, Kund:innen beim Kontowechsel zu unterstützen, z. B. bei der Umstellung von Einzugsermächtigungen. Dies wird gerne an ein anderes Unternehmen ausgelagert. Das Unternehmen finleap connect hat sich auf Anwendungen rund um besagte PSD2-Schnittstelle spezialisiert und bietet als Dienstleistung einen Kontowechsel-Service an:

Wenn diese Firma von der abgehenden Bank mit dem Kontowechsel-Service beauftragt wird, ruft finleap über die besagte PSD2-Schnittstelle die alten Kontoumsätze ab und filtert aus diesen die regelmäßigen Abbuchungen heraus.

Aus den Informationen über regelmäßige Abbuchungen versucht finleap dann automatisiert den entsprechenden Lastschriftempfänger herauszufinden und ihm per Brief die neue Bankverbindung mitzuteilen.

Und weiter:

Um den Kontowechsel-Service zu nutzen, müssen noch ein paar weitere Angaben gemacht werden, denn die Lastschrift-Empfänger ... benötigen natürlich genaue Informationen, welche Kundendaten nun geändert werden sollen. Also eine Kundennummer o. ä. – plus noch einige Daten, um glaubhaft zu machen, dass es wirklich der Kunde ist, der diese Änderung wünscht. Zum Beispiel das Geburtsdatum und natürlich die Anschrift. Mit all diesen Informationen ausgestattet, setzt finleap ein Schreiben auf – „Bitte ändern Sie meine Daten“ – und schickt es dem Lastschrift-Empfänger per Post zu. Das sieht dann so aus, als ob der wechselwillige Kunde dies selbst und eigenhändig getan hätte.

Hierbei kam es offenbar regelmäßig zu einem nicht nachvollziehbaren Versand von Kundendaten an falsche Adressaten, unter anderem an Digitalcourage:

Da der Versand an falsche Empfänger völlig zufällig zu sein scheint, ist davon auszugehen, dass es sich um ein größeres Problem handelt, dass also jeden Monat sehr viele Daten in falsche Hände geraten. Digitalcourage hat den Anbieter mehrmals auf dieses Problem hingewiesen.

Abschließend kommt Laudator Frank Rosengart zu der Bewertung:

Solche detaillierten Informationen aus den Irrläufer-Briefen sind Gold wert in der Hand von Kriminellen. Mit fremden Identitäten lässt sich viel Schaden anrichten für die Betroffenen. Warenbestellbetrug, gezielte Phishing-Attacken und ähnliches. Genug Details stehen in den

versendeten Briefen. Für die Betroffenen auf jeden Fall sehr ärgerlich.

Kategorie Kommunikation

Der BigBrotherAward in der Kategorie *Kommunikation* wurde von padelun angekündigt. Er wurde verliehen an **Zoom Video Communications, Inc.**,

die als US-Unternehmen Daten an Geheimdienste weiterleiten müssen, aber dennoch behaupten, DSGVO-konform zu sein. Zoom untersteht überdies chinesischer Kontrolle und Zensur, da relevante Teile der Entwicklung in China stattfinden.

Der Preis geht auch an alle Gruppen, insbesondere Menschenrechts- sowie Umwelt- und Klimaorganisationen, die Zoom einsetzen und damit ihre Teilnehmer:innen der Überwachung preisgeben, obwohl es freie und datenschutzfreundliche Alternativen gibt.

Aus „Zoom“ habe sich sogar schon ein Verb gebildet, so Laudator padelun:

Das Verb lautet „zoomen“ und hat die Bedeutung „unter Beobachtung der Geheimdienste verschiedener Länder und Firmen Geheimnisse ausplaudern und gleichzeitig sein komplettes Beziehungsnetzwerk offen legen.“ ... Zoom ist der Versuch, Menschen, die miteinander in einer Videokonferenz kommunizieren wollen, in den Strudel des Überwachungskapitalismus zu ziehen.

padelun stellt dazu fest:

Eine Firma wie Zoom, die in den USA ansässig ist, unterliegt dem Cloud Act, dem Patriot Act und dem FISA Act (Foreign Intelligence Surveillance Act). Und die bedeuten, dass eine in den USA ansässige Firma sämtliche Daten von Nicht-US-Bürger:innen an die dortigen Geheimdienste weitergeben muss. Ganz egal, wo die Server stehen, auf denen die Dienste laufen. Ganz egal, was für nette Versprechen in ihren Privacy-Bestimmungen stehen. Firmen dürfen Betroffene nicht einmal darüber informieren, wenn sie Daten weitergegeben haben.

Zoom unterhält bekanntermaßen gute Beziehungen zur Volksrepublik China. Dort sitzt die 700 Personen starke Entwicklungsabteilung. Ursprünglich war dort auch die Erzeugung kryptographischer Schlüssel ansässig, und es ist bekannt geworden, dass zum Teil Konferenzen über den Umweg China geroutet wurden. Außerdem sind Konferenzen aktiv zensiert worden, wenn in ihnen „Tian’amen-Platz“ (Platz des Himmlischen Friedens) angesprochen wurde.

padelun kritisiert auch die bedenkenlose Verwendung von Zoom durch politische Organisationen:

... damit diese hoch politischen Projekte, die sich auf Straßen festkleben, Braunkohlebagger besetzen, BigBrotherAwards vergeben und Seenot-Rettungen orga-



nisieren, ihre Beziehungen untereinander den Geheimdiensten der „Five Eyes“ gegenüber offenlegen müssen. Weil das angeblich sooo einfach ist und alles andere sooo kompliziert. Und nicht nur politische Projekte tun das. Auch Firmen, Forschungslabore, Regierungen – das Wort zoomen hat sich fast schon so fest etabliert wie das Wort googeln.

Und es ist wirklich wie mit der Legende, Mädchen seien schlecht in Mathe: Sag den Menschen, B ist ganz kompliziert und funktioniert nie und dass sie das sowieso gar nicht können, weil sie inkompetent sind. Sag ihnen dann, A dagegen ist kinderleicht und funktioniert immer. Und das scheinbare Wunder geschieht: Während bei Menschen wie mir B (sowohl Jitsi und BigBlueButton – also selbst gehostete geheimdienst- und überwachungskapitalismusfreie Videokonferenzsysteme) immer funktioniert, versagt es bei den Zoomies, als hätte sie ein Fluch getroffen. Plötzlich funktioniert das Mikrofon nicht, die Kamera nicht, der Laptop fällt vom Tisch. Mit Zoom aber geht angeblich alles wie von selbst.

Und weist auf die Folgen hin, wenn wir zugekaufte Produkte nutzen, anstatt selbst eine sichere Infrastruktur aufzubauen:

Woher kommt das Know-How im IT-Bereich, wenn wir dieses Know-How nicht ausbilden? Warum kaufen Universitäten teure (illegale!) Zoom-Lizenzen, statt Videokonferenz-Systeme auf Basis freier Software selbst zu hosten und weiter zu entwickeln? ... Wir brauchen, um in einer friedlichen übermacht-freien Gesellschaft mündige, souveräne, dezentrale Strukturen aufbauen zu können, gut ausgebildete Menschen, die ohne Berührungängste Server aufsetzen, administrieren und sicher am Laufen halten können. Und damit es diese geben kann, dürfen wir unsere Mündigkeit und Souveränität nicht für ein Linsengericht verkaufen.

Kategorie Verbraucherschutz

Der BigBrotherAward in der Kategorie Verbraucherschutz ging an die **Deutsche Post DHL Group**,

für praktizierten Digitalzwang, indem sie ihre Kund:innen dazu zwingt, für die Nutzung der Packstationen ein Smartphone und ihre Post & DHL-App zu nutzen.

Im Gegensatz zu früher, als man sich für die Nutzung einer Packstation anmelden musste, können Pakete nun auch sonst – wenn die Empfänger:in nicht angetroffen wurde – an Packstationen weitergeleitet werden. Neuere „Lean“-Modelle verzichten dabei auf ein eigenes Display und eine eigene Netzanbindung und nutzen das Smartphone der Nutzer:in bzw. die dort installierte App für die Anzeige der Daten und die Datenübertragung. Laudatorin Rena Tangens kritisiert diesen Zwang zur Nutzung eines Smartphones – anders sei es nicht möglich, an das Paket zu gelangen.

Sie kritisiert auch die App selbst:

Der IT-Sicherheitsexperte Mike Kuketz hat das Verhalten der App gründlich geprüft und dabei Folgendes herausgefunden: Die App macht Verbindungen auf u. a. zu Google Firebase (USA), Adobe Inc. (USA), u. a. der Adobe Experience Cloud und zu Google Firebase Remote Config (USA). Weiterhin zu Sentry, und schließlich zum Google-Firebase-Analytics-Tracker.

Zur Begründung des Zeitpunkts werden die Packstationen in den Kontext der Marktentwicklung gestellt:

Tatsächlich war der Briefdienst jahrelang die Cashcow der Post AG, sie hat fettes Plus gemacht. Trotzdem wurde das Porto immer weiter erhöht. Die Vermutung liegt nahe, dass damit die Paketpost quersubventioniert wurde, um mit billigen Paketpreisen die Wettbewerber vom Markt zu verdrängen. Mittlerweile ist die Deutsche Post DHL Group zum weltweit führenden Logistikanbieter gewachsen. ... Jetzt, wo der Paketdienst boomt und Briefe vielfach durch E-Mail ersetzt werden, ist der Briefdienst nicht mehr so ertragreich. ... Die Aufgaben der Postfilialen sollen zukünftig durch weitere Automaten, sogenannte „Poststationen“ erfüllt werden können – das sind aufgemotzte Packstationen, die dann auch Briefdienste anbieten.

Abschließend bewertet Laudatorin Rena Tangens:

Es geht nicht um einen einzelnen Tracker. Sondern es geht um ein ganzes Universum von Dauerüberwachung. Es geht hier auch nicht um irgendeinen Spielkram, den es nur per Smartphone gäbe. Sondern es geht um etwas so Grundlegendes wie an ein Paket zu kommen, das an mich geschickt wurde. Es geht nicht um die Kosten einer einzelnen Briefmarke. Sondern um die rücksichtslose Haltung, Gewinne zu privatisieren und die Verpflichtungen auf die Allgemeinheit abzuwälzen. Und schließlich geht es um die Tendenz, Menschen bei jeder alltäglichen Handlung der Überall-und-nebenbei-Überwachung auszuliefern.

Kategorie Lebenswerk

Der BigBrotherAward in der Kategorie Lebenswerk wurde an **Microsoft** verliehen. Das Unternehmen erhielt den Preis

dafür, dass es mit seiner Marktmacht Menschen, Unternehmen und Behörden zwingt, bei deren digitalen Aktivitäten dauernd Daten in die USA zu übermitteln und sich dadurch in Echtzeit überwachbar zu machen.

Laudator Thilo Weichert begründet die Preisverleihung:

Nicht nur hat der Konzern seine Büro-Software weltweit als Standard etabliert. Nach dem Verdrängen von Alternativen werden die Anwender nun auch gezwungen, beim Betrieb der Software die Microsoft-eigene Cloud zu nutzen. Das Ergebnis: Microsoft kontrolliert praktisch die gesamte Datenverarbeitung.

Microsoft hat schon im Jahr 2002 den BigBrother-Lifetime-Award für eine flächendeckende Urheberrechts-Kontrolltechnologie, das Digital Rights Management, erhalten. 2018 haben wir dem Unternehmen den BBA in der Kategorie Technik verliehen, weil Windows 10 sich dauernd mit der Firmenzentrale in den USA austauscht. Jetzt toppt das Unternehmen mit Office 365 und allen angeschlossenen Diensten die Abhängigkeit der Nutzenden. Dafür gebührt ihm der nächste Lifetime-Award.

Der Konzern beherrscht nicht nur die private und berufliche Verarbeitung und Kommunikation, sondern bemächtigt sich zunehmend unseres Konsum- und Freizeitverhaltens. Teil des Geschäftsmodells von Microsoft sei es dabei, immer komplexere Software auf den Markt zu werfen, so dass die Nutzenden immer leistungsfähigere Endgeräte benötigten. Software solle mit KI angeblich noch „intelligenter“ gemacht werden. Zugleich dränge Microsoft die Nutzenden, Software as a Service, sprich: die Cloud-Angebote von Microsoft – Azure – zu nutzen. Die Software laufe nicht mehr auf dem privaten PC, auch größere Unternehmens-Rechner seien davon immer mehr überfordert. Es sei erklärtes Ziel von Microsoft, so Panos Panay, Chief Product Officer (CPO), „die Linie zwischen Cloud und Endgerät verschwimmen“ zu lassen – also die Datenkontrolle in die Cloud von Microsoft zu verlagern.

Diese Angebote seien nicht mehr datenschutzkonform zu betreiben:

Peter Wedde

Kategorie Behörden und Verwaltung – Laudatio

Der BigBrotherAward 2023 in der Kategorie Behörden und Verwaltung geht an das Bundesfinanzministerium, vertreten durch Bundesfinanzminister Christian Lindner.

Wir verleihen diesen BigBrotherAward 2023 für das seit dem 1. Januar 2023 geltende Plattformen-Steuertransparenzgesetz (PStTG).

Was folgt aus diesem neuen Gesetz – und wen betrifft es?

Das Gesetz betrifft alle Menschen, die über Plattformen im Internet wie etwa ebay oder ebay-Kleinanzeigen private Verkäufe abwickeln, nachdem sie ihren Keller entrümpelt haben.

Stellen Plattformbetreiber fest, dass jemand innerhalb eines Kalenderjahres die Zahl von dreißig Verkäufen und mehr als 2.000,00 € Gesamtumsatz auf ihrer Plattform erreicht, müssen sie die entsprechenden Daten automatisch an das Bundeszentralamt für Steuern übermitteln. Das ist die neue gesetzliche Meldeschwelle. Außerdem müssen diese Informationen nach der Übermittlung für zehn Jahre vorgehalten werden – sowohl von den Plattformbetreibern als auch von der Finanzverwaltung.

Das Gesetz verlangt also eine zehnjährige doppelte Vorratsdatenspeicherung. Und das, obwohl für die meisten Privatverkäufe überhaupt keine Steuerpflicht besteht – selbst wenn sie die völlig willkürlich gesetzte Meldeschwelle überschreiten. Eine enge und

Die Konferenz der deutschen Datenschutzaufsichtsbehörden hat im November 2022 nach jahrelanger Diskussion mit Microsoft einstimmig festgestellt, dass Microsoft 365 nicht mit der DSGVO in Einklang zu bringen sei. Bei jedem monatlichen Update werden über Tausend Software-Veränderungen vorgenommen, die weder nachvollziehbar, geschweige denn dokumentiert sind.

Thilo Weichert's Fazit lautet:

Tatsächlich ist das einzige Ziel des Unternehmens, uns in seine Cloud zu locken, ja zu zwingen. Eine Nutzung der Software ohne personalisierten Account ist kaum noch möglich, erst recht nicht die Installation auf einem vom Internet abgekoppelten Rechner. Microsoft ist eine große Bevormundungsmaschine, die uns unserer digitalen Souveränität beraubt.

Anmerkungen

- 1 Weitere Informationen und Nachweise finden sich auf der Webseite der BigBrotherAwards, <http://www.bigbrotherawards.de>. Von dort stammen auch alle Zitate aus den Laudationes.



Laudator Peter Wedde, Foto: Matthias Hornung, CC BY 4.0

klare Begrenzung der beabsichtigten Verarbeitungszwecke dieser Vorratsdatenspeicherung, die datenschutzrechtlichen Vorgaben entsprechen würde, ist obendrein nicht erkennbar.

Nach der Gesetzesbegründung¹ setzt das Plattform-Steuertransparenzgesetz die sog. „EU-Amtshilferichtlinie“ in deutsches Recht um, die den europaweiten Informationsaustausch zwischen Behörden für Steuerzwecke regelt. Über diesen Zweck schießt das Gesetz allerdings weit hinaus. Offiziell, um „mehr Steuergerechtigkeit“ zu schaffen².



Natürlich ist es in Ordnung, dass beispielsweise Einkünfte aus dauerhaften Vermietungen über *Airbnb* oder Mitwagenangeboten über *Uber* ebenso versteuert werden müssen wie Verkäufe durch professionelle „Powerseller“ über eine *ebay*-Plattform. Nicht in Ordnung ist es, Plattformbetreiber dazu zu verpflichten, alle bei ihnen anfallenden Daten auszuwerten – um diejenigen herausfiltern zu können, die im Kalenderjahr mehr als dreißig private Online-Verkäufe getätigt und dabei mehr als 2.000,00 € eingenommen haben.

Nach der entsprechenden Meldung an das Bundeszentralamt für Steuern kann es privaten Verkäufern jetzt passieren, dass das Finanzamt pauschal Steuern nachfordert – es sei denn, die Verkäufer können anhand von Quittungen nachweisen, wann und zu welchem Preis sie die veräußerten Gegenstände ursprünglich erworben haben. Allerdings werfen viele Menschen Kaufbelege spätestens dann weg, wenn Garantiefristen abgelaufen sind. Manche sogar früher.

Das Argument, es ginge hier um Steuergerechtigkeit, läuft schon deshalb ins Leere, weil private Verkäufe nur in einem beschränkten Umfang steuerpflichtig sind. Nach § 23 Einkommenssteuergesetz gibt es etwa für private Verkäufe von Gegenständen des täglichen Bedarfs (etwa gebrauchte Babybekleidung oder eine nicht mehr benötigte Küchenmaschine) oder für solche, die jemand länger als ein Jahr besitzt, keine Steuerpflicht. Und bei Gegenständen, die innerhalb eines Jahres nach dem Kauf wieder veräußert werden, müssen erzielte Gewinne nur dann versteuert werden, wenn sie mehr als 600,00 € betragen. Die Steuerpflicht ist für private Verkäufe die Ausnahme – und nicht die Regel.

Das Plattformen-Transparenzgesetz gründet aber auf der Annahme, dass den zuständigen Finanzbehörden ohne flächendeckende Informationen durch die Plattformbetreiber steuerpflichtige Erlöse „durch die Lappen“ gehen können. Nach dieser Logik müssten künftig auch hinter jedem privaten Flohmarktstand Kontrolleure der Finanzämter stehen, die Verkaufszahlen und Umsätze erfassen.

Portalbetreiber müssen jetzt zu allen Verkäufen die folgenden Daten verarbeiten, um die Meldepflicht gegenüber der Finanzverwaltung zu erfüllen, die ihnen das neue Gesetz nach § 13 Absatz 2 vorgibt:

- Vor- und Nachnamen der Verkäufer, Geburtsdaten sowie Anschriften,
- Steueridentifikationsnummern und ggf. Umsatzsteuernummern oder Finanzkonten,
- Gebühren, Provisionen und Steuern, die Plattformbetreiber für private Verkäufe einbehalten oder berechnet haben sowie

- Ausgezahlte oder gutgeschriebene Vergütungen, die private Verkäufer von den Plattformbetreibern pro Quartal des Meldezeitraums bekommen

Darüber hinaus müssen die Plattformbetreiber nach § 18 Absatz 1 PStTG eine Plausibilitätsprüfung zu den getätigten Verkäufen vornehmen – anhand aller ihnen legal zur Verfügung stehenden Informationen und Unterlagen. Was an dieser Stelle unter dem Begriff „Plausibilitätsprüfung“ zu verstehen ist, lässt der Gesetzgeber völlig offen. Beispielhaft wird auf einen Abgleich von Anschriften der Verkäufer und deren Steueridentifikationsnummern mit den „Transaktionsunterlagen“ der meldenden Plattformbetreiber verwiesen.

Mit dem Verzicht auf eine abschließende Benennung zulässiger Verarbeitungszwecke stellt das PStTG den Portalanbietern außerdem einen Blankoscheck dafür aus, das Verhalten von privaten Verkäufern umfassend zu durchleuchten und zu analysieren – und die dabei gewonnenen Erkenntnisse für eigene Interessen zu verwenden.

Die gesammelten Daten können zum Beispiel auch dafür genutzt werden, KI-Software so zu trainieren, dass sie Auffälligkeiten aller Art im Kaufverhalten erkennt. Das Gesetz will es ja so. Wie praktisch.

Erforderlich für die vom Gesetzgeber angestrebte Steuergerechtigkeit ist diese umfassende Vorratsdatenspeicherung nicht. Ob es sich wirklich um „private Flohmarktverkäufe“ handelt, oder ob professionelle und damit steuerpflichtige Geschäfte nur als solche bemäntelt werden – das konnten Plattformbetreiber auch vorher schon erkennen. Und sie können auch feststellen, ob bei privaten Weiterverkäufen neuer Gegenstände steuerpflichtige Gewinne anfallen.

Plattformbetreiber wissen schon heute ganz genau, welchen Wert gebrauchte Gegenstände haben und welche Gewinne sich im Einzelfall mit privaten Verkäufen erzielen lassen. Dieses Wissen schlägt sich in „Preisvorschlägen“ nieder, die Anbieter auf vielen „Kleinanzeigenplattformen“ beim Erstellen privater Verkaufsangebote bekommt. Aus diesen Preisvorschlägen lassen sich auch mögliche Gewinne ableiten. Werfen wir zur Veranschaulichung einen beispielhaften Blick ins „Luxussegment“: Für den privaten Verkauf einer brandneuen Rolex *Submariner Date 126610LN* (Ladenpreis aktuell 10.100,00 €) benennt ein großes Verkaufportal nach Eingabe des entsprechenden Schlagworts eine Angebotspreisspanne zwischen 11.000,00 € und 15.900,00 €. Schon ein Verkauf zum Mindestpreis verspricht damit einen schnellen Gewinn oberhalb des steuerfreien Betrags von 600,00 €.

Anders sieht es beim geplanten Privatverkauf einer neuen Jung-hans Max Bill Automatik Uhr (aktueller Listenpreis 1.325,00 €)

Peter Wedde

Peter Wedde ist Professor für Arbeitsrecht und Recht der Informationsgesellschaft an der Frankfurt University of Applied Science sowie Herausgeber und Autor..

aus, für die ein Verkaufspreis von 480,00 und 1.200,00 € vorgeschlagen wird.

Um dem Ziel der Steuergerechtigkeit näher zu kommen, wäre es völlig ausreichend gewesen, im Plattformen-Transparenzgesetz die Verpflichtung zur Meldung von offenkundig einkommenssteuerpflichtigen Gewinnen zu verankern – statt einer ausufernden, umfassenden Vorratsdatenspeicherung ohne transparent und abschließend festgelegten Verwendungszweck, die zurück in die graue Vorzeit führt. Denn etwas Ähnliches gab es vor ziemlich genau vierzig Jahren schon einmal, mit der damals geplanten Volkszählung. Und dazu hat das Bundesverfassungsgericht in seinem Urteil vom 15. Dezember 1983³ festgestellt, sie sei ein Verstoß gegen das *Recht auf informationelle Selbstbestimmung*.

Auch der Europäische Gerichtshof hält eine gesetzlich vorgeschriebene, flächendeckende staatliche Vorratsdatenspeicherung von Personen für unzulässig, die nicht auch nur mittelbar Anlass zur Strafverfolgung geben⁴. Das gilt auch für Menschen, die nicht steuerpflichtige private Online-Verkäufe tätigen.

Vor diesem Hintergrund kann die datenschutzrechtliche Bewertung des Plattformen-Transparenzgesetzes nur wie folgt ausfallen: Eine Vorratsdatenspeicherung, die weitgehend zweckfrei

und für die betroffenen Personen intransparent bleibt, steht im Widerspruch zu den allgemeinen Grundsätzen in Artikel 5 Absatz 1 DSGVO – wie der Nachvollziehbarkeit von Verarbeitungen, der Zweckbindung und der Datenminimierung.

Wir hoffen, dass der Gesetzgeber den BigBrotherAward 2023 zum Anlass nimmt, das Plattformen-Transparenzgesetz umfassend zu überarbeiten und die vorgeschriebene Meldepflicht auf solche Fälle zu beschränken, in denen eine Steuerpflicht offenkundig gegeben ist – statt die Daten von Menschen ins Visier zu nehmen, die online ihre Hamsterkäfige, Kinderwagen oder Wintermäntel verkaufen.

Damit sollte er nicht warten, bis ihm ein Gericht die Arbeit abnimmt. In diesem Sinne, herzlichen Glückwunsch, Bundesfinanzministerium und Bundesfinanzminister Christian Lindner, zum BigBrotherAward 2023.

Anmerkungen

- 1 Bundestagsdrucksache 20/3436 vom 19.9.2022.
- 2 Vgl. Bundestagsdrucksache 20/3436, Seite 38
- 3 Bundesverfassungsgericht vom 15.12.1983 – 1 BvR 209/83.
- 4 Vgl. EuGH vom 20.9.2022 – C-793/19, Rn. 85.

padelun

Kategorie Kommunikation – Laudatio

Der BigBrotherAward in der Kategorie Kommunikation geht an Zoom Video Communications Inc., die als US-Unternehmen Daten an Geheimdienste weiterleiten müssen, aber dennoch behaupten, DSGVO-konform zu sein.

Zoom untersteht überdies chinesischer Kontrolle und Zensur, da relevante Teile der Entwicklung in China stattfinden. Der Preis geht auch an alle Gruppen, insbesondere Menschenrechts- sowie Umwelt- und Klimaorganisationen, die Zoom einsetzen und damit ihre Teilnehmer:innen der Überwachung preisgeben, obwohl es freie und datenschutzfreundliche Alternativen gibt.

Viele Seuchen haben die Menschheit heimgesucht. Ich nenne mal auszugsweise:

- 2500 vor Christus und ab 1500 immer wieder: Pest,
- 1494 die Syphilis,
- 1870 Pocken,
- 1817 bis heute Cholera,
- seit 1901 Typhus,
- seit 1918 Influenza (ja, das gab's schon vor Instagram),
- 1980 AIDS, was auch einige meiner Bekannten hingerafft hat,
- 1992 Windows 3.1,
- 2002 SARS und
- zuletzt, 2020, Covid-19,



Laudator padelun, Foto: Inflac, CC BY 4.0

und da bilden wir uns ja ein, dass das jetzt vorüber ist und haben das in die Schublade der mit regelmäßigen Impfungen zu bekämpfenden Krankheiten reingelegt.

Aber dieses Covid hatte neben teilweise schrecklichen Krankheitsverläufen auch eine oft unbekannte Nebenwirkung, die ebenfalls nicht so leicht auzurotten ist. Diese Nebenwirkung hat einen Namen. Diese Nebenwirkung heißt „Zoom“.

Der BigBrotherAward 2023 in der Kategorie Kommunikation geht an das Videokonferenzsystem **Zoom**, bzw. an **die Menschen, die Zoom verwenden**.



Auch dieses Jahr wurde die BBA-Statue von keinem der Preisträger in Empfang genommen. Schade!

Foto: Matthias Hornung, CC BY 4.0

Aus „Zoom“ hat sich sogar schon ein Verb gebildet. Das Verb lautet *zoomen* und hat die Bedeutung „unter Beobachtung der Geheimdienste verschiedener Länder und Firmen Geheimnisse ausplaudern und gleichzeitig sein komplettes Beziehungsnetzwerk offen legen.“

Was ist Zoom? Und warum ist Zoom schrecklich?

Zoom ist der Versuch, Menschen, die miteinander in einer Videokonferenz kommunizieren wollen, in den Strudel des Überwachungskapitalismus zu ziehen.

Ich zitiere mal aus der Datenschutzerklärung, was Zoom so speichert und verarbeitet:

- Informationen, die üblicherweise verwendet werden, um Sie zu identifizieren, wie z. B. Ihr Name, Ihr Benutzername, Ihre Anschrift, Ihre E-Mail-Adresse, Ihre Telefonnummern und andere ähnliche Identifikatoren,
- Informationen über Ihre Tätigkeit, wie z. B. Ihre Berufsbezeichnung und Ihren Arbeitgeber,
- Kredit-/Debitkarten- oder andere Zahlungsinformationen,
- Facebook-Profilinformationen,
- Allgemeine Informationen über Ihre Produkt- und Servicepräferenzen,
- Informationen über Ihr Gerät, Ihr Netzwerk und Ihre Internetverbindung, wie z. B. Ihre IP-Adresse, MAC-Adresse, andere Geräte-ID, Gerätetyp, Betriebssystemtyp und -version sowie Client-Version,
- Andere Informationen, die Sie während der Nutzung des Dienstes hochladen, bereitstellen oder erstellen („Kundeninhalte“),

Und da steht weiter: „Wir sammeln diese Daten, um Ihnen die beste Erfahrung mit unseren Produkten zu bieten. Meistens erheben wir personenbezogene Daten direkt von Ihnen, direkt

von Ihren Geräten oder direkt von jemandem, der mit Ihnen über Zoom-Dienste kommuniziert, wie z. B. ein Meeting-Gastgeber, Teilnehmer oder Anrufer. Einige unserer Erfassungen erfolgen auf automatisierter Basis – das heißt, sie werden automatisch erfasst, wenn Sie mit unseren Produkten interagieren.“

Mangelhafter Datenschutz und mangelnde Datensicherheit waren häufig Thema in der Presse. Und jedes Mal wurde hier und da an der Legende gestrickt, dass Zoom ja gar nicht so schlimm sei. Ja, einige offensichtliche Sicherheitslücken wurden geschlossen. Aber der Datenschutz? Statt dessen versucht es Zoom mit weißer Salbe, die aus einer Mischung von Feenstaub und Schlangenöl angemischt wird. Sie spannten sogar die Deutsche Telekom als europäische Alternative vor ihren Karren.

Die Telekom stellte in einer Pressemeldung das Projekt *Zoom X* vor, das angeblich Zoom legal in Deutschland nutzbar machen sollte.

Ein Freund, den ich damals fragte, was er davon hielte, schaute sich die Pressemeldung an und antwortete mir:

- Dieses *Zoom X* wendet sich nur an Geschäftskunden. Privatkund:innen zahlen weiter mit ihren personenbezogenen Daten.
- Die Telekom scheint technisch gar nicht nicht wirklich involviert zu sein, wenn man von der Bereitstellung der Einwahlnummern für Retro-Kund:innen absieht.
- Die Telekom schreibt in ihrer PR zum Beispiel: „Die Meeting-Daten von Teilnehmern aus Deutschland werden auf Servern in Deutschland verarbeitet.“
- Diese überspezifische Formulierung *Die Meeting-Daten* lässt offen, ob andere personenbezogene Daten und Meeting-Metadaten trotzdem zum Hauptquartier von Zoom wandern. Bei allen bisher verfügbaren Zoom-Angeboten ist das der Fall, und daran wird sich wohl nichts ändern.
- Die Telekom sagt nicht, wer die Server in Deutschland betreibt. Das lässt die Möglichkeit offen, dass sie bloß Reseller der Vanity-URL-Lösung sind. Eine Vanity-URL, als Beispiel nenne ich mal die fiktive Domain *universitaet.de*, bedeutet nicht, dass der Server auch in Deutschland steht. Der kann genauso gut auch in den USA oder Bulgarien stehen. Und sowieso landen Meeting- und Benutzer-Metadaten immer in der Public Zoom Cloud – in den USA. Zoom ist in Europa nicht DSGVO-konform einsetzbar – und der Gerichtsstand ist: Kalifornien.

Eine Firma wie Zoom, die in den USA ansässig ist, unterliegt dem Cloud Act, dem Patriot Act und dem FISA Act (Foreign Intelligence Surveillance Act). Und die bedeuten, dass eine in den USA ansässige Firma sämtliche Daten von Nicht-US-Bürger:innen an die dortigen Geheimdienste weitergeben muss. Ganz egal, wo die Server stehen, auf denen die Dienste laufen. Ganz egal, was für nette Versprechen in ihren Privacy-Bestimmungen stehen. Firmen dürfen Betroffene nicht einmal darüber informieren, wenn sie Daten weitergegeben haben.

Zoom unterhält bekanntermaßen gute Beziehungen zur Volksrepublik China. Dort sitzt die 700 Personen starke Entwicklungsabteilung. Ursprünglich war dort auch die Erzeugung kryptographischer Schlüssel ansässig, und es ist bekannt geworden, dass zum Teil Konferenzen über den Umweg China geroutet wurden. Außerdem sind Konferenzen aktiv zensiert worden, wenn in ihnen *Tian'amen-Platz* (Platz des Himmlischen Friedens) angesprochen wurde.

Und jetzt zu Ihnen, die Sie Zoom verwenden und andere zum Verwenden anleiten:

Alle lieben Zoom

Kopfschüttelnd muss ich zugestehen, dass Zoom extrem viel Verwendung findet. Angeblich sei das Videokonferenzieren mit Zoom so einfach und es würde immer funktionieren. Und deswegen ist man halt gerne bereit, seine Seele – und die Seele seiner Großmutter – dem Teufel zu verkaufen. Wenn Sie einen Einladungslink zu Zoom versenden, zwingen Sie andere in das Zoomiversum hinein.

Wenn Menschen Zoom ausgesetzt sind, führt das zum sofortigen Verlust jeglicher Technik-Kompetenz. Erst gerade habe ich wieder eine Einladung zu einem Online-Meeting geförderter Projekte einer großen politischen Stiftung erhalten, in dem ganz brav ein Link zu der Videokonferenzplattform BigBlueButton aufgeführt ist (ein Link und eine fünfstellige Raumnummer). Und dann steht da völlig machtunkritisch fett und groß: „Falls die BBB-Konferenz nicht klappt, ist hier ein Zoom-Link, dann wechseln wir dort hin“, und dann folgen zehn umständlich formulierte Zeilen, auf welche Arten man dort gut hingelangen kann.

Damit diese hoch politischen Projekte, die sich auf Straßen festkleben, Braunkohlebagger besetzen, BigBrotherAwards vergeben und Seenot-Rettungen organisieren, ihre Beziehungen untereinander den Geheimdiensten der *Five Eyes* gegenüber offenlegen müssen. Weil das angeblich sooo einfach ist und alles andere sooo kompliziert. Und nicht nur politische Projekte tun das. Auch Firmen, Forschungslabore, Regierungen – das Wort zoomen hat sich fast schon so fest etabliert wie das Wort googeln.

Und es ist wirklich wie mit der Legende, Mädchen seien schlecht in Mathe: Sag den Menschen, B ist ganz kompliziert und funktioniert nie und dass sie das sowieso gar nicht können, weil sie inkompetent sind. Sag ihnen dann, A dagegen ist kinderleicht und funktioniert immer. Und das scheinbare Wunder geschieht:

Während bei Menschen wie mir B (sowohl Jitsi und BigBlueButton – also selbst gehostete geheimdienst- und überwachungskapitalismusfreie Videokonferenzsysteme) immer funktioniert, versagt es bei den Zoomies, als hätte sie ein Fluch getroffen. Plötzlich funktioniert das Mikrofon nicht, die Kamera nicht, der Laptop fällt vom Tisch. Mit Zoom aber geht angeblich alles wie von selbst.

Bei ihnen funktioniert – oh Wunder – nur A, Zoom. Und das liegt zum Großteil an der Psychologie des Marketings und nicht an der Technik. Frei nach dem Motto: „Wenn's bei den Kommerzlösungen nicht funktioniert, liegt's an den Nutzer:innen. Funktioniert die Alternative nicht, liegt's an der Software ...“

Und auch die Zertifizierung des BSI, des Bundesinstituts für Sicherheit in der Informationstechnik, hat keine Aussagekraft für das Datenschutzniveau. Das BSI hat gerade mal nur das Frontend getestet – nicht das Backend, wo die eigentliche Magie passiert.

Read my Lips: Ganz egal, was auch immer in einem Vertrag von Zoom steht. Auch Zoom ist – wie Microsoft, wie Google-Dienste, wie Facebook – nicht legal in Deutschland und Europa einsetzbar. Und das wisst ihr auch.

Und wirklich: Ihr seid nicht cool, weil Ihr wider besseres Wissen dann doch Zoom macht. Ihr seid nicht dann besonders erwachsen, wenn Ihr Dinge tut, die ihr eigentlich nie tun wollt, aber „es ging ja leider nicht anders“. Doch, es geht anders. Selbst wenn Zoom es ein bisschen leichter machen sollte, ist es nicht okay, es zu verwenden.

Ich meinerseits erliege nicht dem Gruppenzwang und nehme an keinen Zoom-Konferenzen teil. Und das ist manchmal nicht leicht, weil mich das von Diskursen ausschließt und manchmal auch Geld kostet, weil ich auf Honorare verzichten muss. Wer Zoom nutzt, ist selbstverletzend, ausgrenzend und unsolidarisch.

Zoom nutzen ist nicht nachhaltig; es blutet uns finanziell und geistig aus

Woher kommt das Know-How im IT-Bereich, wenn wir dieses Know-How nicht ausbilden? Warum kaufen Universitäten teure (illegale!) Zoom-Lizenzen, statt Videokonferenz-Systeme auf Basis freier Software selbst zu hosten und weiter zu entwickeln? Wenn wir in einer Kommunikationsgesellschaft von Kommunikation auch Familien ernähren müssen, dann müssen wir viele, viele IT-Fachkräfte ausbilden. Und zwar *wirklich* ausbilden und

padeluun

padeluun ist einer der Gründerväter von Digitalcourage. Er experimentierte bereits in den späten 80er-Jahren mit öffentlicher vernetzter Kommunikation. Er entwickelte zusammen mit Rena Tangens Konzepte, wie Kommunikation gelingen kann – und scheiterte grandios vor der geballten Finanzmacht der *Internetkonzerne*, die zwar mit viel Geld Kommunikation zerstören, aber ahnungslos, wie sie waren, nichts Brauchbares aufbauen konnten.



ihnen nicht nur beibringen, stundenlang dem Besetzzeichen des Supports irgendeines zugekauften Produkts zu lauschen. Die vielen Sicherheitslücken, von denen wir Tag für Tag in den Medien hören, rühren unter anderem daher, dass wir Zoom nutzen, statt selbst zu installieren, zu warten und weiter zu entwickeln.

Denken wir doch mal in den Dimensionen von Märkten: Wir brauchen, um in einer friedlichen übermacht-freien Gesellschaft mündige, souveräne, dezentrale Strukturen aufbauen zu können, gut ausgebildete Menschen, die ohne Berührungsängste Server aufsetzen, administrieren und sicher am Laufen halten können. Und damit es diese geben kann, dürfen wir unsere Mündigkeit und Souveränität nicht für ein Linsengericht verkaufen.

Ah, ich sehe, die anwesenden Kaufleute haben das gleich verstanden ;)

Ja, ich habe Sie direkt angesprochen. Ich weiß, dass hier im Saal viele sind und viele das Video sehen, die Zoom und anderes vergiftetes Candy nicht anfassen. Ich ahne aber auch, wie viele von denen, die von Datenschutz sprechen, von Souveränität, die Bücher über den Überwachungskapitalismus lesen, politisch aktiv sind – sich letztendlich einen Dreck drum scheren, wirklich etwas zum Besseren zu wenden. Wirklich, ich muss es so hart sagen: Ihr steht Euch selbst und dem Fortschritt der Menschheit im Wege; egal was für tolle digitale Veranstaltungen Ihr macht, wie Ihr über Zukunft redet, Buzzwords aneinanderreicht, smarte Überwachungscities plant und Euch auf die anderen Bösen, die noch schlimmer sind als Ihr, einen – pardon – runterholt.

Thilo Weichert

Kategorie Lebenswerk – Laudatio

Den BigBrotherAward 2023 in der Kategorie Lebenswerk erhält Microsoft dafür, dass es mit seiner Marktmacht Menschen, Unternehmen und Behörden zwingt, bei deren digitalen Aktivitäten dauernd Daten in die USA zu übermitteln und sich dadurch in Echtzeit überwachbar zu machen.

Damit wird Microsoft bereits zum zweiten Mal (zuerst im Jahr 2002) in der Kategorie Lebenswerk ausgezeichnet.

Wenn von US-amerikanischen Datenkraken die Rede ist, dann geht es zumeist um Google und Meta bzw. Facebook, vielleicht auch um Amazon oder verstärkt Apple. Diesen Firmen wird zu Recht vorgeworfen, dass sie global massenhaft Daten sammeln und sie kommerziell, insbesondere für Werbezwecke – unter Missachtung des Datenschutzes – verwerten. Microsoft segelt regelmäßig unterhalb der Wahrnehmungsschwelle, obwohl das Unternehmen erfolgreich die in unseren Augen gefährlichere Datenstrategie verfolgt. Diese setzt weniger auf kurzfristige Werbeerlöse, sondern darauf, Menschen, Unternehmen und Behörden total von seinen Diensten abhängig zu machen.

Nicht nur hat der Konzern seine Büro-Software weltweit als Standard etabliert. Nach dem Verdrängen von Alternativen wer-

Verlasst Eure Hölle und vor allem: Zwingt andere nicht in Eure Hölle hinein, indem Ihr zu Zoom-Videokonferenzen einladet. Denn es ist schwer, dem Gruppenzwang zu widerstehen. Zu viele klicken dann trotz besseren Wissens auf den Link. Man will ja nicht dauernd *die Spielverderberin* sein.

Und klicken Sie nicht mehr auf Zoom-Links. Sie können auch charmant sagen, dass Sie Zoom nicht verwenden und Ihr Gegenüber eine andere Lösung finden muss. Digitalcourage hat in einer Themenwoche Menschen gefragt, wie sie reagieren würden und haben dazu eine kleine Sammlung der Antworten online gestellt.

Sie brauchen gar keine Beispiele? Sie sind selbst verständig und kreativ genug. Dann werden Ihnen auch selbst gute Worte einfallen, um sich der Zoomikalyypse entgegen zu stellen.

Und so, ja, kann ich sagen: „Herzlichen Glückwunsch, Zoom, zum BigBrotherAward 2023 in der Kategorie Kommunikation.“ – Aber ehrlich?! Die Firma Zoom ist mir ziemlich egal. Der Preis geht eigentlich an alle, die sich den Nebenwirkungen der Seuche Covid ergeben haben und Zoom nutzen. Und ich hoffe, dass dieser BigBrotherAward Eure Abwehrkräfte stärkt und Ihr Zoom nie nie nie mehr verwendet.

Herzlichen Glückwunsch an Euch, zum BigBrotherAward 2023 in der Kategorie Kommunikation. Wir sehen uns. Aber nicht auf Zoom.



Laudator Thilo Weichert, Foto: Matthias Hornung, CC BY 4.0

den die Anwender nun auch gezwungen, beim Betrieb der Software die Microsoft-eigene Cloud zu nutzen. Das Ergebnis: Microsoft kontrolliert praktisch die gesamte Datenverarbeitung.

Microsoft hat schon im Jahr 2002 den BigBrother-Lifetime-Award für eine flächendeckende Urheberrechts-Kontrolltechnologie, das Digital Rights Management, erhalten¹. 2018 haben wir dem Unternehmen den BBA in der Kategorie Technik ver-

liehen, weil Windows 10 sich dauernd mit der Firmenzentrale in den USA austauscht². Jetzt toppt das Unternehmen mit Office 365 und allen angeschlossenen Diensten die Abhängigkeit der Nutzenden. Dafür gebührt ihm der nächste Lifetime-Award.

Der Konzern beherrscht nicht nur die private und berufliche Verarbeitung und Kommunikation, sondern bemächtigt sich zunehmend unseres Konsum- und Freizeitverhaltens. Er setzt mit seiner Xbox auf Gaming und will für 69 Milliarden Dollar den Spielehersteller Activision Blizzard kaufen³, um sich die Tür zum sog. Metaverse zu öffnen⁴. Die Endkunden werden mit Desktop-Streaming jeglicher Art beglückt. Durch die Beteiligung an OpenAI zum Preis von 10 Milliarden US-Dollar steigt Microsoft in das Geschäft mit sog. Künstlicher Intelligenz ein und versucht, durch eine Einbindung des Chatbots ChatGPT in seine Suchmaschine Bing den Quasi-Monopolisten Alphabet bzw. Google zu verdrängen. Microsoft stellt den Menschen vorausgefüllte Antworten zur Verfügung und trägt dazu bei, deren Fähigkeit zum eigenständigen kritischen Denken zu mindern⁵.

Teil des Geschäftsmodells von Microsoft ist es, immer komplexere Software auf den Markt zu werfen, so dass die Nutzenden immer leistungsfähigere Endgeräte benötigen. Der neueste Clou ist es, die Software mit KI angeblich noch „intelligenter“ zu machen. Davon profitiert zunächst die Hardware-Industrie, also Prozessor-Hersteller wie AMD oder Intel⁶. Zugleich drängt Microsoft die Nutzenden, *Software as a Service*, sprich: die Cloud-Angebote von Microsoft – Azure – zu nutzen. Die Software läuft nicht mehr auf dem privaten PC, auch größere Unternehmens-Rechner sind davon immer mehr überfordert. Es ist erklärtes Ziel von Microsoft, so Panos Panay, Chief Product Officer (CPO), „die Linie zwischen Cloud und Endgerät verschwimmen“ zu lassen⁷ – also die Datenkontrolle in die Cloud von Microsoft zu verlagern.

Microsoft, das als reiner Softwareanbieter begann, hat inzwischen einen weltweiten Cloud-Marktanteil von ca. 30 %.

Man sollte meinen, die Politik hätte die damit verbundene Gefahr erkannt. Schon die alte CDU/CSU/SPD-Regierung wollte sich im Digitalen von den „Zwängen aus Abhängigkeiten von ausländischen Anbietern oder Monopolen“ befreien, verfolgte aber – so wörtlich – keinen „Big-Bang“-Ansatz. Getan hat sie gegen die Microsoft-Dominanz praktisch nichts. 96 % aller bundesunmittelbaren Behörden nutzten 2018 Microsoft Office sowie Windows, 69 % Windows Server⁸. Auch die Wirtschaft verlässt sich fast ausschließlich auf Microsoft-Produkte. So ist Deutschlands Kfz-Vorzeigehersteller VW praktisch vollständig von Microsoft abhängig. Allein Windows kommt in mehr als drei Viertel aller Unternehmen zum Einsatz⁹.

2022 kippte die Berliner Senatsverwaltung die zuvor beschlossene Versorgung aller Berliner Lehrkräfte mit der dienstlichen Software eines datenschutzkonformen lokalen Anbieters – und stellte alles auf Microsoft Exchange um. Mit der Begründung, dies sei angeblich preiswerter und passe besser zu den Geräten der Lehrkräfte. 10.000 der 34.000 Lehrkräfte waren schon mit neuen Zugängen des lokalen Anbieters ausgestattet¹⁰. Ob Microsoft kurzfristig billiger ist, ist fraglich. Dass die langfristige Bindung an Microsoft letztlich nur dem Unternehmen dient, ist offensichtlich.

Die Konferenz der deutschen Datenschutzaufsichtsbehörden hat im November 2022 nach jahrelanger Diskussion mit Microsoft einstimmig festgestellt, dass Microsoft 365 nicht mit der DSGVO in Einklang zu bringen sei. Bei jedem monatlichen Update werden über Tausend Software-Veränderungen vorgenommen, die weder nachvollziehbar, geschweige denn dokumentiert sind. Die von Microsoft vorgegebenen Vertragsbedingungen sind unklar. Das Unternehmen teilt nicht mit, welche Unterauftragnehmer es einspannt, die ebenso wie Microsoft Personendaten erhalten¹¹. Es bleibt selbst nach mehrfacher Überarbeitung der Dokumente zur Clouddatenverarbeitung offen, welche Daten von dem Unternehmen für eigene Zwecke verwendet werden. Weder für Datenschützer noch für die Nutzenden ist überprüfbar, „ob alle Schritte rechtmäßig sind.“¹² Das Bundeskartellamt hat Ende März 2023 gegen Microsoft ein Verfahren eingeleitet, weil der Verdacht besteht, dass das Unternehmen seine Marktmacht missbraucht¹³.

Zugunsten von Microsoft und anderen Großkonzernen wird immer wieder vorgebracht, sie böten den Anwendenden mehr Cybersicherheit. Diese steile These wurde am 25. Januar 2023 wieder einmal widerlegt, als wegen einer Netzwerk-Konfiguration beim Cloudangebot Azure weltweit Microsoft-Dienste ausfielen¹⁴. 2021 hat das Bundesamt für die Sicherheit in der Informationstechnik (BSI) eine gravierende Schwachstelle in Microsoft-Exchange auf 98 % aller geprüften Systeme festgestellt. Das BSI reagierte darauf mit einer Warnung der Stufe Rot¹⁵. Zweifellos kann Microsoft viel Geld für IT-Sicherheit ausgeben. Zugleich wird deren komplexe Software immer anfälliger für externe Angriffe und Ausfälle. Zudem: Clouds und Einheitssoftware sind wegen des potenziellen größtmöglichen Angriffserfolgs beliebteste Hackerziele. Im Fall eines Internet-Blackouts läuft über die Cloud überhaupt nichts mehr.

Eine zusätzliche Brisanz hat die Konzentration Microsofts auf sein Cloud-Geschäft dadurch, dass die in die USA abfließenden Daten dem Zugriff der dortigen Sicherheitsbehörden und Geheimdienste ausgesetzt sind. Der Europäische Gerichtshof hat

Thilo Weichert

Thilo Weichert ist ehemaliger Datenschutzbeauftragter des Landes Schleswig-Holstein, Vorstandsmitglied der Deutsche Vereinigung für Datenschutz e. V. (DVD – eine unabhängige Bürger.innenrechtsvereinigung, die sich für Datenschutzbelange in Deutschland und Europa einsetzt) sowie Datenschutzexperte beim Netzwerk Datenschutzexpertise.



mit Urteil vom 16. Juli 2020 zum *Privacy Shield* erneut festgestellt, dass das Datenschutzniveau in den USA zu niedrig ist und keine Vorkehrungen gegen behördliche Massenzugriffe enthält¹⁶.

Um den EU-Markt weiterhin zu dominieren, bietet Microsoft verstärkt seine Dienste über europäische Rechenzentren an. Mit einem Anfang 2023 gestarteten *EU Data Boundary* wirbt es um Vertrauen für Microsoft 365, Azure und Konsorten. Microsoft baut derzeit 17 Rechenzentren in Europa auf und aus. Dies ändert aber nichts an dem Umstand, dass US-Behörden auf diese Daten per Cloud-Act und Foreign Intelligence Surveillance Act Zugriff einfordern¹⁷. Diese Gesetze verpflichten Microsoft, auch im Ausland verarbeitete Daten den US-Sicherheitsbehörden zur Verfügung zu stellen und hierüber Stillschweigen zu wahren.

Für deutsche Behörden soll es 2024 eine eigene Microsoft-Cloud geben. Als Betreiber wird das deutsche SAP vorgeschoben¹⁸. Unklar bleibt, ob dadurch wirklich die Kontrolle über die Datenverarbeitung gewährleistet wird.

Marianne Janik ist Vorsitzende der Geschäftsführung von Microsoft Deutschland. Ihr alternativer Traumberuf, so hat sie in einem Interview erklärt, wäre Verteidigungsministerin. Janik hält den US-Cloud-Act für ein rechtsstaatliches Instrument und gibt „bösen Datenschützern“ eine Mitschuld für unsere Digitalisierungsdefizite in Deutschlands. Unklar bleibt, ob sie das „bösen“ ironisch meint¹⁹. Microsoft tut zwar immer so, als sei Datenschutz auch sein eigenes Anliegen.

Tatsächlich ist das einzige Ziel des Unternehmens, uns in seine Cloud zu locken, ja zu zwingen. Eine Nutzung der Software ohne personalisierten Account ist kaum noch möglich, erst recht nicht die Installation auf einem vom Internet abgekoppelten Rechner. Microsoft ist eine große Bevormundungsmaschine, die uns unserer digitalen Souveränität beraubt.

Deshalb:

Herzlichen Glückwunsch, Microsoft

Herzlichen Glückwunsch, Marianne Janik, Vorsitzende der Geschäftsführung von Microsoft Deutschland

Anmerkungen

- 1 <https://bigbrotherawards.de/2002/lebenswerk-microsoft>
- 2 <https://bigbrotherawards.de/2018/technik-microsoft-deutschland>
- 3 Bier, Activision Blizzard: Muss sich Microsoft bei der Übernahme von Call of Duty verabschieden? 13.02.2023, <https://www.gamestar.de/artikel/activision-blizzard-muss-microsoft-call-of-duty-abtreten,3389909.html>
- 4 Freund, Spieltrieb, SZ 02.02.2022, 10; Martin-Jung, Bloß nichts verpassen, SZ 20.01.2022, 17; Mega-Deal setzt Sony unter Zugzwang, SZ 20.02.2022, 21; Brühl/Martin-Jung, Eine Wette im Wert von fast 70 Milliarden Dollar, SZ 19.01.2022, 15.
- 5 Hurtz, Bingen statt googlen, SZ 09.02.2023, 17; Heaven, Microsoft gegen Google gegen alle: Wie ChatGPT einen neuen Suchkrieg auslöst, www.heise.de 17.02.2023, Kurzlink: <https://heise.de/-7517615>.
- 6 Weiß/Mantel, Microsoft bei AMD auf der CES: KI wird alles verändern, wie einst die Maus, www.heise.de 05.01.2023, Kurzlink: <https://heise.de/-7449226>; Martin-Jung, Besserer Schutz vor Hackern, SZ 06.10.2021.
- 7 Zit. nach Eva-Maria Weiß, Mark Mantel (s. o.).
- 8 Bundestagsdrucksache. 19/29476.
- 9 Wie groß ist die Abhängigkeit von Microsoft? www.tagesschau.de 25.01.2023.
- 10 Vieth-Entus, Anbieterwechsel empört Abgeordnete, 08.03.2022, <https://www.tagesspiegel.de/berlin/vier-legislaturperioden-aber-keindurchbruch-die-unendliche-geschichte-der-berliner-schulerdatei-417175.html>
- 11 DSK, Festlegung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, Stand: 24.11.2022, https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365.pdf; Weichert CuA 2/2023, 31 ff.
- 12 Krempf, Datenschutzkonferenz: Microsoft 365 ist und bleibt datenschutzwidrig, www.heise.de 25.11.2022, Kurzlink: <https://heise.de/-7352065>.
- 13 Wilkens, Bundeskartellamt leitet Verfahren gegen Microsoft ein, www.heise.de 28.03.2023, <https://heise.de/-8146965>.
- 14 Muth, Störungen bei Microsoft, SZ 26.01.2023, 5, 1.
- 15 BSI, BSI-Lagebericht 2021: Bedrohungslage angespannt bis kritisch, PM 21.10.2021; zuvor Muth, Schwachstelle bei Microsoft, SZ 09.03.2021, 18.
- 16 EuGH 16.07.2020 – C-311/18, Schrems II.
- 17 Bremmer, Microsoft zieht virtuelle EU-Datengrenze, 15.12.2022, <https://www.computerwoche.de/a/microsoft-zieht-virtuelle-eu-datengrenze,3613485>.
- 18 Wölbert, Digitale Souveränität: Microsoft-Cloud soll 2024 starten, www.heise.de 24.11.2022, Kurzlink: <https://heise.de/-7338725>
- 19 Martin-Jung/Werner, Interview mit Janik, „Wir bleiben in Deutschland unter unseren Möglichkeiten“, SZ 23.11.2022, 18.



Die Geschenke stehen bereit. Wird dieses Jahr auch ein Preis abgeholt? Fotos: Matthias Hornung, CC BY 4.0

Constanze Kurz

Den Geheimdiensten endlich Grenzen setzen

6. Juni 2023 – Dass vom größten Abhörskandal der Geschichte auszugehen sei, stand schon 2013 in den Zeitungen, obwohl die Snowden-Enthüllungen noch jahrelang weitergehen sollten. Zehn Jahre später lohnt der Blick zurück auf Massenüberwachung, Spionageangriffe und einige der Konsequenzen, denn bis heute ist die Überwachung maßlos. Ein Kommentar.

Was Edward Snowden enthüllte, war und ist beispielgebend für viele andere Whistleblower, die mit ihrem Gewissen ringen. Die Art, wie Journalisten mit ihm gemeinsam Übersetzungsarbeit für den Geheimdienstesprech geleistet haben, war oftmals großartig. Die Snowden-Veröffentlichungen waren ein Einschnitt. Wir sprechen heute anders über Geheimdienste, insbesondere in Deutschland nach dem parlamentarischen NSA-BND-Untersuchungsausschuss. Wie viel wir heute dank Edward Snowden wissen und welches Ausmaß die technisierte Massenüberwachung hat, zeigt ein Rückblick auf die im Juni 2013 beginnenden Snowden-Veröffentlichungen¹.

Selbst der damalige Bundesinnenminister Thomas de Maizière (CDU) hat die technisierte Überwachung damals als maßlos beschrieben²:

Was die USA an Aufklärungsmaßnahmen tun, ist zwar ganz überwiegend ihrem Sicherheitsbedürfnis geschuldet, aber sie tun es in einer übertriebenen, maßlosen Anwendung. [...] Wenn zwei Drittel dessen, was Edward Snowden vorträgt oder was unter Berufung auf ihn als Quelle vorgetragen wird, stimmen, dann komme ich zu dem Schluss: Die USA handeln ohne Maß.

Heute können wir uns ein konkretes Bild davon machen, welche technischen Fähigkeiten die Geheimdienste im Detail hatten und haben: nicht nur die der NSA (National Security Agency), sondern auch der Five-Eyes-Geheimdienste aus Kanada, Großbritannien, Neuseeland und Australien. Die Five-Eyes-Überwachung erfasst Ausländer und Einheimische, teilweise als massenhafte, teilweise als gezielte Form von Überwachung. Die größten der Programme sind unter ihren Namen Prism und Upstream heute weithin bekannt, ein Teil dieser inländischen Massenüberwachung der NSA war rechtswidrig³. Sie machten uns auch allen bewusst, wie stark die Zusammenarbeit der Geheimdienste mit kommerziellen Tech-Firmen gediehen war.

Der damalige Chef von Microsoft bezeichnete die Geheimdienste nach Beginn der Snowden-Veröffentlichungen als „persistent threat“, also als eine dauerhafte Bedrohung, die es abzuwehren gilt. Die Tech-Konzerne haben letztlich ihren Umgang mit IT-Sicherheit auch durch Snowden nachhaltig geändert, insbesondere was die Verschlüsselung angeht. Das hat all denjenigen gutgetan, welche die Dienstleistungen der Konzerne nutzen.



Holzschnittdruck von Felipe Crespo, CC BY 3.0

Die positive Folge der Snowden-Veröffentlichungen muss klar benannt werden: Der verschlüsselte Internetverkehr hat deutlich zugenommen. Für typische Dienstleistungen der Tech-Konzerne wie Gmail und WhatsApp wurde die Verschlüsselung angeknipst. Nutzer wissen das vielleicht nicht mal. Aber für die Geheimdienste wurde damit eine wesentlich höhere Hürde gelegt, um die Inhalte auswerten zu können. Diese Folge der Snowden-Veröffentlichungen ist wertvoll, auch jenseits der Überwachung durch Geheimdienste.

Glasfaser-Abhör-Operation

Viele der Geheimdienst-Programme betreffen Massenüberwachung, oft in Form von globalen Operationen. Ein paar der bekanntgewordenen Programme hatten aber einen besonderen Impact, zum einen weil sie technisch besonders anspruchsvoll waren, zum anderen weil sich Höchstgerichte mit ihnen befasst haben. Dazu gehört die Operation Tempora: Das war die Glasfaser-Abhör-Operation des britischen GCHQ für Inhalts- und Metadaten⁴. Der Geheimdienst war und ist ein wichtiger Datenlieferant für die NSA, aber auch für die anderen Five-Eyes-Geheimdienste und für weitere Partnergeheimdienste. Warum der GCHQ als Glasfaser-Datenstaubsauger besonders geeignet ist, liegt schlicht an der geographischen Lage der britischen Inseln, die bereits vor hundert Jahren durch die Verlegung der Telegraphen-Leitungen entstanden ist.



1925 New-York. Kabel-Legung: In Rockaway Beach wurde das Ende eines neuen Unterseekabels an Land gezogen. Es ist das erste direkte Kabel zwischen den Vereinigten Staaten und Süd-Europa. Es läuft von New-York zu den Azoren und von dort über Malaga in Spanien nach Rom, die Verbindung beträgt 4704 Seemeilen.

Bundesarchiv, Bild 102-01035 / Unknown author / CC-BY-SA 3.0

Ein Großteil des kontinentaleuropäischen Datenverkehrs läuft über die britischen Unterseekabel. Diese Quelle wurde extensiv genutzt, nämlich an ungefähr zweihundert Glasfaserkabeln, die angezapft wurden. Tempora wurde Teil eines Gerichtsverfahrens beim Europäischen Gerichtshof für Menschenrechte und von der britischen Regierung auch nicht bestritten. Ungefähr fünfzig Milliarden Metadaten pro Tag wurden gesammelt. Dieser Umfang dürfte sich selbstverständlich unterdessen vergrößert haben, denn schließlich sind zehn Jahre vergangen.

Offensive Hacking-Operationen

Zu den wichtigen Veröffentlichungen aus den Snowden-Papieren zählt das sogenannte Black Budget, welches das Milliarden-Budget der US-Geheimdienste aufzeigt. Dazu entstand auch eine Debatte um das Heer von Vertragspartnern, die sich um die Geheimdienste scharen und von ihnen bezahlt werden. Die ganze Branche um die technischen Geheimdienste herum wurde in neuer Weise beleuchtet. Wie das Pöppeln und Finanzieren dieser Branche die IT-Sicherheit global in Mitleidenschaft gezogen hat, ist bis heute Thema geblieben. Das Black Budget zeigte aber auch, in welcher Liga die US-amerikanischen Geheimdienste spielen, weit jenseits von allem, was die anderen demokratischen Staaten für ihre Geheimdienste ausgeben.

Es gibt einen Bereich der Snowden-Veröffentlichungen, der öffentlich weniger breit besprochen wurde, vielleicht weil er technisch anspruchsvoller ist: die offensiven Hacking-Operationen der NSA. Dazu gehören langjährige Projekte wie Bullrun oder Edgehill in Zusammenarbeit mit dem GCHQ, die faktische Anti-Sicherheits-Operationen waren: Hintertüren bauen, technische Sicherheitsmaßnahmen schwächen. Eine der Snowden-Veröffentlichungen hat dabei die halbe Krypto-Welt elektrisiert, nämlich die erfolgreiche Manipulation von DUAL_EC_DRBG⁵, eines kryptographischen Standardverfahrens. Die Krypto-Community, die heute in den ISO-Standardisierungsgremien sitzt und nun zukünftige Krypto-Standards analysiert und bewertet, lässt sich

seither nicht mehr abspeisen mit Beteuerungen, sondern verlangt Transparenz, auch von der NSA, wenn sie ihre Vorschläge für künftige Standards einreicht.

Zu den offensiven Hacking-Operationen mit der größten politischen Tragweite zählt wohl der Belgacom-Hack⁶. Denn betroffen von dem Hack waren die Spitzen der europäischen Politik mit der EU-Kommission und auch mit dem Europäischen Parlament, mit zahlreichen Botschaften, sogar mit dem NATO-Hauptquartier. Alle großen europäischen Institutionen hatten die Geheimdienste offenbar im Blick.

Kritik an den Geheimdiensten

Eine der größten Peinlichkeiten aus deutscher Sicht war zweifelsohne die Merkel-Spionage⁷. Doch aus dem Abhören der deutschen Regierungschefin folgte – nichts. Es gab zwar monatelange Diskussionen um ein sogenanntes No-Spy-Abkommen, es gab Anrufe zwischen Barack Obama und Angela Merkel. Aber nichts, absolut gar nichts ist in diesem Bereich auch nur verhandelt worden. Die US-Amerikaner haben die deutsche Regierung abtropfen lassen, sich auf keine Verhandlung irgendeiner Art eingelassen, um auch nur einen Anteil der praktizierten Spionage vertraglich auszuschließen.

Das ist deswegen erstaunlich, weil es erheblichen öffentlichen Druck gab. Nach den ersten Snowden-Veröffentlichungen war ein anderer Blick auf die Geheimdienste verbreitet, als man ihn heute (wieder) hat. Einige Texte, die in dieser Zeit geschrieben wurden, zeigen eine Tonalität in Bezug auf die Kritik an den Geheimdiensten, die heute kaum mehr vorstellbar ist.

Auch der BND-NSA-Untersuchungsausschuss hat für einige Zeit einen starken Imagewandel der Geheimdienste hervorgerufen. Nach der öffentlichen Debatte im Parlament über den Abschlussbericht des Untersuchungsausschusses kommentierte Hans-Christian Ströbele (Grüne) die dreisten Lügen⁸, die dem Parlament serviert worden waren. Auch als ein Politiker, der Geheimdienst-Untersuchungsausschüssen in vier Jahrzehnten parlamentarischer Arbeit beigewohnt hatte, zeigte er sich erstaunt:

Wir wissen jetzt durch die Arbeit des Untersuchungsausschusses: Während sie sagten: ‚Wir wissen überhaupt nicht, worum es geht, was das sein soll, vor allem, was wir damit zu tun haben‘, verhandelten sie mit ausländischen Nachrichtendiensten darüber. Erstens über das, was da schon in gemeinsamer Zusammenarbeit gelaufen war, also zum Beispiel bei dem Projekt Eikonol. Aber sie verhandelten auch über neue Zugänge in die Netze. Das war ein Täuschungsmanöver sensationeller Art, so wie ich mir das gar nicht vorstellen konnte.

Eikonol⁹ ist die NSA-BND-Kooperation, um die Glasfaserkabel der Deutschen Telekom in Frankfurt anzuzapfen. Die Dreistigkeit, mit der er als Parlamentarier belogen wurde, überraschte selbst Ströbele.

Es gibt keinerlei Anhaltspunkte, warum das heute anders sein sollte. Ströbele hat als Experte für Geheimdienste stets betont, dass die Kontrolle der Geheimdienste auch in Fragen der tech-

nisierten Massenüberwachung nicht adäquat sei. Dass der neue Kontrollrat, der im BND-Gesetz steht, eine qualitativ bessere Kontrolle ausüben kann, ist nicht zu erwarten.

Doch trotz Snowden und trotz der dreisten Lügen ist diese Massenüberwachung zur Normalität geworden, gesetzlich legitimiert. Nicht nur bei uns, auch in Frankreich, in den Niederlanden, in Schweden, in der Schweiz, in Finnland und in Großbritannien, die allesamt Massenüberwachung gesetzlich legitimiert durchführen.

Was für Deutschland zu fordern ist

Was darf der deutsche Auslandsgeheimdienst BND in Sachen Massenüberwachung aktuell? Er darf massenhaft Telekommunikationsdaten sammeln und auswerten. Was einst rechtswidrig oder an der Grenze des Rechts durchgeführt wurde, ist nun gesetzlich erlaubt. Außer den Kommunikationsinhalten dürfen die Geheimdienste auch weiterhin Metadaten rastern. Zudem darf Maschine-zu-Maschine-Kommunikation ausgewertet werden. Und das Budget ist auf mehr als eine Milliarde Euro angewachsen.

Dass der Geheimdienst mit so gewaltigen Summen finanziert wird, steht öffentlich kaum mehr in Frage. Während es im Gefolge der Snowden-Veröffentlichungen durchaus eine Frage war, ob man den ausufernden Bereich der Geheimdienste vielleicht zurückbauen könnte, wird darüber heute kaum noch gesprochen.

Am 25. Mai 2021 erging ein Urteil des Europäischen Gerichtshofs für Menschenrechte in Straßburg zur britischen Massenüberwachung, dem noch mehr Geltung verschafft werden muss, insbesondere weil es eine stärkere Kontrolle der Geheimdienste verlangt. Der Gerichtshof schreibt eine unabhängige Behörde vor, die den Zweck der Überwachung und auch die Auswahl und Kategorien der Selektoren prüft. Selektoren sind die Merkmale, nach denen die Dienste Daten durchsuchen.

Das bleibt auch für Deutschland zu fordern, denn diese Kontrolle ist beim BND noch zu unterentwickelt. Zudem betont das Urteil die rechtliche Gleichsetzung von Inhaltsdaten und Metadaten, die gleichwertig geschützt gehören. Auch in Diskussionen jenseits der Geheimdienste, etwa bei der Vorratsdatenspeicherung, setzt das Urteil damit Akzente.

Politisch bleibt zu fordern, dass die Minimalanforderungen, die von diesem und anderen Höchstgerichten gestellt werden, nicht mehr die Messlatte sein sollten. Denn einen Blankoscheck für Geheimdienste¹⁰ zur unbegrenzten Überwachung von Millionen Menschen sollten wir nicht mehr ausstellen. Die Parteien der Ampel-Regierung müssen an die Versprechungen erinnert werden, die sie im Wahlkampf gemacht haben und die auch im Koalitionsvertrag stehen.

Betrachtet man die Urteile der Höchstgerichte auf europäischer Ebene, ist es längst Konsens, dass ein Verbot der nicht zielgerichteten Massenüberwachung besteht. Bei der technisierten Massenüberwachung sollte die Ampel schon deswegen endlich eine Trendumkehr wagen.

Quelle: <https://netzpolitik.org/2023/zehn-jahre-snowden-den-geheimdiensten-endlich-grenzen-setzen/>

Anmerkungen

- 1 <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>
- 2 <https://netzpolitik.org/2014/thilo-weichert-weshalb-deutschland-edward-snowden-um-einreise-bitten-muss/>
- 3 <https://www.reuters.com/article/us-usa-nsa-spying/u-s-court-mass-surveillance-program-exposed-by-snowden-was-illegal-idUSKBN25T3CK>
- 4 <https://de.wikipedia.org/wiki/Tempora>
- 5 <https://www.scientificamerican.com/article/nsa-nist-encryption-scan-dal/>
- 6 https://en.m.wikipedia.org/wiki/Operation_Socialist
- 7 <https://web.archive.org/web/20140209185311/http://www.spiegel.de/international/world/merkel-calls-obama-over-suspicious-us-taped-her-mobile-phone-a-929642.html>
- 8 <https://netzpolitik.org/2017/netzpolitik-podcast-136-mit-hans-christian-stroebele-was-edward-snowden-uns-geliefert-hat-ist-die-wahrheit/>
- 9 <https://www.heise.de/news/BND-Operation-Eikonal-Freibrief-fuer-die-Telekom-aus-dem-Kanzleramt-2854406.html>
- 10 <https://netzpolitik.org/2021/massenueberwachung-blankoscheck-fuer-geheimdienste/>

Information zur Autorin siehe Seite 53



Josefine Kulbatzki

Mehr als die Summe der Einzelteile

11. August 2021 – Immer neue Überwachungsgesetze gewähren Polizei und Geheimdiensten weitreichende Zugriffe auf persönliche Daten. Eine Überwachungsgesamtrechnung könnte zeigen, wie die Maßnahmen sich insgesamt auf Grundrechte auswirken. Doch wie lässt sich Überwachung überhaupt berechnen und welche Auswirkungen kann das haben?

Geheimdienste und Ermittlungsbehörden wollen den Zugriff auf Messenger, obwohl sie schon jetzt oft die Chats von Zielpersonen mitlesen können¹; die Bundespolizei darf Staatstrojaner schon im Vorfeld einer Straftat einsetzen² – die Anzahl an Überwachungsgesetzen und -maßnahmen ist hoch und es kommen

stetig³ neue dazu. Online-Durchsuchung, Quellen-TKÜ, Stille SMS, Metadaten-Auswertungen. Es fällt schwer, einen Überblick zu behalten, und noch schwerer einzuschätzen, wie sie sich in ihrer Gesamtheit auf die Grundrechte auswirken. Selbst die Verantwortlichen scheinen manchmal nicht sicher⁴ zu sein, wel-



Foto: Pawel86, pixabay

che Überwachungsmaßnahmen sie eigentlich verwenden, beispielsweise den Staatstrojaner oder klassische Telefonüberwachung.

Das Bundesverfassungsgericht hat 2005 in einem Urteil über den Einsatz des Global Positioning Systems (GPS) als Observationsmethode festgestellt⁵, dass tief in die Grundrechte eingreifende Überwachungsmaßnahmen nicht einzeln betrachtet werden dürften, sondern vor dem Hintergrund bestehender Überwachungsgesetze, damit die Eingriffe in die Grundrechte des einzelnen nicht zu stark würden. Dies wurde 2010 in einem Urteil zur Vorratsdatenspeicherung nochmal bestärkt und der Gesetzgeber zu „größerer Zurückhaltung“⁶ bei der Verabschiedung neuer Überwachungsmaßnahmen ermahnt.

Die *Überwachungsgesamtrechnung* (ÜGR) hat sich seit dem Urteil 2010 als politisches Schlagwort etabliert. Sie könnte die Gesamtwirkung der einzelnen Überwachungsmaßnahmen auf die Grundrechte bewerten, so die Hoffnung. Doch bisher wurde sie nicht konkret umgesetzt. Auch wie sie genau aussehen und was sie bewirken kann, ist nicht geklärt. In jedem Fall braucht es dafür einen Überblick über die bestehenden Maßnahmen. Konstantin von Notz, stellvertretender Fraktionsvorsitzender BÜNDNIS 90/Die Grünen, findet:

Zur Erhöhung der Sicherheit, zum effektiven Schutz von Bürgerrechten und zur Stärkung der Rechtsstaatlichkeit staatlichen Handels braucht es dringend einen Überblick darüber, ob bestehende gesetzliche Regelungen ihre Funktion erfüllen.

Anke Domscheit-Berg, netzpolitische Sprecherin der LINKEN im Bundestag, teilte netzpolitik.org mit, dass die ÜGR überfällig sei, da seit Jahren neue Überwachungsgesetze erlassen würden, ohne dass zwei Voraussetzungen, ihre Effektivität und die Verhältnismäßigkeit, erfüllt seien.

Dass immer wieder Gesetze vom Bundesverfassungsgericht im Nachhinein für verfassungswidrig erklärt werden, verdeutlicht: Ein Instrument, mit dem im Vorhinein geprüft werden kann, ob neue Gesetze mit den Grundrechten vereinbar sind, ist notwendig. Dennoch ist seit 2010 seitens der Politik nicht viel passiert.

Eine Übersicht und dann?

Das Max-Planck-Institut (MPI) zur Erforschung von Kriminalität, Sicherheit und Recht versucht, die Forderung des Bundesverfassungsgerichts umzusetzen und arbeitet aktuell an einem Konzept⁷ für einen „realistischen Einblick in die Überwachungslast“. Die erste Phase des Projektes sieht eine detaillierte Auflistung einzelner Gesetze und was sie beinhalten vor. Sie wurde exemplarisch⁸ für das Szenario der anlasslos gespeicherten Massendaten erstellt. Die Übersicht gibt den aktuellen Status der Überwachungslandschaft für dieses Szenario genau wieder: Welche Behörden können auf welcher Rechtsgrundlage auf welche Informationen zugreifen? Wer erhebt diese Daten?

Auch wenn es diese Auflistungen bisher nur für einzelne Gesetze gibt, sind sie ein erster, wichtiger Schritt. Sie belegen für ausgewählte Beispiele, wie viele unterschiedliche Gesetze Zugriff auf dieselben Datenpools ermöglichen. So könnte auch überprüft werden, ob manche Gesetze den Zugriff auf Datenpools ermöglichen, die über das eigentliche Ziel hinausgehen – erfüllen sie ihre Funktion oder berechtigen sie zu grundloser Datenspeicherung?

Was der Überblick jedoch nicht zeigt: Wie tief greifen die Gesetze in die Grundrechte ein?

Kann Überwachung berechnet werden?

Hierfür hat das MPI ein „periodisches Überwachungsbarometer“ entwickelt⁹. Mit ihm sollen empirische Daten über die Überwachungsintensität, die „Überwachungslast“ der Bevölkerung, erhoben werden können. Dafür sind konkrete Zahlen notwendig: Das MPI gewichtet hierfür die einzelnen Maßnahmen und orientiert sich bei der Bewertung an Urteilen des Bundesverfassungsgerichts, das zwischen „schweren“ und „weniger schweren“ Eingriffen in die Grundrechte unterscheidet. Es berücksichtigt außerdem, auf welcher rechtlichen Grundlage auf die unterschiedlichen Datenpools zugegriffen werden darf. Der Wert, den die Maßnahmen auf dieser Grundlage bekommen, wird dann mit der Häufigkeit der Eingriffe pro Jahr verrechnet, woraus sich ein Gesamtwert für eine spezifische Maßnahme in einem bestimmten Jahr ergibt.

Das MPI versucht in seinem konkreten Vorschlag, die Überwachungslast objektiv darzustellen. Die ermittelten Zahlenwerte allein haben aber noch keine eigene Aussagekraft, sie unterliegen laut MPI dem „politischen Spiel“. Aussagekräftig würden sie im Vergleich: Einmalig abgehörte digitale Kommunikation wird einen niedrigeren Wert erhalten als monatelang abgehörte Kommunikation oder die Durchsuchung alter Kommunikationsinhalte. Ist der Wert *hoch*, könnte beschlossen werden, das beispielsweise eine neue weitere Maßnahme nur mit richterlichem Vorbehalt eingesetzt werden darf.

Vor allem über einen längeren Zeitraum könnte deutlich werden, wie die Überwachungslandschaft sich insgesamt verändert. Das könnte juristische Prozesse beeinflussen. Zeigt ein „Überwachungsbarometer“, wie stark in einzelnen Bereichen bereits in die Grundrechte eingegriffen wird, könnte es zu einer Ent-

scheidungsgrundlage für neue Gesetze oder Reformen bestehender Regeln werden.

Anke Domscheit-Berg sieht die ÜGR zukünftig in der Lage, Gesetze zu verhindern. Wenn Befugnisserweiterungen geplant sind, müsste die zuständige Stelle den damit befassten Ausschüssen eine aktualisierte ÜGR vorlegen, so die Netzpolitikerin:

Wenn ein kritischer Wert bereits erreicht ist, muss es ein Moratorium für neue Überwachungsbefugnisse geben, sowie eine verpflichtende Evaluierung bestehender Regelungen, die nach verschärften Kriterien ihre Effektivität und Verhältnismäßigkeit nachweisen müssen und, wenn das nicht gelingt, aufzuheben sind.

Ist es eigentlich komplexer?

Die reale Überwachungslast dürfte schwer zu berechnen sein, denn nicht immer ist eine ausreichende Datengrundlage vorhanden. Seit 2013 können Behörden etwa bei Internet-Zugangs-anbietern für IP-Adressen Bestandsdaten abfragen, doch hierzu gibt es keine Statistiken¹⁰. Auch in der Neuregelung¹¹ zur Bestandsdatenauskunft wurde keine Statistik-Pflicht¹² aufgenommen.

Die Daten, die durch eine Auskunftspflicht in aktualisierten Polizeigesetzen mancher Bundesländer zukünftig hinzukommen, könnten frühestens nächstes Jahr in das Barometer eingerechnet werden. Welche Informationen beispielsweise der Berliner Verfassungsschutz erhebt, wird in den meisten Bereichen auch nicht statistisch erfasst¹³ oder der Verfassungsschutz will die Informationen zunächst nicht¹⁴ herausgeben.

Auch Zugriffe ausländischer Geheimdienste sind nicht transparent, beides müsste für ein Gesamtbild allerdings berücksichtigt werden. Abgesehen von den Geheimdiensten könnte das Instrument frühestens in zwei bis drei Jahren ein annähernd umfassendes Bild oder eine Entwicklungsrichtung zeigen – wenn die Auskunftspflichten eingehalten werden.

Welche Daten statistisch erfasst und veröffentlicht werden, ist, wie sich in dem neu beschlossenen Gesetz zur Bestandsdatenauskunft zeigt, abhängig vom politischen Willen. Das Gleiche gilt für die Ergebnisse eines Überwachungsbarometers: Was die Werte am Ende aussagen, wann das Maß an Überwachung überschritten ist, ist politische Interpretationssache. Kritiker:innen sehen darin¹⁵ die Gefahr, dass entgegen dem eigentlichen Ziel argumentiert werden könnte: Ist die Grenze an

Überwachungsmaßnahmen noch nicht erreicht, können ja noch mehr Gesetze beschlossen werden.

Freiheit statt Überwachung?

Das Schlagwort *Überwachungsgesamtrechnung* sollte dem Urteil aus Karlsruhe nachkommen: Keine neuen Überwachungs- und Sicherheitsgesetze, ohne die alten zu berücksichtigen und die bestehenden Grundrechtseingriffe im Blick zu behalten. Eine umfassende Übersicht, wie sie das MPI angefertigt hat, bietet eine wichtige Datengrundlage, um vorhandene Gesetze kritisch überprüfen zu können – falls die nötigen Daten vorhanden sind. Eine Alternative schlägt Jörg Pohle¹⁶ mit der *Freiheitsbestandsanalyse*¹⁷ vor. Sie könnte den Gesetzgeber stärker dazu bringen, sich zu rechtfertigen und die Zivilgesellschaft dazu, Auskünfte einzufordern.

Ausgangspunkt ist hier *Freiheit*. Der Gesetzgeber soll auflisten, welche durch die Grundrechte und die Verfassung gesicherten Freiheitsräume noch frei von „tatsächlicher und zu erwartender“ Überwachung sind. Auch hier ist die Grenze, wann zu viel Überwachung herrscht, nicht festgelegt und eindeutig, aber sie wird anders bestimmt: Der Gesetzgeber muss nachweisen, inwiefern trotz zahlreicher Überwachungsmaßnahmen beispielsweise noch von freier Kommunikation gesprochen werden kann.

Auch hier bräuchte man eine Datengrundlage, sind keine Statistiken zu bestimmten Maßnahmen vorhanden, könnte der Gesetzgeber hier verstärkt in die Pflicht genommen werden: Ist beispielsweise unklar, wie häufig IP-Adressen abgefragt werden, würde von der maximalen Eingriffsstärke ausgegangen werden. Um zu beweisen, wie „frei“ Internetdaten von Überwachung sind, damit der angenommene Wert nach unten korrigiert wird, müssten diese Daten offengelegt werden. Einen Vorteil sieht Pohle darin, dass der Gesetzgeber so stärker die Auswirkungen der Gesetze offenlegen müsste und sich nicht hinter technischen Details verstecken kann.

Ob *Überwachungsgesamtrechnung* oder *Freiheitsbestandsanalyse*, für beides muss es eine unabhängige Institution geben, die sich mit der kompletten „Berechnung“ und vor allem der Interpretation der Werte, am besten in Diskussion mit Wissenschaft und Zivilgesellschaft, auseinandersetzt. Anke-Domscheit-Berg könnte sich hierfür den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vorstellen, betont aber auch, dass er mit den notwendigen Ressourcen ausgestattet werden müsste.

Josefine Kulbatzki

Josefine Kulbatzki war von Januar bis April 2021 bei *netzpolitik.org* und schreibt seitdem ab und an für dieses spendenfinanzierte Medium. Sie begeistert sich für viele unterschiedliche Themen rund um Digitalisierung, Gesellschaft und Politik. Momentan arbeitet sie viel zu der Regulierung sozialer Medien in unterschiedlichen Ländern und dem großen Überthema *Überwachung*. Erreichbar per Mail – gerne auch verschlüsselt.

Bisher hält die Regierung eine ÜGR nicht für notwendig, wie aus der Antwort¹⁸ auf eine schriftliche Anfrage von Domscheit-Berg hervorgeht. Sie hält die vorhandenen Maßnahmen zur Überprüfung von Überwachungs- und Sicherheitsgesetzen offenbar für ausreichend. Dabei ist es nur eine Frage der Zeit, bis das nächste Gesetz¹⁹ in Karlsruhe gekippt wird.

Quelle: <https://netzpolitik.org/2021/ueberwachungsgesamt-rechnung-mehr-als-die-summe-der-einzelteile/>

Anmerkungen

- 1 <https://netzpolitik.org/2021/ohne-staatstrojaner-polizei-und-geheimdienste-koennen-whatsapp-mitlesen/>
- 2 <https://netzpolitik.org/2021/bundespolizeigesetz-grosse-koalition-einigt-sich-auf-staatstrojaner-einsatz-schon-vor-straftaten/>
- 3 <https://netzpolitik.org/2020/ulrich-kelber-fordert-ueberwachungsmoratorium/>
- 4 <https://netzpolitik.org/2021/justizstatistik-2019-polizei-nutzt-staatstrojaner-vor-allem-bei-erpressung-und-drogen/>
- 5 https://www.bverfg.de/e/rs20050412_2bvr058101.html
- 6 http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2010/03/rs20100302_1bvr025608.html

- 7 <https://csl.mpg.de/de/aktuelles/konzept-fuer-ein-periodisches-ueberwachungsbarometer/>
- 8 <https://shop.freiheit.org/#!/Publikation/1025>
- 9 <https://csl.mpg.de/de/aktuelles/entwicklung-eines-periodischen-ueberwachungsbarometers-fuer-deutschland/>
- 10 <https://netzpolitik.org/2021/bestandsdatenauskunft-2020-behoerden-fragen-alle-zwei-sekunden-wem-eine-telefonnummer-gehört/>
- 11 <https://dip.bundestag.de/vorgang/.../271425>
- 12 <https://netzpolitik.org/2021/vermittlungsausschuss-huerden-fuer-passwort-und-bestandsdatenauskunft-leicht-erhoeht/>
- 13 <https://fragdenstaat.de/blog/2019/05/02/klage-erfolgreich-berliner-verfassungsschutz-muss-auskunft-geben/>
- 14 <https://www.dr-datenschutz.de/urteil-polizei-uebermittelt-daten-illegal-an-den-verfassungsschutz/>
- 15 <https://www.fiff.de/publikationen/fiff-kommunikation/fk-jhrg-2019/fk-2019-4/fk-4-19-p37.pdf>
- 16 <https://www.hiig.de/en/jorg-pohle/>
- 17 <https://www.fiff.de/publikationen/fiff-kommunikation/fk-jhrg-2019/fk-2019-4/fk-4-19-p37.pdf>
- 18 https://mdb.anke.domscheit-berg.de/wp-content/uploads/2021/03/210331_SF_Maerz3_Ueberwachungsgesamtrechnung.pdf
- 19 <https://www.spiegel.de/netzwelt/netzpolitik/bundesverfassungsgericht-musterkommentar-zu-verfassungswidrigen-ueberwachungsgesetzen-wiederverwendbar-a-235f7c53-410a-420c-8809-8f1e5a042c7e>



Constanze Kurz, Markus Reuter

Horchen, aber nicht hacken

18. Mai 2023 – Die Bundespolizei soll künftig vermehrt Drohnen einsetzen und auch präventiv Telekommunikation überwachen dürfen. Ein „Gewahrsam“ droht für maximal vier Tage. Das geht aus dem Entwurf für das neue Bundespolizeigesetz hervor. Für staatliches Hacken soll es aber keine neuen Befugnisse geben.

Das Bundesministerium des Innern und für Heimat hat vergangene Woche den Referentenentwurf zum neuen Bundespolizeigesetz¹ vorgestellt. Damit wird das Bundespolizeigesetz (BPoLG) von 1994 überarbeitet, auch um dabei einigen Vorgaben des Urteils des Bundesverfassungsgerichts zum BKA-Gesetz² aus dem Jahr 2016 gerecht zu werden.

Da der Referentenentwurf nun vorliegt, läuft die Stellungnahmefrist. Dass der Entwurf noch verändert wird, ist wahrscheinlich. Hat das Gesetz später den Bundestag passiert, ist es auch im Bundesrat noch zustimmungspflichtig.

Telekommunikation abhören

Zwar sollen die Befugnisse der Bundespolizei zur technischen Überwachung in mehreren Bereichen erweitert werden, wenn es nach dem Entwurf aus dem Haus von Innenministerin Nancy Faeser (SPD) geht, nicht jedoch in Sachen Staatstrojaner: Der direkte Eingriff in informationstechnische Systeme von Verdächtigen ist weder in Form der *Quellen-TKÜ* noch als *Online-Durchsuchung* im Entwurf enthalten.

Beim Abhören der Telekommunikation im Zusammenhang mit der Sicherheit der Grenzen oder des Luft- und Bahnverkehrs soll



Fahrzeugmuseum Staßfurt, CC BY-NC-SA

die Befugnis der Bundespolizei allerdings um den Bereich der „präventiven“ Überwachung erweitert werden. „Präventiv“ bedeutet hier, dass noch kein konkreter begründeter Tatverdacht gegen eine Person vorliegt und damit die Strafprozessordnung zur Überwachung nicht herangezogen werden kann, aber dennoch das Abhören von Gesprächsinhalten von Zielpersonen bereits möglich ist.

Maximal für drei Monate kann die Überwachung der Telekommunikation von solchen Fast-schon-Verdächtigen richterlich angeordnet werden. Die betroffenen Telekommunikationsanbieter haben sie dann umzusetzen. Eine Erweiterung der Zeitspanne auf ein weiteres Vierteljahr ist jeweils möglich.

Neu aufgenommen ins Gesetz ist zudem die Verkehrsdatenabfrage, die bei Mobilfunkbetreibern vorgenommen werden darf, wenn eine dringende Gefahr besteht. Diese Befugnis zur Erhebung von Verkehrs- und Nutzungsdaten soll in bestimmten Fällen auch schon im Vorfeld einer dringenden Gefahr gelten, also ohne konkreten Anfangsverdacht, etwa im Zusammenhang mit „lebensgefährdenden Schleusungen“.

Dazu kommt die mit der Verkehrsdatenabfrage technisch eng verbundene und neu ins Gesetz aufgenommene Befugnis für die Bundespolizei, die sogenannte *Stille SMS* auch präventiv zu nutzen. Diese für den Telefonnutzer nicht sichtbaren Kurznachrichten dienen zum einen der Identifizierung von SIM-Karten, zum anderen aber auch der Lokalisierung von Mobilfunkgeräten. Je nach Abstand der beim Telefon eingehenden *Stillen SMS* lassen sich über eine Funkzellenbestimmung unterschiedlich präzise Bewegungsprofile erstellen. Möglich soll auch der Einsatz von sogenannten IMSI-Catchern sein, mit denen im direkten Umkreis der Überwachungsgeräte ebenfalls die Standorte von Mobiltelefonen ermittelt und zugleich auch Telefonate mitgeschnitten werden können.

Neu ins Gesetz aufgenommen wurde eine Berichtspflicht für einen Großteil der Befugnisse zu verdeckten Maßnahmen bei der Verkehrsdaten-, Telekommunikations- oder auch Wohnraumüberwachung, die auf das BKA-Gesetz-Urteil des Bundesverfassungsgerichts zurückgeht. Das Bundespolizeipräsidium wird das Bundesinnenministerium dadurch alle zwei Jahre über die praktische Umsetzung und den Umfang der Überwachungsmaßnahmen informieren. Mit einer zeitlichen Verzögerung soll das Ministerium dann auch den Deutschen Bundestag in Kenntnis setzen. Das soll eine öffentliche Diskussion über verdeckte Überwachungsmaßnahmen ermöglichen.

Drohnen und Kennzeichenerfassung

Die Bundespolizei darf künftig unter bestimmten Bedingungen auch weiterhin Kennzeichen von Fahrzeugen heimlich automatisch erfassen und abgleichen. Die Maßnahmen sollen anlassbezogen, vorübergehend und nicht flächendeckend passieren und müssen dokumentiert werden. Diese Dokumentationspflicht soll neu ins Gesetz kommen und ist eine Folge eines Urteils des Bundesverfassungsgerichts aus dem Jahr 2018 zur automatisierten Kraftfahrzeugkennzeichenkontrolle³. Bei Fällen von unmittelbarer Gefahrenabwehr oder bei Straftaten von erheblicher Bedeutung im Zusammenhang mit der Sicherheit der Grenzen können also weiter verdeckte Kennzeichenscanner zum Einsatz kommen. Finden sich beim automatischen Abgleich der Kennzeichendaten mit dem Fahndungsbestand keine Treffer, „sind die Daten sofort und spurlos zu löschen“.

Die Bundespolizei soll künftig auch Drohnen mit Bild- und Tonaufnahmegeräten mit Aufzeichnungsmöglichkeit nutzen dürfen, nämlich dort, wo sie auch sonst Bild und Ton aufzeichnen darf. Ohne Frage werden die Augen und Ohren der Polizei im Vergleich zu fest installierten Systemen damit mobiler und flexibler, entsprechend höher ist auch der Grundrechtseingriff für die Betroffenen bei jeder Nutzung. Auch eine Livebildübertragung von den Drohnen darf vorgenommen werden. Die Begründung zum vermehrten Drohneneinsatz leitet sich beispielsweise von den baulichen Umgebungen in Bahnhöfen oder Flughäfen oder durch unzugängliches Gelände oder aus bestimmten Veranstaltungsbedingungen her.

Kennzeichnungspflicht

Bürgerrechtliche Fortschritte leitet die Bundesregierung beim Thema individuelle Kennzeichnungspflicht ein: Polizisten und Polizistinnen der Bundespolizei müssen in Zukunft eine Kennzeichnung tragen, die es erlaubt, sie eindeutig zu identifizieren. Diese Kennzeichnungspflicht ist eine langjährige Forderung von Bürgerrechtsorganisationen, um der weitgehenden Straflosigkeit bei von Beamten begangenen Straftaten zu begegnen. Etwa die Hälfte aller Länderpolizeien hat eine solche Kennzeichnungs-

Constanze Kurz und Markus Reuter

Constanze Kurz⁴ ist promovierte Informatikerin, Autorin und Herausgeberin⁵ von Büchern⁶, zuletzt *Cyberwar*⁷. Ihre Kolumne *Aus dem Maschinenraum*⁸ erschien von 2010 bis 2019 im Feuilleton der FAZ. Sie lebt in Berlin⁹ und ist ehrenamtlich Sprecherin¹⁰ des Chaos Computer Clubs. Sie war Sachverständige der Enquete-Kommission „Internet und digitale Gesellschaft“ des Bundestags. Sie erhielt den Toleranz-Preis¹¹ für Zivilcourage und die Theodor-Heuss-Medaille. Kontakt: constanze(at)netzpolitik.org (PGP¹²).

Markus Reuter recherchiert und schreibt zu Digitalpolitik, Desinformation, Zensur und Moderation sowie Überwachungstechnologien. Darüber hinaus beschäftigt er sich mit der Polizei, Grund- und Bürgerrechten sowie Protesten und sozialen Bewegungen. Für eine Recherchereihe zur Polizei auf Twitter erhielt er 2018 den Preis des Bayerischen Journalistenverbandes¹³, für eine TikTok-Recherche 2020 den Journalismuspreis Informatik¹⁴. Bei netzpolitik.org ist er seit März 2016 als Redakteur dabei. Er ist erreichbar unter markus.reuter | ett | netzpolitik.org, auf Twitter unter @markusreuter_ und bei Mastodon¹⁵.

pflicht. Bei der Bundespolizei soll das Kennzeichen „in Form einer Ziffernfolge“ umgesetzt werden.

Beim Racial Profiling, also der Kontrolle von Menschen aufgrund äußerer gruppenbezogener Merkmale, bringt das Gesetz eine Neuerung, die in der Vergangenheit als Mittel zur Kontrolle von Polizeimaßnahmen ins Spiel gebracht worden war: Betroffene von Polizeikontrollen durch die Bundespolizei können sich in Zukunft eine Quittung geben lassen.

Flüchtlinge und Ballsportfreunde bleiben unter Verdacht

Die Bundespolizei soll aufgrund ihres Aufgabenprofils besonders die Grenzen sowie Bahnhöfe, Häfen und Flughäfen im Blick haben, weswegen in den Begründungen im Referentenentwurf oftmals grenzpolizeiliche Beispiele herangezogen werden. In der Fußballszone dürfte der Entwurf mit wenig Freude aufgenommen werden, denn die Überwachungsbefugnisse werden auch mit Veranstaltungslagen beim Sport und Auslandsfußballspielen begründet. Es drohen mehr Meldeauflagen, Aufenthaltsverbote und auch Ausreiseverbote für Fußballfans, die nun auch durch die Bundespolizei verhängt werden dürfen.

Weiterhin droht ein „Gewahrsam“, um ausgesprochene Aufenthaltsverbote und Ausreiseuntersagungen durchzusetzen: Bis zu maximal vier Tage darf die Freiheitsentziehung andauern. Begründet wird er mit der Durchsetzung von Maßnahmen beispielsweise gegen Menschenhändler, aber auch mit der Unterbindung der „Ausreise gewaltbereiter Fußballfans zu Auslandsspielen“.

Andre Meister

Chatkontrolle ist grundrechtswidrig und wird scheitern

17. Mai 2023 – Der Juristische Dienst des EU-Rats bezeichnet die Chatkontrolle als rechtswidrig und erwartet, dass Gerichte das geplante Gesetz wieder kippen. Die EU-Staaten nehmen das Gutachten zur Kenntnis und verhandeln trotzdem einfach weiter. Wir veröffentlichen ein eingestuftes Verhandlungsprotokoll.

Vor einem Jahr hat die EU-Kommission eine Verordnung zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern¹ vorgeschlagen. Das Gesetz soll Anbieter von Internetdiensten verpflichten, per Anordnung die Inhalte ihrer Nutzer:innen zu durchsuchen und strafbare Kinderpornografie² sowie Grooming an ein EU-Zentrum weiterzuleiten – die Chatkontrolle.

Im Bundestag kritisieren alle Sachverständigen bis zum Kinderschutzbund³: Die Chatkontrolle ist nicht notwendig, nicht effektiv und nicht verhältnismäßig. Jurist:innen bezeichnen die Maßnahmen als grundrechtswidrig und erwarten, dass Gerichte die Chatkontrolle kippen. Das sagen die deutschen⁴ und europäischen Datenschutzbeauftragten⁵, die Wissenschaftlichen Dienste von Bundestag⁶ sowie EU-Parlament⁷ und jetzt auch der Juristische Dienst des EU-Rats⁸.

Quelle: <https://netzpolitik.org/2023/bundespolizeigesetz-horchen-aber-nicht-hacken/>

Anmerkungen

- 1 https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwurfe/B1/ref-neustrukturierung-bundespolizeigesetz.pdf?__blob=publicationFile&v=5
- 2 https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/rs20160420_1bvr096609.html
- 3 https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2018/12/rs20181218_1bvr014215.html
- 4 https://de.wikipedia.org/wiki/Constanze_Kurz
- 5 <https://nowyouknow.eu/>
- 6 <http://gewissensbits.gi.de/constanze-kurz/>
- 7 <https://www.randomhouse.de/Buch/Cyberwar-Die-Gefahr-aus-dem-Netz/Constanze-Kurz/C.-Bertelsmann/e537921.rhd>
- 8 <http://www.faz.net/aktuell/feuilleton/aus-dem-maschinenraum/>
- 9 <https://wirsindderosten.de/menschen/constanze-kurz/>
- 10 <https://www.youtube.com/watch?v=hj3gAsqrB18>
- 11 <http://www.ev-akademie-tutzing.de/toleranz-preis-fuer-christian-wulff-und-constanze-kurz/>
- 12 <https://keys.openpgp.org/vks/v1/by-fingerprint/58ACBDA9D67D462D249605444A13B8EE269F8A45>
- 13 <https://netzpolitik.org/2018/bayerischer-journalisten-verband-ehrt-netzpolitik-org-fuer-recherche-zu-polizeitwitter/>
- 14 <https://saarland-informatics-campus.de/ueberuns-aboutus/journalismuspreis-informatik/>
- 15 <https://chaos.social/@markusreuter>



Die EU-Staaten verhandeln den Gesetzentwurf in der Ratsarbeitsgruppe Strafverfolgung. Ende April⁹ ging es erneut ausschließlich um die geplante Verordnung. Wir veröffentlichen ein weiteres Mal¹⁰ das eingestufte Protokoll der Verhandlungsrunde im Volltext¹¹.

Besonders schwerer Eingriff in Grundrechte

Zu Beginn der Sitzung stellte der Juristische Dienst des EU-Rats sein Gutachten¹² vor. Demnach verstößt das geplante Gesetz gegen die Grundrechtecharta¹³. Die Chatkontrolle betrifft alle Nutzer:innen der verpflichteten Kommunikationsdienste, „ohne dass diese Personen auch nur indirekt in eine Situation geraten, die eine strafrechtliche Verfolgung nach sich ziehen könnte“. Diese allgemeine und unterschiedslose Kontrolle ist unverhältnismäßig und erfüllt die Voraussetzungen für Grundrechtseingriffe nicht.

Der Europäische Gerichtshof hat mehrmals klargestellt, dass die Vorratsdatenspeicherung unvereinbar mit der Grundrechtcharta ist. Die Chatkontrolle geht noch über die Vorratsdatenspeicherung hinaus: Sie betrifft nicht nur Verkehrs- und Standortdaten, sondern auch Kommunikationsinhalte. Und sie richtet sich nicht nur gegen Terrorismus und Gefahren nationaler Sicherheit, sondern gegen Straftaten. Wenn das oberste EU-Gericht die Vorratsdatenspeicherung kippt, dann die Chatkontrolle erst recht.

Die Jurist:innen des EU-Rats wählen starke Worte. Die Chatkontrolle „beeinträchtigt den Wesensgehalt der Grundrechte“. Das Grundrecht auf Vertraulichkeit der Kommunikation könne „unwirksam und inhaltsleer“ werden. Es besteht „die ernsthafte Gefahr, sogar den Kern des Grundrechts auf Achtung des Privatlebens“ zu verletzen. Um irgendwie rechtmäßig zu werden, müsste sich die Chatkontrolle auf Personen beschränken, die mit sexuellem Missbrauch in Verbindung stehen.

Zehn Staaten ignorieren Rechtsgutachten

Die EU-Kommission, die den Gesetzentwurf vorgeschlagen hat, widerspricht der juristischen Bewertung des Rats ausdrücklich. Die Kommission geht „von einer grundlegend anderen rechtlichen Bewertung aus“. Sie kündigte an, eine schriftliche Stellungnahme zu erarbeiten, um die Perspektive der Rats-Jurist:innen zu kontern. Die EU-Staaten kündigten ebenfalls an, das Gutachten des EU-Rats zu prüfen. Dann verhandelten sie weiter.

Zehn EU-Staaten haben sich in einer Gruppe gleichgesinnter Staaten zusammengetan und eine gemeinsame Position formuliert¹⁴, die Irland vortrug. Sie fordern explizit, persönliche Kommunikation anlasslos zu durchsuchen, auch wenn die Nutzer:innen nicht im Verdacht stehen, mit Straftaten in Verbindung zu stehen. Die zehn Staaten wollen nicht nur nach bekannten strafbaren Inhalten suchen, sondern auch nach „unbekanntem Material“ sowie nach „Anwerbung von Kindern/Grooming“ – auch wenn dafür keine angemessene Technologie existiert.

Nach langem Streit fordert die deutsche Bundesregierung¹⁵, nur unverschlüsselte Kommunikation zu scannen und verschlüsselte Kommunikation auszunehmen. Dieser Forderung widersprechen die zehn Staaten, sie wollen Ende-zu-Ende-verschlüsselte Dienste nicht ausnehmen. Die Staatengruppe fordert zudem, das Gesetz möglichst noch dieses Jahr zu beschließen.

Undifferenzierte Gesamtüberwachung

Andere Staaten sind kritischer. Österreich äußerte „datenschutzrechtliche und grundrechtliche Bedenken“, der Gesetzentwurf beinhalte eine „undifferenzierte Gesamtüberwachung“. Deutschland verwies auf die Stellungnahme der Bundesregierung und forderte „wesentliche Änderungen“ des Gesetzes, will sich aber „weiterhin aktiv und konstruktiv“ einbringen. Polen betonte: „Verschlüsselung darf nicht gebrochen werden“.

Tschechien fordert, auch neues Missbrauchsmaterial zu suchen, dafür dürfe man die Chatkontrolle nicht auf potenzielle Straftäter beschränken. Die Niederlande hingegen haben mit Blick auf die aktuell existierenden Technologien „erhebliche Zweifel“, ob die Suche nach unbekanntem Material und Grooming verhältnismäßig ist. Estland und Malta fordern, „grundlegende Fragen zu klären, um geeignete, rechtlich tragbare Lösungen für dieses Dilemma zu finden“.

Im weiteren Verlauf diskutierten die Staaten die aktuellen Kompromissvorschläge¹⁶ der schwedischen Ratspräsidentschaft. Schweden kündigte an, dass sich der Ausschuss der Ständigen Vertreter der Mitgliedstaaten¹⁷ auf seiner heutigen¹⁸ Tagung¹⁹ mit der geplanten Verordnung und insbesondere mit „Umfang und Umgang mit Verschlüsselung“ befassen wird. Der Punkt wurde jedoch wieder von der Tagesordnung²⁰ gestrichen – die EU-Staaten streiten weiter.

Quelle: <https://netzpolitik.org/2023/juristisches-gutachten-chatkontrolle-ist-grundrechtswidrig-und-wird-scheitern/>. Dort ist auch das Dokument im Volltext zu finden.

Anmerkungen

- ¹ <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52022PC0209>
- ² <https://netzpolitik.org/2022/strafrecht-die-meisten-tatverdaechtigen-bei-kinderpornografie-sind-minderjaehrige/>
- ³ <https://netzpolitik.org/2023/anhoerung-im-bundestag-neun-zu-null-gegen-die-chatkontrolle/>
- ⁴ https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Telemedien/CSA_Verordnung.html
- ⁵ https://edpb.europa.eu/news/news/2022/proposal-combat-child-sexual-abuse-online-presents-serious-risks-fundamental-rights_de
- ⁶ <https://netzpolitik.org/2022/wissenschaftliche-dienste-chatkontrolle-darf-so-nicht-in-kraft-treten/>

Andre Meister

Andre Meister ist seit 2008 bei netzpolitik.org, seit 2012 festangestellt. Er beschäftigt sich vor allem mit investigativer Recherche. Andre hat Sozialwissenschaften²¹ an der Humboldt-Universität zu Berlin studiert und Abschlüsse in Bachelor²² und Master²³ zu netzpolitischen Themen gemacht. Er ist Gründungsmitglied der Vereine Digitale Gesellschaft²⁴, Gesellschaft für Freiheitsrechte²⁵ und netzpolitik.org, Mitglied im Chaos Computer Club²⁶ sowie Beobachter bei European Digital Rights²⁷. Nebenbei arbeitet er als System-Administrator.

- 7 [https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740248/EPRS_STU\(2023\)740248_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740248/EPRS_STU(2023)740248_EN.pdf)
- 8 https://cdn.netzpolitik.org/wp-upload/2023/05/2023-04-26_Council_Legal-Service_CSAR_8787.pdf
- 9 [https://www.consilium.europa.eu/de/meetings/mpo/2023/4/law-enforcement-police-\(330264\)/](https://www.consilium.europa.eu/de/meetings/mpo/2023/4/law-enforcement-police-(330264)/)
- 10 <https://netzpolitik.org/tag/rags/>
- 11 https://netzpolitik.org/2023/juristisches-gutachten-chatkontrolle-ist-grundrechtswidrig-und-wird-scheitern/#2023-04-17_StaV_RAGS_CSA-VO
- 12 https://cdn.netzpolitik.org/wp-upload/2023/05/2023-04-26_Council_Legal-Service_CSAR_8787.pdf
- 13 <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:12012P/TXT>
- 14 https://cdn.netzpolitik.org/wp-upload/2023/05/2023-04-27_Council_LEWP_LMG_CSAR_8833_Contexte.pdf
- 15 <https://netzpolitik.org/2023/bundesregierung-innenministerium-setzt-sich-bei-chatkontrolle-durch/>
- 16 <https://data.consilium.europa.eu/doc/document/ST-7842-2023-INIT/en/pdf>
- 17 <https://www.consilium.europa.eu/de/council-eu/preparatory-bodies/coreper-ii/>
- 18 17. Mai 2023
- 19 [https://www.consilium.europa.eu/de/meetings/mpo/2023/5/coreper-2-\(323946\)/](https://www.consilium.europa.eu/de/meetings/mpo/2023/5/coreper-2-(323946)/)
- 20 <https://data.consilium.europa.eu/doc/document/ST-9341-2023-INIT/de/pdf>
- 21 <https://www.sowi.hu-berlin.de/de>
- 22 https://cdn.netzpolitik.org/wp-upload/Bachelor_Meister_Vorratsdatenspeicherung.pdf
- 23 <https://cdn.netzpolitik.org/wp-upload/Master-Meister-Zugangsschwerungsgesetz.pdf>
- 24 <https://digitalegesellschaft.de/>
- 25 <https://freiheitsrechte.org/>
- 26 <https://ccc.de/>
- 27 <https://edri.org/>



Daniel Leisegang, Chris Köver, Sebastian Meineck

Die sechs größten Probleme im AI Act

10. Mai 2023 – Seit dem Hype um ChatGPT richten sich viele Blicke auf den geplanten AI Act. Die EU-Verordnung zu Künstlicher Intelligenz ist seit Jahren in der Mache und soll morgen im Parlament eine nächste Hürde überwinden. An mindestens sechs Stellen lauern Probleme.

Der AI Act soll das weltweit erste Gesetz werden, das „Künstliche Intelligenz“ (KI) umfassend reguliert. Dabei geht es nicht nur um seit kurzem gehypte Dienste wie ChatGPT¹. Die EU-Verordnung handelt etwa auch von Kameras am Bahnhof, die verdächtige Bewegungsmuster erfassen sollen, oder von Software in der Personalabteilung, die Bewerbungen sortiert. Vor allem aber soll die Verordnung rote Linien ziehen, in welchen Bereichen KI auf keinen Fall zur Anwendung kommen soll, etwa beim Social Scoring². So nennt man Punktesysteme, die Bürger:innen für unerwünschtes Verhalten bestrafen.

Am morgigen 11. Mai soll die KI-Verordnung eine weitere Hürde nehmen. An diesem Tag stimmen zwei wichtige Ausschüsse³ über den aktuellen Entwurf ab, auf den sich die Verhandler:innen des EU-Parlaments vor rund zwei Wochen geeinigt haben. Voraussichtlich Mitte Juni soll das Plenum des EU-Parlaments⁴ dann grünes Licht geben für den sogenannten Trilog, also die Verhandlungen zwischen Parlament, Ministerrat und Kommission über das endgültige Gesetz.

Ob die KI-Verordnung am Ende aber der versprochene große Wurf wird, muss bezweifelt werden. Denn die im April 2021 von der Kommission als Entwurf vorgelegte Verordnung⁵ weist zahlreiche Leerstellen auf, die ausgerechnet beim KI-Einsatz durch staatliche Behörden und das Militär besonders groß ausfallen. Weitere Lücken klaffen bei Fragen der Transparenz sowie der Möglichkeit von Betroffenen, sich gegen Diskriminierung durch KI-Systeme zu wehren. Die Übersicht:

1. Der AI Act soll staatliche, biometrische Massenüberwachung absegnen

Besonders aufmerksam verfolgen Bürgerrechtsgruppen die Debatte darum, wie die KI-Verordnung biometrische Überwachung regulieren soll⁶. Durch Biometrie – etwa einzigartige Merkmale im Gesicht – lassen sich Menschen identifizieren und massenhaft überwachen, gegebenenfalls auch in Echtzeit. Die Technologie bedroht damit unter anderem Privatsphäre und Versammlungsfreiheit.

Die Kommission möchte den Staaten in ihrem Entwurf beim Einsatz biometrischer Überwachung einige Freiheiten lassen. Zwar stuft sie solche Systeme als „hochriskant“ ein, möchte aber sogenannte „biometrische Echtzeit-Fernidentifizierungssysteme“ in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken dennoch zulassen. Das Parlament sieht dagegen strengere Regeln vor. Demnach zeichnet sich ab, dass die Abgeordneten zumindest den Einsatz biometrischer Überwachung in Echtzeit mehrheitlich ablehnen. Zugleich aber lassen sie die sogenannte retrograde Identifizierung im Nachhinein unter bestimmten Bedingungen zu. Diese wäre beispielsweise erlaubt, wenn sie gerichtlich genehmigt und im Zusammenhang mit schweren Straftaten steht.

Doch auch mit dieser Einschränkung würde die KI-Verordnung einer neuen Form der Massenüberwachung und Vorratsdatenspeicherung den Weg ebnen. Denn auch für eine eingeschränkte retrograde Identifizierung müssten Behörden fortan Videoaufnahmen in großem Umfang erstellen – also den öffentlichen Raum überwachen – und über einen längeren Zeitraum

speichern. Und um diese Aufnahmen abzugleichen, etwa mit dem Gesicht eines gesuchten Verdächtigen, müssten sie zudem biometrische Daten in großem Umfang sammeln und Strafverfolgungsbehörden verfügbar machen.

Für die sogenannte retrograde Videoüberwachung spricht sich auch die Bundesregierung aus⁷ – obwohl der Koalitionsvertrag⁸ das explizit ausschließt. Dort heißt es: „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.“

2. Die Verordnung begünstigt militärische KI-Aufrüstung

Mindestens ebenso gravierend ist eine große Ausnahme, die bereits im Entwurf der EU-Kommission vorgesehen ist: „Diese Verordnung gilt nicht für KI-Systeme, die ausschließlich für militärische Zwecke entwickelt oder verwendet werden.“

Das ist nichts anderes als ein Freifahrtschein für das Militär. Davon profitiert unter anderem die NATO. Das Militärbündnis aus 31 europäischen und nordamerikanischen Mitgliedstaaten hat im Februar begonnen, einen Zertifizierungsstandard für KI⁹ zu erarbeiten. Der Standard soll die Prinzipien umsetzen, die die NATO im Oktober 2021 in ihrer KI-Strategie¹⁰ verabschiedet hat, und legt den Fokus unter anderem auf autonome Waffensysteme.

Damit aber versäumt es die EU, den Einsatz von KI im Rahmen ihrer gemeinsamen Außen- und Sicherheitspolitik zu regulieren und dabei auch auf entsprechende Ambitionen ihrer Mitgliedsstaaten Einfluss zu nehmen – was sie durchaus könnte¹¹. So verfolgt innerhalb der Union allen voran Frankreich bereits seit Jahren eine militärische KI-Strategie. Hinzu kommt: Je weniger der militärische Bereich reguliert ist, desto größer ist die Gefahr eines globalen Rüstungswettlaufs¹².

Immerhin würde die geplante Verordnung sogenannte *Dual-Use-Systeme* strenger regulieren. So nennt man Technologien, die sowohl im zivilen als auch im militärischen Bereich eingesetzt werden. Brisant ist dabei jedoch die Frage, wo genau die Grenze verläuft: Dürfte das Militär beispielsweise auf Forschungsergebnisse und Produkte ziviler Einrichtungen zurückgreifen, um damit eigene Forschung zu betreiben oder gar Waffensysteme zu entwickeln?

3. Staaten wollen gefährliche KI-Systeme für die „nationale Sicherheit“ einsetzen

Bei den Verhandlungen zum geplanten AI Act versuchen einige EU-Staaten und Abgeordnete, weitere Lücken ins Gesetz zu reißen. Konkret geht es um Ausnahmen bei Belangen der „nationalen Sicherheit“. Der von der slowenischen EU-Ratspräsidentschaft angenommene Kompromisstext¹³ hat diese Forderung bereits im November 2021 übernommen, der Rat hat das ein Jahr später bekräftigt¹⁴.

Mit Verweis auf die „nationale Sicherheit“ könnten selbst autoritäre EU-Regierungen wie etwa die in Ungarn nach Belieben selbst gefährlichste KI-Systeme einsetzen. Darunter fallen,

selbst wenn die KI-Verordnung das zunächst untersagt, auch biometrische Massenüberwachung¹⁵ oder Social Scoring für EU-Bürger:innen.

Dass dies dem Missbrauch geradezu Tür und Tor öffnet, zeigt nicht zuletzt die staatliche Spionagesoftware Pegasus¹⁶, angeboten von der israelischen NSO Group. Diese Technologie wurde laut Herstellerangaben ausschließlich für Zwecke der nationalen Sicherheit entwickelt. Inzwischen ist bekannt, dass auch Oppositionelle, Journalist:innen und Dissident:innen in der EU ins Visier gerieten. Nicht nur in Ungarn und Polen, sondern auch in Griechenland und Spanien.

Das EU-Parlament hat diese Gefahr offenbar erkannt. Der Kompromissentwurf, über den morgen abgestimmt wird, beschränkt sich auf die Ausnahmen für militärische Nutzung. Ob der Rat sich damit zufriedengibt oder weiterhin auf die „nationale Sicherheit“ als Ausnahme pocht, wird sich in den Trilog-Verhandlungen zeigen.

4. Es soll weiter aggressive KI-Systeme an den Außengrenzen geben

In den vergangenen Jahren hat die EU ihre Außengrenzen massiv mit KI-Systemen aufgerüstet¹⁷. Sie kontrolliert und überwacht Menschen, die sich in die EU hineinbewegen, und verwandelt die Grenze zum Experimentierlabor für neue Technologien. Ob biometrische Gesichtserkennung, Überwachungsdrohnen über Geflüchtetenlagern oder Scannen nach angeblich verdächtigen Bewegungen – vieles, was beim Einsatz gegen EU-Bürger:innen für einen Aufschrei sorgen würde, scheint an der Grenze akzeptabel. Auch im Asylprozess kommen KI-Systeme zum Einsatz, etwa die Software zur Dialekterkennung, mit der das Bundesamt für Asyl Hinweise auf die Herkunft von Geflüchteten sucht¹⁸.

Auf den ersten Blick nimmt der Entwurf des AI Act die Probleme dieser Technologien ernst: „KI-Systeme, die in der Migrations-, Asyl- und Grenzverwaltung eingesetzt werden, betreffen Menschen, die sich oft in einer besonders verletzlichen Lage befinden und von den Ergebnissen der Maßnahmen der zuständigen Behörden abhängig sind.“ Der Entwurf stuft die Technologien daher als hochriskant ein; hier seien Grundrechte in Gefahr.

Doch unterm Strich dürfte der AI Act am Einsatz der Technologien¹⁹ wenig ändern – nicht einmal dort, wo KI-Systeme größte Gefahren für das Leben, die Sicherheit und weitere Menschenrechte darstellen. So dürfte die EU-Grenzagentur Frontex weiterhin das Mittelmeer oder Grenzzäune mit autonomen KI-Systemen überwachen, auch wenn dies womöglich zu illegalen Pushbacks führt und Menschen dadurch ihr Recht auf Asyl nicht wahrnehmen können. Selbst wissenschaftlich umstrittene Technologien wie etwa der „KI-Lügendetektor“ AVATAR²⁰ dürften weiter an den EU-Grenzen zum Einsatz kommen.

Zivilgesellschaftliche Organisationen wie EDRI und Amnesty International halten das für fahrlässig und fordern seit langem Änderungen²¹ am Gesetzentwurf. Die Aussichten für den besseren Schutz von Grundrechten an der EU-Grenze dürften jedoch gering sein. Erst kürzlich haben EU-Staaten etwa ein neues System geschaffen, das einzelne Personen einer datenbasierten Risikoanalyse unterzieht: das Reisegenehmigungssystem ETIAS²².

Ab Ende des Jahres muss jede Person, die den Schengenraum ohne Visum betreten will, vorher einen Antrag stellen. Ihre Daten werden automatisch mit zahlreichen Datenbanken abgeglichen²³ und auf Risiken überprüft. Die Technologie dahinter ist für Betroffene undurchsichtig²⁴ und wird das auch bleiben, wenn der AI Act nicht nachbessert. Voraussichtlich darf die EU weiterhin von *AI border guards*²⁵ schwärmen, die in Zukunft angeblich lügende Ausländer:innen anhand von Körpersprache erkennen sollen.

5. Es fehlen Rechte für Betroffene, um sich zu wehren

Als eines ist der AI Act sicher nicht geplant worden: als Gesetz zum Schutz von Verbraucher:innen. Im Gegenteil: Im Entwurf der Kommission waren keine direkten Beschwerde-Mechanismen für die Menschen vorgesehen, deren Grundrechte von solchen Systemen verletzt wurden.

Hier versucht der EU-Rat gegenzusteuern. Dessen Position sieht vor, dass Personen bei der zuständigen Aufsichtsbehörde eine Beschwerde einreichen können. Die Organisation Algorithm-Watch weist aber darauf hin, dass diese Rechte nicht annähernd weit genug gehen²⁶. AlgorithmWatch fordert unter anderem: „Betroffenen selbst sollte ein Recht auf Information und auf Erklärung zugesprochen werden, da Transparenz die Voraussetzung dafür ist, dass algorithmische Diskriminierung erkannt wird und Betroffene geeignete Rechtsmittel ergreifen können.“

Trotz der Lücken im geplanten AI Act gibt es Gesetze, die Betroffene von Diskriminierung durch KI-Systeme schützen können. Zum Beispiel müssen große Online-Plattformen laut Digitale-Dienste-Gesetz²⁷ künftig einschätzen, welche Risiken sie verursachen und etwas dagegen unternehmen. Betroffene von Diskriminierung können sich in Deutschland auf das Allgemeine Gleichbehandlungsgesetz²⁸ berufen. Und in der DSGVO (Datenschutzgrundverordnung) steht sogar ein Schutz vor automatisierten Entscheidungen²⁹, die Menschen beeinträchtigen.

Darüber hinaus hat die Kommission im vergangenen September einen neuen Richtlinienentwurf vorgestellt³⁰. Er zielt auf algorithmische Entscheidungssysteme ab und soll klären, wer haftet, wenn ein KI-System Schäden verursacht – etwa, wenn fehlerhaftes Datenmaterial zu Diskriminierung bei der Kreditvergabe oder im Bewerbungsverfahren führt.

Verbände wie BEUC³¹, EDRi³² oder Amnesty International³³ finden allerdings, in der Praxis hilft das zu wenig. Sie haben gehofft, der AI Act könnte die Chance nutzen und Lücken schließen. Die wichtigen Ausschüsse im EU-Parlament haben hierfür bereits grundlegende Anpassungen im Gesetz vorgesehen³⁴.

6. Weiche Definitionen können den AI Act zahnlos machen

Gut gemeint ist nicht gleich gut gemacht – das beschreibt eine weitere und obendrein grundlegende Schwäche des AI Act treffend. Das beginnt bei der Definition von „KI-Systemen“, um die sicherlich noch gerungen wird. Diese Definition hat großen Einfluss darauf, wer sich an strengere Regeln halten muss – und wer

nicht. Soll die KI-Verordnung nur maschinelles Lernen regulieren oder auch viele andere Dinge, die sich „KI“ nennen? Unter anderem die SPD warnte Anfang des Jahres³⁵ vor einer zu engen Definition. Das Argument: Potentiell gefährliche Anwendungen könnten durchs Raster fallen.

Die Frage nach der Definition ist so grundlegend, sie könnte die hehren Ziele des AI Acts untergraben. Im weiten Sinne ist KI ein Sammelbegriff für Anwendungen, die viele Daten zueinander in Beziehung setzen und auf dieser Grundlage Antworten berechnen. Und ausführlich beschreibt der Entwurf der Kommission, was bei KI-Systemen alles schiefgehen kann. Sie können demnach die Menschenwürde verletzen und die Privatsphäre einschränken; sie können sexistisch und/oder rassistisch sein oder Menschen mit Behinderung benachteiligen. Die Liste von Hochrisiko-Systemen ist umfassend und reicht von Lügendetektoren über Deepfake-Erkennung bis hin zu Software, die kriminelles Verhalten vorhersagen soll, sogenanntes Predictive Policing.

Das führt direkt zum nächsten Problem mit Definitionen: Um diese und weitere Gefahren einzudämmen, sollen die Daten hinter solchen KI-Systemen „hinreichend relevant, repräsentativ, fehlerfrei und vollständig sein“. Das klingt traumhaft, aber dieses Ziel zu erreichen, ist leichter gesagt als getan. Streng genommen beschreiben die Worte eine Utopie, denn riesige Datensätze sind nie „frei“ von Fehlern. Und das Wort „repräsentativ“ wirft die Frage auf, was genau die Daten eines KI-Systems repräsentieren sollen. Denn oft spiegeln KI-Systeme gerade die Missstände einer sexistisch und rassistisch strukturierten Realität wider und drohen, diese noch weiter zu verfestigen – und das wäre wohl kaum im Sinne der Gesetzgeber:innen.

Pragmatische Lösungen sind dennoch denkbar, das zeigt etwa ein Fachartikel des deutschen Rechtswissenschaftlers Philipp Hacker in der Zeitschrift *Law, Innovation and Technology*³⁶. Darin macht ein konkretes Beispiel anschaulich, was hinter einem Begriff wie „repräsentativ“ stecken kann: „Wenn die KI eines autonomen Fahrzeugs während des Trainings hauptsächlich mit Menschen weißer Hautfarbe konfrontiert wird, kann es sein, dass sie Menschen dunklerer Hautfarbe nicht oder weniger oft erkennt.“ Im besten Fall kann der AI Act also Entwickler:innen dazu verpflichten, solche Fehler in den Trainingsdaten zu vermeiden.

Was die Verordnung letztlich bewirken kann, hängt also auch maßgeblich davon ab, wie der Gesetzgeber solche Begriffe wie „KI-System“ und „hinreichend repräsentativ“ ausgestaltet. Selbst wenn sich der AI Act durch seinen Namen als das KI-Gesetz schlechthin darstellt – er bildet letztlich nur einen Baustein von etwas Größerem. Es liegt nun an den Organen der EU, wie wichtig dieser Baustein wird.

Quelle: <https://netzpolitik.org/2023/kuenstliche-intelligenz-die-sechs-groessten-probleme-im-ai-act/>

Anmerkungen

1 <https://www.reuters.com/technology/behind-eu-lawmakers-challenge-rein-chatgpt-generative-ai-2023-04-28/>

2 <https://netzpolitik.org/2022/ueberwachung-in-china-totale->

- praeventive-kontrolle/
 3 <https://agenparl.eu/2023/05/09/highlights-artificial-intelligence-act-vote-on-11-may-2023-committee-on-the-internal-market-and-consumer-protection>
 4 <https://www.euractiv.com/section/artificial-intelligence/news/meps-seal-the-deal-on-artificial-intelligence-act/>
 5 <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021PC0206>
 6 <https://netzpolitik.org/2023/ai-act-bundesregierung-setzt-sich-eu-ebene-fuer-mehr-gesichtserkennung-ein/>
 7 <https://netzpolitik.org/2023/ai-act-bundesregierung-setzt-sich-eu-ebene-fuer-mehr-gesichtserkennung-ein/>
 8 https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf
 9 <https://www.behörden-spiegel.de/2023/02/15/nato-zertifizierungsstandard-fuer-kuenstliche-intelligenz/>
 10 https://www.nato.int/cps/en/natohq/news_187934.htm
 11 https://ecnl.org/sites/default/files/2022-03/ECNL_Pagers_on_scope_of_AIA_ECNL_FINAL.pdf
 12 <https://www.deutschlandfunk.de/ki-kuenstliche-intelligenz-waffensysteme-100.html>
 13 <https://data.consilium.europa.eu/doc/document/ST-14278-2021-INIT/en/pdf>
 14 <https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf>
 15 <https://edri.org/our-work/remote-biometric-identification-a-technical-legal-guide/>
 16 <https://netzpolitik.org/2023/pega-untersuchungsausschuss-mit-samthandschuhen-gegen-staatstrojaner>
 17 [https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA\(2021\)690706_DE.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA(2021)690706_DE.pdf)
 18 <https://netzpolitik.org/2022/asylverfahren-bamf-weitet-automatische-sprachanalyse-aus/>
 19 <https://www.bosch-stiftung.de/de/publikation/eus-ai-act-and-its-human-rights-impacts-people-crossing-borders>
 20 <https://www.governmentciomedia.com/ai-lie-detectors-could-soon-police-borders>
 21 <https://edri.org/our-work/civil-society-calls-for-the-eu-ai-act-to-better-protect-people-on-the-move/>
 22 <https://www.etiasvisa.com/>
 23 https://de.wikipedia.org/wiki/Europäisches_Reiseinformations-_und_genehmigungssystem#Datenabgleich
 24 <https://verfassungsblog.de/frontex-and-algorithmic-discretion-part-i/>
 25 <https://www.etiasvisa.com/etias-news/etias-artificial-intelligence-border-control>
 26 <https://algorithmwatch.org/de/schutz-vor-grundrechtsverletzungen-ai-act-agg/>
 27 <https://netzpolitik.org/2022/eu-digitalpaket-das-muessen-eu-laender-und-online-anbieter-jetzt-aendern/>
 28 <https://algorithmwatch.org/de/autocheck-ratgeber-diskriminierung/>
 29 <https://dsgvo-gesetz.de/art-22-dsgvo/>
 30 <https://netzpolitik.org/2022/produkt haftung-eu-kommission-will-klare-haftungsregeln-fuer-ki-systeme/>
 31 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Kunstliche-Intelligenz-ethische-und-rechtliche-Anforderungen/F2665432_de
 32 <https://edri.org/wp-content/uploads/2022/05/Rights-and-Redress-AIA-Amendments-for-online.pdf>
 33 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665634_en
 34 https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-072_Letter_to_european_parliament_committees_imco_libe_ai_act_consideration_of_amendments_on_30_june.pdf
 35 <https://netzpolitik.org/2023/ai-act-spd-fraktion-graetscht-in-die-regierungsposition-bei-eu-verhandlungen/>
 36 <https://www.tandfonline.com/doi/full/10.1080/17579961.2021.1977219>
 37 <https://www.blaetter.de/>
 38 http://www.schmetterling-verlag.de/page-5_isbn-3-89657-068-4.htm
 39 <https://www.alternativer-medienpreis.de/preistraeger-2016/daniel-leisegang/>
 40 <https://www.eurozine.com/>
 41 <https://missy-magazine.de/online-magazin/>
 42 <https://sebmeineck.substack.com/>



Daniel Leisegang, Chris Köver und Sebastian Meineck

Daniel Leisegang ist Politikwissenschaftler und seit August 2022 Co-Chefredakteur bei netzpolitik.org. Zuvor war er Redakteur bei den *Blättern für deutsche und internationale Politik*³⁷. 2014 erschien von ihm das Buch *Amazon – Das Buch als Beute*³⁸; 2016 erhielt er für seinen Beitrag *Facebook rettet die Welt* den Alternativen Medienpreis³⁹ in der Rubrik *Medienkritik*. Daniel gehört dem Board of Trustees von Eurozine⁴⁰ an.

Chris Köver ist seit 2018 Redakteurin von netzpolitik.org. Sie recherchiert unter anderem zur Digitalisierung des Gesundheitswesens, Digitaler Gewalt und dem Datenschutz von Geflüchteten. Vorherige Stationen: WIRED Germany (Redakteurin), Zeit Online (Volontärin), Akademie für Publizistik (Trainerin). Chris war Mitgründerin und Chefredakteurin der Zeitschrift *Missy Magazine*⁴¹ und wurde dafür als eine der Journalist:innen des Jahres ausgezeichnet. Für ihre Recherche *TikToks Obergrenze für Behinderungen* erhielt sie 2020 den Journalist:innenpreis Informatik.

Sebastian Meineck ist seit 2021 Redakteur bei netzpolitik.org. Außerdem schreibt er einen Newsletter über Online-Recherche⁴². Zu seinen vorigen Stationen gehören Funk (Redakteur & Realisator für SoManyTabs), 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. 2022 erhielt eine seiner Recherchen den Ernst-Schneider-Preis.

Womit sich Strafverfolger bald befassen müssen

27. März 2023 – Ein Europol-Bericht widmet sich den Folgen von ChatGPT, wenn Kriminelle die Fähigkeiten des Chatbots für sich ausnutzen: Es drohe vermehrt Phishing und noch mehr Desinformation. Ein Problem für die Strafverfolgung könne auch automatisiert erzeugter bössartiger Quellcode sein.

Heute hat Europol einen kurzen Forschungsbericht mit dem Titel *ChatGPT – The impact of Large Language Models on Law Enforcement*¹ vorgestellt. Der Bericht setzt sich mit der heutigen und der bereits absehbaren kriminellen Nutzung von ChatGPT und der sich daraus ergebenden Strafverfolgung auseinander. ChatGPT ist ein sogenannter Chatbot des Anbieters OpenAI in Partnerschaft mit Microsoft, der im November 2022 veröffentlicht² wurde und plausibel klingende Textantworten produziert.

Im Bereich der *Künstlichen Intelligenz* gehört ChatGPT zur Klasse der sogenannten künstlichen neuronalen Netzwerke und hier speziell der LLMs (Large-Language-Modelle)³, die Sprachmuster nachbilden. Auch die Konkurrenz von Microsoft und OpenAI arbeitet an vergleichbaren KI-Modellen, die nach einem Eingabebefehl verständliche Texte auswerfen.

Wer sich schon länger mit der kriminellen oder generell mit der unethischen Nutzung von Technologien des maschinellen Lernens auseinandersetzt, findet im Bericht des *Europol Innovation Lab* zwar keine augenöffnenden Neuigkeiten. Allerdings bietet dieser eine praxisbezogene Zusammenfassung dessen, womit sich Strafverfolger heute oder in naher Zukunft befassen müssen. Der Bericht ist das Ergebnis verschiedener Workshops, in denen Ermittler von ihren bisherigen Erfahrungen berichtet hatten. Es gibt noch eine erweiterte Berichtsversion, die aber nicht öffentlich zugänglich ist.

Was Ermittlern Sorge bereitet

Ein Problemfeld bei den Sprachmodellen sieht der Europol-Bericht im Bereich Propaganda und Falschinformationen. Da ChatGPT auf Knopfdruck und „in großem Umfang authentisch klingende Texte“ liefere, sei „das Modell ideal für Propaganda- und Desinformationszwecke“. Der Aufwand sei gering, um auf diese Weise Falschnachrichten zu erstellen.

Der Europol-Bericht betrachtet zwar nicht allgemein KI-Anwendungen, sondern nur speziell das textbasierte ChatGPT. Ein Teilbereich, der sich für Desinformation und absichtliche Falschdarstellungen aber in Kombination mit ChatGPT anbietet, ist die Bildgenerierung. Sie hat jüngst große Verbesserungen gezeigt: Erzeugte Bilder von tatsächlichen Fotografien zu unterscheiden, ist bei einer Vielzahl von Bildern kaum mehr möglich.

Laut der Europol-Berichtersteller kann ChatGPT auch Betrug und Techniken des Social Engineerings den Weg ebnen. Insbesondere beim Phishing versucht der Angreifer, potentiellen Opfern fingierte Informationen in vertrauensenerweckendem Aussehen unterzuschieben, meist um an Passwörter und andere persönliche Daten zu gelangen. Weil ChatGPT realistisch wirkende und grammatikalisch korrekte Texte produziert, ist es schon jetzt ein nützliches und skalierendes Werkzeug für Phishing. Auch eine Sprachausgabe⁴

des produzierten Textes erfolgt inzwischen mit nur geringer Verzögerung, was weitere Täuschungsmöglichkeiten eröffnet.

Sorgen bereitet den Ermittlern auch die Möglichkeit des Umgehens oder Entfernens von Nutzungsaufgaben oder Sicherheits-schranken, die Anbieter wie OpenAI zwar eingerichtet haben, die aber durch bestimmte Eingabekommandos nichtig werden. Dieses sogenannte Jailbreaking hat bei ChatGPT die Abkürzung DAN (Do Anything Now, auf Deutsch etwa: Alles kann jetzt getan werden).

Als OpenAI-Geschäftsführer Sam Altman jüngst auf diese Problematik in einem Interview angesprochen wird, sieht er darin kein großes Problem⁵. Altman glaubt, dass Jailbreaking dann unattraktiv werde, wenn Nutzer künftig mehr Kontrolle über die KI erhielten. Dem öffentlichen Teil des Berichts zufolge liegt Europol jedoch kein aktuell funktionierender DAN für ChatGPT vor, so dass nur Vorfälle aus den vergangenen Wochen⁶ einbezogen werden konnten.

Allerdings ist ein DAN-Modus nicht die einzige Variante, um aus ChatGPT potentiell Bössartiges herauszulocken, das der Anbieter gern versteckt hätte. Denn letztlich ist ChatGPT nur ein prachtvoll bunter Papagei, der die Semantik eines Textes nicht erfassen kann. Das gilt umso mehr für Programmiersprachen und automatisierte Quellcode-Generierung. Zudem erfordert es nicht allzu viel Fantasie, um ChatGPT dazu zu bringen, böswillige Quellcode-Fragmente zu produzieren. So stellt der Bericht fest, dass „die Schutzmaßnahmen, die ChatGPT daran hindern, potentiell bössartigen Code bereitzustellen, nur funktionieren, wenn das Modell versteht, was es tut“. Und das tut es bekanntlich nicht. Vor allem die Fähigkeit, natürliche Sprache in zumindest teilweise funktionierenden Quellcode zu gießen, böte schon heute und künftig wohl noch weit mehr Möglichkeiten für kriminellen Missbrauch.

Da Weiterentwicklungen der LLMs eine noch größere Datenbasis aufweisen dürften und außerdem in andere digitale Dienste integriert werden, fällt der Ausblick des Europol-Berichts nicht eben optimistisch aus: Man stelle sich bereits auf „dark LLMs“ ein, die speziell für betrügerische Zwecke trainiert und „kriminelle Geschäftsmodelle der Zukunft“ unterstützen werden.

Quelle: <https://netzpolitik.org/2023/chatgpt-womit-sich-strafverfolger-bald-befassen-muessen/>

Anmerkungen

- ¹ <https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf>
- ² <https://openai.com/blog/chatgpt>

- 3 https://en.wikipedia.org/wiki/Large_language_model
4 <https://twitter.com/ggerganov/status/1640022482307502085>
5 https://www.reddit.com/r/ChatGPT/comments/122f2gh/openai_ceo_sam_altman_talking_about_dan_and/

- 6 <https://www.washingtonpost.com/technology/2023/02/14/chatgpt-dan-jailbreak/>

Information zur Autorin siehe Seite 53



Daniel Leisegang

Prekäre Klickarbeit hinter den Kulissen von ChatGPT

20. Januar 2023 – Arbeiter:innen in Kenia sollten teils traumatisierende Texte lesen, um ChatGPT zu optimieren. Ihr Stundenlohn: bis zu zwei US-Dollar. Eine Recherche des Time Magazines zeigt: Hinter dem Hype um die Künstliche Intelligenz steckt auch eine Geschichte von Ausbeutung im globalen Süden.

Jede Menge Nutzer:innen reden derzeit über und mit ChatGPT. Der mächtige Text-Generator lässt sich in Dialoge verwickeln, erstellt auf Anfrage Essays zu den entlegensten Themen, Gedichte verschiedener Stilrichtungen, komplexe Programmcodes und vieles mehr. Nun zeigt eine Recherche des US-amerikanischen Time Magazine¹, welche Rolle schlecht bezahlte Arbeiter:innen aus Kenia bei der gehypten Anwendung spielen.

ChatGPT stammt von OpenAI, einem US-Unternehmen mit Sitz in Kalifornien. Nachdem OpenAI das Programm im November vergangenen Jahres veröffentlicht hatte, verzeichnete es schon nach nur einer Woche eine Million Nutzer:innen. Innerhalb kurzer Zeit stieg OpenAI zu einer der wertvollsten KI-Firmen weltweit auf. Neben ChatGPT bietet OpenAI den Bild-Generator DALL-E-2 an. In naher Zukunft will das Unternehmen darüber hinaus Anwendungen anbieten, die Videos und menschliche Stimmen generieren.

Der Erfolg von ChatGPT beruht nicht nur auf Codezeilen und Datenbanken, sondern auch auf mühsamer Handarbeit. Denn bevor Millionen Nutzer:innen mit ChatGPT ins Gespräch kamen, haben Arbeiter:innen in Kenia unter prekären Bedingungen die Anwendung optimiert. Sie haben dazu beigetragen, dass die Antworten des Text-Generators „weniger toxisch“ ausfallen, wie aus der Times-Recherche hervorgeht.

Dass auch sogenannte „Künstliche Intelligenz“ nicht ohne menschliche Hilfe auskommt, ist zunächst nicht neu oder überraschend. Auch Konzerne wie Google² setzen dafür Menschen ein. Der neue Bericht liefert allerdings einen eindrücklichen Einblick in die Arbeitsbedingungen hinter den Kulissen. Die Tätigkeit wird dabei nicht etwa zum US-Mindestlohn im Silicon Valley verrichtet, sondern verstärkt in den globalen Süden ausgelagert – mit schlechten Arbeitsbedingungen. In diesem Fall hat das von OpenAI beauftragte Unternehmen Samasource die Zusammenarbeit vorzeitig beendet.

Für die Recherche hat das Time Magazine Hunderte Seiten interner Dokumente von Samasource und OpenAI geprüft und vier Mitarbeitende interviewt, die an dem Projekt gearbeitet haben.

Zwei US-Dollar pro Stunde

Wie OpenAI hat die auch als Sama bekannte Firma ihren Hauptsitz in San Francisco. Samas Angestellte leben dagegen vorwiegend in Kenia, Uganda und Indien, wo sie unter anderem Daten

kennzeichnen und kategorisieren. Nach eigenen Angaben habe Sama dabei geholfen, mehr als 50.000 Menschen aus der Armut zu befreien³.

Im Auftrag von OpenAI beschäftigte Sama seit November 2021 rund drei Dutzend Arbeiter:innen in Kenia. Ihre Aufgabe bestand darin, Textausschnitte auf schädliche Inhalte hin zu lesen und zu markieren. Die entsprechenden Passagen wurden dann in ein Datenset übertragen, mit dem OpenAI einen Sicherheitsmechanismus auf KI-Basis trainierte. Die sogenannten *pre-training filter* dienen dazu, schädliche Textpassagen aus den Trainingsdaten von ChatGPT zu entfernen. Die Grundlage für diese Trainingsdaten bilden Texte, die OpenAI zuvor massenhaft aus dem Internet geschürft hatte.

Die Arbeitskräfte müssen also Inhalte sichten und aussortieren, weil spätere ChatGPT-Nutzer:innen von ähnlichen Inhalten verschont werden sollen. „Die Klassifizierung und Filterung von schädlichen [Texten und Bildern] ist ein notwendiger Schritt, um die Menge an gewalttätigen und sexuellen Inhalten in den Trainingsdaten zu minimieren und Werkzeuge zu entwickeln, die schädliche Inhalte erkennen können“, so ein Sprecher von OpenAI gegenüber dem Time Magazine⁴.

In einer neunstündigen Schicht mussten die Arbeiter:innen bis zu 250 Textpassagen von einer Länge bis zu 1.000 Wörtern lesen, wie aus der Recherche hervorgeht. Zum Vergleich: Dieser Text enthält rund 800 Wörter. Im Gegenzug erhielten die Arbeiter:innen – je nach Dienstalter und Leistung – einen Stundenlohn zwischen 1,32 und 2 US-Dollar. Das entspricht laut Times in etwa dem Gehalt einer Empfangsangestellten in einem Hotel in Nairobi.

OpenAI bezahlte Sama einen vertraglich festgelegten Stundenlohn in Höhe von 12,50 Dollar – und damit bis zu neun Mal mehr als die Arbeiter:innen pro Stunde bekamen. Dieser Betrag habe jedoch sämtliche Kosten des Unternehmens abdecken müssen, rechtfertigt ein Sama-Sprecher die Differenz.

„Vom ständigen Nachdenken verstört“

Für ihr Gehalt mussten die Arbeiter:innen mitunter Beschreibungen lesen, die lebhafteste Darstellungen unter anderem von sexueller Gewalt, Suiziden und Tierquälerei enthielten. „Das war Folter“, sagte einer der Arbeiter gegenüber dem Time Magazine.

„Man liest im Laufe der Woche etliche solcher Beschreibungen. Und wenn es dann Freitag wird, ist man vom ständigen Nachdenken darüber verstört.“

Um die zum Teil traumatisch wirkenden Darstellungen zu verarbeiten, hätten die Arbeiter:innen um psychologische Unterstützung gebeten. Diese habe Sama ihnen aber nur eingeschränkt gewährt. Das Unternehmen widerspricht dieser Darstellung, wie das Time Magazine berichtet: Es habe für die Arbeiter:innen „jederzeit“ die Möglichkeit bestanden, sowohl an therapeutischen Gruppensitzungen als auch an Einzelgesprächen mit professionellen Therapeut:innen teilzunehmen.

Im Februar 2022 beauftragte OpenAI Sama mit einem weiteren Projekt, das die Kategorisierung von Bildern vorsah, heißt es im Bericht. Einige der Bilder sollen demnach Gewalt an Kindern, Morde und Vergewaltigungen gezeigt haben. Unter US-amerikanischem Gesetz soll der Inhalt einiger der Darstellungen verboten gewesen sein.

Wenige Wochen später löste Sama den Vertrag mit OpenAI vorzeitig auf, acht Monate vor dessen Ablauf. Das heißt, die Arbeiter:innen müssen seitdem nicht länger verstörende Daten

für OpenAI sichten. Allerdings mussten die meisten von ihnen daraufhin weniger gut bezahlte Tätigkeiten übernehmen, berichtet das Magazin, andere verloren ihre Anstellung. Sama hat nach eigenen Angaben inzwischen seine Leitlinien überarbeitet. Kürzlich gab das Unternehmen bekannt, aus dem Geschäft mit Inholdemoderation auszusteigen⁵.

Quelle: <https://netzpolitik.org/2023/globaler-sueden-prekaere-klickarbeit-hinter-den-kulissen-von-chatgpt/>

Anmerkungen

- 1 <https://time.com/6247678/openai-chatgpt-kenya-workers/>
- 2 <https://www.vice.com/de/article/59ngya/google-sprachaufnahmen-vice-berichtet-aus-dem-alltag-eines-laushers>
- 3 <https://www.sama.com/blog/we-are-a-b-corp/>
- 4 <https://time.com/6247678/openai-chatgpt-kenya-workers/>
- 5 <https://netzpolitik.org/2023/facebook-in-afrika-neue-inholdemoderation-gesucht/>

Information zum Autor siehe Seite 59



Anna-Lena Schmierer

Datenschutzkonferenz nimmt ChatGPT unter die Lupe

7. April 2023 – Die italienische Datenschutzbehörde sperrte ChatGPT vor wenigen Tagen landesweit und der kanadische Datenschutzbeauftragte hat ebenfalls Untersuchungen eingeleitet. Nun prüft auch die hiesige Datenschutzkonferenz, ob das Unternehmen OpenAI, das ChatGPT anbietet, gegen die DSGVO verstößt.

ChatGPT gerät zunehmend ins Visier von Datenschutzbehörden – und zwar weltweit. Bereits am vergangenen Freitag hatte die italienische Datenschutzbehörde den Chatbot vorläufig landesweit gesperrt. Sie begründete ihr Vorgehen unter anderem damit¹, dass ChatGPT gegen Datenschutz- und Jugendschutzrichtlinien verstoße.

Am Dienstag kündigte dann der kanadische Datenschutzbeauftragte an, einer Beschwerde über die mutmaßliche „Sammlung, Verwendung und Weitergabe von persönlichen Daten ohne Zustimmung“ nachzugehen². Und auch hierzulande gerät ChatGPT unter Druck. Die hiesigen Datenschutzbehörden prüfen, ob der Betrieb von ChatGPT gegen die Datenschutzgrundverordnung (DSGVO) verstößt. Die Behörden in Frankreich und Irland haben ebenfalls Untersuchungen angekündigt³.

ChatGPT ist ein Chatbot des Anbieters OpenAI in Partnerschaft mit Microsoft, der im November 2022 veröffentlicht wurde. Er gehört zur Klasse der sogenannten künstlichen neuronalen

Netzwerke und hier speziell der Large-Language-Modelle (LLM). OpenAI trainiert den Chatbot mit öffentlich zugänglichen Datenmengen, darunter mutmaßlich auch personenbezogene Daten von Nutzer:innen.

Zuständig sind die Landesdatenschutzbehörden

Der Bundesdatenschutzbeauftragte Ulrich Kelber schloss eine Sperrung von ChatGPT in Deutschland gegenüber dem Handelsblatt⁴ nicht aus. Allerdings obliege die Entscheidung darüber den Landesdatenschutzbehörden, da Unternehmen in deren Zuständigkeitsbereich fielen.

Jan Wacke von der baden-württembergischen Landesdatenschutzbehörde erklärt auf Anfrage gegenüber netzpolitik.org: „Wir beobachten die Entwicklung intensiv und werden uns die Anwendung genauer anschauen.“ Es sei wichtig, dass Chatbots wie ChatGPT „auf Grundlage des europäischen Rechtsrahmens und unserer

Anna-Lena Schmierer

Anna-Lena Schmierer ist seit April 2023 Praktikantin bei netzpolitik.org. Sie studiert Publizistik und Kommunikationswissenschaft in Berlin und interessiert sich unter anderem für staatliche Überwachung, digitale Gewalt und soziale Bewegungen.

gesellschaftlichen Werte zum Einsatz kommen.“ Seine Behörde werde sich daher „inhaltlich mit ChatGPT auseinandersetzen und soweit erforderlich mit dem Unternehmen sprechen.“

Etliche offene Fragen

Es gebe „zahlreiche zu klärende Datenschutzfragen“, sagt auch die schleswig-holsteinische Landesdatenschutzbeauftragte Marit Hansen, insbesondere mit Blick darauf, ob OpenAI die in der DSGVO vorgeschriebenen Datenschutz-Folgenabschätzungen⁵ vorgenommen hat. Hansen äußerte gegenüber netzpolitik.org Bedenken, dass das Unternehmen personenbezogene Daten rechtmäßig verarbeite. Es sei unklar, ob OpenAI Betroffenenrechte und Datensicherheit ausreichend wahre – vor allem bei Kindern und Jugendlichen.

Die Datenschutzkonferenz (DSK), das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder, werde den Fall laut Hansen nun eingehend prüfen. Allerdings fehlten noch „weitergehende Informationen, bei-

spielsweise zu den Datenquellen und zur Weitergabe an Dritte mit kommerziellen Interessen“. Diese wolle die DSK zunächst von OpenAI anfragen und im Anschluss auswerten.

Quelle: <https://netzpolitik.org/2023/openai-datenschutzkonferenz-nimmt-chatgpt-unter-die-lupe/>

Anmerkungen

- 1 <https://www.wired.co.uk/article/italy-ban-chatgpt-privacy-gdpr>
- 2 https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230404/
- 3 <https://www.reuters.com/technology/germany-principle-could-block-chat-gpt-if-needed-data-protection-chief-2023-04-03/>
- 4 <https://www.handelsblatt.com/politik/deutschland/nach-vorstoss-in-italien-man-kann-technologie-nicht-mit-verboten-aufhalten-diskussion-um-chatgpt-regulierung-in-deutschland/29075002.html>
- 5 <https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Technik/Datenschutz-Folgenabschaetzungen.html>



FfF e. V.

Mitgliederversammlung des FfF

Berlin, 23. Oktober 2022, ab 14:00 Uhr
Einstein-Saal, Archenhold-Sternwarte Alt-Treptow 1, 12435 Berlin

Versammlungsleitung: Stefan Hügel

Protokollführung: Rainer Rehak

Anwesend: 25 Mitglieder

- **Beschluss der Tagesordnung (TO)**
- **Annahme der Geschäftsordnung (GO)**
- **Bericht des Vorstandes (VS)**
Für den inhaltlichen Jahresbericht 2021/2022 siehe den Vortrag am Samstag / Aufzeichnung:
<https://media.ccc.de/v/fiffkon22-23-fiff-jahresrckblick>
Offizieller Dank des VS an Ingrid Schlagheck in der Geschäftsstelle
- **Berichte der Regionalgruppen (RG)**
Schleswig-Holstein: Bericht zum Projekt „Arbeiten und Leben“
Hamburg: kein Bericht
Bremen: Bericht zum Projekt: Programmatische Ungleichbehandlung durch KI
Niedersachsen: nicht anwesend
Berlin: Bericht zum Projekt Intergalaktischer FfF-Stammtisch und zur überregionalen FfF-Signalgruppe (Codename: FNORDS)
Frankfurt: nicht anwesend
München: Berichte mehrerer Kleinprojekte
- **Finanzbericht durch den Vorsitz**
Folien auf Anfrage

- **Bericht der Kassenprüfgruppe (M. Zallmann)**
Empfehlung einer Entlastung des Vorstands
- **Entlastung des Vorstands**
Vorstand wurde bei 7 (sieben) Enthaltungen einstimmig entlastet (18, 0, 7)
- **Wahl der Kassenprüfgruppe,**
aufgestellt sind M. Zallmann und B. Hoffmann
Kassenprüfgruppe wurde bei 1 (einer) Enthaltung einstimmig (wieder)gewählt (24, 0, 1)
- **Raum für Diskussionen zu Satzung, Zweck und Zielen**
keine Meldungen
- **Anträge der Mitglieder**
keine Anträge eingegangen
- **Informelles Zwischenprogramm**
– Dank an das FfFKon22-Orgateam
– Es wurden 2 (zwei) Gedichte an die RG Berlin vorgetragen
- **Annahme des Protokolls** (inkl. nachträglicher Verbesserung der Formatierung)
Protokoll wurde einstimmig angenommen (25, 0, 0)

Protokollführung (Rainer Rehak)

Versammlungsleitung (Stefan Hügel)



Grundrechte-Report

Grundrechte-Report 2023 der Öffentlichkeit vorgestellt

Präsentatorin Susanne Baer: „Zum Schutz der Grundrechte gibt es noch Einiges zu tun“

Am 23. Mai 2023, dem Tag des Grundgesetzes, wurde der diesjährige Grundrechte-Report – Zur Lage der Bürger- und Menschenrechte in Deutschland im Haus der Demokratie in Berlin der Öffentlichkeit vorgestellt.

Der 27. Grundrechte-Report wirft unter dem Titel *Krieg, Klima, Krise* einen Blick auf die aktuellen Gefährdungen der Grundrechte und zentraler Verfassungsprinzipien anhand konkreter Fälle des Jahres 2022. Der Report analysiert und kritisiert Entscheidungen von Parlamenten, Behörden und Gerichten, aber auch von Privatunternehmen.

Hierzu gehören für das Jahr 2022 grundrechtliche Auswirkungen der Maßnahmen anlässlich des russischen Angriffskriegs auf die Ukraine und die wachsende Armut in Deutschland. Darüber hinaus werden im Report tödliche Polizeigewalt, rassistische Polizeikontrollen und Grundrechtsverletzungen an geflüchteten Menschen thematisiert sowie Einschnitte in die informationelle Selbstbestimmung und Probleme in der deutschen Justiz besprochen. Der Report wird von zehn Bürgerrechtsorganisationen herausgegeben.

Susanne Baer, ehemalige Richterin des Bundesverfassungsgerichts und Professorin für Öffentliches Recht und Geschlechterstudien an der Humboldt-Universität zu Berlin, präsentierte den Grundrechte-Report in diesem Jahr: „Der Krieg in der Ukraine, die wirtschaftliche Lage, die viele Menschen belastet, und die Klimakrise fordern Politik und Gesellschaft – und sie fordern auch die Grundrechte heraus. Gerade wenn es eng wird, kommt es auf diese Rechte an. Der Grundrechte-Report deckt da Probleme auf. Dass im Familienrecht weiter frauenfeindliche Narrative wirksam werden, erschreckt ebenso wie der geschilderte Umgang mit Angriffen auf die Pressefreiheit. Teils müssen sich Justiz, Verwaltung und Gesetzgeber hier deutliche Kritik gefallen lassen. Ich stimme da nicht allem zu, aber das muss diskutiert werden. Berichtet wird ja auch, wo Gerichte bewegt werden können, um Grundrechte in neuen Konstellationen durchzusetzen – in der Polizeiarbeit, bei Streiks oder ‚Klimacamps‘. Klar ist jedenfalls: Grundrechtsfragen gehen alle an – und um überzeugende Antworten müssen wir ringen.“

Simon Lachner, Aktivist der *Letzten Generation*, berichtete bei der Pressekonferenz von seinen Erfahrungen mit dem staatlichen Umgang mit Aktionen der Klimaaktivist:innen. Er sagt: „Wie die Engagierten bei der Letzten Generation vom Rechtsstaat behandelt werden, ist teils erschreckend. Immer wieder sehe ich meine Freunde, wie sie mit Schmerzgriffen von der Straße gezerrt werden oder in die Justizvollzugsanstalt gesperrt werden – teils ohne Gerichtsverfahren, sondern auf Grundlage des Polizeiaufgabengesetzes in Bayern. Auch ich war für zwei Nächte in der Justizvollzugsanstalt in München.“



Grundrechte-Report 2023
Zur Lage der Bürger- und Menschenrechte in Deutschland
Herausgegeben von: Rolf Gössner, Rosemarie Will, Britta Rabe, Benjamin Derin, Wiebke Judith, Sarah Lincoln, Lea Welsch, Rebecca Militz, Max Putzer, Rainer Rehak
Fischer Taschenbuch Verlag
ISBN 978-3-596-70882-6

Benjamin Derin, Rechtsanwalt und Mitglied des Republikanischen Anwältinnen- und Anwältevereins e.V. (RAV), resümiert stellvertretend für die gesamte Redaktion des Grundrechte-Reports: „Ob staatliche Überwachung, Ausweitung von Straf- und Polizeigesetzen oder Abbau von sozialen Sicherungen, wir weisen immer wieder darauf hin, wo die Grundrechte in Gefahr sind. Teile von Staat und Politik scheinen aber umgekehrt die Grundrechte mancher Menschen als Gefahr zu betrachten. Das Beharren auf diesen Rechten ist deshalb ein wichtiger Teil des Einsatzes für eine freiheitliche und soziale Gesellschaft für alle.“

Die Mitherausgeberin des Grundrechte-Reports **Lea Welsch**, Rechtsanwältin und Mitglied des Bundesvorstandes der Vereinigung Demokratischer Juristinnen und Juristen (VDJ) kommentierte: „Auch in diesem Jahr dokumentiert der Grundrechte-Report erneut, dass gerade die Grundrechte derjenigen am meisten bedroht sind, die durch gesellschaftliche Institutionen am wenigsten repräsentiert werden. Dafür eine Öffentlichkeit zu schaffen, ist eines der Anliegen der herausgebenden Organisationen.“

Der Grundrechte-Report 2023 ist ein gemeinsames Projekt von: Humanistische Union, vereinigt mit der Gustav-Heinemann-Initiative • Bundesarbeitskreis Kritischer Juragruppen • Internationale Liga für Menschenrechte • Komitee für Grundrechte und Demokratie • Neue Richtervereinigung • PRO ASYL • Republikanischer Anwältinnen- und Anwälteverein • Vereinigung Demokratischer Juristinnen und Juristen • Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung • Gesellschaft für Freiheitsrechte

So geht nachhaltige Digitalisierung

Bits & Bäume-Buch gibt 28 Impulse

Berlin, 6. Juni 2023 – Von künstlicher Intelligenz über die Umweltauswirkungen der Digitalwirtschaft bis zu globaler Gerechtigkeit: Der digitale Wandel hat viele Baustellen. Und er birgt Risiken. Wie die Gesellschaft nachhaltig digital werden kann, zeigt das Buch „Shaping Digital Transformation for a Sustainable Society“, das heute von dem Bündnis Bits & Bäume auf der Digitalkonferenz Re:publica in Berlin vorgestellt wird. 28 Beiträge von 68 Autor*innen aus Praxis, Zivilgesellschaft und Forschung zeigen Probleme der digitalen Entwicklungen und geben Impulse, wie Digitalpolitik jetzt gestaltet werden kann und muss. Das englischsprachige Buch steht als reine Online-Publikation kostenlos zum Open-Access-Download bereit.

Der Band versammelt Beiträge aus der Bits & Bäume-Community, die im Jahr 2022 zur zweiten Konferenz für Digitalisierung und Nachhaltigkeit (<https://bits-und-baeume.org/konferenz-2022>) mit 2.500 Teilnehmenden in Berlin zusammenkam. Die Konferenz wurde ausgerichtet von 13 Organisationen aus Umweltschutz, Digitalpolitik, Entwicklungspolitik und Wissenschaft.

Digitalisierung und Nachhaltigkeit: „Fortschritt“ muss neu definiert werden

Das Buch zeigt Wege auf, wie die Vision einer nachhaltigen Digitalisierung Wirklichkeit werden kann. Die Autor*innen machen klar, dass Fortschritt im Angesicht der für die User oft unsichtbaren Auswirkungen auf die Umwelt und auf soziale Gerechtigkeit neu definiert werden muss. Angereichert mit Illustrationen und Infografiken gibt das Buch zahlreiche Impulse: etwa wie künstliche Intelligenz designt werden muss, um zur nachhaltigen Transformation beizutragen, oder wie eine Lebenszyklusbewertung von Software aussehen könnte.

Nachhaltiges Tech-Design: Lernen von Good Practice

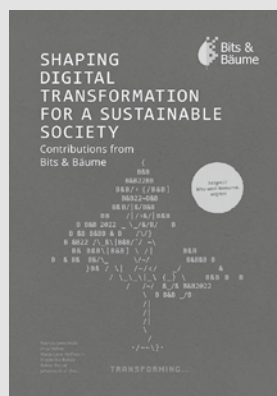
Digitale Tools können Nachbarschaften helfen, regional erzeugten erneuerbaren Strom zu teilen. Andere Anwendungen tragen dazu bei, die Landwirtschaft sozial-ökologisch zu transformieren. Anhand solcher Good-Practice-Beispiele zeigt das Buch, wie digitale Technologien nachhaltig ausgestaltet werden können. Und es verdeutlicht, dass die Zivilgesellschaft Motor des nachhaltigen Wandels sein kann und die Politik zivilgesellschaftliche Akteure bei der Gestaltung einer nachhaltigen digitalen Zukunft einbeziehen muss.

Buch für Einsteiger und Fachleute

Die Beiträge des 150-seitigen Buchs bieten Stoff, um sich in Themen einzulesen oder um andere Aspekte zu vertiefen. So möchte das Buch dazu beitragen, dass die Stimme der Zivilgesellschaft bei der Neuausrichtung der Digitalisierung in Richtung einer nachhaltigen Zukunft besser zu hören ist.

Die Veröffentlichung sowie die Konferenz Bits & Bäume 2022 wurden gefördert von der Deutschen Bundesstiftung Umwelt (DBU) und dem Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV). Die Arbeit von Germanwatch und Forum InformatikerInnen für Frieden

und gesellschaftliche Verantwortung (FlFF) im Rahmen der Konferenz wurden unterstützt von der Stiftung Mercator.



Shaping Digital Transformation
for a Sustainable Society
Jankowski, P., Höfner, A., Hoffmann, M. L., Rohde, F., Rehak, R. & Graf, J. (Eds.)
2023, 152 Seiten
kostenloser download unter:
<https://publication2023.bits-und-baeume.org/>

Weiterführende Links

Zum Sammelband: Shaping Digital Transformation for a Sustainable Society-Contributions from Bits & Bäume, <https://publication2023.bits-und-baeume.org>

DOI: <https://doi.org/10.14279/depositonce-17526>

Bits & Bäume auf der re:publica 1) Book Launch: <https://re-publica.com/de/session/bits-baeume-journal-launch-and-5-year-anniversary-meetup>, 2)

Bits & Bäume-Zukunftsreise: <https://re-publica.com/en/node/2209>

Mehr über Bits & Bäume: <https://bits-und-baeume.org>

Über den Trägerkreis: <https://bits-und-baeume.org/traegerkreis/>

Über die Bits & Bäume: Bits & Bäume ist das größte deutschlandweite zivilgesellschaftliche Bündnis an der Schnittstelle zwischen Digitalisierung und Nachhaltigkeit. Es besteht aus 13 Organisationen aus den Bereichen Umwelt- und Klimaschutz, Digitalpolitik, Entwicklungspolitik und Wissenschaft sowie einer wachsenden Community. Bits & Bäume bringt die Umwelt-, Digital- und Klimabewegungen zusammen und setzt das Thema in Öffentlichkeit und Politik auf die Agenda. In den Jahren 2018 und 2022 richtete das Bündnis in Berlin jeweils eine Bits & Bäume-Konferenz für Digitalisierung und Nachhaltigkeit aus.

Trägerkreis Bits & Bäume: Brot für die Welt, BUND, Chaos Computer Club (CCC), Deutscher Naturschutzring (DNR), Einstein Center Digital Future, Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FlFF), Free Software Foundation Europe (FSFE), Germanwatch, Institut für ökologische Wirtschaftsforschung (IÖW), Konzeptwerk Neue Ökonomie, Open Knowledge Foundation Deutschland (OKF DE), Technische Universität Berlin, Weizenbaum-Institut für die vernetzte Gesellschaft



Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung

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

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

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

FIfF 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:

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

Beiträge an: fiff-L@lists.fiff.de

FIfF-Mitgliederliste

An- und Abmeldungen an:

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

FIfF-Beirat

Ute Bernhardt (Berlin); **Peter Bittner** (Bad Homburg); **Dagmar Boedicker** (München); Dr. **Phillip W. Brunst** (Köln); Prof. Dr. **Christina Claß** (Jena); Prof. Dr. **Wolfgang Coy** (Berlin); Prof. Dr. **Wolfgang Däubler** (Bremen); Prof. Dr. **Christiane Floyd** (Berlin); Prof. Dr. **Klaus Fuchs-Kittowski** (Berlin); Prof. Dr. **Michael Grütz** (München); Prof. Dr. **Thomas Herrmann** (Bochum); Prof. Dr. **Wolfgang Hesse** (München); Prof. Dr. **Wolfgang Hofkirchner** (Wien); Prof. Dr. **Eva Hornecker** (Weimar); **Werner Hülsmann** (München); **Ulrich Klotz** (Frankfurt am Main); Prof. Dr. **Klaus Köhler** (Mannheim); Prof. Dr. **Jochen Koubek** (Bayreuth); Dr. **Constanze Kurz** (Berlin); Prof. Dr. **Klaus-Peter Löhr** (Berlin); Prof. Dr. **Dietrich Meyer-Ebrecht** (Aachen); **Werner Mühlmann** (Calau); Prof. Dr. **Frieder Nake** (Bremen); Prof. Dr. **Rolf Oberliesen** (Paderborn); Prof. Dr. **Arno Rolf** (Hamburg); Prof. Dr. **Alexander Rossnagel** (Kassel); **Ingo Ruhmann** (Berlin); Prof. Dr. **Gerhard Sagerer** (Bielefeld); Prof. Dr. **Gabriele Schade** (Erfurt); **Ralf E. Streibl** (Bremen); Prof. Dr. **Marie-Theres Tinnefeld** (München); Dr. **Gerhard Wohland** (Mainz); Prof. Dr. **Eberhard Zehendner** (Jena)

FIfF-Vorstand

Stefan Hügel (Vorsitzender) – Frankfurt am Main
Rainer Rehak (stellv. Vorsitzender) – Berlin
Michael Ahlmann – Kiel / Blumenthal
Maximilian Hagner – Jena
Alexander Heim – Berlin
Sylvia Johnigk – München
Benjamin Kees (Mitgliedschaft ruhend) – Berlin
Prof. Dr. **Hans-Jörg Kreowski** – Bremen
Kai Nothdurft – München
Prof. Dr. **Britta Schinzel** – Freiburg im Breisgau
Ingrid Schlagheck – Bremen
Anne Schnerrer – Berlin
Dr. **Friedrich Strauß** – München
Prof. Dr. **Werner Winzerling** – Fulda

FIfF-Geschäftsstelle

Ingrid Schlagheck (Geschäftsführung) – Bremen

Impressum

Herausgeber	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF)
Verlagsadresse	FIfF-Geschäftsstelle Goetheplatz 4 D-28203 Bremen Tel. (0421) 33 65 92 55 fiff@fiff.de
Erscheinungsweise	vierteljährlich
Erscheinungsort	Bremen
ISSN	0938-3476
Auflage	1 300 Stück
Heftpreis	7 Euro. Der Bezugspreis für die FIfF-Kommunikation ist für FIfF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FIfF-Kommunikation für 28 Euro pro Jahr (inkl. Versand) abonnieren.
Hauptredaktion	Dagmar Boedicker, Stefan Hügel (Koordination), Sylvia Johnigk, Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht, Ingrid Schlagheck
Schwerpunktredaktion	Stefan Hügel
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	The Blue Marble, von NASA/Apollo 17 crew; taken by either Harrison Schmitt or Ron Evans
Druck	Meiners Druck, Bremen Heftinhalt auf 100 % Altpapier gedruckt.



Die FIfF-Kommunikation ist die Zeitschrift des „Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V.“ (FIfF). Die Beiträge sollen die Diskussionen unter Fachleuten anregen und die interessierte Öffentlichkeit informieren. Namentlich gekennzeichnete Artikel geben die jeweilige Autor:innen-Meinung wieder.

Die FIfF-Kommunikation ist das Organ des FIfF und den politischen Zielen und Werten des FIfF verpflichtet. Die Redaktion behält sich vor, in Ausnahmefällen Beiträge abzulehnen.

Nachdruckgenehmigung wird nach Rücksprache mit der Redaktion in der Regel gern erteilt. Voraussetzung hierfür sind die Quellenangabe und die Zusendung von zwei Belegexemplaren. Für unverlangt eingesandte Artikel übernimmt die Redaktion keine Haftung.

Wichtiger Hinweis: Wir bitten alle Mitglieder und Abonnent:innen, Adressänderungen dem FIfF-Büro möglichst umgehend mitzuteilen.

Aktuelle Ankündigungen

(mehr Termine unter www.fiff.de)

FIfF-Konferenz 2023 in Berlin

„Wir möchten gemeinsam mit euch allen in die Zukunft schauen!“

3. – 5. November, Jugendherberge Berlin-Ostkreuz

FIfF-Kommunikation

3/2023 „IT-Gestaltung für Gute Arbeit“

Katharina Just, Klaus Heß, Dagmar Boedicker

Redaktionsschluss: 4. August 2023

Zuletzt erschienen:

2/2022 Künstliche Intelligenz

3/2022 Digitalisierung in Staat, Politik und Verwaltung

4/2022 100 Jahre Joseph Weizenbaum

1/2023 #FIfFKon22

W&F – Wissenschaft & Frieden

2/22 Kriegerische Verhältnisse

3/22 Krieg gegen die Ukraine

4/22 Gewalt/Ökonomie

1/23 Jenseits der Eskalation

2/23 Klimakrise

vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik

#236 Anleihekäufe der EZB

#237/238 Diskriminierung

#239/240 Krieg und Frieden

#241 Demokratie und Rechtsstaat verteidigen

#242 Kriminalpolitik

DANA – Datenschutz-Nachrichten

1/22 Ampelpolitik

2/22 Social Media

3/22 Datenschutz und andere Grundrechte

4/22 Beschäftigtendatenschutz

1/23 Europäische Entwicklungen

Das FIfF-Büro

Geschäftsstelle FIfF e. V.

Ingrid Schlagheck (Geschäftsführung)

Goetheplatz 4, D-28203 Bremen

Tel.: (0421) 33 65 92 55, Fax: (0421) 33 65 92 56

E-Mail: fiff@fiff.de

Die Bürozeiten finden Sie unter www.fiff.de

Bankverbindung

Bank für Sozialwirtschaft (BFS) Köln

Spendenkonto:

IBAN: DE79 3702 0500 0001 3828 03

BIC: BFSWDE33XXX

Kontakt zur Redaktion der FIfF-Kommunikation:

redaktion@fiff.de

Pale Blue Dot

Anlässlich des 30. Jahrestages wurde eine neue Version des als „Pale Blue Dot“ bekannten Bildes der Voyager-Mission der NASA veröffentlicht. Der Planet Erde ist als heller Fleck im Sonnenstrahl rechts von der Mitte zu sehen und erscheint sanft blau, wie in der 1990 veröffentlichten Originalversion (siehe PIA00452).



Im Jahr 1990 plante das Voyager-Projekt, die Bildkameras der Raumsonde Voyager 1 abzuschalten, um Energie zu sparen. Vor der Abschaltung wurde die Sonde angewiesen, eine Serie von 60 Bildern zu machen, um das so genannte „Familienporträt des Sonnensystems“ zu erstellen. Diese am Valentinstag 1990 durchgeführte Sequenz lieferte Bilder für die Erstellung von Farbansichten von sechs Planeten des Sonnensystems und bildete auch die Sonne in Schwarzweiß ab.

Der Planet nimmt weniger als ein einziges Pixel auf dem Bild ein und ist daher nicht vollständig aufgelöst. (Die tatsächliche Breite des Planeten am Himmel betrug in der Voyager-Kamera weniger als ein Pixel.) Im Gegensatz dazu waren Jupiter und Saturn groß genug, um einen ganzen Pixel in ihren Familienporträtbildern zu füllen.

Quelle: https://commons.wikimedia.org/wiki/File:Pale_Blue_Dot_from_Voyager_1_-_PIA23645.png