H 7625

FIfF Kommunikation

Zeitschrift für Informatik und Gesellschaft

38. Jahrgang 2021 Einzelpreis: 7 EUR 4/2021 – Dezember 2021

Künstliche Intelligenz zieht in den Krieg

ISSN 0938-3476

• Joseph Weizenbaum • Nachhaltige Digitalisierung • Protestlogik •

Mit Dossier: Künstliche Intelligenz zieht in den Krieg

FIfF Kommunikation

Zeitschrift für Informatik und Gesellschaft

Titelbild: *Collage: Janina Thiede*

Inhalt

Ausgabe 4/2021

Editorial

Künstliche Intelligenz zieht in den Krieg – ein klassisches FIfF-Thema bildet den Schwerpunkt dieser Ausgabe der *FIfF-Kommunikation*. Dem Heft legen wir ein gleichnamiges Dossier bei, das in Zusammenarbeit mit der Zeitschrift *Wissenschaft und Frieden* entstanden ist. Beides wurde von Hans-Jörg Kreowski und Aaron Lye konzipiert und redaktionell betreut.

Im Schwerpunkteditorial leiten sie den Schwerpunkt ein und stellen auch den Bezug zum Dossier her:

> *„[…] KI [wird] seit langem in vielfältiger Weise auch militärisch genutzt und gilt in Rüstung und im Kriegswesen als Hauptfaktor, der militärische Überlegenheit garantieren kann. Da das aber alle Seiten so sehen und keine ins Hintertreffen geraten will, bedeutet der Einsatz von KI in diesem Zusammenhang vor allem, dass mit immensen Finanz- und Personalmitteln an der Rüstungsspirale gedreht wird. Während die Entwicklung von Computertechnik und Informatik in den ersten Jahrzehnten seit dem Zweiten Weltkrieg stark vom Geld und von den Wünschen des militärischen Komplexes abhing, sind die Anfänge der Künstlichen Intelligenz ab 1956 eher friedlich angelegt gewesen. Damit war jedoch spätestens mit der Strategic Computing Initiative (SCI) der Vereinigten Staaten von Amerika der Jahre 1983 bis 1992 Schluss. […] KI [ist] nicht zuletzt auch wegen SCI zu einem großen und bedeutenden Fachgebiet der Informatik angewachsen […].“*

Den Kern unserer weiteren Rubrik *Forum* bilden drei Beiträge. Am Anfang steht der Beitrag von Mathias Haimerl: *Zum technologischen Infantilismus der Industrie und des Healthcare-Sektors*. Einleitend stellt er fest:

> *„Während die Digitalisierung voranschreitet und die Abhängigkeit von Computern auf einem nie dagewesenen Level ist, stillen Konzerne ihren Datenhunger auf Kosten des Datenschutzes, wirtschaftlicher Schäden und sogar Menschenleben. Das Ungleichgewicht zwischen den Interessen von Software-Unternehmen und den Endanwendern wird medienwirksam verpackt und quelloffene Software marketing-technisch torpediert.“*

„Revolutionen finden leibhaftig statt“, schreibt Markus Reinisch in seinem Beitrag und leitet ein:

> *„Protestformen als Mittel demokratischer Partizipation spielen sich durch den Einfluss digitaler Medien immer mehr im Virtuellen ab. Trotz immer einfacherer Möglichkeiten, sich mittels sozialer Netzwerke zu organisieren und zu mobilisieren, bleibt der Wert des großen Nein (Armin Nassehi) auf Straßen und Plätzen nach wie vor von großer Bedeutung für die Protestierenden, ihre Anliegen und Sichtbarkeit.“*

In ihrem Beitrag *Herausforderungen und Wege für eine nachhaltige Digitalisierung* untersucht Nelli Leiditz deren Problemfelder und Maßnahmen. Sie sieht die Nutzer:innen in der Verantwortung, Sensibilität sowohl für nachhaltigen Umgang mit der IT als auch für Datenschutz zu entwickeln.

Das militärische Desaster in *Afghanistan* ist fast schon wieder vergessen, ohne dass es zu einer Lösung für die Leidtragenden gekommen wäre. Wir erinnern daran und drucken die *Erklärung der Kooperation für den Frieden zur Afghanistankonferenz*, die am 31. Oktober 2021 in Frankfurt am Main stattfand.

Mit großer Bestürzung haben wir vom Tod von *Heidi Schelhowe* erfahren. Sie war dem FIfF verbunden und leistete wertvolle Beiträge zu FIfF-Konferenzen, zur FIfF-Kommunikation und als Mitglied der Jury des Weizenbaum-Studienpreises. Wir gedenken ihrer mit einem Nachruf, den Ulrike Erb, Wiebke Oeltjen, Karin Vosseberg und Margita Zallmann verfasst haben.

Im Januar 2023 wäre *Joseph Weizenbaum* 100 Jahre alt geworden. Seinem Andenken widmen wir auch Beiträge in der FIfF-Kommunikation. Den Anfang bildet ein Text von 1986, der auf Basis eines Vortrags bei der damaligen Jahrestagung der *Gesellschaft für Informatik* in den *Blättern für deutsche und internationale Politik* erschienen ist. *Ohne uns geht's nicht weiter*, stellte er damals fest und wies auf die Verantwortung der Informatiker:innen für Rüstung, den militärischen Einsatz der Künstlichen Intelligenz und damit für die Beendigung des Einsatzes informatischer Entwicklungen für das Töten hin. Dieser Text kann als einer der Schlüsseltexte für das FIfF gelesen werden und bildet den Auftakt für weitere Beiträge zu Leben und Werk Joseph Weizenbaums. Für die Ausgabe 4/2022, die wenige Tage vor seinem hundertsten Geburtstag erscheinen wird, planen wir dazu einen Schwerpunkt.

Bekanntlich haben wir unsere *Weizenbaum-Medaille* Joseph Weizenbaum gewidmet, die wir an Persönlichkeiten verleihen, die sich durch ihr Wirken in besonderer Weise um die gesellschaftspolitischen Aspekte der Informatik verdient gemacht haben. Im Rahmen unserer FIfF-Konferenz haben wir in diesem Jahr die Weizenbaum-Medaille *Professorin Christiane Floyd* verliehen, die Gründungsvorsitzende des FIfF war und, so Professorin Britta Schinzel, „[…] ihr Fach im Sinne einer gesellschaftlichen Verantwortung für die Informatik aufgefasst, gestaltet und gelebt [hat] – eine außergewöhnliche Persönlichkeit und ein großes Vorbild.“ Die Beiträge der FIfF-Konferenz bilden den Schwerpunkt der kommenden Ausgabe 1/2022.

Wir gratulieren auch der Redaktion von *netzpolitik.org*, mit der wir kooperieren und die in dieser Ausgabe mit Beiträgen zur digitalpolitischen Bilanz Angela Merkels und einem Bericht über die Whistleblowerin Frances Haugen vertreten ist. Die *Humanistische Union* verlieh ihr den *Fritz-Bauer-Preis*, mit dem sie herausragende Verdienste um die Humanisierung, Liberalisierung und Demokratisierung des Rechtswesens würdigt. netzpolitik.org steht damit in einer Reihe mit Persönlichkeiten wie Gustav Heinemann, Ruth Leuze, Regine Hildebrandt, Burkhard Hirsch, Edward Snowden und Hans-Christian Ströbele.

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

Stefan Hügel
für die Redaktion

Der Brief

$f(x) = n^x$

Liebe Freundinnen und Freunde, liebe Mitglieder des FIfF,

viele von uns kennen die alte Legende: Der indische Herrscher *Shihram* gewährte dem Weisen *Sissa ibn Dahir* einen Wunsch für die Erfindung des Schachspiels, das ihn sehr beeindruckte. Dieser gab sich bescheiden und wünschte sich einzelne Weizen- (in anderen Erzählungen Reis-) körner: Ein Korn auf dem ersten Feld des Spielbretts, zwei auf dem zweiten, vier auf dem dritten und so weiter, unter jeweiliger Verdoppelung, bis zum 64-sten Feld. Der Herrscher, leicht pikiert ob dieses lächerlich bescheidenen Wunsches, gewährte ihn gleichwohl. Als er sich nach einigen Tagen nach dem Fortschritt der Erfüllung des Wunsches erkundigte, wurde ihm beschieden, dass es immer noch nicht gelungen sei, die Gesamtmenge der Körner zu berechnen. Am Ende war er die gesamte Ernte seines großen Reiches über hunderte von Jahren schuldig.

Es ist nicht wichtig, ob diese alte Geschichte authentisch ist, ob und wie sie sich genau zugetragen hat. Wichtig ist: Anscheinend haben wir sie bis heute nicht verstanden.

Gerade befinden wir uns in der – je nach Zählung – vierten Welle der Covid-19-Pandemie, und die Infektionszahlen erreichen trotz Impfungen neue Höchstwerte. Inzwischen sind rund 100.000 Menschen allein in Deutschland an der Erkrankung verstorben – eine kaum vorstellbare Zahl. Angehörige, die davon betroffen sind, wissen, welche Tragödie sich hinter jedem Einzelfall verbirgt. Der Verweis auf Vorerkrankungen ist zynisch. Es muss uns wohl langsam klar werden, dass Covid-19 nicht einfach „verschwinden" wird, wie wir am Anfang gerne geglaubt haben.

Wissenschaftliche Erkenntnisse belegen die Wirksamkeit der Impfung. Die Wahrscheinlichkeit einer Erkrankung sinkt, infiziert man sich dennoch, wird die Wahrscheinlichkeit eines schweren oder gar tödlichen Verlaufs sehr gering. Dennoch stecken sich auch geimpfte mit dem Virus an. Das ist leicht zu erklären: Steigt die Zahl der Geimpften, steigt fast zwangsläufig auch die Zahl der infizierten Geimpften. Keineswegs ist das ein Indikator für die mangelnde Wirksamkeit der Impfung. Dennoch entscheiden sich Menschen dagegen – manche aus nachvollziehbaren (wenngleich nicht immer richtigen), manche aus völlig absurd anmutenden Beweggründen. Aber auch geimpfte Menschen sollten sich bewusst sein: Der Impfschutz ist kein Freibrief für Sorglosigkeit. Kontakte müssen weiterhin vermieden, bei Veranstaltungen Abstand gehalten werden. So sehr – und das ist nur ein Beispiel – den Kölner:innen ihr Karneval zu gönnen ist: Der Leichtsinn, der am 11. November dort zu beobachten war, teilweise sogar noch befeuert durch die Medien, macht fassungslos.

Hier ist die Politik gefragt – und erscheint überfordert. Das exponentielle Wachstum der Pandemie, die sich immer weiter beschleunigende Zunahme von Infektionen scheint immer noch nicht verstanden. Zum wiederholten Mal erklären Gesundheitpolitiker:innen, die Entwicklung sei nicht abzusehen gewesen. Manche behaupten es sogar immer noch, nachdem wochenlang in Wissenschaft und Öffentlichkeit darüber diskutiert wurde. Ich erwarte von Politiker:innen, die auf höchster Ebene Verantwortung tragen – mit Unterstützung ihrer Berater:innen und Expert:innen in den Behörden – dass sie in der Lage sind, Entwicklungen auch im Voraus einschätzen zu können. Kurz gesagt: Dass sie die Verantwortung nicht nur „tragen", sondern auch wahrnehmen.

Die Pandemie ist die erste große Herausforderung für die sich gerade zusammenfindende Koalition. Und für die ganze Gesellschaft, die viermal eine Regierung unter Angela Merkel wählte – eine Regierung, die nicht immer durch entschlossenes Handeln auffiel. Einiges spricht für die Annahme, sie wurde genau deswegen gewählt.

In diesen Tagen geht die Regierungszeit von Angela Merkel ihrem Ende entgegen – bei Veröffentlichung dieses Briefs ist es vermutlich schon so weit. Ich fühle mich nicht berufen, hier Bilanz zu ziehen – sicherlich war der unaufgeregte Regierungsstil im Vergleich zu manchem (männlichen) Mitbewerber manchmal wohltuend. Angela Merkel ist es gelungen, der Union ein modernes Gesicht zu geben. Wie nachhaltig das ist, wird man sehen. Gerade gehen die „Konservativen" wieder in Stellung, der rechte Rand der Politik in Deutschland ist stärker, mindestens aber sichtbarer geworden. Die AfD ist in dieser Zeit entstanden; deren Führungsfigur Alexander Gauland war früher Politiker der CDU und bei vielen CDU-Größen der 1970-er und 1980-er Jahre könnte ich mir inhaltlich sehr wohl vorstellen, dass sie die Politik der AfD heute in manchen Bereichen unterstützen würden, darunter der in der CSU immer noch als großes Vorbild gehandelte Franz-Josef Strauß und der hessische CDU-Politiker Alfred Dregger. Welchen Einfluss diese Richtung in der CDU künftig haben wird, bleibt wohl abzuwarten.

Zeitgemäß ist diese Strömung nicht mehr.

„Wir schaffen das!" Die Binsenweisheit, dass ein reiches Land wie die Bundesrepublik Deutschland in der Lage sein sollte, Geflüchteten zu helfen, wird Angela Merkel vor allem von Rechtspopulisten als „Einladung" an die ganze Welt vorgeworfen. Liebe AfD, ich kann Euch beruhigen: Die tatsächliche Politik, die beispielweise mit der Grenzschutzagentur FRONTEX im Namen Europas Krieg gegen die Opfer von Konflikten führt, ist auch von der Regierung Merkel zu verantworten.

Leider wurden auch viele Themen in den letzten 16 Jahren verschlafen und damit sehr viel Zeit verloren. Zu nennen sind die Abwendung der Klimakatastrophe und die Gestaltung einer effektiven und menschengerechten Digitalisierung. Der Umgang mit der Covid-19-Pandemie lässt für die Bewältigung der Folgen des langfristig viel gravierenderen Klimawandels wenig Gutes ahnen.

1998 haben wir miterlebt, wie das „Rot-grüne Projekt“, die Regierungskoalition unter Bundeskanzler Schröder und Außenminister Fischer, ins Leben gerufen wurde. Es war große Aufbruchstimmung: Endlich waren die 16 bleiernen Jahre des Bundeskanzlers Helmut Kohl zu Ende! Und was kam dann? Die ersten Kriegseinsätze ohne UN-Mandat im Kosovo, die Agenda 2010 mit Hartz IV – nein, so hatten wir uns das Rot-grüne Projekt nicht vorgestellt. Doch noch heute spielen Protagonisten der damaligen Politik eine wesentliche Rolle.

Es ist meine wichtigste Erwartung an eine sich nun anbahnende Ampelkoalition: Dass sie die Fehler der damaligen rot-grünen Regierung nicht wiederholt. Leider gibt es dafür Anzeichen: Beispielsweise die mantraartige Wiederholung, dass Deutschland „Verantwortung“ übernehmen muss. Gemeint ist damit häufig nicht wirkliche Verantwortung, sondern die Bereitschaft zu militärischen Interventionen – und das, nachdem die vom damaligen Bundeskanzler Schröder 2001 ausgerufene „uneingeschränkte Solidarität“ in Afghanistan endgültig im Desaster geendet ist. Wir müssen wieder klar machen, was verantwortungsvolle Politik ist, und was nicht. Es mag Gründe geben, eine Zusammenarbeit mit der Linken zu diesem Zeitpunkt abzulehnen – offensichtlich muss sich die Partei erst einmal wieder sortieren; die Wahl hat auch keine entsprechenden Mehrheiten ergeben. Doch eins muss auch klar sein: Deren Ablehnung militärischer Interventionen gehört nicht zu diesen Gründen. Wir sollten endlich aus unserer Geschichte gelernt haben, dass das Militär das Problem und nicht die Lösung ist.

Die Koalitionsverhandlungen fanden großenteils im Verborgenen statt und waren maximal intransparent. Einen ersten Anhaltspunkt lieferte das Sondierungspapier. Nachdem lange Zeit mehr Transparenz in der Politik gefordert wurde, ist das Hinterzimmer das neue Paradigma. Die Grünen haben es vorgeführt – ihre Kanzlerkandidatin wurde vom Olymp herunter dem Wahlvolk präsentiert. Wenn ich mir vorstelle, dass diese Strategie der vollendeten Tatsachen die kommende Legislaturperiode prägen wird, mache ich mir Sorgen – nicht nur als Vertreter einer NGO, die gerne Politik mitgestalten will. Wir werden das genau beobachten.

Mit FIfFigen Grüßen
Stefan Hügel

Das FIfF bittet um Eure Unterstützung

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

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

Bitte unterstützt das FIfF 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

Ulrike Erb, Wiebke Oeltjen, Karin Vosseberg, Margita Zallmann

Heidi Schelhowe * 1949 † 2021

Im August 2021 verstarb die Informatik-Professorin Dr. Heidi Schelhowe (1949–2021). Als Mitstreiterin für eine sozialorientierte Informatik haben ihre Beiträge zum *Computer als Medium* und Projekte zur *Vielfalt der Informatik* die Leitbilddiskussionen in der Informatik im deutschsprachigen Raum mitgeprägt. Die Teilhabe insbesondere von Frauen in der Gestaltung von informationstechnischen Systemen war ihr eine Herzensangelegenheit. Ihre Arbeiten zu Digitalen Medien in der Bildung werden uns weiterhin Inspiration sein, ein vielfältiges Bild der Informatik fortzuschreiben.

Von 1967-1972 studierte Heidi Schelhowe Germanistik und Katholische Theologie an der Albert-Ludwigs-Universität Freiburg und an der Westfälischen Wilhelms-Universität Münster. Ihre Ausbildung für das Lehramt schloss sie mit einem Referendariat an Gymnasien in Bremen ab. Von 1975 bis 1981 war sie als Lehrerin in Bremen tätig. Während dieser Zeit engagierte sie sich politisch, was zu ihrer Entlassung aus dem Staatsdienst führte. 1981 erhielt sie wegen des Radikalenerlasses Berufsverbot. Eine Rehabilitierung erfolgte im Rahmen der Abschaffung des Radikalenbeschlusses in Bremen 2012.

Auf Veränderungen hat Heidi Schelhowe immer mit der Suche nach neuen Herausforderungen reagiert. Von 1982-1989 studierte sie Informatik an der Universität Bremen. Als wissenschaftliche Mitarbeiterin am interdisziplinären Forschungszentrum *Arbeit und Technik* der Universität Bremen hat sie begonnen, sich mit der medialen Seite des Computers und der Interaktion zu beschäftigen und promovierte 1996 mit dem Thema *Das Medium aus der Maschine. Ein Beitrag zur Auffassung vom Computer in der Informatik*. Über Stationen an der Universität Hamburg und der Humboldt-Universität zu Berlin kehrte sie 2001 als Professorin für *Digitale Medien in der Bildung* an die Universität Bremen zurück und initiierte mit ihrer Arbeitsgruppe dimeb (Digitale Medien in der Bildung) eine Vielzahl von Forschungsprojekten.

Bereits während des Studiums hat sie sich für eine sozialorientierte Informatik fachpolitisch engagiert und sich insbesondere für die Teilhabe von Frauen eingesetzt. 1986 hat sie gemeinsam mit engagierten Informatikerinnen die Fachgruppe *Frauen und Informatik* zunächst als Arbeitskreis *Frauenarbeit und Informatik* in der Gesellschaft für Informatik (GI) gegründet und als ihre erste Vorsitzende das Thema *Gender und Informatik* in dem Diskurs zur Weiterentwicklung der Informatik sichtbar gemacht. 1989 hat sie die erste Tagung *Frauenwelt – Computerräume* in Deutschland zu diesem Themenspektrum organisiert. Weitere folgten 1994 *Erfahrung und Abstraktion* und 2004 im internationalen Kontext *GIST – Gender Perspectives Increasing Diversity for Information Society Technologies* sowie 2009 *Gender und ICT*. Im Rahmen der Internationalen *Frauenuniversität* ifu, die 2000 stattfand, war sie Leiterin des zentralen Projektes *Virtuelle ifu*. Mit Projekten wie *InformAttraktiv*, gefördert vom BMBF, hat sie mit vielen Kolleginnen die Fachkultur der Informatik aus der Genderperspektive beleuchtet und somit die Diskussionen zum Bild der Informatik nach innen und außen weiter vorangebracht. Dies sind nur einige Beispiele ihres unermüdlichen Engagements. Die Perspektive auf Gender und Diversity ziehen sich als roter Faden durch ihre Forschungen und Lehrtätigkeiten im Bereich digitale Medien und Bildung.

Im Bereich *Digitale Medien in der Bildung* hat sie mit der Idee *Workshops für junge Menschen* die Ausbildung für Lehrer:innen geprägt. Mit den in ihrer Arbeitsgruppe dimeb durchgeführten Workshops können Kinder und Jugendliche spielerisch für Technik begeistert werden und ihnen werden Gestaltungsmöglichkeiten von Technik eröffnet. Mit ihrem Konzept des „Be-greifens" werden insbesondere Lehrer:innen Handlungsspielräume für die Entwicklung von diversen Zugängen zu Technik aufgezeigt. Mit ihren Arbeiten hat sie dazu beigetragen, dass sowohl in der Informatik als auch in der Lehramtsausbildung der Blick auf die Fachkultur sich verändert. Dabei steht das forschende Lernen im Mittelpunkt und Lernorte, die den Spaß am Lernen fördern, wie z. B. das Bremer Fablab als offene Werkstatt und außerschulischer Lernort (*https://fablab-bremen.org*). In diesem Kontext hat sie viele Projekte unter dem Leitbild *design. make. learn. share.* angestoßen, die auch Inspiration für weitere Fablabs oder Maker Spaces sind.

Bis zum Schluss hat sich Heidi Schelhowe der Wissenschaft verschrieben. Selbst in ihrer größten Herausforderung hat sie an einer wissenschaftlichen Studie zur Weiterentwicklung von Krebstherapien teilgenommen. Mit der Zufriedenheit, Einiges bewegt und für sich selber keine offenen Enden zu haben, ist sie in dem Bewusstsein, dass ihre Zeit nun zu Ende ist, am 11. August 2021 im Kreise ihrer Familie eingeschlafen. Wir werden sie mit ihrer zugewandten und unterstützenden Art als Wegbegleiterin vermissen.

Der Text erschien zunächst im Magazin Frauen machen Informatik *der GI-Fachgruppe Frauen und Informatik. Wir danken den Autorinnen für die Genehmigung zum Nachdruck.*

Das FIfF verleiht die Weizenbaum-Medaille an Prof.in Dr.in Dr.in h.c. Christiane Floyd

Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) verleiht im Rahmen der FIfF-Konferenz am 13. November 2021 in München den Weizenbaum-Ehrenpreis 2021 in Form der Weizenbaum-Medaille an Prof.in Dr.in Christiane Floyd für ihre außerordentlichen Verdienste um die Informatik im gesellschaftlichen Kontext.

Das FIfF stiftet den Weizenbaum-Ehrenpreis in Erinnerung an den Wissenschaftler und Informatik-Pionier Professor Dr. Joseph Weizenbaum, der über Jahrzehnte hinweg einen kritischen Blick auf die Entwicklungen und Auswirkungen der Informatik geworfen und seine Standpunkte streitbar vorgetragen hat. „Mit der Vergabe des Preises wollen wir auch die Bedeutung der Informatik für die gesellschaftliche Entwicklung betonen und auf die kritische, öffentliche Auseinandersetzung mit den Erkenntnissen und Artefakten der Informatik dringen“, erläutert der FIfF-Vorsitzende Stefan Hügel.

Die diesjährige Preisträgerin Christiane Floyd hat ihr Fach Softwaretechnik in Forschung und Lehre einzigartig geprägt. Mit ihren Forderungen nach Partizipation von Nutzenden und Betroffenen bei der Systementwicklung sowie nach Berücksichtigung sozialer und ethischer Anforderungen hat sie die Softwaretechnik maßgeblich beeinflusst und unter Einbeziehung sozialwissenschaftlicher, ethischer und philosophischer Gesichtspunkte beispielhaft ausgestaltet. Das FIfF-Vorstandsmitglied Professorin Dr. Britta Schinzel ergänzt: „Christiane Floyd hat ihr Fach im Sinne einer gesellschaftlichen Verantwortung für die Informatik aufgefasst, gestaltet und gelebt – eine außergewöhnliche Persönlichkeit und ein großes Vorbild.“

„Christiane Floyds Ideen sind heute im Fach weitgehend akzeptiert, aber keineswegs immer durchgesetzt“, stellt FIfF-Vorstandsmitglied Professor Dr. Hans-Jörg Kreowski fest. Die Beteiligung von Benutzenden an der Software-Entwicklung in deren Kontexten ist inzwischen Standard. Ethischen Rücksichten steht jedoch neben immer noch mangelnder Einsicht die undurchdringliche Komplexität heutiger Plattformen, Software-Lösungen und aufkommender Anwendungen von Künstlicher Intelligenz im Wege. „Es scheint, dass die lautstarken Forderungen und Initiativen zu Ethik in der Künstlichen Intelligenz als Vorwand dienen, institutionelle und rechtliche Regulierungen dieser unkontrollierbaren Technik vermeiden zu wollen“, so Professor Kreowski weiter.

Darüber hinaus engagiert sich Christiane Floyd seit 20 Jahren in Äthiopien beim Aufbau des Informatikstudiums und arbeitet mit äthiopischen Kolleginnen und Kollegen in einem Projekt zusammen, das mit Hilfe einer App die Mütter- und Kindersterblichkeit senken soll.

Christiane Floyd war mit ihrer Berufung an die Technische Universität Berlin 1978 die erste Professorin in der Informatik im deutschen Sprachraum. 1984 hat sie sich mit Nachdruck und Engagement an der Gründung des FIfF beteiligt und wurde zu dessen erster Vorsitzenden gewählt.

Zur Person der Preisträgerin

Christiane Floyd wurde 1943 in Wien geboren. Sie studierte dort Mathematik und promovierte 1966 mit einem Thema aus der Algebra. Danach ging sie nach München, um bei Siemens an der Entwicklung eines ALGOL-Compilers mitzuarbeiten. Von 1968 bis 1973 arbeitete sie als Wissenschaftliche Mitarbeiterin an der Universität Stanford im KI-Projekt DENDRAL von Edward Feigenbaum. Danach ging sie als Leiterin des Bereichs Methodenentwicklung der Firma Softlab nach München zurück. Sie hat dort maßgeblich die weltweit erste Programmentwicklungsumgebung *Maestro* mitentwickelt.

Spätestens da fiel ihr auf, dass die Arbeit der Entwicklerinnen und Entwickler durch die Zentrierung auf Formales und Technik entfremdet war und plädierte, dass Informatik keine reine Technikwissenschaft sein dürfe, dass Grundlagen aus den Sozial- und Geisteswissenschaften integriert werden und dass Entwickelnde und Anwendende in Dialog treten müssten. Auf ihrer Professur für Softwaretechnik an der Technischen Universität Berlin entwickelte sie zusammen mit ihrer Arbeitsgruppe seit 1978 dazu mit STEPS (Softwaretechnik für evolutionäre und partizipative Systemgestaltung) die wissenschaftlichen Grundlagen. Diese Pionierleistung partizipativer Softwareentwicklung war anfangs

Christiane Floyd bei der Preisverleihung auf der FIfF-Konferenz 2021 in München

sehr umstritten, ist inzwischen aber weitgehend akzeptiert. Für ihre weitergehende Forderung nach einer kontinuierlichen Einbeziehung ethischer Fragestellungen in Wissenschaft und Praxis der Informatik gilt das noch nicht. 1991 nahm sie einen Ruf auf eine Professur für Softwaretechnik an der Universität Hamburg an, wo sie ihre bahnbrechenden Arbeiten bis zu ihrer Pensionierung 2008 fortsetzte.

Mit ihrer Berufung 1978 an die Technische Universität Berlin war sie die erste Informatik-Professorin im deutschen Sprachraum. 2012 wurde sie zur Honorarprofessorin der Technischen Universität Wien bestellt, 2017 erhielt sie die Ehrendoktorwürde der Fakultät für Elektrotechnik, Informatik und Mathematik der Universität Paderborn, und 2020 erhielt sie von der Klaus-Tschira-Stiftung und der Gesellschaft für Informatik den Klaus-Tschira-Preis.

Seit über 20 Jahren engagiert sich Christiane Floyd in Äthiopien, wo sie einen Promotionslehrgang in Informatik mitaufgebaut hat und in einem Projekt tätig ist, in dem sie mit Wissenschaftlerinnen und Wissenschaftlern des Landes IT-Systeme für das Gesundheitswesen entwickelt. Sie hat sich an der Internationalen Frauenuniversität *Technik und Kultur* (ifu) beteiligt – einem Hochschulreformexperiment anlässlich der Weltausstellung 2000 in Hannover. Sie hat auch mehrfach die jährlich stattfindende Informatica Feminale in Bremen als Dozentin unterstützt. Außerdem ist sie Gründungsmitglied und Mitglied des wissenschaftlichen Beirats des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) und war von 1984 bis 1987 dessen erste Vorsitzende.

Mathias Haimerl

Zum technologischen Infantilismus der Industrie und des Healthcare-Sektors

Während die Digitalisierung voranschreitet und die Abhängigkeit von Computern auf einem nie dagewesenen Level ist, stillen Konzerne ihren Datenhunger auf Kosten des Datenschutzes, wirtschaftlicher Schäden und sogar Menschenleben. Das Ungleichgewicht zwischen den Interessen von Software-Unternehmen und den Endanwendern wird medienwirksam verpackt und quelloffene Software marketing-technisch torpediert. Warum betrifft das Problem jeden Einzelnen von uns? Was können wir dagegen tun? Und warum müssen wir etwas dagegen tun?

Die Bedrohung ist hoch. Firmen [8], Gemeindeverwaltungen [35] und Krankenhäuser [20] werden immer mehr zur Zielscheibe digitaler Bedrohungen. Das Problem ist die Basis vieler Systeme – allen voran im Gesundheitswesen. Als Software-Architekt im Gesundheitssektor bin ich immer wieder erstaunt, wie ignorant an grundlegende Probleme herangegangen wird und schwerwiegende – teure oder potenziell tödliche [13, 14] – Risiken businesstauglich in Kauf genommen werden. Ich bin überzeugt, dass die Gesellschaft die Probleme verstehen muss, damit der Gesundheitssektor in Bewegung kommt, denn heute scheint es nicht genug, wenn es brennt, solange mit dem brennenden System noch Geld zu machen ist.

Das Grundproblem – Informationssicherheit

In einer Zeit, in der soziale Medien das Gefühl für Privatsphäre und Datenschutz anscheinend *wegoptimieren,* scheint das Bewusstsein dafür in der Bevölkerung auch bei anderen Themen zu schwinden. Finden wir es zum Teil noch in Ordnung, wenn unsere Bankdaten über die USA geschickt werden [27], so sind sich doch die meisten Menschen im Klaren, dass Gesundheitsdaten sehr persönlich sind. Warum kümmern wir uns nicht darum? Warum gehen wir davon aus, dass der Arzt *schon weiß, was er tut,* wenn er einen Computer bedient? Warum gehen wir davon aus, der IT-Leiter einer Klinik *weiß was er tut,* wenn er ein neues System aus Werbe- oder Kostengründen einführt?

In diesem Kontext möchte ich die Schutzziele der Informationssicherheit beleuchten, im Vergleich von Windows als proprietärer zu Linux als quelloffener Software.

Vertraulichkeit

Spätestens mit Windows 10 hat Microsoft eine nie dagewesene Datensammelwut begonnen, die sich nur für bestimmte Versionen überhaupt deaktivieren lässt – und dort schwer [31]. Der Aufbau dieser Lauschinfrastruktur, genannt *Event Tracking for Windows (ETW),* ist komplex und tief im System verankert. Technisch gesehen könnte dadurch jede Information, die am Computer aufgerufen oder eingegeben wird, an Microsoft übermittelt werden [15]. Allein dieses standardmäßig aktivierte Modul führt zu einer grundsätzlichen Verletzung der Vertraulichkeit. Das *Need-to-know*-Prinzip [32], eines der Grundprinzipien des Datenschutzes wird hierbei vollständig ignoriert.

Microsoft stellt zwar eine immense Liste mit Art und Umfang der gesammelten Daten online zur Verfügung [18], allerdings ist es bei Firmen, die sich selbst kontrollieren, immer fraglich, inwieweit diese Informationen vollständig und wahrheitsgemäß sind – oder ob die von Microsoft gestellten Hürden die Administratoren von einer Deaktivierung der Telemetrie abhält. Laut Microsoft werden diese Daten erfasst, um das System laufend zu verbessern. Ich selbst habe während der Nutzungszeit von Windows (nach XP) keinerlei Verbesserung erfahren. Da ich Windows und Linux parallel nutze, habe ich einen direkten Vergleich.

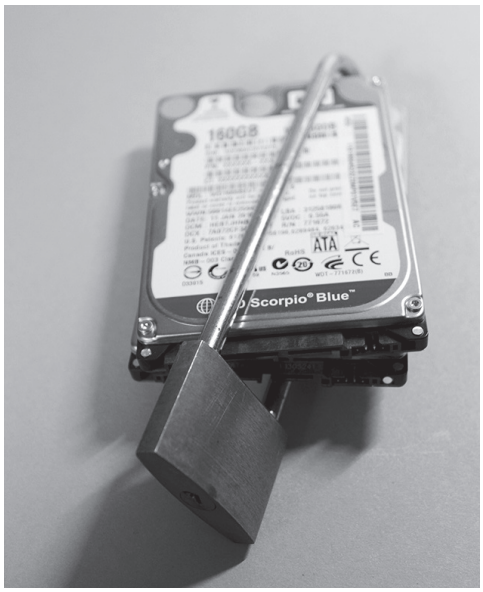
Integrität & Verfügbarkeit

Beide sind Aspekte der Robustheit gegenüber Hackern und Viren, unerwarteten Systemeingaben oder dem Zusammenkommen unterschiedlicher Systemzustände [9]. Alle Windows-Nut-

zer kennen den *Blue Screen of Death (BSOD).* Der Systemkern von Windows stellt bei diversen Konstellationen seine Arbeit ein und zeigt das an. Weiterarbeiten wird verhindert, der Nutzer aufgefordert zu warten, bis genug Informationen gesammelt wurden. Die ungesicherten Daten des Nutzers sind natürlich trotzdem verloren. Aber ein BSOD ist nicht das Ende. Zwar verliert man alle ungesicherten Daten, kann aber den Computer neu starten und in der Regel weiter arbeiten. Anders sieht es bei Verschlüsselungs-Trojanern bzw. Ransomware aus. Ein kleines Stück Software verschlüsselt das System und alle Daten. Ist das erledigt, wird dem Nutzer nur noch der Preis für das Entschlüsseln angezeigt [24]. Diese Art von Schad-Software verbreitet sich aus gutem Grund am stärksten: Ransomware macht das System unverfügbar. Jede Minute, die ein System nicht verfügbar ist, kostet Geld. Je zentraler, desto höhere Kosten, weshalb zwei von drei Unternehmen das Lösegeld bezahlen [28]. Diese Art von Erpressung funktioniert, was zu neuen, besseren Crypto-Trojanern führt. Ein Teufelskreis auf Kosten der Verfügbarkeit. Zwar ist Windows nicht das einzige Betriebssystem, bei dem Systemabstürze oder Ransomware existieren, aber im Vergleich zu anderen Systemen hat Windows das größte Verbesserungspotenzial [25]. Als ich zu Linux wechselte, hieß es: „unter Linux gibt es keine Viren". Das ist zwar nicht korrekt, aber hat einen wahren Kern: Um Viren *scharf zu schalten,* benötigt man Sicherheitslücken, um Administrator-Privilegien zu bekommen. Erst dann kann man im System weitgehend ungestört sein Unwesen treiben. Diese unter Windows zu finden ist kein Problem [1]. Es gibt einen globalen Schwarzmarkt für bisher undokumentierte ZeroDay-Sicherheitslücken, was neben Hackern auch Staaten für sich entdeckt haben [4]. Linux hat hier zwei entscheidende Vorteile:

1. Open Source

   Dadurch, dass die Quelldateien offen für jeden Interessierten einsehbar sind, werden Fehler meist frühzeitig entdeckt und behoben. Grobe Fehler fallen meist früher auf, allerdings manchmal auch erst Jahre später [2]. In der Zeit vom Finden eines Fehlers, bis der Fehler behoben und an alle Endgeräte ausgeliefert ist, muss ein Virus entwickelt, verteilt und *aktiviert/etabliert* werden. Viele Viren werden erst durch die Ausnutzung mehrerer Lücken gefährlich. Dadurch ist es sehr aufwändig und weniger attraktiv, Viren für Linux zu entwickeln.



Informationssicherheit

2. Kurze Updatezyklen

   Windows-Nutzer kennen die großen, in Zyklen verteilten Sicherheitsupdates [5]. Hier werden viele Lösungen für Sicherheitslücken zusammengepackt und ausgeliefert. Es ist prinzipiell schlecht, die Lösung einer Sicherheitslücke zurückzuhalten, um gebündelt auszuliefern. Hier zeigt sich der zweite große Vorteil von Linux: Modularität [22]. Während Windows als Monolith Gesamtupdates von zentraler Stelle erhält, besteht eine Linux-Distribution aus einer Zusammenstellung von Programmen für verschiedene Aufgaben. Jedes dieser Programme (z. B. Datei-Manager, Editor, Shell, …) hat seine eigenen Entwickler, die ihr Projekt aus Eigeninitiative entwickeln. Daher werden Bugs in quelloffenen Programmen meist innerhalb weniger Stunden behoben. Die meisten Distributionen haben dezentrale Verwaltungen, bei denen eine neue Version angekündigt wird. Endanwender können regelmäßig prüfen, ob ein neues Update vorhanden ist, und dieses mit einem Klick installieren. Oder man automatisiert das Ganze mit einem einmaligen Klick [19]. Es kommt nicht selten vor, dass der Patch für eine Lücke, über die ich eben gelesen habe, bereits zur Installation bereitsteht. Wenn die ausgenutzte Lücke durch die Entdeckung des Virus auffällt und innerhalb weniger Stunden geschlossen wird, kann der Virus einige wenige Computer infizieren, sich aber nicht etablieren.

Kein Argument: Verbreitung

Ein zentrales Argument, das häufig an dieser Stelle von Microsoft-Fans angeführt wird, ist, dass Linux nicht so verbreitet sei. Es lohne sich nicht, Malware für Linux zu entwickeln. Betrachten wir die Betriebssysteme aller Geräte weltweit, so hat Linux sogar die größte Verbreitung. Wir dürfen dafür nicht nur PCs, sondern auch Server und Smart Devices betrachten. Die Linux Distribution Android gehört mit über 50 % Marktanteil bei Smartphones zu den größten Treibern der Verbreitung von Linux im letzten Jahrzehnt. Natürlich stieg dadurch die Anzahl an Viren mit Android als Ziel. Allerdings hat genau dieser Trend dazu geführt, dass mehr Lücken in Linux gefunden und gestopft wurden [3].

Das Beispiel Android zeigt auch, dass Sammelupdates den Weg für Viren erleichtern. Während bei anderen Distributionen ganz typischerweise Updates für Einzelpakete durchgeführt werden, nutzen alle mir bekannten Hersteller Sammelupdates und *vertagen* dadurch relevante Sicherheitsupdates. Insgesamt scheinen aber mobile Systeme für Hacker zunehmend uninteressant zu werden, wenn man die aktuellen Statistiken von *Kaspersky* [16] mit denen von 2012 [21] vergleicht.

Status Quo: „Vendor Lock-in"

Auch in Arztpraxen und Krankenhäusern werden fast ausschließlich auf Microsoft Windows basierende Systeme verwendet. Das mag sinnvoll erscheinen, denn jemand, der es gewohnt ist privat

Windows zu nutzen, wird das gleiche System am Arbeitsplatz besser bedienen können. Das entspricht allerdings nicht der Realität. Niemand arbeitet mit dem Betriebssystem, sondern mit den Anwendungen. Kein Buchhalter installiert Treiber. Kein Arzt richtet Netzwerke ein. Dafür gibt es IT-Spezialisten. Natürlich gibt es Ausnahmen, wie Ärzte, die sich selbst für ein Linux-System entschieden haben (und damit sehr zufrieden sind).

Nicht alle Windows-Anwendungen lassen sich auf anderen Systemen (Linux, Mac OS, …) installieren, und die meisten Anbieter bieten ihre Programme nur für Windows an. Warum sollten die Firmen den Aufwand betreiben, die meist aufwändige Migration auf weitere Systeme zu stemmen? Aus rein wirtschaftlichen Motiven ist das widersinnig. Es gibt nur einen kleinen Markt. Würden mehr Anwender Linux nutzen, würde es sich eher rentieren. Aber wo kein Wille, da kein Weg. Warum lohnt sich der Aufbruch ins #*Neuland* trotzdem?

Firmen versuchen Interna intern zu halten. Geschäftsgeheimnisse dürfen nicht jedem zugänglich sein. Insbesondere nicht der Konkurrenz oder noch schlimmer: Menschen, die Geheimnisse der Konkurrenz verkaufen. Offensichtlich war dieses Schutzbegehren Microsoft ein Dorn im Auge. Was lag da näher, als die Office-Anwendungen in die Cloud zu verlagern? Der beste Grund, die persönlichen Daten von lokalen auf fremde Rechner zu laden, ist, dass die Software dort läuft. – Das Ganze ist automatisch immer up-to-date und dadurch sicherer … und billiger! Firmen sind reihenweise auf die günstige Lösung aufgesprungen, ohne sich großartig Gedanken darüber zu machen, was das für die Hoheit über die eigenen Daten bedeutet. Microsoft dürfte bei den Vertragsabschlüssen klar sein, dass der Zugriff auf die Daten jederzeit möglich ist. Das Gegenüber spart sich IT-Fachpersonal, das bisher die Computer aktuell halten muss. Das muss es zwar immer noch, aber zumindest nicht die Office-Programme. Seit der Einführung von Office als Cloud-Version hat sich einiges getan: Die Preise sind gestiegen [29] und sicher sind die Daten natürlich auch nicht [10, 6].

Apropos: Die Cloud-Lösung ermöglicht auch, dass man Office auf Linux-Rechnern verwendet. Im Browser. Mit eingeschränktem Funktionsumfang. Bei vollem Preis. Keine Pointe.

Never touch a running system

Angenommen, Windows wäre ein gutes Betriebssystem. Selbst unter dieser Annahme gibt es sehr gute Gründe, die gegen eine Entwicklung von *Windows-only*-Produkten sprechen, denn die oft gehörte Aussage, dass die Nutzer primär Windows nutzen wollen, ist eine *self-fulfilling prophecy:* Heute behaupten wir, dass es sich nicht rentiert, für Linux zu entwickeln, morgen müssen noch mehr Nutzer ungewollt Windows einsetzen, weil es ihre Software für Linux nicht gibt. Dadurch sinkt der Anteil an Personen, die alternative Systeme nutzen … und so fort. Meine Meinung als Software-Architekt: Wenn der Aufwand betrieben wurde, eine Software zur Marktreife zu entwickeln, dann ist der Aufwand marginal, sie für weitere Systeme zu releasen.

Selbst wenn man von einem Tag auf den anderen eine Komplettlösung mit quelloffener Software anbieten könnte, würde man eher auf Ablehnung stoßen, denn die alten Systeme laufen im Moment ja wunderbar. Dass man sich bei komplexen Systemen, deren Integration Stunden, Tage oder Wochen dauert, lieber auf der Momentaufnahme des laufenden Systems ausruht als die Migration auf ein potenziell besseres oder stabileres System in Kauf zu nehmen, ist so nachvollziehbar wie ignorant und führt zu einem destruktiven Trend: *Updatemüdigkeit*. Updates werden aus diffusen Ängsten nicht zeitnah installiert, wodurch Lücken länger offen bleiben als nötig [34, 26].

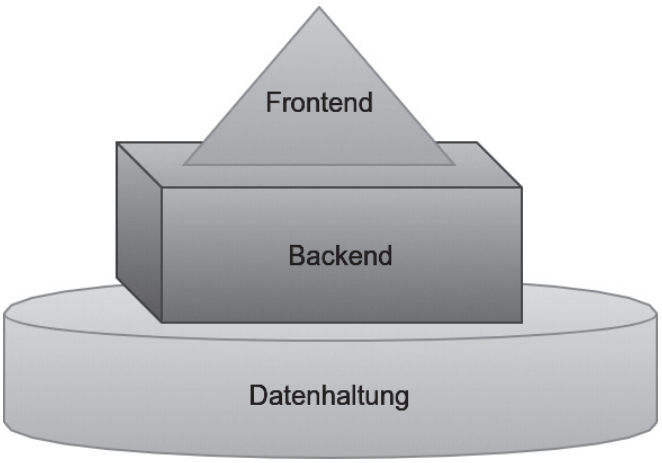
Schlechte Software trainiert uns an, Updates nicht zeitnah zu installieren, wodurch wir Sicherheitslücken aktiv offen halten Die gefühlte Wahrscheinlichkeit von schwerwiegenden Problemen durch die Updates ist höher als die, durch offene Sicherheitslücken bedroht zu werden. Der Schaden eines solchen Angriffs ist aufgrund der potenziellen Höhe schwer zu fassen, nicht nur wirtschaftlich [12], sondern insbesondere, wenn Menschenleben gefährdet sind.

Architektur moderner Software-Systeme

Windows hat maßgeblich zur Verbreitung von privaten Computern beigetragen. Als die Digitalisierung in Büros und Arztpraxen Einzug hielt, kam flächendeckend Windows zum Einsatz. Die anfangs durch Textverarbeitung und Tabellenkalkulation abgebildeten Arbeitsprozesse wurden schnell von Software-Entwicklern aufgegriffen und optimiert. Natürlich auf Windows-Basis. Access, Excel, Word. Eine exe-Datei ausgeführt und das Programm tut, was es soll. Genial. Skaliert nur nicht.

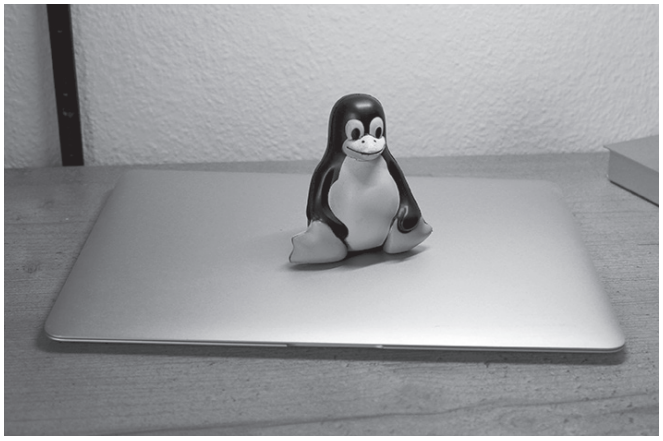
Was in der Verwendung einzelner Verwaltungskomponenten wunderbar funktioniert, lässt sich leider nicht 1:1 auf große Systeme übertragen. Dafür braucht man mehr Rechenleistung als ein normaler Praxiscomputer liefert. Deswegen wird fast alle neu entwickelte Software als verteiltes System aufgebaut. Die eigentliche Software läuft auf einem Server und der Nutzer startet ein Programm zur Visualisierung und Bearbeitung von Daten [30]. Die meisten dieser Server werden übrigens unter Linux betrieben [33]. Und exakt hier ist der Punkt, an dem Systemunabhängigkeit wieder ins Spiel kommt.

Während man noch vor zehn Jahren für jedes Zielsystem eigene Oberflächen bauen musste, ist das heutzutage weder notwendig noch sinnvoll, denn durch den HTML5-Standard wurde der größte Teil von Systemfunktionalität in einheitlichen Schnitt-



Architektur

stellen für Web-Oberflächen zur Verfügung gestellt. Zugriffe auf Systemkomponenten wie 3D-Beschleunigung und Verschlüsselung sind jetzt nativ, sicher und systemunabhängig implementiert [7]. Es gibt also keinen Grund mehr, neu entwickelte Applikationen nur für Windows zu entwickeln.



Tux, das offizielle Maskottchen des freien Linux-Kernels

Weiterführende Gedanken

Haben Sie irgendeinen Aspekt entdeckt, der Ihnen neu, seltsam oder ungemütlich vorkommt? Für mich ist das Ungemütlichste die Frage, ob ich als Mensch, der die Daten einer Vertrauensperson übergibt, ein Recht darauf habe, dass meine Daten entsprechend den Regeln der Informationssicherheit behandelt werden:

Wenn ich im Amt einen Ausweis beantrage und meine kompletten Daten in einen Windows-PC eingetragen werden, wer sagt mir, dass die Microsoft-Telemetrie diese Daten nicht nach Redmond schickt und dabei Geheimdienste und sonstige Trittbrettfahrer meine Daten ausspähen? Habe ich als Bürger die Verpflichtung, mich dieser Missachtung von Datenschutz zu unterwerfen, weil es eine Ausweispflicht gibt? Wenn ich eine medizinische Behandlung möchte, muss ich dann akzeptieren, dass mein Arzt meine Röntgenbilder in ein System einpflegt, das *insecure-by-design* ist [23]? Wenn ich nach einer Operation aufgrund eines Softwarefehlers mein Bein verliere, habe ich Anspruch auf Schadensersatz oder heißt es einfach „Softwareproblem. Kann man nichts machen?“[17] Warum messen wir als Gesellschaft mit zweierlei Maß, so dass wir bei fehlerhafter Hardware klagen, aber vermeidbare Softwarefehler hingenommen werden? Wie können wir das grundlegend ändern?

Wohin müssen wir gehen?

Bei allen aktuellen Problemen im Bereich der Software scheint es, als gäbe es keine Lösungen. Das stimmt so nicht. Wir müssen uns von unserer Veränderungsresistenz lösen und uns der Fehlbarkeit der Software-Entwickler bewusst werden. Aber wir müssen das intelligent anstellen. Softwarefehler werden immer vorkommen. Aber Softwarefehler können, sollen und müssen immer zurück zum Hersteller gegeben werden. Wenn sich bei Ihrem Auto der Beifahrersitz löst, sobald Sie einen bestimmten Radiosender einstellen, werden Sie das Auto auch zu Ihrem Händler zurückbringen. Warum machen Sie das nicht mit Software?

Oder sehen wir die andere Seite: Mein Arbeitgeber verpflichtet Software-Entwickler, einen Windows-PC zu verwenden. Auch wenn das mehr Probleme verursacht, die Arbeitsleistung darunter leidet und eine zentrale Verwaltung von Rechnern natürlich weitere Sicherheitslücken öffnet. Die Realität sieht leider so aus, dass man ein potenziell unsicheres System als Basis hat und mehrere Schichten an Antiviren-Software, Firewalls und sonstigen Softwarelösungen darauf legt, die meisten wiederum proprietär.

Wir müssen weg von dem Denken, dass Kosten und Sicherheit von Software zusammenhängen oder komplexere Software sicherer ist.

Wir müssen hin zu einer IT-Infrastruktur-Denkweise, die auf wissenschaftlichen Erkenntnissen basiert, anstatt unseren gesamten Datenschatz in die Hände von intransparenten Konzernen zu legen.

Wir müssen aufhören,

- kritische Infrastrukturen auf den Produkten von Herstellern aufzubauen, die mehr an Nutzerdaten Interessiert sind als an Stabilität und Datensicherheit, sich aber als *Heilsbringer-as-a-Service* präsentieren.

- unsere IT-Entscheidungen von Betriebswirtschaftlern treffen zu lassen, die sich von Marketing-Experten der Softwarehäuser beim Golfspielen von ihrer Unfehlbarkeit überzeugen lassen.

- nur High-Level Entwickler auszubilden, die nicht mehr verstehen, wie ein Computer funktioniert, sondern nur noch mit einem konkreten Framework umgehen können.

Wir müssen anfangen, die Softwarekosten nicht nur für Entwicklung, Bereitstellung und Wartung zu berechnen, sondern auch die Effizienz der Arbeit mit dem System zu verrechnen und natürlich den potenziellen Schaden bei Infiltration.

Vor allem müssen wir uns aber des zugrunde liegenden Problems bewusst sein. Wir müssen uns Softwarefehlern proaktiv nähern. Ist es ein Fehler? Dann muss er behoben werden. Habe ich etwas falsch gemacht? Vermutlich ein UX-Fehler, ergo sollte er behoben werden. Wir leben in einer Zeit von intuitiven Frontends und *User Experience (UX) Design* im Entwicklungsprozess.

Wir müssen aufhören, mehr und mehr Rechenleistung zu verbrauchen. Software wird heute mit übermäßig viel Framework-Unterstützung geschrieben und braucht dadurch viel mehr Rechenleistung und Speicher als nötig. Das wirkt sich auf den Energieverbrauch aus. Schlechte Software erzeugt also mehr CO_2. Wir müssen beginnen, die Nachhaltigkeit von Software zu bewerten.

Wir müssen aufhören, die Software als schlau und die Benutzer als dumm zu sehen. Software soll den Menschen unterstützen. Nicht ihm die Rechte nehmen, nicht ihn herausfordern.

Und: Wir müssen unser Wissen über Softwareprobleme teilen! Niemand sollte heutzutage gezwungen werden, Einschränkun-

gen oder Kompromisse bei Privatsphäre oder Datenhoheit einzugehen. Niemand sollte gezwungen werden, kostenpflichtige Software zu nutzen, um ins Internet zu gehen oder Briefe zu schreiben. Wir zerstören unser Verständnis von Qualität, Datenschutz und Vertraulichkeit. Das müssen wir stoppen.

Die Firmen und insbesondere der Healthcare-Sektor (nicht nur) in Deutschland geben mehr und mehr die digitale Autarkie aufgrund von Geschäftsbeziehungen und Innovationsangst auf. Durch die Schaffung von mehr Abhängigkeit wird weitere Abhängigkeit geschaffen. Deutschland wächst nicht durch die digitale Adoleszenz zu einem ausgewachsenen, IT-kompetenten Land heran, solange wir uns von Microsoft und Google den digitalen Schnuller geben lassen.

Literatur

[1] Ablon L, Bogart A (2017) Zero days, thousands of nights: the life and times of zero-day vulnerabilities and their exploits. RAND Corporation, ISBN 978-0-8330-9761-3

[3] Barrett B (2016) Hack Brief: Years-Old Linux Bug Exposes Millions of Devices. Wired. https://www.wired.com/2016/01/hack-brief-years-old-linux-bug/. ISSN 1059-1028. Zugegriffen: 7. September 2021

[4] Borchers D (2018) Cyber-Sicherheitspolitik: Fünf Prozent Zero-Day-Lücken für staatliche Überwachung von Kriminellen. Heise online. https://heise.de/-4072578. Zugegriffen: 28. Juli 2021

[5] Born G (2018) Windows 10: Microsoft erklärt die Update-Zyklen. https://www.borncity.com/blog/2018/08/02/windows-10-microsoft-erklrt-die-update-zyklen/. Zugegriffen: 7. September 2021

[6] Born G, Wittenhorst T (2021) Cloud-Datenbank-GAU: Microsoft informiert Azure-Kunden über gravierende Lücke. Heise online. https://heise.de/-6176601. Zugegriffen: 7. September 2021

[15] Bundesamt für Sicherheit in der Informationstechnik (BSI) (2020) Analyse der Telemetriekomponente in Windows 10 – Konfigurations- und Protokollierungsempfehlung (Version 1.2). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Analyse_Telemetriekomponente_1_2.pdf. Zugegriffen: 28. Juli 2021

[9] Eckert C (2012): IT-Sicherheit: Konzepte – Verfahren – Protokolle. 7. überarb. und erw. Aufl. Oldenbourg-Verl. ISBN 978-3-486-70687-1

[10] Einsiedler E (2021) Der EU-US Privacy Shield. Universität Linz, Dissertation. http://epub.jku.at/obvulihs/5833126. Zugegriffen: 7. September 2021

[11] Flade F (2020): Cyberangriff auf Bundestag: Haftbefehl gegen russischen Hacker. – URL https://www.tagesschau.de/investigativ/ndr-wdr/hacker-177.html. Zugegriffen: 7. September 2021

[35] Frankfurter Allgemeine Zeitung (2021): Landkreis liegt lahm: Erster Cyber-Katastrophenfall in Deutschland. In: FAZ.NET. – URL https://www.faz.net/-ikh-admez. ISSN 0174-4909. Zugegriffen: 7. September 2021

[12] Gebauer M (2021) Ransomware-Angriffe kosten im Durchschnitt 570.000 US-Dollar. Heise online. https://www.heise.de/-6158568. Zugegriffen: 7. September 2021

[28] Help Net Security (2021) Only 8back. https://www.helpnetsecurity.com/2021/04/28/ransom-paid/. Zugegriffen: 1. August 2021

[13] Holland M (2021) Vorwürfe an US-Klinik: Möglicherweise erster Todesfall wegen Ransomware-Attacke. https://www.heise.de/-6206624. – Zugegriffen: 2. Oktober 2021

[14] House, M (2021) Attributing Deaths to Ransomware Attacks on Hospitals and Medical Care Facilities. Yale Cyber Leadership Forum. https://bit.ly/3isyzy6. Zugegriffen: 7. September 2021

[8] Jung J (2021) Zwei Drittel der deutschen Unternehmen erleiden Ransomware-Attacken. ZDNet. https://bit.ly/3l1AYRU. Zugegriffen: 7. September 2021

[16] Kaspersky Labs (2020) Mobile Malware: weniger, aber gefährlicher. https://www.kaspersky.de/about/press-releases/2020_mobile-malware-weniger-aber-gefaehrlicher. Zugegriffen: 1. August 2021

[17] von Leitner F. Fefes Blog (Suche nach „Softwareproblem"). https://blog.fefe.de/?q=Softwareproblem. Zugegriffen: 28. Juli 2021

[18] Lich B (2021) Windows 10, Version 21H1, Windows 10, Version 20H2 und Windows 10, Version 2004 – erforderliche Diagnoseereignisse und -felder (Windows 10) – Windows Privacy. https://bit.ly/3Bl1xaB. Zugegriffen: 3. Oktober 2021

[19] Linux Mint (2019) New Features in Linux Mint 19.2 "Tina" Cinnamon Edition – Linux Mint. https://linuxmint.com/rel_tina_cinnamon_whatsnew.php. Zugegriffen: 3. Oktober 2021

[7] MDN contributors (2021) Web APIs. MDN. https://developer.mozilla.org/en-US/docs/Web/API. Zugegriffen: 3. Oktober 2021

[20] Muncaster P (2021) Ransomware Surge Drives 45% Increase in Healthcare Cyber-Attacks. Infosecurity Magazine. https://bit.ly/2Ylegvw. Zugegriffen: 7. September 2021

[21] Namestinov Y, Maslennikov D (2012) Kaspersky Security Bulletin 2012. The overall statistics for 2012. https://bit.ly/3uDdNAl. Zugegriffen: 1. August 2021

[22] Narduzzo A, Rossi A (2003) Modularity in Action: GNU/Linux and Free/Open Source Software Development Model Unleashed. ROCK Working Papers 020. Department of Computer and Management Sciences, University of Trento, Italy. https://ideas.repec.org/p/trt/rockwp/020.html. Zugegriffen 3. Oktober 2021

[23] Pegoraro R (2003) Microsoft Windows: Insecure by Design. Washington Post. https://wapo.st/3l4OlR8. ISSN 0190-8286. Zugegriffen 3. Oktober 2021

[2] Qualys Security Advisory (2021) CVE – CVE-2021-33909. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33909. Zugegriffen: 28. Juli 2021

[24] Richardson R, North M (2017) Ransomware: Evolution, Mitigation and Prevention. International Management, Review 13, Nr. 1, S. 10–21

Mathias Haimerl

Mathias Haimerl ist Doktorand an der JKU Linz und der Technischen Hochschule Ingolstadt und forscht im Bereich *Inklusion im autonomen Verkehr.* Abseits der akademischen Tätigkeit ist er als Software-Architekt bei *Siemens Healthineers* beschäftigt.

[25] Sarr M (2017) Which OS Crashes Less Often: Mac OS X, Linux or Windows?. https://www.fossmint.com/which-os-crashes-less-often-mac-os-x-linux-or-windows/. Zugegriffen: 28. Juli 2021
[26] Schmidt J (2020) Exchange-Lücke: Immer noch viele Server offen. Heise online. https://www.heise.de/-4947221. Zugegriffen: 9. September 2021
[27] Schuppelius DJ (2020) DKB und Cloudflare. https://deinnetzwerkfachmann.de/allgemein/dkb-und-cloudflare/. Zugegriffen: 28. Juli 2021
[29] Spataro J (2021) Microsoft 365 für Unternehmenskunden: Neue Preise ab März 2022. News Center Microsoft. https://bit.ly/2YgjvMo. Zugegriffen: 22. August 2021
[30] Tanenbaum AS, v. Steen M (2002) Distributed systems: principles and paradigms. Prentice Hall. ISBN 978-0-13-088893-8
[31] Tremmel M (2020) Datenschutzbeauftragter: Windows 10 lässt sich ohne Telemetrie betreiben. Golem.de. https://glm.io/146423. Zugegriffen: 28. Juli 2021
[32] Trommler P (2000) The application profile model. Dissertation. Hochsch.-Verl. an der ETH. ISBN 978-3-7281-2739-6
[33] W3Techs. Usage statistics of operating systems for websites. https://w3techs.com/technologies/overview/operating_system. Zugegriffen: 28. Juli 2021
[34] Wittenhorst T (2018) Verschwundene Dateien: Microsoft zieht Windows-10-Update vorerst zurück. https://www.heise.de/-4182651. Zugegriffen: 28. Juli 2021

Markus Reinisch

„Revolutionen finden leibhaftig statt". Die Diskursräume *Straße*, *Netz* und die Protestlogik in Zeiten des Digitalen

Protestformen als Mittel demokratischer Partizipation spielen sich durch den Einfluss digitaler Medien immer mehr im Virtuellen ab. Trotz immer einfacherer Möglichkeiten, sich mittels sozialer Netzwerke zu organisieren und zu mobilisieren, bleibt der Wert des großen Nein (Armin Nassehi) auf Straßen und Plätzen nach wie vor von großer Bedeutung für die Protestierenden, ihre Anliegen und Sichtbarkeit. In der Öffentlichkeit ein Zeichen zu setzen, mit Gleichgesinnten seine Unzufriedenheit zu artikulieren, macht das Wesen von Protest aus. Zu seiner Logik gehören Gruppendynamiken und Identität, die Bilderproduktion sowie Narrative. Die Diskursräume Netz sowie Straße sollen im Folgenden mit Blick auf diese Aspekte der Protestlogik beleuchtet werden. Dabei gilt es auch Begriffe wie Engagement und Partizipation kritisch unter die Lupe zu nehmen, da sie unter dem Einfluss des Digitalen der Gefahr einer Umdeutung unterliegen. Ferner soll die Frage aufgeworfen werden, ob durch die Social-Media-Infrastrukturen und ihre Aufmerksamkeitsökonomie nicht sogar von einer De-Politisierung auszugehen ist.

Politische Debatten verlagern sich – auch ins Netz

2010 und 2011 erlebte die Welt einen bisher nicht gekannten Höhepunkt an sozialen Bewegungen und politischen Protesten, mit Themen aus verschiedenen Lebensbereichen. Die *Repolitisierung der Gesellschaft* (Edgar Forster) zeigte sich auf Straßen sowie auf Plätzen in vielen Ländern, oft durch Netzwerke in den sozialen Medien organisiert: in Hongkong demonstrierte man gegen den wachsenden Einfluss Chinas, in der arabischen Welt nahm die *Arabellion* an Fahrt auf, in New York gab es Protestcamps gegen den Banken- und Börsenkapitalismus (*Occupy Wall Street*), in Toronto eskalierten G-20-Proteste, in Griechenland und Weißrussland gingen Menschen auf die Straße, in Madrid forderten Tausende *Indignados* eine *Democracia Real Ya!* (echte Demokratie sofort).[1] Zahlreiche Disziplinen der Politik- und Sozialwissenschaft beschäftigen sich (erneut) verstärkt mit diesen Entwicklungen und stellen etwa heraus, welche identitätsstiftenden Merkmale eine Protestgruppe als *Kollektiv*, *Wertegemeinschaft*, *Schwarm* oder sonstige Gemeinschaft ausmacht, welche Dynamiken und Motive dabei vorherrschen oder welche Wirkungsabsichten damit auf ein Publikum (z. B. Politiker:innen) verfolgt und erreicht werden.[2] Dabei beobachten sie beispielsweise eine verstärkte „Verlagerung der politischen Debatte aus den Parteien in soziale Bewegungen und andere zivilgesellschaftliche Organisationen."[3] Und ins Digitale, möchte man ergänzen, wo sich auf verschiedenen Social-Media-Netzwerken neue Formen von Partizipation, Deliberation, Foren und Plattformen für Protestartikulation ergeben haben, die es zum Beispiel aus soziotechnischer Sicht kritisch zu betrachten gilt. Dabei kann unterschieden werden: es gibt Bewegungen, die im Netz entstanden sind und die politischen Debatten immer wieder durch wirkungsstarke Bilder auf der Straße prägten. *Pegida* in Deutschland, die *Gelbwesten* in Frankreich sowie *MeToo* sind nur drei Beispiele dafür. Umgekehrt legen Protestaktionen im öffentlichen Raum auch durch ihre Verbreitung und diskursive Verarbeitung im Internet enorme Mobilisierungskräfte frei. Diese Wechselwirkungen waren vor zehn Jahren beim *Arabischen Frühling* zu beobachten. Der Protestforscher Dieter Rucht spricht von einer „Demokratisierung der Demokratie", d. h. das demokratische System habe sich in seiner Qualität durch die gesellschaftlichen Polarisierungen und sonstigen Herausforderungen zu bewähren.

Neujahrsprotest der Hongkonger auf der Straße am 1.1.2020, Foto: Etan Liam, CC BY-ND 2.0

Bilderproduktion und Protestinszenierung

An der *Black-Lives-Matter*-Bewegung infolge des gewaltsamen Tods von George Floyd durch einen weißen Polizisten in den USA lässt sich gut die transnationale Ausrichtung vieler heutiger Protestformen studieren. Insbesondere die sozialen Medien werden hierfür genutzt, denn sie sind durch ihre visuelle Ausrichtung dazu geeignet, Sichtbarkeit herzustellen und die inszenierten Protestformen mitsamt ihrer Botschaft (in diesem Beispiel: *Schwarze Leben zählen*) weltweit sowie in Echtzeit[4] zu verbreiten. Dabei gilt: digitale Plattformen wie Facebook oder Twitter „berichten nicht bloß über Proteste, sondern sind integraler Teil des Aktionsgeflechts einer Protestsituation, deren Sichtbarkeit sie mitbestimmen."[5] Dies geschieht vor allem über die starke Wirkung der (Bewegt-)Bilder beispielsweise auf Social-Media-Kanälen, wo sie geteilt, geliket, verbal kommentiert werden und so im Rahmen der ausgeprägten digitalen Aufmerksamkeitsökonomie ihre Wirkung entfalten. Auf diese Weise können sie zum Beispiel sachliche Debatten befeuern – oder auch empören, skandalisieren oder provozieren. Bilder im Netz sind also prägend, was die Wirkung auf den Diskurs insgesamt angeht. Schankweiler bringt die Funktion der Emotionalisierung durch die Inszenierung und Echtzeit-Vernetzung auf den Punkt: „Die geteilten Bilder vermitteln eine geteilte Gegenwart der Gemeinschaft der Augenzeug:innen – jenen vor Ort und jenen an den Bildschirmen. Es ist diese Gleichzeitigkeit und die Vernetzung, die Bande zwischen den Ereignissen, den Zeug:innen und den Bildern knüpfen und eine Affektgemeinschaft konstituieren."[6] Wie sich das Bildhafte und der Protest zeitlich gegenseitig bedingen können, expliziert die Bildwissenschaftlerin sodann: „Der Protest hat sich entweder noch nicht artikuliert, formiert sich jedoch mit Hilfe der Bilder, oder er ist bereits zu einer Bewegung angewachsen, die Bilder für ihre Ziele einsetzt."[7] Die Bilderproduktion folgt einer den sozialen Netzwerken inhärenten Logik sowie Ästhetik. Sie ist für die Inszenierung des Protests relevant, bei der sowohl das Körperhafte als auch das Affektive von großer Bedeutung ist: „Die Affizierung des (zum Bild gewordenen) Körpers wird zur Botschaft und soll sich übertragen."[8] Vor allem auf die Protest-Gemeinschaft und die Konstruktion von Identität in ihr sowie durch sie. Ihr hauptsächlich performativer Charakter soll im Folgenden skizziert werden.

Demonstration in New York nach dem Tod von George Floyd, organisiert von der Black Lives Matter-Bewegung. Foto: Michael Nigro, CC BY-NC 4.0

Identität: performativ als Aktivitätsnachweis

Der schillernde Identitäts-Begriff kann hier nicht debattiert werden, zu vielschichtig sind die Zugriffe auf ihn aus Sicht sowohl des Subjekts als auch verschiedenster Gruppen. Dennoch gilt es, eine Vorstellung von *Identität* zugrunde zu legen, die es möglich macht, das Kollektiv- und Gruppenprinzip und seine Dynamik im Rahmen von Protestaktionen im Virtuellen sowie auf den Straßen und Plätzen zu verstehen. Mit Blick auf die Rolle der sozialen Netzwerke ist *Identität* nicht etwa im Herderschen Sinne mit starkem Bezug auf Kontinuitäten und Traditionen, sondern vielmehr performativ zu verstehen: das heißt, es stehen Aspekte der Selbstvergewisserung, Selbstermächtigung, Mobilisierung, des Erlebnishaften und der Kommunikation von Protestanliegen im Mittelpunkt gemeinsamen Denkens und Tuns. Sich einer aktiv vor Ort handelnden oder sich im Netz konstituierenden Gemeinschaft zugehörig zu fühlen, heißt heute im Zeitalter des Digitalen oft: die Verbreitung der auf den Plattformen mitgeteilten Botschaften wie „Ich tue was gegen Unterdrückung", „Ich kämpfe gegen die Ungleichbehandlung", „Ich bin aktiv gegen XY", „Ich war dabei" zu forcieren. Mit entsprechend geposteten Protestbildern gilt dies sodann als Ausweis der Beschäftigung, als Nachweis der Gruppenzugehörigkeit und letztlich der Konstituierung eines Gemeinschaftsgefühls über Emotionen. Wer auf den Social-Media-Kanälen nicht aktiv ist, läuft Gefahr, ausgeschlossen zu werden. Groebner macht auf diesen Zusammenhang aufmerksam: „Identität ist nämlich auch jener Begriff, mit dem man die jeweils eigene Besonderheit des Sprechers in der ersten Person installieren kann. Deswegen ist Identität kein Begriff, sondern ein Beschäftigungsausweis."[9] Ähnlich argumentiert Reder, er fasst Protest als „performative[n] Vollzug der Meinungsäußerung in seiner körperlichen Verfasstheit"[10] auf. Diese Artikulation der Meinung kann vor Ort präsentiert werden, aber auch in medial inszenierter Form. Oft wird eine solche hybride Herangehensweise gewählt. So soll das Protest-Handeln zugleich auch Erzählen sein: indem jemand für oder gegen etwas handelnd auf die Straße geht und es anschließend postet – oder umgekehrt sich online engagiert und infolgedessen vor Ort protestiert – konstituiert sich nicht nur Identität, sondern verfestigt sich auch die Narration.

Narrative als Movens des Protests

Das Protest-Narrativ bildet als sinnstiftende Erzählung einen Motor der Mobilisierung. Mit der Verbreitung der Protestanliegen über die sozialen Medien geht es in der Gruppe oder im Kollektiv darum, „Menschen zu bestimmten Protestveranstaltungen zu lenken, den Beteiligten Handlungsvorschläge und -anweisungen zu geben und ein emotionales Narrativ zu konstruieren, das ihr Zusammenkommen im öffentlichen Raum stützt".[11] Das *Monieren*, ein Beweggrund des Protestierens, bedeutet von seinem lateinischen Wortursprung her neben *bemängeln* auch *erzählen*. Diese Erzählung, gewissermaßen das Movens des Protestierens, kann – und muss im Sinne des Narrativs – durch Leitfiguren immer wieder kommunikativ in Erinnerung und auf den Social-Media-Plattformen in Stellung gebracht werden.[12] Greta Thunberg als Pionierin der *Fridays For Future* beispielsweise bedient das Narrativ des menschengemachten Klimawandels und der damit einhergehenden Forderungen bei jeder Gelegenheit. Rucht macht darauf aufmerksam, dass sich die Narrative in dis-

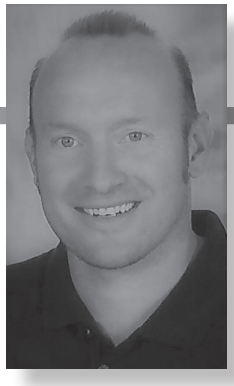
kursiver, zum Beispiel auch protestierender „Auseinandersetzung mit Bezugsgruppen“[13] bewähren müssen. So ist es zu erklären, dass die schwedische Klimaaktivistin in der UNO, beim Weltwirtschaftsgipfel oder bei Autobauern auftritt. Dass sie sich mit Bezugsgruppen auseinandersetzt, die innerhalb des Narrativs kritisch gesehen werden, gehört zur Protestgeschichte. Schließlich ergibt sich das Fortführen des Narrativs „aus dem Wechselspiel von Selbst- und Fremdbildern, die sich im Verlauf anhaltender Interaktionen […] stabilisieren.“[14] Vor allem in den nachbetrachtenden Posts und Debatten zeigt sich in den sozialen Netzwerken einmal mehr, wie solche Narrative performativ hervorgebracht werden[15] und mit Gegennarrativen diskursiv aufeinandertreffen. Wird das Narrativ dabei jedoch absolut gesetzt, was in den Echokammern der sozialen Medien nicht selten mit algorithmischem Zutun geschieht, ergibt sich die Gefahr von Ideologien und möglicherweise aggressiven, gewaltbereiten Protestgruppen. Eine wichtige Rolle bei der Narration spielt auch der bereits erwähnte, in Szene gesetzte Körper im Rahmen der Bildästhetik: „Die Affizierung des (zum Bild gewordenen) Körpers wird zur Botschaft und soll sich übertragen.“[16] Vor allem eben auf die Gemeinschaft(sbildung) im Rahmen der Narration: mit diesem Zugehörigkeitsgefühl, dem auch über eine Bildästhetik verstärkten *sense of belonging* (Ralf Dahrendorf), verfestigt sich das Narrativ.

Wider eine Umdeutung von *Engagement* und *Partizipation*

Das Design der Social-Media-Plattformen, ihre Funktionen (*Buttons*), ihre Gesetze der Aufmerksamkeitsökonomie und das damit verbundene Profitstreben bergen die Gefahr, genuin politische Begriffe wie *Engagement* und *Partizipation* umzudeuten. Auch aus der oben skizzierten sozialethischen Sicht gilt es, z. B. im Rahmen der politischen Bildung auf diese Umdeutungen und die Implikationen aufmerksam zu machen. Im Sinne der Profit- und Aufmerksamkeitsökonomie von Social Media ist *Engagement* technisch verkürzt die Logik von Tweet und Retweet, von Post und Like – also von Aktion und Reaktion. Mit anderen Worten: *Engagement* ist die von den Plattformbetreibern zu erreichende „erhöhte Wahrscheinlichkeit, dass ein bestimmter Nutzer oder eine Nutzerin auf einen bestimmten Reiz reagiert.“[17] Mit diesem behavioristischen Prinzip und den Wahrscheinlichkeiten rund um *Big Data* ergeben sich Online-Profile und letztlich Profite. Durch die algorithmisch erfasste sowie regulierte Form von *Engagement* bleiben die für das Politische wesentlichen Aushandlungsprozesse, Orientierung, „die Frage nach Bedeutung, die vielschichtigen Formen des Einordnens und des Bewertens“[18] auf der Strecke. Ein reiner *Clicktivism* oder *Armchair-Activism*, der die kybernetischen Feedback-Schleifen bedient, hält höchstens die Kommunikation und so die Diskurs-Ordnung am Laufen (vgl. Anm. 11). Leistert gibt dies für den damit korrespondierenden Begriff der *Partizipation* zu bedenken: die von den Online-Plattformen ermöglichten Partizipationsmöglichkeiten seien „genealogisch nicht mit politischer Partizipation verwandt“.[19] Ähnlich wie Stalder konstatiert Leistert mit Blick auf die soziotechnischen Folgen: „Partizipation in den Sozialen Medien ist somit ein prozessiertes und algorithmisches Relationieren“.[20] Durch die Sozialen Medien wird suggeriert, dass es unter dem Aspekt der „Vernetzung“ zahlreiche Möglichkeiten der Partizipation gibt. Doch tatsächlich entpuppen sich viele dieser vermeintlichen Partizipationsversprechen im virtuellen Raum als Engführung im Vergleich zu genuin politischen Mitwirkungsaktionen in einer Demokratie.[21] In Analogie dazu kann es durch die Monopolstellung und Gestaltungsmacht der Internetkonzerne dazu kommen, dass die Gesellschaft insgesamt „in der Sprache der Informationstechnik, mit Begriffen wie Programm, Switches, Protokollen, Betriebssystem“[22] beschrieben wird. Auch hier finden Verkürzungen statt, die auf ein bestimmtes technologisch geprägtes Menschenbild (*homo digitalis*) zurückgehen.

Depolitisierung durch die sozialen Medien?

Letztlich bleibt festzuhalten: trotz aller virtueller Partizipations- und Protestmöglichkeiten kann der demokratische „Kampf um die Neugestaltung der Materialität des Raumes“[23] im Sinne der griechischen *Polis* im Internet schwerlich geführt werden. Er wäre jedoch immens wichtig als elementarer Aushandlungsprozess und diskursive Vergewisserung im Demokratischen, geht man doch davon aus, dass der Kern des Protestgeschehens aus der gemeinschaftlichen diskursiven Aneignung eines Raumes besteht. *Hate-Speech*, *Shitstorms* und viele andere digitale Phänomene der Debattenpolarisierungen zeugen davon, dass die Gestaltung des Diskursraumes *Netz* im Sinne eines öffentlichen Forums (*agora*) nachrangig ist. Auf den Social-Media-Plattformen geht es stattdessen verstärkt um die Protestinszenierung über Bilder und eine Aufmerksamkeitsökonomie. Hierbei sind Infrastruktur und Architektur der Netzwerke weitgehend festgelegt und vorstrukturiert, so dass das „Internet und die sozialen Medien keine virtuelle Agora bieten“[24] können. Zu Ende gedacht und auf die Spitze getrieben, heißt das auch: „Revolutionen finden leibhaftig statt.“[25] Haben also ausgerechnet die digitalen Infrastrukturen eine durch den Straßenprotest 2010/11 zurückgekehrte Politisierung in eine De-Poli-



Markus Reinisch

Markus Reinisch ist Lehrer an einer bayerischen Mittelschule. Er schreibt neben literaturdidaktischen und gesellschaftspolitischen Beiträgen kritisch zu Themen der Digitalisierung für verschiedene Zeitschriften. Vor allem die Prozesse an der Schnittstelle zwischen Bildung und Digitalisierung nimmt er in den Blick. Zuletzt sind von ihm einige Aufsätze zu Big-Data-, Algorithmen- und Kybernetik-Kritik erschienen.

tisierung umgekehrt? Einige Autoren gehen davon aus. Adrian Lobe etwa kritisiert in seinem Aufsatz *Like the dislike*, dass es die Programmtechnik durch die Abwesenheit eines *Dislike*-Buttons von Vornherein nicht zulasse, echte Widerständigkeit zu erzeugen bzw. zu zeigen. Der permanent zum „Ja" sagen algorithmisch konditionierte Nutzer erlebe eine „mechanische Depolitisierung" und ein „passives Revoltiertsein, ein ständiges Um- und Weitergedrehtwerden von Datenpaketen."[26] In dieser Zuschauer-Rolle wird es für den User schwierig, sich als kritisch reflektierendes, politisch aktives Subjekt, zum Beispiel angesichts von *Fake News* und Desinformation zu behaupten. Das schnelle, oft bedeutungsschwache Feedback auf den Social-Media-Plattformen steht den Gegenstimmen bei Protestaktionen vor Ort gegenüber. Damit adäquat umzugehen, d. h. diese Diskurselemente im Rahmen der Meinungs- und politischen Bildung in Identitätsprozesse zu integrieren, ist eine enorme Herausforderung, nicht nur für Heranwachsende. Ob dies jedoch von den Plattformen im Netz geleistet werden kann, bleibt mehr als fraglich, zumal der „Wechsel von Bedeutsamkeit zu Beliebtheit, von Komplexität zu Kurzatmigkeit, von Text zu Bild […] einer Kultur politischer Diskussion prinzipiell entgegensteht."[27] Demokratische Erziehung sowie politische Bildung kommen nicht umhin, über das Themenspektrum *Protest* gerade die dabei beteiligten Diskursräume und -effekte (wie *Echokammern*, „Hate Speech") zu beleuchten und über die unterschiedlichen Formen im Netz und auf der Straße zu sprechen. Letztlich, so gilt es dabei auch deutlich zu machen, ist der nach wie vor grassierende Populismus auch ein Auswuchs von bestimmten Verhaltensmustern und Haltungen in Diskursen, im Netz wie auf der Straße. Ob er dabei vom Virtuellen ins Physische übertragen wird oder umgekehrt, ist dabei einerlei.

Anmerkungen

1 *Vgl. dazu z. B. das Nachrichtenmagazin „TIME" in den USA, das am 26. Dezember 2011 auf der Titelseite den protestierenden Bürger zur Person des Jahres 2011 erklärte: „Person of the Year: The Protester"*

2 *Seit 2013 beispielsweise das „Institut für Protest- und Bewegungsforschung" (ipb) in Berlin oder das Publikationsorgan „Forschungsjournal soziale Bewegungen" (im Folgenden mit FJSB abgekürzt).*

3 *Hummel, Siri und Strachwitz, Rupert Graf: Zivilgesellschaft und gesellschaftlicher Zusammenhalt. In: Aus Politik und Zeitgeschichte (APuZ) 13-15/2021, S. 35 – 41, S. 35*

4 *Vgl. dazu den Begriff der „Echtzeit-Öffentlichkeiten", der nicht nur aus journalistischer Sicht, sondern auch mit Blick auf die Protestlogik interessant ist: Altmeppen, Dieter/Bieber, Christoph/Filipović, Alexander/Heesen, Jessica: Echtzeit-Öffentlichkeiten. Neue digitale Medienordnungen und neue Verantwortungsdimensionen. In: Communicatio Socialis 48 (4/2015), S. 382 – 396*

5 *Beuerbach, Jan: Öffentlichkeit trotz allem. In: Mühlhoff, Rainer/Slaby, Jan/Breljak, Anja (Hrsg.): Affekt – Macht – Netz. Auf dem Weg zu einer Sozialtheorie der Digitalen Gesellschaft. Bielefeld 2019, S. 291 – 314, S. 300*

6 *Schankweiler, Kerstin: Bildproteste. Widerstand im Netz. Berlin 2019, S. 25*

7 *Ebd., S. 56*

8 *Ebd., S. 49; Vgl. dazu auch Breckman, Warren: Der Raum des Politischen. Occupy und die Demokratie des Protestes. In: Zeitschrift für Ideengeschichte, H. 3/2019, S. 51 – 64, S. 63. Er spricht von der „körperliche[n] Manifestation des ausgesetzten Körpers auf der Straße" (S. 63), was an religiöse Prozessionen auf der Straße erinnert.*

9 *Groebner, Valentin: Identität. Anmerkungen zu einem politischen Schlagwort. In: Zeitschrift für Ideengeschichte, H. XII (3/2018), S. 109 – 115, S. 114*

10 *Reder, Michael: Performativität, Differenz und Kritik. Für einen neuen Begriff der (politischen) Öffentlichkeit. In: Kaelin, Lukas/Telser, Andreas/Hoppe, Ilaria (Hrsg.): Bubbles & Bodies. Neue Öffentlichkeiten zwischen sozialen Medien und Straßenprotesten. Bielefeld 2021, S. 19 – 38, S. 24. Vgl. dazu auch Simanowski, Roberto: Facebook-Gesellschaft. Berlin 2016. Er sieht den bei Facebook etwa entstehenden „Identitätswert […] weniger in seinem dokumentarischen als in seinem performativen Effekt" (S. 80).*

11 *Gerbaudo, Paolo, zit. nach Fuchs, Christian: Soziale Medien und Kritische Theorie. Tübingen 2019, S. 164*

12 *Vgl. dazu Schrape, Jan-Felix: Attention, please! Über Sichtbarkeit in der Plattformöffentlichkeit. Erschienen am 20.03.2019 auf www.soziopolis.de. (Letzter Aufruf am 10.10.2021). Er spricht hier vom „organisierte[n] Erarbeiten von kommunikativer Persistenz". Diese ist auch dafür zuständig, die Ordnung des Diskurses im virtuellen Raum aufrecht zu halten.*

13 *Rucht, Dieter: Kollektive Identität: Konzeptionelle Überlegungen zu einem Desiderat der Bewegungsforschung, in: FJBS, Jg. 8 (1/1995), S. 9 – 23, S. 13*

14 *Ebd.*

15 *Vgl. dazu erneut Simanowski (Anm. 10), der beschreibt, wie sich das Erzählen hin zum Performativen verändert und welche kulturellen Folgen dies hat: es „operiert aktionistisch und post-aktiv zugleich: Indem es die Aktionen im Moment ihres Sich-Ereignens selbst sprechen lässt, findet es nicht mehr auf der Ebene der Präsentation der Daten statt, sondern auf der Ebene ihrer Produktion." (S. 86)*

16 *Schankweiler (Anm. 6), S. 49*

17 *Stalder, Felix: Anti-Kommunikation und Wertschöpfung. In: Le Monde Diplomatique. Erschienen am 07.03.2019 in: Le monde Diplomatique (https://monde-diplomatique.de/artikel/!5571198) (Letzter Aufruf am 10.10.2021)*

18 *Ebd.*

19 *Leistert, Oliver: Der Beitrag der Social Media zur Partizipation. In: FJSB, Jg. 26 (2/2013), S. 39 – 48, S. 41 (Hervorhebung des Autors, M.R.)*

20 *Ebd.*

21 *Vgl. dazu Schmidt, Jan-Hinrik: Die sozialen Medien und das Partizipationsparadox, in: Voss, Klaus/Hurrelbrink, Peter (Hrsg.): Die digitale Öffentlichkeit. Band II. Hamburg 2015, S. 57 – 63. Er spricht gar vom „Partizipationsparadox", denn „echte Selbstbestimmung, also das eigenverantwortliche Gestalten von Strukturen und Regeln, ist bei den großen Social-Media-Plattformen nicht vorgesehen." (S. 60)*

22 *Fuchs (Anm. 11), S. 171*

23 *Breckman (Anm. 8), S. 53*

24 *Ebd., S. 64*

25 *Ebd.*

26 *Lobe, Adrian: Like the dislike. Sozialer Widerstand im digitalen System. In: Kursbuch 200/2019, hrsg. von Armin Nassehi. Hamburg 2019, S. 10 – 23, S. 18*

27 *Simanowski (Anm. 10), S. 155*

Nelli Leiditz

Herausforderungen und Wege für eine nachhaltige Digitalisierung

Seit einiger Zeit steigt die Nachfrage nach nachhaltigen Waren und Dienstleistungen. Dabei interessieren sich die Kund:innen vorrangig für die Produkte selbst bzw. die Lieferketten und weniger für die Geschäftsprozesse, welche im Hintergrund zunehmend IT-gestützt sind. Gleichzeitig ist die digitale Transformation unumgänglich und führte in den vergangenen Jahren zu einer Verdopplung der eingesetzten Informations- und Kommunikationstechnik (IKT) (vgl. Echterhoff et al. 2017, S.35).

Durch die Zunahme des Gebrauchs neuartiger Technologien wachsen weltweit die Probleme auf ökologischer, sozialer sowie ökonomischer Ebene. Dennoch bleiben die negativen Auswirkungen durch die Digitalisierung größtenteils unbeachtet, da bisher wenig Problembewusstsein durch die Nutzung von IKT in der Gesellschaft herrscht. Um einer individuellen Verantwortung gerecht zu werden, ist es aus diesem Grund in Zukunft wichtig, die digitale Transformation bzw. deren Anwendungen kritisch zu betrachten und einen nachhaltigen Umgang anzustreben.

Problemfelder der Digitalisierung

Die negativen Auswirkungen, welche durch die Digitalisierung entstehen, können unterschiedlichen Nachhaltigkeitsdimensionen zugeordnet werden (siehe Abbildung 1). Dabei ist zu betonen, dass eine trennscharfe Einordnung nicht möglich ist, da einige Problemfelder mehrere Ebenen betreffen.

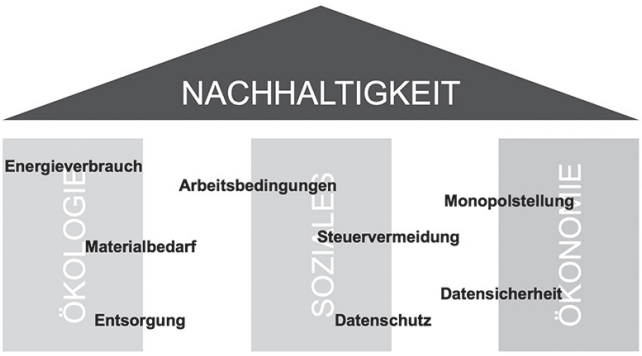


Abbildung 1: Problemfelder, den drei Säulen der Nachhaltigkeit zugeordnet (eigene Darstellung)

Ökologische Dimension

Hauptsächlich leitet der Energieverbrauch digitaler Produkte den Diskurs auf ökologischer Ebene. Deshalb wird zunehmend der Ansatz von *Green IT* angestrebt. Dies betrifft in erster Linie den Stromverbrauch von Servern, deren Einsatz durch die extrem wachsenden Datenmengen und anspruchsvolle Rechenvorgänge stetig zunimmt (vgl. Hintemann 2021, S. 2).

Des Weiteren sollte Energieeffizienz nicht nur bei der Benutzung von Endgeräten sowie der IT-Infrastruktur Beachtung finden, sondern ebenfalls bei der Herstellung. Denn besonders die Produktion der digitalen Endgeräte emittiert Unmengen an Treibhausgasen (vgl. Cook, Jardim 2017, S. 6). Zusätzlich wird bei der Herstellung elektrischer Geräte ein immenser Wasserverbrauch verzeichnet (vgl. WBGU 2019, S. 161). Dies birgt besonders auf langfristige Sicht ein hohes Konfliktpotenzial.

Außerdem entzieht die Förderung von Erzen und Mineralien sowie die Entsorgung der Endgeräte den Menschen in den betroffenen Regionen die Lebensgrundlage, da weite Landstriche kontaminiert werden (vgl. WBGU 2019, S. 161; vgl. World Economic Forum 2019, S. 11 ff.; vgl. Sühlmann-Faul, Rammler 2018a, S. 52). Erschwerend kommt hinzu, dass Konfliktmineralien und seltene Erze bislang mit keinen Materialien substituiert werden können, welche annähernd die gleichen Eigenschaften aufweisen. Dadurch wird in Zukunft eine Abhängigkeit von bestimmten Rohstoffen geschaffen, da das globale Wirtschaftssystem zunehmend auf Digitalisierung angewiesen ist und dieses durch Verknappung kollabieren könnte (vgl. Coughlan et al. 2018, S. 810).

Doch nicht nur Hardware, sondern auch Softwareprodukte haben einen direkten Einfluss auf den Rohstoffbedarf. Diverse Programme, die über einen ähnlichen Funktionsumfang verfügen, verbrauchen im Vergleich untereinander bis zu vier Mal mehr Strom und tragen so unter anderem zu einer schnelleren Abnutzung einzelner Computerkomponenten bei (vgl. WBGU 2019, S. 186; vgl. Gröger et al. 2018, S. 32 f.).

Soziale Dimension

Der eigene Gebrauch des Smartphones macht Kund:innen zu stillen Mitverantwortlichen u. a. für Menschenrechtsverletzungen sowie kriegerischen Auseinandersetzungen in Abbaugebieten (vgl. Sühlmann-Faul, Rammler 2018b, S. 28 ff.). Zudem ist bei der Förderung von Konfliktmineralien in der Demokratischen Republik Kongo sowohl innerhalb als auch außerhalb der Minen Kinderarbeit keine Seltenheit. Minderjährige arbeiten zu einem Lohn, der nicht einmal den Lebensunterhalt deckt (vgl. Amnesty International 2016, S. 28 ff.).

Auch bei Zulieferern der großen Hardwarehersteller herrschen zumeist menschenunwürdige Arbeitsbedingungen. Es werden nicht nur Vorgaben zur Arbeitssicherheit vernachlässigt, sondern ebenfalls die Arbeiter:innen vorsätzlich gesundheitsgefährdenden Stoffen ausgesetzt (vgl. Sühlmann-Faul, Rammler 2018a, S. 60). Das Produktlebensende elektronischer Geräte führt während der Entsorgung im informellen Sektor zusätzlich zu ökologischen und sozialen Problemen. Die Arbeiter:innen in Entwicklungs- und Schwellenländern – unter ihnen etwa ein Drittel Frauen und Kinder – zerlegen auf den Deponien den importierten Elektroschrott aus Industriestaaten. Dabei sind sie und alle Menschen in der Nähe der Deponien schutzlos den Gefahren des elektronischen Mülls ausgesetzt (vgl. Forti et al. 2020, S. 64; vgl. World Economic Forum 2019, S. 18).

Eine hohe Profitmaximierung auf Kosten von Menschenleben und Umwelt sowie eine zusätzliche institutionelle Steuervermei-

dung machen IT-Konzerne zu einem Risikofaktor für die Gesellschaft. Dies ist u. a. problematisch, da nicht nur die finanzielle Macht steigt, sondern andererseits Investitionskosten für die von den IT-Firmen genutzte Infrastruktur auf die Steuerzahler:innen verlagert wird (vgl. Lange, Santarius 2018, S. 131).

Zudem gerät die Demokratie in Gefahr, weil IT-Giganten ihre Machtposition verfestigen und mithilfe von gesammelten sowie verknüpften Datensätzen in die Privatsphäre der Nutzer:innen eingreifen (vgl. WBGU 2019, S. 154; 332 f.). Diese Informationen sind u. U. auch für staatliche Instanzen von großem Interesse (vgl. Bager 2019, S. 65).

Ökonomische Dimension

Der Missbrauch von personenbezogenen Daten sowie auch das Geschäftsmodell der IT-Unternehmen führt zu negativen Auswirkungen hinsichtlich der Wirtschaftlichkeit. Da einige wenige Anbieter einen vorteilhafteren Zugang zu Daten haben, manipulieren und dominieren diese den Markt und schließen Wettbewerber aus. Die *Big Player* sind mittlerweile finanziell so gut aufgestellt, dass sie ihre Mitstreiter problemlos übernehmen könnten (vgl. WBGU 2019, S. 396; vgl. Lange, Santarius 2018, S. 118). Außerdem verhindern anwendungsspezifische Anpassungen wie der *Lock-in-Effekt*[1] die Kompatibilität von Hardware, Software sowie Dienstleistungen und steigern so die Abhängigkeit zu bestimmten Anbietern (vgl. Hilty 2018, S. 74 f.). Diese Faktoren ermöglichen eine Monopolstellung der führenden Konzerne, was weitreichende Folgen für die Gesellschaft und Wirtschaft hat.

Mit steigendem Trend der Digitalisierung nehmen auch Hackerangriffe zu. Um den Datendiebstahl von personenbezogenen und unternehmensspezifischen Informationen zu verhindern, muss die Wahrung der Datensicherheit an oberster Stelle stehen. Dafür muss die eigene IT-Architektur so sicher wie möglich gestaltet sein. Denn Cyber-Kriminalität kann im schlimmsten Fall nicht nur zu hohen wirtschaftlichen Verlusten führen, sondern ebenfalls das Vertrauen kosten (vgl. Pohlmann 2018, S. 196 f.).

Maßnahmen zur Dezimierung negativer Auswirkungen

Nutzer:innen sollten im Umgang mit neuen Technologien einzelne Lebenszyklen betrachten. Jeder Produktlebensphase liegen verschiedene Möglichkeiten für mehr Nachhaltigkeit zugrunde.

Beschaffung

In erster Linie muss beim Kauf jeder einzelnen Hardware überlegt werden, ob die Anschaffung tatsächlich nötig ist. Denn jede zusätzliche Einheit hat Auswirkungen auf die Material- und Energieeffizienz. Dabei ist auch entscheidend, welche Art von Endgerät letztendlich gewählt wird. Aus diesem Grund muss dringend eine vorherige Abwägung inkl. Bedarfsplanung erfolgen.

Sollte der Kauf von Neuware unvermeidbar sein, liefern Gütesiegel und Standards einen orientierenden Überblick bei der Auswahl ethisch vertretbaren Equipments. Hierbei deckt das unabhängige Siegel *TCO Certified* im Vergleich zu anderen Siegeln zusätzlich auch Kriterien in Bezug auf Arbeits- und Sozialstandards ab (vgl. Naumann et al. 2021, S. 28 f.).

Den größten nachhaltigen Effekt hat jedoch die Verlängerung des Hardwareeinsatzes. Deshalb sollte vorab immer geprüft werden, ob bereits vorhandene Endgeräte weiterbenutzt werden können. Dafür bietet sich unter Umständen auch eine Auf- oder Umrüstung der Hardware an. Ebenfalls sollten diesbezüglich beim Kauf Geräte bevorzugt werden, welche robust und reparierfähig bzw. modular erweiterbar sind (vgl. Lübberstedt 2016, S. 32). Aus diesem Grund sollte vorrangig auch wiederaufbereitete Hardware bezogen werden. Denn durch den Erwerb der sogenannten *Refurbished*-Geräte werden die negativen Auswirkungen in allen Nachhaltigkeitsdimensionen reduziert (vgl. Sühlmann-Faul, Rammler 2018a, S. 57).

Gut gefüllter Container am „Wertstoffhof", Foto: dokumol

Auch bei der Beschaffung von Software gilt es Applikationen zu wählen, die keinen unnötig hohen Energiebedarf aufweisen und nicht mit einer beschleunigten Abnutzung bzw. einem schnelleren Hardwareersatz einhergehen. Dabei hat Open-Source-Software im Vergleich zu proprietärer Software den Vorteil, dass u. a. weniger Ressourcen in Anspruch genommen werden und die Unabhängigkeit in vielerlei Hinsicht gewahrt werden kann (vgl. Gröger 2019, S. 10; vgl. Lübberstedt 2016, S. 29).

Nutzung

Es besteht großer Konsens darin, dass IKT-Geräte effizienter werden müssen, um in Zukunft dem steigenden Energiebedarf entgegenzusteuern. In Kombination mit erneuerbaren Energien werden die negativen ökologischen Auswirkungen überdies minimiert (vgl. Lange, Santarius 2018, S. 33 ff.).

Wichtig ist zudem die Reduktion des Datenflusses im Server, welcher nicht nur den Hardwarebedarf, sondern die Rechenleistung und damit auch den Energiebedarf mindert. Besonders Server haben einen hohen Energieverbrauch, weshalb der Einsatz von Rechnern bzw. die Auswahl von Dienstleistern mit Bedacht erfolgen sollte. Ein hoher Nutzungsgrad und eine hohe Auslastung können die Effizienz verbessern. Für eine Effizienzsteige-

rung sollten die Server einer Virtualisierung unterzogen werden und es muss die Möglichkeit bestehen, diese aufzurüsten, falls die Rechenleistung zukünftig nicht mehr ausreicht. Denn auch überdimensionierte Server mindern die Energieeffizienz, wenn diese nicht ausgelastet sind (vgl. Lübberstedt 2016, S. 20 ff.).

Des Weiteren sollte die Nutzung von Cloud-Diensten näher betrachtet werden, da sie heutzutage in vielen Bereichen ein fester Bestandteil sind. Cloud-Lösungen, die meistens in Rechenzentren betrieben werden, weisen durch einen hohen Auslastungsgrad eine gesteigerte Effizienz auf. Doch andererseits kann kritisch hinterfragt werden, ob die Nutzung von Clouds den eigenen CO_2-Fußabdruck verfälscht, da der Ausstoß von Treibhausgasen ausgelagert wird und dadurch die Erfassung dieser Emissionen intransparent erscheint. Zusätzlich basieren datenschutzrechtliche Aspekte in Clouds nicht immer auf Privatsphäre.

Hinsichtlich dieser Kritikpunkte könnten Private Clouds[2] einen Mehrwert bei der Errichtung einer verlässlichen IT-Infrastruktur schaffen. Im Zuge dessen haben die Anwender:innen die volle Kontrolle über die Serverstrukturen in der Cloud und den Energieverbrauch. Nutzer:innen sollten außerdem auf einen vertrauensvollen Serverstandort innerhalb der Europäischen Union achten und sensible Daten im besten Fall verschlüsseln (vgl. Scherschel 2020). Die großen etablierten Anbieter weisen hohe Sicherheitsrisiken auf und gelten daher weitestgehend als nicht vertrauensvoll (vgl. Khan et al. 2018, S. 2).

Die datenschutzrechtliche Problematik sollte auch bei der Verwendung von Messenger- und E-Mail-Providern sowie von Browsern und Suchmaschinen miteinbezogen werden. Verschiedene Anbieter werben mit datenschutzkonformen Diensten, die die negativen Auswirkungen auf der sozialen als auch z. T. ökologischen Ebene minimieren (vgl. Lange, Santarius 2018, S.186; vgl. Sühlmann-Faul, Rammler 2018a, S.140 f.). Es sind genug Alternativen vorhanden, sie müssen nur angewendet werden.

Produktlebensende

Bisher kommt die Kreislaufwirtschaft vielfältig in anderen Bereichen zum Einsatz. Auch IT kann dieser Entwicklung gerecht werden und so die negativen Auswirkungen bei der Herstellung sowie der Entsorgung von Endgeräten vermeiden. Bei Hardware besteht bspw. die Möglichkeit des Konzepts *Device as a Service*. Aus Sicht der Endverbraucher:innen hat der kreislaufwirtschaftliche Ansatz den Vorteil, dass die Geräte auf dem neuesten Stand sind und lediglich die Leistung, jedoch nicht direkt die physischen Güter gekauft werden. Auch haben Unternehmen wie Dell und Fairphone bereits ihr Geschäftsmodell dieser Entwicklung angepasst. Hersteller sind dadurch umso mehr bestrebt, den Erhalt der Technik so lange wie möglich zu gewährleisten und der geplanten Obsoleszenz entgegenzuwirken (vgl. World Economic Forum 2019, S. 17).

Wie schon bereits bei den Beschaffungskriterien erwähnt, sollte die Verlängerung der Lebensdauer von Hardware die oberste Prämisse sein und konsequent umgesetzt werden. Dabei sollte hauptsächlich auf Modularität und eine erleichterte Reparierfähigkeit geachtet werden, um so die verwendeten Rohstoffe in den Geräten zu erhalten. Aus diesem Grund ist die Schaffung eines erhöhten Bewusstseins zum verantwortungsvollen Umgang inkl. einer effizienten Ressourcenrückgewinnung bei der anschließenden Entsorgung essenziell. Dabei ist es umso wichtiger, dass sich die Gesellschaft dafür einsetzt, dass die Akteur:innen innerhalb der IKT-Branche die Verantwortung für die Entsorgung übernehmen. So können negative Auswirkungen in Ländern reduziert werden, wo der Elektroschrott entsorgt wird (vgl. Forti et al. 2020, S. 53).

Fazit

Nutzer:innen tragen die Verantwortung, ein Problembewusstsein im Umgang mit IKT-Produkten zu entwickeln. Ein umsichtiger Konsum schützt nicht nur die Umwelt, sondern auch die Menschen, die in der IKT-Industrie beschäftigt sind. Zudem sollten Verbraucher:innen beim Gebrauch von Diensten und Anwendungen für den Schutz der Privatsphäre sensibilisiert und diesbezüglich aktiv werden. Sinkende Ausgaben für Investitionen und laufende Kosten (wie z. B. der Stromverbrauch) sind ebenfalls ein schlagkräftiges Argument für eine nachhaltige IT. Eine Checkliste fasst die wichtigsten Maßnahmen prägnant zusammen:

Checkliste

- Weniger ist mehr: seltener neue Endgeräte (Laptops & Smartphones) erwerben. Alte Geräte so lange wie möglich durch Reparatur erhalten. Anmietung in Form von DaaS erwägen.
- Vor dem Kauf auf Siegel und Zertifizierungen zu Herstellungsbedingungen und Energieeffizienz achten. Refurbished-Geräte bei der Kaufentscheidung mitberücksichtigen.
- Geräte mit Strom aus erneuerbaren Energien betreiben.
- Open-Source-Software in die Entscheidungsgrundlage einbeziehen, da meistens geringerer Rechenaufwand bei gleichem Funktionsumfang.
- Weniger Daten erzeugen und Datenfluss reduzieren.
- Cloud-Dienste anhand des Standorts und der Energieeffizienz auswählen.
- Internetdienste und -Anwendungen anhand datenschutzrechtlicher Aspekte auswählen, um umstrittene Datenverarbeitungen zu verhindern.
- Alt-Geräte achtsam entsorgen oder an gemeinnützige Organisationen spenden.
- Durch politisches Engagement mehr Druck auf die verantwortlichen Akteur:innen erzeugen.
- Innerhalb des persönlichen Umfelds die Probleme inklusive Lösungsansätze diskutieren, damit aus der Gesellschaft heraus ein Wandel stattfindet.

Referenzen

Amnesty International Hg. (2016) „This is what we die for": Human Rights Abuses in the Democratic Republic of the Congo power the global trade in Cobalt. Online verfügbar unter https://www.amnesty.org/en/wp-content/uploads/2021/05/AFR6231832016ENGLISH.pdf, zuletzt geprüft am 03.09.2021.

Bager J (2019) Universalfahnder. Sechs Allzweck-Suchmaschinen im Vergleich mit Google. In: c´t (6), S. 60–65.

Cook G, Jardim E (2017) Guide to Greener Electronics. Hrsg. v. Nancy Bach. Greenpeace Inc. Washington. Online verfügbar unter https://www.greenpeace.de/sites/www.greenpeace.de/files/publications/20171016-greenpeace-guide-greener-electronics-englisch.pdf, zuletzt geprüft am 03.09.2021.

Coughlan D, Fitzpatrick C, McMahon M (2018) Repurposing end of life notebook computers from consumer WEEE as thin client computers – A hybrid end of life strategy for the Circular Economy in electronics. In: Journal of Cleaner Production 192, S. 809–820. DOI: 10.1016/j.jclepro.2018.05.029.

Echterhoff B, Gausemeier J, Koldewey C, Mittag T, Schneider M, Seif H (2017) Geschäftsmodelle für die Industrie 4.0. In: Kraft P und Jung HH (Hg.) Digital vernetzt. Transformation der Wertschöpfung. Szenarien, Optionen und Erfolgsmodelle für smarte Geschäftsmodelle, Produkte und Services. München: Carl Hanser Verlag, S. 35–56.

Forti V, Baldé CP, Kuehr R, Bel G (2020) The Global E-waste Monitor 2020. Quantities, flows, and the circular economy potential. Online verfügbar unter https://www.itu.int/en/ITU-D/Environment/Documents/Toolbox/GEM_2020_def.pdf, zuletzt geprüft am 03.09.2021.

Gröger J, Köhler A, Naumann S, Filler A, Guldner A, Kern E et al. (2018) Entwicklung und Anwendung von Bewertungsgrundlagen für ressourceneffiziente Software unter Berücksichtigung bestehender Methodik. Hrsg. v. Umweltbundesamt. Dessau-Roßlau. Online verfügbar unter https://www.umweltbundesamt.de/sites/default/files/medien/1410/publikationen/2018-12-12_texte_105-2018_ressourceneffiziente-software_0.pdf, zuletzt geprüft am 03.09.2021.

Gröger J (2019) Leitfaden zur umweltfreundlichen öffentlichen Beschaffung von Software. Hrsg. v. Umweltbundesamt. Dessau-Roßlau. Online verfügbar unter https://www.umweltbundesamt.de/sites/default/files/medien/1410/publikationen/2020-01-21_texte_62-2019_leitfaden_beschaffung_umweltfreundliche_software_korr.pdf, zuletzt geprüft am 03.09.2021.

Hilty LM (2018) Internal Error: Systemdenken fehlt. Green IT im Kontext der Digitalisierung. In: oekom e. V. Hg. Smartopia. Geht Digitalisierung auch nachhaltig? München: Oekom Verlag (Politische Ökologie 155, 36. Jahrgang), S. 71–76.

Hintemann R (2021) Rechenzentren 2020. Energiebedarf der Rechenzentren steigt trotz Corona weiter an. Hrsg. v. Borderstep Institut. Online verfügbar unter https://www.borderstep.de/wp-content/uploads/2021/03/Borderstep_Rechenzentren2020_20210301_final.pdf, zuletzt geprüft am 03.09.2021.

Khan I, Rehman H, Al-khatib MHF, Anwar Z, Alam M (2018) A thin client friendly trusted execution framework for infrastructure-as-a-service clouds 89, S. 239–248. DOI: 10.1016/j.future.2018.06.038.

Lange S, Santarius T (2018) Smarte grüne Welt? Digitalisierung zwischen Überwachung, Konsum und Nachhaltigkeit. München: Oekom Verlag.

Lübberstedt N (2016) Nachhaltige IT-Infrastruktur. Leitfaden zur Umsetzung in KMU. 2. Aufl. Hrsg. v. kaneo GmbH – green IT solutions und Unternehmensgrün e. V. Online verfügbar unter https://www.kaneo-gmbh.de/wp-content/uploads/2017/02/Leitfaden-nachhaltige-IT_kaneo-GmbH_2017-02-17.pdf, zuletzt geprüft am 03.09.2021.

Naumann S, Kern E, Guldner A, Gröger J (2021) Umweltzeichen Blauer Engel für ressourcen- und energieeffiziente Softwareprodukte. Hrsg. v. Umweltbundesamt. Dessau-Roßlau. Online verfügbar unter https://www.umweltbundesamt.de/sites/default/files/medien/479/publikationen/texte_119-2021_umweltzeichen_blauer_engel_fuer_ressourcenund_energieeffiziente_softwareprodukte.pdf, zuletzt geprüft am 03.09.2021.

Pohlmann N (2018) Ohne IT-Sicherheit gelingt keine nachhaltige Digitalisierung. In: Bär C, Grädler T und Mayr R Hg. (2018) Digitalisierung im Spannungsfeld von Politik, Wirtschaft, Wissenschaft und Recht. 2. Band: Wissenschaft und Recht. Berlin/Heidelberg: Springer Gabler, S. 195–212.

Scherschel F (2020) Privatsphäre trotz Cloud. Privacy-Checkliste Cloud-Speicher. In: c´t (13), S. 69.

Sühlmann-Faul F, Rammler S (2018a) Der blinde Fleck der Digitalisierung. Wie sich Nachhaltigkeit und digitale Transformation in Einklang bringen lassen. München: Oekom Verlag.

Sühlmann-Faul F, Rammler S (2018b) Moderne Sklaverei inklusive. Blinde Flecken der Digitalisierung. In: oekom e. V. (Hrsg.): Smartopia. Geht Digitalisierung auch nachhaltig? München: Oekom Verlag (Politische Ökologie 155, 36. Jahrgang), S. 28–32.

WBGU (2019) Unsere gemeinsame digitale Zukunft: WBGU Wissenschaftlicher Beirat der Bundesregierung Globale Umweltveränderungen.

World Economic Forum Hg. (2019) A New Circular Vision for Electronics: Time for a Gobal Reboot. Online verfügbar unter http://www3.weforum.org/docs/WEF_A_New_Circular_Vision_for_Electronics.pdf, zuletzt geprüft am 03.09.2021.

Anmerkungen

1 *Lock-in-Effekt: auch Pfadabhängigkeit genannt: bezeichnet Situationen, in denen eine laufende Entwicklung durch historische Entwicklungen oder Entscheidungen bestimmt wird und damit einem Pfad folgt, dessen Struktur sich im Laufe der Zeit verfestigt (WBGU 2019, S. 483)*

2 *Private Cloud: wird durch die Anwender:innen eigens eingerichtet und betrieben. Eignet sich als eine Alternative zu Public Clouds (wie Dropbox, Google Drive, AWS etc.).*

Nelli Leiditz

Nelli Leiditz hat *Nachhaltige Unternehmensführung* (M. A.) an der Hochschule für nachhaltige Entwicklung Eberswalde studiert. Im Rahmen ihrer Masterthesis hat sie Möglichkeiten für kleine und mittelständische Unternehmen aufgezeigt, wie die digitale Transformation nachhaltig gestaltet werden kann und welche Chancen sich daraus ergeben.

Erklärung der Kooperation für den Frieden zur Afghanistankonferenz am 31. Oktober 2021 in Frankfurt am Main

26. Oktober 2021 – 20 Jahre nach 9/11 und dem danach ausgerufenen „Krieg gegen den Terror" zogen sich die USA und ihre Verbündeten überhastet und planlos aus Afghanistan zurück. Der Großteil der Afghan:innen, die ausländische Truppen unterstützten oder bei westlichen Hilfswerken tätig waren, wurden zurückgelassen. Damit endete trotz medial aufgebauschter Luftbrückenbilder auch der Einsatz der Bundeswehr im Desaster.

- **Die Kooperation für den Frieden fordert die weitere Aufnahme der gefährdeten Afghan:innen und die Aufnahme gefährdeter Menschen aus Kriegsgebieten insgesamt.**

Nach den Anschlägen auf die Twin Towers und das Pentagon waren die Schuldigen schnell lokalisiert: eine Terrororganisation um Osama Bin Laden, die in den 1980-er Jahren von den USA selbst finanziert und bewaffnet worden war. Die NATO rief erstmals wegen des Angriffs auf einen Mitgliedsstaat den Bündnisfall aus. Nicht einmal einen Monat später begann die Operation *Enduring Freedom* (OEF) mit Militäreinsätzen in Afghanistan, Pakistan, Zentralasien, den Philippinen, am Horn von Afrika sowie südlich der Sahara. Wer nur den leisesten Zweifel an der offiziellen Version der Ereignisse oder der Sinnhaftigkeit der militärischen Reaktionen äußerte oder diese hinterfragte, wurde schnell als Verschwörungstheoretiker:in gebrandmarkt.

- **Die Kooperation für den Frieden fordert, Verbrechen, auch Kriegsverbrechen, aufzuklären und vor den internationalen Strafgerichtshof bringen.**

Am 16. November 2001 beschloss der Bundestag den ersten Kriegseinsatz von Bodentruppen und Marineeinheiten seit Ende des 2. Weltkrieges. Unter den insgesamt 3900 Soldat:innen befanden sich bald auch 100 Angehörige des Kommandos Spezialkräfte, die die US-Truppen direkt in Afghanistan unterstützten. Die OEF wurde bis 2014 jährlich verlängert. Parallel dazu wurde die NATO-geführte ISAF-Mission ins Leben gerufen, die vorgeblich der Sicherung des Wiederaufbaus in Afghanistan dienen sollte. Real ging es eher um „die Verteidigung der Sicherheit Deutschlands am Hindukusch" (Struck, 2002) sowie wirtschaftliche und geostrategische Interessen. Die Bundeswehr beteiligte sich bis 2014 mit bis zu 5350 Soldat:innen an ISAF, insgesamt verloren 59 ihr Leben. Danach wurde die Ausbildungsmission *Resolute Support* ins Leben gerufen, für die die Bundeswehr bis zu 850 Soldaten stellte. Keine der Missionen erfüllte ihre vermeintlichen Aufgaben: der Terrorismus wurde nicht besiegt, bei Wiederaufbau, Demokratieentwicklung oder Frauenrechten wurde wenig erreicht, die Korruption blühte wie der Drogenhandel weiter, die Waffen für die afghanische Armee landeten bei den Taliban.

- **Die Kooperation für den Frieden fordert, Auslandseinsätze der Bundeswehr zu beenden, Rüstungsexporte zu stoppen, Abrüstung für Entwicklung und den Rückbau der Bundeswehr bis hin zur völligen Abschaffung.**

Die Interessen der Entscheider:innen in USA, NATO, EU oder Deutschland wurden dagegen bedient: die Kriege in Afghanistan und später im Irak, in Somalia oder Libyen marginalisierten die UN zunehmend und wurden mehr und mehr zu selbstmandatierten US-, NATO- und EU- Einsätzen. Die Region wurde dauerhaft destabilisiert, zivile Hilfsorganisationen zum Teil zum schmückenden Beiwerk militärischen Agierens, die internationale Gerichtsbarkeit für westliche Kombattant:innen ausgehebelt. U. a. wurde Oberst Klein trotz schwerer Verstöße gegen deutsches und internationales Recht sowie Bundeswehr-, ISAF- und NATO-Vorschriften für das Massaker von Kundus nicht zur Verantwortung gezogen. Im Gegenteil: Klein wurde zum Brigadegeneral befördert und ist heute für Personalmanagement und Ausbildung zuständig. Auslandseinsätze der Bundeswehr sind Normalität und finden trotz großer Ablehnung in der Bevölkerung regelmäßig überwältigende Zustimmung im Bundestag. Der Umbau der Bundeswehr hin zur Interventionsarmee ist weit fortgeschritten, die Ausgaben für Militär und Rüstung haben sich seit 2001 verdoppelt. Immer mehr Staaten weltweit setzen bewaffnete Drohnen ein, Tausende Zivilist:innen, darunter viele Kinder, wurden nicht nur in Afghanistan durch Drohnenangriffe getötet. Auch die Bundeswehr will trotz Bedenken und Protesten bewaffnete Drohnen zur Kriegsführung nutzen.

- **Die Kooperation für den Frieden fordert, keine bewaffneten Drohnen für die Bundeswehr anzuschaffen.**

Die fatale Logik militärischen Handelns ist ein weiteres Mal gescheitert. Auch mit noch mehr Soldat:innen, Waffen und Geld wären weder der Terrorismus besiegt noch der Krieg in Afghanistan zu gewinnen gewesen. Der mit unglaublicher Ignoranz nur drei Tage nach dem Abzug von den EU- Außen- und Verteidigungsministern vollmundig verkündete Aufbau einer EU-Armee wird nichts ändern. Die zunehmenden weltweiten Konflikte lassen sich nur zivil transformieren, die im letzten Jahr sinnlos für Militär aufgewendeten unvorstellbaren 1.981 Milliarden US-Dollar werden dringend für den Kampf gegen Armut, Hunger, Krankheiten und die Folgen der Klimakrise benötigt.

- **Die Kooperation für den Frieden fordert Hilfe für die afghanische Bevölkerung durch zivile und UN-Organisationen, um eine humanitäre Katastrophe zu verhindern.**

- **Die Kooperation für den Frieden fordert, People-to-people-Beziehungen zur Zivilbevölkerung im Kriegsgebiet auf- und auszubauen, kulturellen, sportlichen, beruflichen Austausch und Entwicklungszusammenarbeit zu pflegen.**

Referenz

Afghanistankonferenz am Sonntag, den 31. Oktober 2021 von 11:00-19:00 Uhr, Gewerkschaftshaus Frankfurt, Wilhelm-Leuschner-Str. 69-77, 60329 Frankfurt am Main und online, http://www.koop-frieden.de/index.php/erklaerung-der-kooperation-fuer-den-frieden-zur-afghanistankonferenz-am-311021-frankfurtm

Hans-Jörg Kreowski

Digital Humanism – How to shape digitalisation in the age of global Challenges?

Kurzer Bericht über den Workshop

Die *International Society for the Study of Information* (IS4SI) veranstaltet alle zwei Jahre einen Summit mit mehreren Konferenzen und Workshops zu einem weitgefächerten Themenspektrum mit Hunderten Teilnehmer:innen aus aller Welt. Die bisherigen Summits fanden in Wien 2015, in Göteborg 2017 und in Berkley 2019 statt. In Wien war das FIfF mit einem Cyberpeace-Workshop vertreten und in Göteborg mit einem Workshop zu Transhumanismus. In diesem Jahr hat der Summit online unter dem Obertitel **Information Study for the Benefit of Humanity: Learning from the Past and Building the New Normal** stattgefunden, geleitet vom IS4SI-Präsidenten Marcin J. Schroeder (Tohoku University, Japan). In diesem Rahmen haben Wolfgang Hofkirchner (Technische Universität Wien) und ich den *Digitalen-Humanismus-Workshop* mit Unterstützung des *Bremen Research Cluster for Dynamics in Logistics* (LogDynamics) vom 14. bis 16. September 2021 organisiert. Der Workshop war eine gemeinsame Veranstaltung des Arbeitskreises *Emergente Systeme, Information und Gesellschaft* der IS4SI, des *The Institute for a Global Sustainable Information Society* (GSIS), und der *Leibniz-Societät der Wissenschaften zu Berlin* einerseits sowie andererseits des *Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung* (FIfF). In der Einladung zu Beiträgen heißt es: „This workshop focusses on discussing the foundations of Digital Humanism as well as steps towards its implementation from the design to the use of information and communication technologies for a techno-eco-social transformation to cope with the global challenges." Beiträge waren erwünscht aus verschiedenen Disziplinen von den Sozial- und Humanwissenschaften bis zu allen Gebieten der Informatik.

Der Begriff *Digitaler Humanismus*, der einen gesellschaftlichen Prozess der Digitalisierung unter humanistischen Bedingungen benennt, wurde vom Philosophen Julian Nida-Rümelin in seinem zusammen mit Nathalie Weidenfeld verfassten und 2018 erschienenen Buch gleichen Titels geprägt. Er war auch einer der beiden Hauptvortragenden. Den zweiten Hauptvortrag hat Rainer Zimmermann zum Thema *Humanism revisited* gehalten. Beide Vorträge und das Workshopthema insgesamt wurden dann als Abschluss des ersten Tags in einer Podiumsdiskussion mit Kirsten Bock, Yagmur Denizhan, José María Díaz Nafría und Rainer Rehak reflektiert. Das FIfF war da mit Kirsten und Rainer exzellent vertreten. An den folgenden zwei Tagen wurden die 24 Vorträge zu den eingereichten Beiträgen gehalten, weitgefächert geordnet in acht Gruppen: Futures of science and technology, Education and development, Global strategies, Evolution of technology, Values for design, Design, Concepts of digitalisation und Humanism in the Anthropocene. Autor:innen, Titel und Abstracts der Beiträge findet man unter *https://gsis.at/2021/08/10/is4si-2021-digital-humanism-workshop-programmed/*. Bald werden dort auch die Video-Mitschnitte der Vorträge zu sehen sein.

Auch im Programm war das FIfF gut mit fünf Vorträgen von FIfF-Mitgliedern repräsentiert:

- **Peter Brödner:** *Resuming experiences in human-centred design of computer-assisted knowledge work processes*
- **Christiane Floyd (zusammen mit Rahel Bekele, Tesfaye Biru):** *The potential of ICT for development: Vision and implementation in TEMACC-Ethiopia*
- **Hans-Jörg Kreowski:** *A world worth living – Can Artificial Intelligence help to reach the goal?*
- **Henning Lübbecke:** *Informatics and society in German computer sciences bachelor courses*
- **Christian Stary:** *Does system-of-systems thinking work for self-governance of digitally transforming systems*

Außerdem werden im Nachgang zum Summit auch noch drei- bis fünfseitige Kurzfassungen der Beiträge gesammelt und in den Proceedings von MDPI publiziert. Darüber hinaus sind alle Autor:innen eingeladen, Langfassungen bei der Zeitschrift New Explorations: Studies in Culture and Communication einzureichen, die inspiriert ist durch die Zeitschrift Explorations: Studies in Culture and Communication von Edmund Carpenter und Marshall McLuhan von 1953 bis 1972.

Der Workshop war geprägt von einer bemerkenswerten inter- und transdisziplinären Breite. Die Autor:innen kommen aus 15 Ländern auf fünf Kontinenten. Die lebhaften Diskussionen legen nahe, das Thema weiterzuführen und zu vertiefen.

Hans-Jörg Kreowski und Aaron Lye

Cyberpeace – für Frieden, Freiheit und eine lebenswerte Welt

Die Cyberpeace-Rubrik haben wir in der vorigen FIfF-Kommunikation 2+3/2021 gestartet, um von aktuellen Entwicklungen rund um das Thema Cyberpeace zu berichten. In dieser Ausgabe umfasst die Rubrik ausnahmsweise den ganzen Schwerpunkt. In der nächsten Ausgabe soll dann die Rubrik aber wieder für Ankündigungen, Berichte, kurze Texte und Stellungnahmen rund um das Thema Cyberpeace zur Verfügung stehen.

Alle Leser:innen sind aufgerufen, die Rubrik für eigene Beiträge zu nutzen. Sie können jederzeit an uns geschickt werden: *kreo@fiff.de* und *lye@fiff.de*.

Stefan Ullrich und Andrea Knaut

Joseph Weizenbaum: Ohne uns geht‘s nicht weiter

Der Aufruf von FIfF-Gründungsmitglied Joseph Weizenbaum hat auch 25 Jahre später nichts von seiner Aktualität verloren, im Gegenteil. Heute werden die militärischen Gerätschaften der KI, vor denen Weizenbaum unermüdlich warnte, längst eingesetzt. Verteilte Waffensysteme, die mittels Bilderkennung und autonomer Flugsteuerung ein perfektes, zielgenaueres und täterloses Töten aus der Ferne versprechen, werden bequem vom Sportsessel aus bedient. Dieses Versprechen sei jedoch eine kollektive Delusion, so der vehemente Kritiker des militärisch-industriellen Komplexes. Joseph Weizenbaum war ein Mahner, aber kein Pessimist, er appellierte ebenso unermüdlich an die Vernunft der gestaltenden Menschen, doch bitte nicht bei dem mörderischen Wahnsinn unserer Zeit mitzumachen. Dieser Text ist ein Wiederabdruck mit freundlicher Unterstützung der *Blätter für deutsche und internationale Politik* und des Fachbereichs *Informatik und Gesellschaft* der Gesellschaft für Informatik e. V.

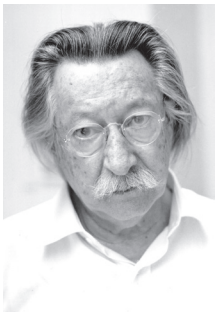


Foto: Universität Bremen

Joseph Weizenbaum

Ohne uns geht‘s nicht weiter

Künstliche Intelligenz und Verantwortung der Wissenschaftler

Joseph Weizenbaum, Professor für Informatik am M.I.T., dem Massachusetts Institute of Technology in Cambridge/USA und als Koryphäe in Sachen Künstliche Intelligenz weltbekannt, hat einen nicht alltäglichen Vortrag gehalten. Auf einer Fachtagung der Gesellschaft für Informatik (GI) in Karlsruhe – Referenten u. a. von Siemens, dem Kernforschungszentrum Karlsruhe, verschiedenen Universitäten, Hochschulen und Instituten von Arbeitgeber- und Arbeitnehmerverbänden sprachen dort vom 15. bis 17. Juli 1986 zum Tagungsthema Arbeit und Informationstechnik – verlangte Weizenbaum von den Experten den Mut, von tiefverwurzelter Neigung zu Euphemismen hinsichtlich des Endnutzens ihrer Arbeit und von geschönten Begriffen, von Verdrängungsmechanismen und „der verbreitetsten Geisteskrankheit unserer Zeit“, der Überzeugung der Einzelnen nämlich, daß sie machtlos seien, Abschied zu nehmen. „Wir sind dazu in der Lage, wir haben die Macht, den weltpolitischen Zustand konkret und radikal in eine neue, lebensfördernde Richtung zu wenden“, plädiert Weizenbaum.

Professor Weizenbaum hat seinen – in deutscher Sprache gehaltenen – Vortrag freundlicherweise für den Abdruck in den Blättern überarbeitet. Untertitel und Zwischenüberschriften stammen von der Redaktion. Herrn Klaus Theo Schröder, dem Leiter der GI-Tagung, danken wir für seine Vermittlung. – D. Red.

Wann immer ich nach Europa komme, besonders in die Bundesrepublik, staune ich über die Normalität des alltäglichen Lebens. Sicherlich weil ich doch *Outsider* bin, nur ab und zu diesen Kontinent und dieses Land besuche, sehe und spüre ich Zustände und Dinge, die Euch schon so normal erscheinen müssen wie die Autobahnen, die *Musik*, von der man überfallen wird, im Restaurant, im Fahrstuhl usw., oder sogar so *natürlich* wie Eure schönen Parks, die Fernsehantennenwälder, die von den Dächern Eurer Häuser wachsen, also so alltäglich, daß Ihr sie nicht mehr ohne weiteres wahrnehmen könnt. All das haben wir in den USA auch, und all das ist genauso unsichtbar für uns wie für Euch.

Aber trotz der immer tiefer greifenden Amerikanisierung Eures Landes und Eurer Städte bleibt doch etwas Europäisches, das nicht verdrängt oder alltäglich gemacht werden sollte. Oder irre ich mich? Ich meine Eure geographische Lage und das, was heutzutage von ihr abhängt und aus ihr folgt. Und damit meine ich z. B. Eure Grenzen mit dem anderen Deutschland, die massive Präsenz von Militär jeder Art, die Löcher in vielen Eurer Straßen, die im Ernstfall mit nuklearen Landminen ausgestattet werden sollen, die geringe Entfernung jedes Bürgers von einem Kernwaffenlager usw. Ich meine mit anderen Worten Eure rein physikalische, aber auch psychologische, unmittelbare Nähe zur letzten Katastrophe.

In einem gewissen Sinn sind wir in Amerika gar nicht weiter von der Katastrophe entfernt als Ihr hier. Nicht nur Tschernobyl ist überall, die Kriegsbedrohung ist überall, der Krieg ist jedermanns Feind! Im Falle eines Krieges, ob unbeabsichtigt von der Technologie selbst ausgelöst oder von einem sogenannten Staatsmann, der den Knopf drückt, weil er glaubt seine Pflicht tun zu müssen, werdet Ihr vielleicht zehn Minuten früher sterben als wir in der Festung Amerika. Aber wir haben keine Löcher für Landminen, die russische Panzerregimenter aufhalten sollen. Und unsere Minuteman-Raketensilos sehen wir nur ab und zu, wenn es irgend jemand gefällt, sie uns im Fernsehen zu zeigen. Wie leidenschaftlich unsere Regierung auch versucht uns zu überzeugen, daß die bösen Sowjets uns genauso unmittelbar gefährden wie Euch Europäer, z. B. aus Richtung Kuba und Nicaragua, wir glauben es nicht. (Grenada konnten wir doch noch in letzter Minute überwältigen, Dank der vielen Milliarden von Dollars, die es unserem Militär erlaubten, eine der riesigen militärischen Macht Grenadas entsprechende Stufe der Rüstung zu erreichen. Ronald Reagan, wir danken Dir!).

Vielleicht würde es mehr erstaunen, wenn der Durchschnittsamerikaner sich der Gefahr, in der wir alle stehen, tatsächlich bewußt wäre, als daß er sich so wenig darum kümmert. Die historischen Kriegserfahrungen Amerikas fördern eben eher eine

Uns kann nichts passieren-Haltung, als eine Furcht vor scheinbar weit entfernten Bedrohungen.

Mir ist auch bewußt, daß es rein emotionell für Euch – wie für Jeden – nicht möglich ist, lange in großer und unmittelbarer Lebensgefahr zu leben, ohne daß ein Mechanismus einsetzt, der diese Gefahr aus dem Bewußtsein ausschließt, sie höchstens ab und zu wieder eindringen läßt. Aber wenn eine, unter anderen Umständen gesunde, Verdrängung ein systematisch verführendes Verhalten bedingt oder ein möglicherweise rettendes Verhalten ausschließt, dann ist es an der Zeit, sie durch einen bewußten, tiefen Blick in den Abgrund zu ersetzen, um in der Schrecklichkeit selbst einen Anlaß zur Aktion, zur Rettung zu finden.

Wir haben die Macht, der Entwicklung eine neue Richtung zu geben

Diese Zeit ist für uns Informatiker gekommen, denn wir sind dazu in der Lage, wir haben die Macht, den weltpolitischen Zustand konkret und radikal in eine neue, lebensfördernde Richtung zu wenden. Um den Mut dazu zu gewinnen – denn wir sind weder Heilige noch Helden –, müssen wir eben verstehen, daß für uns selbst als Einzelne ebenso wie für die, die wir lieben, unser gegenwärtiges Verhalten viel gefährlicher, ja lebensbedrohender ist, als das, was die gesunde Einsicht in unsere Lage und die Vernunft selbst von uns jetzt verlangen.

Ich sage es ganz einfach: Es ist eine prosaische Wahrheit, daß die Waffen und Waffensysteme, die heute jeden Menschen auf der Erde mit Mord bedrohen und außerdem durch ihre Entwicklung, Herstellung und Verkauf alle Völker dieser Erde verarmen lassen, auch ohne *gezündet* (oder *benutzt* – welch ein Wort! Als ob der Gebrauch solcher Instrumente irgendeinen menschenwürdigen Nutzen haben könnte!) zu werden; die täglich unzählige Menschen, besonders Kinder, dem Scharfrichter namens Hunger übergeben, daß diese Geräte ohne die ernstliche – sogar begeisterte – Mitwirkung von Informatikern und Computerfachleuten überhaupt nicht hätten entwickelt werden können. Ohne uns geht es nicht weiter! Ohne uns kann das Wettrüsten – besonders das qualitative Wettrüsten nicht weitermarschieren.

Sagt uns diese einfache, offensichtliche, deutliche Tatsache etwas? Ich glaube schon: Erstens, daß wir *Computerexperten* – wie auch Spezialisten in anderen technischen Bereichen – an der heutigen gefährlichen Weltlage mitschuldig sind. Unter anderem sollte das uns zumindestens klar machen, daß wir, diejenigen unter uns, die ihre aktuelle und latente Macht gedankenlos dem Tod statt dem Leben widmen, wenig Recht dazu haben, die Politiker, die sogenannten Staatsmänner und -frauen, zu schelten, weil sie uns keinen Frieden bringen. Ohne uns könnten sie weder einander noch die Bevölkerung dieser Erde bedrohen. Schöne Plakate zu machen, die dann in eindrucksvollen Demonstrationen herumgetragen werden, kann eine Verdrängung der Verantwortung der Einzelnen sein, wenn die Einzelnen sich nicht darum kümmern, ob ihre tägliche Arbeit nicht zuletzt die Geräte des Massenmordes, gegen den sie gerade demonstrieren, ermöglicht.

Allmachtdrang auf der Computerbühne

An dieser Stelle denke ich besonders an die sogenannte künstliche Intelligenz (KI). Viele der technischen Aufgaben und Probleme in diesem Bereich der Informatik sind für die Phantasie und Schöpfergabe der technischen Arbeiter besonders anregend. Denen unter uns, die ihre spielerischen Baukastenphantasien noch nicht ganz sublimiert haben, oder denen, die ihren Allmachtdrang auf der Computerbühne, d. h. als Computersysteme, befriedigen, ihnen sind Ziele, z. B. aus dem Computer ein denkendes Wesen zu machen, dem Computer ein beinahe menschliches Verständnis der gesprochenen Menschensprache zu verleihen, dem Computer *Augen* zu geben usw., fast unwiderstehliche Versuchungen. Die Aufgaben sind eben äußerst hinreißend, spannend – Robert Oppenheimer nannte solche Probleme *süß* – und außerdem werden solche Forschungsaktivitäten großzügig finanziert. Die Gelder fließen allerdings – jedenfalls in Amerika – meistens aus den Kassen des Militärs.

In diesem Bereich ist es eben so irrsinnig verlockend, so verführerisch, sich einfach in den Einzelheiten, den Unterproblemen und den Unterproblemen der Unterprobleme zu verlieren, oder vielleicht besser gesagt, zu verstecken. Die eigentlichen Probleme, an denen man arbeitet und die so großzügig unterstützt werden, werden verkleidet und verwandelt, bis die Darstellungen der aktuellen Probleme bloße Märchen sind, harmlose, unschuldige, liebenswürdige Märchen.

Ein Beispiel: Ein Student schilderte mir seine voraussichtliche Doktorarbeit, indem er das folgende Bild ausmalte: Ein Kind – vielleicht sechs oder sieben Jahre alt – sitzt vor dem Bildschirm, auf dem, in voller Farbe natürlich, eine kleine Katze und ein kleiner Bär zu sehen sind. Das Kätzchen spielt mit dem Ball. Jetzt spricht das Kind den Bildschirm an: „Du, der Bär, Du mußt dich bedanken, wenn Dir etwas gegeben wird." Das System antwortet mit einer synthetischen, aber angenehmen Stimme: „Danke, ich habe verstanden." Dann wieder das Kind: „Kätzchen, gib' Deinem Freund den kleinen Ball." Sofort sehen wir am Bildschirm, wie die Katze den Ball mit einem schleierhaften Lächeln dem Bären überreicht. Dann hören wir den Bären sagen: „Vielen Dank, mein liebes Kätzchen." Also das und ähnliches soll das System, das den Kern der Doktorarbeit des Studenten bilden soll, leisten. Technisch gesehen muß das System gesprochene Aufträge verstehen – das allein ist schon gar nicht einfach –, solche Aufträge in ganz und gar nicht triviale Änderungen des eigenen Programms übersetzen und schließlich diese Modifizierungen nahtlos in das System einbauen. Durchaus nicht trivial, würde ich behaupten … und dazu noch richtig rührend.

Die Übersetzung des Märchens

Jetzt eine Übersetzung in die eigentliche Praxis: Ein Kampfflugzeugpilot wird von seinem *Pilotenassistentensystem* angesprochen: „Sir, ich sehe eine feindliche Panzerkolonne in den Koordinaten Soundso. Erbitte Befehl." Der Pilot darauf: „Wenn Du so etwas siehst, stör' mich nicht, vernichte die Scheißkerle und notier Dir die Aktion. Ende!" „Zu Befehl, Sir!", antwortet das System und die Raketen fliegen Richtung Erde los.

Dieses Pilotenassistentensystem ist eines der drei Waffensysteme, die in der sogenannten *Strategic Computing Initiative* des amerikanischen Militärs explizit, offen und ausdrücklich als Aufgaben für die *künstliche Intelligenz* beschrieben sind; Forschung und Entwurf dazu werden in den nächsten Jahren mit rund 600 Mio. Dollar vom Militär unterstützt.

Es ist jetzt nicht mein Vorhaben, über solche oder andere militärische Systeme zu schimpfen oder sie zu verdammen. (Obwohl ich zugebe, daß mir dies Spaß machen würde.) Ich will mit diesem Beispiel aus der aktuellen Praxis der künstlichen Intelligenz in Amerika die sprachliche Verhüllung und deren Wirkung, das Nachdenken zu verhindern und letztlich das Gewissen zu beruhigen, bloßlegen.

Ich weiß nicht recht, ob es gerade unsere Branche der Wissenschaft oder sogar der Unterbereich *künstliche Intelligenz* ist, der eine so außerordentliche Neigung zu Euphemismen an den Tag legt. Wir sprechen so furchtbar leicht von Computern, die sehen, erkennen, verstehen, entscheiden, beurteilen usw. können, ohne unsere eigene Oberflächlichkeit und maßlose Naivität in diesen Dingen zu erkennen. Wir betäuben unsere eigenen Fähigkeiten, die Qualitäten unserer eigenen Arbeit zu erkennen, und was viel wichtiger ist, uns den Endzweck unserer täglichen Arbeit bewußt zu machen.

… diese psychologische Entfernung ist astronomisch groß

Die psychologische Entfernung zwischen der Vorstellung des eben erwähnten Studenten, der sich einbildet, er spiele mit Kätzchen und Bären, die sich Bälle zuwerfen, und der Tatsache, daß irgendwann ein junger Mann, ihm selbst ähnlich, der auch Eltern hat und vielleicht eine Freundin, in einem von einer Rakete gezündeten Feuer verbrennt – und daß diese Rakete von einem auf seiner Forschung beruhenden Pilotenassistentensystem abgeschossen wird, diese psychologische Entfernung ist astronomisch groß. Es ist genau diese ungeheure Entfernung, die es möglich macht, erst nicht zu wissen und schließlich gar nicht mehr zu fragen, ob die Arbeit, die man leistet, vernünftig ist oder der Wirksamkeit der Mordmaschinen dient.

Man kommt nicht aus diesem Zustand heraus, ohne immer wieder zu fragen: „Was mache ich eigentlich? Auf welche Verwendung läuft meine Arbeit letztendlich hinaus?“ Und schließlich: „Bin ich zufrieden oder schäme ich mich, zu solcher Anwendung beigetragen zu haben?“

An dieser Stelle denke ich an einen berühmten amerikanischen Journalisten, der während einer terroristischen Entführung verlangte, daß die Israelis jeden Tag, an dem die Geiseln der Libanesen nicht freigelassen würden, eine bestimmte Zahl – ich glaube es waren zehn – ihrer Kriegsgefangenen auswählen und erschießen sollten. Man sollte solche Vorschläge überhaupt nicht machen. Aber wenn man schon daran denkt, sollte man sich erst fragen: „Bin ich bereit, selbst jeden Tag Männern tief in die Augen zu blicken und ihnen zu sagen ‚Du' oder ‚Du heute nicht' und den, den ich zum Tod auswähle, mit eigener Hand mit der Pistole zu erschießen, erst den Ersten, dann den Zweiten und so weiter? Und kann ich das dann am nächsten Tag wieder durchführen?“

1998 in Bremen (von links nach rechts): Klaus Brunnstein, Frieder Nake, Wolfgang Coy, Joseph Weizenbaum, Gunna Wendt, Wilfried Brauer, Hans-Jörg Kreowski, Jürgen Friedrich Foto: Universität Bremen

Die Frage: Könnte ich so etwas mit eigener Hand tun?

So sollten wir uns auch selbst fragen, wenn wir die verschönende Sprechweise abgelegt haben und ernsthaft über unsere Arbeit als Informatiker und Computerfachleute sprechen. „Du, mein Kollege von früher, Du arbeitest doch an einer Maschine, die mit 2^{15} (und noch mehr) Mikrocomputern simultan funktioniert. Mit Hilfe solcher Computer kann man ganz neue, viel wirksamere, kleinere und leichtere Wasserstoffbomben erst simulieren und dann herstellen. Stell' Dir mal vor, Du wärst 1945 Augenzeuge in Hiroshima gewesen und hättest die hautlosen Menschen sterben sehen. Willst Du das tausendmal wieder machen – mit Deiner Hand unschuldige Menschen wieder so zu Tode quälen? Wenn Du meinst, daß nur etwas so Schreckliches den Frieden erhalten kann – und Du deswegen weitermachen würdest –, dann können wir das diskutieren. Aber wenn Du Nein sagst – Du könntest so etwas nicht mit eigener Hand tun –, dann mußt Du doch mit dieser Arbeit aufhören!“ Ähnliches könnte man im Zusammenhang mit dem Versuch, den Computer das Sehen zu lehren, fragen. Denn jeder Fortschritt in dieser Sache verleiht Raketen wie Cruise und Pershing noch präzisere Zielgenauigkeit – und am Ziel wird gemordet.

Einer solchen Argumentation wird oft entgegengehalten, der Computer sei doch bloß ein Werkzeug, das für Gutes oder Böses angewendet werden könne und das an sich wertfrei und neutral sei. Konkret bedeutet diese Antwort, daß der einzelne Techniker nicht wissen könne, ob seine Arbeit schließlich guten oder bösen Zwecken dient. Deswegen könne er auch nicht für das verantwortlich gemacht werden, wozu die Ergebnisse seiner Arbeit letzten Endes angewandt werden.

Ich sehe die Verkörperung dieses Arguments täglich im Nebengebäude des Hauses, in dem sich mein Arbeitszimmer im MIT (Massachusetts Institute of Technology, d. Red.) befindet, das sogenannte Draper Laboratory. Dieses weltberühmte wissenschaftliche Labor ist fast ausschließlich der Steuerung von Raketen aller Art und der Unterseebootnavigation gewidmet. Manche der Wissenschaftler, die dort schon jahrelang ihre Arbeit tun, sagen, daß ihre Arbeit ebensogut Menschen zum Mond und wie-

der zurück gebracht habe, wie sie garantiere, daß die Raketen, die auf Moskau zielten, im Ernstfall tatsächlich Moskau träfen. Sie könnten im voraus nicht wissen, welches von diesen zwei Zielen sie bedienten. Genauso die Informatiker. Der Student, der mit seinem intelligenten Bildschirmgerät sprechen möchte, denkt tatsächlich nur an Anwendungen, die mit Kinderspielen zu tun haben. Vielleicht wird er gar nicht von der Strategic Computing Initiative des Pentagons unterstützt – vielleicht hat er nie von dieser SCI gehört. Man kann ihn doch nicht für Beziehungen zu Dingen verantwortlich machen, von denen er nichts wissen kann. Oder?

Damit kommen wir zu einem Kernpunkt der Sache: Wir wissen heute mit aller Sicherheit, daß jedes wissenschaftliche und technische Ergebnis, wenn überhaupt möglich, vom Militär aufgegriffen und zu militärischen Zwecken eingesetzt wird. Der Computer – einschließlich seiner ganzen Entwicklungsgeschichte – ist vielleicht das Parade-Beispiel. Aber wir sollten auch an alles, was mit dem Fliegen zu tun hat, oder mit der Zerbrechlichkeit des physikalischen Kerns, oder mit technischen Kommunikationsmöglichkeiten, und an so viele andere Ergebnisse des menschlichen Genius denken, um uns davon zu überzeugen, daß in der konkreten Welt, in der wir heute leben, die Beweislast jeweils eher auf der Seite ruht, die behauptet, eine bestimmte technische Entwicklung sei gegen die Gier des Militärs immun, als auf der Gegenseite.

Unter diesen Umständen können die auf technischen Gebieten Beschäftigten ihrer Verpflichtung, nach dem *Endnutzen*, der letztendlichen Verwendung ihrer Arbeitsergebnisse, zu fragen, nicht entkommen. Und wenn sie einmal wissen, zu welchen Zwecken ihre Arbeit benutzt wird, müssen sie sich entscheiden, ob sie persönlich und mit ihren eigenen Händen diesen Zwecken dienen können und wollen.

Aber das Militär ist nicht an sich ein Übel, und eine technische Entwicklung, die vom Militär übernommen wird, ist deswegen nicht unbedingt menschenfeindlich. Beim gegebenen Zustand der historischen Entwicklung der Souveränität der Nationen, also in der Irrenanstalt, in der wir jetzt leben, braucht der Staat sein Militär, so wie die Stadt ihre Feuerwehr braucht.

Eine Feuerwehr, die nebenher Brandstiftung betreibt

Niemand plädiert aber für eine Feuerwehrwache an jeder Straßenecke, und keine Stadt wünscht sich eine Feuerwehr, die in den Dörfern außerhalb der Stadt Brandstiftung als Nebengeschäft betreibt. Und doch sehen wir unsere ganze Welt täglich mehr und tiefgreifender militarisiert. Und in fast jedem Erdteil brennen „kleine" Kriege, die oft unter anderem dem Zweck dienen, die *High-Tech*-Waffen der Supermächte zu erproben. Mehr als die Hälfte aller Naturwissenschaftler und Ingenieure der Welt arbeiten mehr oder weniger direkt für militärisch unterstützte Institutionen. Das ist schlimm. Gegen dieses Übel muß Widerstand geleistet werden.

Wir müssen auch erkennen, daß nur unsere tiefverwurzelte Gewohnheit, unsere Sprache zu schönen, um unser Gewissen nicht aufzuwecken, uns überhaupt erlaubt, von Waffen und Waffensystemen zu sprechen, wo doch in Wahrheit von Atomsprengkörpern und Wasserstoffbomben die Rede ist. Das sind ja keine Waffen! Das sind Massenmordmaschinen und Massenmordmaschinensysteme, und so müssen wir sie auch nennen, klar und deutlich. Wenn man einmal erkennt und verinnerlicht, daß die sogenannte Kernwaffe nichts anderes ist als ein *Instant Auschwitz* – ein Sofortvernichtungslager –, ein Auschwitz ohne Schienen, ohne Transporte, ohne Mengele und Eichmann – aber eben doch ein Auschwitz –, kann man dann an Systemen mitarbeiten, die so etwas auf lebende Städte lenken sollen? Das, liebe Kollegen und Kolleginnen, frage ich auch. Aber Ihr müßt auch selbst solche Fragen stellen, Eure Antworten ernstlich und mit Bedacht in Euch selbst suchen, und diese Antworten in Eurem Tun zum Leben erwecken.

Die verbreitetste Geisteskrankheit unserer Zeit

Sicherlich, die am weitesten verbreitete Geisteskrankheit unserer Zeit ist die Überzeugung der Einzelnen, daß sie machtlos seien. Diese (selbsterfüllende) Delusion kommt bestimmt, als Einwand gegen meine These, an dieser Stelle ins Spiel. Ich verlange ja, daß eine ganze Berufsgruppe sich weigert, an dem selbstmörderischen Wahnsinn unseres Zeitalters weiter mitzumachen. „Das ist doch wirkungslos! Ja, wenn niemand mehr an solchen Sachen arbeiten würde … Aber das ist unmöglich. Wenn ich es nicht mache, macht es jemand anders." Und so weiter.

Erstens und auf der trivialsten Ebene, muß ich sagen, daß der Spruch „Wenn ich es nicht mache, macht es jemand anders" keine Basis des moralischen Handelns sein kann. Denn mit dieser These kann jedes Verbrechen begründet werden, z. B. „Wenn ich dem Besoffenen sein Geld nicht abnehme, nimmt es doch der nächste Kerl." Nein, das geht nicht.

Aber überhaupt nicht trivial ist die Frage: „Was bedeutet Effektivität, Wirksamkeit in diesem Kontext?" Ganz bestimmt ist es keine *entweder/oder*-Frage, keine binäre Angelegenheit. Würde die These, die ich hier ausspreche, einen Wissenschaftlerstreik auslösen, dann würde sie bestimmt als effektiv beurteilt werden. Aber ich habe andere, viel bescheidenere Maßstäbe für Effektivität im Auge.

George Orwell hat einmal geschrieben: „Die höchste Pflicht der Intellektuellen unserer Zeit ist, die einfachsten Wahrheiten in den einfachsten Worten auszusprechen." Für mich bedeutet dies zuerst, die Absurdität unserer Welt zu artikulieren, d. h. sie herauszuschreien in meinem Tun, mit meiner Stimme und mit meiner Schrift. Damit hoffe ich, Studenten, Kollegen, alle die ich irgendwie direkt ansprechen kann, wachzurütteln. Damit hoffe ich alle, die schon in ähnliche Richtungen denken und handeln, zu ermutigen und von ihnen ermutigt zu werden. Denn Mut ist, wie Angst, ansteckend! Das ist auch Erfolg, nicht wahr? Außerdem bringe ich die Themen, die ich hier vorlege, auf die Tagesordnung und trage dazu bei, eine Debatte einzuleiten und zu legitimieren. Das sind bescheidene Ziele, die erreicht werden können.

Aber letztlich spreche ich die größeren Ziele an. Nukleare Massenmordgeräte, wie auch Kernkraftwerke, aus der Welt zu schaffen. Die Welt so umzuordnen, daß Arbeitern in einem Land nie wieder eingeredet werden kann, es sei lebensnotwendig, ihre Familie mit Fleisch und Blut und Tränen anderer Menschen in anderen Ländern zu ernähren. (Das ist eben das heutige Schicksal vieler Arbeiter in vielen Ländern – nicht nur derer, die in Waffenfabriken und Labors ihr Brot verdienen, sondern auch derer

unter uns, die täglich dabei sind, die High-Tech-Waffen noch weiter zu schärfen.) Die Welt so umzuordnen, daß jeder Mensch auf dieser Erde über die materiellen Bedingungen eines menschenwürdigen Lebens verfügt. (Es wird oft gesagt; wenn wir Elektronik und Informatik richtig entwickeln, könne dieses Ziel in vielleicht 40 bis 50 Jahren erreicht werden. Aber diese Aussage ist eine Verdrängung: wir könnten heute anfangen, diese Aufgabe zu verwirklichen. Die Technologie dafür fehlt uns nicht – der politische Wille fehlt uns.)

Was heißt *unmöglich*?

Ich hörte Elie Wiesel einmal sagen: „Wir müssen glauben, das Unmögliche sei möglich." Das bedeutet, denke ich, mehrerlei: Hätten wir glauben können, daß „das Land der Dichter und Denker" – oder Menschen überhaupt – Menschenvernichtungsfabriken hervorbringen könnte, die an reiner Effizienz mit den Automobilfabriken Amerikas konkurrieren können, dann hätten wir vielleicht nicht Bergen-Belsen erleben müssen. Das Schreckliche, das unmöglich erschien, war möglich und ist zustande gekommen.

Andererseits war es vor 150 Jahren in Amerika „unmöglich", die Sklaverei abzubauen. Die gesamte Wirtschaft der amerikanischen Südstaaten hing von der Baumwolle ab und diese konnte weder gepflanzt noch geerntet werden ohne Einsatz der unbezahlten Arbeit tausender wie Tiere behandelter Menschen, aus deren Elend der weiße Master Gewinn herauspressen konnte. Aber trotzdem fiel es, zuerst wenigen Träumern in Massachusetts, dann immer mehr Realisten im damaligen Amerika ein, daß das Ummögliche möglich gemacht werden mußte: Die Sklaven mußten befreit und die Sklaverei abgebaut werden. Und es war möglich. Und es wurde Wirklichkeit.

Die unmöglichen Ziele, die ich eben darstellte, sind erreichbar. Wir müssen das glauben. Ich weiß, ich kann ihre Umsetzung in Realität nicht alleine schaffen. Aber ohne mich geht es nicht. Es geht auch nicht ohne uns. Ich habe doch kein Recht, etwas von Euch zu verlangen. Aber da Ihr, zusammen mit unseren Mitarbeitern und Mitarbeiterinnen in der weiten Welt draußen, die Macht habt, entweder die Effizienz der heutigen Mordgeräte noch höher zu schrauben und dabei den Tod meiner Kinder noch sicherer zu machen, oder den ganzen Wahnsinn zu Fall zu bringen und dabei meinen Kindern und Euch selbst eine Chance zu geben, in Würde zu leben, als Menschen, bitte ich Euch alle, nicht nur in meinem Namen, sondern sicherlich zu Gunsten vieler Menschen, die nicht hier anwesend sind, meiner Kinder zum Beispiel – ich bitte Euch: bedenkt was ihr tatsächlich bewirkt, bedenkt, in welchem Rahmen und zu welchen Zwecken Eure Arbeit angewendet wird. Dann überlegt: „Will ich diesen Zwecken mit meinen eigenen Händen dienen?"

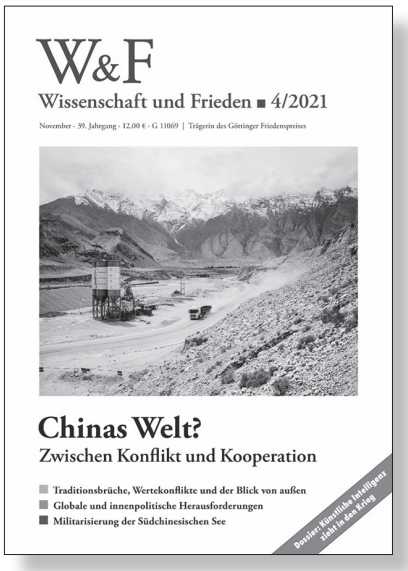
Der Beitrag erschien in: Blätter für deutsche und internationale Politik, 9/1986, S. 1037-1045. Wir danken der Redaktion für die Genehmigung zum Wiederabdruck.

Wissenschaft & Frieden 4/2021: Chinas Welt? – Zwischen Konflikt und Kooperation

Kaum eine Entwicklung verläuft aktuell so rasant wie die Formierung eines neuen *Feindbilds China*: Das Land wird als wirtschaftlicher, ideologischer und militärischer Rivale betrachtet oder auch als *systemischer Konkurrent*. In diesem aufgepeitschten Diskursklima fällt es schwer, die Lage ruhig zu analysieren. Das aktuelle Heft W&F 4/21 will helfen, dieser Analyse Raum zu bieten.

Die Autor:innen im Heft betonen die Notwendigkeit einer kritischen Betrachtung der inneren und globalpolitischen Entwicklungen Chinas, allerdings unter Wahrung eines Maßstabs der Verhältnismäßigkeit. Dadurch bietet das Heft spannende Einblicke u. a. in die Gestaltungsspielräume der Zivilgesellschaft, die aktuelle Militärpolitik des Landes oder auch zu den sozioökonomischen Konflikten rund um Klima- und Stadtpolitik. Nicht weniger erkenntnisreich sind die Beiträge zur Formierung des neuen Feindbildes im Westen und dem zögerlich-ambivalenten Umgang der EU mit China. Natürlich wirft auch „Wissenschaft und Frieden" einen frischen Blick auf das Südchinesische Meer, denn die Militarisierung des Indopazifik erreicht dieser Tage mit immer neuen Militärpakten und Abkommen neue Höhen. Gerade hier ist es bedeutsam, den schrillen Tönen eine ruhige Analyse entgegenzusetzen.

Darüber hinaus behandeln die Beiträge außerhalb des Schwerpunktes die Rolle von Gatt:innen aus dem diplomatischen Bereich auf dem Westphälischen Friedenskongress, dem Konzept und der Praxis der *Kommunalen Konfliktberatung* sowie der systemischen Herausforderung der Konfliktverschärfung durch Lebensmittelverschwendung. Ein theoretischer Beitrag zum Konzept der *slow violence* rundet die Ausgabe ab.



W&F 4/21 | November | 64 Seiten | 12 € (print) / 9 € (epub) | *wissenschaft-und-frieden.de*

Ein Blick in die Zukunft: Der Einsatz von Schwärmen in einem Tactical-UAS-Bataillon *(UAS=Unmanned Aerial System) Quelle:* Bundeswehr/Amt für Heeresentwicklung*, aus: Künstliche Intelligenz in den Landstreitkräften – Ein Positionspapier des Amts für Heeresentwicklung; die Illustration veranschaulicht, dass zukünftige KI-Kriege Tod und Zerstörung bringen wie bisherige Kriege.*

Hans-Jörg Kreowski und Aaron Lye

Künstliche Intelligenz zieht in den Krieg

Editorial zum Schwerpunkt

Seit einigen Jahren wird ein Riesenrummel um die Künstliche Intelligenz (KI) gemacht. Nach bemerkenswerten Erfolgen bei Spielen wie Schach und Go sowie in der Sprach- und Bildverarbeitung hat KI nicht nur in der medialen Öffentlichkeit eine immense und anhaltende Aufmerksamkeit erregt, sondern auch Politik und Wirtschaft auf den Plan gerufen. Weltweit wird in der KI eine Schlüsseltechnologie für zukünftige Wertschöpfung gesehen. Viele Staaten haben deshalb KI-Strategien ausgearbeitet, in denen beschrieben wird, wie die Entwicklung und der Einsatz von KI-Systemen in Wirtschaft, Verwaltung, Bildung und Wissenschaft organisatorisch und finanziell gefördert werden soll. In vielen Fällen ist dabei auch thematisiert, dass KI-Systeme nur zum Wohle der Menschen genutzt und ethisch bedenkliche und risikoreiche Anwendungen ausgeschlossen werden sollen. Die Gefahren, die mit der Nutzung von KI-Systemen verbunden sein können, werden allerdings nicht annähernd so drastisch formuliert wie von Elon Musk, der KI für die „größte existenzielle Bedrohung" hält, die es gibt, oder von Stephen Hawking, der KI als „möglicherweise größten Fehler" bezeichnet hat, der je gemacht wurde. Es fällt bei den KI-Strategien der verschiedenen Staaten auch auf, dass der militärische Komplex weitgehend ausgespart ist.

Tatsächlich wird KI seit langem in vielfältiger Weise auch militärisch genutzt und gilt in Rüstung und im Kriegswesen als Hauptfaktor, der militärische Überlegenheit garantieren kann. Da das aber alle Seiten so sehen und keine ins Hintertreffen geraten will, bedeutet der Einsatz von KI in diesem Zusammenhang vor allem, dass mit immensen Finanz- und Personalmitteln an der Rüstungsspirale gedreht wird. Während die Entwicklung von Computertechnik und Informatik in den ersten Jahrzehnten seit dem Zweiten Weltkrieg stark vom Geld und von den Wünschen des militärischen Komplexes abhing, sind die Anfänge der Künstlichen Intelligenz ab 1956 eher friedlich angelegt gewesen. Damit war jedoch spätestens mit der *Strategic Computing Initiative* (SCI) der Vereinigten Staaten von Amerika der Jahre 1983 bis 1992 Schluss. Als Antwort auf das japanische *Fifth-Generation-Computer*-Projekt hat die *Defense Advanced Research Projects Agency* (DARPA) 500 Millionen (oder auch mehr) US-Dollar für die Entwicklung von Maschinenintelligenz ausgegeben, wobei es drei zentrale Aufgabenstellungen gab: ein Assistenzsystem für Kampfpiloten, ein Schlachtenlenksystem für die Marine und autonome Landfahrzeuge für die Armee. Zum Ende der 1980-er Jahre wurde das Budget wegen mangelnder Erfolge gekürzt. Aber es bleibt festzuhalten, dass es einsetzbare Systeme der genannten Art inzwischen gibt – wissenschaftliche und technologische Durchbrüche dauern meist viel länger als gedacht – und dass KI nicht zuletzt auch wegen SCI zu einem großen und bedeutenden Fachgebiet der Informatik angewachsen ist.

Unter dem Titel *Künstliche Intelligenz zieht in den Krieg* soll mit einigen Schlaglichtern auf die Verflechtung von KI und Rüstung in diesem Schwerpunkt eingegangen werden.

- Den Auftakt bildet der ganz außergewöhnliche Beitrag von Isabella Hermann und Tom Turtschi. Zu dem gemeinsamen Werk hat Tom Turtschi eine Kurzgeschichte beigetragen, die Isabella Hermann in den Kontext von Science-Fiction-Literatur stellt. Die Geschichte handelt von einem Krieg gegen Badbats, der von der menschlichen Kriegspartei mit modernen, vor allem KI-gestützten Waffen geführt wird.

- Ein wesentlicher Anlass, 1984 das FIfF zu gründen, war der drohende Einsatz von automatischen Frühwarnsystemen in Europa. Viele besorgte Fachleute haben damals befürchtet, dass wegen der kurzen Vorwarnzeiten einerseits und der eklatanten Fehlerhaftigkeit großer Softwaresysteme andererseits ein Atomkrieg aus Versehen eine virulente Gefahr darstellt. In ihrem Beitrag zeigen Karl Hans Bläsius und Jörg Siekmann, dass sich bis heute daran nichts geändert hat, nur dass die Öffentlichkeit inzwischen davon viel weniger Kenntnis nimmt.

- Aaron Lye setzt sich in seinem Beitrag damit auseinander, dass Militär und Geheimdienste in den USA seit einigen Jahren ihre gigantischen Datensammlungen von Cloud-Services kommerzieller Anbieter verwalten lassen – ein Milliardengeschäft. Großkonzerne des Silicon-Valley spielen damit eine wesentliche Rolle in der Kriegsführung. KI-gestützte Kriegsführung wird von ihnen forciert und machbar.

- Bevor es mit der üblichen Art von Artikeln in der *FIfF-Kommunikation* weitergeht, folgt erneut etwas Ungewöhnliches. Krysztof Daletski hat uns ein Gedicht geschickt, in dem er die wachsende Bereitschaft in Deutschland beklagt, Krieg wieder als führbar zu sehen. Es handelt sich um eine leicht veränderte Version der Erstpublikation im Blättchen (*https://das-blaettchen.de/2019/02/vorkriegsnotizen-47105.html*).

- In seinem Beitrag beschäftigt sich Christoph Marischka weniger mit der technologischen Seite des „KI-Kriegs", sondern mit der Rolle von Staat und Kapital. Die Entwicklung von Technik und Technologie muss finanziert werden, ohne dass unmittelbar Profite erzielt werden können. Das ist eine Domäne des Risikokapitals, was im militärischen Kontext gar nicht riskant ist, weil der Staat mit Steuergeldern solche Unternehmen absichert.

- Thomas Reinhold geht in seinem folgenden Artikel darauf ein, dass die militärische Vereinnahmung neuer Technologien wie KI bestehende internationale Rüstungskontrollabkommen infrage stellt. Er fragt, wie Rüstungskontrolle und Nichtverbreitungskontrolle von KI-gestützten und Cyberwaffen in der Praxis funktionieren kann. Er erwartet von Informatiker:innen, die diese Waffen entwickeln, dass sie auch Verantwortung bei der Rüstungskontrolle übernehmen.

- Der Beitrag von Christian Heck ist ein Nachdruck des Newsletters *Disruptive News* 21/2 von der Webseite *ground zero*, die von dem Bereich *Experimentelle Informatik* der Kunsthochschule für Medien Köln betrieben wird. Er weist darauf hin, dass der Mensch durch den Einsatz von Killerdrohnen verdinglicht wird, eine Sache, die man auch zerstören kann. Eine Reihe von Einzelbeispielen erinnern daran, dass Drohnenkrieg häufig zu Kollateraltötungen (Collateral Murder) führen.

- Den Schwerpunkt beschließt der Abdruck eines öffentlichen Appells gegen die Bewaffnung der Bundeswehr-Drohnen und für die Ächtung autonomer tödlicher Waffen. Die Initiative dazu ging aus von Wissenschaftler:innen aus KI und Informatik, darunter mehrere FIfF-Mitglieder, getrieben von Sorge, dass die künftige Regierungskoalition von der bisherigen Nichtbewaffnung der Killerdrohnen Abstand nimmt und damit auch die Tür zu autonomen tödlichen Drohnen weit öffnet.

Nimmt man die Artikel in dem beiliegenden Dossier 93 der Zeitschrift *Wissenschaft und Frieden* hinzu, entsteht ein etwas vollständigeres Bild. Dort geht Thomas Reinhold auf die technischen Möglichkeiten ein, die KI mit Fokus auf militärische Anwendungen bietet, und leitet daraus die neuen Herausforderungen für Rüstungskontrolle ab. Elke Schwarz richtet ihren Blick in Richtung Silicon Valley und weist darauf hin, dass der Mensch beim Einsatz von KI-Systemen leicht die Kontrolle verlieren kann, was im Krieg ethisch und völkerrechtlich problematisch ist. Christoph Marischka setzt sich in seinem Beitrag mit der Mitwirkung deutscher Forschungseinrichtungen bei der Entwicklung von Bilderkennungsmethoden im militärischen Kontext auseinander. Marius Pletsch behandelt in seinem Beitrag eine Problematik, die im militärischen Kontext erst in letzter Zeit in den Fokus gerückt ist: das Zusammenwirken von Soldat:innen und (teil)autonomen Waffensystemen. Hans-Jörg Kreowski und Aaron Lye schließlich stellen eine jüngst begonnene und für die nächsten Jahrzehnte geplante Entwicklung eines neuen europäischen Kampfflugzeugs (FCAS) vor, bei der KI als allumfassende Querschnittstechnologie eingesetzt werden soll.

Das Thema hat viele Facetten, die nur teilweise behandelt und diskutiert werden konnten. Es bleiben diverse Fragen bezüglich des Wechselverhältnisses von KI und Krieg offen, auf die eingegangen werden müsste. Dazu gehören:

- Sind Drohnenschwärme, die z. B. die Überlegenheit in zukünftigen Luftkämpfen sichern sollen, mit den Methoden der Schwarm-Intelligenz modellierbar und implementierbar, die sich an Ameisenkolonien, Bienenstöcken und Vogelschwärmen orientiert? Oder haben sie nur das Wort *Schwarm* gemeinsam?

- Betrieb und Einsatz von Waffensystemen mit vielen Komponenten, die jeweils mit diversen Sensoren ausgestattet sind, produzieren gigantische Datenberge. Sind die Methoden und Algorithmen der Datenwissenschaft (Data Science) geeignet und in der Lage, die sinnhaft auszuwerten und so die Kriegsführung zu optimieren? Oder ist das die Suche nach Stecknadeln, wo nur Heu ist?

- Wie alles, was programmiert wird und werden soll, sind KI-Algorithmen und KI-Systeme durch die Grenzen der Berechenbarkeit beschränkt. Insbesondere bedeutet das, das geht, was sich durch formale Regeln auf digitalen Informationsstrukturen modellieren lässt. Folgen Krieg, Kriegsplanung und Kriegsführung solchen Regeln? Wohl kaum, denn Krieg ist weder eine Rechenaufgabe noch ein Spiel wie Schach. Trotzdem wird es angestrebt. Wie denken sich also Befürworter:innen diese KI-Systeme für die Kriegsplanung und -führung?

- KI-gestützte Killerdrohnen sind schon lange eine Wirklichkeit, die auch immer wieder medial rezipiert wird. Andere Bereiche des militärischen Komplexes sind wesentlich weniger im Fokus der Wahrnehmung. Wieweit ist der Einsatz von KI in den anderen Domänen, beispielsweise bei den Landstreitkräften oder in der Marine, fortgeschritten?

Auch wenn in diesem Schwerpunkt viele Einzelaspekte angesprochen sind, fehlt ein Gesamtbild zum Thema KI-Krieg. Was passiert und ist in dieser Hinsicht bei Staaten und Militärbündnissen geplant? Wie verhält sich das zueinander? Die vielen offenen Fragen zeigen, dass die Auseinandersetzung mit diesem Thema weitergeführt werden muss. Das ist aber nicht nur eine Aufgabe der Friedensbewegung, sondern bedarf auch einer viel stärkeren und systematischen wissenschaftlichen Aufarbeitung.

Isabella Hermann und Tom Turtschi

Die Doppelblind-Mission – ein Spiel?

Der Science-Fiction-Autor Tom Turtschi und ich haben uns mit dem Fokus dieser Ausgabe KI zieht in den Krieg *dazu entschlossen, einen gemeinsamen Beitrag zu verfassen: Er schreibt eine Science-Fiction-Story, in der das Thema eine Rolle spielt, und ich schreibe Theoretisch-Analytisches drum herum.[1] Aber warum Künstliche Intelligenz und Krieg überhaupt aus der Perspektive von Science-Fiction angehen? Science-Fiction ist schließlich kein (Technology-)Foresight, das konkrete Zukunftsszenarien abbildet, und will es (meistens) auch gar nicht sein.*

Genau deswegen! Denn Science-Fiction erzählt nicht über die Zukunft, sondern Geschichten mit, über und durch fiktive Wissenschaft und Technologie. Das Genre reflektiert aktuelle soziotechnische Trends, indem es Extremsituationen schafft, die aktuelle Tendenzen der Gegenwart, aber auch Urängste und Ursehnsüchte des Menschen wie unter einem Vergrößerungsglas erscheinen lassen. Die häufig in Science-Fiction-Filmen und -Romanen gewählte Erzählperspektive der Zukunft ist zuvorderst dazu da, die Veränderungen in der Science-Fiction-Welt im Vergleich zu der uns bekannten Welt zu plausibilisieren. Es handelt sich also mehr um einen Schritt zur Seite als nach vorn – was jedoch wegen der Kreativität durchaus für Foresight-Prozesse gewinnbringend sein kann, die in ihrer Methodik feststecken können (Steinmüller 2016).

So ist Science-Fiction das Popkultur- und Kunstgenre, das an den Grenzrändern (*Boundary*) entsteht, wo sich grundlegende Menschheitsfragen mit aktuellen Wertediskussionen, Trends und Ereignissen sowie der Wissenschafts- und Technikentwicklung treffen (Abbildung 1). Im *Matrix*-Franchise von 1999, wo Maschinen und Menschen Krieg gegeneinander führen, werden beispielsweise sowohl die grundlegende Angst vor Beherrschung, aber auch Erlösungsphantasien, die damals real existierende Unsicherheit durch die bevorstehende Jahrtausendwende und die Folgen des Neoliberalismus sowie die zunehmende Digitalisierung und Technisierung der Welt aufgegriffen.

Die fiktive Technologie kann dabei näher oder weiter weg von unserer bekannten Realität liegen, aber auch eine Metapher darstellen (Vint 2021:6). Hier kommt es neben der Intention der Autor:innen vor allem auf die Deutung der Rezipient:innen an, wo sie eine Geschichte auf einem *Science-Fiction-Kontinuum* verorten (Abbildung 2). Wenn man so will, kann man *Matrix* als reale Warnung vor dem Bau „intelligenter" Maschinen begreifen, oder die Maschinenherrschaft als generelles Bild für Unterdrückung, Totalitarismus oder Kolonialismus auslegen. Relevant ist allerdings, dass – ganz gleich wo man die Technik im Kontinuum verortet – Science-Fiction ihre Geschichten in-

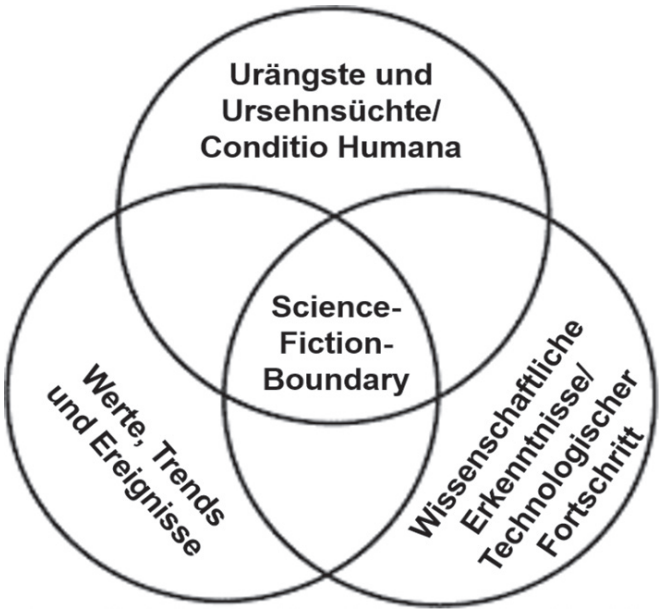


Abbildung 1: Science-Fiction als Boundary Management

nerhalb des vorherrschenden Paradigmas des wissenschaftlichen Denkens erzählt. Das unterscheidet die Science-Fiction beispielsweise vom Genre der Fantasy, das vergleichbar einem Märchen, einer Sage oder einem religiösen Ursprungsmythos funktioniert (Dath 2019:75). Nicht zufällig formierte sich Science-Fiction als Genre in der Ära der Moderne mit ihren sozialen Umwälzungen und dem Glauben an den technischen Fortschritt.

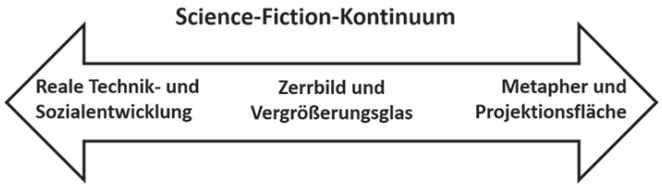


Abbildung 2: Das Science-Fiction-Kontinuum

Nun aber zu Tom Turtschis Kurzgeschichte in drei Akten.

Die Doppelblind-Mission

Der Nebel im Tal ist undurchdringlich.

Diesig, trübe, und das Restlicht, das durch die zähflüssigen Wolken und die Baumkronen bis nach unten dringt, ist zu spärlich für eine optische Peilung. Ich schalte auf Infrarot und zapfe die Sensoren an, die das Gelände verminen.

Ich morphe die Drohne zu einem faustgroßen Avatar mit zwei Raupen, Panzerung und Lasergun – an Fliegen ist in diesem Suppentopf eh nicht zu denken. Mit dem Joystick navigiere ich vorsichtig durch das Unterholz. Spähe durch moosbehaarte Büsche und triefende Farne, die sich wie Palmwedel über mir zu einem Baldachin schließen, umrunde haushohe Kiesel, erreiche ein Pilzfeld und verkrieche mich unter einen der Schirme.

Die Geduld zahlt sich aus, keine halbe Stunde später schält sich aus der Falschfarbendarstellung auf meinem Display ein riesiges Monster. Die Flecken konturieren sich zu einem Gorgonen mit sechs Beinen, drei Köpfen – er breitet seine Arme aus und flattert bedrohlich mit ausladenden Flügeln.

Ich gleite unter dem Pilz hervor und nehme das Unding ins Visier. Zögere einen Moment – ein Segment spaltet sich ab, umrundet das geflügelte Monster, kommt auf mich zu. Ich schieße auf die beiden Teile. Der Vierbeiner sackt zusammen, Fittiche wirbeln über den Boden, zucken, verenden in Agonie. Das Wesen teilt sich erneut, der Restrumpf löst sich von den Flügeln und hastet auf zwei Beinen davon.

Ein enttarnter Badbat!

Genau so werden sie in den Posts ehemaliger Kämpfer beschrieben: Feige, degenerierte Mutanten, mit einem ekelhaften Geschwür auf der Stirn.

Augenloses Fledermausgesindel, das mit seinem Dreck die ganze Zivilisation bedroht – sie sitzen im Hochland an den Quellen, wie die Regierung seit Jahren betont. Ich nehme die Verfolgung auf. Mit etwas Glück führt mich das Ding in den Unterschlupf, und ich schaffe es dieses Mal, das Nest auszuräuchern.

Die Sensoren liefern genügend Daten, um das Gelände mit der Karte abzugleichen und damit ich die Fährte nicht verliere.

Feindkontakt beim Wasserfall.

Eine ganze Horde! Diese Badbats sind riesig, doppelt so groß wie das geflohene Exemplar.

Ich presche auf das offene Feld und drücke eine erste Salve mit biomechanoiden Luchsspinnen ab. Das Batallon eiert aus meinem Bauch und krabbelt davon, ich lasse die Spinnen in alle Richtungen ausschwärmen und konzentriere mich, jede in Position zu bringen, um ihre Giftladung in die Stirnwülste der Badbats abzusetzen. Ich verliere die Übersicht – das Bewusstsein in 60 Teile aufzuspalten und für die Zielpeilung mit den Sensordaten abzugleichen bringt meine Fähigkeit zum Multitasking an Grenzen – aber in diesem Moment spüre ich den Kick des Brainbooster, der mir im Schädel explodiert. Eine ganze Kohorte – ich fühle die Spinnen bis in die Spitzen aller 480 Extremitäten und fokussiere, prozessiere und schieße und schieße. Mein Score steigt auf 97.

Die Überlebenden ziehen sich zurück.

Ich folge dem Gesindel, quere Murgänge, Zonen mit Totholz, Lichtungen.

Nach weiteren zwei Scharmützeln stehe ich vor einer Felswand. Die alte Mine! Endlich habe ich das Nest gefunden.

Ich erwarte einen Torwächter, aber beim Eingang taucht eine ganze Meute auf. Hinter jedem Badbat, den ich ausschalte, bringen sich drei neue in Stellung. Ich werde umzingelt, der Brainbooster zeigt kaum Wirkung, ich lasse meine Division Luchsspinnen vollständig ausschwärmen und schalte in den autonomen Modus der Schwarmintelligenz. Mein Score steigt rasend, klettert über neunhundert. Wunderhübsche Pixelhaufen explodieren rundum im Nebel, wie bei einem nächtlichen Feuerwerk zerstieben die Köpfe der Badbats – damn, what the hell … ein Störsignal, der Kontakt zu den Spinnen bricht ab … Schmerz durchzuckt mich, die strukturelle Integrität der Hüllenpanzerung meines Avatars zerfällt … Zischen, Wasser dringt in die Elektronik, Funken sprühen, dann verabschiedet sich das Display und mir wird Schwarz vor Augen.

Der erste Teil der Geschichte lädt dazu ein, sie auf der linken Seite des Science-Fiction-Kontinuums zu platzieren. Auch wenn die aufgespannte Welt verfremdet ist, findet man Technologien, die aktuelle, reale und denkbare Entwicklungen für die Kriegsführung aufnehmen: *Virtual Reality* (Triandafillidis 2021), *Memetic Warfare* (Giesea 2016), Drohnen in allen Ausprägungen (Franke 2018), Forschung zu Schwarmintelligenz (Ekelhof/Paoli 2020), Gamification (Eastwood 2021), Biotechnologie (Reding/Eaton 2020:94-103) – das alles gibt es und in all diesen Bereichen spielt KI eine oder die entscheidende Rolle als *Technology Enabler* – ganz abgesehen von vollautonomen Waffensystemen (Scharre 2018). Im Text werden mögliche Einsatzfelder neuer KI-ermöglichter Technologien bei einer verdeckten Mission in feindlichem Gebiet betrachtet, die schon im Heute oder in naher Zukunft vorstellbar sind.

Ich richte mich auf, ziehe die VR-Einheit über den Kopf. Die Brille verheddert sich mit den Kabeln der Elektrodenkappe. Georgi, der wissenschaftliche Leiter, eilt zu Hilfe. Der schlaksige Kerl mit Nickelbrille streicht eine fette Haarsträhne aus der Stirn, nestelt an den Drähten und ist voller Anerkennung: „Gratuliere, ein Score von

1023 ist nicht übel, seit der letzten Trainingseinheit hast du deine Leistung fast verdoppelt!"

Ich schiebe das Lob zurück: „Dein Synapsenbooster kam genau im richtigen Moment. Ohne den Energiestoß hätten mich die Monster bereits beim Wasserfall kalt gemacht."

Die Freude währt nur kurz, bei der Manöverbesprechung herrscht mich der befehlshabende Offizier an: „Sie wurden zu früh enttarnt! Bei verdeckten Operationen gilt, unsichtbar zu bleiben. Der Feind darf den Angriff nicht als solchen erkennen. Verstecken, Soldatin, verschleiern, verbergen, vertuschen – und dann eliminieren! Das nächste Mal setzen Sie die Luchsspinnen aus dem Hinterhalt ein."

Ich nicke. „Ich werde mir das für den Ernstfall merken."

„Ernstfall?" Der Offizier vernichtet mich mit einem einzigen Blick. „Wer garantiert Ihnen, dass der Ernstfall nicht soeben stattfand?" Seine Stimme wird schneidend wie die Kreide eines Oberlehrers auf der Schiefertafel: „Sie kennen den Wert der Doppelblind-Einsätze. Sie dürfen nicht wissen, ob sie die Mission simulieren oder gerade durchführen, genau so wenig wie wir vom Befehlsstab. Wenn die objektive Datenlage über den Feind durch Emotionalität getrübt wird, vermindert das die Effizienz unserer Aktionen. Empathie war nie ein guter Ratgeber im Kampf um das Überleben, Soldatin!"

Hier rutscht die Geschichte weiter in die Mitte des Science-Fiction-Kontinuums, in der ich die Idee der Doppelblind-Mission verorte. Hier laufen die Fäden eines Gegenwartskommentars und einer extremen fiktiven Einsatzform zu einem kritischen Zerrbild zusammen. In der Doppelblindmission ist Krieg in erster Linie ein virtuelles Spiel, und erst nachgeordnet ein realer Einsatz, da weder die Soldatin noch der Befehlshaber wissen, ob es sich um eine Simulation handelt oder nicht. Das hat zur Folge, dass wohl alle Soldat:innen im Allgemeinen zuvorderst das Ziel verfolgen, eine möglichst hohe Punktzahl zu erreichen, um das „Spiel" zu gewinnen. Wenn es sich aber lediglich um ein Spiel handelt, muss sich niemand mit möglichen Hintergründen, Folgen und Opfern des Einsatzes auseinandersetzen.

Der Nebel im Tal durchnässt die Kleider, das Haar klebt in Strähnen auf dem Wulst über ihren blicklosen Augen. Flink flitzt sie um Stämme, hüpft über Farne, Wurzeln und Steine. Ada ist auf der Pirsch. Verbotenerweise. Der Vater sieht es nicht gern, wenn sie alleine durch die Wälder streift. Aber sie ist ja nicht alleine, Pluto tollt an ihrer Seite.

Ada verfolgt den Adler.

Sie hat ihn bei den Pilzen geortet, wo er Dohlen jagt, die geschickt durch das Unterholz hüpfen. Der Bergadler erlegt seine Beute so wie der Fuchs das Kaninchen, in wildem Zickzack über Stock und Stein – die Vögel haben die Fähigkeit verloren, durch die Luft zu gleiten und sich von oben auf das Opfer zu stürzen. Schon vor langer Zeit, sagte der Alte vom Berg, nach den letzten Bomben, die den Himmel verdunkelt und den triefenden Schleier zwischen die Berge auf das Tal gelegt haben. Wozu sollten Vögel fliegen, hier bei uns, wo du deine Finger bei ausgestrecktem Arm nicht sehen kannst?

Ada stellt sich vor, wie sie den Bergadler füttern wird.

Er ist rasch gefangen, mit Plutos Hilfe. Er treibt ihn auf sie zu, sie schließt beide in die Arme, ihren Hund, den Vogel, glücklich, übermütig.

Pluto knurrt, reißt sich los – jetzt ortet auch sie mit dem Echolot die faustgroße Raupe, die zehn Schritte entfernt aus den Pilzen kriecht. Es zischt, zweimal, Pluto jault und stürzt, panisch lässt sie den Adler fahren und ergreift die Flucht.

Das Herz schlägt ihr in der Kehle, Äste peitschen ins Gesicht, sie fiepst und zirpt und rennt, so schnell sie nur kann.

Beim Wasserfall berichtet sie den Arbeitern atemlos von der Raupe, eilt weiter zu den alten Minen, nach Hause.

„Eine teuflische Raupe? Wo denkst du hin, Kind. Wir leben in einem friedlichen Tal, gemeinsam mit allen Wesen, hier gibt es keine gefährlichen Tiere. Wo ist Pluto?" Verzweifelt trommelt Ada an Vaters Brust, schiebt seine tröstende Hand zu Seite.

Oben beim Eingang treffen sie auf ein Gemetzel. Alle drängen raus, stürzen sich auf den glitzernden Teufel, in die Schar giftiger Spinnen, bis ihre Köpfe explodieren.

Vater ist entsetzt. Zerrt Ada zur Seite, in den Schutz eines vermoosten Busches. Er tippt ihr an der Stirn auf die Stelle, wo sich der Wulst quer über die beiden leeren Augenhöhlen zieht.

„Wir mögen keine Augen haben, Ada, aber wir sind nicht blind: Wir haben einen Wulst auf der Stirn wie die Delphine, um zu sehen. Wie die Fledermäuse empfangen wir das Echo der Dinge, wenn wir die Welt mit Tönen ertasten. Nutze deine Sinne, nutze deinen Kopf! Du musst die Schale der Raupe knacken, wie bei einer Nuss. Dann schubst du sie ins Wasser. Los, Mädchen!"

Ada nickt.

Das Geschoss der Spinne trifft ihn exakt über der Nasenwurzel. Vaters Zirpen erstirbt. Seine gebuchtete Stirn zermantscht wie eine überreife Melone, die aus großer Höhe auf einen Felsen prallt.

Ada packt einen Stein.

Stößt ein hochfrequentes Trillern aus und peilt über das Echo die Raupe – auf zwei Uhr, exakt dreiundvierzig Schritte von ihr entfernt.

Sie lauscht dem Wispern der Spinnen, horcht, wie diese mit dem Mutterwesen und untereinander kommunizieren, ein mächtiger Chor. Ada bietet alle Kräfte auf und ihr entfährt ein gläserner Schrei, der ihr selber das Blut in den Adern gefrieren lässt, aber das ganze Wispern übertönt. Sie schreit, schreit und geht unbehelligt auf die Raupe zu, hebt den Stein und zertrümmert mit einem einzigen Schlag deren harten Schild …

Diesen Teil der Geschichte möchte ich noch weiter auf die rechte Seite des Science-Fiction-Technik-Kontinuums setzen. Denn hier geht es um prinzipielle Fragen, die durch Technologien verschärft werden, aber unabhängig vom technologischen Fortschritt bestehen. Zunächst erfahren wir nun, dass die vorher noch virtuell anmutende Umgebung nicht nur real ist, sondern für die Doppelblindmission offensichtlich durch Sensoren, die die von der Soldatin gesteuerte Drohne mit Informationen versorgen, verfälscht wurde. Aus den Badbats, den feigen und degenerierten Mutanten, werden humane Lebewesen, aus dem Gorgonen – der Tarnung – werden Tiere. Das Land wurde von früheren Bombardements verwüstet. Es handelt sich offensichtlich um einen Kampf um wertvolle oder lebenswichtige Ressourcen, an deren Quellen die Angegriffenen laut „Regierungsangaben" sitzen. Wir befinden uns in einem hybriden und asymmetrischen Ressourcenkrieg, in dem die Grenzen zwischen Kombattant:innen und Zivilist:innen verschwommen gemacht werden. Durch Propaganda- und Fehlinformationen sowie Mittel der psychologischen Kriegsführung werden die Beteiligten manipuliert und die Kampfhandlungen legitimiert. Die in der Geschichte dargestellte verfremdete Welt mit ihren KI-Technologien ist nicht der vorwiegende Grund dafür, treibt die Problematik aber auf die Spitze. Die Überlegung, für welche Art von realen Konflikten die Geschichte stehen könnte, möchte ich Ihnen als Leser:innen selbst überlassen.

Die Shortstory im Gesamten zeigt exemplarisch, was Science-Fiction als *Boundary Management* bedeutet: die Überlagerung der verschiedenen Ebenen der Urängste, aktueller Trends sowie Technologieentwicklung machen das Spannende und Faszinierende des Genres aus. Es lohnt sich – wie im oben gewählten Beispiel des *Matrix*-Franchise – auch andere Science-Fiction-Darstellungen aus neuer Perspektive zu betrachten – zumal es sich häufig um Computer und Roboter handelt, die autonom agieren, außer Kontrolle geraten und sich gegen die Menschen stellen (Irsigler, Orth 2018). Oft genug geht es dabei nicht um eine kritische Technikreflektion oder gar Technikfolgenabschätzung, sondern KI dient vielmehr als Platzhalter, um über menschliche Problematiken nachzudenken (Hermann 2019, 2020, 2021). Beispiele zum Thema Krieg im weitesten Sinne sind die Folge *The Ultimate Computer* aus *Star Trek: The Original Series* von 1968, der Film *Colossus: The Forbin Project* von 1970, *Dark Star* von 1974, *War Games* von 1983, das *Terminator*-Franchise ab 1984, *I, Robot* (2004), die Serie *Battlestar Galactica* (2004-2009), *Robocop* (2014) oder das *Control Threat Assessment System* in der zweiten Staffel von *Star Trek: Discovery* (2019).

Dabei sollte man natürlich nicht außer Acht lassen, dass Science-Fiction auch vom Entertainment und Disaster Porn lebt, und die bestehenden Verhältnisse auch nicht nur kritisiert, sondern – wie jedes Genre und Medium – selbst für Propagandazwecke von der Wirtschaft, Regierungen, oder dem Militär eingesetzt wird (McIntosh 2016). Wichtig bleiben also die kontextuelle Einordnung und kritische Reflektion jedes Einzelnen. Und weil gute Science-Fiction dabei kreativ und originell ist, ist dies nicht nur eine intellektuelle Übung, sondern darf auch Spaß machen.

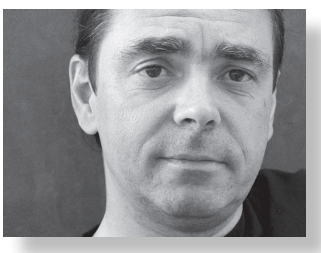
Referenzen

Dath, Dietmar (2019) Niegeschichte: Science Fiction als Kunst- und Denkmaschine. Verlag Matthes & Seitz, Berlin.

Ekelhof, Merel/Paoli, Giacomo Persi (2020) Swarm Robotics: Technical and Operational Overview of the Next Generation of Autonomous Systems. The United Nations Institute for Disarmament Research (UNIDIR), Genf.

Easton, Brent M. (2021) The Gamification of War In a 'War Room' Is a Dangerous Trend. 19fortyfive (https://www.19fortyfive.com/about-us/).

Franke, Ulrike (2018) Military Robots and Drones. In Galbreath, David/Deni, John (Hrsg.): Routledge Handbook of Defence Studies. Routledge, New York S. 339-349.



Isabella Hermann und Tom Turtschi

Isabella Hermann befasst sich als promovierte Politikwissenschaftlerin mit dem Science-Fiction-Genre als Spiegel der Gegenwart und Wegweiser in die Zukunft. Zuletzt koordinierte sie eine interdisziplinäre Arbeitsgruppe zu Künstlicher Intelligenz und menschlicher Verantwortung an der Berlin-Brandenburgischen Akademie der Wissenschaften und war Programmleiterin des Present Futures Forum an der Technischen Universität Berlin.

Tom Turtschi verzieht sich als Autor gerne in die Zukunft, um aus sicherer Distanz die toxischen Stoffe der Gegenwart zu explorieren. Bei den Feldversuchen im richtigen Leben betätigt er sich als Gestalter und Szenograf. Gemeinsam mit seiner Frau betreibt er die Agentur hof3, ein Atelier für Ausstellungen, Erlebniswelten und Multimedia. Er lebt im ländlichen Emmental zusammen mit Katzen, Schafen, Bienen, Hühnern und Enten auf einem Permakulturbetrieb.

Giesea, Jeff (2016) It's time to embrace memetic warfare. Defence Strategic Communications Volume 1, S. 67-75 (https://stratcomcoe.org/publications/its-time-to-embrace-memetic-warfare/164).
Hermann, Isabella (2021) Artificial intelligence in fiction: between narratives and metaphors. AI & Society (https://doi.org/10.1007/s00146-021-01299-6).
Hermann, Isabella (2020) Beware of fictional AI narratives. Nature Machine Intelligence 2, S. 654 (https://doi.org/10.1038/s42256-020-00256-0).
Hermann, Isabella (2020) Künstliche Intelligenz in der Science-Fiction: Zwischen Magie und Technik. FIfF-Kommunikation 4/2020 „Digitalisierung der Bildung", S.12-17 (https://www.fiff.de/publikationen/fiff-kommunikation/fk-2020/fk-2020-4/fk-2020-4-content/fk-4-20-p12.pdf).
Irsigler, Ingo/Orth, Dominik (2018) Zwischen Menschwerdung und Weltherrschaft: Künstliche Intelligenz im Film. APuZ 6–8/2018, S. 39–46 (https://www.bpb.de/apuz/263688/zwischen-menschwerdung-und-weltherrschaft-kuenstliche-intelligenz-im-film).
McIntosh, Jonathan (2016) Military Recruitment and Science Fiction Movies. Popculture Detective (https://popculturedetective.agency/2016/military-recruitment-and-science-fiction-movies).
Reding, D./Eaton, J. (2020) Science & Technology Trends 2020-2040 – Exploring the S&T Edge. NATO Science & Technology Organization, Brüssel (https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf).
Scharre, Paul (2018) Army of None: Autonomous Weapons and the Future of War. W.W. Norton, London.
Steinmüller, Karlheinz (2016) Antizipation als Gedankenexperiment: Zukunftsforschung und Science-Fiction. In: Reinhold P u. a. Hg. (2016) Einblicke, Ausblicke, Weitblicke. Aktuelle Perspektiven in der Zukunftsforschung. Lit Verlag, Wien/Zürich, S. 320–338.
Triandafillidis, Nikita (2021) Implementation of virtual reality and the effects in cognitive warfare. Modern Diplomacy (https://moderndiplomacy.eu/2021/07/21/implementation-of-virtual-reality-and-the-effects-in-cognitive-warfare/).
Vint, Sherryl (2021) Science Fiction. MIT University Press, Cambridge.

Anmerkung

1 *Das Experiment lag nicht nur in der eher ungewöhnlichen Artikelkombination, sondern vor allem darin, dass wir uns hinsichtlich Aufbau und konkretem Inhalt der Geschichte nicht abgesprochen haben. Es handelte sich also auch um eine persönliche Doppelblindmission, ich wusste nicht, welche Geschichte Tom Turtschi schreiben würde, und er wusste nicht, wie ich diese einrahmen würde.*

Karl Hans Bläsius und Jörg Siekmann

KI in militärischen Frühwarnsystemen

Computergestützte Frühwarn- und Entscheidungssysteme sollen einen Angriff mit Atomwaffen rechtzeitig erkennen, damit bei entsprechender Situationsbewertung die eigenen atomaren Trägerraketen gegebenenfalls vor einem vernichtenden Einschlag aktiviert werden können. Im Falle eines Fehlalarms könnte so auch ein Atomkrieg aus Versehen ausgelöst werden. Die Zeit zur Bewertung einer potenziellen Angriffssituation liegt im Bereich weniger Minuten. Ein neues Wettrüsten wird diese Zeitspanne verkürzen. Für eine Analyse und Bewertung von Alarmmeldungen bleibt für Menschen daher so wenig Zeit, dass hierfür verstärkt automatische Systeme eingesetzt werden sollen. Aufgrund der unsicheren Datengrundlagen können aber auch automatische Systeme keine sicheren Entscheidungen treffen.

Abschreckungsstrategie

Die Sicherung der atomaren Zweitschlagfähigkeit ist die Grundlage der Abschreckungsstrategie, die bis heute jeden potenziellen Angreifer abgehalten hat, einen atomaren Angriff zu starten. Wer angegriffen wird, kann den Einschlag von Atomwaffen abwarten und hat danach immer noch genügend Zeit und Potenzial, einen vernichtenden Gegenschlag auszuführen, im Schlagwort: „Wer als erster schießt, stirbt als zweiter."

Um auch bei einer Gefährdung der Zweitschlagfähigkeit reagieren zu können, haben die Atommächte computergestützte Frühwarn- und Entscheidungssysteme entwickelt und installiert, mit dem Ziel, einen Angriff rechtzeitig zu erkennen, um die eigenen atomaren Trägerraketen vor dem vernichtenden Einschlag aktivieren zu können. Eine solche Strategie wird als *Launch-on-warning*-Strategie bezeichnet.

Auch wenn die Abschreckungsstrategie weitere bewusste Atomwaffeneinsätze bisher verhindert hat, schützt sie nicht vor einem Atomkrieg aus Versehen, z. B. in Folge eines Fehlers in einem Frühwarnsystem. In der Vergangenheit gab es einige Situationen, in denen es nur durch großes Glück nicht zu einem Atomkrieg aus Versehen kam.

Militärische Frühwarn- und Entscheidungssysteme

Militärische Frühwarn- und Entscheidungssysteme dienen der Erkennung eines Angriffs durch Atomraketen auf der Basis von Sensordaten. Sensordaten können Hinweise auf, aber keine sicheren Erkenntnisse über mögliche Bedrohungen liefern. Es kann also zu Fehlalarmen kommen, wobei ein Angriff mit Atomraketen angezeigt wird, obwohl keine Bedrohung vorliegt. Solche Fehlalarme können ganz unterschiedliche Ursachen haben. Neben unklaren oder falsch bewerteten Sensordaten haben z. B. auch Hardware-, Software- oder Bedienungsfehler zu falschen Alarmmeldungen geführt.

Die Datengrundlage für die Bewertung einer Alarmmeldung ist vage, unsicher und unvollständig. Zur Situationsbewertung sind deshalb neben den Sensordaten viele weitere Aspekte zu berücksichtigen, wie z. B. die weltpolitische Lage und die Einschätzung des „Gegners". In Friedenszeiten und Phasen politischer Entspannung sind die Risiken gering, dass die Bewertung einer Alarmmeldung zu einem atomaren Angriff führt. Die Situation kann sich drastisch ändern, wenn politische Krisensituationen vorliegen, eventuell mit gegenseitigen Drohungen, oder wenn in zeitlichem Zusammenhang mit einem Fehlalarm weitere Ereignisse eintreten, die zur Alarmmeldung in Zusammenhang ge-

setzt werden könnten. In einer solchen Situation könnte eine Alarmmeldung als echt gedeutet werden und einen eigenen Angriff scheinbar rechtfertigen. So könnte es zu einem Atomkrieg aus Versehen kommen.

Eine steigende Anzahl verfügbarer Sensoren und Überwachungssysteme, auch im Weltraum, erhöht die zu verarbeitende Datenmenge, wobei gleichzeitig die Vorwarnzeiten weiter reduziert werden, z. B. durch neue Waffensysteme wie Hyperschallraketen. So sind für die Klassifikation von Sensordaten und die Bewertung einer Alarmsituation immer mehr computergestützte Verfahren insbesondere der Künstlichen Intelligenz (KI) erforderlich, um für gewisse Teilaufgaben Entscheidungen automatisch zu treffen, bzw. menschliche Entscheidungen vorzubereiten. Dabei ist es unerheblich, ob solche automatischen Systeme als intelligent angesehen und dem Gebiet der Künstlichen Intelligenz zugeordnet werden oder nicht.

Automatische Entscheidungen

Entscheidungen in Frühwarnsystemen beruhen auf umfangreichen Daten, die von den Sensoren geliefert werden, sowie auf Kontext-Informationen, Gefährdungsanalysen oder Analysen der weltpolitischen Lage. Sowohl im Falle von menschlichen Entscheidern als auch bei automatischen Entscheidungen werden solche Daten und Informationen benötigt und müssen entscheidungsrelevant zusammengefasst werden. Diese Datengrundlage ist allerdings unsicher, vage und unvollständig.

Unsicherheit, Vagheit, Unvollständigkeit

Zunächst ein Beispiel für sicheres Wissen:

> *Wenn x Kind von y ist und y Kind von z ist, dann ist x Enkel von z*

Eine solche Regel kann als gültig angenommen werden. Schlüsse, die darauf basieren, führen wieder zu gültigen, korrekten Ergebnissen, sofern die Prämissen korrekt waren. Die Aspekte Unsicherheit, Vagheit, Unvollständigkeit treffen hier nicht zu.

Das nächste Beispiel zeigt eine unsichere Regel:

> *Wenn x ein Auto ist und y ist der Besitzer von x, dann ist y derzeitiger Nutzer von x.*

Eine solche Regel gilt nicht immer, es kann Ausnahmen geben. Der Nutzer eines Autos könnte ein Kind des Besitzers sein. Auch bei Firmen können Besitzer und Nutzer unterschiedlich sein. Diese Regel ist also unsicher und gilt nur mit einer gewissen Wahrscheinlichkeit.

Beispiel für einen vagen Zusammenhang:

> *Wenn x ein schweres Auto ist, dann benötigt x viel Kraftstoff.*

Die Frage ist hier: was bedeutet „schwer“, was bedeutet „viel“. In diesem Beispiel können die Aussagen *x ist ein schweres Auto* und *x benötigt viel Kraftstoff* nicht einfach mit den Wahrheitswerten wahr und falsch belegt werden. Diese Eigenschaften sind vage und der Wahrheitswert könnte hier als ein beliebiger Wert (reelle Zahl) zwischen 0 und 1 dargestellt werden, wobei 0 für falsch und 1 für wahr steht.

Bei vielen Anwendungen ist es nicht möglich, vollständige und sichere Informationen zu erlangen. Stattdessen müssen Annahmen getroffen werden, die in typischer Weise gelten oder zu erwarten sind. Auf dieser Basis können dann Schlüsse gezogen und Entscheidungen getroffen werden.

> *Beispiel: Wenn x ein Vogel ist, dann kann x fliegen.*

Dies ist zwar typisch, gilt im Normalfall, aber es gibt Ausnahmen. Ein Strauß ist ein Vogel, kann aber nicht fliegen.

Die Künstliche-Intelligenz-Forschung hat Verfahren entwickelt, um mit den unterschiedlichen Arten von Wissen und deren Grad an Glaubwürdigkeit umzugehen, aber die Schlussfolgerungen gelten dann ebenfalls nicht absolut, sondern nur mit gewisser Wahrscheinlichkeit.

Automatisches Schließen bei unsicherer Datengrundlage

In der Praxis gibt es viele Zusammenhänge, die unsicher sind, also nicht uneingeschränkt gelten. Unser normales Alltagswissen ist vage, unsicher und unvollständig. Trotzdem sind auch in solchen Situationen Schlussfolgerungen möglich und eventuell notwendig.

Besonders wichtig sind Methoden des probabilistischen Schließens. Hierbei werden numerische Werte für die Gültigkeit von Formeln verwendet, die dann beim Schlussfolgern miteinander verrechnet werden. Verschiedene Wahrscheinlichkeitsmodelle unterscheiden sich darin, wie Formeln verknüpft werden können und wie die Wahrscheinlichkeitswerte dann verrechnet werden. Auch zur Darstellung und Verarbeitung von vagen Werten werden meist numerische Werte verwendet.

In vielen Fällen kann Unsicherheit oder Unvollständigkeit so behandelt werden, dass zunächst eine „normale“, „typische“ Regelanwendung erfolgt. Typisch ist, dass Vögel fliegen können und dass der Besitzer eines Autos auch ein Nutzer dieses Autos ist. Solange nichts Gegenteiliges bekannt ist und kein Widerspruch entsteht, kann ein entsprechender Schluss gezogen werden. Im Falle eines Konfliktes müssen dann geeignete Maßnahmen zur Auflösung des Konfliktes getroffen werden. Auch für diese Art von Schlussfolgerungen gibt es unterschiedliche Methoden in der KI, insbesondere logische Verfahren.

Unabhängig vom gewählten Verfahren ist die Behandlung von Vagheit und Unsicherheit recht komplex und die Schlussfolgerungen sind ebenfalls unsicher, das heißt diese können auch falsch sein. Falsche Annahmen und falsche Schlussfolgerungen führen häufig zu Inkonsistenzen. In diesen Fällen können Korrekturmaßnahmen vorgenommen werden. Solange keine Inkonsistenzen auftreten, kann automatisch nicht festgestellt werden, dass ein Schluss falsch ist.

Unsicherheit in Frühwarnsystemen

Auch die Datengrundlage für Entscheidungen in Frühwarnsystemen ist vage, unsicher und unvollständig. Dies gilt sowohl für Menschen als auch für Maschinen. Fehler in Frühwarnsystemen sind z. B. durch spezielle Lichteffekte von Mond oder Sonne oder durch die Erfassung von Vogel-Schwärmen durch Radaranlagen entstanden.

Mit neuen technischen Möglichkeiten wird die Vielfalt an Sensordaten zur Erkennung eines Raketenangriffs wachsen. Auch die Vielfalt der Objekttypen, die zu erkennen sind, wird wachsen, z. B. durch eine zunehmende Anzahl an Objekten im Luftraum (Drohnen) und im Weltraum (Satelliten, Weltraumwaffen, Abwehrsystem). Zusätzlich können Kollisionen mit Weltraumschrott und ein Verglühen in der Erdatmosphäre Sensorsignale verursachen, die von den Frühwarnsystemen erfasst werden und schwer interpretierbar sind. Die Unsicherheit der Daten in Frühwarnsystemen wird also eher noch wachsen.

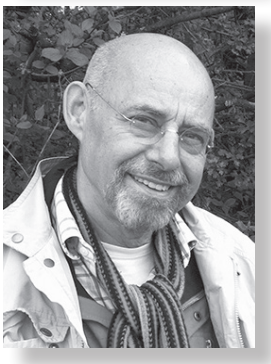
Bei der Bewertung von Sensorsignalen spielen auch vage Werte wie Helligkeit und Größe eine Rolle. Signale werden auch nicht immer auftreten, können also unvollständig sein. Dies kann insbesondere für neue lenkbare Raketensysteme gelten, die einer Erfassung ausweichen können. Des Weiteren sind für die elektronische Kampfführung Systeme wie *Kalaetron Attack* entwickelt worden, die es ermöglichen sollen, eine Erkennung durch die gegnerische Flugabwehr abzuwehren.[1] Im Falle einer Angriffsmeldung kann also nicht sichergestellt werden, dass die Daten auf Basis mehrerer unabhängiger Signalquellen überprüft werden können.

Kontextwissen

In Friedenszeiten und Phasen politischer Entspannung sind die Risiken relativ gering, dass die Bewertung einer Alarmmeldung zu einem atomaren Angriff führt. In solchen Situationen werden von menschlichen Entscheidern im Zweifelsfall Fehlalarme angenommen. Die Situation kann sich jedoch drastisch ändern, wenn politische Krisensituationen vorliegen, eventuell mit gegenseitigen Drohungen oder wenn in zeitlichem Zusammenhang mit einem Fehlalarm weitere Ereignisse eintreten. Hierfür werden bei einer Bewertung Ursachen gesucht, d. h. es wird versucht kausale Zusammenhänge zu finden. Wenn solche kausalen Zusammenhänge gefunden werden und logisch plausibel sind, besteht die große Gefahr, dass diese als gültig angenommen werden, d. h. dass die Alarmmeldung als gültig angenommen wird, auch wenn es um zufälliges zeitliches Zusammentreffen von unabhängigen Ereignissen geht.

Wenn die weltpolitische Lage und sonstige Kontextinformationen von automatischen Entscheidungskomponenten eines Frühwarnsystems nicht verwendet werden, dann sind Fehlalarme immer gefährlich, auch in Friedenszeiten. Wenn Komponenten von Frühwarnsystemen auch solches Kontextwissen für ihre Entscheidungen verwenden sollen, dann gilt auch hier, dass die Datengrundlage hochgradig vage, unsicher und unvollständig ist.

Die Bewertung der weltpolitischen Lage ist Gegenstand eines Projektes mit dem Namen *Preview*, das die Bundeswehr im März 2018 gestartet hat, mit dem Ziel, auf der Basis von Methoden der Künstlichen Intelligenz Krisen und Kriege vorherzusagen. Dazu sollen große Datenmengen automatisch analysiert werden. Ausgewertet werden hierbei Internet-Quellen sowie militärische und wirtschaftliche Datenbanken und auch Geheimdienstinformationen. Die Art der verwendeten Daten umfasst ein großes Spektrum, wozu auch Handelsdaten, Marktpreise, demographische Entwicklungen, Kriminalitätsraten, Meinungen in sozialen Netzwerken oder Daten über politische Gewalt gehören. Die KI-Plattform Watson soll u. a. eingesetzt werden, um solche Informationen zu verarbeiten und zu bewerten. Auch in anderen Staaten (z. B. Schweden, USA) gibt es solche KI-basierten Systeme zur Vorhersage von Krisen und Kriegen.[2]



Karl Hans Bläsius und Jörg Siekmann

Karl Hans Bläsius war bis 2017 Professor an der Hochschule Trier, Fachbereich Informatik. Fachgebiete: Logik, Funktionale Programmierung, Dokumentanalyse, Künstliche Intelligenz. Er beschäftigt sich mit Frühwarn- und Entscheidungssystemen und Atomkrieg aus Versehen seit 1983 und ist Mitinitiator der Seite *www.atomkrieg-aus-versehen.de*.

Jörg Siekmann, geb. 1941, war von 1991 bis 2006 Professor für Informatik und Künstliche Intelligenz an der Universität des Saarlandes und ist seitdem dort Seniorprofessor. Er promovierte 1976 in Artificial Intelligence an der University of Essex und wurde 1983 auf die erste deutsche Professor für Informatik und Künstliche Intelligenz an der Technischen Universität Kaiserslautern berufen. Er war maßgeblich beteiligt am Aufbau der KI-Forschung in Deutschland, ist Gründer und erster Sprecher der KI-Fachgruppe in der Deutschen Gesellschaft für Informatik (GI) und war Sprecher des SFB-378 Ressourcenadaptive kognitive Prozesse. Von 1991 bis 2006 war er Direktor des 1989 von ihm mitgegründeten Deutschen Forschungszentrums für Künstliche Intelligenz (DFKI) und war Koordinator der Universität des Saarlandes für Digitale Bildung. Er wurde 2019 von der GI zu einem der zehn einflussreichsten KI-Forscher gewählt.

Auch wenn solche Vorhaben wie das Projekt *Preview* sinnvoll zur frühzeitigen Erkennung von potentiellen Krisen, z. B. in Afrika, sein können und es derzeit keine Hinweise auf einen Zusammenhang mit Frühwarn- und Entscheidungssystemen für die Erkennung eines nuklearen Angriffs gibt, kann ein solcher Zusammenhang eintreten: Wenn ein Frühwarnsystem einen Raketenangriff meldet und diese Situation über mehrere Alarmstufen hinweg in den entsprechenden Krisensitzungen bewertet wird, ist es durchaus möglich, dass Kommissionsmitglieder auch Zugriff auf ein solches System zur Kriegsvorhersage haben. Wenn dieses KI-System in einer solchen Situation einen Krieg vorhersagt, kann dies erheblichen Einfluss auf die Bewertung der Alarmmeldung durch die Kommissionsmitglieder haben.

Entscheidungsvorschläge

In der deutschen Öffentlichkeit wird mit großer Übereinstimmung gefordert, dass Entscheidungen zur Tötung von Menschen nicht durch Maschinen erfolgen dürfen, sondern dass eine solche Entscheidung nur von Menschen getroffen werden darf. Solche Forderungen betreffen vorwiegend autonome Waffensysteme, aber sie müssen gleichermaßen auch für Gegenreaktionen auf Alarmmeldungen in Frühwarnsystemen gelten.

Auch wenn eine solche Forderung eingehalten wird, haben Menschen in der Regel wegen der kurzen Zeitspanne keine echte Entscheidungsmöglichkeit. Die einem maschinellen Entscheidungsvorschlag zu Grunde liegenden Informationen sind zu komplex, um diese in der kurzen verfügbaren Zeit (nur wenige Minuten) überprüfen zu können. Eine fachliche Beurteilung der von einem KI-basierten System getroffenen Entscheidungen durch Menschen ist in der kurzen verfügbaren Zeit praktisch unmöglich. Dies gilt schon deshalb, weil die automatische Erkennung oft auf Hunderten von Merkmalen basiert. Die automatischen Systeme können in der Regel keine einfachen nachvollziehbaren Begründungen liefern. Selbst wenn Erkennungsmerkmale von einem System ausgegeben werden, könnten diese nicht in der verfügbaren Zeit überprüft werden.

Dem Menschen bleibt deshalb meist nur zu glauben, was das System liefert.

Vergleich Entscheidungen Mensch – Maschine

Bestimmte Teilaufgaben von Frühwarnsystemen können nur mit Hilfe von automatischen Systemen gelöst werden. Aufgrund der schnellen Trägersysteme müssen automatische Systeme zur Klassifikation von Flugobjekten und der Bestimmung von Merkmalen, wie Geschwindigkeit, Höhe und Zielrichtung verwendet werden, ohne maschinelle Unterstützung wären Menschen überfordert.

Bei anderen Bewertungsaspekten, wie z. B. Plausibilität eines Angriffsmusters, Erwartungshaltung oder der politischen Weltlage, kann nicht grundsätzlich gesagt werden, ob automatische Entscheidungen besser sind oder die von Menschen. Dies kann von vielen Aspekten abhängen. Maschinen können in einem gegebenen Zeitintervall viel mehr Daten verwenden, Menschen haben derzeit sicher noch bessere Beurteilungsfähigkeiten.

Dazu zwei Beispiele, Beispiel 1:

> *Im Januar 2020 hatten die USA den iranischen General Soleimani mit einem Drohnenangriff getötet. Als Vergeltungsangriff hat der Iran wenige Tage später amerikanische Stellungen im Irak angegriffen. Kurz danach wurde im Iran ein ukrainisches Verkehrsflugzeug aus Versehen abgeschossen. Die Bedienungsmannschaft kam zu dem Ergebnis, dass es sich bei dem Flugobjekt um einen angreifenden Marschflugkörper handeln könnte. Die Fehlentscheidung kam vor allem dadurch zustande, dass die Bedienungsmannschaft mit Krieg oder einem Angriff der USA gerechnet hatte. In dieser Situation hätte eine Maschine möglicherweise besser entschieden, denn die reinen Fakten, wie Größe des Radarsignals, hätten vermutlich gegen einen Marschflugkörper gesprochen. Vielleicht hätte eine Maschine in der Kürze der Zeit auch mehr Informationen, wie z. B. Flugpläne, berücksichtigen können. Die Bedienungsmannschaft hatte den politischen Kontext vermutlich überbewertet.*

Beispiel 2:

> *Ein Satellit des russischen Frühwarnsystems meldet am 26. September 1983 fünf angreifende Interkontinentalraketen. Da die korrekte Funktion des Satelliten festgestellt wurde, hätte der diensthabende russische Offizier Stanislaw Petrow nach Vorschrift die Warnmeldung weitergeben müssen. Er hielt einen Angriff der Amerikaner mit nur fünf Raketen aber für unwahrscheinlich und entschied trotz der Datenlage, dass es vermutlich ein Fehlalarm sei und verhinderte damit eine Katastrophe mit atomarem Schlag und Gegenschlag. Der Vorfall ereignete sich während einer instabilen politischen Lage: Die Nachrüstung durch Mittelstreckenraketen stand an und wenige Wochen vorher hatten die Sowjets aus Versehen eine koreanische Passagiermaschine über internationalen Gewässern abgeschossen. Möglicherweise hätte eine Maschine aufgrund der Fakten den Angriff eher als echt eingeschätzt und Gegenreaktionen eingeleitet. Petrow hatte gefühlsmäßig auf einen Fehlalarm gehofft, wollte nicht für den millionenfachen Tod von Menschen verantwortlich sein und hat sich entsprechend entschieden.*

Bei Entscheidungen des Menschen kann das Ergebnis unter anderem davon abhängen, wer gerade Dienst hat und wie die Grundeinstellung und momentane Verfassung desjenigen ist.

Bei Entscheidungen durch Maschinen kann das Ergebnis unter anderem abhängen von der Wahl von Merkmalen mit Prioritäten durch die Programmierer oder einer vorhandenen Datenbasis als Lerngrundlage. Bei der Festlegung von Merkmalen und Prioritäten durch Programmierer bzw. der Festlegung einer Lerngrundlage sind die Auswirkungen für bestimmte Alarmsituationen nicht abschätzbar.

Steigendes Risiko

Es ist zu erwarten, dass das Risiko eines versehentlichen Atomkriegs in den nächsten Jahren und Jahrzehnten stark steigen wird.

Fehlalarme in Frühwarnsystemen kommen regelmäßig vor, sie werden im Normalfall aber nicht bekannt. Bekannt geworden sind viele Vorfälle während der Kubakrise und zu Zeiten des *Kalten Krieges* zu Beginn der 1980-er Jahre, oft erst Jahrzehnte nach diesen Vorfällen. Ansonsten werden Fehlalarme bekannt, wenn sie irrtümlich an einen großen Empfängerkreis gehen, wie 2018 auf Hawaii[3] und im Dezember 2020 in Ramstein[4]. In der Vergangenheit gab es auch viele Fehlalarme, bei denen ein Massenangriff mit Atomraketen gemeldet wurde.

Es kann also davon ausgegangen werden, dass es auch in den kommenden Jahren und Jahrzehnten viele Fehlalarme in Frühwarnsystemen geben wird, auch solche, die Massenangriffe melden. Dies gilt auch deshalb, weil es heute deutlich mehr Atommächte gibt als in den 1980-er Jahren und diese auch Frühwarnsysteme haben oder aufbauen werden.

Wenn ein Massenangriff gemeldet wird, ist es vermutlich nicht sinnvoll, diesen nur mit einer oder wenigen Atomwaffen zu beantworten. Eine Gegenreaktion müsste auch mit vielen Atomwaffen erfolgen. Bei einem Atomkrieg aus Versehen besteht deshalb die Gefahr, dass viele Atomwaffen zum Einsatz kommen könnten, mit einem nuklearen Winter als Folge.

Der Klimawandel wird zu mehr Krisen führen und neue technische Entwicklungen werden die Komplexität von Frühwarnsystemen so stark erhöhen, dass die Beherrschung solcher Systeme immer schwieriger wird.

Der Klimawandel wird dazu führen, dass verschiedene Regionen unbewohnbar werden und damit vermehrt Klimaflüchtlinge verursachen. Der verfügbare Lebensraum wird kleiner, wichtige Ressourcen, wie zum Beispiel Wasser, werden knapper. Dadurch wird es in Zukunft häufiger politische Krisen und eventuell sogar kriegerische Konflikte geben. Als Folge werden Raketenangriffsmeldungen in Frühwarnsystemen deutlich gefährlicher.

In den letzten Jahren hat ein neues Wettrüsten in verschiedenen militärischen Dimensionen begonnen. Die meisten dieser Entwicklungen sind noch am Anfang und die Folgen kaum kalkulierbar. Dies gilt für neue Trägersysteme von Atomwaffen, wie Hyperschallraketen, die geplante Bewaffnung des Weltraums, den Ausbau von Cyberkriegskapazitäten und die zunehmende Anwendung von Systemen der Künstlichen Intelligenz bis hin zu autonomen Waffensystemen. Alle diese Aspekte spielen auch in Frühwarnsysteme zur Erkennung von Angriffen mit Atomraketen hinein und werden die Komplexität dieser Systeme deutlich erhöhen. Unkalkulierbar sind hierbei insbesondere potenzielle Cyberangriffe, wobei Komponenten oder Daten eines Frühwarnsystems manipuliert werden könnten.

Ein „Atomkrieg aus Versehen" ist nicht direkt vorhersehbar. Wie bei sonstigen Unfällen in technischen Systemen gibt es keine Vorwarnung. Ein Atomkrieg aus Versehen kann plötzlich innerhalb weniger Minuten als Folge einer Eskalationsspirale und falscher Einschätzungen geschehen. Die Gefahr einer mangelnden Beherrschbarkeit der Kategorie nuklearer Waffen sehen auch Lahl und Varwick aufgrund der gestiegenen Anzahl von Atommächten einerseits und immer ausgereifteren technischen Entwicklungen und komplexeren strategischen Entscheidungsfeldern andererseits.[5] Weitere Informationen enthalten die Internetseiten zu *Atomkrieg aus Versehen*.[6]

Fazit

Weder Menschen noch Maschinen können bei Alarmmeldungen in Frühwarnsystemen in so kurzer Zeit fehlerfrei entscheiden, da die Datengrundlage unsicher, vage und unvollständig ist und eine Überprüfung durch Menschen in der kurzen verfügbaren Zeit nicht möglich ist.

Es ist weder möglich, zu sagen, dass im Zweifelsfall Menschen die bessere Entscheidung treffen, noch gilt, dass im Zweifelsfall Maschinen die bessere Entscheidung treffen, aber:

Es darf nicht sein, dass von der Entscheidung eines einzelnen Menschen oder einer Maschine das Überleben der gesamten Menschheit abhängt. Deshalb ist der Ansatz, Frühwarnsysteme zu verwenden, um frühzeitig Atomangriffe zu erkennen und eventuell einen Gegenangriff zu starten, bevor die gegnerischen Raketen einschlagen, grundsätzlich untragbar, unabhängig davon, ob letztendlich Menschen, Maschinen oder eine Mischform aus beidem entscheiden. Diese Problematik kann durch den Einsatz von KI-Technologien nicht behoben werden.

Anmerkungen

1 *Behördenspiegel, Mai 2020, Seite 45, https://issuu.com/behoerden_spiegel/docs/2020_mai*
2 *Süddeutsche Zeitung, 23.7.2018, Seite 5 und 9.10.2018, Seite 16*
3 *https://www.heise.de/newsticker/meldung/Hawaii-Raketenalarm-war-keine-Fehlbedienung-sondern-Absicht-3956046.html*
4 *https://edition.cnn.com/2020/12/14/politics/russia-missile-drill-false-alarm-us-base/index.html*
5 *Lahl, Varwick: Sicherheitspolitik verstehen, Wochenschauverlag, 2021*
6 *https://atomkrieg-aus-versehen.de/*

Die Antwort auf Rüstung und Krieg – mit oder ohne KI.
Foto: Ralf Cüppers 2019, CC-BY

Aaron Lye

Transformation geheimdienstlicher und militärischer Serverinfrastruktur in den USA durch kommerzielle Cloud-Provider am Beispiel Amazon

Das aktuell wichtigste Teilgebiet der Künstlichen Intelligenz (KI) ist Maschinelles Lernen (ML). Unter Verwendung statistischer Verfahren und Softwaretechniken wird ein Modell mit bekannten Daten trainiert, indem es Muster und Strukturen erkennt und anhand einer vorher definierten Logik daraus Schlussfolgerungen zieht, um dann für unbekannte Daten Vorhersagen zu treffen. Die Einsatzgebiete sind vielfältig: So können beispielsweise Objekte, Gesichter, Basisemotionen und Laufwege in Fotos und Videos identifiziert, Sprache erkannt und übersetzt, Spiele gespielt oder Daten klassifiziert und Anomalien erkannt werden. Das Training eines Modells erfordert allerdings genügend Daten und Rechenleistung.

Lange war ML ein akademisches Thema. Aber selbstverständlich haben die Entwicklungen in diesem Bereich bei Geheimdiensten und Militärs früh Interesse geweckt. Seit einigen Jahren ist die Nachfrage nach dieser Technologie in vielen Bereichen der Gesellschaft groß. Viele Unternehmen versprechen sich durch sie Profite. Staaten versuchen, gesellschaftliche Probleme durch sie zu „lösen".

Die Problematik um KI ist bekannt – wird aber weitgehend ignoriert. Zu nennen sind beispielsweise die Fehleranfälligkeit, Verzerrungen, Automation-Bias oder auch Intransparenz durch Black-Box-Algorithmen.

Die große Nachfrage nach komplexer Mathematik und Software im Bereich ML wird durch immer einfacher nutzbare Implementierungen ermöglicht und bedient. Insbesondere sind die Softwarebibliotheken von Facebook (*PyTorch*) und Google (*TensorFlow*) zu nennen. Cloud-Provider liefern in der Regel entsprechende Infrastruktur, indem sie on-demand Cloud-Dienste eines Rechenzentrums über das Internet anbieten, von Festplattenspeicher über virtuelle Server bis hin zu höheren Softwarefunktionen. Was als *Software-as-a-Service* (SaaS, also Software, die zentral auf einem Server läuft und dezentral von Clients genutzt werden kann) begann, ist mittlerweile zu *Platform-as-a-Service* (PaaS, vereinfacht gesagt: Cloud-Instrastruktur für Entwicklung) und *Infrastructure-as-a-Service* (IaaS, vereinfacht gesagt: einfaches Verwalten von skalierbarer Server-Infrastruktur, Speicher und Rechenleistung) gewachsen. *Machine-Learning-as-a-Service* (MLaaS) wird inzwischen von allen großen Cloud-Anbietern angeboten. Das System *Rekognition* von Amazon ist eines der bekanntesten Beispiele. Die Technik wird damit wesentlich mehr Unternehmen, Behörden und Institutionen zugänglich, die zuvor aufgrund mangelnder Größe oder Expertise nicht mit ML arbeiteten.

Amazon Web Services (AWS) ist der profitabelste Geschäftsbereich des Mutterkonzerns Amazon und wird von Branchenanalyst:innen als Marktführer im Bereich Cloud Computing angesehen. Nach Schätzungen der Synergy Research Group hat Amazon im Jahr 2021 einen Marktanteil von 32 % (im Vergleich: Microsoft Azure 20 %, Google Cloud 9 % und IBM Cloud 5 %). Der Jahresumsatz der Branche beträgt 150 Mrd. US $. Außerdem ist AWS der dominierende Cloud-Anbieter für US-Bundesbehörden, die US-Geheimdienste und das US-Verteidigungsministerium (Department of Defense, DoD).

Inspiriert durch einen Artikel von Schelling[1] aus dem Jahr 2019 soll im Folgenden exemplarisch an Amazon die Zusammenarbeit von kommerziellen Cloud-Anbietern des Silicon-Valley mit US-Geheimdiensten und *DoD* aufgezeigt werden.

Commercial-Cloud-Services für Geheimdienste

Seit fast einem Jahrzehnt speichert der US-Nachrichtendienst *National Security Agency* (NSA) Daten, einschließlich Signaldaten und anderer Überwachungs- und Geheimdienstinformationen, welche die Agency aus verschiedenen Quellen rund um den Globus bezieht, in einem intern betriebenen Data-Lake, einer riesigen Datensammlung, die Analyst:innen der NSA und anderer Geheimdienste abfragen und analysieren können.

Der *War on Terror* legitimierte die massive Ausweitung, das Abfangen, Speichern und Auswerten von Kommunikations- und Metadaten weltweit als auch erhebliche Budgeterweiterungen. Das Ausmaß und insbesondere die Techniken sind durch die Leaks von Edward Snowden im Jahr 2014 bekannt geworden.

Die gewaltige Zunahme von Daten war ein technisches Problem, welches durch einfaches Hinzufügen weiterer Server nicht behoben war. Im Jahr 2010 entschied die NSA deshalb ihre Daten zu zentralisieren und Cloud Computing umzusetzen, um ihren Analyst:innen möglichst viele Informationen einfach zugänglich zu machen. Wichtiger Teil des Vorhabens war es aber auch, der *Intelligence Community* (IC), also anderen US-Geheimdiensten, die Daten und Dienste zugänglich zu machen.

Als Unternehmen des privaten Sektors begannen, die Cloud für billigeres, skalierbares *On-Demand-Computing* zu nutzen, betrachtete die NSA diesen Ansatz als die beste Möglichkeit, den massiven Datenzuwachs zu verwalten. Im Jahr 2010 entschied sich die NSA für die Cloud als *Repository of Choice* – ein gemeinsamer Raum, in dem alle Analyst:innen den gesamten Datenbestand der gesammelten Informationen der Behörde durchsuchen können.[2]

Das 1,5 Mrd. US $ teure Rechenzentrum der NSA in Bluffdale, Utah, veranschaulicht den Umfang der Bemühungen. Dabei handelt es sich im Wesentlichen um einen 1 Million Quadratmeter großen Speicher für Signalinformationen, der ausdrücklich für die Erfassung digitaler Daten konzipiert wurde.

Lange Zeit bestand die private Cloud der NSA aus zwei parallelen Clouds. Die erste war eine interne Cloud, auf welche die Mitarbeiter:innen der NSA zugreifen konnten. Die zweite, *GovCloud* genannt, war für die Geheimdienstgemeinschaft über das *Joint Worldwide Intelligence Communications System* verfüg-

NSA Data Center in UTAH
Foto: ParkerHiggins (Electronic Frontier Foundation) taken by an employee of the Electronic Frontier Foundation during an airship flight. CC0 1.0

bar. Mit der GovCloud fungiert die NSA als Cloud-Service-Anbieter für andere Geheimdienstbehörden und ermöglicht ihnen, Dienste wie Datenverarbeitung und Analysen zu bestellen.

Diese parallelen Clouds wurden Ende 2015 zusammengeführt, um die Belastung durch die Wartung getrennter Systeme sowie die Abhängigkeit der Behörde von unterschiedlichen Datenbanken zu beseitigen.

Als Parallelentwicklung unterzeichnete der US-Auslandsgeheimdienst *Central Intelligence Agency* (CIA) im Jahr 2013 einen Vertrag, den sogenannten *Commerical Cloud Service* (C2S) contract, mit AWS für eine Cloud. In ihm sollte Amazon mit der Implementierung von Cloud Computing bei der CIA und anderen *Intelligence Agencies* (Geheim- und Nachrichtendiensten) beginnen. Zunächst hatte nur die CIA ihre Serverinfrastruktur umgestellt. 2014 bekamen die anderen 16 Geheimdienste Zugriff auf die AWS-Hardware hinter Firewalls der Geheimdienste. Die Projektlaufzeit beträgt 10 Jahre und soweit bekannt beträgt das Auftragsvolumen 600 Mio. US $. AWS sollte eine Vielzahl von Cloud Computing-Services bereitstellen. Amazon erhielt dafür alle Sicherheitsfreigaben, um Daten bis hin zum Top-Secret-Level zu hosten und zu verarbeiten. Dies ermöglichte es den Geheimdiensten, diverse Datenquellen, wie Kommunikation oder Bilder aus Kameras und von Satelliten, in einem neuen und einzigen Framework zusammenzubringen, zu verarbeiten und insbesondere auch mit kommerziellen KI-Methoden Vorhersagen zu treffen.[3] Im November 2017 gab AWS die sogenannte *Secret Region* offiziell bekannt.

Seitdem hat die IC diese Beziehungen kontinuierlich ausgebaut. Das Folgeprojekt von C2S wurde bereits im November 2020 begonnen. Strategisch wurde entschieden, zu diversifizieren. So hat die CIA den geheimen *Commercial Cloud Enterprise* (C2E) *contract* an fünf der größten Cloud-Service-Provider, namentlich AWS, Google, IBM, Microsoft and Oracle, vergeben.[4] Diese sollen sowohl Cloud Hosting Capabilities für die 17 Intelligence Agencies als auch SaaS bereit stellen. Es ist davon auszugehen, dass damit auch MLaaS gemeint ist. Diese fünf Unternehmen konkurrieren jetzt um spezifische Aufträge für bestimmte geheim- und nachrichtendienstliche Nachfragen. Die Vertragslaufzeit beträgt 15 Jahre. Die Vertragssumme wurde von der CIA geheimgehalten. Mutmaßlich beträgt die Summe mehrere 10 Mrd. US$.

Die NSA GovCloud und die von AWS entwickelte C2S-Cloud (jetzt diversifiziert in der C2E-Cloud) der CIA bilden zusammen die wesentliche Cloud-Infrastruktur für die geteilten Daten der Geheimdienste. Beide Clouds vereinfachen es, Analysetools aus- und maschinengestützte Datenfusion und Big-Data-Analysen durchzuführen. Insbesondere werden durch die Anbindung an die kommerziellen Clouds neben den ML-Funktionen der CIA und der NSA weitere Funktionen zugänglich, die von den Unternehmen entwickelt wurden. Von Anfang an war klar, dass die interoperablen Clouds Daten teilen, um eine zunehmende Vielfalt von Anfragen der Geheimdienste abzudecken.[5]

2020 wurde bekannt, dass die NSA ebenfalls einen kommerziellen Cloud-Anbieter hinzuziehen wolle, um den Anforderungen gerecht zu werden, die sich aus dem exponentiellen Datenwachstum und den massiven Verarbeitungs- und Analyseanforderungen ergeben.[6] Die Details sind spärlich, aber die Akquisition ist Teil des Vorstoßes der NSA, die GovCloud zu modernisieren. Das Projekt mit der Bezeichnung *Hybrid Compute Initiative* soll die Geheimdienstdaten der NSA von ihren eigenen Servern auf Server eines kommerziellen Cloud-Anbieters verlagern. Im Juli 2021 wurden dann weitere Details bekannt. Die NSA hatte den hochklassifizierten Auftrag *WildandStormy* im Umfang von 10 Mrd. US $ für die Umstrukturierung der Cloud-Infrastruktur zunächst an AWS vergeben.[7] Die Existenz des geheimen Vertrags wurde öffentlich, weil Microsoft gegen die Entscheidung Berufung einlegte (Solicitation Number H98230-20-R-0225). Das *Government Accountability Office* wies daraufhin die NSA an, die Vergabe durch eine Reevaluierung der vorgelegten Konzepte der Unternehmen zu prüfen. Tut die NSA dies nicht, so soll sie die Gründe vor dem Nationalen Kongress erklären.

Kurz danach, im September 2021, wurde öffentlich, dass die NSA weitere 2 Mrd. US $ für einen Hochleistungsrechner ausgibt. Gewinner des sogenannten *Greenlake High-Performance Computing Contract* ist *Hewlett Packard Enterprise*.

Aber nicht nur in den USA unterhält Amazon Verträge mit Geheimdiensten. Die Financial Times berichtete kürzlich, dass AWS einen Cloud Contract gewonnen hat, um Top-Secret-Daten für die Britischen Geheimdienste zu hosten[8]. Teil des Vertrages ist, dass AWS ein „Hoch-Sicherheits-Cloud-System" für die *Government Communications Headquarters* (GCHQ) bereitstellen soll. Dieses soll auch vom Britischen Inlandsgeheimdienst *Security Service* (*Military Intelligence Section* 5, MI5) und Auslandsgeheimdienst *Secret Intelligence Service* (SIS, *Military Intelligence Section* 6, MI6) genutzt werden. Der *Single Vendor Cloud Contract* soll bis zu 1.4 Mrd. US $ über die nächste Dekade Wert sein. Die Daten sollen im Vereinigten Königreich verbleiben und AWS soll keinen Zugang zu den Daten erhalten.

Commercial-Cloud-Services für das Pentagon

Da die AWS Secret Region auch Behörden und Institutionen der US-Regierung zur Verfügung steht, welche nicht zu den US-Geheimdiensten zählen, die aber über einen angemessenen Netzwerkzugang der Geheimhaltungsstufe Secret verfügen, begann im März 2018 dem *DoD* unterstellte *Transportation Command* seine Daten in die Secret Region zu migrieren. Wenig später migrierte auch das *National Ground Intelligence Center*, welches

Informationen über feindliche Bodenkräfte sammelt und auswertet, seine Daten.[9] Seitdem sind viele Daten der Streitkräfte dorthin migriert und Cloud-Dienste von AWS werden rege genutzt.

Auch Google arbeitete zeitweise mit dem Pentagon an dem umstrittenen *Project Maven*. Offiziell stieg das Unternehmen nach massiven Mitarbeiter:innenprotesten im April 2018 aus dem Vorhaben aus.[10] Ziel des US-Militärprojekts war das Erkennen von Zielen mittels Künstlicher Intelligenz, um Drohnenoperateur:innen die Überwachung und das Töten zu erleichtern. Insbesondere sollten Objekte (Autos, Gebäude, Menschen) erkannt und klassifiziert werden.[11] AWS soll weiterhin daran beteiligt sein. Foreign Policy meldete, dass Maven bereits an mindestens fünf geheimen Standorten in der Praxis getestet werde.[12] Der Mittlere Osten und Afrika werden explizit genannt.

Wegen dieser engen Verbindungen und entsprechenden Zertifizierungen für das Hosting und die Verarbeitung von Top-Secret-Dokumenten galt Amazon als unangefochtener Favorit bei der Vergabe des nächsten großen Projekts des Pentagons, der *Joint Enterprise Defense Infrastructure* (JEDI), welches im Jahr 2019 ausgeschrieben wurde. Das Volumen des Vertrages wird auf 10 Mrd. US $ geschätzt. Allerdings dürften die daraus entstehenden Profite deutlich höher liegen. Ziel des Projekts ist der Aufbau einer Cloud-Infrastruktur für das Pentagon. Beworben hatten sich wieder AWS, Microsoft, Google, IBM und Oracle. Aber nur eines der Unternehmen konnte für den Single Vendor Cloud Contract die Zusage bekommen. Nachdem Google (angeblich wegen der Proteste) die Bewerbung zurückzog und im April 2019 berichtet wurde, dass IBM und Oracle nicht weiter als Kandidaten für die Realisierung des Projekts einbezogen werden, blieb es spannend, ob die Entscheidung zugunsten von Amazon oder Microsoft ausfällt.[13] Nachdem zwischenzeitlich der Auftrag an Microsoft vergeben wurde und Amazon gegen diese Entscheidung klagte, hat sich das DoD dazu entschieden, den JEDI-Auftrag zu annulieren. „Das Projekt […] entspräche nicht mehr den Bedürfnissen des Militärs", erklärte das Pentagon. Kurzerhand wurde ein *Multiple Award Contract* mit dem Projektnamen *Joint Warfighting Cloud* ausgeschrieben, in dem sowohl AWS als auch Microsoft als Cloud-Provider agieren können.[14] Das Pentagon adressierte öffentlich direkt neben AWS und Microsoft auch Google, IBM und Oracle als Vertragspartner. Die New York Times berichtete, dass Google sich für das neue Projekt neu bewarb.[15]

Wo Amazon-Chef Jeff Bezos sich und sein Unternehmen in den sich verschärfenden Großmachtkonflikten verortet und welche Rolle er der Zusammenarbeit zwischen High-Tech-Unternehmen und dem Militär beimisst, untermauerte er 2019 in aller Deutlichkeit. In seiner Rede auf dem *Reagan National Defense Forum* in Kalifornien (einem Treffen von US-Militärführern und Verteidigungsunternehmen) warnte er insbesondere vor dem wachsenden Einfluss Chinas und vor einem Verlust der technologischen Vormachtstellung der USA weltweit. Bezos machte klar, dass er bereit sei, seine Dienste anzubieten: „Wir werden das Verteidigungsministerium unterstützen. Dieses Land ist wichtig."[16]

Fazit

Seit fast einer Dekade findet eine gravierende Verlagerung geheimdienstlicher und militärischer Daten in die Cloud kommerzieller Anbieter statt. Die Beziehungen von Big-Tech zu Geheimdiensten und Pentagon wurden über Jahrzehnte aufgebaut. Nachdem sich vor allem der Marktführer AWS in dem Aufbau, dem Umzug und der Etablierung positioniert hatte, ist jetzt eine deutliche Diversifizierung bemerkbar.

Der Artikel konzentriert sich auf das Treiben von Amazon. Das ist durchaus sinnvoll, weil AWS aktuell eine besondere Stellung innehat. Dennoch ist die Darstellung unvollständig und ein Zerrbild der eigentlichen Situation. Viele weitere Akteure und Entwicklungen hätten benannt werden müssen – anderes ist aufgrund der Tatsache, dass es sich um geheimdienstliche und militärische Angelegenheiten handelt, nicht bekannt.

Es ist festzuhalten, dass die in diesem Artikel diskutierten Projekte nicht einfach nur weitere und neue Kommunikations- und Infrastrukturprojekte der Geheimdienste und des Pentagons sind. Stattdessen zeigen sie auf, dass die Großkonzerne des Silicon-Valley eine wesentliche Rolle in der Kriegsführung spielen. KI-gestützte Kriegsführung (von der Auswertung immer mehr Sensordaten um militärische Gesamtsituationen zu erfassen, logistische und taktische Optimierung sowie automatisierte Entscheidungen von Truppenbewegungen und Angriffen) wird forciert und machbar.

Anmerkungen

1 *Arkadi Schelling. Künstliche Intelligenz als Cloud Service: Folgen für Gesellschaft, Geheimdienst und Militär. IMI-Analyse 16/2019*
2 *Frank Konkel. NSA Turns to the Cloud to Help Manage Data Deluge. 14. November 2014. Nextgov*
3 *Frank Tonkel. The Details About the CIA's Deal With Amazon. 17.07.2014. The Atlantic.*
4 *Ross Wilkers. CIA makes awards for intelligence community's next massive cloud contract. 20 November 2020. Washington Technolgy*
5 *Frank Konkel. NSA 'Systematically Moving' All Its Data to The Cloud. 6. Juni 2018. Nextgov.*
6 *Frank Konkel. NSA Awards Secret $10 Billion Contract to Amazon. 10. August 2021. Nextgov.*
7 *Nick Wakeman. NSA told to rethink $10B cloud award to Amazon Web Services. 29 Oktober 2021. Washishington Technology*

Aaron Lye

Aaron Lye ist Informatiker. Er hat als Doktorand an der Universität Bremen gerade seine Dissertation über Fusionsgrammatiken und Reaktionssysteme abgeschlossen, gefördert mit einem Promotionsstipendium der Rosa-Luxemburg-Stiftung. Weitere Interessengebiete sind Kryptographie und Quantum Computing. Seit 2013 ist er Mitglied im Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF).

8 *John Hewitt Jones. AWS inks cloud contract with UK spy agencies. FEDSCOOP. 26 Oktober 2021. (Sekundärquelle, Primärquelle ist nicht zugänglich)*

9 *Frank Konkel. Another Defense Agency to Tap CIA's Commercial Cloud. 31.05.2018. Nextgov.*

10 *Jürgen Wagner. Maven: Geheime Standorte. IMI-Aktuell 2019/138. 25. Februar 2019*

11 *Fang, Lee; „Google Is Quietly Providing AI Technology for Drone Strike Targeting Project", The Intercept, 06.03.2018.*

12 *Lara Seligman. No, the Pentagon Is Not Working on Killer Robots—Yet. 13. Februar 2019. Foreign Policy*

13 *Jürgen Wagner. JEDI: Microsoft vs. Amazon. IMI-Aktuell 2019/217. 12. April 2019*

14 *Jürgen Wagner. JEDI: Microsoft vs. Amazon (II). IMI-Aktuell 2021/372. 7. Juli 2021*

15 *Daisuke Wakabayashi und Kate Conger. Google Wants to Work With the Pentagon Again, Despite Employee Concerns. 3. November 2021. New York Times*

16 *Jürgen Wagner. Amazon: Tech-Geopolitik. IMI-Aktuell 2019/698. 10. Dezember 2019*

Vorkriegsnotizen

*von **Krysztof Daletski***

1

Die Regierung erklärt, sie will investieren:
zusätzlich dreißig Milliarden pro Jahr
ins Militär.

Freuen dürfen sich schon
die Hochschulen auf Forschungsgelder,
die Konzerne auf Rüstungsaufträge,
die Jugendlichen auf Karrieren
in der Armee.

Bestens gerüstet werden wir sein
für den kommenden Krieg.

Aber: wie wäre es denn,
wenn wir nicht investierten
und der Krieg bliebe aus?

2

Die Stimmung der Truppe wird wieder besser.

Nach all diesen Jahren des Sparens.
Nicht mal ein zünftiger Feind.
Immer nur hocken in der Kaserne,
das ist doch nicht attraktiv für Soldaten.

Endlich wird investiert
in Ausrüstung und Personal.
Aufwärts geht es nun wieder.
Allenthalben ist Aufbruchstimmung.

Bin ich der einzige, den das beunruhigt?
Und der sich fragt: wohin
die Truppe wohl aufbricht?

3

Nicht nur Soldaten, auch Informatiker,
Ingenieure und Journalisten
sind jetzt gefragt.

Angestrengt sitzen sie vor den Monitoren.
Äußerste Sorgfalt erfordert die Arbeit

an der Software der Fernlenkwaffe:
Ein Fehler im Code und Orte bleiben unzerstört;

an der Sensorik der Wärmebildkamera:
Ein falsches Signal und Fremde bleiben ungetötet;

an der Kampagne zur Rechtfertigung:
Ein falsches Wort und das eigene Volk
bleibt ohne Hass.

Krysztof Daletski

Krysztof Daletski ist ein Liedermacher vom Niederrhein (*http://songs.dalitio.de*).

Christoph Marischka

KI und der Risiko-Kapital-Staat

Das Ökosystem der V2

Unter dem Titel *Peenemünde – Die Geschichte der V-Waffen* beschreibt Walter Dornberger die Entstehung und den Betrieb jener Heeresversuchsanstalt, welche er als Generalmajor der deutschen Wehrmacht kommandiert hat. Wenn der Ort sich heute als „Wiege der Raumfahrt" darstellt, so blendet dies zwar den primären Zweck und die unmittelbare Wirkung der dortigen Entwicklung – eine Revolutionierung und Entgrenzung der Kriegführung – aus, ist aber sachlich auch richtig. Wie der technische Leiter der Versuchsanstalt, Wernher von Braun und auch dessen Stellvertreter, Eberhard Rees, ging Dornberger nach der bedingungslosen Kapitulation der deutschen Wehrmacht in die USA und war dort weiter in der Raketenentwicklung für die NASA und die Rüstungsindustrie tätig. Rees schreibt in seinem Geleitwort zum oben genannten Buch, dass sowohl „die russischen Sputnik-Satelliten Ende der fünfziger Jahre" als auch „die amerikanische Explorer-Serie […] mit Raketen in eine Umlaufbahn um die Erde gebracht [wurden], die auf der Technologie des A4, also der Rakete V2 basierten."[1]

Dornberger beschreibt in seinem Buch ausführlich, wie über Jahre verschiedene Raketenöfen in verschiedenen Versuchsständen erprobt, unterschiedliche Materialien und Anordnungen, unterschiedliche Treibstoffe, Mischungsverhältnisse, Methoden der Einspritzung, Zerstäubung, Kühlung, Stabilisierung, Steuerung usw. ausprobiert wurden. Technologie-Entwicklung ist eben keine (reine) Wissenschaft, sondern auch ein ständiges Versuchen und Scheitern. Dazu wurde auf der Versuchsanstalt eine umfassende Infrastruktur geschaffen mit eigenen Kraftwerken, Flughäfen, Messständen, Windkanal, Fertigungsstätten, Sauerstoffwerk, KZ-Außenlagern, Fernwärmeleitungen und der dritten S-Bahn in Deutschland. Darüber hinaus waren neben der Wehrmacht (Heer und Luftwaffe) sowohl führende Unternehmen wie AEG, Siemens usw. eingebunden, als auch kleine und mittelständische Unternehmen, die einzelne Komponenten (z. B. Raketenöfen, Messgeräte, Stabilisierungskreisel, Brems- und Fallschirme) lieferten, für die es sonst kaum einen oder noch gar keinen Markt gab. Auch an verschiedenen Universitäten wurden Einzelkomponenten entwickelt und Modelle entworfen. Heute würde man dies ein *Ökosystem* nennen. Eher am Rande spricht Dornberger auch von „Angebern, Scharlatanen und Semiwissenschaftlern", welche „mit Übertreibungen und Phantasieangaben operierten", um sich auf dem Feld zu etablieren.

KI-Ökosysteme

In der sogenannten *Künstlichen Intelligenz* werden aktuell auf verschiedensten Feldern massive Fortschritte versprochen und erwartet, unter anderem im Gesundheitswesen, der Landwirtschaft, der Energieversorgung, der *Mobilität der Zukunft* und natürlich und vor allem auch der Konsumgüterindustrie und der Unterhaltungselektronik. Im Bereich der *Inneren Sicherheit* kommen KI-Verfahren bereits unter anderem bei der Visa-Vergabe, der Gesichtserkennung an Grenzübergängen, bei der Überwachung von Sammelunterkünften und im Asylverfahren (z. B. KI-gestützte Dialekterkennung) zur Anwendung.[2] Auch die Streitkräfte weltweit erwarten sich von KI künftig massive Vorteile in unterschiedlichsten Bereichen. Diese reichen von der automatisierten Lagerlogistik und vorausschauenden Wartung, der medizinischen Versorgung und autonomen Transportsystemen über die Entscheidungsunterstützung auf strategischer (z. B. Krisenfrüherkennung durch „Beobachtung" sozialer Netzwerke) und taktischer (sogenannte *combat clouds*) Ebene, die sogenannte Strategische Kommunikation (*Chat-Bots* zur Rekrutierung, Erkennung von *Fake News*), die Erkennung von Cyber-Angriffen bis hin zur Zielerkennung und zu autonomen Waffensystemen und Schwärmen.[3]

Es besteht somit ein breites Interesse in verschiedenen politischen und industriellen Kreisen zur (Weiter-)Entwicklung Künstlicher Intelligenz. Anders als in Peenemünde, wo die konkreten Spezifika (Maße und Transportfähigkeit, Reichweite, *Nutzlast* in Form von Sprengladung usw.) des A4 bzw. der V2 früh definiert waren, ist dieses Interesse bislang relativ unspezifisch. Es soll einfach an KI geforscht und in KI und entsprechendes Humankapital investiert werden. Wo sich dann tatsächlich Vorteile hieraus gewinnen lassen oder tatsächlich *Disruptionen* entstehen werde sich dann zeigen – und zwar in Form marktfähiger Produkte, die auf eine Nachfrage treffen bzw. diese generieren. Hierbei sollen Startups und mit ihnen verbunden Risikokapital eine zentrale Rolle spielen. Das gilt für zivile Märkte ebenso wie den Rüstungsmarkt. Entsprechende Maßnahmen, Institutionen und Strukturen, die zur Schaffung eines entsprechenden Ökosystems beitragen können und sollen, werden im folgenden anhand einiger Beispiele dargestellt.

Das Programm der letzten Bundesregierung

Bereits das Programm der letzten (schwarz-roten) Bundesregierung war vor allem auch ein technologiepolitisches Programm, welches unter der Chiffre der *Digitalisierung* und *Künstliche Intelligenz* für verschiedene gesellschaftliche Probleme (wie das Gesundheitssystem, Pflegenotstand, Klimawandel) technologische Lösungen in Aussicht stellte. Um schnell zu marktfertigen Produkten zu kommen, waren quer durch verschiedene Politikbereiche verschiedene Maßnahmen vorgesehen. Bereits in der einleitenden Zusammenfassung unter dem Titel *Eine neue Dynamik für Deutschland* werden unter anderem *„[s]teuerliche Forschungsförderung"* und „eine Allianz für schnelleren Transfer von Forschungsergebnissen in marktfähige Produkte" angekündigt. Hierfür war unter anderem vorgesehen, „Forschungscampi aus[zu]bauen", in „ausgewählten Forschungsfeldern […] starke Anreize für die Zusammenarbeit der Forschungs- und Wissenschaftseinrichtungen [zu] setzen", „Konzepte für Zukunftscluster [zu] entwickeln und um[zu]setzen sowie rechtliche Barrieren für Wissenschaftskooperationen ab[zu]bauen". Auch sollte „die direkte Forschungsförderung des Bundes stärker auf den Wissens- und Technologietransfer in die Wirtschaft [ausgerichtet]" werden. Außerdem wurden „neue

Instrumente zur Förderung von Sprunginnovationen“ sowie – unter der Überschrift *Für eine modern ausgerüstete Bundeswehr* – die Gründung einer *Agentur für Disruptive Innovationen in der Cybersicherheit und Schlüsseltechnologien* angekündigt.

Als zentrale Elemente der angestrebten Anwendung von Forschung in Produkten werden auch hier Startups hervorgehoben, zu deren Förderung ebenfalls ein breites Maßnahmenbündel vorgesehen war, unter anderem, indem man „den Zugang zu der Forschungsförderung für Startups deutlich erleichter[t]“, „Startups und Gründungen aus der Forschung“ fördert und sich auf europäischer Ebene für „eine einheitliche Europäische Startup Definition einsetz[t], um spezielle zielgenaue Fördermaßnahmen zu ermöglichen“ und „Rahmenbedingungen [schafft], die Unternehmen und Startups eine unbürokratische Skalierung von digitalen Geschäftsmodellen ermöglich[en]“. Zu Startups im High-Tech-Bereich gehört jedoch auch viel Risikokapital. Das wusste auch die Bundesregierung und hielt im Koalitionsvertrag fest: „Wir brauchen in Deutschland eine deutliche Ausweitung des Volumens des Wagniskapitalmarktes, um insbesondere Unternehmen in der Wachstumsphase zu unterstützen“. Hierzu kündigte man an, „die Bedingungen für Wagniskapital weiter [zu] verbessern“, unter anderem durch eine Vereinfachung von „Besteuerungsverfahren“ und die „Einführung steuerlicher Anreize zur Mobilisierung von privatem Wagniskapital über die bisherigen Maßnahmen hinaus“. Darüber hinaus wollte man auch mehr „institutionelle Anleger für Investitionen in Startups“ mobilisieren und hielt fest: „An diesen Wagniskapitalfinanzierungen sollen sich Privatwirtschaft, öffentliche Hand, KfW [Kreditanstalt für Wiederaufbau] und europäische Finanzpartner beteiligen.“

Damit hat der Koalitionsvertrag wesentliche Forderungen übernommen, welche während der Koalitionsverhandlungen im Oktober 2017 in einer gemeinsamen Stellungnahme von Spitzenverbänden der Industrie und Forschung unter dem Titel *Wissenschaft und Forschung als Fundament unserer Zukunft weiter stärken* veröffentlicht wurde.[4] Kurz nach der Veröffentlichung dieser Stellungnahme wendete sich Max-Planck-Präsident Martin Stratmann unter dem Titel *Der Staat muss auch riskante Projekte fördern* über den Tagesspiegel an die Öffentlichkeit. Darin warb er für die Einrichtung einer Agentur nach dem Vorbild der Forschungsförderung des Pentagon: „Es lohnt ein Blick in die USA: Dort werden solche Innovationsprojekte über die Defense Advanced Research Projects Agency (DARPA) sehr wirkungsvoll umgesetzt. So hat DARPA maßgeblich das Internet entwickelt und die Kommerzialisierung des Positionsbestimmungssystems GPS ermöglicht. Voraussetzung für den Erfolg: Autonomie, Verzicht auf politische Steuerung, Rekrutierung herausragender Projektmanager, und: eine Kultur, die Scheitern gestattet und damit die Voraussetzung schafft für den eigentlichen Erfolg. Auch wir sollten mehr die Chancen im Risiko sehen!“[5]

Sowohl die gemeinsame Stellungnahme als auch Stratmann im Tagesspiegel betonen zwar die Bedeutung von Startups bzw. „hoch risikoreiche[r] Projekte und Geschäftsmodelle“, schweigen aber weitgehend zur impliziten Rolle von Risikokapital und den hierfür zu schaffenden Rahmenbedingungen. Umso mehr hervorgehoben wird diese hingegen in einer Publikation unter dem Titel *Artificial Intelligence – A strategy for European startups*, welche die „Unternehmensberatung“ Roland Berger gemeinsam mit dem Risikokapitalfonds Asgard 2018 veröffentlicht hat. Um eine zur USA und China wettbewerbsfähige Position zu erlangen, solle die europäische Politik Startups als wichtigste technologische und wirtschaftliche Triebkräfte der KI fördern. „Dies erfordert eine tiefgreifende Änderung der Form des öffentlichen Engagements im Innovationsökosystem und die Anpassung von Förderprogrammen speziell für Startups.“ Gefordert werden auch hier (auf europäischer Ebene) Steuererleichterungen für Forschung und Risikokapital, die Einrichtung einer Agentur nach dem Vorbild der DARPA und umfangreiche öffentliche Investitionen in riskante Investitionen. Vor allem aber zielt das Papier auf Maßnahmen ab, die öffentliche Mittel als Hebel und Absicherung für private Investitionen wirken lassen sollen: „Europa hat keine andere Wahl, als seine Finanzierungsquellen für Innovationen massiv zu diversifizieren und private Beteiligungsfonds, Investmentbanken, Pensionsfonds und Staatsfonds einzubeziehen.“[6]

Cyber-Agentur und SprinD

Den seit Jahren immer wieder erhobenen Forderungen nach einer deutschen DARPA kam die Bundesregierung, wie im Koalitionsvertrag angekündigt, nach. Einerseits gründete sie im gemeinsamen Verantwortungsbereich des Innen- und des Verteidigungsministeriums die sogenannte Cyber-Agentur als bundeseigene GmbH mit Sitz in Halle (Saale).[7]

Laut einem Bericht des im Verteidigungsministerium angesiedelten Aufbaustabs der Agentur besteht deren Aufgabe in der „zielgerichtete[n], am Bedarf der inneren und äußeren Sicherheit orientierte[n] Beauftragung“ von „Forschungseinrichtungen durch staatliche Einrichtungen“. Hierzu „analysiert“ sie die „Innovationslandschaft“. Nach den Worten des Gründungsdirektors Igel soll sie „Forschung stimulieren und koordinieren“: „Es geht um Forschungsfragen, die zum Beispiel das Bundeskriminalamt, die Bundespolizei, die Marine, die Luftwaffe haben könnten.“ Als Handlungsfelder identifizierte der Aufbaustab „unter anderem die Quantentechnologie, Künstliche Intelligenz oder alternative Rechnerarchitekturen“. Konkreter benannt werden unter anderem „DNA-basierte“, „organisch-elektrochemische“ sowie „neuromorphe und neuronale Architekturen“. Konkret werden auch „Autonomie und Entscheidungsfindung“ und „Lagebilder und Lagebilddarstellung“ sowie Sensorik als Forschungsthemen genannt. „[A]bhängig vom Schwerpunkt des spezifischen Programms“ ist dabei vorgesehen, dass die Agentur „Programmbüros an anderen Standorten in Deutschland“ einrichtet. „Dabei handelt die Cyberagentur bewusst als Wagniskapitalgeber und schließt nicht aus, dass sich manche beauftragten Forschungen und Entwicklungen als Irrweg erweisen.“

Parallel hierzu wurde im benachbarten Leipzig, ebenfalls als bundeseigene GmbH, die „Bundesagentur für Sprunginnovationen“ (SprinD) gegründet. Gründungsdirektor Rafael Laguna de la Vera, der selbst als Investor und Unternehmer tätig war, beschreibt deren Aufgabe so: „Wir nehmen die Projekte, die zu groß und zu riskant sind, wo ein normaler Finanzinvestor vielleicht nicht gut beraten ist, zu investieren. Wir entwickeln sie zu einem Grad, wo dann Business Angels [Finanzinvestoren] auch einsteigen können und auch sollen.“

Künstliche Intelligenz in den Landstreitkräften

2019 veröffentlichte das Amt für Heeresentwicklung ein *Positionspapier* zum Thema *Künstliche Intelligenz in den Landstreitkräften*. Es stellt ein Ergebnis des Formats *Technology meets Capabilities* dar, einer Workshopreihe, die dem Austausch zwischen dem Heer, „der Forschung und der Industrie" dienen soll. In ihm werden nicht nur fünf zentrale *Handlungsfelder* (Anwendungsbereiche von KI) benannt (Bildanalyse, taktische unbemannte Systeme, Führung, Material und Infrastruktur, Analyseverfahren), sondern auch sechs *Treiber* (T1-T6), die „nicht beeinflusst oder vermieden werden" könnten – Sachzwänge sozusagen, die im wesentlichen mit wachsendem Tempo und Datenmengen begründet werden und damit, wie sie potentiellen Feinden Vorteile verschaffen könnten (die man als Bundeswehr stattdessen lieber selbst realisieren will). Die grundsätzliche Logik wird bereits als T[reiber]1 dargestellt: „Ein gegnerischer Einsatz von KI-basierten Komponenten kann zu Fähigkeitslücken des Heeres führen." Jede antizipierte Fähigkeit des Gegners sollte also zuvor selbst erlangt werden oder es sollten zumindest Abwehrmechanismen zur Verfügung stehen.

Unter T2 (*Zunehmende Dynamik des Gefechtes*) wird antizipiert, dass KI dazu beitrage „in Gefechten mit erhöhter Dynamik schneller, zielgerichteter und effektiver führen und agieren zu können" während T5 (*Zunehmende Informationsmenge und -dichte*) unterstellt, „KI erlaubt eine möglichst effektive und effiziente Nutzung von Information und sichert somit die Informations- und Führungsüberlegenheit beim Umgang mit einer hohen Menge von Daten unter hohem Zeitdruck". T6 (*Zunehmende Dynamik in der IT-und KI-Entwicklung*) wirkt zunächst eher als Wiederholung von T1, nämlich dass „Rüstungskonzerne potentieller Gegner an der Entwicklung KI-gestützter Waffensysteme arbeiten […]. Die sich daraus ergebende Erosion eigener Fähigkeiten führt über die Zeit zu einer deutlichen Bedrohungszunahme." Befürchtet und zugleich vorbereitet wird als „zentrales Element der zukünftigen Gefechtsführung" der „Hyperwar", „die Kombination klassischer Gefechtsführung mit Wellen von Cyberangriffen und Angriffen durch große Mengen automatisiert und autonom gesteuerter Systeme".

Es geht also um Tempo bzw. Dynamik und das nicht nur auf dem Schlachtfeld, sondern auch in der Forschung, Entwicklung und Implementierung. „In stark automatisierten und autonomen Systemen definiert sich die Überlegenheit ganz wesentlich über die Qualität der Algorithmen, der Rechenleistung und den Grad der Miniaturisierung […]. Da diese Komponenten praktisch komplett auf Dual-Use beruhen, bestimmt die Geschwindigkeit der zivilen Entwicklungen auch das Tempo des Wettrüstens im internationalen Umfeld."[8]

„Move Fast and Break Things"

Der *Cyber Innovation Hub* (CIH) der Bundeswehr bezeichnet sich als alles mögliche: „Do-Tank", „das digitale Schnellboot für unsere Streitkräfte", „erste militärische digitale Innovationseinheit in Europa", Bindeglied zwischen „agilem Startup-Mindset" und der Bundeswehr. Eingerichtet wurde er schon 2017 – noch unter Verteidigungsministerin von der Leyen im Zuge der Aufstellung des Organisationsbereiches und Kommandos der Bundeswehr für den Cyber- und Informationsraum – in einer Fabriketage in Berlin mit vielen Paletten, Vintage-Möbeln und „Raum für Ideen". Ziel war es explizit, eine Schnittstelle zwischen militärischer Kultur und Denken einerseits und jener Kultur zu schaffen, wie man sie für die Startup-Szene, Entrepreneure und Risiko-Kapitalgeber:innen imaginiert: jung, divers, leger und extravagant. Dieses Spannungsfeld bestimmt auch die Außendarstellung des CIH: Auf der Homepage wird man geduzt und die Bilder von den Veranstaltungen suggerieren ein ungezwungenes Miteinander von Uniformierten und lässig gekleideten Zivilist:innen in bewusst unaufgeräumt und spontan wirkenden Arrangements von Sitzgelegenheiten. Hier darf man auch mal Fehler machen oder zumindest übertreiben, z. B. mit einem auf Facebook veröffentlichten Mime des CIH, welches das Bild eines zugleich fahrenden und schießenden Panzers mit dem Motto von Mark Zuckerberg verband: „Move Fast and Break Things."

Ziel ist es ganz offenkundig, sich an die Startup-Szene anzubiedern und dieser die Bedürfnisse des Militärs mitzuteilen. Auf der anderen Seite sollen auch das Militär und Beschaffungswesen transformiert werden: Weg von komplizierter, hierarchischer und langfristiger Planung, die alle Eventualitäten einbeziehen und jeden Fehler vermeiden will, hin zu flachen Hierarchien, rascher Entscheidungsfindung und Bereitschaft zu Risiken und Scheitern.

Eines der vielen Veranstaltungsformate des CIH ist die sogenannte *Smart Solutions Challenge*. Dabei sind Angehörige der Bundeswehr aufgerufen, Produkte zu entwerfen und anschließend als *Intrapreneure* zu agieren. Umgesetzt wird dies offenbar nach dem Vorbild der Fernsehshow *Die Höhle des Löwen*. Bei der letzten Runde der Challenge wurden aus zunächst 85 Vorschlägen von Angehörigen des CIH und der Bundeswehr-Universitäten elf Projekte ausgewählt, die weiterkamen. Kriterium war hier unter anderem „ob die Projekte schnell zu realisieren

Foto: Stephan Röhl, CC BY-SA 2.0

Christoph Marischka

Christoph Marischka ist Mitglied im Vorstand der Informationsstelle Militarisierung e. V. und aktiv im *Bündnis gegen das Cyber Valley*. Aus seiner Auseinandersetzung mit diesem KI-Forschungscluster ging auch das Buch *Cyber Valley – Unfall des Wissens* hervor.

sind". Anschließend erhielten die dahinterstehenden Teams bzw. *Intrapreneure* vom CIH Unterstützung bei der weiteren Ausarbeitung – darunter Kontakt zu jenen Dienststellen, bei denen eine spätere Verwendung des Produkts möglich wäre – sowie ein *Pitch-Coaching*, um sie auf die Präsentation vor der Jury vorzubereiten. Diese dauerte letztlich drei Minuten, wobei die Jury anschließend noch fünf Minuten Zeit hatte, Nachfragen zu stellen. Als Vertreter:innen der Privatwirtschaft gehörten der Jury Uwe Horstmann (*Founding Partner Project A Venture Capital*), Vera Schneevoigt (*Chief Digital Officer bei Bosch*) und Deepa Gautam-Nigge (*Global Lead SAP Next-Gen Ecosystem*) an. Drei Projekte wurden schließlich ausgewählt und mit „den nötigen Ressourcen" ausgestattet.

Bundeswehrgeneral Alfons Mais, der seine Karriere vor allem bei den Heeresfliegern – unter anderem in Bosnien, Kosovo und Afghanistan – gemacht hat, gab im Juli 2021 dem Handelsblatt ein Interview, in dem er unter anderem „ethische Vorbehalte" im Hinblick auf „Robotik […] verknüpft mit Künstlicher Intelligenz" problematisierte. Das Interview endet mit der Positionierung: „Ich frage die Parlamentarier immer wieder: Wollen Sie sich junge Menschen Europas vorstellen, die zum Beispiel gegen chinesische Roboter kämpfen müssen?". Das im Thesenpapier des Amtes für Heeresentwicklung als T1 eingeführte Argument des Wettrüstens wird auch hier wieder mit dem Anspruch moralischer Überlegenheit ins Feld geführt: „Während wir noch über die ethische Dimension von Künstlicher Intelligenz diskutieren, haben potenzielle Gegner wie zum Beispiel China oder Russland diese Bedenken nicht."

Auch Mais kennt hierfür die Lösung: „Ich bin überzeugt, dass wir auch bei klassischen militärischen Problemen jetzt mit Startups zusammenarbeiten müssen […]. Es dauert einfach zu lange. Militärische Plattformen wie Panzer oder Hubschrauber sind heute fahrende und fliegende Computer. Da sind zehnjährige Innovationszyklen eigentlich nicht mehr akzeptabel […]. In Deutschland sind wir einfach zu risikoavers. Das wäre auch ein Vorteil an Startup-Kooperationen. Startups betreten den Markt schon mit einem anderen Risikobewusstsein, das wir nutzen, unterstützen und auch auf unserer Seite akzeptieren müssen, wenn dabei Ressourcen nicht zum Ziel führen."[9]

The Startup Nation

Mais wirbt auch für das israelische Modell der *Startup Nation*: „Das Militär in Israel beispielsweise hat eine unglaubliche Innovationskraft. Der Druck der permanenten Bedrohung sorgt dafür, dass alles wie in einer Brutkammer viel schneller geht. Und durch das riesige Reservistenkorps ist die Rückkoppelung zur Industrie viel besser." Auch Roland Berger und Asgard verweisen auf die Israel als Vorbild. Hier heißt es unter anderem: „Israel steht weltweit an dritter Stelle, was die Zahl der KI-Startups im Land angeht, und an erster Stelle, was die Zahl der KI-Unternehmen pro Einwohner angeht. Aufgrund von Bedenken hinsichtlich der nationalen Sicherheit wurde ein Schwerpunkt auf KI-Sicherheitsanwendungen gelegt. In der Tat basieren heute 30 Prozent des israelischen Grenzschutzes auf KI-Systemen." Auch die EU-Grenzschutzbehörde Frontex arbeitet mit mehreren Startups zusammen, die aus dem Umfeld des israelischen Militärs entstanden sind. So findet sich unter den sogenannten *Frontex Files* eine Präsentation des Unternehmens Seraphim Optronics, in dem es seine Überwachungssysteme ((M)UGI, (Mini-)Unattended Ground Imaging Sensors) vorstellt. Ein anderes, ebenfalls von ehemaligen Militärangehörigen gegründetes Startup, Windward, hat Frontex Lizenzen seiner Software verkauft, die KI-gestützt Daten aus dem Schiffsverkehr auswerten und Risikobewertungen vornehmen. Beide Unternehmen (und teilweise auch die dahinterstehenden Kapitalfonds) werden in einer Liste mit (aktuell) 67 Unternehmen und Forschungseinrichtungen aufgeführt, die auf unterschiedliche Arten in das EU-Grenzregime eingebunden sind, welche unter dem Titel *Border Business* auf dem Portal *migration-control.info* veröffentlicht wurde.[10] Dabei wird auch klar, dass das israelische Modell gar nicht so einzigartig ist oder zumindest längst Nachahmung findet. So wurde etwa auch das französische Unternehmen A-NSE von einem ehemaligen Vize-Admiral der französischen Marine gegründet und lieferte unter anderem für Frontex Überwachungszeppeline. Gerade im Hinblick auf KI-Anwendungen finden sich auf dieser Liste weitere Startups auch aus anderen Staaten, darunter Travizory Border Security aus der Schweiz, das KI-gestützt und auf Grundlage biometrischer Daten für Flughäfen und Visa-Behörden arbeitet und Reisende kategorisiert. Auch das niederländische Startup *Pandora Intelligence* hat Frontex schon seine Dienste angeboten und beschreibt sich selbst als Lieferant „der neuesten Generation von Analyse-Software für Polizeibehörden, Regierungen und Ministerien, Nachrichtenagenturen und -dienste, militärische Organisationen und Sicherheitsregionen."[11]

Wie auch Windward setzt Pandora Intelligence auf die KI-gestützte Auswertung von öffentlich zugänglichen Daten. Das Feld der Unternehmen, welche entsprechende Anwendungen – nicht nur in den Bereichen Verteidigung und Innere Sicherheit, sondern auch bei Gesundheitsanwendungen, Immobilien- und sonstigen Investitionsfonds – anbieten, ist nahezu unüberschaubar. Absehbar werden zumindest nicht alle die geweckten Erwartungen erfüllen können und dauerhaft Abnehmer finden. Öffentliche Auftraggeber wie Polizeien (oder eben Frontex) und im wachsenden Maße auch das Militär sind beliebte Referenzen, auch wenn sie oft nur kurzfristige Lizenzen im Rahmen der Marktsichtung erwerben. Auch die Zahl der (Risiko-)Kapitalfonds, die sich auf entsprechende Portfolios spezialisiert haben, ist in den vergangenen Jahren deutlich angewachsen. Über gute Kontakte z. B. in die Sicherheitsbehörden (aber auch ins Gesundheitswesen, Verkehrsministerium …) können sie ihren Schützlingen zumindest kurzfristig Aufträge verschaffen. Vieles spricht dafür, dass auch das reichlich dubiose Unternehmen *Augustus Intelligence* ein solches Geschäftsmodell verfolgte. Gegründet wurde es 2019 von einem ehemaligen Mitarbeiter von Roland Berger und Pascal Weinberger, einem Entrepreneur und mutmaßlichen Startup-Multimillionär, der jedoch bereits mehrfach zumindest der Hochstapelei überführt wurde. Aktionär der ersten Stunde und später auch einer der Direktoren war der ehemalige Verteidigungsminister zu Guttenberg; der ehemalige Verfassungsschutzpräsident Maaßen und der ehemalige BNP-Präsident Hanning hatten Aktienoptionen erhalten und wurden im Gegenzug als Berater geführt. Vermutlich wurde von ihnen erwartet, dass sie sich wie Guttenberg und Amthor bei der Bundesregierung um Unterstützung des Unternehmens bemühen, das angeblich über 100 Mio. US $ an Investitionen eingesammelt hatte und zwischenzeitlich mit bis zu 250 Mio. US $ bewertet wurde. Welche famosen KI-Anwendungen das Unter-

nehmen den umworbenen Ministerien anzubieten hatte, blieb allerdings bis zuletzt unklar. Im April 2021 meldete es schließlich Insolvenz an.

Dieses Schicksal droht der Investmentgesellschaft In-Q-Tel nicht, denn diese wird direkt aus dem Haushalt des US-amerikanischen Auslandsgeheimdienstes CIA finanziert. Nach Angaben des deutschen Verfassungsschutzes vergibt es „Risikokapital an junge Unternehmen, insbesondere im Bereich der Informationstechnologie“[12], wobei es offenbar darum geht, die entsprechenden Technologien für das US-amerikanische Militär bzw. die Geheimdienste zugänglich zu machen oder zumindest dem Zugriff Dritter zu entziehen. Ende 2020 war In-Q-Tel beim Dresdner Startup *Morpheus Space* eingestiegen, einer auf Antriebe für Nano-Satelliten spezialisierte Ausgründung der TU Dresden, die zuvor auf verschiedenen Ebenen Fördergelder aus der öffentlichen Hand erhalten hatte. Dies sorgte für Kritik von verschiedenen Seiten.

Dass öffentliche Gelder in private Profite überführt werden, indem Risiken sozialisiert und Gewinne privatisiert werden, ist jedoch eine zentrale Funktion des angestrebten Ökosystems und eine – gar nicht so neue – Form der politischen Steuerung technologischer „Innovation“.

Anmerkungen

1 *Walter Dornberger (2020) Peenemünde – Die Geschichte der V-Waffen. RhinoVerlag, Ilmenau 2. Auflage 2020.*

2 *Vgl. beispielhaft: Petra Molnar, Lex Gill (2018) Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System, https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf.*

3 *Einen sehr guten Überblick über diskutierte Anwendungsbereiche liefert z. B. das Programm der Tagung „Künstliche Intelligenz – Chancen und Risiken für die Bundeswehr“ der Studiengesellschaft der Deutschen Gesellschaft für Wehrtechnik mbH, einsehbar unter: https://www.dwt-sgw.de/fileadmin/redaktion/SGW-Veranstaltungen/2019/9F9_KI2/9F9_KI_Bw_Programm_281019.pdf*

4 *Die Stellungnahme findet sich unter: https://www.mpg.de/11543958/Stellungnahme-Wissenschaft-und-Industrie.pdf.*

5 *Martin Stratmann (2017) Der Staat muss auch riskante Projekte fördern, Tagesspiegel (18.10.2017), dokumentiert unter: https://www.mpg.de/11679923/der-staat-muss-auch-riskante-projekte-foerdern.*

6 *Asgard, Roland Berger (2018) Artificial Intelligence – A strategy for European startups, https://www.rolandberger.com/publications/publication_pdf/roland_berger_ai_strategy_for_european_startups.pdf.*

7 *Die folgenden beiden Absätze sind weitgehend gleichlautend einem anderen Text des Autors entnommen, der sich mitsamt der jeweiligen Quellen unter folgender URL finden lässt: https://www.imi-online.de/2020/07/02/ein-diskreter-dammbruch-der-ruestungsforschung/*

8 *Das Thesenpapier, aus dem alle Zitate in diesem Abschnitt entnommen sind, findet sich hier: https://www.bundeswehr.de/resource/blob/156024/d6ac452e72f77f3cc071184ae34dbf0e/download-positionspapier-deutsche-version-data.pdf.*

9 *Larissa Holzki (2021): Bundeswehrgeneral fordert: „Auch bei klassischen militärischen Problemen jetzt mit Start-ups zusammenarbeiten“, Handelsblatt.de (29.07.2021).*

10 *Siehe: https://migration-control.info/bobusi/.*

11 *Zitiert nach dem entsprechenden Eintrag in der „Border Business Liste“, siehe: https://migration-control.info/bobusi/pandora-inteligence (Stand 2.11.2021).*

12 *Bundestags-Drucksache 19/23509, https://dserver.bundestag.de/btd/19/235/1923509.pdf.*

Thomas Reinhold

Zur Rolle und Verantwortung der Informatik für die Friedensforschung und Rüstungskontrolle

Die Ursprünge des Internets, so wie wir es heute kennen, basierten auf der Idee eines Austauschs von Ideen, Informationen und Codes. Obwohl die technischen Konzepte bereits durch den Wunsch nach einem staatlichen und militärischen Kommunikationssystem motiviert waren, welches auch nukleare Angriffe überstehen konnte, waren ein Großteil der ohnehin wenigen Nutzer:innen Akademiker:innen und Wissenschaftler:innen. Im Laufe der Jahre entwickelten sie so eine Technologie, die den freien Informationsfluss unterstützt. Dabei sah es lange Zeit danach aus, als könnte sich diese Idee hin zu einem weltweit freien und zugänglichen Netz entwickeln. Seit einigen Jahren, spätestens jedoch seit der Entdeckung von Stuxnet im Jahr 2010, wissen wir jedoch, dass auch Militär und Geheimdienste den sogenannten Cyberspace als Domäne für ihre Zwecke entdeckt haben. Angesichts der Abhängigkeiten moderner Gesellschaften von IT-Diensten und den zugrunde liegenden Infrastrukturen ist es zweifelsohne notwendig, die nationale IT-Sicherheit zu fördern und militärische Abwehrkapazitäten in diesem Bereich aufzubauen. Allerdings zeigen die Snowden-Enthüllungen oder der UNIDIR-Cyber-Index[1], dass immer mehr Staaten den Cyberspace auch als militärische Domäne betrachten, in der sie offensive Fähigkeiten entwickeln (müssen) oder diese bereits einsetzen. So ist es bei den US-Streitkräften inzwischen Pflicht, dass jeder Einsatz im Feld durch eine eigene Cyber-Einheit begleitet wird, die für Aufklärung, strategische Unterstützung und offensive Operationen zuständig ist. Diese Entwicklung ist auch an Deutschland nicht vorbeigegangen, wo die Bundeswehr eine eigenständige militärische Einheit, das Kommando *Cyber- und Informationsraum* (KdoCIR), eingerichtet hat, welche ab diesem Jahr voll einsatzfähig sein soll[2]. Inwieweit dieses neue Kommando offensive Fähigkeiten entwickeln und einsetzen darf (und auch wird), ist allerdings trotz zahlreicher öffentlicher Nachfragen und parlamentarischer Debatten weiterhin offen. Vieles deutet jedoch darauf hin, dass die bereits bestehenden Fähigkeiten der Vorgänger-Einheit *Computer-Netzwerk-Operationen* für solche Zwecke weitergenutzt und ausgebaut werden.

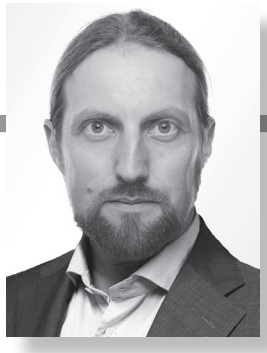
Wo militärische Kräfte in den Cyberspace vordringen, hat die internationale Gemeinschaft nach wie vor Schwierigkeiten, die in den letzten Jahrzehnten für die internationale Sicherheits-

und Außenpolitik entwickelten Regeln und Standards auf diesen neuen Bereich anzuwenden. Obwohl mittlerweile weitestgehend Einigkeit über die Gültigkeit des internationalen Völkerrechts auch im Cyberspace herrscht, bleibt die konkrete Anwendung dieser Normen oft unklar. Dies ist vor allem darauf zurückzuführen, dass der Cyberspace einige spezifische technische Merkmale aufweist, die sich stark von den bisherigen militärisch genutzten Domänen Luft, Wasser, Land und Weltall sowie deren technologischen und physikalischen Eigenschaften unterscheiden. So liegen beispielsweise der Cyberspace und die darin gespeicherten Informationen im Wesentlichen in virtueller Form vor. Auch wenn sich die Hardware einem bestimmten Standort zuordnen lässt, trifft dies nicht zwingend für die gespeicherten oder verarbeiteten Daten zu, insbesondere im Zeitalter des Cloud-Computing. Hinzu kommt, dass Software, wie alle anderen Daten, nahtlos dupliziert werden kann, sodass etablierte Maßnahmen der Rüstungskontrolle, welche auf dem Prinzip der Lokalisierung oder Quantifizierbarkeit beruhen, auf den Cyberspace nicht übertragbar sind. Die Virtualität und die zahllosen Möglichkeiten eines Angreifers, sich zu verbergen oder gar falsche Spuren zu legen, erschweren die Zurechnung von Cyberangriffen (Attribution), stellen jedoch eine zentrale Voraussetzung für jede nationale Selbstverteidigungsmaßnahme im Rahmen der UN-Charta dar[3]. Das letzte der offenkundigsten Beispiele für die technischen Besonderheiten des Cyberspace betrifft den ausgeprägten Dual-Use-Charakter von IT-Hard- und Software, der es erschwert, zwischen zu regulierender militärischer und zulässiger ziviler Nutzung betroffener Geräte zu unterschieden.

In Ergänzung zu diesen Schwierigkeiten ergibt sich eine weitere Herausforderung für die Sicherheit, Verfügbarkeit und Integrität der IT: die Nachfrage staatlicher Organisationen wie nationaler Nachrichtendienste, Strafverfolgungsbehörden oder der Streitkräfte an Schwachstellen in Hardware und Software zum Zwecke ihrer – zugegebenermaßen diskutablen – Aufgabenerfüllung. Neben Cyberkriminalität fördert diese Praxis die Entwicklung von Märkten für den Handel mit Sicherheitslücken und erhöht damit die Anreize, das Wissen über Schwachstellen zu verbergen und zu monetarisieren, anstatt es zur Stärkung der öffentlichen IT-Sicherheit offenzulegen. Die *EternalBlue*-Vorfälle im Zusammenhang mit den *WannaCry*[4]- und *NotPetya*[5]-Malware-Kampagnen, die immense wirtschaftliche Schäden verursachten, haben eindrucksvoll gezeigt, wie schnell sich ein solches Verhalten sowohl auf Wirtschaftssysteme als auch auf Zivilgesellschaften weltweit auswirken kann.

Aus Sicht der internationalen Sicherheit haben diese Entwicklungen der Militarisierung des Cyberspace zu einer Situation geführt, in der sich Streitkräfte einerseits zunehmend auf offensive Operationen in diesem Bereich vorbereiten. Andererseits fehlen gleichzeitig geeignete Maßnahmen, um diese Gefährdung der internationalen Sicherheit einzugrenzen oder überhaupt einschätzen zu können. Im Gegensatz zu konventionellen Waffen wie Raketen ist zum Beispiel noch unklar, wie der potenzielle Schaden einer Cyberwaffe gemessen oder kategorisiert werden kann. Dieses Ungleichgewicht hat zu nationalen Sicherheitsbedenken, unter anderem aufgrund von Vermutungen über das militärische Leistungsvermögen potenzieller Gegner, geführt und ein neues Wettrüsten mit Cyberwaffen ausgelöst, wodurch die internationale Lage zunehmend destabilisiert wird.

Dabei war die internationale Gemeinschaft in der Vergangenheit bereits mit solchen Situationen neuer technologischer Entwicklungen und deren „militärischer Vereinnahmung“ konfrontiert, wie im Fall von atomaren, biologischen und chemischen Waffen. Die politische Antwort auf diese Bedrohungen bestand stets in der Ausarbeitung von Vereinbarungen und Verträgen zur Eingrenzung der militärischen Nutzung dieser Technologien. Auch wenn dies oft langer Verhandlungsphasen bedurfte, in vielen Fällen mit Rückschritten und Enttäuschungen verbunden war und einige Probleme noch immer Gegenstand von Debatten und Auseinandersetzungen sind, so stellen derartige politische Maßnahmen wichtige Schritte auf dem Weg zu einer Rüstungskontrolle oder Nichtverbreitung von Waffen dar. Diese benötigen allerdings eine gemeinsame Grundlage für eine effektive Um- und Durchsetzung: Mittel zur gegenseitigen Kontrolle der Einhaltung jeglicher Art von Vereinbarungen. Bei diesen Verfahren der so genannten Verifikation handelt es sich um praktische Maßnahmen, die auf der Zählung, Messung oder Überwachung bestimmter technologischer Entwicklungen, Arsenale, Produktionsanlagen oder zuvor vereinbarter Limitierungen beruhen. Für das bekannteste Verifikationsregime ist die Internationale Atomenergie-Organisation (IAEO), eine internationale Organisation unter Führung der Vereinten Nationen, zuständig. Diese überwacht, unter anderem, das zivile Atomprogramm des Iran durch Besuche und Inspektionen von Kernkraftwerken und Anreicherungsanlagen, um so die Mengenbegrenzung von atomwaffenfähigem Kernmaterial zu kontrollieren. Wie bereits erwähnt, ist die Adaption derartiger Maßnahmen auf den Cyberspace aufgrund seiner spezifischen technischen Eigenschaften jedoch nicht möglich. Darüber hinaus ist es noch weitgehend unklar, ob alternative Verfahren existieren oder wie diese funktionieren könnten. Gleichsam verfügt der Cyberspace jedoch über einen wichtigen und einzigartigen Vorteil gegenüber allen früheren technologischen Entwicklungen: Er ist eine vollständig von Menschen geschaffene Domäne, deren „Naturgesetze“ von Informatiker:innen und IT-Praktiker:innen geschaffen und weiterentwickelt werden. Informatiker:innen setzen sich seit langem für IT-Sicherheit, Datenschutz und die Um-



Thomas Reinhold

Thomas Reinhold ist wissenschaftlicher Mitarbeiter und Doktorand am Fachgebiet Wissenschaft und Technik für Frieden und Sicherheit (PEASEC) der TU Darmstadt. Er befasst sich mit IT-gestützten Möglichkeiten für Rüstungskontrolle militärischer Aktivitäten im Cyberspace sowie den Problemen einer Militarisierung von Künstlicher Intelligenz.

setzung und Wahrung demokratischer Rechte in Software, Diensten und Infrastrukturen ein. Neben diesen Persönlichkeitsrechten erfordert die neue Situation bezüglich geheimdienstlicher und militärischer Akteure nun jedoch die Stärkung weiterer gefährdeter Werte, wie etwa des internationalen Friedens und der Sicherheit sowie der Unversehrtheit globaler IT-Infrastrukturen. Gleichzeitig müssen Maßnahmen wie die friedliche Nutzung und Weiterentwicklung der Domäne Cyberspace in den zugrunde liegenden technischen Systeme etabliert werden. So stellt sich beispielsweise die Frage, wie das Zerstörungspotenzial von *Cyber-Waffen* begrenzt oder geheimdienstliche und militärische Aktivitäten im Cyberspace transparent und kontrollierbar gestaltet werden können. Während Anonymität für Zivilist:innen im Cyberspace notwendig ist und geschützt werden muss, könnten militärische Netzwerke – also Teilsysteme, die in der Regel ohnehin bereits besonderen politischen Regeln unterliegen und aufgrund ihres spezifischen Zwecks stark reguliert sind – modifiziert werden, um Zugriffe auf fremde Netzwerke nachvollziehbar zu gestalten.

Diese Gedankenspiele führen zu einer sehr wichtigen Schlussfolgerung: Wenn es die Informatiker:innen sind, die den Cyberspace gestalten und seine zukünftige Entwicklung entscheidend mitbestimmen, dann sind auch sie es, denen in Anbetracht der oben beschriebenen Herausforderungen die Aufgabe der Entwicklung technischer Lösungsansätze zufällt. Der Schwerpunkt sollte darauf liegen, wie IT gestaltet werden muss, um eine friedliche und sichere Entwicklung des Cyberspace zu ermöglichen. Davon ausgehend ergibt sich eine Vielzahl von Fragen und Herausforderungen, die es zu lösen gilt: Wie können Rüstungskontrolle und Nichtverbreitungskontrolle von Cyberwaffen in der Praxis funktionieren? Wie könnten neue Ansätze zur Sicherung und Kontrolle der Entwicklung, des militärischen Einsatzes und der Nichtverwendung solcher Technologien aussehen, welche die Prinzipien etablierter Regeln und Normen für staatliches Verhalten in dieser Domäne abbilden? Welche messbaren Parameter und Eigenschaften gibt es für Software und Hardware, die für eine Dual-Use-Differenzierung herangezogen werden können? Lassen sich Kriterien finden, um potentiell eher unkritische, defensive Maßnahmen der Cyberverteidigung von solchen Maßnahmen oder Werkzeugen, die auch offensiv gegen Gegner eingesetzt werden, abzugrenzen? Und zu guter Letzt: Wie können Verifikationsmaßnahmen von militärischen Cyber-Fähigkeiten als Grundlage für Vereinbarungen und Verträge aussehen?

Vielleicht gibt es auf viele dieser Herausforderungen keine zufriedenstellenden Antworten. Aber es ist dringend geboten, diese Fragen anzugehen. Um es mit den Worten von J. F. Kennedy zu formulieren: „Wann, wenn nicht jetzt? Wer, wenn nicht wir?"

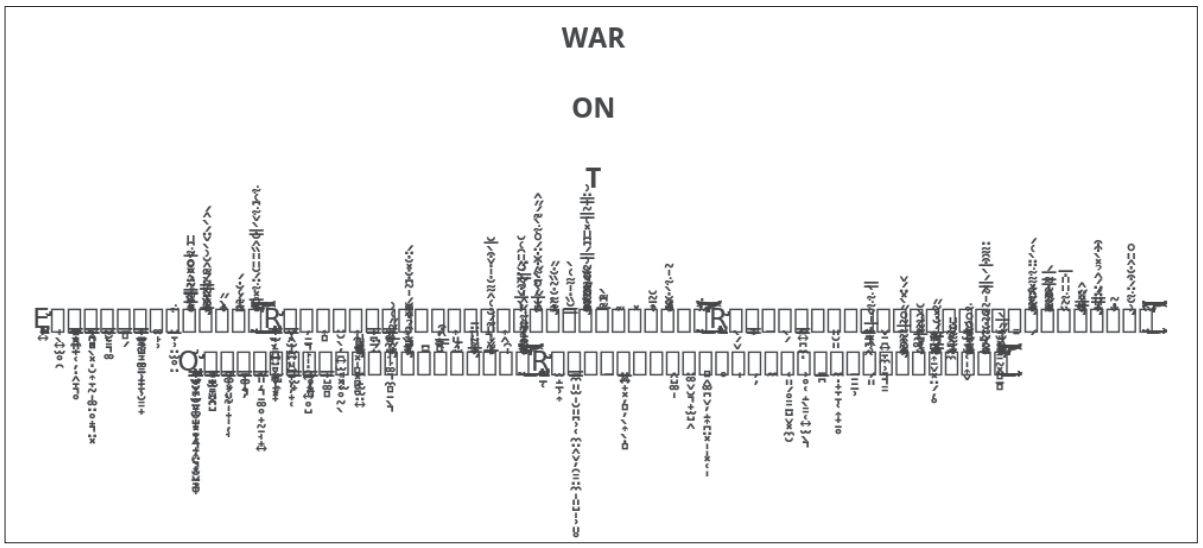
Anmerkungen

1 *Der Cyber-Index – Internationale Sicherheitstrends und Realitäten" http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf*
2 *https://www.bmvg.de/de/themen/cybersicherheit/cyber-verteidigung/entwicklung-des-org-bereich-bei-der-bw*
3 *Charta der Vereinten Nationen – http://www.unric.org/de/charta*
4 *Informationen zur EternalBlue-Sicherheitslücke und zur WannaCry-Schadsoftware-Kampagne https://cyber-peace.org/cyberpeace-cyberwar/relevante-cybervorfalle/wannacry-eternalblue/*
5 *Informationen zur NotPetya-Schadsoftware-Kampagne https://cyber-peace.org/cyberpeace-cyberwar/relevante-cybervorfalle/petya_notpetya/*

Christian Heck

War on Error

Am 15. August 2021 hatten die militant-islamistischen Taliban praktisch kampflos die afghanische Hauptstadt Kabul eingenommen. Niemand hat damit gerechnet, so Heiko Maas, Bundesminister des Auswärtigen, „*das war offensichtlich eine Fehleinschätzung, die die komplette internationale Gemeinschaft, auch ich und die Bundesregierung hatten*." In der Nacht zum 31. August 2021 verließ die letzte US-Militärmaschine das Land.



Viel zu lange richteten die Geheimdienste der NATO-Verbündeten ihre Blicke auf Zahlen, auf Graphendarstellungen, Heatmaps und Texte statt auf Menschen. Auf Listen und Datenbanken und statistische Auswertungen statt auf den Alltag und die Bedürfnisse gesellschaftlicher Subjekte. Viel zu lange richteten sie ihre Blicke auf Zahlen von Streitkräften, die sie ausbildeten, den Ausbildungsstand, den Ausrüstungsstand anstatt auf Gesellschaft und Kultur derer, die sie im Kampf gegen die Taliban auszubilden versuchten. Viel zu lange richteten sie ihre Blicke auf symbolische Repräsentationen von Menschen. Auf technische Bilder, Mobilfunktelefonnummern, GPS-Daten, auf softbiometrische Datensätze, Lebensmuster und Bewegungsprofile. Auf Daten und Technologien, die nun in nicht zu verachtenden Teilen in den Händen der Taliban liegen[1].

Gleich dem französischen Philosophen Grégoire Chamayou für sein Buch *Ferngesteuerte Gewalt – Eine Theorie der Drohne*[2] nehmen wir heute eine Reflexion der anarchistischen Philosophin Simone Weil in den 1930er Jahren als Leitfaden:

> *„Es wäre das denkbar unzulänglichste Vorgehen, sich dem Krieg und den Phänomenen der Gewalt von den Zielen her, die verfolgt werden, zu nähern, als vielmehr auf die durch die Art der eingesetzten Mittel notwendig implizierten Folgen zu untersuchen."*

So sehen wir uns die Waffen etwas genauer an. Ihre spezifischen Eigenschaften. Die Mittel und Wege, die Handlungen bestimmen, durch die man sieht und durch die man tut und die einen beim Denken helfen. Waffen, die letzten Endes auch die Wirkkraft der jeweiligen Handlungen mitbestimmen. Also die Übertragungen von Handlungswissen und Handlungsmacht in diese technischen Objekte hinein und von dort in uns zurück.

Wir fragen uns heute:

Wie wird der Mensch durch diese Technologien verdinglicht? Zu einer materiellen Sache, die benutzt, schlimmstenfalls zerstört werden kann? Zu einem Zeichen?

How to make human machine readable?

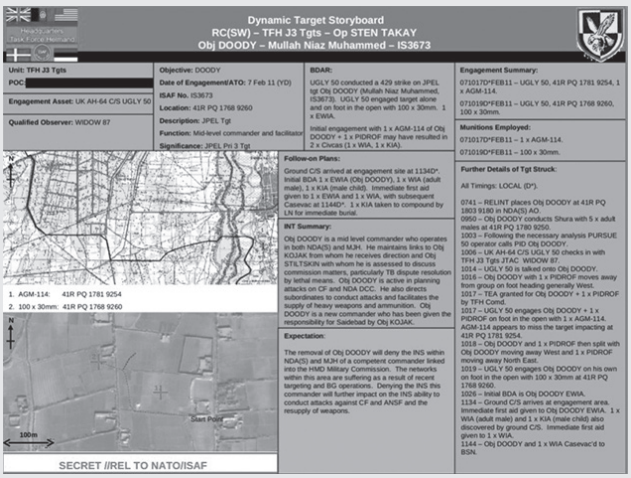
Wann wird Töten zu einer technisch-administrativen Maßnahme, wird Mensch zu einer Variablen, die durch eine weitere ersetzt, zu einer Konstanten, die ohne weiteres gelöscht werden kann?

Ab welchem Punkt tastet die Maschinenlesbarmachung gesellschaftlicher Subjekte die Würde des Menschen nicht nur ab, sondern an?

Die folgenden zehn Beispiele zeigen den Horror und die Perfidie von *War on Error*.

„Gorgon Stare Test uncovers Major Glitches The US Air Force's much-touted new Intelligence, Surveillance and Reconnaissance (ISR) System for use with remotely piloted Aircraft which is developed ***to be used in Afghanistan has significant operational glitches and is not ready to be fielded****, Air Force Field Testers conclude."*[3]

Bildquelle: „Gorgon Stares operational glitches", by Christian Heck

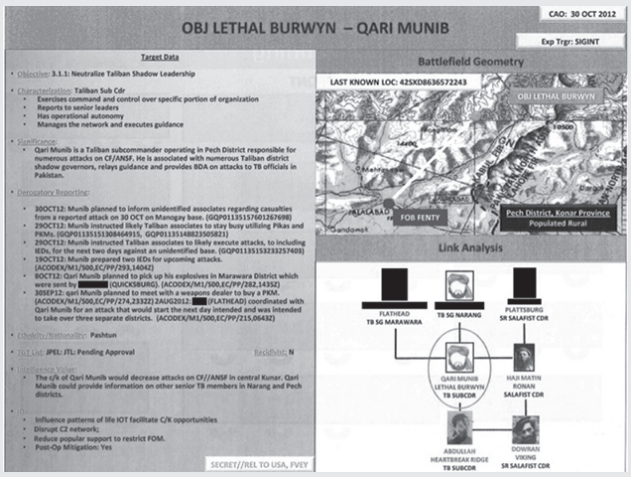


Mullah Niaz Muhammed bekam den Namen Doody, die ISAF No. IS3673 und er lebte in 41R PQ 1768 9260, bis zu seiner Ermordung in 41R PR 17897 92491 am 071017D*Feb11 durch eine UGLY 50 .AGM-114, bei welchem versehentlich auch ein KIA (ein kleiner Junge) getötet + 1 WIA (sein Vater) schwer verwundet wurde.

Bildquelle: „Ob DOODY – Mullah Niaz Muhammed – IS3673"[4]

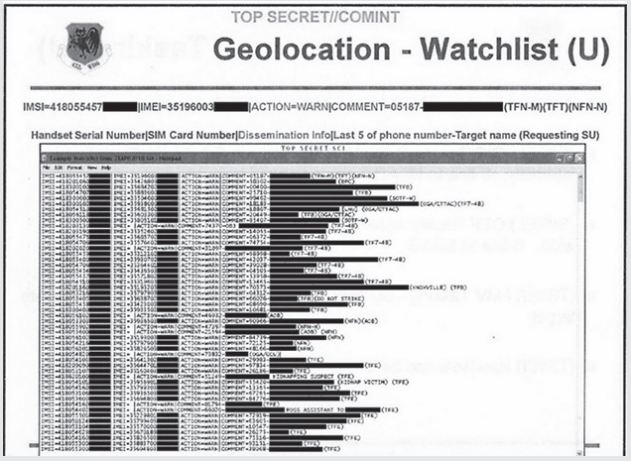
Bildquelle: U.S. Army Cyber Command

„Als bei einem Hubschrauberangriff im Februar 2011 dreiundzwanzig Gäste einer afghanischen Hochzeit getötet wurden, konnten die in Nevada auf Knöpfe drückenden Bediener der Aufklärungsdrohne die Schuld für ihren Irrtum auf die Informationsüberflutung schieben und sich darauf berufen, daß ihre Bildschirme mit Daten ‚vollgerotzt' würden – sie verloren den Überblick, gerade weil sie auf die Bildschirme schauten. Zu den Opfern des Bombardements gehörten auch Kinder, aber das Bedienpersonal ‚hatte sie inmitten des Strudels von Daten übersehen' – ‚wie ein Büroangestellter, dem in den täglichen Mailfluten eine dringliche Nachricht entgeht'. Und dem niemand vorwerfen könnte, daß er sich damit unmoralisch verhalten habe…"[5]



Die Informationen auf der *Baseball Card* und in dem Ordner über die Zielperson stammen vor allem von Geheimdiensten und können von den sie beurteilenden Menschen auch falsch interpretiert worden sein. „Das ist natürlich keine todsichere Methode", sagte die Quelle. „Man muss sich einfach darauf verlassen, dass die Computer und die Analysten beim Sammeln und Auswerten der vielen Daten und Informationen keine Fehler gemacht haben."[7]

Bildquelle: „Operation Haymaker"[6]



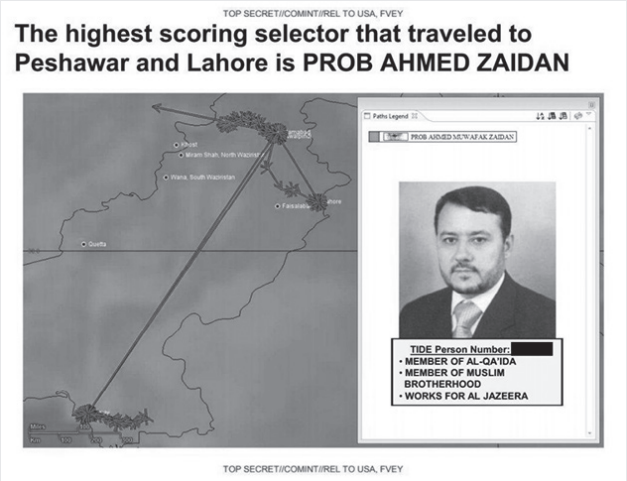
Bereits im letzten Jahr haben wir berichtet, dass die **US- Geheimdienste ihre Zielpersonen hauptsächlich über deren Mobiltelefone orten.** Mit dem Programm GILGA-MESH, das die Drohne zu einem „Sendeturm" macht, in den sich Mobiltelefone einloggen können, lässt sich die genaue Position der telefonierenden Person bestimmen. Die Grafik zeigt zeigt eine „Watchlist" (Überwachungsliste) von SIM-Card-Nummern.[9]

Bildquelle: „Geolocation Watchlist"[8]

*„Wenn jemand, der als hochwertige Zielperson galt, irgendwo in Somalia ins Telefon gesagt hätte, ‚Die Hochzeit ist in den nächsten 24 Stunden', wäre das für eine codierte Botschaft gehalten worden und hätte in Europa und in den USA die höchste Alarmstufe ausgelöst, auch wenn er uns nur verscheißern wollte", lästerte Flynn. „**Weil sich SIGINT ganz leicht austricksen lässt, muss es durch andere Erkenntnisquellen wie HUMINT (Aussagen von Informanten oder aus Verhören) verifiziert werden.** Man muss sicherstellen, dass man wirklich die gesuchte Person gefunden hat, denn **abgehört wurde ja nur ein Telefon.**"*[10]

In der von einer *Intelligence, Surveillance and Reconnaissance Task Force* (einer Sonderkommission zur Bewertung der Ergebnisse von Spionage, Überwachung und Aufklärung) des Pentagons erarbeiteten Studie werden die öffentlichen Erklärungen der US-Regierung über ihre Drohnen-Kampagne gegen hochrangige Terroristen, die eine akute Bedrohung für die USA darstellen sollen, teilweise bestätigt, teilweise wird ihnen aber auch widersprochen. **Es wird offen zugegeben, dass es nur sehr selten zur Festnahme von Terroristen kam und dass mit so genanten *Signature Strikes*[11] häufig unbekannte Personen nur wegen ihres „verdächtigen Verhaltens" umgebracht wurden.**[12]

Man nutze **Telefonnummern oder E-Mail-Adressen als Selektoren**, um die Kommunikation von Zielpersonen aus großen Datenströmen herauszufischen; **mit Hilfe der dadurch gewonnenen Informationen sei es dann möglich, diese Personen zu finden, anzuvisieren und umzubringen**. „Man muss schon sehr viel Vertrauen in die dabei eingesetzte Technologie haben", gab die Quelle, die *The Intercept*, die Leaks zuspielte, zu bedenken. **„Ich kenne unzählige Beispiele, bei denen die so gesammelten Informationen fehlerhaft waren."** Das sei der Hauptgrund für die Tötung unbeteiligter Zivilisten. **„Oft entdecken die mit überwachenden Geheimdienstler erst nach Monaten oder sogar Jahren, dass sie die ganze Zeit das Telefon der Mutter der Zielperson überwacht haben."**[13]



Bildquelle: „SKYNET: Courier Detection via Machine Learning"[14]

Ahmad Muaffaq Zaidan wuchs in Syrien auf. Er spricht fließend Arabisch und traf im Zuge einer Reportage Osama bin Laden im November 2000 in Kabul. Einige Monate später wurde er zur Hochzeit von bin Ladens Sohn in Kandahar eingeladen, über die er auch für das Fernsehen berichtete. Nach dem Einmarsch der USA in Afghanistan 2001 wurde Zaidan einer der wenigen Empfänger von Al-Qaida-Videobändern, die in den darauffolgenden zehn Jahren veröffentlicht wurden.

Nach der Logik des Random Forest (der SKYNET-Lern-Algorithmus) ist die Erkennung von Zaidan keineswegs irrtümlich gewesen, im Gegenteil, der Algorithmus hat so funktioniert wie er konzipiert wurde, er erzeugte einen rationalen Selektor auf Basis der Bewegungsmuster der *couriers*. Er lernte, Teile von Welt durch die Einwirkung von Zufälligkeit zu differenzieren, bzw. zu *klassifizieren*.

„We see how the war on terror in Afghanistan started and how it is ending now: It's with drones and civilian casualties", sagt der afghanische Journalist Emran Feroz in einem Interview mit *Democracy Now!* Bereits der allererste Angriff am 7. Oktober 2001 traf nicht Taliban-Chef Mullah Omar, sondern namenlose Afghanen, so Feroz weiter. „Dieses Szenario hat sich stets wiederholt. Bis heute."[15]

Bildquellen: Frames von „How a U.S. Drone Strike Killed the Wrong Person"[16]

Dienten die letzten Jahre in Afghanistan als Trial-and-Error-Zone zur Erforschung disruptiver Kriegstechnologien? Zahlreiche technische Fehler und militärische Fehlentscheidungen in dieser neuen Art des High Tech-Krieges legen diesen Verdacht nahe.

Fehler, die dem Design *disruptiver Technologien* immanent sind. Disruptive Technologien werden nicht mehr im Labor erprobt. Sie werden unausgereift in Gesellschaften hineingeworfen. Das ist es, was wir im Moment miterleben. Mitten unter uns findet ihr Trial-and-Error statt – im zivilen Raum, in Kriegsgebieten und in *Combat Zones. Dabei ist eine Combat Zone ein Gebiet, das vom US-Präsidenten per Executive Order als ein Gebiet bezeichnet wird, in dem US-Streitkräfte an Kampfhandlungen teilneh-*

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.

men oder teilgenommen haben. Afghanistan (und der darüber liegende Luftraum) wurde durch Executive Order No. 13239 ab dem 19. September 2001 als Combat Zone ausgewiesen.[17]

Etablierte sowie alt eingesessene Firmen setzen zur Leistungssteigerung ihrer bestehenden Produkte (im Sinne eines Fortschritts) auf (in der Gesellschaft) bereits erprobte Technologien, die *sustaining technologies*, so der US-amerikanische Wirtschaftswissenschaftler Clayton Christensen in seinem Buch *The Innovator's Dilemma* (1997). Disruptive Technologien bieten dem Markt ein anderes Wertversprechen. Start-Up-Unternehmen, die *Big* bzw. *New Tech Industries*, insbesondere die Eliten der Künstliche-Intelligenz-Forschung stellen im Vergleich zu nachhaltigen Technologien zwar schlechtere und unausgereifte Produkte her (im Sinne eines Rückschritts also), sie schaffen jedoch gänzlich andere Zielgruppen im Blickfeld und fördern gezielt traditionelle und Mainstream-Kunden im Umgang mit ihren Produkten.

Anmerkungen

1 *https://theintercept.com/2021/08/17/afghanistan-taliban-military-biometrics/*
2 *https://www.passagen.at/gesamtverzeichnis/thema-3/ferngesteuerte-gewalt/*
3 *Welsch, William. Gorgon Stare test uncovers major glitches. 24.01.2011. URL: https://defensesystems.com/articles/2011/01/24/gorgon-stare-test-shows-serious-glitches.aspx (letzter Zugriff 27.10.2021).*
4 *http://www.spiegel.de/international/world/secret-docs-reveal-dubious-details-of-targeted-killings-in-afghanistan-a-1010358.html*
5 *Bauman, Zygmunt. Daten, Drohnen, Disziplin. Berlin: Suhrkamp. 2013*
6 *Jung, Wolfgang. Ein Glossar mit Bildern, Dekodierung der Sprache des verdeckt geführten US-Drohnen-Krieges. 28.10.2015. URL: https://www.luftpost-kl.de/luftpost-archiv/LP_13/LP20015_281015.pdf. Übersetzung des Artikels »A Visual Glossary« von Josh Begley, The Intercept, 15.10.2015. URL: https://theintercept.com/drone-papers/a-visual-glossary/ (letzter Zugriff 27.10.2021)*
7 *https://theintercept.com/document/2015/10/14/operation-haymaker/*
8 *Jung, Wolfgang. Ein Glossar mit Bildern, Dekodierung der Sprache des verdeckt geführten US-Drohnen-Krieges. 28.10.2015. URL: https://www.luftpost-kl.de/luftpost-archiv/LP_13/LP20015_281015.pdf. Übersetzung des Artikels »A Visual Glossary« von Josh Begley, The Intercept, 15.10.2015. URL: https://theintercept.com/drone-papers/a-visual-glossary/ (letzter Zugriff 27.10.2021)*
9 *https://theintercept.com/document/2015/10/14/geolocation-watch-list/10 Jung, Wolfgang. Feuern auf Verdacht, Fehler der Geheimdienste und die Grenzen der Drohnen-Technologie. 06.11.2015. URL: https://www.luftpost-kl.de/luftpost-archiv/LP_13/LP20015_281015.pdf. Übersetzung des Artikels »Firing Blind« von Cora Currier und Peter Maass, The Intercept, 15.10.2015. URL: https://theintercept.com/drone-papers/firing-blind/ (letzter Zugriff 27.10.2021)*
11 *http://www.luftpost-kl.de/luftpost-archiv/LP_13/LP01613_030213.pdf*
12 *Jung, Wolfgang. Die Befehlskette für die gezielten Tötungen, Die tödliche Bürokratie hinter Obamas Drohnen-Krieg. 30.10.2015. URL: https://www.luftpost-kl.de/luftpost-archiv/LP_13/LP20115_301015.pdf. Übersetzung des Artikels »The Kill Chain« von Cora Currier, The Intercept, 15.10.2015. URL: https://theintercept.com/drone-papers/the-kill-chain/ (letzter Zugriff 27.10.2021)*
13 *Jung, Wolfgang. Der Mordkomplex. Aus geheimen Militärdokumenten geht hervor,wie Obamas Drohnen-Krieg abläuft. 26.10.2015. URL: https://www.luftpost-kl.de/luftpost-archiv/LP_13/LP19915_261015.pdf. Übersetzung des Artikels »The Assassination Complex« von Jeremy Scahill, The Intercept, 15.10.2015. URL: https://theintercept.com/drone-papers/the-assassination-complex/ (letzter Zugriff 27.10.2021)*
14 *https://theintercept.com/document/2015/05/08/skynet-courier/*
15 *Amy Goodman. U.S. Winds Down Afghanistan Occupation Like It Began, with Drone Strikes & Civilian Casualties. 30.08.2021. URL: https://www.democracynow.org/2021/8/30/emran_feroz_afghanistan_us_withdrawal*
16 *The New York Times, 10.09.2021. URL: https://www.nytimes.com/2021/09/10/world/asia/us-air-strike-drone-kabul-afghanistan-isis.html*
17 *https://www.irs.gov/newsroom/combat-zones*

Der folgende öffentliche Appell gegen die Bewaffnung von Drohnen und für die Ächtung autonomer tödlicher Waffen ist am 1. November 2021 verschickt und veröffentlicht worden. Die Initiative dazu ging insbesondere von Wissenschaftler:innen der Unversity of Oxford aus und mehrere FIfF-Mitglieder konnten als Erstunterzeichner:innen gewonnen werden. Der Brief steht jetzt auch auf der Webseite: ***https://aiscientists4peace.org/*** und kann dort von allen, die wollen, unterschrieben werden. Hoffentlich nutzt das auch etwas.

Die Bewaffnung von Drohnen für die Bundeswehr stoppen – autonome Waffensysteme ächten!

Öffentlicher Appell von Forscher:innen der Künstlichen Intelligenz und Informatik

Sehr geehrte Vorsitzende der Parteien SPD, Bündnis 90/Die Grünen und FDP,
sehr geehrte Verhandlungsführende der Koalitionsverhandlungen,
sehr geehrte Mitbürger:innen der Bundesrepublik,

wir wenden uns als Forscher:innen der Künstlichen Intelligenz und Informatik und als Bürger:innen an die Politik und die Öffentlichkeit, damit die Bewaffnung von Drohnen für die Bundeswehr aus humanitären wie aus sicherheitspolitischen Gründen gestoppt wird.

Als Forscher:innen der Künstlichen Intelligenz (KI) und Informatik sprechen wir uns entschieden gegen autonome Waffensysteme aus, so wie viele Tausend unserer internationalen Kolleg:innen.[1] Eine Maschine „sieht" einen Menschen nur als eine lange Liste aus Zahlen, und „versteht" den Wert eines Menschenlebens nicht. Sie

kann die weitreichenden Auswirkungen ihrer „Entscheidungen" nicht „begreifen". Die Tötung von Menschen sollte niemals aufgrund algorithmischer Formeln automatisiert ablaufen. Eine solche Entmenschlichung der Entscheidung über Leben und Tod durch autonome Waffensysteme muss weltweit geächtet werden! Zudem sind die heutigen KI-Algorithmen bei weitem nicht so objektiv und robust, wie es oft den Anschein erweckt. In realen Situationen mit realen Daten können Algorithmen unzuverlässig, fehlerhaft und undurchschaubar sein. Soziale Ungerechtigkeiten und Vorurteile werden durch Algorithmen oft verstärkt.

Die Revolution in der Künstlichen Intelligenz hat eine Algorithmen-gesteuerte Kriegsführung in absehbarer Zukunft möglich gemacht. Bisher gibt es jedoch keine nationalen oder internationalen Kontrollregime, die dieser bereits stattfindenden Entwicklung Einhalt gebieten.

Die Bewaffnung von Drohnen macht eine autonome Waffenführung prinzipiell möglich und stellt einen kritischen Wendepunkt dar. Der wissenschaftlich-technologische Stand ist mittlerweile so weit fortgeschritten, dass jede moderne ferngelenkte bewaffnete Drohne nur ein Software-Update von einer vollautonomen tödlichen Waffe entfernt ist, ohne dass dies nachgewiesen werden kann! Bewaffnete Drohnen müssen jetzt vermieden werden, bevor der Entwicklung hin zu vollautonomen Waffen kein Einhalt mehr geboten werden kann. Im öffentlichen Diskurs über die Bewaffnung von Drohnen wird die Gefahr einer schleichenden Automatisierung der Kriegsführung bisher unzureichend reflektiert – diese Debatte muss geführt werden! Denn mit der Bewaffnung von Drohnen wird eine kritische Schwelle zur Automatisierung der Kriegsführung überschritten: hin zur Entwicklung von Waffen, deren Angriff auf Menschen automatisiert abläuft, ohne weitere menschliche Entscheidung, Aufsicht oder Möglichkeit eines Abbruchs. **Die dringend gebotene internationale Ächtung von vollautonomen letalen Waffen, die sich auch die bisherige Bundesregierung auf die Fahnen schreibt, muss daher bewaffnete Drohnen einschließen.**

Bereits der Einsatz von vom Menschen gesteuerten bewaffneten Drohnen hat die Schwelle zum Einsatz militärischer Gewalt gesenkt und den Krieg weiter entgrenzt, Drohnenangriffe finden dauerhaft und häufig ohne Kriegserklärung statt. Die technologische Hochrüstung mit bewaffneten Drohnen hat militärisch und technologisch überlegenen Staaten wie den USA außergerichtliche Tötungen vereinfacht, die fast ausschließlich People of Colour treffen.[2] Autonome Waffen würden die Möglichkeit globaler Überwachung und Tötungen als potentielle Gefahr definierter Menschen verstärken und die Kontrolle über die Elimination dieser Menschen nicht nur rechtlichen Normen, sondern auch zunehmend menschlichem Einfluss entziehen.

Die zunehmende Automatisierung von bewaffneten Drohnen verschärft gleichzeitig die Gefahr einer militärischen Konfrontation zwischen Staaten, die mit solchen Waffen ausgerüstet sind. Wird aufgrund eines realen militärischen Zwischenfalls oder eines Fehlalarms ein autonomes Waffensystem aktiviert, wird sich eine militärische Eskalation nicht mehr aufhalten lassen. Damit droht eine Verschärfung globaler Instabilität.

Diese Szenarien sind keine ferne Dystopie – im Juni dieses Jahres haben die Vereinten Nationen in einem Bericht bekannt gegeben, dass in Libyen vermutlich eine Drohne einen vollautonomen Angriff durchgeführt hat. Sicher bestätigen, ob dieser Angriff tatsächlich von einer vollautonomen Waffe durchgeführt wurde, konnten die Vereinten Nationen nicht.[3,4] Dieser Vorfall zeigt exemplarisch: Mit einer Verbreitung von bewaffneten Drohnen ist die globale Ausweitung autonomer Waffen auch über die technologisch führenden Staaten hinaus absehbar und bisher weder zu kontrollieren noch zu stoppen. Eine Nicht-Bewaffnung von Drohnen kann politisch entschieden und auf internationaler Ebene kontrolliert werden, die schleichende Entwicklung hin zu immer autonomeren Waffen aufgrund immer komplexerer Algorithmen ist dagegen ein intransparenter Prozess, der sich weitgehend der Möglichkeit öffentlich-demokratischer, geschweige denn internationaler Kontrolle entzieht.

Angesichts der rasanten Entwicklung der Künstlichen Intelligenz ist die Entwicklung und Verbreitung von modernen bewaffneten Drohnen der Dammbruch für einen globalen Rüstungswettlauf hin zu autonomer Kriegsführung, der jetzt gestoppt werden kann und muss.[5] Die Lösung der drängenden Zukunftsfragen macht globale zivile Zusammenarbeit für Sicherheit und menschliche Entwicklung unumgänglich: Ein Bruchteil der Mittel, die aktuell für die Technologisierung und Automatisierung des Krieges verwendet werden, würden ausreichen, um in globalem Ausmaß Sicherheit und menschliche Entwicklung umfassend zu befördern. Allein das von der französischen, deutschen und spanischen Regierung bis 2040 geplante „Future Combat Air System", ein auf teilautonomen, bewaffneten Drohnen-Schwärmen basierendes Kampfsystem, soll bis zu 500 Milliarden Euro kosten.[6] Schon die Kosten dieses Projektes entsprechen dem Doppelten der Mittel, die nach den Vereinten Nationen jährlich notwendig wären, um weltweit den Hunger zu beenden.[7] Der Stopp der Ausbreitung von bewaffneten Drohnen und ihre internationale Abrüstung sind für die Realisierung der sozialen wie der politischen Menschenrechte, für eine menschenwürdige Zukunft auf diesem Planeten geboten.

Wir appellieren daher an die Vertreterinnen und Vertreter der Parteien im deutschen Bundestag, an die Wissenschaft und die Zivilgesellschaft: Stoppen Sie die Bewaffnung von Drohnen für die Bundeswehr. Setzen Sie sich für einen sofortigen Stopp der Verbreitung von bewaffneten Drohnen und für eine Ächtung von bewaffneten Drohnen und autonomen Waffensystemen ein.

Anmerkungen

1 *https://futureoflife.org/open-letter-autonomous-weapons*
2 *https://middle-east-online.com/en/bidens-drone-wars*
3 *https://www.deutschlandfunkkultur.de/kampfdrohnen-und-lenkwaffen-wir-sehen-zunehmend-autonomie.1264.de.html?dram:article_id=498368*
4 *https://www.defenseone.com/ideas/2021/06/libyas-uav-strike-should-galvanize-efforts-autonomous-weapons/174449/*
5 *https://www.blaetter.de/ausgabe/2021/august/angriff-der-killerroboter-wenn-der-algorithmus-toetet*
6 *https://www.handelsblatt.com/politik/deutschland/militaerprojekt-fcas-bund-gibt-ersten-millionenbetrag-fuer-deutsch-franzoesischen-kampfjet-frei/24422282.html?ticket=ST-133154-akS4lvfTuOAPja-gE7UqD-cas01.example.org*
7 *https://taz.de/Weltweiter-Ruestungsausgaben-Rekord/!5678650/*

Ingo Dachwitz

Verschenkte Jahre

Netzpolitische Bilanz der Ära Merkel

In der Netzpolitik hinterlässt Angela Merkel einen Scherbenhaufen: Stockender Breitbandausbau, gefloppte Verwaltungsmodernisierung, miserable IT-Sicherheit. Nur bei einem Thema ging es so richtig voran. Analyse eines Scheiterns.

Eines der berühmtesten Zitate von Angela Merkel lautet, dass „das Internet für uns alle Neuland" sei. Man kann diese Äußerung aus dem Jahr 2013 in diesen Wochen wieder häufig lesen, sie fehlt in kaum einem Rückblick auf 16 Jahre Kanzlerschaft. Der damals auf einer Pressekonferenz neben Merkel stehende Barack Obama musste sich bei den Worten der deutschen Regierungschefin ein Schmunzeln wohl verkneifen, schließlich ging es gerade um den NSA-Überwachungsskandal. Technologische Führerschaft der USA, das war für Obama von Beginn an ein Kernprojekt seiner Präsidentschaft. Merkels Herangehensweise hingegen, das soll das Zitat heute meist verdeutlichen, gilt als uninteressiert, unbedarft, unambitioniert.

Als Angela Merkel 2005 Kanzlerin wurde, gab es weder Smartphones noch Social Media in ihrer heutigen Form. Man kann es aufgrund ihrer sedierenden Rhetorik leicht vergessen, aber die Regierungsjahre der CDU-Politikerin fallen in eine Phase massiver Umbrüche. Der Soziologe Zygmunt Bauman beschreibt unsere Gegenwart als Zeit des Interregnums[1]: Die alte gesellschaftliche Ordnung ist für alle erkennbar abgelöst, doch eine neue ist noch nicht in Kraft. Diese Zeitenwende von epochalem Ausmaß hat nicht nur, aber auch mit der Digitalisierung zu tun. Vernetzung, Datafizierung, Automatisierung und der vereinfachte Zugang zu Wissen und Diskursen – die Entwicklungen der letzten Jahrzehnte verändern unsere Welt von Grund auf.

Diesen Wandel zu gestalten gilt als eine der größten Herausforderungen des frühen 21. Jahrhunderts. Und Angela Merkel, auch darin sind sich die meisten Beobachter:innen dieser Tage einig, ist daran gescheitert. Jahr für Jahr sorgt die schlechte Platzierung Deutschlands in internationalen Rankings[2] zur Digitalisierung für Schlagzeilen. Wie ernst es um den digitalen Fortschritt im Land steht, haben zwischen faxenden Gesundheitsämtern und Schulen ohne Mailadresse spätestens in der Corona-Pandemie viele Menschen erfahren müssen.

Verwalten statt gestalten, moderieren statt regieren

Dabei hat Merkel in ihren Jahren als Kanzlerin immer wieder bewiesen, dass sie ein Gespür für gesellschaftliche Veränderungen hat und aus gesellschaftlichen Stimmungen auch gegen Widerstände politische Projekte formen kann. Die Energiewende ist ein Beispiel, die Abwehr von Geflüchteten an den europäischen Außengrenzen ein anderes.

Angela Merkel, Chancellor, Germany, EU2017EE Estonian Presidency, Photo: Annika Haas (EU2017EE), CC BY 2.0

Warum gelang ihr das nicht auch beim digitalen Wandel? Dass dieser im letzten Jahrzehnt zum gesellschaftlichen Megathema wurde, ist selbstverständlich auch ihr nicht verborgen geblieben. Immer wieder betonte die Naturwissenschaftlerin in Reden die große Bedeutung einer gelungenen Digitalisierung[3]. Sie kündigte dutzende Initiativen an, setzte zahlreiche Beratungsgremien ein, ließ mehrere Minister eine Digitale Agenda auflegen und rief zuletzt ein Digitalkabinett ins Leben. Und doch hinterlässt Angela Merkel einen Scherbenhaufen.

Ein naheliegender Erklärungsansatz ist der reaktive Stil der Kanzlerin. Nachdem sie 2005 als (neoliberale) Reformerin angetreten ist und dabei fast das Rennen um die Kanzlerschaft verloren hätte, hat sie von allzu großen Veränderungsambitionen Abstand genommen. Verwalten statt gestalten, moderieren statt regieren – das schien Merkels Credo. Wenn sie doch größere Projekte aufsetzte, dann erst auf mächtigen Druck von außen. Es war das Atomunglück von Fukushima, das sie zur Energiewende trieb. Es waren die brennenden Geflüchtetenunterkünfte und die stark fallenden Umfragewerte ihrer Partei, wegen der sie die humanistische Fluchtpolitik des Sommers 2015 gegen den EU-Türkei-Deal eintauschte.

Dieser ereignisgetriebene Druck fehlte in vielen Digitalfragen offenbar, zumindest bis zur Corona-Pandemie. Nehmen wir etwa die Modernisierung des Staates. Statt einem zentral koordinierten Vorgehen mit Modellprojekten im unmittelbaren Verwaltungsbereich des Bundes wurschtelten die Regierungen unter

Merkel jahrelang an Einzelprojekten herum. Während in Dänemark online geheiratet werden kann, scheitert hierzulande ein Versuch nach dem anderen. Oder die Projekte ziehen sich ins schier Endlose.

Die Konsolidierung der Bundes-IT etwa ist schon heute ein Milliardengrab[4]. Nach fünf verlorenen Jahren musste der Prozess 2020 komplett neu aufgesetzt werden und kommt trotzdem nicht vom Fleck, einige Bereiche werden laut Innenministerium frühestens 2032 fertig modernisiert sein. Die elektronische Patientenakte soll nach mehr als einem Jahrzehnt Arbeit und Milliardenausgaben[5] für die Gematik-Infrastruktur in diesem Jahr gestartet sein, nur nutzt sie niemand. Auch die digitalen Funktionen des Personalausweises sind bis heute ein Ladenhüter[6]. Und erinnert sich noch jemand an De-Mail[7]?

Die Liste ließe sich unendlich fortführen. „Es ist ja leider kaum mehr möglich, als Privatperson den Überblick über die Vielzahl der gescheiterten Digitalprojekte des Landes zu behalten", fasste Sascha Lobo kürzlich treffend zusammen[8].

Kupfer statt Breitband, weil die Telekom es so wollte

Vom Internet als Neuland sprach Angela Merkel zum ersten Mal im Jahr 2001, wenn auch in anderen Worten. Die frisch gewählte CDU-Vorsitzende besuchte damals die Büros des Internetkonzerns Yahoo in München und gab zu, dass die Politik beim Thema Internet noch „Nachholbedarf" habe. „Auch wir werden in diesem Bereich eine kleine Bildungsoffensive brauchen", so Merkel. Zu oft hinke die Politik den technischen Entwicklungen hinterher. Trotz der frühen Ankündigung: Diese Distanz zu allem Digitalen sollte Merkel in den nächsten 20 Jahren niemals aufholen.

Als Kanzlerin schlenderte sie später Jahr für Jahr über die IT-Messe CeBit in Hannover. Sie ließ sich von Unternehmen neue Produkte und Ideen vorführen, staunte und fragte interessiert nach, solange sie da war. Doch nachhaltig war ihr Interesse selten. Allerdings: Allein mit Desinteresse und Zögerlichkeit lässt sich Merkels Scheitern nicht erklären. Ein zweites Erklärmuster zeigt sich beim Blick auf die Modernisierung der digitalen Infrastruktur. Denn am mangelnden Bewusstsein für die Bedeutung des Breitbandausbaus kann es nicht gelegen haben. Die schlechte Internetversorgung in weiten Teilen der Bundesrepublik sorgt schließlich bis heute nicht nur für jämmerliche Platzierungen im internationalen Vergleich, sondern auch für Frust bei der Kernklientel der CDU: der Wirtschaft. Wie soll sie digitale Dienstleistungen und Innovationen entwickeln, wenn die Menschen sie nicht abrufen können?

Bereits im Jahr 2013 versprach Merkel deshalb persönlich: 50 Mbit pro Sekunde für jeden Haushalt bis Ende 2018. Das galt damals schon als wenig ambitioniert, doch nicht einmal dieses Versprechen konnte die Kanzlerin einlösen. Und zwar bis heute nicht. Der Grund dafür liegt in der fehlgeleiteten Ausbaupolitik des Bundes. Weil die Kommunikationsnetze in Deutschland im Besitz privater Unternehmen sind, ließ die Bundesregierung ihnen beim Breitbandausbau lange Zeit freie Hand.

Vor allem ein Konzern mit besten Verbindungen in die Bundesregierung ging dabei lange einen Weg, der heute als klar gescheitert gilt: die Deutsche Telekom.

Statt frühzeitig und mit allen verfügbaren Mitteln moderne Glasfaserkabel zu verlegen, setzte der ehemalige Staatskonzern lange Zeit weiter auf Kupfer. Mit sogenanntem VDSL-Vectoring sollten die alten Leitungen aufgemöbelt werden. Bei diesem technischen Verfahren zur Verminderung von Störeffekten lässt sich die Übertragungsrate der Kupferleitungen in einem gewissen Maße steigern. Gefördert durch dem Konzern wohlgesonnene Entscheidungen der formell unabhängigen Bundesnetzagentur war das billiger und sorgte auch schneller für kurzfristige Erfolge.

Eine nachhaltige Lösung war das aber eben nicht[9]. Doch erst nach etlichen vergeudeten Jahren wechselte die Bundesregierung den Kurs und entschied 2018, Vectoring nicht mehr zu fördern[10].

Eine fatale Mischung

Es ist in diesem Fall also nicht so, dass Merkel nicht um das Problem gewusst hätte oder nicht an einer Lösung interessiert war – sie glaubte einfach nur viel zu lange den falschen Versprechen der falschen Lobbyisten. Und auch noch nach der Kurskorrektur überließ sie das Schlüsselressort für den Infrastrukturausbau Ministern von der CSU[11], und damit einer Partei, die es als größten Erfolg ihrer Politiker feiert, möglichst viele Fördergelder nach Bayern geschleust[12] zu haben. An vielen anderen Stellen hingegen kommen die Fördermillionen für den Breitbandausbau bis heute nicht an[13].

Mangelnder Gestaltungswille und einseitige Offenheit für die falschen Interessenvertreter – es ist diese fatale Mischung, mit der sich ein Großteil von Merkels netzpolitischer Misere erklären lässt. Denn gerade weil die Bundeskanzlerin es bis zum Schluss vermied, sich selbst tief in die Materie einzuarbeiten und unter Nutzung ihrer Richtlinienkompetenz Führung zu übernehmen, konnten Lobbyvertreter:innen eine besonders große Rolle spielen. Denn wo eine Regierung selbst keine Ideen und Ziele entwickelt, haben sie leichtes Spiel.

Unter Angela Merkel hieß das: Vor allem Lobbyist:innen aus Wirtschaft und Sicherheitsbehörden fanden zu Digitalthemen immer ein offenes Ohr. Denn die Digitalisierung betrachtete die CDU-Politikerin bis zum Schluss vor allem durch die Brillen der Sicherheits- und Wirtschaftspolitik. Zivilgesellschaftliche Organisationen und andere Vertreter:innen gesellschaftlicher Interessen hatten es hingegen schwer[14]. Weitreichende Empfehlungen einer Enquête-Kommission zum Thema Internet und Gesellschaft etwa verschwanden in der Schublade.

Besonders deutlich wurde diese Schieflage immer einmal im Jahr, wenn die Bundesregierung zum Digitalgipfel lud. Bei dem 2006 als IT-Gipfel ins Leben gerufenen Event kamen Merkel und andere hochrangige Regierungsvertreter:innen regelmäßig mit Wirtschaftsvertreter:innen zusammen, um über digitalen Fortschritt zu plaudern und Pläne zu schmieden. Die Zivilgesellschaft durfte höchstens Zaungast spielen[15], nur in Ausnahmefällen durfte auch mal ein Gewerkschafter mitdiskutieren.

Am Ende doch die Erbin Helmut Kohls

Und damit zurück zum Thema Breitband: Dass der Vectoring-Kurs von Telekom und Verkehrsministerium scheitern würde, davor warnte die digitale Zivilgesellschaft[16] Mitte der 2010er Jahre bereits seit langem. Ein Ausweg, um zumindest im öffentlichen Raum vernünftigen Netzzugang gewährleisten zu können, wären frei verfügbare WLANs gewesen, wie sie etwa die Freifunkbewegung seit Jahren organisiert. Doch diese Form der digitalen Nachbarschaftshilfe blockierte die Bundesregierung mit dem weltweit einzigartigen Rechtskonstrukt der WLAN-Störerhaftung[17].

Es sorgte bis 2017[18] dafür, dass hierzulande nicht die Verursacherin für Rechtsverstöße im Internet haftete, sondern diejenige, die anderen Internetzugang gewährte. Cafés, Kirchen und Geschäfte verzichteten aufgrund der Rechtsunsicherheit lange Zeit lieber darauf, andere Menschen von ihren WLANs profitieren zu lassen. Aufgrund des massiven Lobbydrucks der Urheberrechtsverwerter konnte dieser rechtliche Sonderweg erst nach etlichen Jahren und mehreren Anläufen[19] korrigiert werden. Und selbst heute noch werden Menschen verurteilt[20], weil sie für die Vergehen anderer in ihren WLANs haften.

Dass in den 2010er Jahren überhaupt noch Kommunikationsnetze aus Kupfer die deutsche Infrastrukturlandschaft dominierten, geht übrigens auf Helmut Kohl zurück[21]. Der kassierte bei Amtsantritt Anfang der 1980er Jahre einen Beschluss der sozialliberalen Vorgängerregierung für einen 30-jährigen Glasfaser-Ausbau-Plan, mit dem die Bundesrepublik bis 2015 komplett an Glasfasernetze angeschlossen werden sollte. Der CDU-Politiker förderte stattdessen lieber Kabelfernsehen[22]. Mit dem Versagen beim Breitbandausbau erweist sich Angela Merkel dann also doch noch als Erbin ihres einstigen Mentors.

Nur bei einem Thema ging es richtig voran

Überhaupt: Helmut Kohl. Wer eine netzpolitische Bilanz von Merkels Regierungsjahren zieht, kann gar nicht anders, als an den Reformstau zu denken, den der andere Dauerkanzler Ende der 1990er Jahre hinterließ.

Gleichwohl sollte man nicht sagen, dass es unter Angela Merkel in der Netzpolitik überhaupt keine Bewegung gegeben habe. Bei einem Thema ging es nämlich ordentlich voran: dem Ausbau der staatlichen Überwachung. Gleich zweimal führte die Regierung Merkel die anlasslose Vorratsdatenspeicherung von Kommunikationsdaten ein[23], forcierte den Ausbau der Videoüberwachung[24] und erlaubte allen erdenklichen Polizeibehörden und Geheimdiensten, auf biometrische Daten zuzugreifen[25] und den Staatstrojaner einzusetzen[26]. Merkel selbst trat zwar eher selten als sicherheitspolitische Hardlinerin auf, doch egal ob sie Thomas, Hans-Peter oder Horst hießen, die Innenminister von CDU und CSU konnten sich meist auf den Rückhalt der Kanzlerin verlassen.

Daran änderten auch diverse höchstrichterliche Urteile aus Karlsruhe und Luxemburg nichts. Tatsächlich wurde es in den letzten 16 Jahren zur Methode des Innenministeriums, an Überwachungsgesetze wie an eine Verhandlung auf dem Basar heranzugehen: Erstmal formuliert man sie so weitgehend wie möglich – sollte es dann Verfassungsbeschwerden und höchstrichterliche Korrekturaufträge geben, kann man ja immer noch nachbessern. Vierzehn Überwachungsgesetze haute das Bundesverfassungsgericht der Regierung in den letzten 16 Jahren um die Ohren.

Auch die Koalitionspartnerinnen verhinderten das nicht. Immerhin hatte die Union zwölf Jahre die SPD an ihrer Seite, die weder Willens noch in der Lage war, sich dem Ausbau des Überwachungsstaates entgegenzustellen. Lediglich Justizministerin Sabine Leutheusser-Schnarrenberger (FDP) leistete so etwas wie Widerstand. Als eine der letzten großen Bürgerrechtler:innen in der FDP verhinderte sie nach einem Urteil des Bundesverfassungsgerichts Anfang der 2010er Jahre die Wiedereinführung der Vorratsdatenspeicherung. Oder genauer gesagt: Sie verzögerte sie.

Ihr Nachfolger Heiko Maas (SPD) brauchte nicht lange, um das für die Kriminalitätsbekämpfung weitgehend wirkungslose Überwachungsinstrument auf Geheiß seines Parteivorsitzenden 2015 wieder einzuführen. Noch bevor sie an den Start ging, wurde die VDS 2017 wieder ausgesetzt[27] – wegen verfassungsrechtlicher Bedenken.

Die massivsten innenpolitischen Verschärfungen seit der Zeit der RAF

Auch der größte Überwachungsskandal der letzten 30 Jahre fällt in Merkels Amtszeit. Als der ehemalige NSA-Mitarbeiter Edward Snowden[28] 2013 enthüllt, wie umfassend die Überwachung der Geheimdienste der USA und der anderen Five-Eyes-Staaten ist, erfährt die Öffentlichkeit, dass nicht nur die Kommunikation von Milliarden Menschen weltweit untersucht wird, sondern auch das Handy der Kanzlerin abgehört wird. „Ausspähen unter Freunden, das geht gar nicht“, zeigt sich Merkel öffentlich entrüstet.

Wenig später bringt ein parlamentarischer Untersuchungsausschuss ans Licht, dass der deutsche Bundesnachrichtendienst ein erschreckendes Eigenleben entwickelt hat und tief in die Machenschaften der US-Dienste verwickelt ist. Unter anderem assistierte der Auslandsgeheimdienst dem großen Bruder aus Übersee beim massenhaften Mitschneiden der Kommunikation direkt am weltweit größten Internetknoten[29] DE-CIX in Frankfurt.

Die Enthüllungen konterkarieren die gezielte Unbedarftheit, mit der Merkel 2013 in ihrer Rede vom Neuland auf den NSA-Skandal reagierte. Die Aufsicht über den Geheimdienst liegt in der Zuständigkeit des Kanzleramts und damit direkt in ihrer Verantwortung. Dass der Überwachungsausbau nicht etwa gegen Merkels Willen, sondern mit ihrem Segen geschieht, zeigt spätestens die Reaktion auf die neuen Erkenntnisse über den BND: 2017 legalisiert die Große Koalition mit einer neuen gesetzlichen Grundlage[30] im Wesentlichen das, was der Geheimdienst zuvor jahrelang illegal gemacht hat. Außerdem werden seine finanziellen Mittel erhöht: Seit den Snowden-Enthüllungen hat sich das Budget des BND mehr als verdoppelt.

So trägt Angela Merkel die Verantwortung für die massivsten innenpolitischen Verschärfungen seit der Zeit der RAF[31]. Das ist für eine konservative Kanzlerin nicht eben verwunderlich. Erstaunlich ist vielmehr, dass Merkel am Ende ihrer Amtszeit selbst bei vielen Linken die Aura einer liberalen oder gar progressiven Politikerin hat. Dass ausgerechnet eine in der DDR aufgewachsene Politikerin die Geheimdienste hochrüstet, hat ihrem Image nicht geschadet. Zu weit weg ist das Thema Überwachung für viele Menschen, um sich dauerhaft empören zu können.

Hausgemachte IT-Unsicherheit

Dabei ist die Kehrseite dieser einseitigen Innenpolitik für viele Menschen täglich spürbar: Der Staat kommt seinem grundrechtlichen Schutzauftrag für die IT-Sicherheit der Bürger:innen nicht vernünftig nach. Als etwa der Krypto-Trojaner Wannacry, den Kriminelle aus dem digitalen Waffenarsenal der NSA[32] entwenden konnten, im Frühjahr 2017 Krankenhäuser und Bahnhöfe lahmlegte, versetzte dies die Republik in Aufregung. Inzwischen gehören solche Meldungen zur Tagesordnung. Weder die Systeme von Unternehmen noch die des Bundestages sind ausreichend geschützt. In der Bevölkerung herrscht Verunsicherung, die Digitalwirtschaft schätzt den volkswirtschaftlichen Schaden sogenannter Cyber-Angriffe auf mehr als 200 Milliarden Euro jährlich[33].

Doch der Staat wird das Problem nicht in den Griff bekommen, solange staatliche Stellen ein Interesse daran haben, dass Sicherheitslücken in IT-Systemen nicht geschlossen, sondern gehortet werden. Bis heute ist das Bundesamt für Sicherheit in der Informationstechnik dem Innenministerium unterstellt, das die Kompetenzen der staatlichen Hacker permanent ausweitet und mit ZITiS ein eigenes Institut gegründet hat, um verschlüsselte Kommunikation besser brechen zu können[34].

Auch hier zeigt sich, wie fatal die Merkel'sche Mischung aus digitalem Desinteresse und einseitiger Offenheit für die Einflüsterungen mancher Lobby-Gruppen ist. Die Chefs der Geheimdienste und Sicherheitsbehörden sind mindestens einmal pro Woche zur Besprechung im Kanzleramt. Dass die Kanzlerin auch mal die Expertise des Chaos Computers Clubs angefragt hätte, ist hingegen nicht bekannt. Dass Angela Merkel in Fragen der IT-Sicherheit nie auf zivilgesellschaftliche Player ohne Eigeninteresse, sondern immer nur auf den staatlichen Sicherheitsapparat gehört hat, wird noch jahrelang für enormen Schaden sorgen.

Bürger:innen sollten Daten geben, nicht der Staat

Bei kaum einem Thema wird die Schlagseite von Merkels netzpolitischer Agenda so sichtbar wie in der Datenpolitik. Während die Bundeskanzlerin sich im Einklang mit Verbänden der Digitalwirtschaft immer wieder explizit dafür aussprach, persönliche Daten als Rohstoff zu betrachten und die Bürger:innen wiederholt zu mehr Freigiebigkeit aufforderte[35], hatte sie für offene Daten seitens des Staates wenig Liebe.

Bis heute gibt es im Bund kein Transparenzgesetz, das Behörden dazu verpflichten würde, den Bürgerinnen und Bürgern weitreichende Informationen proaktiv zur Verfügung zu stellen. Das kürzlich reformierte Open-Data-Gesetz enthält immer noch keinen Rechtsanspruch auf offene Daten, sodass hier keine Fortschritte zu erwarten sind. Und vor Gericht kämpfen derzeit gleich mehrere Ministerien dagegen, dass sie die offiziellen SMS und Twitternachrichten ihrer Minister:innen zugänglich machen müssen.

Gleichzeitig schoss Merkel in ungewohnter Deutlichkeit gegen den Datenschutz für Bürgerinnen und Bürger. In den Verhandlungen um die Datenschutzgrundverordnung (DSGVO) der EU versuchte das Innenministerium mit dem Segen der Kanzlerin, Grundsätze des deutschen Datenschutzrechts zu verwässern. Auch als dieses Unterfangen scheiterte und die DSGVO 2016 inklusive solcher Maßgaben wie Zweckbindung und Datenminimierung verabschiedet wurde, gab sich Merkel damit nicht zufrieden. Trotz sich häufender Datenskandale, Stichwort Cambridge Analytica, schoss die Kanzlerin in Reden regelmäßig gegen den Datenschutz[36].

Teilweise übernahm sie dabei das Framing des Industrieverbandes Bitkom sogar wörtlich, etwa als sie ab 2016 ein *Ende der Datensparsamkeit* und ein neues Zeitalter des *Datenreichtums* ausrief. Sie wolle zudem künftig nicht mehr von *Datenschutz*, sondern lieber von *Datensouveränität* sprechen, verkündete sie in dieser Zeit[37]. Sie habe gehört, das solle sie jetzt so machen, gab Merkel in einer Rede auf dem IT-Gipfel in der ihr eigenen unprätentiösen Art zu Protokoll. Dass diese Parole vom Industrieverband Bitkom ausgegeben wurde, musste sie in diesem Setting nicht dazusagen.

Datenpolitik in der Sackgasse

Nun ist die Datenschutzgrundverordnung alles andere als perfekt, aber sie gilt fünf Jahre nach ihrer Verabschiedung weltweit als Goldstandard und als Grundstein eines europäischen Weges der Digitalisierung: Zwischen dem völlig enthemmten Überwachungskapitalismus der USA und dem staatlich gesteuerten Überwachungskapitalismus Chinas steht zumindest der Versuch einer grundrechtschonenden Regulierung. Wer auf dem digitalen Binnenmarkt der EU agieren möchte, muss sich unabhängig vom Sitzland an die hier geltenden Regeln halten. Dass die Bundeskanzlerin trotz der Verabschiedung des Mammutgesetzes weiter dagegen agitierte, will so gar nicht zum Image der nüchternen und ideologiefreien Politikerin passen.

Ins Bild passt dann jedoch, dass die Bundesregierung sehenden Auges auf das Chaos rund das Wirksamwerden der DSGVO im Mai 2018 zulief[38]. Der Industrieverband Bitkom hatte lange vorher gewarnt, dass sich ein Großteil der Unternehmen im Land noch nicht auf das neue Datenschutzrecht eingestellt habe. Doch statt hier aufzuklären, mit hilfreichen Werkzeugen unter die Arme zu greifen oder mit Standards und Zertifizierung für Orientierung zu sorgen, beließ Merkel es bei rhetorischen Angriffen.

Diese Grabenkampfmentalität führte zu einer Dauerblockade in der Datenpolitik: Lange Jahre gab es weder Impulse, wie Daten zum Wohle der Gesellschaft besser genutzt werden könnten, noch wurde der Datenschutz weiterentwickelt. Die vom Lobbying der Datenindustrie[39] aufgehaltene ePrivacy-Reform etwa, mit der die EU schon lange das Cookie-Chaos im Netz aufgeräumt haben wollte, ist bis heute nicht verabschiedet[40].

Erst in ihrer letzten Amtszeit fand das Kanzleramt zu einer realistischeren Datenpolitik, was allerdings weniger an der Bundeskanzlerin als an ihrem neuen Kanzleramtschef und Digitalkoordinator Helge Braun gelegen haben dürfte. Eine von der Bundesregierung eingesetzte Datenethikkommission schrieb der Bundesregierung eine Kurskorrektur ins Stammbuch und machte dutzende Vorschläge zur Weiterentwicklung des Datenschutzes[41]. Von denen ist bis heute zwar keiner umgesetzt, in der 2020 beschlossenen Datenstrategie der Bundesregierung[42] ist jedoch ein Paradigmenwechsel zu beobachten: Datenschutz wird nicht mehr als Hemmnis, sondern als Voraussetzung für die Verwertung von Daten beschrieben. Außerdem soll der Staat nun doch zum Vorreiter werden und mehr Daten über sein eigenes Handeln öffentlich zur Verfügung stellen.

Die scheidende Kanzlerin dürfte froh sein, dass es nicht mehr sie ist, die die Umsetzung dieser Ankündigung zu verantworten hat.

Schluss mit Neuland

„Wer gibt schon gerne zu", soll Angela Merkel bei ihrem Yahoo-Besuch im Jahr 2001[43] gefragt haben, „dass er in diesem Bereich oft noch Analphabet ist?" Irgendwann hat sie offenbar entschieden: ich. Ich bin so jemand. Mehr noch: Sie hat entschieden, dass sie ihre Distanz zu allem Digitalen in den nächsten 20 Jahren wie eine Monstranz vor sich hertragen würde. Noch im Jahr 2018 hat Merkel deshalb ihre Neuland-Metapher in anderen Worten wiederholt. Wegen des „Shitstorms", den sie 2013 kassiert habe, wolle sie das Wort selbst nicht mehr in den Mund nehmen, sagte die Kanzlerin auf dem Digitalgipfel. Und doch sei das Internet „undurchschrittenes Terrain"[44].

Die Schritte in das unbekannte Digitale, das für so viele Menschen längst schon Alltag ist, Angela Merkel wollte sie bis zum Ende ihrer Kanzlerinschaft nicht gehen. Abwarten, moderieren, verwalten – das gilt vielen als der richtige Politikstil für die Krisen der letzten Jahre. Der digitale Wandel aber hätte gestaltet werden müssen.

Sowohl Yahoo als auch die CeBit sind heute verschwunden und auch Angela Merkel ist als Kanzlerin bald Geschichte. Dass all die Reden vom Aufholen und dem „jetzt aber wirklich Ernst machen" am Ende überwiegend Ankündigungen blieben, dass die Infrastruktur marode ist und Digitalisierung heute oft gleichbedeutend mit Verunsicherung, dass der Reformstau lang ist und die ungelösten Konflikte zahlreich, all das ist ihr netzpolitisches Erbe. Eine fatale Mischung aus Desinteresse, Visionslosigkeit und einseitiger Offenheit für die falschen Interesenvertreter:innen zieht sich wie ein Muster durch ihr Wirken.

Wer auch immer die Netzpolitik der nächsten Jahre bestimmt, sollte aus Angela Merkels Fehlern lernen. Es braucht jetzt echten Gestaltungswillen. Es braucht einen Blick auf die Digitalisierung, der sie nicht auf Sicherheits- und Wirtschaftspolitik verengt, sondern als Gesellschaftspolitik begreift. Und es braucht eine Netzpolitik, die alle im Blick hat und in der nicht nur wenige Gehör finden.

Quelle: https://netzpolitik.org/2021/netzpolitische-bilanz-der-aera-merkel-verschenkte-jahre/

Anmerkungen

1 *https://de.wikipedia.org/wiki/Interregnum*
2 *https://www.handelsblatt.com/politik/international/standortwettbewerb-drittletzter-von-20-staaten-frankreich-und-italien-haengen-deutschland-bei-der-digitalisierung-ab/27569412.html?*
3 *https://archiv.cdu.de/artikel/merkel-digitaler-wandel-wie-industrielle-revolution*
4 *https://netzpolitik.org/2021/it-konsolidierung-des-bundes-pleitenserie-ohne-ende/*
5 *https://www.tagesschau.de/wirtschaft/verbraucher/epa-elektronische-patientenakte-101.html*
6 *https://www.ccc.de/system/uploads/225/original/ccc-stellungnahme-eID.pdf*
7 *https://netzpolitik.org/2015/de-mail-das-tote-pferd-wird-weitergeritten-wieviel-das-kostet-soll-geheim-bleiben/*
8 *https://www.spiegel.de/netzwelt/netzpolitik/nora-e-rezept-und-id-wallet-deutschland-ist-das-digitale-schilda-a-b1c6458f-4857-4449-beab-fff8b683484e*
9 *https://netzpolitik.org/2017/vectoring-ausbau-der-telekom-deutschland-fuehrt-in-die-sackgasse/*
10 *https://netzpolitik.org/2018/kanzleramt-klare-absage-an-kupfer-beim-breitbandausbau/*
11 *https://netzpolitik.org/2018/nun-offiziell-bundesrechnungshof-zerpflueckt-ex-minister-alexander-dobrindt/*
12 *https://twitter.com/ARD_BaB/status/1436349189823385605*
13 *https://netzpolitik.org/2020/immer-noch-bleiben-viele-foerdermittel-liegen/*
14 *https://netzpolitik.org/2018/altmaier-baer-und-braun-ueber-datenschutz-redet-die-regierung-am-liebsten-mit-der-industrie/*
15 *https://netzpolitik.org/2015/it-gipfel-bundesregierung-diskutiert-gesellschaftlichen-wandel-mal-wieder-fast-nur-mit-unternehmen/*
16 *https://www.tagesspiegel.de/themen/breitbandausbau-in-*

Ingo Dachwitz

Ingo Dachwitz ist Kommunikationswissenschaftler und seit 2016 Redakteur bei netzpolitik.org. Er schreibt und spricht über Datenpolitik, Überwachungskapitalismus und den digitalen Strukturwandel der Öffentlichkeit. Ingo gibt Workshops für junge und ältere Menschen in digitaler Selbstverteidigung und lehrt an Universitäten zur politischen Ökonomie digitaler Medien. Außerdem moderiert er Veranstaltungen und Diskussionen, etwa auf der re:publica oder beim Netzpolitischen Abend in Berlin. Ingo ist Mitglied des Vereins Digitale Gesellschaft sowie der sozialethischen Kammer der EKD und berät kirchliche Organisationen bei der digitalen Transformation. Kontakt: Ingo ist per Mail an ingo | punkt | dachwitz | ett | netzpolitik.org (PGP-Key[45]) erreichbar und als @roofjoke auf Twitter unterwegs.

deutschland/schnelles-internet-die-bundesregierung-verkennt-wie-innovation-entsteht/12584478.html
17 https://netzpolitik.org/2015/netzrueckblick-die-stoererhaftung-eine-einfuehrung/
18 https://netzpolitik.org/2017/wlan-gesetz-bundestag-schafft-stoererhaftung-endlich-ab-ermoeglicht-aber-netzsperren/
19 https://netzpolitik.org/2016/kommentar-zur-stoererhaftung-rechtssicherheit-sieht-anders-aus/
20 https://freifunkstattangst.de/2021/10/25/verurteilung-der-alten-dame-vom-lg-koeln-bestaetigt/
21 https://netzpolitik.org/2018/danke-helmut-kohl-kabelfernsehen-statt-glasfaserausbau/
22 https://www.deutschlandfunk.de/zehn-jahre-nach-ende-des-briefmonopols-die-gelbe-post-im.724.de.html?dram:article_id=407169
23 https://netzpolitik.org/2015/vds-im-bundestag-reaktionen-aus-presse-politik-ngos-und-verbaenden/
24 https://netzpolitik.org/2017/bundestag-beschliesst-ausbau-der-videoueberwachung-kennzeichen-scanner-und-bodycams-fuer-die-bundespolizei/
25 https://netzpolitik.org/2017/im-gesetz-zum-elektronischen-personalausweis-versteckt-sich-ein-automatisierter-abruf-fuer-geheimdienste/
26 https://netzpolitik.org/2021/bundespolizeigesetz-grosse-koalition-einigt-sich-auf-staatstrojaner-einsatz-schon-vor-straftaten/
27 https://netzpolitik.org/2017/bundesnetzagentur-keine-strafe-wenn-provider-vorratsdaten-nicht-speichern/
28 https://netzpolitik.org/tag/edward-snowden/
29 https://netzpolitik.org/2014/eikonal-wie-der-bnd-der-nsa-zugang-zum-internetknoten-de-cix-schenkte/
30 https://netzpolitik.org/2016/warum-alle-gegen-das-bnd-gesetz-sind-ausser-der-bundesregierung/
31 https://netzpolitik.org/2017/chronik-des-ueberwachungsstaates/
32 https://www.zeit.de/digital/internet/2017-05/wannacry-microsoft-nsa-hackerangriff-usa-regierung
33 https://www.sueddeutsche.de/wirtschaft/cyber-angriffe-wirtschaft-schaden-1.5374489
34 https://netzpolitik.org/2018/36-millionen-euro-zitis-baut-supercomputer-zur-entschluesselung/
35 https://netzpolitik.org/2018/merkel-in-davos-initiative-neue-soziale-datenmarktwirtschaft/
36 https://netzpolitik.org/2016/angela-merkel-auf-den-medientagen-datenschutz-stoert/
37 https://netzpolitik.org/2016/angela-merkel-hat-gehoert-dass-sie-datenschutz-jetzt-datensouveraenitaet-nennen-soll/
38 https://netzpolitik.org/2018/datenschutzgrundverunsicherung-danke-merkel/
39 https://netzpolitik.org/2017/eprivacy-die-lobbymacht-der-datenindustrie/
40 https://netzpolitik.org/2020/online-tracking-womoeglich-letzte-chance-fuer-die-eprivacy-verordnung/
41 https://netzpolitik.org/2019/regierungsberaterinnen-fordern-strengere-regeln-fuer-daten-und-algorithmen/
42 https://netzpolitik.org/2021/datenstrategie-der-bundesregierung-die-richtung-stimmt-aber-der-weg-ist-noch-weit/
43 https://www.t-online.de/digital/id_89878396/cdu-jahrestag-vor-20-jahren-erklaerte-angela-merkel-nachholbedarf-in-sachen-internet.html
44 https://www.facebook.com/ZDFheute/photos/das-internet-im-jahr-2018-nicht-mehr-neuland-aber-doch-noch-nicht-durchschritten/10157011092460680/
45 https://keys.openpgp.org/search?q=ingo.dachwitz%40netzpolitik.org

Alexander Fanta

Eine Insiderin, die es besser machen will

Enthüllungen über Facebook sorgen für globale Schlagzeilen. Dahinter steht eine Frau, die jahrelang von innen heraus auf Veränderung gedrängt hatte. Erst als Frances Haugens Rufe ungehört verhallten, ging sie an die Öffentlichkeit.

Irgendwann zu Jahresbeginn 2021, als die USA und der Rest der Welt mit der Corona-Pandemie kämpfen, fasst Frances Haugen einen Entschluss. Die Facebook-Mitarbeiterin kopiert heimlich zehntausende Seiten an internen Forschungspapieren des Konzerns. Papiere, die zeigen, wie viel der Konzern über die zerstörerische Wirkung seiner Produkte wusste – und wie wenig er dagegen getan hat. „Ich habe begriffen, okay, ich muss das auf eine systematische Art tun und ich muss genug davon mitnehmen, so dass niemand daran zweifeln kann, dass das real ist", sagt Haugen später[1].

Die Enthüllungen aus Haugens Papieren sorgen für Schlagzeilen auf der ganzen Welt. Am 13. September veröffentlicht das Wall Street Journal die erste Geschichte daraus. Sie enthüllt, dass Facebook Millionen von Promis von seinen Regeln ausnimmt[2] – ein Privileg, das von Politiker:innen wie Donald Trump schamlos missbraucht wurde.

Frances Haugen, Facebook whistleblower, gives evidence to the UK Parliament, Foto: UK Parliament 2021/ Annabel Moeller, CC BY-NC-ND 2.0

Es folgen weitere Schlagzeilen, weitere Enthüllungen zahlreicher Medien – die Facebook Papers. Aus ihnen geht hervor, dass Facebook über Hassbotschaften und Aufrufe zur Gewalt gegen muslimische Minderheiten in Indien Bescheid wusste, aber nichts unternahm[3]. Oder, dass Facebook trotz interner Warnun-

gen über die rapide Verbreitung von Verschwörungsmythen im Vorfeld der US-Wahl 2020[4] passiv blieb. Bis heute weist der Konzern die Verantwortung für die Ausbreitung von Falschinformation über angebliche Wahlmanipulation, die im Sturm auf das Kapitol am 6. Januar gipfelte, meilenweit von sich.

Ein erster großer Auftritt – und Facebook fällt aus

Nach wochenlanger Aufregung tritt Haugen selbst vor die Kamera. In der Fernsehsendung *60 Minutes*[5] spricht die Whistleblowerin erstmals in der Öffentlichkeit, Bilder von ihrem Auftritt gehen um die Welt. Einen Tag später fallen Facebook, Instagram und WhatsApp weltweit für mehrere Stunden aus – das sorgt für höhnische Kommentare, auch wenn Expert:innen eher ausschließen[6], dass ein Zusammenhang besteht.

Nur einen weiteren Tag darauf sagt Haugen vor dem US-Kongress aus. Das Zeugnis, das sie dort über ihren Ex-Arbeitgeber ablegt, ist vernichtend. Die Konzernführung um Mark Zuckerberg wisse genau, wie sie Facebook und Instagram sicherer machen könne, doch sie verzichte auf Maßnahmen, um ihre astronomischen Profite nicht zu gefährden. Es brauche nun endlich Maßnahmen der Politik. „Die werden diese Krise nicht ohne Ihre Hilfe lösen", lautet ihr Appell an die Kongressabgeordneten. Kommende Woche soll Haugen auch vor dem EU-Parlament sprechen[7].

Haugens selbstsicheres Auftreten weckte Neugier bei der Weltpresse. Wer ist die 37-Jährige?

Ein Blick auf ihren Lebenslauf[8] zeichnet das Bild einer Insiderin mit Parade-Lebenslauf: Geboren und aufgewachsen im Präriestaat Iowa als Tochter eines Arztes und einer Priesterin, studiert Haugen Informatik, geht als Produktmanagerin zum noch jungen Google-Konzern. Nach drei Jahren wechselt sie für ein Managementstudium nach Harvard. Dann gründet sie selbst ein Startup, eine Dating-App. Der Eigengründung, bei der sie nach wenigen Monaten wieder aussteigt, folgten klassische Stationen einer Silicon-Valley-Laufbahn: Wieder Google, Yelp, Pinterest – und schließlich Facebook.

Eine Erkrankung und eine Freundschaft, die Haugen prägt

Doch hinter diesem eindrucksvollen Lebenslauf verbirgt sich auch eine private Tragödie. 2011 wird Haugen mit Zöliakie diagnostiziert, eine durch Glutenunverträglichkeit verursachte Autoimmunerkrankung, die ihre Nerven schädigt und ihr große Schmerzen zufügt. Zeitweise kann sie sich kaum bewegen, wie sie später dem Wall Street Journal erzählt[9]. Drei Jahre später landet sie wegen Blutgerinnseln auf der Intensivstation.

Ein Freund der Familie hilft ihr damals, wieder auf die Beine zu kommen. Ein Jahr lang hilft der junge Mann ihr im Alltag. Doch dann bemerkt Haugen bei ihm eine Veränderung, so schildert sie es später. „Es war eine wirklich wichtige Freundschaft, und dann habe ich ihn verloren." Haugens junger Helfer verbringt immer mehr Zeit in obskuren Online-Foren, bald versinkt er in einem Morast an rassistischen Verschwörungsmythen. Haugen, die ihm helfen will, ist ratlos. Die Freundschaft endet. „Es ist die eine Sache, Desinformation zu studieren und eine andere, jemanden an sie zu verlieren."

Als Haugen im Juni 2019 bei Facebook anfängt, hat sich die Welt gegen den Social-Media-Konzern gewandt. Der Skandal um Cambridge Analytica und die Wahl von Donald Trump, der sich massiv manipulativer Wahlwerbung in dem sozialen Netzwerk bedient[10], haben bleibende Schäden an Facebooks Image hinterlassen. Doch ja, der Konzern gelobt Besserung. Immer wieder versprechen Zuckerberg und sein Team, die Flut an Falschinformationen und Hetze auf den Kanälen des Konzerns einzudämmen.

„Ich habe viel Verständnis für Mark"

Den Gelöbnissen zum Trotz läuft intern ein anderes Spiel, bemerkt Haugen. „Ich habe viel Verständnis für Mark", sagt sie später bei *60 Minutes*[11]. Der Facebook-Gründer habe es „nie darauf angelegt, eine hasserfüllte Plattform zu schaffen. Aber er hat es zugelassen, dass Entscheidungen getroffen werden, deren Nebeneffekte darin bestehen, dass hasserfüllte, polarisierende Inhalte mehr Verbreitung und mehr Reichweite erhalten."

Haugens Aufgabe bei Facebook ist es, als Teil des 200 Köpfe zählenden *Civil Integrity Teams* gegen Wahlmanipulation in dem sozialen Netzwerk vorzugehen. Sie soll Tools bauen, mit denen sich schädliche Formen der Einflussnahme durch zielgerichtetes Werbe-Targeting aufspüren lassen sollen. Doch das Projekt ihres kleinen Teams scheiterte nach Angaben Haugens[12], weil ihr Facebook dafür einfach nicht die nötige Zeit einräumte.

Immer wieder muss sie demnach mitansehen, wie der Konzern Hinweise auf bedrohliche Entwicklungen auf seiner Plattform ignoriert. Für Herkulesaufgaben wie den Kampf gegen Sklaverei, Zwangsprostitution und Organhandel stellt Facebook nur ein paar Leute ab. Als sie gefragt habe, warum nicht mehr Leute dafür angestellt werden, habe der Konzern „so getan, als sei es nicht in seiner Macht, mehr Stellen zu schaffen".

Fast zwei Jahre wird Haugen bei Facebook bleiben. Als ihre Bemühungen scheitern, berät sie sich mit ihrer Mutter, der Priesterin. Diese rät ihr, zu tun, womit sie Leben retten könnte, erzählt sie später dem Wall Street Journal[13]. Wenig später kontaktiert Haugen einen Reporter der Zeitung und beginnt, massenhaft Dokumente über das Vorgehen des Konzerns von den Firmenservern zu kopieren.

Frühere Whistleblowerin nahm Enthüllungen vorweg

Haugen ist nicht die einzige Whistleblowerin, deren Enthüllungen den Facebook-Konzern entgegen seines heilen PR-Sprechs ins Rampenlicht zerren. Vor über einem Jahr veröffentlichte Buzzfeed News Auszüge aus einem internen Papier[14] der Datenwissenschaftlerin Sophie Zhang. Darin warnte Zhang ihren Arbeitgeber eindringlich davor, die eigene Plattform werde in einigen Ländern des globalen Südens für manipulative politische Kampagnen missbraucht.

Von Zhang geleakte interne Dokumente, über die der Guardian[15] und andere Medien berichtet, bauen medialen Druck auf[16]. Sie nehmen einiges an Schilderungen über das interne Kontrollversagen bei Facebook vorweg, auf das auch Haugens Enthüllungen ein Schlaglicht werfen.

Die Aussagen von Zhang und Haugen könnten nicht nur mediale Konsequenzen haben: Beide Whistleblowerinnen übergaben Dokumente an die US-Marktaufsichtsbehörde SEC. Sie prüft, ob Facebooks Wegsehen strafrechtliche Folgen haben könnte.

Nach den spektakulären Enthüllungen ringt Facebook nun um Deutungshoheit. Vor wenigen Tagen kündigte der Konzern an, sich künftig *Meta Platforms Inc.* nennen zu wollen – ein Schritt, der mit der Umbenennung Googles in Alphabet verglichen wird. In beiden Fällen bleibt der Name des jeweils bekanntesten Produkts, Suchmaschine und soziales Netzwerk, davon unberührt.

Kurz darauf lässt Facebook wissen[17], dass es sein System zur Gesichtserkennung in Fotos und Videos stoppe. Damit will der Konzern auf wachsende Bedenken gegen die Technologie reagieren, wohl aber auch von den Enthüllungen Haugens ablenken.

Die Whistleblowerin muss sich inzwischen gegen Berichte wehren, sie habe sich gegen Ende-zu-Ende-Verschlüsselung ausgesprochen. Das hatte das britische Blatt Daily Telegraph verbreitet[18], ihr dabei aber das Wort im Mund verdreht, wie sie vor dem britischen Unterhaus sagt[19]. „Ich unterstütze den Zugang zur Ende-zu-Ende-Verschlüsselung und verwende jeden Tag quelloffene Ende-zu-Ende-Verschlüsselung."

Die kommenden Wochen tourt Haugen durch die Welt und erzählt ihre Geschichte. Brüssel, Berlin, Portugal stehen auf dem Programm[20], weitere Stationen werden wohl folgen. Finanziert wird ihre Reisetätigkeit[21] von einem Schwergewicht der Technologiebranche, eBay-Gründer Pierre Omidyar, der mit seinem Vermögen auch kritische NGOs und das Investigativmedium The Intercept finanziert. Davon abhängig sei sie aber nicht, sagt Haugen der New York Times[22]. Sie habe „rechtzeitig in Krypto-[Währungen] investiert" und habe auf absehbare Zeit keine Geldsorgen. Der Aufregung, die ihre Enthüllungen entfacht haben, kann Haugen daher wohl mit Gelassenheit entgegensehen.

Quelle: https://netzpolitik.org/2021/frances-haugen-eine-insiderin-die-es-besser-machen-will/

Anmerkungen

1 *https://www.youtube.com/watch?v=_Lx5VmAdZSI*
2 *https://www.wsj.com/articles/facebook-files-xcheck-zuckerberg-elite-rules-11631541353?mod=article_inline*
3 *https://www.washingtonpost.com/technology/2021/10/24/india-facebook-misinformation-hate-speech/*
4 *https://www.nytimes.com/2021/10/22/technology/facebook-election-misinformation.html*
5 *https://www.youtube.com/watch?v=_Lx5VmAdZSI*
6 *https://www.businessinsider.com/facebook-outage-likely-not-linked-whistleblower-claims-hearing-frances-haugen-2021-10*
7 *https://www.europarl.europa.eu/news/de/press-room/20211011IPR14619/facebook-files-meps-to-invite-whistleblower-frances-haugen-to-a-hearing*
8 *https://www.linkedin.com/in/franceshaugen/*
9 *https://www.wsj.com/articles/facebook-whistleblower-frances-haugen-says-she-wants-to-fix-the-company-not-harm-it-11633304122*
10 *https://netzpolitik.org/2019/werben-wie-donald-trump/*
11 *https://www.youtube.com/watch?v=_Lx5VmAdZSI*
12 *https://www.wsj.com/articles/facebook-whistleblower-frances-haugen-says-she-wants-to-fix-the-company-not-harm-it-11633304122*
13 *https://www.wsj.com/articles/facebook-whistleblower-frances-haugen-says-she-wants-to-fix-the-company-not-harm-it-11633304122*
14 *https://www.buzzfeednews.com/article/craigsilverman/facebook-ignore-political-manipulation-whistleblower-memo*
15 *https://www.theguardian.com/technology/series/the-facebook-loophole*
16 *https://netzpolitik.org/2021/desinformation-auf-facebook-erst-handeln-wenn-es-zu-spaet-ist/*
17 *https://www.reuters.com/technology/facebook-will-shut-down-facial-recognition-system-2021-11-02/*
18 *https://www.telegraph.co.uk/news/2021/10/24/facebook-whistleblower-warns-dangerous-encryption-will-aid-espionage/*
19 *https://techcrunch.com/2021/10/25/facebook-whistleblower-frances-haugen-raises-trust-and-security-questions-over-its-e2e-encryption/*
20 *https://www.spiegel.de/netzwelt/netzpolitik/frances-haugen-kommt-nach-berlin-ein-date-mit-dem-whistleblower-popstar-a-410fde53-2cc6-42a5-ab92-39db166ab37f*
21 *https://www.politico.com/news/2021/10/20/tech-billionaire-aiding-facebook-whistleblower-516358*
22 *https://www.nytimes.com/2021/10/24/business/media/facebook-leak-frances-haugen.html*
23 *https://www.otto-brenner-stiftung.de/wissenschaftsportal/informationsseiten-zu-studien/medienmaezen-google/*
24 *https://keys.openpgp.org/vks/v1/by-fingerprint/E60418D343710F1C82C2B73B2271FE6D4CD84C62*

Alexander Fanta

Alexander Fanta berichtet als EU-Korrespondent von *netzpolitik.org* über die Digitalpolitik der Europäischen Union. Er schreibt über neue Gesetze und recherchiert investigativ über große Technologiekonzerne und ihr Lobbying. Er ist Ko-Autor der Studie *Medienmäzen Google*[23] über Journalismusförderungen des Konzerns. 2017 war Alexander Stipendiat am Reuters-Institut für Journalismusforschung an der Universität Oxford, wo er zur Automatisierung im Journalismus forschte. Davor war er Außenpolitikjournalist bei der österreichischen Nachrichtenagentur APA. E-Mail: *alexander.fanta@netzpolitik.org* (PGP[24]). Twitter: *@FantaAlexx*. WhatsApp/Threema: +32483248596.

Dagmar Boedicker

Sabine Pfeiffer: Digitalisierung als Distributivkraft

Eine etwas andere Analyse zum digitalen Kapitalismus

Sabine Pfeiffer hat wieder ein hochinteressantes Buch geschrieben; besonders für Menschen, die auch an der Volkswirtschaft interessiert sind. Bei ihrer Suche nach dem wirklich Neuen *an der Digitalisierung nimmt sie immer wieder die marxistische Perspektive ein, kein Schaden, wenn sie die Positionen anderer Wissenschaftler untersucht. Zu denen gehören Mariana Mazzucato (Ökonomin), Armin Nassehi, Philipp Staab (beide sind Soziologen, Staab gab einen Einblick in seine Positionen auf der FIfFKon 2021 in München), Dan Schiller (Wirtschafts- und Technikhistoriker) oder Michael Betancourt (kritischer Theroretiker, Historiker und Künstler). Die drei letztgenannten haben sich wie viele andere von Pfeiffer betrachtete Autoren bemüht zu beschreiben, was den digitalen Kapitalismus vom klassischen Industriekapitalismus unterscheidet, wenn auch nicht zur vollständigen Zufriedenheit der Autorin. Sie macht drei Leerstellen im bisherigen Diskurs aus: Die Analyse des Werts, der Wertrealisierung und der Distributivkraft. Diese Themen analysiert sie ausführlich und anregend in fünf Kapiteln, gefolgt von empirischen Illustrationen, u. a. zu GAFAM und der Plattform-Ökonomie. Den Abschluss bildet ein Kapitel über die Folgen unserer Wirtschaftsweise. Sehr optimistisch ist es nicht.*

> *„Meine These der Distributivkraft versucht Digitalisierung dahingehend zu verstehen, dass ein Großteil der aktuell dadurch entfachten Aktivitäten letztlich vor allem auf eines abzielt: die Realisierung von Wert auf Märkten. Es geht also nicht mehr nur um das Schaffen neuer Werte, sondern vereinfacht gesagt darum, sicherer, schneller und möglichst garantiert auf Dauer auf dem Markt erfolgreich zu sein." (S. 18f)*

Pfeiffer äußert milde Kritik an ihrer Kerndisziplin:

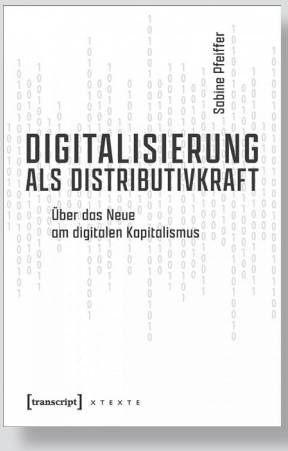
> *„[…] die Soziologie […] meidet Theorieangebote, die zumindest versuchen, alles zusammenzudenken. Zudem nimmt die Soziologie Technik oft nicht in ihrer konkreten Erscheinungsform ernst, sondern macht sie entweder zu etwas »rein« Sozialem oder missbraucht sie als vage Metapher für große, aber nicht immer weiterführende Gesellschaftsdiagnosen." (S. 12)*

Sie nimmt sich selbst nicht von Kritik aus, wenn sie bemängelt, dass die Disziplin das, was sie analysiert, nicht immer präzise benennt und angibt „was genau dafür analytisch (nicht aber real oder empirisch) ausgeblendet wird" (S. 115) und empfiehlt:

> *„Was sich im Sozialen, in der Arbeit, im Leben, in der Gesellschaft wandelt, lässt sich nur über Technik und Wirtschaft verstehen. Und über ihre jeweiligen und gemeinsamen Pfadabhängigkeiten." (S. 12)*

Im dritten Kapitel geht es Pfeiffer um den Wertbegriff, sie analysiert zunächst die Ökonomin Mariana Mazzucato, die sich in ihrem Buch „Making and Taking" mit Schöpfung und Abschöpfung von Wert befasst:

> *„Die Analyse oder gar das Ausrufen eines digitalen Kapitalismus ist nicht ihre Absicht. Im Zentrum ihrer Betrachtung steht der Kasinokapitalismus […] und die Kritik an volkswirtschaftlichen Indikatoren, die Zusammenhänge zwischen der Wertgenerierung und der Wertabschöpfung verschleiern."(S. 83)*



Sabine Pfeiffer
Digitalisierung als Distributivkraft – Über das Neue am digitalen Kapitalismus
Transcript Verlag Bielefeld, 2021
Broschur, 319 Seiten
IISBN: 978-3-8376-5422-6
Open Access als PDF unter:
https://www.sabine-pfeiffer.de/digitalisierung-als-distributivkraft

Pfeiffer reibt sich an der starken Betonung des Immateriellen durch Scott Lash und andere.

> *Code ist nicht nichts, er ermöglicht Bestimmtes und verhindert Anderes. Software beispielsweise ist sehr konkret optimiert für einen bestimmten Prozessortyp, lauffähig unter einem bestimmten Betriebssystem usw. Auch das Immaterielle trägt eine bestimmte Zwecksphäre, eine potenzielle Nützlichkeit in sich – einen Gebrauchswert. (S. 92)*

Ihr ist es wichtig, den Gegensatz von Gebrauchs- und Tauschwert nicht dualistisch sondern dialektisch zu betrachten. Läge nämlich das grundsätzlich Neue im digitalen Kapitalismus, müsste man die Verschiebung zwischen beiden Werten so genau untersuchen, wie das beispielsweise Polanyi getan hat. Sie tut es eben selbst und kommt zum Schluss, dass weder eine Unknappheit an Tauschwerten oder Kapital noch das Immaterielle wirklich neu sind. Deshalb wendet sie sich im

vierten Kapitel der Produktivkraft und dann im fünften der Wertrealisierung zu, die sie als die eigentliche Herausforderung für viele Unternehmen betrachtet. Karl Polanyis Analyse der Marktentwicklung in seiner „Great Transformation" und Karl Marx' Ausführungen zur Produktivkraftentwicklung bescheinigt sie große „Klarheit, empirische[n] Ernsthaftigkeit und analytische[n] Breite" (S. 101) es seien hilfreiche Instrumente für die weitere Suche nach dem wirklich Neuen. Das leuchtet ein, schließlich wird Polanyi heute viel gelesen und beispielsweise die Eignung seiner Erkenntnisse auch für die große sozial-ökologische Transformation geprüft. Die Autorin findet bei ihm, anders als bei anderen, die Einsicht in die vielen Ursachen für eine wirtschaftliche Revolution, sei es die industrielle oder die der *Industrie 4.0*. Während Polanyi den Wandel vom Kaufmann zum Unternehmer und damit den Produktionsprozess wie eine *Blackbox* behandelt, befasst sich Marx ausführlich damit, weil in dieser Phase Mehrwert und Profit entstehen. Er und Engels entwickelten ein komplexes sozio-technisches Konzept um die Produktivkraftentwicklung mit dem Ziel wachsender Wertschöpfung. Dieses Konzept hält Pfeiffer für weiterhin relevant, teilweise habe es sich auch im *Economic Complexity Index (ECI)* von Ceasar A. Hidalgo und Ricardo Hausman niedergeschlagen. Im Abschnitt 4.3 nimmt sie sich eine Anzahl Autorinnen und Autoren mit deren Verengungen und Missverständnissen bei der Anwendung auf den digitalen Kapitalismus vor.

Produktion und Konsum

Für Marx war die Wertrealisierung angesichts wachsender Produktion und begrenzter Konsumption ein Problem, das gab es also schon im Industriekapitalismus. Schon immer muss im Kapitalismus das Produzierte verkauft werden und noch heute ist der Konsum die Achillesferse des Kapitalisten, auch wenn Zentralbanken immer mehr Geld drucken:

> *Die ökonomische Logik von Produktion im Kapitalismus erzwingt unvermeidlich eine zunehmende Ausdehnung: erst der Produktion selbst, dann der Märkte und des Konsums. (S. 139)*

Bei dieser Ausdehnung spielt die Digitalisierung eine große Rolle. In einer Kritik der Warenästhetik sucht Wolfgang Fritz Haug die neuen Widersprüche in dieser und stellt fest, dass die Produktivkraftentwicklung auch „Technologien des Imaginären" revolutioniere: E-Commerce, Werbung, Ausschalten des Zwischenhandels, Gewinnerwartung als Versprechen von Gebrauchswert eines Unternehmens, … Das lässt sich als Verweis auf die Aufmerksamkeits-Ökonomie lesen; ein Kauf kann erst zustande kommen, wenn die Werbung wahrgenommen wird. Jean Baudrillard schreibt über Konsum als Struktur und die immer schneller steigende Produktivität, verbunden mit radikaler Entfremdung. Die Entfremdung führe in ein Zeitalter des Konsums, in dem es vor allem darum gehe, durch soziale Praktiken Statusabgrenzung zu erreichen. Weil die Kaufkraft aber nicht mit wachse und ungleich verteilt sei, wandelten sich verbreiteten Instrumente der Finanzierung: Leasing, Konsumkredite, Ratenzahlung und Kreditkarten, „bis das individuelle Konsumkartenhaus zusammenfällt und ein Verbraucherinsolvenzverfahren greift." Ferretti/Vandone bezeichnen das als „Industry of Personal Debt" (S. 147). Hier zieht Pfeiffer eine Parallele von den Codes für Kauf- und Konsumverhalten zu den Programmcodes und Algorithmen, die sie vermitteln (in personalisierter Werbung und digitalen Monopolen). Im Abschnitt 8.2 behandelt sie diesen Aspekt ausführlicher.

Auch Zygmunt Bauman befasst sich anhand von drei Fallbeispielen mit dem „Leben als Konsum", in dem Menschen sich selbst vermarkten, die in einer Doppelfunktion gleichzeitig Waren vermarkten und selbst diese Waren sind. Menschen eignen sich neue Arbeitsfähigkeiten an: „Werbung, Marketing, Suchmaschinenoptimierung, Influencing usw." (S. 150) Es bleibt das Grundproblem des Kapitalismus, den Mehrwert auf dem Markt zu realisieren, was die Digitalisierung einerseits vorantreibt, andererseits riskanter macht, weil alle Unternehmen die Instrumente nutzen, allerdings je nach Größe mit unterschiedlichen Voraussetzungen und Erfolgen. Neu ist allerdings auch das nicht. Überproduktion und Minderkonsum hängen zusammen, was ein Problem nicht nur für die Konsumenten, sondern vor allem für den Planeten ist. Auch das hatte Marx bereits vorausgesehen.

Das Neue – Distributivkraft

Gut vorbereitet mit analytischen Instrumenten und Überlegungen, kann sich die geneigte Leser:in im sechsten Kapitel auf das Neue einlassen, die Betrachtung der Distributivkraft als Mittel zum erfolgreichen Verkauf im digitalen Kapitalismus. Pfeiffer listet die Maßnahmen auf, mit denen die Prozesse in Unternehmen, auf Märkten und durch politische Regulierung optimiert werden sollen (S. 160): die Konsumwilligkeit durch geplante Obsoleszenz, Marketing, Werbung, Nudging; ein Kaufzwang durch Nutzung statt Kauf bei Abo-Modellen, Streaming- oder anderen Cloud-Diensten; mehr und effizientere Kaufgelegenheiten; optimierte Logistik beim Verkauf und Prognosen des Konsumverhaltens. An diesem Strang zieht auch die Politik: Sie erhält die Konsumfähigkeit trotz erschwerter Bedingungen aufrecht, dehnt Märkte durch Freihandels-Abkommen und Ähnliches aus, schafft die Bedingungen für eine zielgerichtete Bildung der Profis. Der gesellschaftliche Diskurs setzt Innovation gleich mit Markterfolg statt sozialem Fortschritt, der Begriff der Disruption wird eingeführt und als positiv propagiert. Wertrealisierung ist das neue Ziel von Wissenschaft und Berufen, und Distribution kostet. Karl Marx sagte dazu bereits:

> *Diese sämtlichen Kosten werden nicht gemacht in der Produktion des Gebrauchswerts der Waren, sondern in der Realisation ihres Werts; sie sind reine Zirkulationskosten. (S. 161)*

Im sechsten Kapitel analysiert Pfeiffer drei Ebenen der Distributivkräfte: Werbung und Marketing; Transport und Lagerung; Steuerung und Prognose, sie beschreibt Kontinuitäten und neue Aspekte, wie sie sich besonders in den Techniken der GAFAM zeigen. Im siebten präzisiert sie den Begriff und schließt die dritte Leerstelle, bevor sie im achten Kapitel empirisch

überprüft, ob ihre Distributivkraft-Brille dabei hilft, den real existierenden digitalen Kapitalismus klarer zu sehen.

Das neunte Kapitel zeigt auf etwa 20 Seiten, was für tiefgreifende Veränderungen sich in der Arbeitswelt und beim Einsatz der Technik, aber eben auch im Kapitalismus selbst zugetragen haben. Hier geht es um Reproduktion und Destruktion und den Blick auf die ökologischen Folgen dieser Wirtschaftsweise. Kann die Künstliche Intelligenz/das maschinelle Lernen ein Ausweg sein? Kann intelligente(re) Technik der menschlichen Dummheit abhelfen? Ich verrate Pfeiffers Meinung dazu nicht, sie hat aber auch da genau hingeguckt.

Empfehlung

Nicht alle Soziologen schreiben gut, Sabine Pfeiffer kann das, sogar wenn es um ein ökonomisches Thema geht. Sie entwickelt eine analytische Perspektive, die Technikentwicklung, ökonomische Logik und gesellschaftliche Dynamik gemeinsam statt als sequenzielle Abfolge betrachtet. Ihr Buch ist didaktisch aufgebaut, mit einer Einführung in die Inhalte jedes Kapitels, die sie dann vertieft, verständlich und ohne unnötige Längen. Anspruchsvoll ist es aber schon; die geschätzte Leser:in sollte Pfeiffers kritisches Interesse für die Volkswirtschaftslehre teilen. Ein Grundverständnis der Marxschen Ideen hilft, ist aber nicht Voraussetzung.

Dagmar Boedicker

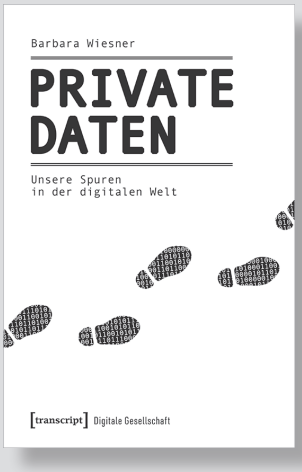
Barbara Wiesner: Private Daten – Unsere Spuren in der digitalen Welt

Barbara Wiesner hat ein schönes, kurzes Büchlein über das Verhältnis von Komfort und Selbstbestimmung geschrieben. Sie nennt Privatheit, was uns ermöglicht zu sprechen und zu handeln, ohne dass andere davon wissen, seien es nun GAFAM[1] oder wer auch immer. Es ist weniger ein Buch für Engagierte im FIfF e. V. als vielmehr eins, das Sie Menschen in die Hand drücken können, die als Laien wenig darüber wissen, was bei der Verarbeitung ihrer Daten geschieht und welche Folgen das haben kann. Wiesner lässt es nicht bei einer Beschreibung dieses Zusammenhangs bewenden, sie gibt auch Hinweise, wie Nutzerïnnen sich schützen können.

Private Daten muss niemand am Stück lesen, jedes Kapitel steht für sich und Zitate ziehen sich durch das Buch, an denen die geneigte Leserïn beim Stöbern anhalten und sich weiter in den Text schwingen kann. Wiesner hat gut recherchiert, ein langes Literaturverzeichnis liefert Anregungen zum Weiterlesen, und sie greift die wesentlichen Aspekte heraus. Diese Aspekte können zwei Seiten haben: Der Sohn des Philosophen Michael Sandel lebt völlig entspannt mit der Tatsache, dass die NSA weiß, mit wem er kommuniziert. Würden seine Eltern es wissen (wollen), empfände er das als Verletzung seiner Rechte (S. 46f). Ein anderes Beispiel: Wenn Eric Schmidt von Alphabet (Google) findet, dass Menschen nur tun sollten, was andere Menschen wissen dürften (S. 51), spricht es nicht für sein Demokratieverständnis.

Wiesner ist weder Missionarin noch Besserwisserin, sie lässt die Fakten einfach einfließen, wie beispielsweise die Tatsache, dass bei einem ersten *Smart-Home*-Projekt die Daten ganz selbstverständlich nur den Hausbewohnern zur Verfügung standen. Dazu muss sie keine Ausführungen über die Begehrlichkeiten von Datenkraken ausbreiten, vielmehr erläutert sie, dass auch heute noch für den Komfort beim eigenen Heim die Verbindung ins Internet nicht erforderlich ist.

Wenn es um die Begehrlichkeiten von Staaten und ihren Sicherheitsbehörden geht, sind die sich keineswegs alle einig. Wiesner zitiert zwei hochrangige ehemalige Sicherheitspolitiker der USA, die für übertrieben halten, was andere als das Ende der Strafverfolgung und Prävention bezeichnen – die Verschlüsselung. Auch hier weist sie auf die zwei Seiten der Medaille hin: Über Hintertüren entschlüsselbare Kommunikation oder Trojaner machen die Kommunikation für alle unsicher.



Barbara Wiesner
Private Daten – Unsere Spuren in der digitalen Welt
Transcript Verlag Bielefeld, 2021
Broschur, 107 Seiten
ISBN: 978-3-8376-5605-3

Fazit

Ich finde das Buch gut geeignet als Weihnachtsgeschenk für Freunde und Bekannte, mit denen wir uns schon mal über den sogenannten Datenschutz unterhalten haben, vor allem, wenn sie nicht glauben, alles darüber zu wissen. Sogar wer „mir doch egal" denkt, könnte sich bereitfinden, angesichts der Kürze und angenehmen Lesbarkeit doch etwas Zeit dafür aufzubringen. Es lohnt sich.

Anmerkung

1 Google, Amazon, Facebook, Apple, Microsoft – die großen Fünf

FIfF e.V.

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

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

FIfF-Mailinglisten

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

FIfF-Mitgliederliste
An- und Abmeldungen an:
http://lists.fiff.de/mailman/listinfo/mitglieder

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

FIfF online

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

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

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

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

FIfF-Beirat

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

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 – 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
Philip Love – Bremen

Impressum

Herausgeber	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF)
Verlagsadresse	FIfF-Geschäftsstelle Goetheplatz 4 D-28203 Bremen Tel. (0421) 33 65 92 55 *fiff@fiff.de*
Erscheinungsweise	vierteljährlich
Erscheinungsort	Bremen
ISSN	0938-3476
Auflage	1 200 Stück
Heftpreis	7 Euro. Der Bezugspreis für die FIfF-Kommunikation ist für FIfF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FIfF-Kommunikation für 28 Euro pro Jahr (inkl. Versand) abonnieren.
Hauptredaktion	Dagmar Boedicker, Stefan Hügel (Koordination), Sylvia Johnigk, Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht, Ingrid Schlagheck
Schwerpunktredaktion	Hans-Jörg Kreowski, Aaron Lye
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	Collage von Janina Thiede
Druck	Meiners Druck, Bremen Heftinhalt auf 100 % Altpapier gedruckt.

KLIMAneutral produziert

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

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

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

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

Aktuelle Ankündigungen

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

FIfF-Kommunikation

1/2022 FIfFKon 2021 – Selbstbestimmung in digitalen Räumen
Dagmar Boedicker u. a.
Redaktionsschluss: 4. Februar 2022

2/2022 Künstliche Intelligenz, Automatisierung und Ethik
Hans-Jörg Kreowski, Stefan Hügel
Redaktionsschluss: 6. Mai 2022

3/2022 Politik, Staat und Verwaltung
Jörg Pohle, Stefan Hügel
Redaktionsschluss: 5. August 2022

4/2022 100 Jahre Joseph Weizenbaum
Stefan Ullrich, Andrea Knaut
Redaktionsschluss: 4. November 2022

Zuletzt erschienen:

3/2020	Technologie und Ökologie
4/2020	Digitalisierung in der Bildung
1/2021	FIfFKon 2020 – Datenschutz, Usability, Barrierefreiheit und Sicherheit – Teil 1
2+3/2021	FIfFKon 2020 Teil 2

W&F – Wissenschaft & Frieden

2/21	Völkerrecht in Bewegung. Von Krisen, Kritik und Erneuerung
3/21	Frieden lernen, aber wie? – Aktuelle Fragen der Friedenspädagogik
4/21	Chinas Welt? – Zwischen Konflikt und Kooperation

vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik

#230	30 Jahre Deutsch-Deutsche Wiedervereinigung
#231/232	Zwei Jahre Datenschutz-Grundverordnung
#233	Kirchliches Sonderarbeitsrecht

DANA – Datenschutz-Nachrichten

2/21	Bildung
3/21	E-Government
4/21	E-privacy-Verordnung

Das FIfF-Büro

Geschäftsstelle FIfF e. V.
Ingrid Schlagheck (Geschäftsführung)
Philip Love
Goetheplatz 4, D-28203 Bremen
Tel.: (0421) 33 65 92 55, Fax: (0421) 33 65 92 56
E-Mail: fiff@fiff.de
Die Bürozeiten finden Sie unter *www.fiff.de*

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

Kontakt zur Redaktion der FIfF-Kommunikation:
redaktion@fiff.de

Schluss FIfF

Hans-Jörg Kreowski

Es trifft nicht zu, dass die scheidende Bundesregierung wenig geleistet hat, sie hat immerhin die deutsche Sprache bereichert

merkeln = mit weitgehender Untätigkeit vielerorts Ansehen einheimsen

scholzen = Geld ausgeben mit Bumms

seehofern = reaktionäre Innenpolitik mit Modelleisenbahn nachbauen

maasen = nahezu wirkungslos für internationalen Ausgleich werben

altmaiern = den Reichen Extraprofite zuschanzen

lambrechten = sich um Recht bemühen, es aber selten bekommen

heilen = sich für Benachteiligte einsetzen, ohne dass die das merken

kramp-karrenbauern = Töten und Getötet-Werden zum normalen Beruf erklären

klöcknern = ohne Rücksicht auf Klima und Natur landwirtschaften

giffeyen = lieber bürgermeistern

spahnen = Maßnahmen lediglich ankündigen

scheuern = viel Geld in den Sand setzen durch verqueres Verkehren

schulzen = der Umwelt zuliebe, doch wenig erreichen

karliczeken = ahnungs- und ideenlos wissenschaften

müllern = fast fortschrittliche Entwicklungen anstoßen trotz CSU-Parteibuch

braunen = mit einer Farbe im Namen farblos bleiben

bären = Flugtaxis mit Digitalisierung verwechseln

Geeignete Texte für den SchlussFIfF bitte mit Quellenangabe an *redaktion@fiff.de* senden.