H 7625

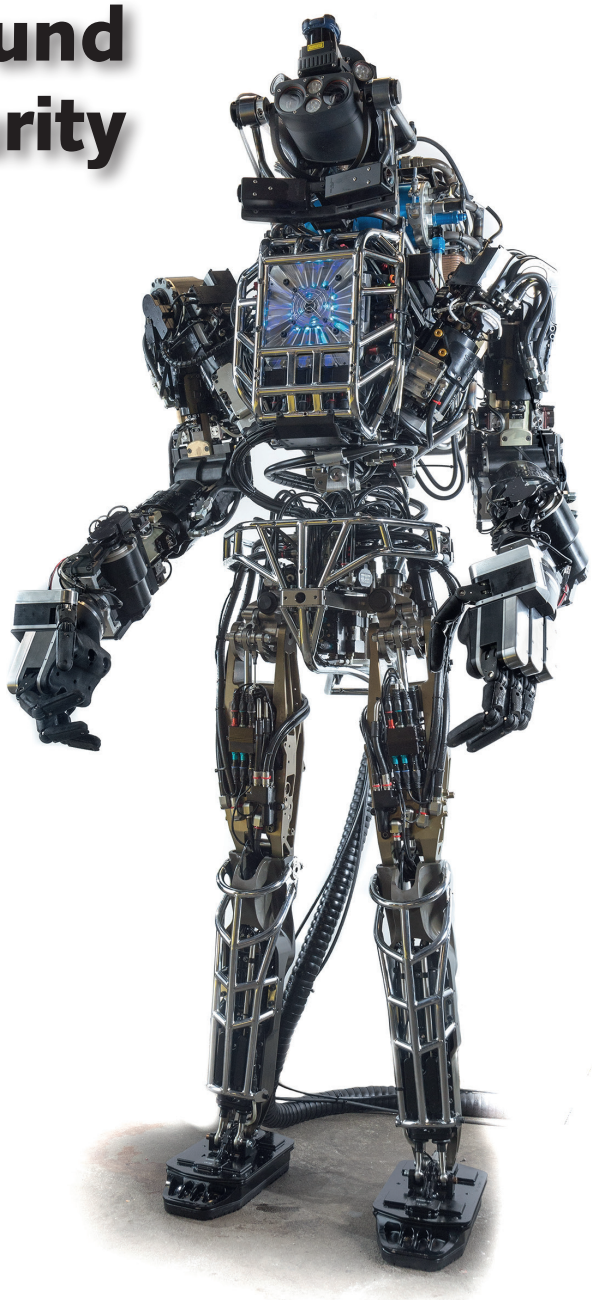
FIfF-Kommunikation

Zeitschrift für Informatik und Gesellschaft

36. Jahrgang 2019 Einzelpreis: 7 EUR 3/2019 – September 2019

Cyberpeace und IT-Security

BigBrother-Awards 2019



ISSN 0938-3476

• Ankündigung FIfFKon • Alternativen zu Gated Communities • Veränderung durch Algorithmen •

FIfF Kommunikation

Zeitschrift für Informatik und Gesellschaft

Inhalt

Ausgabe 3/2019

inhalt

Titelbild: BigBrotherAward (Symbolbild) (Links)
„Atlas“ von Boston Dynamics, Defense Advanced Research Projects Agency (DARPA), 2013 (Rechts)

Editorial

Cyberpeace und IT-Security sind wesentliche Kernthemen des FIfF. Wir verstehen uns als sowohl in der digitalen Bürgerrechtsbewegung als auch in der Friedensbewegung verankert, und wollen zwischen diesen beiden Bereichen vermitteln und die Gemeinsamkeiten herausarbeiten. So ist dieses Thema wieder einmal Schwerpunkt einer Ausgabe der *FIfF-Kommunikation*, der von *Michael Ahlmann*, *Sylvia Johnigk*, *Hans-Jörg Kreowski* und *Kai Nothdurft* gestaltet wurde.

Nach dem Schwerpunkteditorial, das detailliert in die Thematik einführt, enthält der Schwerpunkt vier Beiträge, die den Luftwaffenstützpunkt im Schleswig-Holsteinischen Jagel, autonome Kampfroboter und Fragen der Roboterethik, Rüstungskontrolle im Cyberspace und mögliche Folgen des Verstoßes staatlicher Institutionen gegen das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zum Inhalt haben.

Tornado der deutschen Luftwaffe auf dem Flugplatz in Jagel bei Schleswig – Foto: Wusel007, CC BY-SA 3.0

Schon vor fünf Jahren, zu Beginn der Kampagne *Cyberpeace,* diskutierten wir die Frage nach der Bedeutung des Cyberwar, der sich kaum mit den sonstigen Kriterien bewaffneter Konflikte messen lässt. Kritiker des Konzepts wenden ein, dass das Kriterium für einen Krieg – 1.000 Tote durch direkte Kampfhandlungen pro Jahr (vgl. bei *Department of Peace and Conflict Research* der *Universität Uppsala*) – in einem Cyberwar noch niemals annähernd erreicht wurde. Glücklicherweise, muss man ergänzen, doch dennoch entstehen jenseits solcher Definitionen reale Gefahren aus diesen Operationen. Dass Cyberwar eine echte Bedrohung und keine Schimäre ist, stellten *Sylvia Johnigk*, *Hans-Jörg Kreowski* und *Kai Nothdurft* schon damals in ihrem Beitrag klar, den wir in der Rubrik *Retrospektive* erneut abdrucken.

Für die Arbeit des FIfF leitet die Schwerpunktredaktion eine klare Forderung ab:

> *„Gerade die von uns durchgeführten Analysen der zu erwartenden Bedrohungen durch Cyberkrieg haben sich also leider erneut als realistisch und keineswegs schwarzmalerisch erwiesen. Umso mehr muss es auch in den nächsten Jahren eine Kernaufgabe des FIfF bleiben, Transparenz zu schaffen. Ebenso wichtig ist aber auch, wahlentscheidend große Personengruppen zu diesem Thema aufzuklären und sich nicht auf die kritische Analyse im akademisch-fachlichen Diskurs zu beschränken."*

Sie nennt dabei als Beispiel unser Video *Cyberpeace statt Cyberwar*, das im Rahmen der Cyberpeace-Kampagne entstanden ist.

Die Rubrik *Forum* enthält neben dem gewohnten *Brief* drei Beiträge: Wie auch in anderen Bundesländern wurde in Hessen 2018 die *Verschärfung des Polizei- und des Verfassungsschutzgesetzes* massiv vorangetrieben. Die mit dem Einsatz von Überwachungssoftware verbundenen Risiken für Bürgerrechte und IT-Sicherheit bleiben dabei außer Acht. Besonders gravierend in Hessen ist die Software *Hessen-Data* des US-Unternehmens *Palantir*, die weitgehende Analysen durch Verknüpfung unterschiedlicher Datenbestände bereits im Vorfeld von Straftaten ermöglichen soll und die nun aufgrund der Gesetzesnovelle eingeführt werden kann. Bereits bei der Anhörung im Hessischen Landtag war das FIfF im Februar 2018 beteiligt; in einer Verfassungsbeschwerde greifen nun die Gesellschaft für Freiheitsrechte (GFF), die Humanistische Union, die Datenschützer Rhein-Main und das FIfF die neuen Bestimmungen an. Wir drucken die dazu veröffentlichte Pressemitteilung; die Beschwerdeschrift ist bei der GFF im Netz zu finden.

Die Veränderung des Sozialen durch Algorithmen untersucht *Markus Reinisch* in seinem Beitrag. Sie werden nicht mehr nur für technische Problemlösungen, sondern auch zu Rationalisierung in sozialen Bereichen eingesetzt, und stellen ein Werkzeug zur Erfassung und gezielten Verteilung von Informationen dar. Darüber hinaus beschreibt der Autor Algorithmen als einflussreiche Kulturtechnik und Diskursfigur. Er weist darauf hin, dass

> *„letztlich … Algorithmen – trotz aller Fortschritte um Deep Learning – auf einer distanzierenden Meta-Ebene niemals über ein Bewusstsein darüber verfügen (werden), dass mit ihrem Einsatz eine enorme gesellschaftliche Verantwortung einhergeht. Gerade die Fähigkeiten, kritisch Distanz zu einem Objekt aufzunehmen sowie daraufhin Entscheidungen zu treffen, wird Menschen vorbehalten bleiben, die auch die Verantwortung dafür übernehmen. Denn es wird immer gelten: ‚Vom menschlichen Lernen ist das algorithmische Lernen kategorial verschieden.'"*

Die Risiken durch Datenspeicherung und -auswertung und die daraus entstehenden *Gated Communities* durch Anbieter sozialer Netze wie Facebook und mögliche Alternativen dazu diskutieren *Katharina Nocun* und *Patrick Breyer* in ihrem Beitrag, den wir mit freundlicher Genehmigung aus der Zeitschrift **vor***gänge* nachdrucken. Neben der Überwachung und Analyse der Mitglieder bis hin zu intimen Lebensäußerungen wird eine Infrastruktur geschaffen, die ein Ausbrechen schwierig oder unmöglich machen soll. Sie mahnen politischen Handlungsbedarf an:

> *Soziale Netzwerke sind Teil unserer politischen Wirklichkeit. Es ist essentiell, dass wir in einer demokratischen Gesellschaft darüber diskutieren, nach welchen Regeln die neue Öffentlichkeit funktionieren soll – und welche Formen der Verwertung und Manipulation wir als gefährlich erachten. Darauf zu hoffen, dass eine Strategie zur Maximierung des Unternehmensgewinns zufällig auch das gesellschaftlich bestmögliche Ergebnis hervorbringt, wäre mehr als naiv. Höchste Zeit, dass sich die Politik hier bewegt.*

Chor „One Voice“ bei der Preisverleitung
Foto: Mischa Burmester, CC BY- SA 4.0

Über die *BigBrotherAwards 2019* berichten wir wie gewohnt und drucken eine Auswahl von Laudationes ab. Mit dem bereits oben angesprochenen Thema der Spähsoftware *Hessen-Data* befasst sich *Rolf Gössner* mit seiner Laudatio auf den *Hessischen Innenminister* Peter Beuth, die Risiken von DNA-Analysen zur Ahnenforschung behandelt *Thilo Weichert* in der Laudatio auf das Unternehmen *Ancestry.com* und die Nutzung von Sprechproben verbunden mit der unkritischen Anwendung von Machine Learning zur Beurteilung von StellenbewerberInnen kritisiert *Rena Tangens* in ihrer Laudatio auf das Unternehmen *Precire*.

Unsere Rubrik *Netzpolitik.org* beginnt mit einem Beitrag von *Lorenz Hilty* von der Konferenz *Bits & Bäume*, in dem er sich mit der Material- und Ressourcenverschwendung durch die kurzen Lebenszyklen von IT-Geräten auseinandersetzt, und sie enthält zwei Beiträge von *Markus Reuter*, in denen er Twitter-Strategien der AfD und Hasspostings von rechts analysiert. *Matthias Monroy* schreibt über die geplante europaweite Abfrage von Gesichtsbildern und *Anna Biselli* über Blockchain-Forensik.

Die detaillierte Ankündigung unserer FIfF-Konferenz 2019, *Künstliche Intelligenz als Wunderland*, vom 22.–24. November 2019 in Bremen mit den geplanten ReferentInnen rundet die Ausgabe ab. Freut Euch auch in diesem Jahr auf eine spannende Konferenz zu diesem wichtigen Thema.

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

Stefan Hügel
für die Redaktion

Der Brief

Kommunikation

Liebe Leserinnen und Leser, liebe Mitglieder des FIfF,

in meiner Kindheit, bei Gesprächen mit Gleichaltrigen auf der Straße oder auf dem Fußballplatz, fiel mir früh etwas auf: Sagte jemand etwas (vermeintlich) falsches, so reagierten manche auffällig aggressiv: „Was redest Du für einen Unsinn“, oder gleich persönlich: „Du Depp!“ Damals fragte ich mich schon, ob man andere nicht auch einfach ruhig und sachlich auf einen Irrtum hinweisen, oder gar das Thema einfach auf sich beruhen lassen hätte können. Zumal – wer bei der zu klärenden Frage gerade Recht hatte, war nicht immer sofort klar. Freilich ging es dabei eher um Fragen wie: in welcher Spielminute des Weltmeisterschaftsendspiels 1974 verwandelte Paul Breitner den Elfmeter zum Ausgleich? (Ehe Ihr jetzt nachschauen müsst: laut Wikipedia war es die 25.)

Eine extreme und weniger amüsante Form dieser Aggressivität ist inzwischen als *Hate-Speech* in der Diskussion. Das wird heute i. d. R. mit sozialen Medien in Verbindung gebracht. Aber wenn wir uns anschauen, was über Persönlichkeiten, die in der öffentlichen Debatte standen, früher teilweise hereinbrach – ich denke an Persönlichkeiten wie Willy Brandt oder den damaligen Hessischen Generalstaatsanwalt Fritz Bauer – sehen wir, dass sich gar nicht so viel geändert hat; allenfalls hat die Menge zugenommen: Auch sie waren Hass ausgesetzt, der bis zur Morddrohung reichte. Heute ist ein Tweet schnell geschrieben und verschickt. In den 1960-er und 1970-er Jahren musste man die Morddrohung auf einen Zettel schreiben, in einen Briefumschlag stecken, zur Post gehen, eine Briefmarke kaufen und den frankierten Brief dann in den nächsten Briefkasten werfen. Recht viel Aufwand, um einem unbekannten Menschen seinen Hass mitzuteilen. Und trotzdem wurde es gemacht.

Heute haben wir das Internet. Eine fantastische Möglichkeit, global zu kommunizieren, zu lernen, Freundschaften zu schließen und vieles mehr. Klar, wir müssen die Chancen und Risiken des Internet und seiner Plattformen und Anwendungen kritisch gegeneinander abwägen und es so gestalten, dass es größtmöglichen Nutzen für die Verständigung der Menschen stiftet. Weder naiver Technikoptimismus à la *Digital first* noch pauschale Ablehnung bringt uns weiter. Die elektronische Kommunikation entwickelt sich zu einer Kulturtechnik – irgendwann vielleicht wie heute Lesen und Schreiben –, die wir vor allem unseren Kindern von Anfang an kritisch vermitteln müssen.

Dazu gehört aber auch: Bei der Verbreitung von Hass wirkt das Internet als Brandbeschleuniger. Ein Tweet ist schnell verschickt, andere stimmen ein, so entsteht der Shitstorm, manchmal aus nichtigem Anlass.

Besonders gravierend wird dies dann, wenn solche Hass-Kampagnen gezielt hervorgerufen und orchestriert werden. Hier tun sich aber auch „klassische“ Organisationen prominent hervor: z. B. die AfD im Bereich der Parteipolitik und die *Bild* im Be-

reich der Presseerzeugnisse. Man hat den Eindruck, dass beide die Möglichkeiten sozialer Medien gezielt nutzen – zur Optimierung der Wählerstimmen oder der Auflage. Wie die AfD strategisch Twitter nutzt, um ihre politischen Botschaften gezielt zu streuen hat nichts mit den völkerverbindenden Möglichkeiten eines weltumspannenden Kommunikationsnetzes zu tun (siehe dazu Seite 50 in dieser Ausgabe). Die *Bild* ist bereits seit Jahren als Blatt verrufen, das es mit Wahrheit und fairer Berichterstattung nicht immer so genau nimmt. Erschreckend ist die Konsequenz und Skrupellosigkeit, mit der Debatten zugespitzt und zu politischen Hetzkampagnen entwickelt werden.

Ein besonderes Beispiel für eine derartige Kampagne konnten wir gerade beobachten: Am Frankfurter Hauptbahnhof stieß ein – späteren Medienberichten zufolge wohl psychisch erkrankter – Mann eine Mutter und ihr Kind auf die Gleise. Der achtjährige Junge wurde von einem einfahrenden ICE überrollt und starb. Dieses furchtbare Ereignis, und die Tatsache, dass der Verursacher aus Eritrea stammt, nahm die Oppositionsführerin (!) im Deutschen Bundestag, Alice Weidel, sogleich zum Anlass, erneut gegen die Bundesregierung und ihre vermeintlich zu flüchtlingsfreundliche Politik zu hetzen. So ein Ereignis für politische Stimmungsmache zu missbrauchen, ist widerwärtig.

Neben den Reaktionen auf solche Ereignisse werden auch einzelne Personen immer wieder zur Zielscheibe von Hasskampagnen, wenn sie Meinungen vertreten, die in konservativen und rechten Kreisen nicht genehm sind. Dem Gefühl nach sind häufig Frauen davon betroffen – sehen die *Hater* in ihnen vielleicht ein leichteres Opfer? Im Jahr 2000 wurde die Fernsehshow *Big Brother* zum ersten Mal ausgestrahlt. Eine der Teilnehmerinnen, „Manuela", geriet schnell ins Visier der ZuschauerInnen. Sie wurde als „Zicke" und „Schlampe" beschimpft; anscheinend versammelte sich damals sogar ein wütender Mob vor dem Studio, der ihren sofortigen Rauswurf aus dem *Big-Brother-Haus* forderte. Man mag eine solche Gruppendynamik unglaublich finden, in einer Gesellschaft, die auf ein kooperatives Miteinander angewiesen ist. Ist es eine solche Dynamik, die auch bereits 1933 in letzter Konsequenz das Naziregime möglich gemacht hat?

Heute beobachten wir solche massiven Hasskampagnen zu gesellschaftlich kontroversen Themen. Themen, bei denen viele etwas zu verlieren haben oder zu verlieren zu haben glauben. Diese Debatten, die u. a. von den oben genannten Institutionen immer wieder angeheizt werden, sind heute vor allem die vermeintlich zu liberale Flüchtlingspolitik und die sich immer deutlicher abzeichnende Klimakatastrophe. Die Journalistin Dunja Hayali veröffentlichte wiederholt Tweets und Kommentare, die sie aufgrund ihrer Haltung erhalten hat. Es ist erschreckend: Einige dieser Kommentare kann man mit Kategorien zivilisierten Zusammenlebens nicht mehr bewerten.

Ein anderes Beispiel ist die schwedische Klimaaktivistin Greta Thunberg. Klar – bei den Maßnahmen, die zum Klimaschutz mittlerweile notwendig sind, haben wir alle eine Menge zu verlieren. Durch jahrzehntelanges Nichtstun – „die Frau Merkel macht das doch ganz gut" – haben wir das Zeitfenster für konkrete Maßnahmen zum Klimaschutz immer kleiner gemacht. Heute stehen wir offensichtlich vor der Situation, dass nur vergleichsweise drastische Maßnahmen die unvermeidliche Erderwärmung noch begrenzen können. Diese Maßnahmen werden schmerzhaft sein – doch das haben wir uns selbst zuzuschreiben. Greta Thunberg und der von ihr maßgeblich initiierten Bewegung *Fridays for Future* haben wir zu verdanken, dass der Problematik endlich das notwendige öffentliche Interesse zuteil wird.

Und was passiert? Als „krank" wird Greta Thunberg bezeichnet, als „fremdgesteuert" – von Menschen, die niemals auch nur annähernd so viel bewegen werden, wie es Greta schon mit 16 Jahren geleistet hat. Ich wünsche mir, dass sie in diesem Jahr den Friedensnobelpreis erhält – ich kann mir keine geeignetere vorstellen.

Klar – Greta Thunberg braucht starke Unterstützer: Eine weltweite Bewegung vertritt man nicht eben mal vom Kinderzimmer aus. Klar – ihre Reise mit einer Segelyacht über den Atlantik ist ein eher symbolischer Akt, der nicht als Modell für normale Geschäftsreisen taugt. Und klar – in einer weltweiten Bewegung sind inhaltliche Differenzen unvermeidlich: ob Kapitalismuskritik notwendig ist oder nicht, oder vielleicht auch ob Steuern, Emmissionszertifikate oder freiwillige Selbstverpflichtungen der beste Weg sind, um den Ausstoß von CO_2 dauerhaft und nachhaltig zu reduzieren. Aktuell versuchen es manche mit einer Form des Ablasshandels, indem man das freigesetzte CO_2 durch Investitionen in „klimafreundliche" Projekte kompensieren will. Eins ist klar: Die bisherigen Versuche waren definitiv nicht ausreichend. Doch PolitikerInnen – ausgerechnet auch der Grünen – betonen sogleich reflexhaft, sie lehnten es ab, „Menschen ihren Lebensstil vorzuschreiben".

Wird es Zeit, zur Gründung einer neuen ökologischen Partei aufzurufen?

Aber ich wollte über Kommunikation schreiben. Es ist nichts neues: auch diese ist letztlich interessengesteuert. Letztlich hilft es nur, Hasskampagnen konsequent entgegenzutreten – auch das ist Demokratie. Den Rahmen setzt das Grundgesetz, Art. 5:

> *(1) Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Die Pressefreiheit und die Freiheit der Berichterstattung durch Rundfunk und Film werden gewährleistet. Eine Zensur findet nicht statt.*
>
> *(2) Diese Rechte finden ihre Schranken in den Vorschriften der allgemeinen Gesetze, den gesetzlichen Bestimmungen zum Schutze der Jugend und in dem Recht der persönlichen Ehre.*

Das muss der Konsens sein, auf dessen Basis wir uns verständigen. Dem Versuch, dieses Recht zu untergraben – dazu gehört auch die Einschüchterung durch Hass und Beschimpfungen – müssen wir, ebenso wie seinem Missbrauch, entschieden entgegentreten. Aber auch eins ist klar: Es ist nicht schon dann eine Verletzung der Meinungsfreiheit, wenn jemand der eigenen Meinung widerspricht.

Mit FIfFigen Grüßen
Stefan Hügel

FIfF e. V. – Pressemitteilung

Verfassungsbeschwerde gegen Polizeigesetz und Verfassungsschutzgesetz Hessen eingelegt

Hessentrojaner und Hessendata greifen Grundrechte an

Berlin/Wiesbaden, 2. Juli 2019 – Die Gesellschaft für Freiheitsrechte e. V. (GFF) hat gemeinsam mit der Humanistischen Union (HU), den Datenschützern Rhein Main (dDRM) und dem Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) heute in Karlsruhe eine Verfassungsbeschwerde gegen das neue Hessische Polizeigesetz und Verfassungsschutzgesetz eingelegt.

Die Beschwerde richtet sich gegen die Ausweitung der Überwachungsbefugnisse für Polizei und Verfassungsschutz. „Mit dem Hessentrojaner und der Big-Data-Analysesoftware Hessendata liegt Hessen beim Angriff auf die Freiheitsrechte im Ländervergleich weit vorne" sagt Sarah Lincoln, Juristin bei der Gesellschaft für Freiheitsrechte.

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

Der Einsatz des sogenannten Hessentrojaners gefährdet die IT-Sicherheit aller BürgerInnen. Die Polizei kann IT-Sicherheitslücken geheim halten und sie für Überwachungsmaßnahmen ausnutzen, statt darauf hinzuwirken, dass sie schnellstmöglich vom Hersteller geschlossen werden. Dieselben Sicherheitslücken können dann aber auch Cyberkriminelle und ausländische Geheimdienste für Cyberangriffe nutzen.

„Der geringe potenzielle Gewinn an Sicherheit durch den sogenannten Hessentrojaner steht in einem extremen Missverhältnis zur massiven Gefährdung von unzähligen IT-Systemen weltweit", führt Roman Peters von dieDatenschützer Rhein Main aus.

„Als Journalist und Bürgerrechtler bange ich um meine Informationsquellen", erklärte der Marburger HU-Regionalvorsitzende und Beschwerdeführer Franz-Josef Hanke. „Ich kann künftig nicht mehr darauf hoffen, dass mir von Überwachung bedrohte Menschen überhaupt noch etwas über Telefon oder Email anvertrauen."

Unter den sieben BeschwerdeführerInnen sind neben HU-Regionalvorsitzenden Franz Josef Hanke auch die Rechtsanwältin Seda Başay-Yıldız, Klaus Landefeld als Vorstandsmitglied des Verbands der Internetwirtschaft eco und DE-CIX Aufsichtsrat sowie Silvia Gingold, Lehrerin in Ruhestand und Tochter des jüdischen Widerstandskämpfers Peter Gingold, die aufgrund ihres antifaschistischen Engagements seit ihrer Jugend unter Beobachtung des Verfassungsschutzes steht.

Das neue Verfassungsschutzgesetz sieht unter anderem den weitreichenden Einsatz von verdeckten Ermittlern, die Ortung von Mobilfunkgeräten und die Überwachung von Reiserouten vor. Einmal erhobene Daten kann der Verfassungsschutz nahezu voraussetzungslos an andere öffentliche Stellen und an ausländische Regierungen weiterleiten. Betroffene selbst haben nur sehr eingeschränkte Auskunftsrechte darüber, welche Daten über sie erhoben wurden.

Für die angegriffenen Überwachungsbefugnisse hat die Hessische Landesregierung inzwischen bereits zweimal den *Big Brother Award* erhalten, mit denen jährlich Datensünder in Wirtschaft und Politik prämiert werden.

Die **Gesellschaft für Freiheitsrechte e. V.** (GFF) initiiert, koordiniert und finanziert gerichtliche Verfahren, um die Grund- und Menschenrechte zu verteidigen. Sie bringt dafür geeignete KlägerInnen mit exzellenten JuristInnen zusammen, um gemeinsam gerichtlich gegen Rechtsverletzungen vorzugehen.

Im Internet: *info@freiheitsrechte.org / freiheitsrechte.org / @freiheitsrechte*

***die*Datenschützer Rhein Main** sind eine Bürgerrechtsgruppe, die sich im Bereich Datenschutz und Informationsfreiheit engagiert. Sie beschäftigen sich u. a. mit den Themen Sozialdatenschutz, Digitalisierung des Gesundheitswesens, Videoüberwachung und Vorratsdatenspeicherung.

Im Internet: *info@ddrm.de / ddrm.de / @Dat3nschutz*

Als größte und älteste Bürgerrechtsorganisation Deutschlands engagiert sich die **Humanistische Union** (HU) seit 1961 für Freiheitsrechte und Demokratie.

Im Internet: *info@humanistische-union.de / humanistische-union.de / @humunion*

Das **Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V.** (FIfF) sind ca. 700 Fachleute aus der Informatik, dem IT-Bereich und IT-nahen Berufsfeldern, die sich kritisch mit den Auswirkungen des IT-Einsatzes in unserer Gesellschaft auseinandersetzen.

Im Internet: *fiff@fiff.de / fiff.de / @FIfF_de*

Weitere Informationen: *https://freiheitsrechte.org/polizeigesetz-hessen/*

Beschwerdeschrift:
https://freiheitsrechte.org/home/wp-content/uploads/2019/07/2019-07-01-VB-Hessen-finalohneAdressen.pdf

Markus Reinisch

Die Veränderung des Sozialen durch Algorithmen

*„*Algorithmus *war einmal ein unschuldiges, ein bisschen langweiliges Wort, so ähnlich wie* Grammatik *oder* Multiplikation*“, schrieb die Schriftstellerin und Journalistin Kathrin Passig vor sechs Jahren im Rahmen ihrer Algorithmenkritik.[1] Mittlerweile ist es alles andere als langweilig, beeinflussen Algorithmen doch viele Lebensbereiche massiv und stehen für eine veränderte, mathematische Sicht auf die Welt. Sie werden nicht mehr nur für technische Problemlösungen, sondern vermehrt in sozialen Bereichen zur Rationalisierung eingesetzt. Vermutlich hat Frau Passig die beiden Vergleichs-Begriffe Grammatik und Multiplikation mit Bedacht gewählt, denn beide haben mit der Eigenart von Algorithmen entscheidend zu tun: Zum einen wird der einflussreiche Zeichencode, die grammatikalische Struktur der Algorithmen, häufig als undurchschaubare Black Box diskutiert. Zum anderen stellt der Algorithmus ein wirkungsmächtiges Werkzeug zur Erfassung und massenhaften, aber gezielten Verteilung von Informationen (Multiplikation) dar.*

Im Folgenden geht es neben diesen beiden Aspekten um den Algorithmus als einflussreiche „Kulturtechnik und Diskursfigur“[2] im Gefolge von *Big Data*. Allen voran wird beleuchtet, wie durch die Aufwertung seiner mathematischen Logik und durch seinen verstärkten Einsatz die bisherige Vorstellung des Sozialen grundlegenden Veränderungen unterworfen ist. So lässt sich zeigen, mit welchen Folgen die Algorithmisierung im Begriff ist, Gemeinschaften durch *Netzwerke* abzulösen. Das Beispiel von Bildungseinrichtungen, v. a. Schulen, belegt wie notwendig es ist, das Humane und Soziale gegenüber der Technisierung durch Algorithmen zu verteidigen, nicht nur auf der Bildungsebene.

Die Wegbereiter: Quantifizierung vieler Lebensbereiche und statistische Weltsicht

Mit dem *Hype* um Big Data geht ein neuer Primat von Zahlen und Messbarkeiten sowie eine Verbesserung von Quantifizierungsmethoden einher, im Digital-Diskurs allgemein mit *Datafication* bezeichnet. Sie haben verschiedene Ausprägungen erfahren, wie beim *Quantified Self* rund um Körperdaten oder im *Internet of Things* mit sensorisierten (Haushalts-)Gegenständen. Das Vermessen, Analysieren und Berechnen im Sinne der Big-Data-Analytics soll genaue Vorhersagen vor allem für menschliches, individuelles wie soziales Verhalten garantieren. Dahinter steckt nicht mehr ein kausales Denkmodell, sondern ein Software-basierter Glaube an Korrelationen, der mit seiner Wenn-Dann-Logik eine problematische „gesellschaftliche Determinationsformel“[3] darstellt. Die damit verbundene statistische Sicht auf die Welt beruht auf probabilistischen Berechnungen, für die verschiedene Arten von Algorithmen eine wichtige Rolle spielen. Im Kern geht es um die Frage: Mit welcher Wahrscheinlichkeit lassen sich aus einem großen, algorithmisch angehäuften Datenberg bestimmte Schlüsse für Aspekte menschlichen Verhaltens ziehen? Wie wahrscheinlich ist es beispielsweise, dass ein straffällig gewordener Mensch, dessen juristisches Fehl-Verhalten mit dem Instrumentarium von Big Data in Daten *übersetzt* wurde, in Zukunft in welchem Stadtviertel erneut mit dem Recht in Konflikt gerät? *Predictive Policing* als Instrument zur Prognose und Prävention ist nur eines von mehreren ethisch höchst fragwürdigen Beispielen, die aus einer neu aufgelebten mathematisch-statistischen Weltsicht und dem Big-Data-Hype erwachsen. Die Bezeichnungen „Softwarization of Society“ (David M. Berry, 2014) und vor allem „Algorithmic Turn“ (William Uricchio, 2011) verweisen auf die kulturellen Folgen der Zahlen- und Datenbankgläubigkeit.

Partizipationsparadox und *Black Box*: die Gesellschaft als Zuschauer

In der Radiotheorie über den Rundfunk der 20er-Jahre forderten Bertolt Brecht und später Hans Magnus Enzensberger, das Radio solle in seiner Rolle als Empfänger auch zum Sender werden, um demokratischere Partizipationsmöglichkeiten zu schaffen. Seit dem Web 2.0, als *partizipatives* bzw. *Mitmach-Netz* vielfach gefeiert, weiß man: Jeder kann mühelos zum Sender werden. Seit Big Data weiß man jedoch auch: Die dabei ge-

sendeten Daten werden für bestimmte Zwecke gezielt algorithmisch abgeschöpft, Mitsprache und -gestaltung bleiben marginal. Der Mediensoziologe Jan-Hinrik Schmidt spricht vom „Partizipationsparadox". Mit Blick auf die *Sozialen Netzwerke* stellt er fest: „Die Teilhabe der Nutzerschaft […] steigert letztlich den Wert einer Plattform. Doch echte Selbstbestimmung, also das eigenverantwortliche Gestalten von Strukturen und Regeln, ist bei den großen Social-Media-Plattformen nicht vorgesehen."[4] Dieses Paradox lässt sich für weitere Bereiche, in denen mit Algorithmen operiert wird, folgendermaßen umformulieren: Einerseits versuchen große Datenkonzerne, die Gesellschaft von den Vorzügen der Algorithmen zu überzeugen (kognitive Entlastung, Zusammenfassen und führen von Daten, Koordinieren, passgenaue Nutzung etc.). Andererseits verschleiern sie aber die *Grammatik* ihrer Algorithmen, wodurch sie Einzelne und die Gesellschaft immer mehr zum Be-schauen und Be-staunen degradieren. Der amerikanische Mathematiker Steve Strogatz warnt vor einem „Zuschauer-Sport", wenn selbst die besten Mathematiker nicht mehr begreifen, wie der Computer zu den Rechenergebnissen gelangte, und man nicht anders könne, als sich den Ergebnissen schlicht anzuschließen. Die als Black Box bezeichnete Intransparenz der Algorithmen ist „in vielen Fällen so konzipiert, dass sie sich nicht einmal im Nachhinein nachvollziehen lassen. Sie können nur noch experimentell, aber nicht mehr logisch überprüft werden. Solche Algorithmen sind im Grund Black Boxes, Objekte, die nur über ihr äußeres Verhalten verstanden werden können, deren innere Struktur sich aber der Erkenntnis entzieht."[5] Die in dieser Hinsicht sicherlich treffende Bezeichnung „Black-Box-Gesellschaft" (Frank Pasquale) meint schlicht: Wir wissen nicht, in welchem Umfang bereits Daten von uns erfasst wurden und was mit ihnen passiert.

Algorithmisierung des Sozialen I: Dazugehören

Indem in immer mehr Lebensbereichen (Arbeit, Freizeit, Gesundheit, Haushalt) Daten erhoben und damit immer mehr Weltausschnitte *datafiziert* und algorithmisiert werden, taucht eine Reihe von Fragen auf, die gesellschaftlich hoch relevant sind: Wer ist an der skizzierten subjektiven Auswahl beteiligt, (wie) kann diese demokratisch gestaltet werden, was bedeutet die Zunahme von Algorithmen-Einsatz für den gesellschaftlichen Umgang? Dieter Mersch stellt dazu fest: Unser „Zugang zur Welt, zum Realen, sogar das Denken, Handeln, Entscheiden sowie Kommunikation, Öffentlichkeit oder das Soziale werden in einem hegemonialen Akt […] algorithmisiert."[6] Mit der permanenten Selbstdarstellung, dem ständigen *Posten* und *Teilen* von Bildern, Videos, Zahlen, Werten und Bewertungen (wie *Likes/Dislikes)* in den von Algorithmen durchsetzten Sozialen Netzwerken geht es vielen um Imagepflege und ums Dazugehören. Sozialer Druck bedeutet heute: „Sein ganzes Leben samt allen Fehlern und Missgriffen in öffentlich zugänglichen Verzeichnissen verschlagwortet zu haben, erscheint als das bestmögliche Antidot gegen das Gift des Ausgeschlossenwerdens."[7] Formen der Selbstdarstellung und des sozialen Drucks gab es sicher schon eh und je, die neuen Qualitäten zeigen sich jedoch in dreifacher Hinsicht: im hohen Ausmaß und an der hohen Frequenz an freiwilliger Eigenaktivität, an der Schnelllebigkeit der Kommunikation und an der ständigen Selbstvergewisserung im Sinne von „Ich werde gesehen (beobachtet, bemerkt, erfasst), also bin ich."[8] Dass die Algorithmen in den *Sozialen Medien* mit ihrem Filterblasen-Effekt diese Prozesse aufrecht erhalten, ist in der Forschung bereits hinreichend dargelegt worden. Eine bestätigende Antwort auf einer *Sozialen Plattform,* in einem Forum, menschlich oder von einem Bot erzeugt, oder ein algorithmisch empfohlener Link auf eine thematisch sehr ähnliche Internet-Seite kann für diese Art der Selbstvergewisserung und des Dazugehörens bereits völlig ausreichen.

Algorithmisierung des Sozialen II: Relevanz, *Rankings* und Empfehlungen

Algorithmen arbeiten mit der Erfassung von Nutzerdaten, Identitätszuschreibungen und Ähnlichkeitsermittlungen, dabei gilt das Prinzip der Relevanz, jedoch nicht im Sinne der Frage *Was sollen wir verstehen bzw. wissen?*, sondern zumeist im Sinne einer marktorientierten Klick-Ökonomie. Dass sich Relevanz immer weniger aus gesellschaftlichen Aushandlungsprozessen ergibt, sondern mehr und mehr aus errechneten Nutzer-Interaktionen, Wahrscheinlichkeitsberechnungen und Statistiken, ist Zeichen der neuen Algorithmen- und Statistikgläubigkeit. Der Drang zur Vermessung, oft um Vergleiche anzustellen und um sich im Bezug zu anderen auch grafisch im Blick zu haben, bedeutet auch, dass ständig Wertigkeiten (Relevanzen) gesetzt werden. Indem vorgegeben wird, welche Verhaltensweisen, Eigenschaften und Haltungen einen höheren Wert besitzen und so erstrebenswerter sind als andere, werden gesellschaftliche Anreize gesetzt. Vor allem mithilfe der Sozialen Medien werden die Wichtigkeit von *Rankings* und die Darstellung in *Ratings* permanent kommuniziert, wobei gilt: *Up to date* sein, heißt ganz im Sinne von *Updaten*, den jeweils aktuellen Werten nachzueifern und diesen Prozess, auch mit Misserfolgen, transparent zur Schau zu stellen. Auch hier ein Beispiel: Zunächst zeichnen *Lifelogging*-Geräte wie eine beim Joggen getragene Fitness-Uhr die Daten auf. Die mitgelieferte Software dokumentiert so transparent die Leistung, beispielsweise in Kurven-Diagrammen. Indem die Daten über die Software oder eine Plattform des Uhr-Herstellers online gehen, kommen Algorithmen und der Vergleich mit Gleichgesinnten ins Spiel: Die Leistungsdaten werden automatisiert und vernetzt sowie Empfehlungen, passend zum Leistungsstand, generiert (Routen, Trainingseinheiten, Laufgruppen). Der Algorithmus als Voraussetzung also, sich jederzeit und einfach mit anderen vergleichend in Beziehung zu setzen. Die gesellschaftlich relevanten Fragen hierbei sind, mit welcher Penetranz er in unser Leben eingreift, d. h., warum er in Bereichen auftaucht, in denen wir weder Empfehlungen bekommen noch Rankings sehen wollen.

Netzwerke statt Gemeinschaften, Referenz statt Reflexion

Die beiden Soziologen Zygmunt Bauman und David Lyon legen in ihrem Buch *Daten, Drohnen, Disziplin – Ein Gespräch über flüchtige Überwachung* anschaulich dar, inwieweit die digitalen Techniken, insbesondere die Sozialen Medien „das Gewebe zwischenmenschlicher Beziehungen und Bindungen"[9] grundlegend verändern. Das als das *Soziale* der Plattformen

oder Medien vielfach Angepriesene zeigt sich bei näherem, kritischen Hinsehen als Transformation: Nicht mehr in realen Gemeinschaften, sondern in virtuellen Netzwerken wird agiert und kommuniziert. Auch wenn der englische Trend-Begriff *Community* in eine andere Richtung zu weisen scheint, gilt für die Netzwerk-Logik: Seichtheit statt Tiefe, Oberflächlichkeit statt Profundität, *Coolness* statt Wärme, Flüchtigkeit statt Herzlichkeit, Vergnügen statt Verlässlichkeit.[10] Bauman zitiert den französischen Soziologen Jean-Claude Kaufmann, der 2011 über die Art der Kontakte in Netzwerken schrieb: „Mit einem Klick schaltet man ein, mit einem Klick schaltet man aus. […] Das mit einer Maus ausgestattete Individuum denkt, es hätte seine sozialen Beziehungen auf diese Weise unter Kontrolle."[11] Der Algorithmus mit seiner bestätigenden Funktion bestärkt Nutzerinnen und Nutzer in diesem Gefühl, alles unter Kontrolle zu haben – und motiviert sie möglicherweise, ihre Netzwerk-*Freundschaften* auszubauen. Dieter Mersch, Medienphilosoph, beschreibt die Veränderungen ähnlich und beklagt, dass unsere bisherige Idee des Sozialen „ihren Sinn dadurch einbüßt, dass im Rahmen von Digitalität Fakten und Wissen durch Daten, Reflexion durch Referenz, Praxis durch Operativität, Gerechtigkeit durch Partizipation und Vertrauen durch Zugänglichkeit ersetzt werden."[12] Der massenhafte Einsatz von Algorithmen mit seinem großen Potenzial zur geistig einengenden und verstärkenden Filterblase verhindert kritisches Nachdenken. Eine Diskussion über „Technik als soziale[n] Akteur" (Robert Gugutzer) und eine kritische Reflexion des eigenen Mediengebrauchs finden kaum statt. Das fördert eine Gesellschaft ohne echte Gemeinschaft, in der Individualisierung und Personalisierung zur gesellschaftlichen Norm erhoben worden sind.

Ausblick: Orte der Gemeinschaft und der Reflexion am Beispiel Schulen

Gegen die fortschreitende Algorithmisierung des Sozialen gilt es, Orte der realen Gemeinschaft und der Reflexion aufrechtzuerhalten bzw. neu zu schaffen. Dafür bieten sich die Schulen an, zunächst als Ausblick *ex negativo*. Wenn Schulen zu einem Experimentierfeld für algorithmengestützte Big-Data-Anwendungen werden sollen, wie es etwa Jörg Dräger und Ralph Müller-Eiselt vorschlagen, dann kann der Aufschrei nicht laut genug sein. Beide möchten im Rahmen ihrer geforderten „Bildungsrevolution" das Prinzip von *Industrie 4.0* mittels Algorithmen auf das Soziale des Lehrens und Lernens übertragen („Schule 4.0")[13], was schlicht nicht funktionieren kann und zu einer unsozialen, unkooperativen und unkommunikativen „systematischen De-Humanisierung"[14] von Bildung führen muss. Was für ein Unterricht den beiden selbst ernannten Bildungsexperten von Bertelsmann im Zuge der Digitalisierung und Algorithmisierung vorschwebt, fasst der Medienpädagoge Ralf Lankau zusammen: „Algorithmen bestimmen aufgrund der Leistungsfähigkeit, Geschwindigkeit, Fehlerquote, Frustrationstoleranz und anderer Parameter des Probanden die zu erreichenden Lernziele. Software prüft, ob die angestrebten Kompetenzstufen erreicht werden"[15]. Ähnlich wie die Datenkonzerne mit der passgenauen, nutzerorientierten *Personalisierung* daherkommen, argumentieren Dräger/Müller-Eiselt mit der schülerorientierten „Individualisierung" des Lernens, wobei sie übersehen, dass Algorithmen nicht zur Individualisierung im Sinne von (Persönlichkeits-)Bildung, wohl aber zur technischen Gleichmacherei in der Lage sind, was im Bildungsbereich niemand ernsthaft wollen kann. Zudem führt das so beschriebene Szenario zur Vereinzelung und zurück zum Frontalunterricht: Schüler sitzen allein vor dem Monitor und tippen die algorithmisch berechneten Aufgaben ein. Lehrer scheinen dabei genauso obsolet zu werden wie ästhetische, real-sinnliche Erfahrungen (beispielsweise in der Natur), Spontanes oder Irrationales. Schule als Ort der Gemeinschafts(bildung), des selbstbestimmten Lernens „mit Kopf, Herz und Hand" (Pestalozzi) und der Reflexion – Fehlanzeige!

Nicht nur das Sozialsystem Schule, auch universitäre Einrichtungen sowie Erwachsenenbildung müssten in den Digitalisierungsdebatten deutlich machen: Die Theorie unserer Institutionen, in denen Menschen als lernende Subjekte miteinander interagieren, ist vereinbar mit verschiedenen Modellen der Medienbildung und -kompetenz. Bei diesen Modellen geht es auch um das Lernen mit digitalen Medien. Sie ist nicht vereinbar mit Konzepten („Bildung 4.0"), die auf den Primat der Technik und der Automatisierung von Lernprozessen setzen. Unsere Bildungsorte müssen sowohl das Soziale als auch die Subjektivität von lernenden Gemeinschaften gegen die Algorithmengläubigkeit, gegen ökonomische und technokratische Ansätze verteidigen. Denn es ist sicher, dass das Soziale auch mit modernster digitaler Algorithmen-Technik „nicht einfach wie ein lebloses und bewusstloses Ding vermessen werden kann, da soziale Akteure über Reflexivität verfügen."[16]

Es darf jedoch nicht Aufgabe allein der Schulen sein, ein kritisch-reflexives Denken über Algorithmen und ihren Einsatz als

Markus Reinisch

Markus Reinisch ist Lehrer an einer bayerischen Mittelschule. Er schreibt neben literaturdidaktischen Texten zu aktuellen medien-, gesellschafts- und bildungspolitischen Themen für verschiedene Zeitschriften. *markus.reinisch@gmx.de*

Werkzeuge der Digitalisierung, beispielsweise im Bereich der Suchmaschinen anzubahnen und zu sichern. Hier sind neben der Schul- und Medienpädagogik auch Bildungspolitik, Soziologie und Psychologie gefragt. Überall, wo Lern-Gemeinschaften sich, um beim Suchmaschinen-Beispiel zu bleiben, Zugang zu Informationen verschaffen, ist unter dem Primat der Pädagogik altersgerecht bewusst zu machen: Hier sind Algorithmen am Werk, die gemäß uns unbekannten Kriterien (Black Box) Informationen vorstrukturieren, priorisieren oder auch vorenthalten. Damit haben die Algorithmen entscheidend Anteil an unserem Bildungsprozess und greifen nicht nur in soziale Praktiken, sondern auch in die Subjektwerdung und die Bildung der Persönlichkeit und Identität folgenreich ein. Wenn Meinungsbildung nicht mehr auf einer (ergebnis)offenen Diskussionskultur, sondern bereits in der Schule auf algorithmischen Rechenergebnissen fußt, wenn Prozesse der Informationssuche und Identitätsbildung gezielt beeinflusst werden, dann ist aus bildungstheoretischer und schulpraktischer Sicht Vorsicht geboten. Lehrpläne dürfen nicht zu einem algorithmischen Regelwerk des Silicon Valley verkommen, das vorschreibt, welche errechneten Lernmodule der umfänglich vermessene Schüler zugespielt bekommt. Neben den an gesellschaftlichen Veränderungen ausgerichteten curricularen Inhalten muss genügend Freiraum vorhanden sein für die Vermittlung und Einübung von Werten wie Respekt, Empathie, Miteinander, Fairness etc. Dies gelingt nur in einem sozial-kommunikativen, aushandelndem Umgang miteinander – und nicht durch eine als *Individualisierung* verschleierte Vereinzelung vor den Bildschirmen.

Letztlich werden Algorithmen – trotz aller Fortschritte um *Deep Learning* – auf einer distanzierenden Meta-Ebene niemals über ein Bewusstsein darüber verfügen, dass mit ihrem Einsatz eine enorme gesellschaftliche Verantwortung einhergeht. Gerade die Fähigkeiten, kritisch Distanz zu einem Objekt aufzunehmen sowie daraufhin Entscheidungen zu treffen, wird Menschen vorbehalten bleiben, die auch die Verantwortung dafür übernehmen. Denn es wird immer gelten: „Vom menschlichen Lernen ist das algorithmische Lernen kategorial verschieden."[17]

Anmerkungen

1 *Passig, Kathrin: Warum wurde mir ausgerechnet das empfohlen? In: Süddeutsche Zeitung, online unter: https://www.sueddeutsche.de/digital/zur-kritik-an-algorithmen-warum-wurde-mir-ausgerechnet-das-empfohlen-1.1253390 (Stand: 30.11.18)*
2 *Bächle, Thomas Christian: Digitales Wissen, Daten und Überwachung zur Einführung. Hamburg 2016, S.14*
3 *Simanowski, Roberto: Data Love. Berlin 2016, S. 77*
4 *Schmidt, Jan-Hinrik: Die sozialen Medien und das Partizipationsparadox. In: Voss, K./Hurrelbrink, P. (Hrsg.): Die digitale Öffentlichkeit. Band II, Hamburg 2015, S. 57-63, S. 60*
5 *Stalder, Felix: Kultur der Digitalität. Berlin, 2016, S. 96*
6 *Mersch, Dieter: Digital Criticism. Für eine Kritik ›algorithmischer‹ Vernunft. In: Diaphanes 3/2017 (10.12.2017), online unter: https://www.diaphanes.de/titel/digital-criticism-5312 (Stand: 30.11.18)*
7 *Bauman, Zygmunt/Lyon, David: Daten, Drohnen, Disziplin. Ein Gespräch über flüchtige Überwachung. Berlin 2014, S. 37f.*
8 *Ebd., S. 160*
9 *Ebd., S. 63*
10 *Vgl. ebd., S. 56*
11 *Zit. nach Baumann/Lyon 2014, S. 65*
12 *Mersch (vgl. Fußnote 6)*
13 *Dräger, Jörg/Müller-Eiselt, Ralph: Die digitale Bildungsrevolution. Der radikale Wandel des Lernens und wie wir ihn gestalten können. München 2015*
14 *Lankau, Ralf: Bildung 4.0. Per Algorithmus automatisch klug? Online unter: https://bildung-wissen.eu/fachbeitraege/bildung-4-0-per-algorithmus-automatisch-klug.html (Stand: 30.11.18)*
15 *Ebd.*
16 *Reichert, Ramón: Einführung. In: Ders. (Hg.): Big Data. Analysen zum digitalen Wandel von Wissen, Macht und Ökonomie. Bielefeld 2014, S. 9-34, S. 22*
17 *Bächle (vgl. Fußnote 2), S. 45*

Katharina Nocun und Patrick Breyer

Alternativen zur Gated Community

Gegen die Informationsflut, die soziale Netzwerkanbieter wie Facebook und Co. heute über ihre NutzerInnen speichern und auswerten, sehen viele Geheimdienste blass aus. Doch die umfassende Überwachung der eigenen Mitglieder und ihrer Kontakte in der „Außenwelt" ist nur ein kritischer Aspekt der sogenannten Social Media*. Katharina Nocun und Patrick Breyer skizzieren, mit welchen Mitteln diese Anbieter Gated Communities aufbauen, die im Gegensatz zur vielbeschworenen Offenheit und Pluralität des Netzes stehen und es den einmal gewonnenen KundInnen schwer machen sollen, daraus wieder auszubrechen. Nocun und Breyer stellen Alternativen zu den marktdominierenden Netzwerken vor, die technologisch offene Lösungen verfolgen und damit für eine Demokratisierung der Social Media stehen.*

I Überwachung

Es gibt viele gute Gründe, Facebook & Co. den Rücken zu kehren. Im Dezember 2018 veröffentlichte Gillian Brockell ihr ganz persönliches Trauma. In der Washington Post schreibt sie: „Ich weiß, dass ihr wusstet, das ich schwanger war. Es war meine Schuld. Ich konnte diesen Instagram-Hashtags nicht widerstehen – #30weekspregnant, #babybump. Ich klickte sogar ein oder zweimal auf Umstandsmoden-Werbung, die Facebook mir vorsetzte. Was soll ich sagen, ich bin der ideale ‚interagierende' Nutzer." Gillian Brockell beschreibt in ihrem Beitrag eine Datenspur, die viele werdende Eltern unbewusst anlegen: Poster

der Babyparty werden auf Facebook geteilt, die Wiege wird bei Google recherchiert und Amazon weiß anhand der Bestellungen, ab wann man von der Schwangerschaft wusste.

Personalisierte Werbung ist für viele ein Ärgernis. Für Gillian Brockell war es weit mehr als das. Den IT-Giganten dieser Welt hält sie vor: „Habt ihr mich nicht ‚Übungswehen vs. Frühgeburt' und ‚Baby bewegt sich nicht' googeln sehen? Habt ihr nicht meine drei Tage der Stille in sozialen Netzwerken mitbekommen, die höchst ungewöhnlich für eine Intensivnutzerin wie mich waren? Und dann der Post mit Schlagwörtern wie ‚todunglücklich', ‚Problem' und ‚Fehlgeburt' und die 200 Tränen-Emojis von meinen Freunden? Ist das nichts, dass ihr tracken könntet?" In den Monaten nach ihrer Fehlgeburt wurde Gillian Brockell online von Werbung verfolgt, zu deren Zielgruppe sie nicht mehr gehörte: Still-Kleidung, DVDs mit Ratgebern für den gesunden Babyschlaf und Kinderwagen. In der Parallelwelt der personalisierten Werbung war Gillian Brockell Mutter. In der Realität weinte sie sich in den Schlaf.

Innerhalb kürzester Zeit ging diese Geschichte in den sozialen Netzwerken viral. Das Mitgefühl war ebenso groß wie die Empörung. Natürlich meldete sich bald ein Facebook-Vertreter mit dem Hinweis, Nutzer könnten in ihren Einstellungen einige wenige Werbekategorien (Alkohol, Haustiere, Kinder) gezielt stumm schalten. Das stimmt wohl. Aber reicht das? Gillian Brockell schreibt, ihr fehlte in der schweren Situation einfach die Kraft dazu, sich durch die (für Übersichtlichkeit nicht gerade bekannten) Einstellungen Facebooks zu wühlen. Vielen Nutzern wird es ähnlich ergangen sein. Allein in den USA gibt es jährlich geschätzte 24.000 Fehlgeburten. Es gäbe eine einfache, aber wirkungsvolle Lösung, mit diesem Problem umzugehen. Aber dass Facebook-Nutzer eines Tages aktiv in bestimmte Werbekategorien wie z. B. „Ja, ich will Hochzeitskleider angezeigt bekommen" einwilligen, oder die Plattform ganz auf personalisierte Werbung verzichtet, ist extrem unwahrscheinlich. Informationen über Lebensumbrüche wie „Hochzeit" und „Familiengründung" und die Möglichkeit, dazu passende Werbung schalten zu können, ist für Werbekunden hochattraktiv. Wahrscheinlicher ist, dass der Facebook-Algorithmus eines Tages Fehlgeburten anhand trauriger Posts erkennen und dann bestimmte Werbekategorien von alleine ausblenden wird; oder dass Instagram automatisiert geplatzte Hochzeitsträume wahrnimmt. Doch ob es zur Lösung beitragen würde, die eine Übergriffigkeit durch eine noch größere reparieren zu wollen, ist aus Datenschützer-Sicht mehr als fraglich.

Es wundert kaum, dass immer wieder Nachrichten durchs Netz geistern mit der Frage: „Hört die Facebook-App mich heimlich ab?" Wenn Nutzer erschreckend passende Werbung angezeigt bekommen, und sie selbst überzeugt davon sind, keinerlei Informationen z. B. über den Umstand einer Schwangerschaft oder Urlaubspläne preis gegeben zu haben, dann muss dies noch nicht heißen, dass die App mithört. Diese wiederkehrenden Erlebnisse vieler Nutzer zeichnen vielmehr ein sehr gutes Bild der umfassenden Möglichkeiten von Big-Data-Analysen. Mit Hilfe großer Datensammlungen lassen sich Muster erkennen und Wahrscheinlichkeiten ermitteln. Nutzer brauchen nicht zu verkünden, dass sie bald heiraten. Die Statistik gibt gute Hinweise darauf, wie hoch die Heiratswahrscheinlichkeit im Zusammenhang mit anderen Faktoren wie etwa Geschlecht, Herkunft und Alter sowie dem Verhalten im Freundes- und Familienkreis steht. Was wir bei Facebook vorgesetzt bekommen, hängt nicht nur von unserem Verhalten, sondern auch von dem Verhalten unserer Kontakte sowie statistischen Werten ab. Facebooks Datensammlung kann man sich kaum entziehen. Durch Eingaben Dritter wird selbst ein Facebook-Asket mit hoher Wahrscheinlichkeit längst miterfasst. Hunderte Millionen hochgeladene Adressbücher erlauben sogar Rückschlüsse über Offline-Beziehungen. Facebook trackt außerdem das Verhalten von Nutzern und Nicht-Nutzern außerhalb des Netzwerks per Like-Button. Die Linie zwischen personalisierter Werbung und psychologischem Profiling verschwimmt dabei zunehmend, wenn Werbekategorien wie „Stress" etabliert werden. 2017 berichtete die Zeitung *The Australian* unter Berufung auf interne Dokumente von Facebook, das Unternehmen könne anhand der Datenspur emotional instabile Teenager gezielt aufspüren. Facebook dementierte dies nicht, sondern stellte nur klar, diese Daten würden nicht für Werbezwecke verwendet. Das ist wenig beruhigend.

Es kann durchaus aufschlussreich sein, als Inhaber eines Facebook-Accounts einen Teil seiner Nutzerdaten zum Download anzufordern. Zwar gibt Facebook nur einen winzig kleinen Teil seines Datenschatzes an die Betroffenen heraus. Doch selbst dieser vergleichsweise kleine Datensatz kann sehr aussagekräftig sein. Alle Suchanfragen seit dem ersten Tag der Anmeldung könnten alle Schwärmereien der Teenagerzeit abbilden. Wer bei der Smartphone-App zwischenzeitlich die Standorterfassung aktiviert hatte, kann die Routen von Reisen und Kneipentouren aus längst vergangener Zeit bis auf die Hausnummer genau nachverfolgen. Nicht wenige Nutzer stellen bei derartigen Datenabfragen fest, dass Unternehmen ihre Kundendaten ohne Rechtsgrundlage mit Facebooks „Custom Audience"-Programm abgeglichen haben. Als der österreichische Datenschutz-Aktivist Max Schrems im Jahr 2011 seine Nutzerdaten bei Facebook anforderte, sorgte die 1.222 Seiten umfassende Antwort für einen globalen Skandal. Es stellte sich heraus, dass Facebook sogar nie abgeschickte Nachrichten und gelöschte Mitteilungen gespeichert hatte. Das muss wohl dieser „rechtsfreie Raum Internet" sein, von dem in Innenministerkonferenzen so häufig die Rede ist.

Viele Nutzer haben ihren Beziehungsstatus bei Facebook nicht gesetzt. Trotzdem ist es nicht unwahrscheinlich, dass der Betreiber des Sozialen Netzwerks diesen längst kennt. Eine von Facebook unterstützte Studie befasste sich ausgiebig mit der Frage, ob sich romantische Beziehungen anhand der Datenspur erkennen lassen. In den ersten 100 Tagen, bevor zwei Facebook-Nutzer ihren Beziehungsstatus öffentlich machen, nimmt die Zahl der ausgetauschten Timeline-Posts für gewöhnlich kontinuierlich zu und ebbt nach dem Beziehungs-Coming-Out wieder deutlich ab. Die Profile von Lebensgefährten zeigen im Verlauf der Zeit eine sehr charakteristische Überschneidung von Freundeskreisen. Am Tag der Trennung steigt die Zahl unserer Interaktionen mit dem (Ex-)Partner laut einer Facebook-Studie im Schnitt um 225 Prozent an. Nach der ersten Trennungswoche stabilisiert sich die Anzahl der Nachrichten wieder auf einem niedrigen Niveau. Die größte Sammlung von Verhaltensdaten, die es jemals in der Menschheitsgeschichte gab, ist in privater Hand. Und die Informationen, die daraus über unser Intimleben abgeleitet werden können, sind alles andere als trivial.

Eine Untersuchung von Wissenschaftlern der renommierten Cambridge-Universität kam zu dem Ergebnis, dass eine Ana-

lyse unserer Facebook-Likes vollkommen ausreicht, um daraus intime Informationen über uns ableiten zu können. Allein anhand der Likes konnten die Wissenschaftler in einem Versuch mit 58.466 Freiwilligen erstaunliche Schlüsse ziehen. In 88 Prozent der Fälle konnten die Forscher erfolgreich erraten, ob ein Mann schwul war – und zwar selbst dann, wenn er dies nicht in seinem Profil erwähnte. 85 Prozent der Teilnehmer konnten treffsicher als Republikaner oder Demokrat identifiziert werden. Bei 82 Prozent traf die Prognose zu, ob die Versuchsteilnehmer Christ oder Muslim waren. Selbst Raucher erkannte die Software zu 73 Prozent. Auch Informationen zu Intelligenz, Drogenkonsum oder ob das Profil zu einem Scheidungskind gehört, konnten mit gewisser Wahrscheinlichkeit aus den Likes abgeleitet werden. Forscher der US-Universität Stanford geben an, anhand von 70 Likes sagen zu können, ob jemand eher ein introvertierter oder extrovertierter Typ ist.

Eine Studie der Wissenschaftlerin Wu Youyou von der University of Cambridge und ihrer Kollegen bestätigt, dass es möglich ist, anhand der Facebook-Likes Einblick in die „Big Five" eines Menschen zu bekommen. In der Persönlichkeitspsychologie werden damit die fünf essenziellen Persönlichkeitseigenschaften des Menschen zusammengefasst: Offenheit für neue Erfahrungen, Gewissenhaftigkeit, Geselligkeit, Empathie und Neurotizismus. Wer die „Big Five" eines Menschen kennt, hat als Werber leichtes Spiel, denn unser Kaufverhalten wird nachweislich von den jeweiligen Ausprägungen dieser Charaktereigenschaften beeinflusst. Bereits zehn ausgewertete Likes erlaubten dem Algorithmus, genauere Vorhersagen über unsere Persönlichkeit zu treffen, als es ein Arbeitskollege vermag. Bei 70 Likes übertraf der Algorithmus die Kenntnisse enger Freunde, bei 150 die der Eltern oder Geschwister und bei 300 ausgewerteten Likes sogar die Genauigkeit der Einschätzung des Lebensgefährten.

Diese immense Datensammlung dient vor allem der Maximierung des Unternehmensgewinns. Soziale Netzwerke generieren Werbeeinnahmen durch das knappe Gut Aufmerksamkeit. Die Kunden sind nicht wir Nutzer, sondern andere. Die rote Linie, wie weit wir Unternehmen in unseren innersten Kern lassen, wie weit wir unser Handeln ökonomisch verwertbar machen, hat sich stillschweigend bis in die Mitte von auf Facebook ausgetragenen Beziehungskonflikten verschoben. Der Bilder-Dienst Instagram gehört heute ebenso zu Facebook wie WhatsApp. Der Konzern ist damit endgültig zum ultimativen Datensilo für soziale Interaktionen geworden. Unter den Millionen Nachrichten, die über die zum Konzern gehörenden Dienste täglich ausgetauscht werden, sind die ersten Schritte des Enkelkinds, politische Aufrufe – oder erotische Fotos. Facebook kann anhand seiner Daten mit hoher Treffsicherheit nicht nur die politische Einstellung vorhersagen, sondern auch, wer Wortführer und wer nur Mitläufer ist. Für ein Unternehmen, das seinen Gewinn mit personalisierter Werbung macht, sind solche Informationen Gold wert. Für repressive Regimes sind solche Listen allerdings ebenfalls ein feuchter Traum.

Soziale Netzwerke sind ein zentraler Ort für gesellschaftliche Debatten, sie sind Werkzeug politischer Willensbildung. Es ist wahr, dass auch kleine Initiativen ohne großes Budget von Facebook profitieren. Aber wer viel Geld hat, der kann sich bei Facebook eben auch eine Überholspur kaufen. Im Zwei-Klassen-Netzwerk ist Reichweite, und damit Aufmerksamkeit, käuflich. In Bezug darauf, was „echt" ist und was finanziell gepusht wurde, lässt die Transparenz zu wünschen übrig. Nutzer sehen nicht, wie hoch der Anteil von durch Werbung erzielten „Likes" zu einem Post ist. Ist ein Beitrag wirklich beliebt oder hat jemand einfach nur ein großes Werbebudget darauf geworfen? Derzeit haben Nutzer keine Möglichkeit, dies zu durchblicken. Dabei können solche Informationen sich stark darauf auswirken, wie wir Parteien oder Organisationen sehen. Derzeit ist es möglich, sich mit hinreichender Finanzkraft so zu präsentieren, als wäre eine Initiative in der Bevölkerung extrem populär – selbst wenn dies nicht stimmt. Doch das ist nicht das einzige Problem. Bei sogenannten „Dark Posts" bleibt verborgen, welchen Zielgruppen welche Postings angezeigt werden. Ein Anrecht darauf, das „ganze Bild" einer Kampagne sehen zu können – etwa um zu überprüfen, ob Wahlversprechen an verschiedene Zielgruppen einander widersprechen – gibt es nicht. Transparenz fehlt auch beim Newsfeed-Algorithmus. Nutzer haben keine Möglichkeit, nachzuvollziehen, warum ihnen bestimmte Nachrichten bevorzugt angezeigt werden – und andere dafür gar nicht. Facebook überwindet damit nicht nur die alte Gatekeeper-Funktion des klassischen Journalismus, sondern ersetzt sie durch einen neuen Mechanismus: seine Algorithmen zur Generierung des Newsfeeds. Die Regeln, die sie vorgeben, sind hochproblematisch.

Es ist wichtig zu hinterfragen, ob die Art und Weise, wie Facebook die Dienstleistung „soziales Netzwerk" organisiert, für uns nicht langfristig vor allem Nachteile bringt. Datenschutzdebatten, die einzig um die individuelle Betroffenheit kreisen, verfehlen den Kern des Problems. Das Risikopotential ist größer als die Summe der Einzelschicksale. Es geht auch um kollektive Risiken für die demokratisch verfassten Gesellschaften. Deshalb würden selbst fortschrittliche Datenschutzgesetze, die zu verbindlichen Löschfristen und umfassender Datensparsamkeit führen, eines der zentralen Probleme nicht lösen: die zentralistisch aufgebaute Infrastruktur etablierter sozialer Netzwerke. Sie trägt dazu bei, dass wir uns überhaupt in diese Situation haben manövrieren lassen. Es ist nur folgerichtig, bei der Suche nach Lösungen aus dieser Misere den Staat in die Pflicht zu nehmen.

II Alternative soziale Netzwerke

Das neue Jahr fängt bei vielen mit guten Vorsätzen an. Am 21. Januar 2019 postete der frisch ernannte Bundesbeauftragte für Datenschutz und Informationsfreiheit Ulrich Kelber folgende Nachricht auf Twitter: „Guten Morgen, ich habe mich entschlossen, neben Twitter auch Mastodon zu nutzen, über die Instanz http://bonn.social (Hallo, @Sascha_Foerster). Freue mich auch dort über Gesprächspartner und bin gespannt, ob automatisches Crossposting funktioniert :-)" Den Anstoß für diese Entscheidung könnte ein offener Brief des Bloggers und IT-Sicherheitsexperten Mike Kuketz gegeben haben, in dem es heißt: „Offenen bzw. freien Netzwerken wie Mastodon fehlt es noch immer an Medien, öffentlichen Institutionen und Politikern, die mit gutem Beispiel vorangehen und die Alternativen unterstützen. Sie wären überrascht, wie viele Menschen bereits jetzt schon auf Mastodon aktiv sind, denen das Thema Datenschutz wirklich am Herzen liegt." Für das alternative soziale Netzwerk Mastodon war dieser Neuzugang ein großer Gewinn, erhöhte diese Nachricht doch seine Sichtbarkeit als alternatives soziales Netzwerk. Die Entwickler und Förderer der dezentralen Plattformen können

Verbündete gut gebrauchen, denn sie stehen vor einer schwierigen Aufgabe: Wie tritt man in Konkurrenz zu einem Netzwerk, dass alles daran setzt, Wettbewerb gar nicht erst zuzulassen?

Ulrich Kelber hat seinen Twitter-Account mit Mastodon gekoppelt. Seine Tweets werden automatisch auch von seinem Mastodon-Account verbreitet. Die Möglichkeit derartiger Brücken steigert die Attraktivität der neuen Netzwerke immens. Wie viele Nutzer haben schließlich die Zeit, noch ein zusätzliches Netzwerk zu füttern? Beim Telekommunikationsmarkt ist garantiert, dass stets Interkonnektivität zwischen Telefonnetzen gewährleistet werden muss. Die Gated Community von Facebook zu verlassen, stellt Nutzer hingegen vor ein vergleichbares Problem, als würden sie zu einem Telefonanbieter wechseln, bei dem man Kunden aus anderen Netzen nicht mehr anrufen kann – und leider machen diese 90 Prozent des eigenen Adressbuchs aus. Betreiber alternativer sozialer Netzwerke versuchen zwar beständig, einen automatisierten Austausch zwischen Facebook-Nutzerkonten und ihrem Netzwerk zu ermöglichen. Die Bemühungen scheitern jedoch regelmäßig daran, dass Facebook schlichtweg kein Interesse daran hat, eine solche Kompatibilität zuzulassen. Facebook erlaubt seinen Nutzern bewusst keine gleichberechtigte Kommunikation mit Accounts anderer Netzwerke. Neben anderen Argumenten, die dagegen sprechen, würde eine solche Öffnung nicht zuletzt auch die eigene marktbeherrschende Position gefährden. Denn Kompatibilität verschiebt den Referenzpunkt des Netzwerkeffekts von einem Anbieter zu allen Anbietern der selben Technologie. Derzeit profitieren die *Big Player* vor allem vom Netzwerkeffekt in Kombination mit einer Struktur der *Gated Communities*.

Die unsichtbare Hand des Marktes regelt sicherlich eine Menge – Wettbewerb auf dem Markt für soziale Netzwerke gehört nicht dazu. Netzwerkeffekte und mangelnde Kompatibilität führen zu einer lähmenden „The Winner takes it all"-Struktur. Denn die meisten Menschen entscheiden sich nicht aufgrund von Features oder in den AGB garantierten Nutzerrechten für das „beste" soziale Netzwerk, sondern für das Netzwerk mit den meisten für sie relevanten Kontakten. In vielen Familien ist der WhatsApp-Familienchat längst zentrale Anlaufstelle für Neuigkeiten und Updates zu den Enkelkindern. Auch Content-Anbieter achten in erster Linie auf die Reichweite und damit die für sie relevante Nutzerzahl, jedoch weniger auf andere Aspekte. Als Online-Magazin auf diese Kanäle zu verzichten, bedeutet oftmals, auf einen Großteil der Leser zu verzichten. Sich auszuklinken kann sowohl im beruflichen wie im privaten Kontext für den Einzelnen mit konkreten Nachteilen verbunden sein. Das weiß Facebook genauso gut wie jeder andere große Plattformbetreiber. Von „freier Wahl" zu sprechen, wenn es quasi einen de facto-Standard der Mehrheit gibt, ist eine Farce.

Aktionen wie *#Deletefacebook* werden von der Unternehmensleitung daher vermutlich eher gelassen gesehen. Die Nutzer haben eine extrem schlechte Verhandlungsposition. Die Wechsel- und Ausstiegskosten sind oft immens – materiell und immateriell. Das macht die Nutzer zu Bittstellern. Und das ist ein Problem. Wenn Verbraucher keine echte Wahl haben, werden Verhandlungen auf Augenhöhe unmöglich. Die Ausnutzung einer marktbeherrschenden Position verbinden viele mit höheren Preisen oder schlechterer Qualität. Bei mehrseitigen Plattformmärkten wie sozialen Netzwerken kann sich dies einerseits in höheren Preisen für Werbung und Transaktionsgebühren niederschlagen. Aber auch auf der Marktseite, die nur indirekt monetarisiert wird, kann Marktmacht negative Folgen haben, etwa in Form von Abstrichen beim Datenschutz und Nutzerrechten, einem Übermaß an Werbung sowie mangelhaftem Service (z. B. Fehlen von Beschwerdehotlines).

Dezentrale Alternativen wie Mastodon, Diaspora oder Friendica haben sich vom Konzept des zentralen Anbieters verabschiedet. Die Software zum Betreiben einer „Instanz" des Netzwerks steht unter freier Lizenz. Es ist ausdrücklich vorgesehen, dass die neuen Netzwerke aus möglichst vielen solcher Datenknoten bestehen können. Zudem streben einige Netzwerke Kompatibilität durch geteilte Standards untereinander an. Es geht diesen Projekten explizit nicht darum, ein „europäisches Facebook" als Gegenmodell zu erschaffen, sondern ein Netzwerk neuartiger Prägung, das sich der Eigendynamik personalisierter Werbeformen ausdrücklich entziehen will. Ziel ist ein dezentrales Netzwerk der Netzwerke, welches den Nutzern maximale Freiheit erlauben soll, sich den Server oder das Netzwerk ihrer Wahl selbst zu wählen. Nutzer sollen selbst entscheiden können, wem sie ihre digitale Identität anvertrauen wollen. Im Zweifel können Nutzer auch selbst ihre eigene „Instanz" innerhalb eines Netzwerks betreiben.

Dezentrale soziale Netzwerke bergen natürlich auch neue Herausforderungen für den Datenschutz. Jeder Betreiber einer Instanz kann die Hausregeln selbst bestimmen – das gilt auch für den Datenschutz und die Sicherheitsstandards. Nutzer müssen sich entweder damit abfinden, dass öffentliche Postings oder Profildaten global öffentlich zugänglich sind, oder ihr Verhalten anpassen und deutlich mehr Vorsicht walten lassen, bevor sie einen Kontakt annehmen und ihm damit Zugriff auf ihre Daten gewähren. Die Verteilung von Daten auf dezentrale Netzwerke führt eben auch zu einer Verteilung von Risiken und Verantwortung – im Guten, wie im Schlechten.

Die Herausforderung, vor der man steht, ist gewaltig. Doch strategisch wurde einiges richtig gemacht. Bei lokalen Instanzen von Mastodon zeigt sich bereits, wie lokale Netzwerkeffekte Wachstum anregen. Statt sich wahllos um Nutzer zu bemühen, ist die erfolgreichere Strategie, in der Nische zu wachsen. Nicht anders ist schließlich einst „The Facebook" vorgegangen, das den Zugang zum Netzwerk anfangs auf Studenten bestimmter Universitäten beschränkte. Bei der dem CCC nahestehenden Mastodon-Instanz chaos.social waren im Januar 2019 5.000 zumeist deutschsprachige Nutzer angemeldet. Sie hatte im letzten Jahr zwischenzeitlich keine neuen Nutzer mehr aufgenommen, der Andrang war zu groß. Man strebte lieber ein „gesundes Wachstum" an und wollte dem bestehenden Sozialgefüge Zeit geben, um zusammenzuwachsen. Statt Wildwuchs zu fördern bemühte man sich lieber darum, eine gesunde Debattenkultur zu etablieren, da dies für nachhaltiges Wachstum und den langfristigen Erfolg entscheidend ist. Dies bedeutet auch, dass nicht alle Inhalte hier toleriert werden. In den Hausregeln der Instanz untersagen die Betreiber ausdrücklich rassistische, nationalistische und sexistische Inhalte. Das trägt zu einem konstruktiven Ton bei.

Mastodon und andere dezentrale Netzwerke zeigen, dass die Vision sozialer Netzwerke zumindest in der Nische höchst er-

folgreich sein kann. Mastodon empfängt Twitter-Nutzer mit einer äußerst vertrauten Nutzeroberfläche und Tools, um den Account mit einem Twitter-Konto zu verknüpfen. Während einige wie Ulrich Kelber weiterhin bei Netzwerken wie Twitter aktiv sind und viele Postings „nur" nach Mastodon umleiten, sind andere ganz umgezogen. Wer im Bereich Datenschutz, IT-Security oder Netzpolitik unterwegs ist, kann sich in einigen Instanzen bereits heute recht heimisch fühlen.

III Wie kann man alternativen Netzwerken zum Durchbruch verhelfen?

Die Durchsetzung des Datenschutzrechts gegen die digitalen Quasi-Monopolisten könnte dazu beitragen, dass alternative Netzwerke eine faire Chance bekommen. Denn das oft „Datenkapitalismus" genannte Geschäftsmodell von Facebook, Twitter oder Google beruht auf einer systematischen Missachtung des Rechts auf informationelle Selbstbestimmung. Die Konzerne verschaffen sich Wettbewerbsvorteile durch Rechtsbruch. Wer nicht von den Informationen und Kontakten auf diesen Plattformen abgeschnitten sein will, muss in die Aufzeichnung und Auswertung jeder Eingabe und jedes Klicks einwilligen – und damit quasi in einen permanenten Persönlichkeitstest. Obwohl Whistleblower, Dissidenten, Stalking-Opfer und andere Gruppen auf eine anonyme Nutzung angewiesen sind, verbieten die Konzerne dies und fordern den Klarnamen oder eine Handynummer ihrer Nutzer.

Diese Totaldurchleuchtung im Netz dürfte schon nach dem geltenden Datenschutzrecht unverhältnismäßig und illegal sein. Auch Einwilligungsklauseln sind Allgemeine Geschäftsbedingungen, die von Gerichten darauf überprüft werden können, ob sie die Nutzer unangemessen benachteiligen oder von Grundgedanken gesetzlicher Schutzregelungen abweichen. Schwammige Generalklauseln, träge Aufsichtsbehörden, eingeschränkte Klagerechte und jahrelange Gerichtsverfahren durch alle Instanzen erschweren die Durchsetzung des Datenschutzrechts gegen die globalen Internetkonzerne aber ungemein. Die DSGVO ermöglicht den Behörden zwar, höhere Bußgelder zu verhängen, doch es wird noch dauern, bis sich Verbesserungen in den Nutzungsbestimmungen niederschlagen. Viele Probleme bleiben auch nach dem Inkrafttreten des neuen europäischen Datenschutzrechts bestehen.

Das fortschrittliche deutsche Telemediengesetz, das ein Recht auf Anonymität und das Verbot einer Protokollierung unserer Online-Aktivitäten zum Grundsatz macht, wird seit Inkrafttreten der europäischen Datenschutz-Grundverordnung nicht mehr angewandt. Die geplante europäische Verordnung über den Datenschutz bei der elektronischen Kommunikation (ePrivacy-Verordnung) wird nach intensivem Lobbying der Werbebranche und der Verlage ausgebremst und aufgeweicht. Sie gilt außerdem nur für einen Teil der Tracking-Technologie. Europa braucht deswegen ein Internet-Datenschutzgesetz, das explizit eine anonyme Internetnutzung ermöglicht und uns vor kommerziellem Stalking, nämlich der minutiösen Aufzeichnung unserer Internetnutzung, schützt. Geschäftsmodelle, die auf eine Bespitzelung sämtlicher Nutzer ohne deren freie Einwilligung aufbauen, sind nicht schutzwürdig. Es gibt keine „Nützlichkeiten" und „Vorteile", die einen derartigen Persönlichkeitsstriptease aufwiegen könnten.

Daneben muss Europa den Nutzern kommerzieller sozialer Netzwerke und Messengerdienste ermöglichen, den Anbieter zu wechseln, ohne den Kontakt zu Informationsquellen und Freunden zu verlieren. Ein reines Recht auf „Datenportabilität", wie im Rahmen der DSGVO vorgesehen, reicht dafür nicht aus. Eine Zusammenschaltung der sozialen Netzwerke ähnlich der Mobilfunk-Netze würde es ermöglichen, sich auch nach dem Wechsel zu einem anderen Anbieter weiter mit seinen bisherigen Kontakten auszutauschen. Die Fachwelt nennt dies „Interoperabilitätspflicht". Bisher haben die einflussreichen Konzerne verhindert, dass diese Lösung ernsthaft politisch diskutiert wird, doch mit jedem Datenskandal wird klarer, dass wir neue Lösungen brauchen. Auch wenn es keineswegs trivial ist, sich bei technisch diversen Netzwerken auf einheitliche Standards zu verständigen, sollten zumindest das Ziel gesetzt und die Umsetzungsmöglichkeiten intensiv ausgelotet werden. Maßnahmen, die höchstwahrscheinlich allein dem Ausbremsen von Konkurrenz dienen, müssen hinterfragt werden. Zusätzliche Funktionen über den gemeinsamen Standard hinaus bleiben jedem Anbieter unbenommen.

Wir brauchen kein europäisches Facebook, wenn es am Ende nur die problembehaftete Struktur des derzeitigen Platzhirsches kopiert. Es wäre daher an der Zeit, dass sowohl Deutschland als auch die EU-Kommission stärker in die Förderung von Forschungsprojekten zur Verbesserung dezentraler Alternativen investieren. Ebenso braucht es eine Unterstützung für die Erarbeitung praktikabler gemeinsamer Standards. Die bisherigen Initiativen sind maßgeblich auf das Engagement engagierter Einzelpersonen aus der Freie-Software-Bewegung zurückzuführen. Trotz nicht abreißender Kritik an Facebooks Gebaren im Zuge des Skandals um Cambridge Analytica hält sich der Staat hier bei der konkreten Unterstützung bisher bedeckt. Das muss sich ändern.

Öffentliche Stellen sollten außerdem ihrer Vorbildfunktion besser gerecht werden. Die in der Politik verbreitete Klage über die Dominanz von Facebook, Twitter und Co. steht in auffälligem Gegensatz zu der Anzahl an Präsenzen öffentlicher Stellen und Amtsträger auf eben diesen Plattformen. Internet-Quasimonopolisten mit Exklusivinformationen zu füttern und die Abhängigkeit von ihnen dadurch weiter zu verstärken, sollte ein Ende haben. Es ist ein Leichtes, Informationen zumindest auch über nicht-kommerzielle Netzwerke zu verbreiten – wie es der Bundesdatenschutzbeauftragte neuerdings tut.

Soziale Netzwerke sind Teil unserer politischen Wirklichkeit. Es ist essentiell, dass wir in einer demokratischen Gesellschaft darüber diskutieren, nach welchen Regeln die neue Öffentlichkeit funktionieren soll – und welche Formen der Verwertung und Manipulation wir als gefährlich erachten. Darauf zu hoffen, dass eine Strategie zur Maximierung des Unternehmensgewinns zufällig auch das gesellschaftlich bestmögliche Ergebnis hervorbringt, wäre mehr als naiv. Höchste Zeit, dass sich die Politik hier bewegt.

Referenzen

Brockwell, Gillian (2018): Dear tech companies, I don't want to see pregnancy ads after my child was stillborn, in: Washington Post, 12.12.2018. Unter: https://www.washingtonpost.com/lifestyle/2018/12/12/dear-tech-companies-i-dont-want-see-pregnancy-ads-after-my-child-was-stillborn/?noredirect=on&utm_term=.eac113134e91 (aufgerufen am: 25.01.2019).

Chaos.Social (2019): Rules. Unter: https://chaos.social/about/more (aufgerufen am: 25.01.2019).

Dachwitz, Ingo (2017): Verhaltensbasierte Werbung: Facebook identifiziert emotional verletzliche Jugendliche, in: Netzpolitik.org, 02.05.2017. Unter: https://netzpolitik.org/2017/verhaltensbasierte-werbung-facebook-australien-analysiert-emotionen-und-aengste-von- jugendlichen/ (aufgerufen am: 25.01.2019).

Diuk, Carlos Greg (2014): The Formation of Love, in: Facebook Data Science, 14.02.2014. Unter: https://www.facebook.com/notes/facebook-data-science/the- formation-of-love/10152064609253859/?fref=mentions (aufgerufen am: 25.01.2019).

Friggeri, Adrien (2014): When Love Goes Awry, in: Facebook Data Science, 15.02.2014. Unter: https://www.facebook.com/notes/facebook-data-science/when-love-goes-awry/10152066701893859/?fref=mentions (aufgerufen am: 25.01.2019).

Kelber, Ulrich: Twitter-Nachricht vom 21.01.2019: https://twitter.com/UlrichKelber/status/1087254951351541761 (aufgerufen am: 25.01.2019).

Kosinski, Michal; Stillwell, David; Kohli, Pushmeet; Bachrach, Yoram; Graepel, Thore (2012): Personality and Website Choice, in: Proceedings of ACM Web Science Conference (WebSci '12), ACM New York, 2012.

Kosinski, Michal; Stillwell, David; Graepel, Thore (2013): Private traits and attributes are predictable from digital records of human behavior, in: Proceedings of the National Academy of Sciences of the United States of America, PNAS Band 110/15, S. 5802–8505, 09.04.2013.

Kosinski, Michal; Stillwell, David; Matz, Sandra; Nave, Gideon (2017): Psychological targeting as an effective approach to digital mass persuasion, in: Proceedings of the National Academy of Sciences of the United States of America, PNAS Band 114/48, S. 12714–12719, 28.11.2017.

Kuketz, Mike (2019): Offener Brief an den Bundesdatenschutzbeauftragten, in: kuketz-blog.de, 14.01.2019. Unter: https://www.kuketz-blog.de/offener-brief-an-den-bundesdatenschutzbeauftragten-kelber/ (aufgerufen am: 25.01.2019).

Wu Youyou, Michal Kosinski, and David Stillwell (2015): Computer-based personality judgments are more accurate than those made by humans, in: PNAS January 27, 2015 112 (4) 1036-1040; published ahead of print January 12, 2015 https://doi.org/10.1073/pnas.1418680112 (aufgerufen am: 25.01.2019).

Der Beitrag erschien in **vor***gänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik #225/226 (Band 58, Heft 1/2, 2019). Wir danken herzlich Autorin, Autor und Redaktion herzlich für die Genehmigung zum Nachdruck.*

Patrick Breyer und Katharina Nocun

Dr. **Patrick Breyer**, Jahrgang 1977, ist Jurist, Bürgerrechtler und langjähriges Mitglied der Piratenpartei Deutschland. Er studierte Jura und promovierte 2004 an der Johann Wolfgang Goethe-Universität Frankfurt am Main mit einer Arbeit über „Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland". Nach einer Anstellung als Richter am Amtsgericht Meldorf gehörte er von 2012 bis 2017 dem Landtag in Schleswig-Holstein an, wo er seit April 2016 Vorsitzender der Piratenfraktion war. Im Mai diesen Jahres wurde er für die Piratenpartei ins Europäische Parlament gewählt. Breyer gehört zu den Initiatoren der neuen (digitalen) Datenschutzbewegung in Deutschland und hat zahlreiche Klagen gegen Kommunikations-Überwachungsmaßnahmen geführt bzw. unterstützt, so etwa Verfassungsbeschwerden gegen die Vorratsdatenspeicherung, gegen den Passwortzugriff bei der Bestandsdatenauskunft nach dem TKG, gegen die Surfprotokollierung oder den Informationszugang zu Gerichtsverfahren.

Katharina Nocun ist Bürgerrechtlerin, Publizistin und Ökonomin. Sie leitete bundesweit Kampagnen zum Schutz der Bürgerrechte, u. a. für die Bürgerbewegung Campact e. V., den Verbraucherzentrale Bundesverband und Mehr Demokratie e. V. Edward Snowden bedankte sich persönlich für die von ihr geleitete Kampagne „Asyl für Snowden". Sie klagt derzeit gegen mehrere Überwachungsgesetze vor dem Bundesverfassungsgericht (u. a. die Reform der Bestandsdatenauskunft sowie die Vorratsdatenspeicherung) und ist Mitglied im Beirat des Whistleblower-Netzwerk e. V. 2017 wurde sie von der Humanistischen Union Marburg und der Stadt Marburg für ihr zivilgesellschaftliches Engagement mit dem „Marburger Leuchtfeuer für soziale Bürgerrechte" ausgezeichnet.

Den AutorInnen über alternative Kurznachrichtendienste folgen:
https://chaos.social/@kattascha bzw. *https://pirati.cc/patrickbreyer.*

Michael Ahlmann, Sylvia Johnigk, Hans-Jörg Kreowski und Kai Nothdurft

Cyberpeace und IT-Sicherheit

Editorial zum Schwerpunkt

Seit dem offiziellen Start unserer Cyberpeace-Kampagne sind inzwischen fast fünf Jahre vergangen. Motiviert durch die zunehmenden Gefahren, die sich aus der Nutzung von Computern als D-Waffen in einer zunehmend digitalisierten und vernetzten Welt ergeben, hat das FIfF besorgniserregende Entwicklungen vorausgesehen und aufklärend vor den Risiken eines Cyberkriegs gewarnt. Die Kampagne hatte und hat den ambitionierten Anspruch, diese Entwicklung einzudämmen und aufzuhalten. Auch sollten alternative Nutzungsszenarien insbesondere des Internets vorangetrieben werden. Diese mittelfristigen Ziele konnten nur sehr eingeschränkt verwirklicht werden, wie aktuelle Entwicklungen zeigen. Dss ist jedoch kein Grund zu verzagen oder gar aufzugeben, sondern sollte uns vielmehr als Ansporn dienen, unsere Bemühungen zu verstärken.

D-Waffen werden bereits unter Missachtung des Völkerrechts auch gegen zivile Infrastrukturen eingesetzt. So tauchte im Dezember 2017 mit *Triton* eine Malware auf, die nicht nur das Steuerungssystem von Industrieanlagen sabotiert, wie es bereits seit 2010 mit dem *Stuxnet*-Wurm geschieht, sondern die sogar gezielt deren Safety-Funktion zu sabotieren versuchte.[1] Die Safety-Funktion ist eine Notabschaltung, die bei einer Disfunktion ein geordnetes Herunterfahren der betroffenen Anlage gewährleisten soll. Durch einen Programmierfehler arbeitete die Schadsoftware nicht wie vom Angreifer gewünscht. Stattdessen löste sie genau diesen Shutdown aus. IT-Sicherheitsexperten, die die Malware analysierten, vermuten, dass eigentlich die Deaktivierung dieser Safety-Funktion intendiert war, da diese Funktion gezielt angegriffen wurde.[2] Damit wurde das erste Mal nachweislich eine Malware eingesetzt, die das explizite Ziel hatte, lebensbedrohende Manipulationen in Steuerungsanlagen herbeizuführen. Die Schadfunktion der Malware besitzt dieses Potenzial leider auch weiterhin, denn von dem Schadprogramm geht immer noch Gefahr aus. Gefunden wurde Triton erstmals in der Steuerungsanlage einer Gasraffinerie, wo Triton eine Explosion hätte auslösen können, wenn es wie vorgesehen funktioniert hätte. Die Malware-Funktionen wurden auch noch bei weiteren Angriffen nachgewiesen, und die angegriffene Safety-Funktion kommt noch in vielen anderen Anlagen zum Einsatz. Auch werden Steuerungssysteme, wenn überhaupt, wesentlich seltener und später gepatcht als etwa gängige Server-Betriebssysteme. Daher muss davon ausgegangen werden, dass weiterhin viele Steuerungsanlagen anfällig für Triton-basierte Angriffe sind.

Gerade die von uns durchgeführten Analysen der zu erwartenden Bedrohungen durch Cyberkrieg haben sich leider erneut als realistisch und keineswegs als Schwarzmalerei erwiesen. Umso mehr muss es auch in den nächsten Jahren eine Kernaufgabe des FIfF bleiben, Transparenz zu schaffen. Ebenso wichtig ist es, wahlentscheidend große Personengruppen zu diesem Thema aufzuklären und sich nicht auf die kritische Analyse im akademisch/fachlichen Diskurs zu beschränken. Das Internet gibt uns dazu die Werkzeuge an die Hand. Wer, wenn nicht wir, kann und sollte diese auch nutzen? Das im Rahmen der Kampagne entstandene Video *Cyberpeace statt Cyberwar* mit inzwischen über 14.900 Aufrufen auf YouTube und über 1.100 auf Vimeo war ein wichtiger Schritt in diese Richtung und darf nicht der letzte bleiben.

Unser aktueller Schwerpunkt umfasst verschiedene Themen aus dem Bereich *Informatik und Rüstung*, die vom Drohnenkrieg über autonome Waffen und Rüstungskontrollfragen bis zum Widerspruch zwischen dem IT-Sicherheitsgesetz und der Entwicklung offensiver Cyberwaffen reichen:

- *Ralf Cüppers*, *Siglinde Cüppers* und *Stephan Schlereth* erläutern zunächst die militärisch-strategische Geschichte und Funktion des Drohnen- und Tornado-Luftwaffenstandorts *Jagel* in Schleswig-Holstein und beschreiben anschließend den friedenspolitischen Widerstand dagegen.

- *Henning Lübbecke* stellt die Frage, ob autonome Kampfroboter einen „Silberstreif am Horizont" für kriegsführende Demokratien bedeuten können, da sie die Chance zu bieten scheinen, eigene Verluste zu begrenzen und ethische Regeln zu befolgen. Er zieht für seine Bewertung mehrere aktuelle Abhandlungen zu autonomen Systemen und Roboterethik heran.

Die weiteren Artikel behandeln Cyberpeace-Themen im engeren Sinne:

- *Thomas Reinhold* führt zunächst kurz ein in verschiedene Ansätze von Rüstungskontrolle im allgemeinen in seinem

Beitrag *Rüstungskontrolle für den Cyberspace – Herausforderungen und erste Ansätze. Dann widmet er sich* den spezifischen Anforderungen, vor denen die Rüstungskontrolle bei digitalen Waffen steht. Diese reichen von Kontroversen bei Definitionen, was Gegenstand und Umfang der Kontrolle sein soll, bis zu der Frage, welche Institution für die Kontrollaufgabe legitimiert sei. Er gibt eine Übersicht über verschiedene Ansätze von internationalen Institutionen und nationalen Initiativen und bewertet diese.

- *Ingo Ruhmann* und *Ute Bernhardt* untersuchen in ihrem Beitrag zum IT-Sicherheitsgesetz, inwieweit sich staatliche Institutionen strafbar machen, wenn sie offensiv „Cyber"-Angriffe durchführen und in Konflikt mit dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität Informationstechnischer Systemen geraten.

Anmerkungen

1 *https://www.technologyreview.com/s/613054/cybersecurity-critical-infrastructure-triton-malware/*

2 *https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html*

Ralf Cüppers, Siglinde Cüppers, Stephan Schlereth

Jagels Beitrag zur vernetzten Operationsführung von Bundeswehr und NATO und unser friedenspolitischer Widerstand

In Jagel befindet sich der größte Militärflughafen der NATO in Europa. Unser Artikel beleuchtet den Drohnen- und Tornadostandort der Luftwaffe bei Schleswig und seine militärisch-technische Ausrüstung, die vernetzte Operationsführung von Bundeswehr und NATO und den Anteil Jagels dran. Wir beschreiben die seit Juni 2015 in Jagel monatlich stattfindenden Mahnwachen und weiteren Aktionen, die von der Deutschen Friedensgesellschaft – Vereinigte KriegsdienstgegnerInnen (DFG-VK) – organisiert und mit verschiedenen Organisationen gegen diesen Standort gestaltet werden. Weitere Informationen liefert die Website www.bundeswehrabschaffen.de*, auf der auch weitere Aktionen zu diesem Thema angekündigt werden und dokumentiert sind.*

NATO und Bundeswehr in Jagel

Schon in den Kriegen während des Zerfalls von Jugoslawien von 1991 bis 2001 waren verschiedene Tornado-Varianten – Mehrzweckkampfflugzeuge, die jetzt in Jagel stationiert sind – zur elektronischen Kampfführung und Aufklärung im Einsatz. Sie sind darauf spezialisiert, gegnerische Luftabwehrstellungen zu orten und mit Raketen „auszuschalten" (ECR = Electronic Combat Reconnaissance). Tornados zur abbildenden Aufklärung (Recce = Kurzform von Reconnaissance) aus Jagel flogen hinterher und scannten das Land ein – Brücken, Transformatorstationen oder auch die chinesische Botschaft. HARM-Raketen (Homing Anti Radiation Missile), die von den Tornados transportiert werden, verfügen über eine Fähigkeit, die „fire and forget" genannt wird. Sie suchen selbständig ihr Ziel und zerstören es.

Die Heron-1-Drohnen, die Piloten aus Jagel in Masar-e Sharif in Afghanistan steuern, sind dort seit 2010 im Spionageeinsatz – die gesammelten Daten tragen zum Lagebild der NATO bei. Das Töten übernehmen NATO-Bomber – mal Militärstellungen der Aufständischen, mal Hochzeitsgesellschaften. Aufklärung ist auch hier Beihilfe zum Mord. Krieg beginnt also in Schleswig-Holstein.

Jagels militärische Aufträge

- Erhalt der militärischen Einsatzbereitschaft mit bemannten und unbemannten Flugobjekten (Tornados und Drohnen),
- Durchführung von Aufklärungsaufträgen,
- Beteiligung an militärischen Einsätzen zur Landes- und Bündnisverteidigung, der NATO, und unter dem Mandat der Vereinten Nationen,
- Durchführung von Einsätzen der weiträumigen Signal- und Bilderfassung aus der Luft (SIGINT),
- Bekämpfung von Überwasserzielen mit *Fire and Forget*-Waffen wie GBU, HARM und IRIS T (seit 2009),
- Unterstützung der Elektronischen Kampfführung (EloKa) aus der Luft durch signalerfassende Aufklärung feindlicher Radarstationen und Funkstationen, Ortung und Zerstörung feindlicher Radaranlagen und Funkstationen mit HARM (seit 2013); damit wurde der militärische Auftrag des aufgelösten Jagdbombergeschwaders 32 Lechfeld vom Jagdbombergeschwader 51 Jagel vollständig übernommen,
- Übernahme des Ausbildungszentrums für die abbildende und signalerfassende Aufklärung der Luftwaffe (seit 2016); damit wurde auch dieser militärische Auftrag vom Jagdbombergeschwader 51 Jagel vollständig übernommen; seitdem werden alle Soldaten aller Teilstreitkräfte der Bundeswehr, die mit abbildender oder Signalaufklärung befasst sind, in Jagel ausgebildet,
- Auswertung der Einsatzbilder aus den Aufklärungsflügen direkt am Standort Jagel (seit 2016),
- Ausbildungs- und Übungsflüge aller Drohnenpiloten der Heron I, vor allem am Flugsimulator (seit April 2017),

- nachdem 2018 die Deutsche Luftwaffe die Ausbildung in Holloman in New Mexico (USA) aufgeben hat, werden mittlerweile alle Tornado-Piloten und Waffensystemoffiziere in Jagel ausgebildet,

- Zielaufklärung mit Tornados und Drohnen und Feststellung der eigenen Waffenwirkung –, obwohl Zielvernichtung nicht ausdrücklich erwähnt ist.

Der Tornado ECR

An Stelle der zweiten Bordkanone ist diese Variante des Mehrzweckkampfflugzeugs mit integriertem ELS *(Emitter Locator System)* ausgestattet – einem weltweit einzigartigen Verbund von Sensor und Waffe. Das ELS bestimmt die Position und verschiedene andere Parameter eines gegnerischen Radars und weist sie direkt, also ohne Umweg über einen menschlichen Entscheidungsträger, dem HARM-Suchkopf für die schnelle Bekämpfung zu. Damit der Suchkopf sein Ziel zerschlagen kann, steuert die Rakete selbstständig auf den Ort zu, der ihm vorher in seine Software eingegeben wurde und korrigiert den Kurs nach der vom Ziel abgegebenen Strahlung; das erklärt den Begriff Homing Anti-Radiation Missile.

Seit 2015 sind alle Tornados ECR mit der Software ASSTA 3 ausgestattet (ASSTA: Abkürzung für *Avionic System Software Tornado in Ada* (Ada ist eine NATO-weit eingesetzte Programmiersprache, ähnlich Pascal und Modula2), Avionic ist zusammengesetzt aus Aviatic – von lat. avis = Vogel – und Electronic und bezeichnet die Gesamtheit der elektrischen und elektronischen Geräte an Bord eines Fluggeräts einschließlich der Fluginstrumente). Mit dieser Software kommandiert das Aufklärungssystem den Piloten und erteilt die Anweisung, wohin er fliegen soll, wenn es die Signalwirkung empfängt. Dies ist die Umkehr bisheriger Befehlsstrukturen: Das Aufklärungssystem befiehlt dem Piloten – und nicht umgekehrt. Der Pilot bekommt keine Informationen darüber, was das Aufklärungssystem aufklärt, was es erkennt, denn es schickt seine Erkenntnisse und Ergebnisse an die Auswertungsstation und bekommt von dort neue Aufklärungsaufträge.

Mit der Software kommunizieren das Aufklärungs- und das Waffensystem, ohne dass der Pilot daran beteiligt ist und Einfluss darauf nehmen könnte. Das Aufklärungssystem teilt dem Waffensystem mit, wann die günstigste Position erreicht ist, um das Waffensystem auszulösen. Dieses kommuniziert über die Software mit dem Computer der Bodenstation, ob es losfliegen soll, nicht mit dem Piloten. Dadurch ist der Pilot nur noch derjenige, der dafür sorgt, das Aufklärungs- und Waffensystem sicher durch die Luft in die Nähe der militärischen Ziele zu transportieren.

Militärdrohnen

Wesentliche Aufgabe einer Militärdrohne ist zunächst das Ausspähen eines Kriegseinsatzgebiets. Diese Informationen gibt sie an ihre Bodenstation weiter, die in sicherer Entfernung vom Einsatzgebiet der Drohne sein kann. Hier kommunizieren der Drohnenpilot und der Waffensystemoffizier in sicherer Entfernung vom Einsatzgebiet der Drohne mit ihr. Der Drohnenpilot erteilt den Marschbefehl und teilt der Drohne mit, wohin sie fliegen und welche Ziele sie beobachten soll. Der Waffensystemoffizier erteilt den Schießbefehl, wenn eine Kampfdrohne das Ziel auch vernichten soll.

Eine Militärdrohne kämpft nie allein. Sie hat die Funktion, aus ihrer großen Höhe ein gesamtes Kriegeseinsatzgebiet zu überblicken. Dafür kann sie der Besatzung einer Fregatte, eines Kampfhubschraubers, Panzers sowie den Bodentruppen Informationen liefern, die diese aus ihrem Blickwinkel nicht erfassen können. Die Drohne ist also eine Netzwerkerin, die Bilder und Informationen über das aktuelle, aber auch über das künftige Kriegsgeschehen allen daran Beteiligten zur Verfügung stellt. Sie ersetzt kein anderes Kriegsmittel, sondern ergänzt und unterstützt sie.

Abbildung 1: Die Heron 1, aufgenommen in Jagel
Foto: Stephan Schlereth, CC BY-SA 3.0

Die Heron 1 hat eine Nutzlast von nur 250 kg. Damit werden das *Synthetic Aperture Radar* (SAR) und das *Multi-Mission Optronic Stabilized Payload* (MOSP), das 28 bis 32 kg wiegt, transportiert. Die Kampfdrohne kann nach Bedarf auch eigene Raketen oder Bomben abwerfen und Ziele vernichten.

Vernetzte Operationsführung

Bei der Bundeswehr heißt der Informationsaustausch im Netzwerk „Vernetzte Operationsführung". Um die Informationen und Bilder der Drohne an die Bodenstation zu senden und auch an andere weiter zu geben, werden Satelliten benötigt. Zur Aufrüstung der Bundeswehr mit Drohnen gehört daher parallel auch immer die Aufrüstung der Satelliten. *Vernetzte Operationsführung und die Bewaffnung der Bundeswehr mit Drohnen gehören zusammen* (siehe Abbildung 2).

In Schleswig-Holstein befinden sich wichtige Einrichtungen für EloKa, wie die Bundeswehr die Elektronische Kampfführung nennt. In Flensburg ist die zentrale Ausbildungsstätte – die Schule für Strategische Aufklärung der Bundeswehr –, in Bramstedtlund in Nordfriesland die leistungsfähigste Wullenwever-Antennenanlage Deutschlands und in einer verbunkerten Anlage ein Auswertungszentrum für die damit gewonnenen Aufklärungsdaten. In Stadum (ebenfalls Nordfriesland) sind die

Luftbildauswertung

Luftbilder aus Mali, die von Heron-1 Drohnen erzeugt werden, gelangen über Satellit nach Gelsdorf und mit Datenleitung nach Jagel, die Lagebilder und die Zielkoordinaten, die von den LuftbildauswerterInnen erstellt werden, gehen auf demselben Weg zurück. Die Satellitenbilder der SAR-LUPE (Gelsdorf) werden ab 2019 auch in Jagel ausgewertet

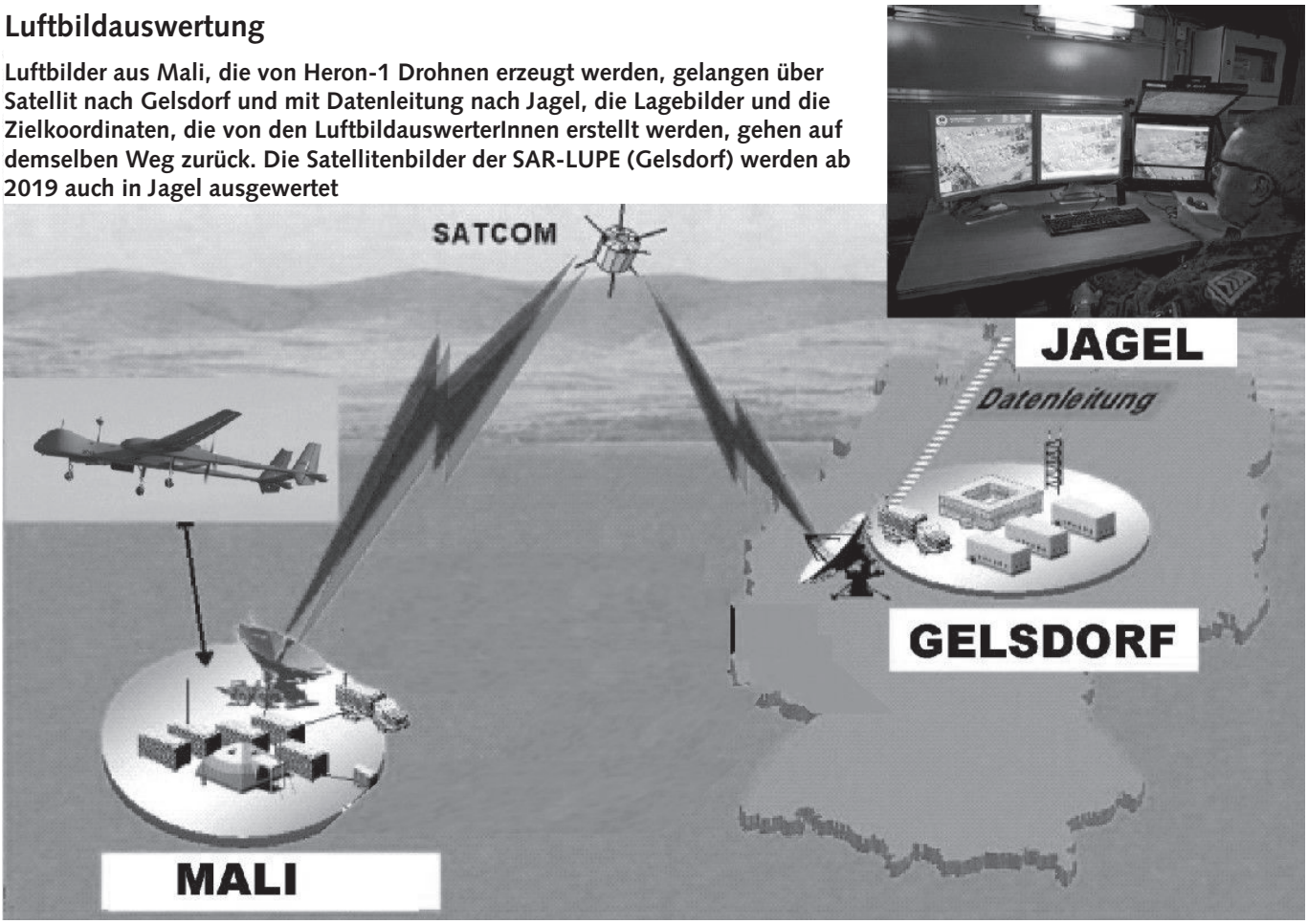


Abbildung 2: Schema der Luftbildauswertung – Bild: Ralf Cüppers, CC BY-SA 3.0

Kaserne und die Büros für die EloKa-Einheit jüngst ausgebaut und modernisiert worden.

Die deutsche Bevölkerung ist empfindlich, wenn es um tote deutsche Soldaten geht – normalerweise interessiert sich kaum jemand für die Bundeswehr-Einsätze in Afghanistan oder in Mali. Gibt es aber eigene Opfer, werden Rufe laut, die Soldaten abzuziehen. Um das Leben der eigenen Soldaten zu schonen, fordern unsere Politiker und Militärs daher den Einsatz von bewaffneten Drohnen. Darin steckt aber auch das Problem: Durch Automatisierung der Kriegsführung mittels Kampfdrohnen und Robotern Kriege wieder führbar und gewinnbar zu machen, ist erklärtes Ziel von Politik und Militär. In den Vorstellungen der Militärs können durch Kampfdrohnen und andere Roboter Gegner getötet werden, ohne eigene Verluste an Menschenleben in Kauf zu nehmen. Wenn die Politik glaubt, das Risiko eigener Opfer sei gering, scheint man eher bereit, die Bundeswehr in aggressive Auslandseinsätze zu schicken. Hinzu kommt, dass Kampfdrohnen leichter zu verlegen und einzusetzen sind als die sonst verwendeten bemannten Kampfflugzeuge.

Weitere Planung

Der Tornado ist ein Auslaufmodell. Im Jahr 2022 soll der letzte Tornado die Bundeswehr verlassen – denn wenn der Pilot eines Tornados nur noch die Funktion eines Chauffeurs hat, ist er verzichtbar. Die Drohne Heron I übernimmt schon jetzt ohne Piloten die Arbeit der Tornados Recce und ECR in nur einem Luftfahrzeug.

Hier kommt die EloKa der Bundeswehr ins Spiel, die seit 2013 eine immer größere Rolle spielt. Für deren Auswertungs-, Störungs- und Zerstörungsarbeit ist es *effizienter*, wenn sie gleichzeitig von den Standorten der Radar- und Funkanlagen Bilder bekommt, um die Umgebung der Standorte zu erkennen – vor allem aber, um zu erfahren, wann sich ein Fahrzeug oder Mensch mit einem Funkgerät oder einem Radar entfernt und wohin es oder er sich bewegt, um darüber Informationen für die strategische Langzeitaufklärung zu erhalten. Für die effektive Auswertung werden Aufklärungsergebnisse in Echtzeit benötigt. So gesehen ist es nachvollziehbar, wenn der Standort für Drohnen Jagel ist, denn mit dem Tornado ECR gibt es hier schon Erfahrungen im Umgang mit teilautomatisierten Aufklärungssystemen – und das Personal dafür.

Die Drohne Heron I ist ein System der EloKa der Bundeswehr. Die Kommunikation erfolgt über die Software direkt zur Auswertungsstation, und sie bekommt auch ihre weiteren Anweisungen von dort. Sie kann als Aufklärungsdrohne in Echtzeit Signale wie der ECR erkennen, kann diese stören und den Absender täuschen. Gleichzeitig kann sie in Echtzeit die Bilder von Fahrzeugen oder Bunkern bereitstellen, in denen sich Radar- oder Funkstationen befinden. Sie hat eine lange Verweildauer im Einsatzgebiet und muss nicht wie der Tornado ständig betankt werden.

Auch der Einsatz der Kampfdrohne Heron-TP, die in Israel seit 2010 eingesetzt wird, soll ab dem Frühjahr 2020 von Jagel aus organisiert werden. Die Ausbildung der Drohnenpiloten und

Waffensystemoffiziere für diese Drohne begann im Februar 2019. Die deutsche Variante G-Heron-TP kann aus einer Höhe von bis zu 9.150 Meter ein militärisches Einsatzgebiet mit optischer Sensorik rund um die Uhr wetterunabhängig beobachten und Fotos und Videofilme von den Akteuren im Einsatzgebiet liefern. Diese aus der Heron 1 weiterentwickelte Drohne wird als bewaffnete Drohne für die Bundeswehr angeschafft. Mit ihrem Turboprop-Triebwerk mit 1200 PS kann sie Nutzlasten von 1800 Kilogramm transportieren, die Abflugmasse beträgt bis zu 4650 Kilogramm. Mit 13 Metern Länge und 26 Metern Spannweite ist sie deutlich größer als das Vorgängermodell Heron 1 (etwa 6 x 12 Meter). Die Einsatzdauer beträgt bis zu 26 Stunden.

Noch strittig ist die Anschaffung der Munition für diese Drohne: ob, und wenn ja, welche. Frau von der Leyen wollte Munition, die sowohl für Flächenbombardierungen tauglich ist als auch für gezieltes Töten. Die G-Heron-TP kann vielseitig bewaffnet werden, wie der Jagdbomber Tornado IDS. Sie vereinigt alle Möglichkeiten des Tornado IDS in einem unbemannten Flugobjekt.

Unser friedenspolitischer Widerstand

Die Forderung „Keine Kampfdrohnen für die Bundeswehr" ist unzureichend, denn die Drohne ist nur ein Bestandteil der *Vernetzten Operationsführung* der Bundeswehr. Auch ohne Kampfdrohnen kann die Bundeswehr Kriege führen. Wenn wir keine Kriege und keine Rüstung mehr wollen, dann müssen wir das Militär abschaffen. Wir können nur bei uns anfangen und nicht darauf warten, dass andere damit beginnen ihr Militär abzuschaffen.

Der DFG-VK Landesverband Hamburg-Schleswig-Holstein hatte schon in den 80er Jahren bei den Friedensfahrradtouren *Kampf dem Atomtod – Verweigert Alle Kriegsdienste* gegen den Tornado-Standort in Jagel demonstriert. Es gab dorthin einen Ostermarsch, bevor die Tornados aus Jagel gegen Jugoslawien eingesetzt wurden. Seit Sommer 2015 haben in Jagel nunmehr insgesamt 41 Mahnwachen stattgefunden.

Aktionsbeispiele der vergangenen vier Jahren in Jagel

- Vorträge: beispielsweise zu Cyberpeace und Cyberwar, zur Umweltschädigung durch Kerosinverbrennung oder Fluglärm oder zur Tätertraumatisierung; diese Vorträge sind sowohl Schulungen der regelmäßigen MahnwachenteilnehmerInnen als auch der Öffentlichkeit, denn sie werden auch in verschiedenen Medien abgedruckt.

- Begegnungen untereinander mit Beiträgen zum Standort von AntimilitaristInnen, PazifistInnen, KirchenvertreterInnen, DKP, Linkspartei, GewerkschafterInnen und AnarchistInnen; Sie bilden ein friedliches Netzwerk,

- Friedensfahrradtouren *Jagel Rund*, bei denen wir den Standort Jagel außen mit Fahrrädern umrunden; die Strecke beträgt über 20 km; dabei können einzelne Objekte auf dem Standort betrachtet werden.

- Teilnahme am *Lauf zwischen den Meeren* über den Standort mit einer Laufstaffel, die dafür trainiert und mit der Trikotwerbung *Frieden schaffen ohne Waffen* im besten Drittel mitläuft – vor der Bundeswehrmannschaft; dazu kommen Infostände vor der Hauptzufahrt in Jagel und beim Zieleinlauf in Damp an der Ostsee.

- Ostermärsche vom Bahnhof Schleswig nach Jagel,

- Konzerte der *Lebenslaute* und des *Intercultural Music Project*, in dem Flüchtlinge aus den Ländern Musik machen, gegen die von Jagel aus Krieg geführt wird,

- Tanzen: Unter dem Motto *Wir tanzen dem Militär vor/auf der Nase herum* wurde unter Anleitung einer Volkstanz-Lehrerin getanzt. Das hat sich bei den kalten Wintermahnwachen bewährt, aber auch in diesem August soll wieder getanzt und musiziert werden.

- *Offenes Kriegsatelier* mit KünstlerInnen und kreativen Menschen vor mehreren Toren des Standorts; die Künstler Knut Andresen und Tomislav Laux brachten dazu eigene Bilder

Ralf Cüppers, Siglinde Cüppers und Stephan Schlereth

Dr. **Ralf Cüppers**, Arzt für Psychotherapeutische Medizin und **Siglinde Cüppers**, Gesundheitspädagogin, arbeiten in einer Psychotherapiepraxis in Flensburg. Beide sind aktiv im DFG-VK Landesverband Hamburg-Schleswig-Holstein. Sie engagieren sich seit vielen Jahren friedenspolitisch und organisieren die Mahnwachen in Jagel.

Stephan Schlereth ist Informatikkaufmann und arbeitet als Projektsachbearbeiter in Flensburg. Er ist seit 2012 Mitglied im FIfF und engagiert sich für friedenspolitische Themen rund um Cyberkrieg bzw. Cyberpeace.

mit. Beim zweiten *Kriegsatelier* gegen den Tag der Bundeswehr am 15. Juni 2019 machten vier Frauen eine szenische Lesung aus George Brants *Am Boden*, das den Arbeitsalltag einer Drohnenpilotin beschreibt; die Lesung wurde als Video aufgezeichnet. Zwei Aktivisten hatten einen Kriegs–Schau–Platz gestaltet, in den das Ausstellungsobjekt der Bundeswehr integriert wurde.

- Meditation: Unter Anleitung einer Yoga-Lehrerin wurde vor einem Tor als *Tor der Stille* meditiert, und damit dieses Tor aus Protest gegen den Fluglärm blockiert. Während dieser Meditation wurde tatsächlich nicht geflogen.

- Blockadeaktionen: Einige Mahnwachen werden als solche angemeldet, bei anderen Mahnwachen blockiert die Bundeswehr sich selbst, indem sie zuvor die Tore schließt.

Was haben wir erreicht?

Zu den Mahnwachen in Jagel gibt es auf der Seite www.jagel.bundeswehrabschaffen.de und in den Sozialen Medien viele Zugriffe, großes Interesse und positive Rückmeldungen. In der regionalen Monatszeitschrift *Gegenwind* wurden und werden alle Mahnwachen angekündigt und Artikel auf der Basis der gehaltenen Vorträge veröffentlicht. Einige Beiträge erschienen in Printmedien wie *Zivilcourage*, *Unsere Zeit*, *Junge Welt*, aber auch in *bürgerlichen* Lokalzeitungen; Beiträge werden in Online-Zeitungen und Blogs kopiert und veröffentlicht.

Der Drohnen- und Tornadostandort Jagel kann seine Untaten nicht mehr im Verborgenen ausüben. Unsere Mahnwachen seien „fester Bestandteil“ des Standortes, war in der bürgerlichen Presse zu lesen. Auch wenn der *shz-Verlag* unsere Presseerklärungen in der Regel nicht veröffentlicht, können wir feststellen, dass die dort angesprochenen Themen danach in eigenen Beiträgen der RedakteurInnen auftauchen.

Es gibt einen festen Stamm von Teilnehmenden, die bei fast allen Mahnwachen dabei sind, wenn es ihre Zeit erlaubt. Dann gibt es Aktive, die gezielt zu Mahnwachen kommen, wenn es ihr Thema ist: Jede Mahnwache hat ein neues und besonderes Thema, damit bleibt es auch für die regelmäßig Teilnehmenden vielfältig und bunt. Da das Thema Jagel mit der Aufrüstung der Bundeswehr mit Cyberkrieg, Drohnen und Elektronische Kampfführung eng verbunden ist, sind auch InformatikerInnen vom FIfF regelmäßig dabei.

Weitere Planungen

Die monatlichen Mahnwachen vor dem Drohnen- und Tornadostandort Jagel werden fortgesetzt. Anfang 2020, eventuell am 2. Februar, soll die G-Heron-TP bereitgestellt werden und sie ist dem Fliegerhorst Jagel zugeordnet. Wir werden die Entwicklung der Bereitstellung und auch die Munitionsbeschaffung für die Bewaffnung beobachten und zu allen Mahnwachen den aktuellen Stand mitteilen – als Mobilisierung für den Tag, an dem die G-Heron-TP nach Jagel kommt.

Henning Lübbecke

Kampfroboter – Der „Silberstreif am Horizont“ für die Beteiligungen demokratischer Staaten an Kriegen?

Unbemannte Systeme scheinen aus Sicht der Militärs die perfekte Lösung für die Kriegsführung demokratischer Staaten zu sein. Mit der Autonomisierung der Systeme stellt sich die Frage nach der Verantwortung für ihre Taten. Können Roboter ethisch handeln und für ihre Handlungen zur Verantwortung gezogen werden? Der folgende Beitrag spürt einer Antwort auf diese Frage nach.

Der *Silberstreif*

Unbemannte Systeme scheinen aus Sicht vieler VerteidigungspolitikerInnen und deren UnterstützerInnen in Wissenschaft, Verwaltung und Industrie die perfekte Lösung für die Kriegsführung demokratischer Staaten zu sein. Eine High-Tech-Transformation, die sie unbesiegbar macht. Autonome Roboter mit künstlicher Intelligenz und Lernfähigkeiten agieren präziser, schneller und verarbeiten mehr Daten, als jede Soldatin, jeder Soldat dies könnte.

Der erste Golfkrieg, mit massivem Einsatz ferngesteuerter Waffen, hat diesen Traum von der unbesiegbaren High-Tech-Armee scheinbar bestätigt. Die Kriege in Afghanistan und Iran haben bereits sein Scheitern gezeigt. Der Einsatz von Kampfrobotern in asymmetrischen Konflikten führt häufig zu Guerilla-Taktiken und terroristischen Anschlägen auf der Gegenseite. Die Aufstandsbekämpfung in den Städten kostet mehr Menschenleben, insbesondere von (US-)SoldatInnen, als der traditionelle Landkrieg. Die Drohneneinsätze in der Grenzregion von Afghanistan und Pakistan sind ein Beispiel dafür, dass zivile Verluste und Kollateralschäden nur bedingt zurückgehen (11).

Man geht davon aus, dass schon die reine Existenz von Kampfrobotern die Hemmschwelle für ein militärisches Engagement in Demokratien senkt (11, 14). Dabei sind zwei Trends zu beobachten. Der erste ist die vielschichtigere und wirksamere Bewaffnung der Kampfroboter selbst und die zunehmende Bewaffnung der Armeen demokratischer Staaten mit Kampfrobotern. Beides führt zu einem neuen Wettrüsten (11, 14). Der zweite Trend ist die Autonomisierung. Aus ferngesteuerten Systemen werden zunehmend autonome Systeme (11).

Ebenso besteht die Gefahr eines High-Tech-Krieges zwischen zwei Nationen, der dann zu einem Weltraumkrieg eskalieren kann, um dort die eigenen Satelliten zu schützen (14).

Kampfroboter versus SoldatInnen

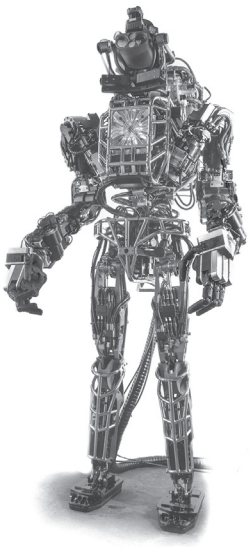
Ein Roboter ist eine konstruierte Maschine, die *wahrnimmt*, *denkt* und *handelt* (8). Autonomie von Robotern ist die Fähigkeit, in einer realen Welt ohne externe Steuerung zu arbeiten (8).

Kampfroboter werden zu Land, Luft und See eingesetzt. Sie können Minen räumen, Verletzte bergen, Verstecke überprüfen und Ziele attackieren. Dabei können sie ihre eigenen Kampfentscheidungen fällen, obwohl heutzutage noch ein Mensch als EntscheiderIn eingebunden ist (8, 11, 12).

Roboter, Drohnen, Minendetektoren und ähnliches wurden im letzten Jahrzehnt auf dem Schlachtfeld eingesetzt, um die Zahl der getöteten SoldatInnen zu verringern, taktische und operationale Überlegenheit zu erreichen und den emotionalen und traumatischen Stress der SoldatInnen zu reduzieren (10, 11, 12, 14).

Kampfroboter sind in der Regel deutlich billiger als ihre bemannten Alternativen. So kostet eine Drohne erheblich weniger als ein Kampfflugzeug und die Ausbildung einer bzw. eines FlugzeugpilotIn ist erheblich teurer als die einer bzw. eines DrohnenPilotIn (11, 14).

Einige ExpertInnen halten Kampfroboter für besser geeignet als Menschen, Normen und Rechte im Krieg einzuhalten (12, 14). Sie gehen davon aus, dass Kampfroboter zukünftig Ziele besser erkennen können als Menschen und deshalb besser zwischen feindlichen SoldatInnen und feindlichen Einrichtungen auf der einen Seite und Zivilisten und zivilen Einrichtungen auf der anderen Seite unterscheiden können. Roboter haben keine psychischen Probleme und vorgefertigten Meinungen. Sie können mehr und schneller Informationen aus unterschiedlichen Quellen verarbeiten als Menschen (14). Roboter sind nicht von emotionalem und/oder traumatischem Stress während der Kampfhandlungen betroffen (10). Sie kennen keine Emotionen wie Ärger, Hass, Feigheit oder Schwäche (8). Deshalb wird unterstellt, dass Kampfroboter in Kampfsituationen zuverlässiger reagieren (12) und weniger stressbedingte Fehlentscheidungen treffen als Menschen (8, 12).



Aus dem Jahr 2013: Prototyp von Boston Dynamics „Atlas". Er soll für das US-Verteidigungsministerium Fahrzeuge steuern und in gefährlichen Umgebungen arbeiten.

Autonome Roboter und ihre Konsequenzen

Die zunehmende Autonomisierung und Bewaffnung der Kampfroboter führt dazu, dass der Mensch im Entscheidungsprozess zu langsam erscheint. Aus dem *Man in the loop* wird der *Man on the loop* und letztendlich der *Man out of the loop*. Trifft bei einem ferngesteuerten Kampfroboter noch der Mensch die Entscheidung zu töten oder zu zerstören, so wird diese Entscheidung beim autonomen Kampfroboter vom Roboter getroffen. Dies führte zu einer Reihe ethischer und rechtlicher Fragen hinsichtlich Differenzierung, Verhältnismäßigkeit und Verantwortung (11).

Verantwortung

Eine fundamentale Bedingung für das Kämpfen eines *gerechten Kriegs* ist, dass eine individuelle Person für den Tod von Zivilisten verantwortlich gemacht werden kann (10).

Boden-Kontrollstation für Drohnen-Einsätze
Foto: Gerald Nino, CBP, U.S. Dept. of Homeland Security

SoldatInnen sind nicht für Kriege verantwortlich, aber für ihre Handlungen. Das bedeutet, dass sie den Einsatz von Gewalt sorgfältig abwägen müssen und dieser verhältnismäßig sein muss (12, 14).

Leider zeigen Untersuchungen, dass dies nicht immer der Fall ist (12). In der Hitze des Gefechts können Angst, Wut und Rachegefühle zu unethischem Verhalten von SoldatInnen führen (10). Andererseits gibt es die Vermutung, dass die allermeisten SoldatInnen das Töten vermeiden und nur allgemein in die Richtung, statt gezielt auf ihre Feinde zu schießen (12).

Kampfroboter hingegen haben keine Emotionen in dieser Form und auch keine Bedenken dieser Art (12).

Mit der Nutzung von Kampfrobotern stellt sich die Frage nach der Verantwortung für ihre Taten. Wer kann für ein Kriegsverbrechen verantwortlich gemacht werden, das von einem Roboter begangen wurde? Eine Operateurin, ein Operator kann nur verantwortlich gemacht werden, wenn sie oder er die Kontrolle und Steuerung über den Roboter und dessen Verhalten hatte. Also nur für Entscheidungen, die die Operateurin oder der Operateur auch selbst getroffen hat. Wurde eine Operateurin bzw. ein Operateur gezwungen, eine Aktion durchzuführen

oder hatte sie oder er keine Eingriffsmöglichkeiten, können sie oder er nicht dafür verantwortlich gemacht werden (8, 10). ProgrammiererInnen können für ein nicht vorhersagbares Verhalten von Robotern nicht verantwortlich gemacht werden (8, 14). Für die Übernahme der Verantwortung kämen neben den OperateurInnen und den ProgrammiererInnen auch noch die HerstellerInnen des Roboters, das Waffenkontrollteam, die EinkäuferInnen, die Einsatzkommandeurin bzw. der Einsatzkommandeur oder die Präsidentin bzw. der Präsident als Oberbefehlshaberin oder Oberbefehlshaber in Frage (8). All dies erscheint unangemessen bei autonom agierenden Kampfrobotern (14).

Kampfroboter stellen daher eine Herausforderung für das internationale Recht dar, da sie die Grundannahme in Frage stellen, wonach ein Mensch die Entscheidung, zu töten, trifft (12).

Mit zunehmender Autonomie von Robotern erscheint es den ProtagonistInnen sinnvoll, die Verantwortung auf die Roboter zu übertragen (8). Aus diesem Grund gibt es Bestrebungen, Robotern ethisches Verhalten beizubringen.

Ethik von Robotern – Roboterethik

Es wird erwartet, dass das moralische Urteilsvermögen von Robotern sich ähnlich rasant entwickelt wie ihre kognitiven Fähigkeiten, Wahrnehmungsfähigkeiten und motorischen Fähigkeiten (13). Die fortschreitenden Fähigkeiten von Robotern, selbständig Entscheidungen zu treffen, erfordern Mechanismen die das korrekte Verhalten garantieren (13). Dabei geht es nicht ausschließlich um die korrekte Ausführung einer Handlung, sondern auch um deren Rechtmäßigkeit und ihre ethische Zulässigkeit.

Damit Roboter menschliche Werte und Normen in ihren Entscheidungsprozessen berücksichtigen, müssen diese Werte und Normen zunächst hinterlegt und entsprechende Programme geschrieben werden.

Die Grundlage der meisten Ansätze der Roboterethik kommt aus der Science-Fiction-Literatur. Sie entspringt *Isaac Asimovs* Roman *Runaround* (3). Ihm sind die folgenden drei Robotergesetze entnommen, die zur Grundlage der Roboterethik wurden:

1. Ein Roboter darf kein menschliches Wesen (wissentlich) verletzen oder durch Untätigkeit (wissentlich) zulassen, dass einem menschlichen Wesen Schaden zugefügt wird.

2. Ein Roboter muss den ihm von einem Menschen gegebenen Befehlen gehorchen – es sei denn, ein solcher Befehl würde mit Regel eins kollidieren.

3. Ein Roboter muss seine Existenz beschützen, solange dieser Schutz nicht mit Regel eins oder zwei kollidiert (3, 13, 16).

Damit der Roboter die Asimovschen Robotergesetze einhalten kann, muss er wissen, wie die ihm gestellte Aufgabe gelöst werden kann, physisch in der Lage sein, die Aufgabe zu lösen, die Aufgabe zum richtigen Zeitpunkt lösen können, zur Aufgabenlösung im Rahmen seiner Rolle verpflichtet sein und prüfen können, ob die Ausführung und das Ergebnis gegen Normen, Regeln und Gesetze verstoßen (5).

Die Gefahrlosigkeit von Robotern ist notwendig, aber nicht ausreichend. Smarte Roboter sollten mehr als nur gefahrlos sein, sie sollten explizit ethisch sein – fähig ihre Aktion zu wählen und zu rechtfertigen, sie sollten Schaden vermeiden (13).

Um die Risiken, die von Robotern ausgehen, zu minimieren, können sie so programmiert werden, dass sie Gesetze und ethische Regeln einhalten. Dabei ist zunächst zu klären, welche Regeln und Gesetze in die Programmierung eingehen (11). Dafür müssen die ausgewählten Gesetze interpretiert und ausgelegt werden (8). Die Drohnen-Einsätze der USA in Pakistan zeigen beispielhaft, wie unterschiedlich dabei die Interpretationen des Kriegsrechts sein können (8, 15). Die Interpretation von Regeln und Gesetzen ist nicht eindeutig und entzieht sich daher auch einer allseits als korrekt anerkannten Programmierung.

Bei der Programmierung von Ethik sind die folgenden Fragen zu beantworten:

- Welche ethische Grundlage wird benutzt?

- Gibt es übereinstimmende rechtliche und moralische Gefahren bei der Konstruktion von Kampfrobotern?

- Sollen Kampfroboter als Werkzeuge, wie beispielsweise Gewehre, angesehen und behandelt werden (8)?

Um ethisches Verhalten zeigen zu können, muss der Roboter drei Kompetenzen besitzen: die Fähigkeit, den Zustand der Welt korrekt zu erfassen und zu verstehen, die Fähigkeit, korrekte Entscheidungen und Abschätzungen hinsichtlich der ethischen Akzeptanz der Aktionen unter den gegebenen Umständen zu machen, sowie die Fähigkeit, seine Aktivitäten der Förderung ethischen Verhaltens anzupassen (4, 12). Darüber hinaus sollte er die Fähigkeiten besitzen, einem unethischen Akt zu widerstehen (14).

In der Annahme, dass jede mögliche, komplexe Situation korrekt formalisiert und in Realzeit berechnet werden kann und es sich mit Ethik ebenso verhält (14), wurden Modelle zur Implementierung von Ethik und ethischen Entscheidungen umgesetzt.

Dabei ist klar, dass es unmöglich ist, einen ethisch unfehlbaren Roboter zu bauen (12). Aber es gibt die Vermutung, ethische Probleme algebraisch zu lösen (12).

Ethik-Implementierung

Die meisten Robotersteuerungs-Architekturen beruhen auf einem 3-Schichtenmodell. In diesem Modell ist jede Steuerungsschicht durch den Abstraktionsgrad und zeitlichen Rahmen beschrieben. Die oberste Schicht ist der Langzeitziel-Controller. Als nächstes werden die Ziele in eine Menge von Aufgaben geteilt, die ausgeführt werden müssen. Abschließend werden die Aufgaben in Aktionen aufgeteilt, die ausgeführt werden können (13).

Zu einer solchen Architektur kann eine vierte Schicht für das ethische Verhalten hinzufügen. Diese vierte Schicht agiert wie ein Controller, der das beabsichtigte Verhalten der anderen drei Schichten evaluiert, bevor es ausgeführt wird (13).

Für die Ethik-Implementierung schlagen Arkin et al. (1, 2) ein Modell vor, dass aus einem Simulationsmodul und einem Evaluationsmodul besteht. Das geltende Kriegsrecht sowie die aktuellen Einsatzregeln werden in einer Datenbank hinterlegt. Im Simulationsmodul werden die möglichen Handlungsoptionen in der jeweiligen Situation simuliert und die Ergebnisse an das Evaluationsmodul weitergegeben. Im Evaluationsmodul werden die Handlungsoptionen anhand der hinterlegten Regeln bewertet. Die Handlungsoption, die gegen keine Regeln verstößt, wird gewählt. Das Evaluationsmodul verhält sich dabei wie ein Wächter. Es lässt nur (ethisch) zulässige Handlungen zu. Deshalb wird das Evaluationsmodul als *Ethical Govenor* bezeichnet. Was passiert, wenn keine solche Option gefunden wird, bleibt in der Literatur offen.

Während der Kampfhandlung und danach wird im Rahmen eines *Self-Assessments* das Verhalten des Roboters überprüft. Dabei sollen die Kollateralschäden bewertet werden, die die Aktionen des Roboters zur Folge haben. Die Bewertung wird in einer Variablen *Schuld* akkumuliert. Für die Variable Schuld gibt es Schwellwerte. Wird ein solcher Schwellwert erreicht, stehen bestimmte Waffensysteme dem Roboter zukünftig nicht mehr zur Verfügung. Dies geht soweit, dass der Roboter am Ende nicht mehr in der Lage ist, eine tödliche Kampfhandlung auszuführen. Ein solches System wird laut seiner Urheber Arkin und Ulam nie perfekt sein, aber besser als eine menschliche Soldatin oder ein menschlicher Soldat, wenn es um die Einhaltung internationalen Kriegsrechts geht (1).

Moralischer Rückzug des Menschen und (fehlende) Moral des Roboters

Kämpfen hinter dem Bildschirm ist nicht so emotional potent wie Kämpfen auf dem Schlachtfeld (10). Das Steuern eines Kampfroboters kommt der Erfahrung eines Computerspiels nahe. Dadurch werden die Konsequenzen des Handelns nicht so intensiv wahrgenommen wie bei einem Einsatz auf einem Schlachtfeld (14). Für SoldatInnen, die Videospiele in ihren Jugendjahren gespielt haben, ist kein großer Unterschied zwischen einem Videospiel und einer ferngesteuerten Kampfhandlung zu erkennen. Moralischer Rückzug, mangelndes Schuldbewusstsein und verschwindende Selbstbeschränkung sind die Folge. Zusätzlich beeinflussen und steigern die Abnahme der Kontrollorientierung, das „Photoshopen" des Krieges, die Moralisierung der Technik und die Entscheidungsgeschwindigkeit den moralischen Rückzug der OperateurInnen. Die Entpersonalisierung der Kampfhandlung führt zu einer Dehumanisierung der Gegner (10). Mit der zunehmenden Autonomie der Kampfroboter wird der moralische Rückzug weiter vorangetrieben, da die OperateurInnen nun nicht einmal mehr steuernd in die Kampfhandlungen eingreifen können.

Autonome Roboter werden auch zukünftig keine Gefühle, keine sozialen Fähigkeiten und kein Gewissen haben. Auch das Gefühl, Teil dieser Welt zu sein, fehlt ihnen. Gefühle, soziale Fähigkeiten und das Zusammengehörigkeitsgefühl sind die Voraussetzungen, um moralische Entscheidung zu treffen (12).

Einhaltung von Recht, Gesetz und ethischen Regeln

Sauer und Schörnig gehen davon aus, dass selbstlose Roboter, die ihre eigene Existenz dem ethischen Programm unterordnen und nicht von Stress, Müdigkeit oder begrenzten kognitiven Möglichkeiten eingeschränkt sind, dafür aber über schnelle Entscheidungsfähigkeiten verfügen, die Rechtmäßigkeit in bewaffneten Konflikten erhöhen können (11). Um die Risiken zu minimieren, die von Robotern ausgehen, können sie so programmiert werden, dass sie Gesetze und ethische Regeln einhalten. Dabei ist zunächst zu klären, welche Regeln in die Programmierung eingehen (12). Gesetze müssen hierfür interpretiert und ausgelegt werden (8, 11). Der Prozess der Interpretation und Auslegung lässt sich nicht in Software abbilden. Die Drohneneinsätze der USA in Pakistan zeigen beispielhaft, wie unterschiedlich solche Interpretationen sein können (8, 15).

Roboter, die die rechtlichen Anforderungen an bewaffnete Konflikte erfüllen sollen, müssen in der Lage sein, in unklaren Situationen auf der Basis von subjektiven Analysen vorzugehen. Unklarheit und Subjektivität machen Verstöße wahrscheinlicher, was den Absichten und Zielen der Ethikprogrammierung zuwiderläuft (7). Es ist schon eine Herausforderung, zu definieren, wer eine Zivilistin oder ein Zivilist ist, speziell vor dem Hintergrund irregulärer Kriege (11). Um die rechtlichen Anforderungen der *situativen Wahrnehmung* zu erfüllen, muss ein Roboter in der Lage sein, z. B. die Intentionen einer/s Anderen zu verstehen und ihr oder sein Verhalten in der bestimmten Situation vorherzusagen. Potenzielle Mehrdeutigkeiten auf dem Schlachtfeld, wie ein Kind, das ein Gewehr aufhebt, sind nahezu unbegrenzt, oft subtil und erfordern ein Niveau an menschlichem Verständnis, das Roboter nicht erreichen. Aufmerksamkeit erlaubt Anpassung und Reaktion im Falle von Zweifel. Zweifel ist ein fundamentaler Faktor bei der umfassenden Beurteilung einer Situation. Ohne vollständige Kenntnis, was angegriffen wird, und ohne angemessenes Wissen, wie ZivilistInnen betroffen sind, wird das Ergebnis Kollateralschäden und verletzte ZivilistInnen umfassen. Dass das *Sense-Think-Act*-Paradigma[1] ausreicht, Regeln in diesem Ausmaß durch den Roboter selbst anzupassen, darf bezweifelt werden (7).

Henning Lübbecke

Henning Lübbecke studierte Informatik an der Technischen Hochschule Darmstadt. Seit 2013 ist er Sprecher der Fachgruppe *Informatik und Inklusion* im Fachbereich *Informatik und Gesellschaft* der Gesellschaft für Informatik (GI) und im FIfF schon bestens ausgewiesen durch seinen Workshop *Teilhabe an der allgegenwärtigen Kommunikation* auf der FIfFKon 2015 in Erlangen. Aktuell ist er bei einer Bundesbehörde beschäftigt sowie als Lehrbeauftragter an der HS Bund tätig.

Technische Probleme

Die Zuverlässigkeit von Kampfrobotern hängt von ihrem Design und ihrer Software ab (8). Insbesondere Software enthält Fehler (8). Die formale Verifikation so komplexer Systeme ist nicht in einer realistischen Zeitspanne vorstellbar, wenn sie überhaupt möglich ist. Fehler in der Software dieser Systeme lassen sich daher nicht ausschließen (14).

Die grundlegende Robotertechnologie ist leicht zu beherrschen, so dass mittlerweile mehr als 40 Staaten in der Lage sind, Militärroboter herzustellen (8). Aus dem *Silberstreif* kann schnell ein *Bumerang* werden. Drohnen und Roboter lassen sich für vergleichsweise wenig Geld aus zivilen Komponenten zusammenbauen. Das Knowhow hierfür ist leicht zugänglich (11, 14).

Da Kampfroboter in der Regel vernetzt sind, bestehen für sie dieselben Sicherheitsrisiken wie für Smartphones oder PCs (8). Es besteht ein hohes Risiko des Hackens von Kommunikationsstrukturen. Große Datentransfervolumen, wie sie zwischen Robotern und ihren Kommandozentralen entstehen, sind anfällig gegen Abhören und Geräusche. Es ist höchst wahrscheinlich, dass fremde Kräfte sich bemühen, Roboter durch Hackangriff auf ihre Kommunikationsinfrastruktur außer Gefecht zu setzen. Ein gehackter Roboter in den Händen Aufständischer ist extrem gefährlich, insbesondere für die eigenen SoldatInnen (8, 14).

Die derzeitige Technologie ist nicht in der Lage, zwischen ZivilistInnen und feindlichen SoldatInnen auf einem urbanen Schlachtfeld des 21. Jahrhunderts zu unterscheiden (7). ExpertInnen sind sich uneinig, ob Roboter jemals ausreichend zwischen Beteiligten und Unbeteiligten unterscheiden können (11).

Fazit

Kampfroboter – der *Silberstreif am Horizont* für die Beteiligungen demokratischer Staaten an Kriegen? Nein. Kampfroboter schonen das Leben der eigenen SoldatInnen, nicht aber das der Menschen auf der Gegenseite. Ethische Entscheidungen sind nicht berechenbar und entziehen sich damit auch der Möglichkeit, sie algorithmisch zu ermitteln. Kampfroboter können daher zwar Regeln einhalten, aber nicht ethisch handeln (12). Kampfroboter befördern eine neue Rüstungsspirale. Sie erhöhen die Kriegsgefahr, da sie zu einem Sinken der Hemmschwelle für einen Kriegseintritt führen und durch ihre leichte Kopierbarkeit von vielen, auch nichtstaatlichen Akteuren genutzt werden können. Der Einsatz von Kampfrobotern ist unmoralisch, weil dafür niemand zur Verantwortung gezogen werden kann und sie selbst nicht bestraft werden können (12). Deswegen ist es erforderlich, autonome Kampfroboter zu verbieten (6, 14).

Literatur

(1) Arkin RC, Ulam P (2009) An ethical adaptor: Behavioral modification derived from moral emotions. In: 2009 IEEE International Symposium on Computational Intelligence in Robotics and Automation-(CIRA). IEEE, S. 381-387.

(2) Arkin RC, Ulam PD, Duncan B (2009) An ethical governor for constraining lethal action in an autonomous system. Georgia Institute of Technology, 2009.

(3) Asimov I (1950) „Runaround". I, Robot (The Isaac Asimov Collection ed.). New York City: Doubleday. p. 40.

(4) Briggs GM, Scheutz M (2014) How robots can affect human behavior: Investigating the effects of robotic displays of protest and distress. International Journal of Social Robotics, 6. Jg., Nr. 3, S. 343-355.

(5) Briggs GM, Scheutz M (2015) „Sorry, I Can't Do That": Developing Mechanisms to Appropriately Reject Directives in Human-Robot Interactions. In: 2015 AAAI fall symposium series.

(6) GI-Stellungnahme „Tödliche autonome Waffensysteme (LAWS) müssen völkerrechtlich geächtet werden", https://gi.de/fileadmin/GI/Allgemein/PDF/GI-Stellungnahme_LAWS_2019-02.pdf (abgerufen am 28. Mai 2019)

(7) Herbach JD (2012) Into the Caves of Steel: Precaution, cognition and robotic weapon systems under the International Law of Armed Conflict. Amsterdam LF, 4. Jg., S. 3.

(8) Lin P, Abney K, Bekey G (2011) Robot ethics: Mapping the issues for a mechanized world. Artificial Intelligence, 175. Jg., Nr. 5-6, S. 942-949.

(9) Rast M (2014) Domänenübergreifende Modellierung und Simulation als Grundlage für virtuelle Testbeds. Apprimus.

(10) Royakkers L, van Est R (2010) The cubicle warrior: the marionette of digitalized warfare. Ethics and information technology, 12. Jg., Nr. 3, S. 289-296.

(11) Sauer F, Schörnig N (2012) Killer drones: The 'silver bullet' of democratic warfare?. Security Dialogue, 43. Jg., Nr. 4, S. 363-380.

(12) Sullins JP (2010) RoboWarfare: can robots be more ethical than humans on the battlefield?. Ethics and Information technology, 12. Jg., Nr. 3, S. 263-275.

(13) van der Elst D, Winfield A (2018) An architecture for ethical robots inspired by the simulation theory of cognition. Cognitive Systems Research, 48. Jg., S. 56-66.

(14) Weber J (2009) Robotic warfare, human rights & the rhetorics of ethical machines. Ethics and robotics, S. 83-103.

(15) Wikipedia, Seite „Drohnenangriffe in Pakistan". In: Wikipedia, Die freie Enzyklopädie. Bearbeitungsstand: 27. April 2019, 14:48 UTC. URL: https://de.wikipedia.org/w/index.php?title=Drohnenangriffe_in_Pakistan&oldid=187966509 (abgerufen am 23. Mai 2019)

(16) Wikipedia, Seite „Robotergesetze". In: Wikipedia, Die freie Enzyklopädie. Bearbeitungsstand: 15. Mai 2019, 14:31 UTC. URL: https://de.wikipedia.org/w/index.php?title=Robotergesetze&oldid=188601410 (abgerufen am 23. Mai 2019)

Anmerkung

1 *Das sogenannte* Sense-Think-Act-Paradigma *gilt als operative Definition eines (mobilen) Roboters. Ein besonderer Aspekt der mobilen Robotik ist die Interaktion des Roboters mit seiner veränderlichen, oft unbekannten und unstrukturierten Umgebung. Diese muss mit entsprechender Sensorik erfasst und mit geeigneten Algorithmen mit semantischer Bedeutung versehen werden (Sense). Für vollständig autonome Systeme sind moderne Methoden der künstlichen Intelligenz von Bedeutung (Think), beispielsweise zur Selbstlokalisation, Navigation und Handlungsplanung. Zur Bewegung in verschiedensten Umgebungen sind unterschiedlichste Antriebstechniken notwendig und die Manipulation der Umwelt erfordert häufig hoch redundante Kinematiken mit der entsprechend komplexen Regelung (Act). (entnommen aus: [Rast, Malte: Domänenübergreifende Modellierung und Simulation als Grundlage für Virtuelle Testbeds, Dissertation, RWTH Aachen University, 2014, ISBN 987-3-86359-283-7])*

Thomas Reinhold

Rüstungskontrolle für den Cyberspace – Herausforderungen und erste Ansätze

Das Konzept der Rüstungskontrolle wurde als politische Reaktion auf die Rüstungsdynamiken im internationalen Staatensystem entwickelt. Rüstungskontrolle ist dabei im Kern ein normatives Unterfangen, das vom Prinzip der Verhinderung zukünftiger Kriege geleitet wird und sich dabei auch mit den Bedingungen und Umständen befasst, die zu bewaffneten Konflikten führen. Das Konzept kann als „einseitige Maßnahmen, bilaterale und multilaterale Abkommen sowie informelle Regime (…) zwischen Staaten bezeichnet werden, um bestimmte Kategorien von Waffen oder militärischen Operationen einzuschränken oder zu reduzieren, um stabile militärische Gleichgewichte zu erreichen und so Spannungen und die Wahrscheinlichkeit von Konflikten zu verringern" (Den Dekker, 2004).

Diese Aufgabe kann dabei in drei verschiedene Teile aufgegliedert werden (Müller & Schörnig, 2006):

- Kriegsprävention und Verringerung der Konfliktwahrscheinlichkeit, Begrenzung der Beschleunigung der Rüstungsdynamik und ihrer Ursachen und Verringerung der Wahrscheinlichkeit von Präventivschlägen,
- Schadensbegrenzung bei bewaffneten Konflikten, Begrenzung des Umfangs von Leid, Tod und Zerstörung durch bestimmte Waffensysteme mit massivem Zerstörungspotenzial oder andere Waffen, die in großem Umfang eingesetzt werden können,
- Senkung der für Rüstung ausgegebenen Mittel.

Vor diesem Hintergrund betrachtet, enthalten konkrete Rüstungskontrollansätze die folgenden individuell festgelegten Maßnahmen, die in Form von Verträgen für bestimmte Waffen, Waffenteile und Waffentechnologien zwischen Staaten vereinbart werden:

- Transparenz über militärische Fähigkeiten,
- stabile und dauerhafte Kommunikation in den zwischenstaatlichen Beziehungen,
- Definition und Kontrolle quantitativer und qualitativer Grenzen für Waffentechnologien,
- Beschränkung oder Verbot der Verbreitung von Waffen, Waffenteilen oder Waffentechnologien,
- Festlegung spezifischer Überprüfungsmaßnahmen, die es Staaten ermöglichen, die Übereinstimmung anderer Vertragsparteien zu überprüfen.

Diese Ansätze sind nicht notwendigerweise kompatibel, da der Fokus in einer konkreten Situation immer von der Konfiguration und dem Niveau des politischen, wirtschaftlichen oder (erwarteten) militärischen Konflikts abhängt. Das ist auch wichtig im Hinblick auf die realistische Einschätzung der Möglichkeiten und der erwarteten Ergebnisse der Rüstungskontrolle in bestimmten Situationen. Rüstungskontrolle kann daher nicht mit Abrüstung gleichgesetzt werden, deren Ziel in jedem Fall in der konkreten Reduktion von Waffen bis hin zu deren kompletter Abschaffung liegt.

Maßnahmen der Rüstungskontrolle

Rüstungskontrollbemühungen sind fast immer ein allmählicher Prozess, dessen Erfolg oft nur vorübergehend ist und von den politischen Umständen und den verantwortlichen Akteuren abhängt. In vielen Fällen ist die Ausgangssituation geprägt von zwei oder mehr Vertragsstaaten mit einem gewissen Maß an Misstrauen oder Unsicherheiten hinsichtlich der gegenwärtigen oder geplanten militärischen Aktivitäten anderer Staaten, die als Bedrohungen wahrgenommen werden. Dazu zählen bspw. ein aggressives territoriales Verhalten sowie die qualitative oder quantitative militärische Bewaffnung. Neue militärisch genutzte Technologien und ein ggf. unzureichendes Verständnis ihrer invasiven oder zerstörerischen Fähigkeiten verschärfen solche angespannten Situationen. Die aktuellen Debatten über Cyberwaffen veranschaulichen diese Situation: Einerseits ist noch unklar, was genau Cyberwaffen im sicherheitspolitischen Kontext sind, und ob offensive militärische Handlungen im Zusammenhang mit dem Cyberspace dem üblichen Ansatz der Verwendung von „militärischer Gewalt" entsprechen. Ebenso ist international umstritten, wie militärische Cyber-Tools bewertet, verglichen und kategorisiert werden können um sie im Rahmen völkerrechtlicher Normen zu regulieren. Andererseits verdeutlichen internationale Studien die steigende Nachfrage der Streitkräfte nach Kapazitäten im Zusammenhang mit Cyber-Mitteln (UNIDIR, 2013).

Angesichts vergleichbarer Herausforderungen des Misstrauens, der Aufrüstung und der Gefahr von Konflikten durch Zufall oder aufgrund von Missverständnissen wurde bereits in der Zeit des Kalten Krieges das Konzept der *vertrauensbildenden Maßnahmen (CBM)* entwickelt. Diese Maßnahmen, die ursprünglich von der Konferenz für Sicherheit und Zusammenarbeit in Europa (KSZE) eingeführt wurden, beabsichtigen durch schrittweise und gegenseitige Zugeständnisse den Informationsaustausch und die Verringerung des militärischen Drucks eine Zusammenarbeit zwischen den Staaten herzustellen (CSCE, 1986). Ein wichtiges, niedrigschwelliges Element bildeten dabei oft unpolitische Gespräche über die technischen Aspekte der Sicherung von Waffen und der benötigten Einrichtungen, um auf diese Weise aktive Kommunikationskanäle zwischen gegnerischen Parteien aufzubauen, wobei der Schutz der jeweils eigenen Bevölkerung vor unerwünschten und zerstörerischen Auswirkungen von Waffentechnologien durch versehentliche Auslöser als kleinster gemeinsamer Nenner aller Staaten fungierte.

Neben der Anbahnung und Etablierung zwischenstaatlicher Beziehungen hängt die Stabilität von Rüstungskontrollabkommen außerdem entscheidend von Möglichkeiten ab, die Einhaltung

von Vereinbarungen gegenseitig zu überprüfen. Diese *Verifizierungsmaßnahmen* reichen dabei von Verfahren, die eine Kontrolle ohne Vor-Ort-Bewertung ermöglichen, wie Kameraüberwachung von relevanten Anlagen, Luftbildaufnahmen oder seismische Sensoren, über die strukturierte Erhebung und den Austausch von Daten zu Lagerbeständen und Handelsvolumen bis hin zu Vor-Ort-Inspektionen mit der Zählung und Messung von Lagerbeständen und der Überprüfung von versiegelten Einrichtungen.

Die Herausforderungen von Rüstungskontrollmaßnahmen im Cyberspace

Der Cyberspace als Domäne weist einige sehr spezifische Merkmale auf, die sich stark von den anderen Domänen wie Land, Luft und See unterscheiden. Dazu gehören die Virtualität dieser Domäne und der darin enthaltenen Informationen, die nicht physische Repräsentierung von Code und die nahtlose Duplizierung von Daten. Diese Merkmale stellen insbesondere für die praktische Seite von Rüstungskontrollvereinbarungen große Herausforderungen dar und unterminieren einen Großteil der etablierten Ansätze. Neben den technischen Schwierigkeiten beruhen diese Probleme auch auf den unterschiedlichen Auffassungen der Staaten hinsichtlich des Cyberspace und der Frage der staatlichen Souveränität in diesem Bereich. Unklar ist weiterhin die Frage, welchem internationalen Komitee oder Institution die Überwachung und Kontrolle der technischen Weiterentwicklung des Cyberspace übertragen werden kann, die seine langfristige friedliche Ausrichtung sicherstellt und in der die internationale Staatengemeinschaft gleichberechtigt vertreten ist. Eine ähnliche Herausforderung ergibt sich mit Bezug auf die Frage nach einer international legitimierten Institution, die mit der Untersuchung von mutmaßlichen Cyberattacken staatlichen Ursprungs betraut werden könnte, um nationale Einzelinteressen im Rahmen des *Blame-Game* auszugleichen (Davis II et al., 2017). Das derzeitige Fehlen einer international einheitlichen Klassifizierung von Cyberwaffen oder jeglicher Art von bösartigen Cyber-Hilfsmitteln verschärft diese Situation weiter, da die sich daraus ergebende Unberechenbarkeit ein „Gleichgewicht der militärischen Cybermächte" verhindert, bei dem Staaten zustimmen, militärische Fähigkeiten einheitlich und vergleichbar einzuschränken. Darüber hinaus handelt es sich bei Cyberwaffen oft um *One-Shot-Waffen*, die mit ihrem Einsatz ihre zukünftige Wirkung verlieren, indem sie ihre Angriffsvektoren offenbaren. In der Summe führt dies zu einer eher zurückhaltenden internationalen Debatte über die Offenlegung der Cyber-Kapazitäten von Staaten.

Erste Ansätze der Rüstungskontrolle im Cyberspace

Über die letzten Jahre ist das internationale Verständnis der Gefahren einer unkontrollierten Militarisierung des Cyberspace und der Notwendigkeit von Cyber-Rüstungskontrollmaßnahmen gewachsen. Nachfolgend sollen einige der Ansätze vorgestellt werden, die verschiedene Akteure auf verschiedenen Ebenen der zwischenstaatlichen Zusammenarbeit unternommen haben.

1. Die Wassenaar-Exportkontrollvereinbarung und ihre Erweiterung von 2013

Das *Wassenaar-Übereinkommen über die Kontrolle der Ausfuhr konventioneller Waffen sowie Güter und Technologien mit doppeltem Verwendungszweck* ist ein multilaterales System zur Kontrolle von Rüstungsexporten. Es wurde 1996 mit dem Ziel gegründet, die Transparenz des Handels mit Rüstungsgütern zwischen den inzwischen 42 Vertragsstaaten zu verbessern (Wassenaar, 2011). 2009 wurde die Regulierungs-Liste um solche Güter erweitert, die sowohl für zivile als auch für militärische Zwecke verwendet werden können. Die Mitgliedsstaaten verpflichten sich, den Export dieser kritischen Güter zu kontrollieren, Ausfuhranfragen zu prüfen und im Verdachtsfall wegen des Potenzials für sicherheitskritische oder menschenrechtsgefährdende Anwendung abzulehnen. Handelsdaten werden zweimal jährlich zwischen den Mitgliedstaaten ausgetauscht. Ende 2013 wurde die Vereinbarung durch die Aufnahme von *Intrusion-Software* (als eine Zusammenfassung von Überwachungs-, Spionage- und Sabotage-Software) in den Katalog der kritischen Güter erweitert. (Wassenaar, 2013). Eines der Probleme des Wassenaar-Abkommens ist jedoch seine Umsetzung, die in die Souveränität und Verantwortung jedes Mitgliedstaats fällt und unabhängig voneinander erfolgt. Entscheidungen und Ausfuhrkontrollen werden in den Mitgliedstaaten nicht einheitlich gehandhabt und für standardisierte Verfahren besteht keine Verpflichtung. Die kollektive Kontrolle der internationalen Verbreitung kritischer Güter, ein wesentlicher Bestandteil der klassischen Rüstungskontrollvereinbarungen, ist daher nur eingeschränkt möglich und erreicht keine allgemeine Gültigkeit. Dennoch könnte der Ansatz als Blaupause für einen potenziell globalen Ansatz zur Regulierung betrachtet werden, wenn er mit konsequenten und harmonisierten nationalen Ausfuhrgesetzen kombiniert und einer internationalen Kontrollinstanz wie einer UN-Organisation unterstellt wird.

2. Der Vorschlag des EU-Parlaments für eine EU-Verordnung zur Kontrolle der Ausfuhr von Gütern mit doppeltem Verwendungszweck von 2018

Auf der Grundlage des Wassenaar-Abkommens hat die Europäische Kommission begonnen, die weitere Regulierung solcher Waren im Rahmen eines einheitlichen Systems der Ausfuhrkontrolle für die EU-Länder zu erörtern (EU-Kommission, 2016a) voranzutreiben. Der Standpunkt des EU-Parlaments folgt dabei den Grundsätzen des Wassenaar-Abkommens über die Regulierung von Technologien, die zur Cyberüberwachung und Menschenrechtsverletzungen eingesetzt werden können (EU-Kommission, 2016b). Bei der Bewertung der Ausfuhrgenehmigung müssen die Mitgliedstaaten jedoch über die mutmaßliche Verwendung der Güter hinausgehend das Risiko einer Umgehung der festgelegten Regeln berücksichtigen. Die geplante Verordnung verfolgt außerdem einen Ansatz der *Catch-All-Kontrolle,* der die Regulierung auch für nicht explizit gelistete Technologieelemente ermöglichen sowie die Kontrolle zukünftiger, aktuell noch nicht berücksichtigter Entwicklungen umfassen soll. Neben dem Ansatz eines EU-weiten gemeinsamen Ausfuhrkontrollgesetzes wird ein System der Sorgfaltspflicht für Exportstaaten und den Exporteur selbst, sowie die Zuständigkeit für standardisierte Berichte über nationale Exportkontrollmaßnahmen vorgeschlagen. Dies soll die Schwäche des Wassenaar-Ansatzes aufheben, einer nationalen

Souveränität in Bezug auf die spezifischen Exportvorschriften und Berichterstattungsverfahren. Der Vorschlag des EU-Parlaments wird derzeit mit dem Rat der EU diskutiert.

3. Empfehlungen der Gruppe der Regierungsexperten der Vereinten Nationen aus dem Jahr 2015

Die Generalversammlung der Vereinten Nationen befasst sich seit 1999 in mehreren Beschlüssen mit dem zunehmend relevanten Thema des Cyberspace, seinem Potenzial für wissenschaftlichen und technologischen Fortschritt sowie seiner Nutzung für bösartige Zwecke. 2003 wurde dazu die Einrichtung einer Expertengruppe (UN GGE) beschlossen, die sich mit den Bedrohungen dieses Bereichs, aber auch den Chancen und Möglichkeiten der internationalen Zusammenarbeit im Bereich der Informations- und Kommunikationstechnologie befassen soll. Die letzte erfolgreiche Gruppe aus dem Jahr 2015 hat eine Reihe freiwilliger, unverbindlicher Normen für verantwortungsbewusstes Staatsverhalten empfohlen (UN GGE, 2015). Dabei wurde einerseits die staatliche Souveränität im Cyberspace betont, andererseits aber auch auf die staatliche Verantwortung bei Cyber-Aktivitäten verwiesen, die vom jeweiligen Staatsgebiet ausgehen:

Die Normen empfehlen den Staaten zusammenzuarbeiten, um schädliche IKT-Praktiken zu verhindern. Staaten sollten nicht wissentlich zulassen, dass ihr Territorium für international rechtswidrige Handlungen mit IKT verwendet wird. Kein Staat sollte IKT-Aktivitäten durchführen oder wissentlich unterstützen, die die Nutzung und den Betrieb kritischer Infrastruktur absichtlich beschädigen. Staaten dürfen die Informationssysteme der autorisierten Notfallteams eines anderen Staates nicht beschädigen oder ihre eigenen Teams nutzen, um sich an böswilligen internationalen Aktivitäten zu beteiligen. (Auszug aus UN GGE, 2015)

Diese unverbindlichen Normen wurden von der UN-Generalversammlung angenommen und mit dem Aufruf an ihre Mitgliedsstaaten verbunden, sich daran bei der Nutzung von Informations- und Kommunikationstechnologien zu orientieren. Auch die G20 hat ihren Staaten empfohlen, diese Empfehlungen umzusetzen (UNODA, 2017).

4. Vorschläge der OSZE für vertrauensbildende Maßnahmen

In den letzten zwei Jahren hat die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) zwei Entscheidungen erlassen, die sich auf „vertrauensbildende Maßnahmen zur Verringerung der durch die Nutzung von IKT bedingten Konfliktrisiken" beziehen. Die dafür von der Organisation entwickelten Maßnahmen sollen die „zwischenstaatliche Zusammenarbeit, Transparenz, Vorhersehbarkeit und Stabilität verbessern und (…) das Risiko von Fehlwahrnehmung, Eskalation und Konflikten verringern". Die Maßnahmen sind freiwillig, aber die OSZE hat ihre Mitgliedstaaten angewiesen, ihre politischen Entscheidungen, Gesetzgebung und ihr Verhalten auf diese Prinzipien zu stützen. Die meisten Vorschläge betreffen zwischenstaatliche Konsultationen, die Definition einer gemeinsamen Terminologie für den Cyberspace und seiner Bedrohungen sowie den Informationsaustausch in Bezug auf die Sicherheit und Nutzung von IKT sowie insbesondere die Risiken für kritische nationale und internationale IKT-Infrastrukturen und deren Integrität (OSZE, 2016). Obwohl diese Vorstöße *nur* das politische Verhalten von Staaten betreffen, sollten die Bemühungen als äußerst wertvoll angesehen werden. Die OSZE spielt als internationale Organisation eine wichtige Rolle, die Staaten verbindet, indem sie eine wichtige und etablierte Plattform für Dialog und Entscheidungsfindung bietet, die als Grundlage für Verhandlungen und weitere Vereinbarungen dienen kann.

5. Staatsgetriebene Vorschläge für staatliche Normen und Verantwortlichkeiten im Cyberspace

Neben den genannten multilateralen Ansätzen haben in den letzten Jahren auch verschiedene Staaten Vorschläge für verbindliche Normen und Regeln für das Verhalten von Staaten im Cyberspace entwickelt. Diese Vorschläge sind dabei jedoch zum Teil von nationalen außenpolitischen Prioritäten bestimmt oder spiegeln nationale Ansichten und Bedenken hinsichtlich der Souveränität des Staates und der inneren Sicherheit wider.

Ende Oktober 2018 unterbreiteten sowohl Russland als auch die USA jeweils zusammen mit anderen unterstützenden Staaten dem Ersten Ausschuss der Generalversammlung der Vereinten Nationen zwei getrennte Vorschläge zur Weiterentwicklung von Normen und Verantwortlichkeiten für das Verhalten von Staaten im Cyberspace. Beide Vorschläge betonen, dass Staaten Informationstechnologie nicht dazu verwenden sollten, Aktivitäten durchzuführen, die der Aufrechterhaltung des Weltfriedens und der internationalen Sicherheit entgegenstehen oder in die inneren Angelegenheiten anderer Staaten eingreifen. Der russische Vorschlag (UN, 2018a), der von 26 anderen Ländern, einschließlich China, unterstützt wird, bekräftigt dabei explizit die Empfehlungen der UN-GGE und definiert eine umfassende Liste an Grundsätzen für verantwortungsvolles Verhalten. Eine Besonderheit dieses Vorschlags besteht darin, dass er die staatliche Souveränität über den nationalen Anteil des Internets unterstreicht und daraus ein Recht der Staaten ableitet, alle Informationen prüfen und regulieren zu dürfen, die innerhalb nationaler IT-Systeme und IT-Netzwerken geteilt, übertragen, gespeichert und verteilt werden. Auch der von den USA geführte Vorschlag (UN, 2018b), der von 35 Nationen unterstützt wird, bestätigt Ergebnisse der UN-Expertengruppen. Er fordert dabei jedoch eine weitere Konzentration auf die Frage, wie das Völkerrecht auf die Nutzung von ITK durch den Staat angewendet werden kann, ohne dabei neue Räume nationaler Souveränität zu definieren, die mit der Redefreiheit und anderen Menschenrechten in Konflikt stehen.

Abschließend sollen zwei weitere Vorschläge erwähnt werden, die beide 2018 veröffentlicht wurden. Zum einen der von der französischen Regierung vorgestellte *Pariser Aufruf für Vertrauen und Sicherheit im Cyberspace* (France-Gov, 2018). Der unverbindliche Aufruf zielt darauf ab, bestehende institutionelle Mechanismen zur „Begrenzung von Hacking- und Destabilisierungsaktivitäten" im Cyberspace zu fördern und konzentriert sich auf Hauptaufgaben: Regulierung staatlicher Aktivitäten auf der Grundlage von Normen, staatliche Souveränität im Cyberspace und Schutz der Bürger. Das Dokument fördert eine umfassende und koordinierte Regulierung des Cyberspace, insbesondere die

Wahrung von Frieden und Sicherheit auf internationaler Ebene mit einer stärkeren Steuerung durch UN Gremien. Es erkennt die Anwendbarkeit des humanitären Völkerrechts auf den Cyberspace an, einschließlich der Menschenrechte und des Völkergewohnheitsrechts. Die Rolle und Verantwortung der staatlichen Akteure in Cyber-Konflikten soll gestärkt werden und aktive Cyber-Abwehrmaßnahmen von Unternehmen sollen ausgeschlossen werden. In gleicher Weise werden „offensive Operationen nichtstaatlicher Akteure" und der Einfluss ausländischer Staaten auf demokratische Prozesse wie Wahlen verurteilt. Das Dokument fordert, dass der „öffentliche Kern des Internets" vor feindlichen Akteuren geschützt wird, und fordert von der Industrie ein stärkeres Engagement für „Sicherheit durch Design" in Produkten und Dienstleistungen. Eine zweite Erklärung, die ähnliche Ziele verfolgt, ist die *Commonwealth Cyber Declaration* (Commonwealth, 2018), die auf dem Treffen der Regierungschefs aller Commonwealth-Staaten 2018 verabschiedet wurde. Die Erklärung ist im Hinblick auf die vielen kleineren und wirtschaftlich weniger relevanten Staaten relevant, die darin die Bedeutung des Cyberspace für ihre Nationen betonen, die Unversehrtheit dieser Domäne fordern und ein Mitbestimmungsrecht an deren Entwicklung zum Ausdruck bringen. Die Commonwealth Cyber Declaration ist daher zusammen mit den Maßnahmen der OSZE eines der stärksten zwischenstaatlichen Signale für eine friedliche Entwicklung des Cyberspace. Beide erkennen den Cyberspace als Grundlage nationaler wie internationaler sozialer, wirtschaftlicher und politischer Entwicklung an und betonen die Gefahren einer Destabilisierung des Cyberspace durch einseitige verdeckte Aktivitäten einzelner staatlicher Akteure.

Referenzen

Commonwealth. (2018) Commonwealth Cyber Declaration.

CSZE. (1986) Document of the Stockholm Conference on Confidence- and Security-Building Measures and Disarmament in Europe Convened in Accordance with the Relevant Provisions of the Concluding Document of the Madrid Meeting of the Conference on Security and Co-operation, iss. 2. Retrieved from https://www.osce.org/fsc/41238?download=true

Davis II, John S., Boudreaux, Benjamin, Welburn, Jonathan William, Aguirre, Jair, Ogletree, Cordaye, McGovern, Geoffrey, & Chase, Michael S. (2017) Stateless Attribution: Toward International Accountability in Cyberspace. Rand. Retrieved from http://www.rand.org/pubs/research_reports/RR2081.html

EU-Kommission (2016a) Commission proposes to modernise and strengthen controls on exports of dual-use items

EU-Kommission (2016b) Regulation setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (recast). Retrieved from http://trade.ec.europa.eu/doclib/docs/2016/september/tradoc_154976.pdf

France-Gov (2018) Paris Call for Trust and Security in Cyberspace

Müller, H., & Schörnig, N. (2006) Rüstungsdynamik und Rüstungskontrolle: Eine exemplarische Einführung in die internationalen Beziehungen (Vol. Aussenpolitik und internationale Ordnung). Nomos. Retrieved from http://books.google.com/books?id=yphePQAACAAJ

OSCE (2016) Beschluss Nr. 1202 – Vertrauensbildende Massnahmen der OSZE zur Verminderung der Konfliktrisiken, die sich aus dem Einsatz von Informations- und Kommunikationstechnologien ergeben PC.DEC/1202. Retrieved from http://www.osce.org/de/pc/228501?download=true

Reinhold, Thomas, & Reuter, Christian (2019) Arms Control and its Applicability to Cyberspace. In Information Technology for Peace and Security – IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace (pp. 207–231). Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-25652-4_10

UN-GGE (2015) Consensus report 2015 – Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security – A/70/174 . Retrieved from http://undocs.org/A/70/174

UN (2016) Resolution adopted by the General Assembly on 23 December 2015. Retrieved from https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2016/01/A-RES-70-237-Information-Security.pdf

UN (2018a) Draft resolution by Russia and other states concerning the developments in the field of information and telecommunications in the context of international security

UN (2018b) Draft resolution by the USA and other states on advancing responsible State behaviour in cyberspace in the context of international security

UNIDIR (2013) The Cyber Index – International Security Trends and Realities. Retrieved from http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

Wassenaar (2011) Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies – Guidelines & Procedures,including theInitial Elements. Retrieved from http://www.wassenaar.org/guidelines/docs/5 – Initial Elements.pdf

Wassenaar (2013) The Wassenaar Arrangement on export controls for conventional arms and dual-use goods and technologies – List of dual-use goods and technologies and munitions list. Retrieved from https://www.wassenaar.org/app/uploads/2019/consolidated/WA-LIST%20%2813%29%201.pdf

Thomas Reinhold

Thomas Reinhold hat Informatik und Psychologie studiert und ist seit 2004 als Wissenschaftler und Freelancer für Software-Sicherheit tätig. Seit 2010 ist er Non-Resident Fellow am IFSH in der Projektgruppe IFAR² mit dem Forschungsschwerpunkt der Konsequenzen einer Militarisierung des Cyberspace und der Entwicklung von praktischen Maßnahmen der Friedenssicherung in dieser Domäne. 2015 leitete er die bundesweite Cyberpeace Kampagne des Vereins *Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung* (FIfF e. V.). Als Experte für die Gefahren des Cyberwar und die Herausforderungen für Cyberpeace wurde er 2017 als Mitglied des *Transatlantischen Cyber-Forums* der *Stiftung Neue Verantwortung* sowie in die *Research Advisory Group* der *Global Commission on the Stability of Cyberspace* berufen. Darüber hinaus ist er seit vielen Jahren im Forschungsverbund *Naturwissenschaft, Abrüstung und internationale Sicherheit* (FONAS e. V.) aktiv und Mitglied der *Arms Control Association*.

Ingo Ruhmann und Ute Bernhardt

IT-Sicherheitsrecht 2.0 – Einschränkungen statt Schutz von Grundrechten

Der Schutz von Persönlichkeitsrechten und des Grundrechts auf informationelle Selbstbestimmung war von Beginn an abhängig von adäquaten technischen und organisatorischen Schutzmaßnahmen gegen die missbräuchliche Nutzung von Daten und gegen Eingriffe in IT-Systeme. Spätestens mit dem 2008 definierten Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[1] ist die Exekutive in besondere Weise aufgefordert, technische, organisatorische und rechtliche Maßnahmen zu treffen, um digitale Schutzrechte zu gewährleisten. Zusammen mit dem Fernmeldegeheimnis gibt es einen klar formulierten Rahmen von Grundrechten, dem Rechtsetzung und die Praxis zur IT-Sicherheit folgen müssten. Die gegenwärtige Entwicklung wird dem nicht gerecht.

Die zunehmende Zahl von IT-Sicherheitsvorfällen, die sich nicht allein gegen Unternehmen und Privatpersonen richten, sondern auch gegen den Bundestag, Ressorts der Bundesregierung und internationale Einrichtungen, dokumentiert die Dringlichkeit, den Schutz der IT-Systeme zu verbessern. Die Untersuchung der Art und Intensität einiger Vorfälle hat verdeutlicht, dass die früher dominierenden Angreifer mit privatem oder kriminellem Hintergrund zunehmend durch staatliche Akteure ergänzt wurden, die über Ressourcen in vorher nicht gekanntem Ausmaß verfügen und diese auch intensiv – gegen Verbündete ebenso wie gegen Wettbewerber – einsetzen.

Die Bundesregierung hat 2015 darauf regulatorisch reagiert durch die Verabschiedung des IT-Sicherheitsgesetzes.[2] Nachgelegt wird nun das „*IT-Sicherheitsgesetz 2.0*“.[3] Nicht minder umfangreich fiel die Reaktion auf exekutiver Ebene aus. Die Aufgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI), des Bundesamtes für Verfassungsschutz (BfV), des Bundeskriminalamtes (BKA) und des Bundesnachrichtendienstes (BND) wurden erweitert und mit erheblichen Personalzuwächsen unterlegt. Mit der Errichtung der *Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITIS)* des Innenressorts und der *Agentur für Disruptive Innovationen in der Cybersicherheit und Schlüsseltechnologien (ADIC)* von Innen- und Verteidigungsressort wird die zielgerichtete Entwicklung und Bereitstellung von Werkzeugen für Cyber-Aktivitäten für Stellen des Bundes verfolgt, begleitet durch die Restrukturierung des ehemaligen *Kommandos Strategische Aufklärung* und dessen Migration in das *Kommando Cyber- und Informationsraum (KdoCIR)* der Bundeswehr. Die neuen Aufgaben von ZITIS, ADIC und KdoCIR, aber auch des BND und BfV sind allerdings keineswegs auf den Schutz der Integrität, Verfügbarkeit und Vertraulichkeit von IT-Systemen bezogen. Ihre Aufgabe ist es, Sicherheitslücken in IT-Systemen zu finden, neue Angriffsformen zu entwickeln und diese Hintertüren für staatliche Stellen nutzbar zu machen. Ihr Organisationszweck steht daher in einem starken Spannungsverhältnis zum verfassungsmäßigen Schutz von Grundrechten.

Wie viele andere Bereiche der IT-Sicherheit auch[4], so laufen Entwicklung, Einsatz und Nutzung von Angriffswerkzeugen sowie die dafür notwendigen Vorarbeiten nicht nur verfassungsmäßigen Grundsätzen zuwider. Wie im Folgenden nachgezeichnet wird, stehen viele der erforderlichen Arbeitsschritte in konkretem Widerspruch zum Strafrecht und zum internationalen Recht. Die aufgeworfenen Fragen sind komplex, vielfach neu und im deutschen Recht in keiner systematischen Weise in Beziehung zueinander gesetzt. Hier sollen daher vor allem die verschiedenen Dimensionen einer rechtlichen Bewertung unterzogen und mögliche Konsequenzen aufgezeigt werden. Ausgehend von einer Binnensicht des deutschen Rechts bei konkreten Eingriffen in IT-Systeme wird untersucht, welche rechtlichen Neuerungen geplant sind, um Ansätze für spezifische Eingriffe zu erhalten und auch die als „Hack-Backs“ bezeichneten Angriffe auf IT-Systeme außerhalb des deutschen Staatsgebiets vorzubereiten.

Das Recht

Staatliches Handeln basiert auf Gesetzen. Der Aufbau von Behörden und jede Verwendung öffentlicher Mittel sind abhängig von der Definition von Aufgaben, die sich aus den in den Verfassungen von Bund und Ländern vorgesehenen Rechten und Pflichten ableiten lassen müssen. Wenn exekutives Handeln in die Rechte Dritter – möglicherweise sogar Grundrechte – eingreift, so sind gesetzlich möglichst klar definierte Rechtsnormen erforderlich. Das darauf bezogene Exekutivhandeln sollte richterlich – oder wenn dies der Aufgabe nach nicht möglich ist, notfalls durch vergleichbare Konstruktionen wie parlamentarische Kontrollgremien – überprüfbar sein.

Das Grundrecht auf Unverletzlichkeit der Wohnung ist im Strafrecht nicht nur gegen die Entnahme von Wertgegenständen – Einbruchdiebstahl – geschützt, sondern beim Hausfriedensbruch auch gegen unerwünschtes Betreten. In der Strafprozessordnung ist formuliert, unter welchen Bedingungen durch staatliche Stellen in das Grundrecht auf Unverletzlichkeit der Wohnung eingegriffen und auf die Kompetenz von Schlossern für die nicht-konsensuelle Schaffung von Zugängen zurückgegriffen werden darf.

In der digitalen Sphäre werden solche im Analogen selbstverständlichen Grundsätze infrage gestellt. Schon beim Staatstrojaner wurde nicht ausgeschlossen, die Trojaner-Software bei Bedarf über einen physischen Zugang – d. h. den verdeckten Einbruch in die Räume der Zielperson – zu installieren.[5] Die Bundesregierung hatte bei der Reform des BSI-Gesetzes 2007 die Idee, dem BSI die Befugnis zu geben, ohne richterlichen Beschluss die Geschäftsräume eines Betreibers von Kommunikationstechnik zu betreten und sich „Zugang zu Gebäuden, Einrichtungen und informationstechnischen Systemen verschaffen“, „wenn dies zur Abwehr einer dringenden Gefahr für die Kommunikationstechnik des Bundes erforderlich sei“[6]. Davon nahm sie nur zögerlich Abstand. Diese Idee taucht nun modifiziert im *IT-Sicherheitsgesetz 2.0* wieder auf, eingeschränkt auf die Betriebsräume der Betreiber der von Bundesbehörden genutzten IT-Systeme. Anstatt also den Bundesbehörden Auflagen bei der Vergabe von Aufträgen an Rechenzentren zu machen, wird das BSI generell gesetzlich zum Eingreifen befugt. Noch weiter geht die Bundesregierung im „IT-Sicherheitsgesetz 2.0“ mit einem geplanten § 163g der Strafprozessordnung (StPO)[7], nach dem die Sicher-

heitsbehörden „auch gegen den Willen des Inhabers auf Nutzerkonten“ und die „Funktionen, die ein Anbieter eines Telekommunikations- oder Telemediendienstes dem Verdächtigen zur Verfügung stellt“ […] zugreifen“ können sollen. Dazu muss ein Nutzer den Sicherheitsbehörden die Zugangsdaten zu ihren Online-Diensten herausgeben, damit die Behörden die Online-Konten übernehmen und im Namen des Nutzers agieren können. Die Zulässigkeit der neuen Regelung wird an die Voraussetzungen des bestehenden § 100g StGB geknüpft. Der erlaubt die Abfrage von Verkehrsdaten wie etwa Funkzellen bei Verdacht auf schwere oder gemeingefährliche Straftaten, solchen gegen das Betäubungsmittelgesetz, bei Schleuser-Tätigkeit sowie bei Waffenhandel. Erlaubt würde danach die Identitätsübernahme durch den § 163g StPO aber – so § 100g STGB – auch bei „einer Straftat von auch im Einzelfall erheblicher Bedeutung“ oder wenn ein Verdächtiger eine Tat „in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat […] oder eine Straftat mittels Telekommunikation begangen hat“. Da alle Computer-Straftaten „mittels Telekommunikation“ begangen werden, ist die Folge, dass jeder Verdacht auf eine solche ausreichend wäre für eine Identitätsübernahme durch die Sicherheitsbehörden. Das ist nicht nur eine neue Dimension von Grundrechtseingriffen, sondern dürfte obendrein bei der Attribution von Cyberangriffen ganz neue Komplikationen aufwerfen. All dies sind Regelungsideen, die übertragen auf die analoge Welt als rechtswidriger Eingriff unmittelbar nachvollziehbar wären. Aber auch das Grundrecht auf informationelle Selbstbestimmung und das auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sind strafrechtlich in ähnlicher Weise gegen Einbruch in Systeme, Diebstahl oder Manipulation von Daten, gegen den Handel mit Einbruchswerkzeugen und einige Spezifika geschützt. Neu ist, dass die Bundesregierung die Entwicklung technischer Vorkehrungen zur Schaffung von Zugängen nun selbst in die Hand nimmt.

Der Austausch über Sicherheitslücken und die dazu verwendeten Mittel ist für IT-Sicherheitsexperten immer mit einem strafrechtlichen Risiko verbunden. Dem aktuellen Wortlaut des § 202c Strafgesetzbuch (StGB) nach macht sich bereits strafbar, wer Computerprogramme entwickelt, die Sicherungsmaßnahmen überwinden können und den Zugang zu geschützten Daten ermöglichen, oder sie „herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht“. Die Bundesregierung begründete die Einführung dieser Regelung: Die „Gefährlichkeit und Schädlichkeit von Hacking-Angriffen zeigen sich vor allem in jüngster Zeit auch in Deutschland (z. B. durch den Einsatz von Key-Logging-Trojanern, Sniffern oder Backdoorprogrammen)“[8]. Nun plant die Bundesregierung im *IT-Sicherheitsgesetz 2.0* überdies die Einführung eines § 200e StGB, um den „unbefugten Zugang zu einem Informationstechnischen System“ für sich oder einen Dritten unter Strafe zu stellen[9].

Neue Behörden und Befugnisse

Aufgabe von ZITIS ist, Zugangs- und Entschlüsselungswerkzeuge zu entwickeln bzw. einzukaufen und anderen zur Verfügung zu stellen. ZITIS hat also die Aufgabe, die technischen Mittel für genau die beiden hier beschriebenen Gesetzesverstöße zu entwickeln, zu beschaffen und anschließend anderen Behörden zu überlassen, ohne dass dafür gesetzliche Ausnahmen geschaffen wurden. Die Agentur für Disruptive Innovationen (ADIC) von Innen- und Verteidigungsressort setzt einen Schritt davor an und verfolgt die Entwicklung von IT-Sicherheitstechnik ebenso wie die von Angriffswerkzeugen für zivile Behörden und die Bundeswehr. Die Bundesregierung schließt zwar aus, Malware-Implantate in kritischen Infrastrukturen anderer Staaten „ohne die entsprechenden, insbesondere völkerrechtlichen, Rechtsgrundlagen einzusetzen“[10]. Nicht ausschließen will sie aber deren Entwicklung und auch deren Einsatz auf Rechtsgrundlagen, deren Prüfung sie noch nicht abgeschlossen hat.[11] Wohlgemerkt: Der Schutz von IT-Systemen ist Verfassungsauftrag und Grundrecht, eine Verbesserung des gesetzlichen Schutzes ist daher eindeutig zu begrüßen. Umso deutlicher ist dann aber der Bedarf, die Befugnisse der Behörden ebenso klar zu regeln.

Denn ZITIS kann sich auf kein Sonderrecht berufen. Die Spionagetätigkeit des BND bedeutet auch das Eindringen in fremde IT-Systeme. Auch die Bundeswehr soll im Kriegsfall in gegnerische IT-Systeme einbrechen. Das BSI entstammt zwar als Zentralstelle für das Chiffrierwesen dem BND,[12] prüft heute aber auf Basis eines eigenen Gesetzes IT-Sicherheitsaspekte und entwickelt und testet zivile Chiffriersysteme[13]. ZITIS soll der Bundesregierung zufolge die Behörden der Inneren Sicherheit mit informationstechnischen Fähigkeiten unterstützen. ZITIS sei kein Nachrichtendienst und habe keine Eingriffsbefugnisse und keine Sonderrechte.[14] ZITIS arbeitet somit entgegen strafrechtlicher Regelungen. Die Aufgabe der ADIC ist zwar abstrakter und in die Forschung vorverlagert; aber das Strafrecht sieht für Forschungsarbeiten aber keine Ausnahme vor. Die Tätigkeit der so Beschäftigten ist damit strafbar.

Um Sicherheitsvorfälle zu erkennen, müssen befallene Systeme forensisch untersucht werden bzw. die Datenkommunikation mit Hilfe von Auswertungssoftware – *Intrusion-Detection*-Systemen – auf Anomalien hin analysiert werden. Aufgabe der ZITIS-Abteilung TKÜV sind Arbeiten zur „Telekommunikationsüberwachung (u. a. Verbesserung des internationalen Datenaustauschs auf Grundlage der Europäischen Ermittlungsanordnung und der Auswertung von IP-Daten)“.[15] Aus rechtlicher Sicht stellt sich aber die Frage, woher die Daten für die Auswertung stammen. Für das auf Verdacht erfolgende Protokollieren und Auswerten von beliebigem, bei einem Provider durchlaufenden Datenverkehr (*Deep Packet Inspection*) wurde im § 100 Telekommunikationsgesetz (TKG) eine erweiterte Befugnisnorm nur für die Provider selbst geschaffen. Weder das BSI noch andere Behörden sind derzeit befugt, Kommunikationsdaten von Providern anzufordern und zu analysieren. Lediglich der BND kann bei der strategischen Kommunikationsüberwachung des Datenverkehrs mit dem Ausland Daten sammeln, die zur Analyse von Angriffen nutzbar sind. Strafverfolgungsbehörden dürfen derzeit nur Telekommunikations-*Verkehrsdaten* anfordern.[16] Die Weitergabe der von Fachleuten klassifizierten Kommunikationsinhalte bei IT-Sicherheitsvorfällen ist eine Straftat[17].

Der Schutz des Fernmeldegeheimnisses wird erst dann umgangen werden, wenn das BSI mit dem IT-Sicherheitsgesetz 2.0 durch eine Ergänzung an § 109 TKG Provider anweisen kann, protokollierte Kommunikationsdaten zu übergeben, um die Daten automatisiert auszuwerten – und sie 10 Jahre lang zu speichern[18]. ADIC oder ZITIS dürften aber auch dann nicht legal

über Kommunikationsdaten für IT-Sicherheitsanalysen verfügen. Diese können nur von einem Provider oder einer staatlichen Stelle stammen, die diese Daten unter Bruch des Fernmeldegeheimnisses weitergegeben hat.

Rechtliche Befugnisse und Aufgaben der alten und neuen Behörden zur IT-Sicherheit stehen also in einem wenig systematischen und widersprüchlichen Verhältnis zueinander.

Hack-Backs in Krieg und Frieden

Zu den neuen Operationsideen in der staatlichen IT-Sicherheit haben sich „Hack-Backs" gesellt, der offiziellen Darstellung zufolge die Beantwortung eines Cyberangriffs in der Regel aus dem Ausland durch gleichartige Gegenmaßnahmen. Lassen wir hier zunächst den Spannungs- und Verteidigungsfall beiseite, dann steht in einem an Recht und Gesetz gebundenen System auch diese Idee mit dem Strafrecht in einem nicht überbrückbaren Spannungsverhältnis.

§ 303 StGB stellt unter Strafe, Datenverarbeitungsanlagen oder Datenträger zu zerstören, zu beschädigen, unbrauchbar zu machen, zu beseitigen oder zu verändern. Nichts anderes ist das Ziel von Hack-Backs: Das Eindringen in fremde IT-Systeme, das Löschen von dort abgelegten Daten, das Hinterlegen und Installieren von Schadsoftware, die Außerbetriebnahme des gehackten Systems und andere Manipulationsformen.

Die Idee der Hack-Backs produziert einen ganz neuen Zielkonflikt. Zur Schadenminderung erlaubt das TKG in § 109 den Providern, Datenverkehre von und zu einer Störquelle einzuschränken, umzuleiten oder zu unterbinden. Das BSI soll nach dem *IT-Sicherheitsgesetz 2.0* Provider in Zukunft dazu anweisen können. Eine Störung oder ein Angriff wären damit zu beenden. Allerdings wäre ein von Providern – etwa durch Vorkehrungen in Routing-Tabellen – effektiv blockiertes IT-System auch für Hack-Backs der Sicherheitsbehörden nicht mehr direkt erreichbar. Wer Hack-Backs einsetzen will, wird den Angreifer also nicht einfach vom Internet-Datenverkehr aussperren wollen – oder muss seinerseits Zugangswege über Dritte suchen und die Auseinandersetzung über deren Wege führen – was eine Ausweitung des Angriffs nach sich ziehen dürfte.

Auch das Argument, die internationale Kooperation sei zu umständlich, trägt nicht. Die Bundesregierung hat sich mit der *Budapest Convention on Cybercrime* zur Kooperation und gegenseitigen Unterstützung bei Cyberattacken verpflichtet. Ausgenommen davon sind nach Art. 27 (4) der Konvention nur Fälle „nationaler Souveränität" und „essentieller Interessen". Unkooperatives Verhalten verrät implizit seine (sicherheits-) politischen Beweggründe und damit die Beteiligung staatlicher Stellen. Dies wiederum sieht das *Tallinn-Manual* – Ergebnis eines von der NATO beauftragten Expertenkreises – recht eindeutig: Von staatlichen Stellen nicht unterbundene Angriffe gegen IT-Systeme in einem anderen Staat stellen einen Bruch internationalen Rechts dar. Angriffe von staatlichen Stellen auf andere Staaten stellen Kriegshandlungen dar. Sie rechtfertigen sogar konventionelle militärische Gegenschläge, wenn die Schäden die Wirkung von Militärschlägen erreichen. Gegen IT-Systeme in anderen Staaten gerichtete Hack-Backs sind daher keine Lösung in transnationalen Cyber-Vorfällen, sondern ein Bruch internationalen Rechts oder gar der Weg zu Kriegshandlungen.[19]

Praxis der Hack-Backs sind präemptive Eingriffe

Doch damit nicht genug. Im Vorfeld der Cyber-Sicherheitskooperation zwischen den USA und der VR China 2015 sickerte durch, die US-Dienste würden das Abkommen nicht akzeptieren, wenn sie auf ihre Implantate in den Systemen der VR China verzichten müssten.[20] Prominente Datendiebstähle bei US-Behörden machten zugleich klar, dass die chinesischen Cyber-Akteure den USA nicht nachstehen. Zu den wenig beachteten Snowden-Enthüllungen gehört auch, dass der für elektronische Kriegsführung zuständige US-Geheimdienst NSA in Systeme gegnerischer Dienste einbricht, dort Implantate hinterlässt und sich Erkenntnisse von gegnerischen Aufklärungserfolgen auf dritter Seite und sogar vierter Seite beschafft. Die NSA weiß dadurch, dass und wie andere Dienste ihre Werkzeuge in allerlei fremden IT-Systemen einbauen – und dass konkurrierende Dienste dasselbe tun. Den Cyberkriegern dieser Welt ist also bekannt, dass alle Seiten ihre Cyberwaffen in den Infrastrukturen ihrer Zielländer in Stellung gebracht haben und bei Bedarf losschlagen können.

Hack-Backs sind keineswegs nur eine Notwehr-Maßnahme. Hack-Backs dienen dem Ausschalten der IT-Infrastruktur von vermuteten Gegnern, und zugleich der Vorbereitung solcher Cyber-Operationen. Dies hat die Bundesregierung als Handlungsoption nicht ausgeschlossen, wenn es die Rechtslage hergibt.[21] Dazu gehört, die Urheberschaft zu verschleiern und Fährten zu nichts ahnenden Dritten zu legen. Die Bundesregierung erklärte „False Flag"-Angriffe – zu Deutsch: das Kapern von Rechnern in Drittstaaten und deren Missbrauch für Cyberangriffe – zur zulässigen Kriegslist.[22]

Der russischen Seite wird vorgeworfen, Hacker für staatliche Zwecke als digitale Söldner einzusetzen.[23] Mit dem in Deutschland geplanten Zwang zur Herausgabe persönlicher Zugangsdaten zu Online-Diensten bei Straftaten, die „mittels Telekommunikation begangen werden", damit die Behörden die eigenen Online-Konten übernehmen und damit operieren können, entsteht eine ganz neue und eigene Form der Verwicklung von Hackern, IT-Sicherheitsfachleuten, Internetnutzern und staatlichen Stellen für Cyber-Operationen in einem Maße, das man bei Spionagefilmen für maßlos übertrieben halten würde.

Fazit

Wenn Behörden wie BND, BfV, ZITIS, ADIC und die Bundeswehr erst nach Sicherheitslöchern suchen, um dann in IT-Systeme einzugreifen und Hack-Backs durchzuführen, kompromittieren sie nicht nur die Sicherheit der IT-Infrastruktur, sondern setzen für ihr Eingriffshandeln voraus, dass die Missetäter ungestört weiter operieren können. Die meisten der beteiligten Behörden dürften nicht einmal über die Daten verfügen, die sie benötigen, um Gefährdungen aufzuspüren oder Angriffswege zu finden.

Mit der Entwicklung von Angriffsoptionen anstelle einer ausgebauten Kooperation mit staatlichen Stellen anderer Länder verstößt die Bundesregierung gegen internationales Recht. Hack-

Backs sind nicht nur keine Antwort auf IT-Sicherheitsvorfälle, sondern als Mittel zum Setzen von Implantaten in gegnerische IT-Systeme und Infrastrukturen essenzielle Voraussetzung für die Vorbereitung und Führung von Cyberkonflikten. Im Spannungsfall bringen Hack-Backs hoch riskante Eskalationsgefahren mit sich und geben angegriffenen Staaten einen völkerrechtlich legitimierbaren Grund, gegen Deutschland mit militärischen Mitteln vorzugehen. Mit dem *IT-Sicherheitsgesetz 2.0* sollen hierfür weitere Grundlagen geschaffen werden.

Vergleichbar zu den Zeiten des Kalten Kriegs haben wir bei Cyberwaffen ein Maß an gegenseitiger Abschreckung erreicht, das kooperative Maßnahmen dringend erforderlich macht, um eine schnelle und gefährliche Eskalation zu verhindern. Die notwendige Bedingung zur Bekämpfung von mehrstufigen Angriffen ist die Kooperation von Stellen in den verschiedenen betroffenen Staaten, um den Urhebern von Angriffen auf die Spur zu kommen. Die USA, Russland und die VR China hatten bis 2015 bereits eine dreiseitige Cyber-Sicherheitskooperation zuwege gebracht. Wer IT-Sicherheit erhalten will, muss als nächste Schritte auf den Ausbau von Kooperations- und Informationsstrukturen in internationalen Abkommen abzielen. Das setzt verantwortliches politisches Handeln voraus. Hack-Backs und die damit verbundenen Wege zur Schwächung der IT-Sicherheit sind das genau nicht.

Anmerkungen

1 *Bundesverfassungsgericht, Urteil des Ersten Senats vom 27. Februar 2008 - 1 BvR 370/07, 1 BvR 595/07*
2 *Bundesgesetzblatt, Teil I, Nr. 31, 17.7.2015, S. 1324*
3 *Am 3.4.2019 veröffentlicht von netzpolitik.org unter https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/#2019-03-27_BMI_Referentenentwurf_IT-Sicherheitsgesetz-2*
4 *Ingo Ruhmann, Ute Bernhardt: IT-Sicherheit, das EU-Recht und die Grundrechte: Neustart erforderlich; Gutachten des Netzwerks Datenschutz-Expertise, Mai 2016, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_eugh-itsig-2016.pdf*
5 *Vgl. etwa Dirk Fox in seinem Gutachten für das BVerfG, erschienen als Artikel: „Realisierung, Grenzen und Risiken der „Online-Durchsuchung“, DuD, Nr 31 (2007), S. 827-834, https://www.secorvo.de/publikationen/online-durchsuchung-fox-2007.pdf*
6 *Zitiert nach: http://www.dradio.de/dlf/sendungen/computer/849757/*
7 *Zitiert nach dem Entwurfstext bei netzpolitik.org, a.a.O.*
8 *So die Begründung der Gesetzesnovelle durch die Bundesregierung in Bt.-Drs. 16/3656, S. 9.*
9 *Auch dies zitiert nach dem Entwurfstext bei netzpolitik.org, a.a.O.*
10 *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Tobias Pflüger, Andrej Hunko, Michel Brandt, weiterer Abgeordneter und der Fraktion DIE LINKE: Rechtlich-organisatorischer Rahmen militärischer Cyber-Operationen, Bt.-Drs. 19/11920, Frage 9b*
11 *Ebd. Antwort auf die Fragen 3 bis 5*
12 *Ute Bernhardt; Ingo Ruhmann: Mutation einer Geheimdienststelle; in: Computerwoche, Nr. 12, 23. März 1990, S. 44–47*
13 *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) vom 14.08.2009*
14 *So die Bundesregierung in der Vorbemerkung und zu Frage 1 in der Antwort auf die Kleine Anfrage Struktur und Tätigkeit der Zentralen Stelle für Informationstechnik im Sicherheitsbereich, der Abg. Hahn u.a, Bt.-Drs. 19/6246*
15 *Ebd. Antwort auf Frage 22*
16 *Gemäß §100g StPO muss ein Provider Details der in Anspruch genommenen Telekommunikationsdienste und die Beteiligten an dem Telekommunikationsvorgang gemäß §96 TKG an Strafverfolgungsbehörden weitergeben.*
17 *Ingo Ruhmann, Ute Bernhardt: Der EuGH-Entscheid als Anstoß für mehr Rechtssicherheit in der IT-Sicherheit; DuD, Nr. 1, 2017, S. 34–38, S. 35f*
18 *So die geplante Änderung an §109 TKG im Entwurf des IT-Sicherheitsgesetz 2.0*
19 *Michael N. Schmitt (ed.): The Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge, 2013, S. 26ff*
20 *David E. Sanger: U.S. and China Seek Arms Deal for Cyberspace, New York Times, Sept. 19, 2015, http://www.nytimes.com/2015/09/20/world/asia/us-and-china-seek-arms-deal-for-cyberspace.html?_r=0*
21 *Vgl. Endnote 10, Antwort der Bundesregierung auf Frage 9b, Bt.-Drs. 19/11920*
22 *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan van Aken, Andrej Hunko, Christine Buchholz, weiterer Abgeordneter und der Fraktion DIE LINKE, „Elektronische Kampfführung der Bundeswehr“, BT-Drs. 18/3963, Antwort auf Fragen 30–33; Für die Nutzung ziviler IT-Systeme für solche Operationen siehe Plenarprotokoll der Fragestunde der 16. Sitzung des Deutschen Bundestages vom 19.2.2014, Antwort auf Frage 8, S. 1165 f.*
23 *So etwa beim Angriff auf den Bundestag: Wie russische Hacker Deutschland angriffen, Spiegel Online, 2.3.2018, https://www.spiegel.de/spiegel/spionage-wie-russische-hacker-deutschland-angriffen-a-1196180.html*

Ingo Ruhmann und Ute Bernhardt

Ingo Ruhmann ist Informatiker und arbeitet im Bereich Technikfolgenabschätzung, Forschungspolitik, IT-Sicherheit, Information Warfare, *Cyberwar*, Geschichte der Geheimdienste und Datenschutz. Er ist Lehrbeauftragter im Studiengang *Security Management* der Fachhochschule Brandenburg. Er ist Mitglied des FIfF und war Vorstandsmitglied von 1991 bis 1998.

Ute Bernhardt ist Informatikerin und beschäftigt sich seit Jahren mit Forschungspolitik, Datenschutz und IT-Sicherheit, dem Verhältnis von Wissenschaft und Frieden sowie der Beziehung von Informatik und Militär. Sie hat Lehraufträge an der Fachhochschule Bonn-Rhein-Sieg und der FernUni Hagen. Sie ist Mitglied des FIfF und war FIfF-Vorstandsmitglied von 1991 bis 1998.

Stadttheater Bielefeld 2019 – Foto: Jens Reimerdes, CC BY-SA 4.0

Stefan Hügel

BigBrotherAwards 2019

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

Wir fassen in diesem einleitenden Beitrag des Schwerpunkts zum BigBrotherAward 2019[1] zunächst die Laudationes für die PreisträgerInnen kurz zusammen. Danach drucken wir drei Laudationes im Wortlaut ab. Die Verleihung fand am 8. Juni 2019 im Stadttheater Bielefeld statt. Moderiert wurde sie von der Journalistin Golineh Atai.

Moderatorin Golineh Atai – Foto: Markus Benter, CC BY-SA 4.0

Kategorie *Behörden & Verwaltung*

Der BigBrotherAward in der Kategorie *Behörden & Verwaltung* ging an den **Innenminister des Landes Hessen, Peter Beuth (CDU)**,

1. *für die bundesweit erstmalige Anschaffung einer Analysesoftware der CIA-nahen Firma Palantir,*

2. *dafür, dass diese umstrittene US-Firma über Einsatz und Betrieb der Software Zugang zum Datennetz der hessischen Polizei erhält, und*

3. *dafür, dass mit dieser Analysesoftware Massendaten aus polizeieigenen und externen Quellen in Sekundenschnelle automatisiert verknüpft, analysiert und ausgewertet werden können – mit fatalen Auswirkungen auf Grundrechte, Datenschutz und Rechtsstaat.*

Laudator Rolf Gössner erinnert zunächst daran, dass die schwarz-grüne Hessische Landesregierung bereits im Vorjahr mit einem BigBrotherAward ausgezeichnet worden war, für die Verschärfung des Hessischen Verfassungsschutz- und Polizeigesetzes. Dieses ist inzwischen in Kraft, es gibt Verfassungsbeschwerden dagegen.

Auf Basis dieses Gesetzes wurde nun die US-amerikanische Firma *Palantir* beauftragt, ihre Analysesoftware *Gotham* bei der hessischen Polizei in Betrieb zu nehmen, mit spezifischen Anpassungen, unter der Bezeichnung *Hessen-Data*. Dies wird durch §25 des neuen Hessischen Polizeigesetzes ermöglicht, der Datenanalysen zur vorbeugenden Bekämpfung von über 40 Straftaten erlaubt.

Das US-amerikanische Unternehmen Palantir wurde 2004 gegründet, mit finanzieller Unterstützung der CIA. Diese Firma wurde nun damit beauftragt, die hessischen Polizeidatenbanken mit externen Datenbanken, z. B. Social-Media-Diensten zu verknüpfen und zu analysieren. Dabei ist nicht auszuschließen, dass auch vertrauliche Daten in die USA abfließen – dort unterliegt Palantir aber dem *Foreign Intelligence Surveillance Act* (FISA), nach dem Daten auf Anforderung an US-Geheimdienste übermittelt werden müssen.

Hessen-Data soll Datenanalysen liefern, durch die Bedrohungslagen leichter erkannt und terroristische „Gefährder" identifiziert werden können. Es geht also um Aufklärung im Vorfeld von Gefahren, wenn noch keine Straftat begangen wurde. Damit entwickelt sich Polizeiarbeit hin zu geheimdienstlicher Arbeit:

> *Hessen-Data ist ein Dammbruch für die polizeiliche IT-Arbeit: Bislang waren die Polizeidaten-Bestände der Strafverfolgung und Gefahrenabwehr nicht miteinander verknüpft, weil personenbezogene Daten aus datenschutzrechtlichen Gründen prinzipiell nur für den Zweck verwendet werden dürfen, für den sie erhoben wurden – also entweder für Strafverfolgung oderfür Gefahrenabwehr. Dieser Zweckbindungsgrundsatz wird mit Hessen-Data aufgehoben.*

Zusammenfassend schließt Rolf Gössner:

> *Die Analyseplattform Hessen-Data steht im Dauerkonflikt mit dem Recht auf informationelle Selbstbestimmung als Ausprägung des Allgemeinen Persönlichkeitsrechts (Artikel 2 Abs. 1 GG). Außerdem wird mit dem Einsatz der Palantir-Software eine wichtige Grundsäule des Datenschutzes buchstäblich niedergerissen: nämlich das Prinzip der Zweckbindung, wonach personenbezogene Daten grundsätzlich nur für den Zweck verwendet werden dürfen, für den sie erhoben worden sind. Und das Ganze auch noch weitgehend ohne wirksame Kontrolle und in einer unheiligen Allianz mit einem*

Hauptakteur des US-amerikanischen Militär- und Geheimdienstkomplexes.

Die vollständige Laudatio von Rolf Gössner ist ab Seite 39 nachzulesen.

Kategorie *Arbeitswelt*

In der Kategorie *Arbeitswelt* gibt es 2019 keinen BigBrother-Award. Peter Wedde erläuterte im Interview aber exemplarisch einige Möglichkeiten der Überwachung von MitarbeiterInnen durch ihre Arbeitgeber. Auch wenn viele Unternehmen den Datenschutz ernst nähmen – sei es aus Einsicht oder sei es wegen der zu erwartenden Strafen – gebe es häufig kleinere Fälle, die nicht an die Öffentlichkeit kommen, da das Interesse bei Journalisten an solch „unbedeutenden" Fällen gering ist. Er nannte einige Beispiele:

- Unzulässige Überprüfung der Daten von VertriebsmitarbeiterInnen mit Korrelation von Leistungsdaten mit der Gehaltsdatenbank und anschließender Kündigung „teurer" MitarbeiterInnen, wenn aus Sicht des Arbeitgebers die Leistung nicht ausreicht.

- Überwachung von externen Dienstleistern bei Banken, die mit kritischen Gelddaten zu tun haben, mit zwei Kameras (auf den Monitor und auf die Tastatur gerichtet). Bei MitarbeiterInnen der Bank kann der Betriebsrat durchsetzen, dass sie nicht mit Kameras überwacht werden; der Betriebsrat des externen Dienstleisters kann das nicht. Begründet wird die Überwachung mit Anforderungen der BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht), die jedoch auf Nachfrage dort nicht bestätigt werden – solche Überwachung sei schließlich nicht rechtens.

- Spracherkennungssoftware in Call Centern, die Anfragen z. B. darauf analysiert, ob eine AnruferIn lügt oder nicht, oder die die MitarbeiterInnen des Call Centers selbst aufgrund ihrer Stimme überwacht.

Peter Wedde weist auch auf die Bedeutung von Betriebsräten hin: Diese gebe es nur in etwa einem Drittel der Unternehmen. Wenn es Betriebsräte gibt, können sie regeln, was mit IT-Systemen passiert; sie können aber nicht verhindern, dass Arbeitgeber rechtswidrig handeln und haben dann nur schwache Eingriffsmöglichkeiten. Der Datenschutz unterliegt auch nicht der Mitbestimmung und Betriebsräte können Systeme letztlich nicht verhindern. Häufig verhielten sich betriebliche Datenschutzbeauftragte bei Datenschutzverstößen auch loyal zum Arbeitgeber und bieten wenig Unterstützung bei Beschwerden. Öffentliche Datenschutzbehörden sind unzureichend ausgestattet, um Eingaben zeitnah bearbeiten zu können.

Kategorie *Biotechnik*

Thilo Weichert hielt die Laudatio in der Kategorie *Biotechnik*. Dieser Preis ging an das Unternehmen **Ancestry.com**, weil es

das Interesse an Familienforschung dazu ausnutzt, Menschen zur Abgabe von Speichelproben zu veranlassen.

Früher wurde Familien- oder Ahnenforschung als Hobby betrieben, indem man beispielsweise Geburts-, Heirats- und Sterbeurkunden, Familienstammbäume oder Kirchenbücher auswertete. Heute bietet die DNA-Analyse die Möglichkeit, Verwandtschaftsbeziehungen nachvollziehen zu können. Man sendet eine Speichelprobe an ein Labor und erhält weitgehende Erkenntnisse über Verwandtschaft oder Herkunft. Vor allem in den USA gibt es mittlerweile viele Firmen, die solche Analysen anbieten.

Marktführer ist das Unternehmen *Ancestry.com*, gefolgt von der Google-Gründung *23andMe*. Ancestry.com ist inzwischen auch auf dem deutschen Markt präsent und hat eine Niederlassung in München eröffnet.

Das Angebot, so das Unternehmen, sei datenschutzkonform: „Sicherheit und Datenschutz genießen bei Ancestry oberste Priorität", so heißt es auf der Webseite. Jedoch, so Thilo Weichert:

Der Haken liegt – wie so oft – im Kleingedruckten und ist im Falle von Ancestry in einem dichten Gestrüpp von Bestimmungen verborgen: einer 16seitigen Datenschutzerklärung, elf Seiten Allgemeine Geschäftsbedingungen und siebeneinhalb Seiten Einwilligung in das Forschungsprojekt Ancestry Human Diversity Project.

Und weiter:

Mit dem Einsenden des Speichels erfolgt die Zustimmung zu den Datenschutzbestimmungen, wonach Ancestry selbst mit meinen Daten unbeschränkt über (Zitat) „Merkmale, persönliche Gesundheit und persönliches Wohlbefinden" Forschung durchführen kann. Wird dem Ancestry Human Diversity Project zugestimmt, so kommen „mitwirkende Partner" ins Spiel. Die Partner befinden sich (Zitat) „in den Vereinigten Staaten und anderen Ländern". Dabei kann es sich um „akademische Einrichtungen sowie Non-Profit-Organisationen, gewinnorientierte Unternehmen und Regierungsbehörden" handeln.

Doch damit nicht genug:

Menschen, die dort ihre DNA analysieren liessen, gerieten mitsamt ihren Familien ins Visier der Polizei, etwa weil sie mit dem so genannten „Golden State-Killer" auch nur entfernt verwandt sind. Um den Täter zu ermitteln, wurde die gesamte Verwandtschaft von den Ermittlern ausgeforscht. Kein Wort bei Ancestry.com über die potenzielle Strafverfolgung von biologischen Verwandten.

Als Fazit schließt Thilo Weichert:

Anbieter wie Ancestry missbrauchen das Interesse an Familienforschung, um einen Genom-Schatz für die kommerzielle Forschung anzuhäufen, denn das ist ihr eigentliches Geschäftsmodell. Die Datenschutzrechte der Probengeber und ihrer Verwandten müssen respektiert werden. Die deutschen Datenschutz- und Aufklärungspflichten werden aber von Ancestry aus Profitinteresse bewusst ignoriert. Wir sehen hier einen Trend: Nach der Ausbeutung von Internetdaten wird die Ausbeutung von Gendaten das nächste ganz große Ding. Ancestry ist der

Platzhirsch, der keine Datenschutz- oder Grundrechtsskrupel kennt.

Die vollständige Laudatio von Thilo Weichert ist ab Seite 41 nachzulesen.

Kategorie *Kommunikation*

Der BigBrotherAward in der Kategorie *Kommunikation* wurde an das Unternehmen **Precire Technologies GmbH** in Aachen verleihen. Es erhielt den Preis

für ihre wissenschaftlich zweifelhafte, wahrscheinlich rechtswidrige und gefährliche Sprachanalyse.

Laudatorin Rena Tangens erläuterte: Precire analysiert Sprechproben, um dadurch den Charakter eines Menschen herauszufinden, und damit auch z. B. seine oder ihre Eignung für eine ausgeschriebene Stelle. Dazu werde eine Probe von 15 Minuten benötigt, die nach Parametern wie Stimmhöhe, Lautstärke, Modulationsfähigkeit, Sprechtempo, Rhyhtmus analysiert wird. Das Ergebnis wird mit bereits vorhandenen Sprechproben verglichen und so auf den Charakter geschlossen. Der wissenschaftliche Wert dieser Analysen ist umstritten, doch ...

… Precire ... behauptet, ihr Verfahren sei wissenschaftlich abgesichert. Und winkt mit einer Buchveröffentlichung im wirtschaftswissenschaftlichen Springer Gabler Verlag. … Doch von seriöser Wissenschaft kann hier keine Rede sein, rügt Dr. Uwe Kanning, Professor für Wirtschaftspsychologie an der Hochschule Osnabrück in seiner Buchrezension. Er argumentiert, es existiere keine unabhängige Forschung zum Thema, der Algorithmus sei eine Blackbox und Geheimnis des Anbieters. Die vorhandenen Studien haben keine eigenen Zahlen erhoben, sondern sind Masterarbeiten, die sich auf die Daten stützen, die Precire ihnen zur Verfügung gestellt hat.

Fragen ergeben sich auch bei der Objektivität, sagt Rena Tangens. Ein Mitgründer von Precire erklärt: „Eine Maschine ist weniger fehleranfällig als ein Recruiter. Eine Maschine kann nur objektiv." Doch ...

… das ist eine äußerst naive Sicht der Dinge. Computer „verstehen" uns nicht. Das dürfen wir aber nicht mit Neutralität verwechseln. Computerprogramme sind auch voreingenommen, denn sie werden von Menschen programmiert. Menschen, die ihre eigenen Wertvorstellungen für selbstverständlich halten und in die Software mit einfließen lassen. Menschen mit bestimmten Fragestellungen, Zielen und Motiven. Und vor allem wird die Software mit einer ausgewählten Personengruppe als Referenz trainiert, die dann bestimmt, was als „normal", gut oder schlecht gilt.

Abschließend beschreibt Rena Tangens die Konsequenzen aus dieser Technologie:

Emotions- und Motivationserkennung per Sprachanalyse ist gefährlich, denn sie kann ohne unser Wissen irgendwo im Hintergrund passieren, wann immer wir sprechen. Diese Art der Sprachanalyse ist geradezu darauf angelegt, uns zu übervorteilen. So werden die einzelnen Menschen immer ohnmächtiger und unangreifbare Macht wandert immer mehr zu großen Konzernen, Versicherungen, Banken und staatlichen Stellen, die Zugriff auf unsere Daten und solche Technologie haben.

Die vollständige Laudatio von Rena Tangens ist ab Seite 43 nachzulesen.

Kategorie *Technik*

Laudator Frank Rosengart – Foto: Jens Reimerdes, CC BY-SA 4.0

Der BigBrotherAward in der Kategorie *Technik* wurde von Frank Rosengart angekündigt. Er geht an das **Technical Committee CYBER des Europäischen Instituts für Telekommunikationsnormen (ETSI)**,

für seine Bemühung, das Enterprise-Transport-Security-Protokoll (ETS) als Teil des neuen technischen Standards für die Verschlüsselung im Internet festzulegen und damit abgesicherte Verbindungen mit einer Sollbruchstelle auszustatten.

Internationale Gremien wie die Internet Engineering Task Force (IETF), gemeinsam mit Kryptographie-ExpertInnen, haben den Verschlüsselungsstandard Transport Layer Security (TLS) 1.3 entwickelt, die für die nächsten Jahre als sicher gelten soll. Doch …

… noch während der Beratungen über TLS 1.3 meldeten sich unter anderem Vertreter der Finanzindustrie zu Wort und wandten ein, dass sie strenge Compliance-Auflagen hätten, die es erforderlich machen, auch verschlüsselte Kommunikation, z. B. von Finanzberatern mit ihren Kunden, zu protokollieren – zum Beispiel um nachweisen zu können, dass sie gesetzestreu arbeiten. Sie behaupteten, sie bräuchten einen Nachschlüssel, um trotz Verschlüsselung für Dritte selbst alles lesen zu können. Dabei handelt es sich zwar um Daten, die sie auch auf ihren Servern im Klartext lesen könnten, aber für eine IT-Abteilung ist es einfacher, solche Daten an einem zentralen Punkt abzugreifen.

Das sehen offenbar auch Geheimdienste so, z. B. der GCHQ, der über Mitglieder des National Cyber Security Centre auch im

Technical Committee CYBER beim Europäischen Institut für Telekommunikationsnormen (ETSI) vertreten ist. ETSI entwickelte den Standard ETS (Enterprise-TLS) – mit Nachschlüssel, der beim Server-Betreiber hinterlegt ist:

> *Der Haken beim ETS-Standard ist aber, dass staatliche Stellen die Server-Betreiber verpflichten können, einen solchen festen Schlüssel einzustellen und diesen herauszurücken, um damit sämtliche Kommunikation mit Internetseiten im Nachhinein entschlüsseln zu können, zum Beispiel versendete Nachrichten.*

Und:

> *Eine besondere Gemeinheit ist außerdem, dass dieser „kaputte" Verschlüsselungsstandard für Browser und damit die NutzerInnen nicht vom „echten" zu unterscheiden ist. Es wird weiterhin das Schlüsselsymbol angezeigt; und der Browser hat technisch kaum eine Möglichkeit zu erkennen, ob ein fester Verbindungsschlüssel hinterlegt ist.*

Frank Rosengart schließt seine Laudatio:

> *Daher raten wir allen Entwicklern und technisch Verantwortlichen, einen großen Bogen um ETS zu machen und das deutlich sicherere TLS 1.3-Protokoll zu verwenden. Fatalerweise haben technisch nicht versierte Nutzerinnen und Nutzer kaum eine Möglichkeit, darauf Einfluss zu nehmen. Dieser zweite, unsichere ETS-Standard schafft eine verheerende Situation für die Online-Sicherheit.*

Kategorie *Verbraucherschutz*

Den letzten BigBrotherAward an diesem Abend, in der Kategorie *Verbraucherschutz*, kündigte padeluun an. Er ging an **Zeit Online …**

> *… dafür, dass sie*
>
> 1. *auf ihren Websites zeit.de und mycountrytalks.org zum Teil in großem Stil Werbetracker, wie auch das Facebook-Pixel einsetzen,*
>
> 2. *dafür, dass sie 2017 bei ihrem Projekt „Deutschland spricht" alle personenbeziehbaren Daten inklusiv der politischen Meinung auf den Rechnern von Google abgespeichert und verarbeitet haben und*
>
> 3. *dass sie sich für das Nachfolgeprojekt „My Country Talks" nicht nur von dem nimmersatten Werbeunternehmen mit Weltmachtsanspruch Google bei ihrem Projekt sponsern lassen, sondern dass sie zusätzlich Trackingtools eingebunden haben, mit denen Informationen an Dritte weiter gegeben werden können.*

Zeit Online hat im Jahr 2017 das Projekt *Deutschland spricht* durchgeführt, in dem Menschen unterschiedlicher Meinung ins Gespräch kommen sollten. Dieses Projekt wurde, so Laudator padeluun, zu Recht mit dem Grimme-Preis ausgezeichnet. Er kritisiert aber, dass die Daten der Teilnehmenden mitsamt ihren politischen Meinungen mit den Cloud-Tools der Google-Office-Suite verarbeitet und gespeichert wurden. Diese Tools würden auch sonst für große Teile der vernetzten Redaktionsarbeit genutzt. Den Informationen im Netz zufolge werden die Clouddienste anscheinend in Mountain View, Kalifornien von der Google LLC betrieben.

Der Verweis auf entsprechende Verträge und das EU-US-Privacy-Shield reiche dabei nicht aus, denn

> *Privacy Shield ist Augenwischerei. Das kann ich in 40 Treffern auf ZEIT ONLINE nachlesen. In 160 weiteren Treffen lese ich auf den Webseiten von ZEIT ONLINE, dass es da FISA gibt. Das heißt* Foreign Intelligence Surveillance Act *(auf deutsch: Gesetz zur Überwachung in der Auslandsaufklärung). Demnach dürfen die US-Geheimdienste bei allen US-Firmen ungehindert auf die Daten von Nicht-US-Bürgern zugreifen, wann immer sie wollen – egal, wo der Server steht. Und wie wir durch Edward Snowden gelernt haben, hatten die US-amerikanischen Behörden eine Standleitung zu Google.*

Außerdem …

> *… werden die Webseiten von Zeit Online über ein sogenanntes Content Delivery Network namens Fastly ausgeliefert. Die von mir getesteten IP-Nummern weisen nach Paris, aber Fastly ist eine US-amerikanische Firma, die in San Francisco, Kalifornien, angesiedelt ist. Und wie gesagt: FISA – der Foreign Intelligence Surveillance Act – gilt auch dann, wenn die Server US-amerikanischer Firmen in Europa stehen.*

Inzwischen gebe es eine neue Software, die mehreren Ländern genutzt wird. Diese ist nun nicht mehr bei Google gehostet, sondern in der Amazon Cloud.

„Das tun doch alle", sei häufig die Erklärung, so padeluun. Doch:

> *„Das tun doch alle", ist sicherlich kein guter Satz, um zu erklären, warum man Ethik und Moral außer acht lässt. Und wir kennen uns mit dieser Herausforderung durchaus aus: Auch wir Idealisten müssen Geld einnehmen, damit wir das ganze Jahr arbeiten und auch, um zum Beispiel die BigBrotherAwards finanzieren können.*

padeluun fährt fort:

> *Google ist aber einer der gierigsten Konzerne, der ein Datenmonopol anstrebt, und sich überall breit macht mit freundlichen bunten Lettern, Kicker in seine Firmenräume stellt, wo die Mitarbeiter der EU-Parlamentarier gern zum Feierabend auf 'ne Mate vorbeikommen und chillen, der kleine Wettbewerbe für Webdesigner ausschreibt, eine Konferenz hier und zwei Lehrstühle dort mitfinanziert, der (wie Facebook auch) Reisen ins „Valley" für Journalisten sponsert und Seminare und komplette Journalismus-Stipendien vergibt. Sprich: Google, Facebook und Co betreiben „Landschaftspflege" wie*

aus dem Lehrbuch der Lobbyarbeit. Was kann es da besseres geben, als mal der Zeit Online *eine Software für ein freundliches, verbindendes Projekt zu finanzieren?*

Abschließend fordert er:

Deshalb, ..., wünsche ich mir: Kehr um vom Weg, den Überwachungskapitalismus voranzutreiben und die Daten Eurer Leserinnen und Leser als Preis für Eure journalistische Arbeit zu verschachern. Gebt Google das Geld … wieder zurück. Sucht hartnäckig weiter nach Möglichkeiten, Journalismus ehrenvoll und in Würde zu betreiben und zu finanzieren. Verlange das auch von Deinen Herausgebern und Verlegern! Das wäre wahre Innovation.

Der Preis wurde exemplarisch an *Zeit Online* verliehen, da ein Großteil vergleichbarer Angebote vergleichbare Tracker enthalten.

Anders als die meisten PreisträgerInnen erschien Jochen Wagner, der Chefredakteur von *Zeit Online*, zur Preisverleihung. Er räumte ein, dass einige der Kritikpunkte auch aus seiner Sicht berechtigt sind, z. B. wird der Facebook-Pixel in die Seiten von *Zeit Online* eingebunden. Es seien aber nicht alle Punkte korrekt. Im Blog *Glashaus* bei Zeit Online nimmt er dazu auch schriftlich Stellung:

[D]as Projekt Deutschland spricht *wurde 2018 und wird 2019 über die genannte Plattform* My Country Talks *organisiert, so wie mittlerweile zahlreiche internationale Projekte. Die Plattform ist eine Eigenentwicklung mit einem aufwändigen Sicherheits- und Datenschutzkonzept. Google-Dienste werden dafür nicht genutzt, bis auf den vorgeschalteten Service reCaptcha, der Spam-Attacken und Bot-Angriffe blockiert. Insbesondere speichert die Plattform nicht „politische Ansichten von Menschen auf Servern in den USA". Alle Daten liegen in Deutschland.*

Aus Sicht von *Zeit Online* wurden die Webseite von *Zeit Online* selbst, die Marketing-Webseite *mycountrytalks.org* und die App von *My country talks* verwechselt. Ob bei der Nutzung immer trennscharf in den einzelnen Bereichen navigiert wird, ist nicht klar. Dass *Zeit Online* den Facebook-Pixel ausliefert, ist zu kritisieren; der Verweis darauf, dass „viele reichweitenstarke journalistische Angebote" dies tun, macht es nicht besser.

Weiter heißt es:

Der ZEIT-Verlag nutzt unternehmensweit die kostenpflichtige Variante G Suite für Unternehmen, bei der die Auftragsdatenverarbeitung und der Datenschutz geregelt sind. Eine Nutzung dieser Daten durch Google ist vertraglich ausgeschlossen,

Ob die üblicherweise sehr komplexen Vertragsbedingungen schlussendlich ausreichend sind, um tatsächlich einen angemessenen Schutz der Daten zu gewährleisten, wäre zu überprüfen.

Als Reaktion nahm padeluun auf der Webseite der BigBrotherAwards Stellung:

Jochen Wegner hat unter großem respektvollem Applaus den BigBrotherAward für Zeit Online persönlich entgegengenommen. Wir haben tatsächlich nur das öffentlich einsehbare Frontend von mycountrytalks.org untersucht (bei dem mittlerweile alle Tracker abgeschaltet sind). Zeit Online beteuert in ihrem Blog Glashaus, dass sie unsere früher schon geäußerte Kritik gehört hatten und die neu programmierte Anwendung, die als Snippets in den Websites der Partnermedien eingebunden wird, extrem datensparsam arbeitet. Seine Erläuterungen klingen plausibel. Wir werden das im weiteren Dialog mit Zeit Online weiter beobachten. Besonders die Einbindung der Snippets auf den trackingverseuchten Websites der Partnermedien dürfte eine Herausforderung sein. Am Wesenskern meiner Laudatio ändert sich nichts.

„*Vielleicht entsteht daraus eine größere Debatte über den Einfluss, den ein so großer Konzern wie Google auf den deutschen Journalismus haben kann*", kommentierte die Moderatorin Golineh Atai abschließend bei der Preisverleihung.

Lob und Tadel

Im Abschnitt *Lob und Tadel* werden Organisationen und Menschen genannt, denen die Jury keinen Preis verliehen hat, die sie aber dennoch für erwähnenswert hält. Tadel gab es für:

- Mood Tracker, die helfen, die eigene Stimmung zu reflektieren und einzuordnen, ob man möglicherweise unter einer Depression leidet. Dazu verarbeiten sie sensibelste Daten über die psychische Gesundheit der NutzerIn. Ein solcher Mood Tracker ist Moodpath, ein anderer Selfapy. Eine Analyse von Moodpath hat aufgedeckt, dass er IP-Adresse, Google-Werbe-ID, den Paketnamen der App und ihre Versionsnummer, die Android-Version, das Gerät, die Displayauflösung und evt. weitere Daten an Facebook übermittelt.

- Berliner Verkehrsbetriebe (BVG) für die fortgesetzte Videoüberwachung ohne Transparenz über die Weiterverarbeitung. Inzwischen wurde bekannt, dass die Kameras auch in der Lage sind, Tonaufnahmen zu erstellen und zu versenden. Dies ist laut BVG deaktiviert – das kann aber nicht überprüft werden.

- „Smart Card" – Edeka in Porta Westfalica, der den EASY-Shopper betreibt, der den Komfort beim Einkaufen erhöhen soll: durch Scannen des Preises, Erstellen einer Einkaufsliste und GPS-gesteuertes Navigieren zum gewünschten Artikel im Einkaufsmarkt. Doch dazu braucht man eine App oder eine Rabattkarte, die mit der Einkaufsliste die Vorlieben beim Einkauf erhebt und speichert.

Lob gab es für die freie Ärzteschaft und Jens Ernst, der in der Telematik-Infrastruktur für den Austausch von Gesundheitsdaten auf eine Fehlkonfiguration aufmerksam gemacht hat, die dazu führte, dass Antivirenprogramme und Firewalls deaktiviert werden und damit Daten von Patientinnen und Patienten ungeschützt im Netz liegen. Dies sei ein fahrlässiger Umgang mit sensiblen Gesundheitsdaten, der erst dadurch öffentlich wurde.

Publikumspreis

Die Publikumswahl wurde erstmals sowohl mit Wahlzetteln im Saal als auch durch eine Online-Abstimmung durchgeführt. Beide Gruppen wählten mit jeweils ca. der Hälfte der abgegebenen Stimmen den Preisträger in der Kategorie *Behörden & Verwaltung*, den **hessischen Innenminister Peter Beuth** zum Gewinner des Publikumspreises.

Anmerkung

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

Rolf Gössner

Kategorie Behörden & Verwaltung – Laudatio

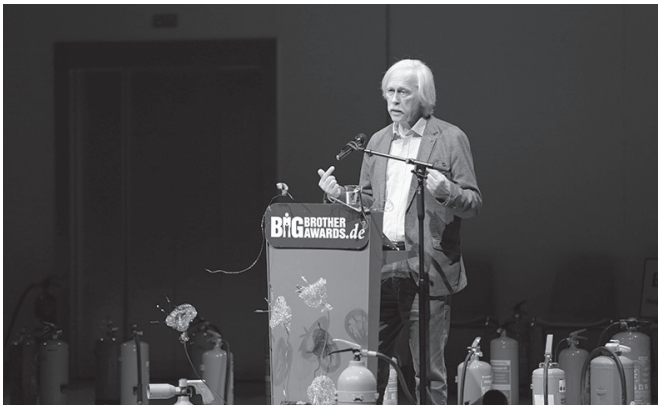
Der BigBrotherAward 2019 in der Kategorie „Behörden & Verwaltung" geht an den hessischen *Innenminister Peter Beuth* (CDU).

Er erhält den Negativpreis

1. für die bundesweit erstmalige Anschaffung einer Analysesoftware der CIA-nahen Firma Palantir,

2. dafür, dass diese umstrittene US-Firma über Einsatz und Betrieb der Software Zugang zum Datennetz der hessischen Polizei erhält, und

3. dafür, dass mit dieser Analysesoftware Massendaten aus polizeieigenen und externen Quellen in Sekundenschnelle automatisiert verknüpft, analysiert und ausgewertet werden können – mit fatalen Auswirkungen auf Grundrechte, Datenschutz und Rechtsstaat.



Laudator Dr. Rolf Gössner – Foto: Jens Reimedes, CC BY-SA 4.0

Ja, wir haben die schwarz-grünen Regierungsfraktionen in Hessen schon letztes Jahr mit einem BigBrotherAward ausgezeichnet, und zwar für ihre damals geplante Verschärfung des Verfassungsschutz- und Polizeigesetzes[1]. Trotz aller Proteste sind diese Gesetze im Juli 2018 verabschiedet worden und seitdem in Kraft. Damit darf die hessische Polizei inzwischen neue Überwachungsmaßnahmen weit im Vorfeld eines Verdachts oder einer möglichen Gefahr ergreifen – etwa Staatstrojaner installieren oder Menschen in elektronische Fußfesseln legen, von denen sie nur annimmt, dass sie künftig Straftaten begehen könnten.

Damit aber nicht genug: Um diese neuen präventiven Aufgaben zu erfüllen und die dabei anfallende Datenflut zu bewältigen, holte sich die Polizei auch noch die umstrittene CIA-nahe Firma Palantir ins Haus. Deshalb kommen wir erstmals in der Geschichte der deutschen BigBrotherAwards nicht darum herum, einen zweiten Straf-Preis in Folge an einen Datenfrevler derselben Regierungskoalition desselben Bundeslandes verleihen zu müssen.

Der hessische Innenminister Peter Beuth ist dafür verantwortlich, dass die US-Firma Palantir beauftragt worden ist, ihre Analysesoftware *Gotham* im IT-System der hessischen Polizei zu installieren und in Betrieb zu setzen. Benannt ist diese Software nach jener fiktiven, von Kriminalität und Korruption verseuchten Stadt, in der Batman Verbrecher jagt und für Recht und Ordnung sorgt. Nachdem die *Gotham*-Software an hessische Polizei-Bedürfnisse angepasst worden ist, heißt sie *Hessen-Data*. Zur Nutzung ermächtigt wird die Polizei mit § 25a des verschärften Hessischen Polizeigesetzes (HSOG), weshalb dieser Paragraf auch spöttisch „Palantir-Ermächtigung"[2] genannt wird. Danach dürfen umfangreiche Datenanalysen durchgeführt werden zur vorbeugenden Bekämpfung von über vierzig Straftaten, die in § 100a Abs. 2 StPO (Telekommunikationsüberwachung) aufgelistet sind, sowie zur Abwehr bestimmter Gefahren.

Was aber ist nun so problematisch und grundrechtsschädigend an dieser Verknüpfungs- und Analysesoftware der US-Firma *Palantir*?

Palantir, benannt nach den *sehenden Steinen* aus *Herr der Ringe*, ist „eine der umstrittensten Firmen des Silicon Valley", so die *Süddeutsche Zeitung*. Sie gilt nach Einschätzung der US-Bürgerrechtsvereinigung ACLU als „Schlüsselfirma in der Überwachungsindustrie"[3]. Der US-„Star-Investor" und Milliardär Peter Thiel, der bereits den Online-Bezahldienst Paypal mitgegründet hatte, gründete die Firma im Jahr 2004 mit finanzieller Unterstützung des US-Geheimdienstes CIA. Die Kundenliste der Firma liest sich wie das Who-is-who der US-Militär- und Sicherheitsbürokratie: CIA, FBI, NSA, Pentagon, Marines und Airforce[4]. Oder anders ausgedrückt: Als Hauslieferant dieser Behörden ist die Firma tief in den militärisch-digitalen Komplex der USA verstrickt und ihr Geschäftsmodell heißt: BigData for BigBrother[5]. Peter Thiel sitzt zudem im Aufsichtsrat von Facebook und hat Donald Trumps Wahlkampf mit über einer Million US-Dollar unterstützt[6].

Die hessische Polizei beauftragte also diese hoch umstrittene Überwachungsfirma damit, ihre Polizeidatenbanken mit Social

Media-Daten und anderen externen Dateien zu verknüpfen und zu analysieren. Es ist dabei keineswegs auszuschließen, dass vertrauliche Polizeidaten aus Hessen in die USA abfließen könnten – zumal bis zu sechs Software-Entwickler der Firma mit eigenen Laptops die Analysesoftware installierten, sie für die hessische Polizei betrieben und Servicezugriff haben. Als US-Firma ist Palantir übrigens auch dem FISA-Act unterworfen, dem berüchtigten *Foreign Intelligence Surveillance Act* (Gesetz zur Überwachung in der Auslandsaufklärung). Und das bedeutet: Alle Informationen über Nicht-US-Bürger und -Bürgerinnen, zu denen Palantir – wie und wo auch immer – Zugang bekommt, müssen im Fall einer Anordnung auch an US-Geheimdienste übermittelt werden[7]. Und es gibt, so sehen es die Oppositionsfraktionen von FDP und *Die Linke* im hessischen Landtag, keine verlässlichen Kontrollmechanismen, um das zu verhindern[8].

Mit der Dateienverknüpfungs- und -auswertungssoftware *Hessen-Data* sollen Bedrohungslagen leichter erkannt und so genannte terroristische Gefährder identifiziert und aufgespürt werden können – also Menschen, die keine Straftaten begangen haben, denen polizeilicherseits aber aufgrund bestimmter Indizien oder Verhaltensweisen solche künftig zugetraut werden. In der modernen Polizeiarbeit geht es längst nicht mehr nur um die Abwehr konkreter Gefahren, sondern um polizeiliche „Aufklärung" weit im Vorfeld mutmaßlicher Gefahren, wie sie mit der letzten Polizeirechtsverschärfung in Hessen legalisiert worden ist. Damit begibt sich die Polizei auf geheimdienstliches Terrain, wo sie prinzipiell nichts zu suchen hat. Und folgt man dem neuen schwarz-grünen Koalitionsvertrag von Dezember 2018, könnte die Analysesoftware künftig auch schon unterhalb der Schwelle der Bekämpfung von islamistischem Terrorismus und Organisierter Kriminalität eingesetzt werden – und damit in weit größerem Ausmaß als ursprünglich vorgesehen[9]. Inzwischen gibt es übrigens auch eine Mobilversion von *Hessen-Data*, um etwa Zielpersonen zu orten und polizeiliche Observateure koordinieren zu können[10].

Hessen-Data ist ein Dammbruch für die polizeiliche IT-Arbeit: Bislang waren die Polizeidaten-Bestände der Strafverfolgung und Gefahrenabwehr nicht miteinander verknüpft, weil personenbezogene Daten aus datenschutzrechtlichen Gründen prinzipiell nur für den Zweck verwendet werden dürfen, für den sie erhoben wurden – also entweder für Strafverfolgung oder für Gefahrenabwehr. Dieser Zweckbindungsgrundsatz wird mit *Hessen-Data* aufgehoben[11]. Mehr noch: Es werden nicht nur unterschiedliche Polizeidatenbanken, sondern auch noch die Verkehrs- und Inhaltsdaten aus Telekommunikationsüberwachungen zusammengeführt und durchforstet sowie Daten aus unterschiedlichen Informationssystemen anderer Behörden wie etwa des Melde- und Ausländerzentralregisters. Doch damit nicht genug: Ein Dammbruch ist auch, dass mit *Hessen-Data* erstmals auch Informationen aus sozialen Medien und Netzwerken wie Facebook, Twitter, Whatsapp, Instagram oder YouTube automatisch abgerufen, zusammengeführt und in Windeseile mit polizeilichen Daten abgeglichen werden können.

Mithilfe dieser rasanten Dateien-Verknüpfung und Daten-Analyse liefert die Palantir-Software der Polizei – grafisch spannend aufbereitet – komplexe Bewegungs- und Kontaktbilder, Beziehungsgeflechte und Personendossiers sowie Anomalien oder Verhaltensmuster von Menschen[12]. Wer kommuniziert oder trifft sich mit wem? Welche persönlichen Kontakte, Verbindungen und Zusammenhänge gibt es zwischen bestimmten Ereignissen, Personen, Gruppen oder Institutionen? Wer verhält sich ungewöhnlich oder verdächtig? Auch bloße Kontakt- und Begleitpersonen, Zeugen, Hinweisgeber oder Geschädigte können dabei ins Visier der Fahnder geraten, auch wenn sie nur in loser oder zufälliger Verbindung mit mutmaßlich Verdächtigen stehen.

Dabei geht es nicht mehr in erster Linie um harte Beweise, sondern um mehr oder weniger zufällige Analyseergebnisse dieser automatisiert zusammen gemixten Datensammlungen. Stellen Sie sich vor, Ihre alltäglichen Aktivitäten, mit denen Sie Unmengen digitaler Spuren hinterlassen, machen Sie plötzlich verdächtig, weil sie aus ihrem ursprünglichen Zusammenhang gerissen und in einen vollkommen anderen, neuen Kontext gestellt werden. Vielleicht kommt Ihnen die hessische Polizei „auf die Spur", nur weil Sie zufällig zur falschen Zeit am falschen Ort waren, eine Wohnung in der Nähe eines Tatortes haben oder einfach mit einer anderen Person verwechselt worden sind. Dieses Analysesystem scheint zwar sehr leistungsfähig zu sein – aber auch recht manipulations- und willküranfällig.

Durch die neuen Überwachungsermächtigungen der hessischen Polizei können solche Analyseergebnisse für die Betroffenen zu besonders gravierenden Konsequenzen führen. Denn wer im Rahmen der Dateienverknüpfung und Datenanalyse als auffällig, als angebliche Risikoperson oder so genannter Gefährder herausgefiltert wird, hat unter Umständen mit dem heimlichen präventiven Einsatz von Staatstrojanern auf seinen Geräten zu rechnen, kann unter Meldeauflagen, Aufenthalts- und Kontaktverbote gestellt, in elektronische Fußfesseln gelegt, in Präventiv- oder Strafhaft genommen werden.

Auf welche Weise die Software *Hessen-Data* ihre Analysen vornimmt, bleibt Geschäftsgeheimnis der Firma Palantir. Damit entziehen sich die Algorithmen hinter den möglichen polizeilichen „Erkenntnissen" der öffentlichen und demokratischen Kontrolle[13].

Bemerkenswert ist im Übrigen, wie die Kooperation der hessischen Polizei mit Palantir eingefädelt worden ist[14]. Ein Untersuchungsausschuss des hessischen Landtags befasste sich im vergangenen Jahr monatelang mit der Frage, ob die Auftragsvergabe an Palantir möglicherweise rechtswidrig erfolgt ist und welche Rolle der Innenminister dabei spielte. Diese Fragen sind bis heute nicht wirklich eindeutig geklärt. Jedenfalls erfolgte die Vergabe auf intransparente Weise; die Leistungsbeschreibung war auf Palantir und ihre Software zugeschnitten, so dass andere mögliche Anbieter keine gleichberechtigte Chance hatten, obwohl es Alternativen gab.

Es macht darüber hinaus misstrauisch, wenn die Öffentlichkeit über den Kaufpreis der Palantir-Software im Dunkeln gelassen wird. Ihr Wert beträgt nach offizieller Mitteilung „0,01 Euro ohne MwSt". Gegenüber *Spiegel-online*[15] räumte das hessische Innenministerium ein, dass dies „nicht der tatsächliche Preis" sei, wollte diesen aber aus „Gründen des öffentlichen Sicherheitsinteresses des Landes Hessen" nicht nennen. Wie kann eine solche Information die öffentliche Sicherheit gefährden – werden etwa Straßenunruhen oder gar Anschläge befürchtet? Hessens Innenminister Beuth nimmt offensichtlich lieber Speku-

lationen in Kauf, als transparent zu arbeiten, wie es in einer Demokratie selbstverständlich sein sollte.

Fazit: Der Einsatz der wohl millionenschweren Palantir-Software bedeutet eine neue Qualität der Datenverarbeitung – die Polizei schwärmt gar von einem „Quantensprung in der polizeilichen Arbeit". Oder anders und klarer ausgedrückt: Mit *Hessen-Data* geht das schwarz-grün regierte Hessen einen weiteren großen Schritt in Richtung Kontroll- und Überwachungsstaat.

Die Analyseplattform *Hessen-Data* steht im Dauerkonflikt mit dem Recht auf informationelle Selbstbestimmung als Ausprägung des Allgemeinen Persönlichkeitsrechts (Artikel 2 Abs. 1 GG). Außerdem wird mit dem Einsatz der Palantir-Software eine wichtige Grundsäule des Datenschutzes buchstäblich niedergerissen: nämlich das Prinzip der Zweckbindung, wonach personenbezogene Daten grundsätzlich nur für den Zweck verwendet werden dürfen, für den sie erhoben worden sind. Und das Ganze auch noch weitgehend ohne wirksame Kontrolle und in einer unheiligen Allianz mit einem Hauptakteur des US-amerikanischen Militär- und Geheimdienstkomplexes. Da können wir nur sagen:

Herzlichen Glückwunsch, Herr Innenminister Peter Beuth, zum BigBrotherAward 2019.

Anmerkungen

1 *https://bigbrotherawards.de/2018/politik-cdu-gruene-landtag-hessen*
2 *https://police-it.org/palantir-in-hessen-vereint-daten-von-facebook-und-co-mit-polizeilichen-datenbanken*
3 *Oliver Voss, Glaskugel der Geheimdienste, in: Tagesspiegel 5.6.2018: https://www.tagesspiegel.de/wirtschaft/start-up-palantir-glaskugel-der-geheimdienste/22636184.html*
4 *https://www.tagesspiegel.de/wirtschaft/start-up-palantir-glaskugel-der-geheimdienste/22636184.html*
5 *Mitarbeiter von Palantir stehen zudem im Verdacht, Kontakte zur Firma Cambridge Analytica unterhalten zu haben, die mit illegal erlangten Facebook-Daten versucht haben soll, die letzte US-Präsidentschaftswahl zu beeinflussen. Das berichteten Spiegel-online und Zeit-online am 6.4.2018: https://www.zeit.de/digital/2018-04/palantir-software-hessen-kriminalitaet-islamismus-cambridge-analytica; https://netzpolitik.org/2018/whistleblower-ueberwachungskonzern-palantir-hat-cambridge-analytica-bei-illegalen-methoden-geholfen/*
6 *https://www.manager-magazin.de/digitales/it/peter-thiel-milliardaer-spendet-fuer-donald-trump-1-25-millionen-dollar-a-1116969.html*
7 *https://de.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act*
8 *Frankfurter Rundschau am 11.1.2019, D4: https://www.fr.de/rhein-main/fdp-org26312/schwarz-gruen-setzt-palantir-11415221.html*
9 *https://www.gruene-hessen.de/partei/files/2018/12/Koalitionsvertrag-CDU-GR%C3%9CNE-2018-Stand-20-12-2018-online.pdf*
10 *Hessen-Data, in: FR 5.4.2019, D2 f.: https://www.fr.de/rhein-main/agenten-thriller-12113844.html*
11 *Tobias Singelnstein, Big Data bei der Polizei: Hessen sucht mit US-Software nach Gefährdern, in: Grundrechte-Report 2019, Frankfurt/M. 2019*
12 *https://www.golem.de/news/palantir-in-deutschland-wo-die-polizei-alles-sieht-1810-137211.html*
13 *Der Technische Direktor der Hessischen Zentrale für Datenverarbeitung (HZD), bei der die Server von Palantir unter Polizeibegleitung aufgestellt wurden und nun betrieben werden, hat im Untersuchungsausschuss erklärt, keinerlei Einblick zu haben, welche Daten und in welchem Umfang Informationen verarbeitet werden und wer Zugriff auf die Daten bekomme. Das liege allein in der Verantwortung von Polizei und Innenministerium; https://www.fr.de/rhein-main/agenten-thriller-12113844.html*
14 *Im Mai 2016 besuchte eine hessische Delegation die US-Firma im Silicon Valley, mit dabei der CDU-Innenminister und BBA-Preisträger Peter Beuth. Ursprünglich hatte man nach einer Software zur Bekämpfung von Cyber-Kriminalität gesucht. Zurück aus dem Silicon Valley waren plötzlich Terrorbekämpfung und Staatsschutz die neuen Zielvorgaben, und Palantir wurde als einziger sinnvoller Software-Anbieter in Betracht gezogen. https://police-it.org/palantir-in-hessen-vereint-daten-von-facebook-und-co-mit-polizeilichen-datenbanken*
15 *http://www.spiegel.de/netzwelt/netzpolitik/palantir-software-polizei-hessen-kauft-bei-umstrittenem-us-unternehmen-a-1201534.html*

Thilo Weichert

Kategorie Biotechnik – Laudatio

Der BigBrotherAward 2019 in der Kategorie Biotechnik geht an die Firma *Ancestry.com* mit ihrer Niederlassung in München,

weil sie das Interesse an Familienforschung dazu ausnutzt, Menschen zur Abgabe von Speichelproben zu veranlassen.

Familienforschung – auch Ahnenforschung oder Genealogie genannt – ist ein relativ harmloses Hobby: Wer bin ich? Wo komme ich her? Mit wem bin ich verwandt? Diese Fragen wurden früher mit Geburts-, Heirats- und Sterbeurkunden, Familienstammbäumen und Kirchenbüchern beantwortet. Die Gentechnik eröffnet nun ganz neue Erkenntnismöglichkeiten, da die Analyse unserer Gene, unserer DNA, verrät, mit wem wir biologisch verwandt sind – bis zum 3. oder 4. Grad. Selbst die sogenannte biogeografische Herkunft unserer Urahnen, also die Frage, in welcher Region meine Familienmitglieder in vergangenen Generationen gelebt haben, lässt sich mit einer gewissen Wahrscheinlichkeit genetisch bestimmen.

DNA ist die englische Abkürzung für Desoxyribonukleinsäure – deoxyribonucleic acid – die wissenschaftliche Bezeichnung für unser Genom, also die Gesamtheit unserer Erbanlagen. Die Erkenntnisse daraus sind verblüffend. Kein Wunder, dass viele Familienforschende ihren Speichel zur Untersuchung einsenden, um mehr über sich herauszubekommen.

Familienforschung als Hobby ist in den USA weit verbreitet. Viele Firmen bieten hierzu ihre Dienste an. Der Marktführer ist *Ancestry.com* mit angeblich derzeit mehr als 10 Millionen Kund-

Innen weltweit und 20 Milliarden weiteren Datensätzen und Urkunden, gefolgt von der Google-Gründung *23andMe* mit 5 Millionen DNA-Analysen[1].

Ancestry hat in München eine Niederlassung eingerichtet und drängte kurz vor Weihnachten 2018 massiv auf den deutschen Markt. Versprochen wird eine „Selbstentdeckungsreise", „Erstaunliches über sich selbst", ein „Schlüssel in die Vergangenheit". Das Ganze für einen Einführungspreis von 79 €, heute 89 € incl. Mehrwertsteuer zuzüglich Versand. Ein Schnäppchen, denn immerhin hat im Jahr 2003 die erste Entschlüsselung des gesamten menschlichen Genoms mit seinen über 3 Milliarden Basenpaaren im Rahmen des Human Genome Projectes noch 3 Milliarden Euro gekostet. 2008 fielen die Kosten pro Genom auf eine Million Euro. 2011 war ein Next Generation Sequencing schon für 10.000 € zu haben. Ein Jahr später konnte erstmals das 1000-Euro-Genom mit der inzwischen verfügbaren Rechenpower und neuen Analysemethoden innerhalb weniger Stunden analysiert werden.

Das Angebot ist nicht nur „billig", sondern auch einfach zu bekommen: Im Internet kann ich ein Ancestry-Konto einrichten und mir damit ein Testkit bestellen. Meine Speichelprobe wird an ein Labor geschickt; 6 bis 8 Wochen später kann ich im Internet über den Account die Ergebnisse abrufen. Toll!

Dass da alles mit guten Dingen zugeht, dafür verbürgten sich angeblich Ende 2018 auf der Internetseite von *ancestry.com* noch viele deutschsprachige „Partner", etwa viele Landesarchive, die Deutsche Nationalbibliothek, das Deutsche Auswandererhaus, die Marineschule Mürwik, das Schweizerische Bundesarchiv oder der niedersächsische Landesverein für Familienkunde. Nur: Von uns auf ihre Partnerschaft angesprochen, hatten diese davon keine Ahnung. Schnell verschwand dann auch diese illegale Werbemethode.

Das Angebot sei, so heißt es auf der Internetseite, datenschutzkonform. (Zitat:) „Sicherheit und Datenschutz genießen bei Ancestry oberste Priorität". Die Kunden blieben (Zitat) „Eigentümer ihrer Daten". Die Daten sowie die Gewebeproben würden auf Anforderung der Betroffenen wieder gelöscht bzw. vernichtet. Eine Weitergabe an Dritte erfolge nicht – außer, soweit (Zitat) „gesetzlich erforderlich" oder „Sie geben uns Ihre ausdrückliche Zustimmung". Also alles paletti?

Der Haken liegt – wie so oft – im Kleingedruckten und ist im Falle von Ancestry in einem dichten Gestrüpp von Bestimmungen verborgen: einer 16-seitigen Datenschutzerklärung[2], elf Seiten Allgemeine Geschäftsbedingungen[3] und siebeneinhalb Seiten Einwilligung in das Forschungsprojekt *Ancestry Human Diversity Project*[4].

Mit dem Einsenden des Speichels erfolgt die Zustimmung zu den Datenschutzbestimmungen, wonach Ancestry selbst mit meinen Daten unbeschränkt über (Zitat) „Merkmale, persönliche Gesundheit und persönliches Wohlbefinden" Forschung durchführen kann. Wird dem *Ancestry Human Diversity Project* zugestimmt, so kommen „mitwirkende Partner" ins Spiel. Die Partner befinden sich (Zitat) „in den Vereinigten Staaten und anderen Ländern". Dabei kann es sich um „akademische Einrichtungen sowie Non-Profit-Organisationen, gewinnorientierte Unternehmen und Regierungsbehörden" handeln.

Wer in dieses *Ancestry Human Diversity Project* einmal seine Einwilligung erteilt, gibt die Kontrolle über seine genetischen Daten aus der Hand und hat keinen Einfluss mehr darauf, wer was und wo damit forscht. Ca. 80 % der Einsendenden geben gemäß Presseberichten bei *23andMe* ihre DNA für „Forschungszwecke" frei und machen weitere Angaben zu sich und ihrer Familie[5]. Bei Ancestry dürfte es ähnlich sein.

Damit nicht genug: Den Kunden als „Eigentümern ihrer Daten" wird von Ancestry jegliche Auskunft verweigert über die sogenannte Forschung, über Methoden, Partner oder Rückschlüsse, die daraus gezogen werden. Was dahinter steckt, wird offenkundig, wenn man sich die junge, aufstrebende Branche der Gendatenkraken genauer ansieht. So schloss der Ancestry-Konkurrent 23andMe, der nur einen halb so großen Datenbestand hat, kürzlich mit dem Pharmakonzern GlaxoSmithKline über 300 Mio. US-Dollar einen Kooperationsvertrag zur Nutzung der Daten. Das Geschäftsmodell dieser Anbieter ist nicht die Ahnenforschung, sondern es geht um das ganz große Geld mit den Gendaten, mit insbesondere der Pharmaindustrie als Abnehmer.

Das Ganze ist also keine Win-Win-Geschichte, bei denen Kunden einfach für eine Dienstleistung bezahlen, die sie bestellt haben. Tatsächlich werden die Betroffenen abgezockt. Die Abzocke erinnert an Google, Facebook und Co. mit Internetdaten. Die Betroffenen erhalten außer spärlichen Auswertungsergebnissen keine Auskunft über die Nutzung ihrer Daten, geschweige denn, dass sie – als vermeintliche „Dateneigentümer" – an den Gewinnen beteiligt würden. Im Gegenteil: Ihnen wird von Ancestry gar verboten, ihre eigenen Analyseergebnisse an Dritte weiterzugeben[6].

Welche weiteren Begehrlichkeiten die Daten der Firma Ancestry wecken, ist 2018 aus den USA bekannt geworden. Menschen, die dort ihre DNA analysieren ließen, gerieten mitsamt ihren Familien ins Visier der Polizei, etwa weil sie mit dem so genannten *Golden-State-Killer* auch nur entfernt verwandt sind. Um den Täter zu ermitteln, wurde die gesamte Verwandtschaft von den Ermittlern ausgeforscht. Kein Wort bei Ancestry über die potenzielle Strafverfolgung von biologischen Verwandten.

Ancestry erteilt deutschen Kunden vor der DNA-Analyse auch keine humangenetische Beratung, obwohl diese verpflichtend im deutschen Gendiagnostikgesetz vorgesehen ist. Die Firma prüft auch nicht, ob eine Person berechtigt ist, die eingesendeten Speichelproben untersuchen zu lassen. So könnte z. B. ein Vater DNA von sich und von seinen Kindern einsenden, um auf diesem Weg de facto einen Vaterschaftstest machen zu lassen. Ancestry klärt ihn weder darüber auf, dass er sich damit nach deutschem Recht strafbar macht, noch dass seine biologischen Verwandten ein „Recht auf Nichtwissen" haben und welche gravierenden familiären Verwerfungen und psychischen Folgen so ein Schritt haben kann, etwa wenn per DNA-Test die Unehelichkeit eines Kindes herauskommt oder ein angeblich anonymer Samenspender plötzlich ans Tageslicht gezerrt wird.

Nichts gegen Genanalysen. Diese können für die Familienforschung, insbesondere aber für die Medizin eine wichtige Erkenntnisquelle sein. Doch sollten die Probengeber sich darüber im Klaren sein, was sie da tun. Anbieter wie Ancestry missbrauchen das Interesse an Familienforschung, um einen Genom-

Schatz für die kommerzielle Forschung anzuhäufen, denn das ist ihr eigentliches Geschäftsmodell. Die Datenschutzrechte der Probengeber und ihrer Verwandten müssen respektiert werden. Die deutschen Datenschutz- und Aufklärungspflichten werden aber von Ancestry aus Profitinteresse bewusst ignoriert. Wir sehen hier einen Trend: Nach der Ausbeutung von Internetdaten wird die Ausbeutung von Gendaten das nächste ganz große Ding. Ancestry ist der Platzhirsch, der keine Datenschutz- oder Grundrechtsskrupel kennt.

Deshalb erhält Ancestry den BigBrotherAward 2019. Herzlichen Glückwunsch.

Anmerkungen

1 *https://www.consumerreports.org/health-privacy/how-to-delete-genetic-data-from-23andme-ancrestry-other-sites/*
2 *https://www.ancestry.de/cs/privacyphilosophy*
3 *https://www.ancestry.de/cs/legal/termsandconditions*
4 *https://www.ancestry.de/dna/lp/informedconsent-v4-de*
5 *http://www.bbc.com/capital/story/20190301-how-screening-companies-are-monetising-your-dna*
6 *Allgemeine Geschäftsbedingungen von Ancestry, https://www.ancestry.de/cs/legal/termsandconditions, Punkt 2*

Rena Tangens

Kategorie Kommunikation – Laudatio

Der BigBrotherAward 2019 in der Kategorie Kommunikation geht an die *Precire Technologies GmbH* in Aachen

für ihre wissenschaftlich zweifelhafte, wahrscheinlich rechtswidrige und gefährliche Sprachanalyse.

Precire – haben Sie noch nie gehört? Das mag sein. Aber es ist möglich, dass Precire schon von Ihnen gehört hat.

Stellen Sie sich einmal vor, Sie hätten sich auf eine neue Stelle beworben. Und – juchhu! – die erste Hürde ist geschafft: Sie haben eine Einladung zum Interview – allerdings per Telefon.

„Bitte beschreiben Sie den Ablauf eines typischen Sonntags."

Nanu, das ist nicht die Frage, die Sie am Anfang eines Job-Interviews erwarten.

„Wie war Ihr letzter Urlaub?"

Die Rückfrage: „Warum interessieren Sie sich dafür?" ist sinnlos. Denn erstens wird dieses Telefon-Interview von einem Computer geführt, zweitens interessiert der sich überhaupt nicht für Sie, und drittens interessiert sich auch die Firma, die hinter diesem Job-Test per Telefon steht, nicht für den Inhalt Ihrer Antworten. Der Computer am Telefon will einfach nur eine Sprechprobe von Ihnen – und dafür muss er Sie dazu bringen, 15 Minuten über irgendwas zu reden.

Laudatorin Rena Tangens – Foto: Jens Reimerdes, CC BY-SA 4.0

„Was macht Ihnen in Ihrem aktuellen oder erlernten Beruf am meisten Freude?"

Hm, der Kontakt mit Menschen?! Scherz. Aber es geht wie gesagt nicht darum, was Sie sagen, sondern wie Sie es sagen. Precire, das ist die Firma, mit deren Telefonstimme Sie da sprechen, behauptet, dass die Stimme jedes Menschen so unverwechselbar sei wie seine DNA. Und Precire behauptet, dass sie aus einer 15-Minuten-Stimmprobe den Charakter eines Menschen erkennen könnten und wie geeignet er oder sie für den Job ist.

Precire zerlegt dafür die aufgenommene Sprachprobe in angeblich über 500.000 Bestandteile und analysiert alles Mögliche: Stimmhöhe, Lautstärke, Modulationsfähigkeit, Sprechtempo und Rhythmus. Dazu die Häufigkeit der Wörter, die Länge der Sätze, die Länge der Pausen, wie verschachtelt die Sätze sind, wie viele Füllwörter und wie oft „man" oder „ich" verwendet werden, wie variabel die Stimme ist und die Akustik. Und der Computer beurteilt auch gleich, ob die Sprache emotional oder wissenschaftlich, zurückhaltend oder direkt ist. Dafür vergleicht Precire die gefundenen Sprachmuster mit denen von Testpersonen aus ihrem Datenpool. Und dann schlägt Precire Ihnen kurzerhand die Psychotest-Ergebnisse von ähnlich klingenden Testpersonen zu – und schließt daraus auf Ihren Charakter.

Als Ergebnis kommen dann Beurteilungen heraus wie die für die freie Journalistin Eva Wolfangel, die Precire im Selbstversuch getestet hat: Sie sei extrem neugierig (8 von 9), glücklicherweise auch sehr verträglich (ebenfalls 8), kontakt- (7) und risikofreudig (6) – doch gleichzeitig attestiert ihr das System einen „distanzierten Kommunikationsstil", sie sei „wenig unterstützend"[1].

Mal so, mal so, einerseits, andererseits. Klingt wie das Wochenhoroskop auf einer Kreuzworträtsel-Seite. Hier eine kleine Kostprobe aus solchen Horoskoptexten:

„Du wünschst dir, dass deine Mitmenschen dich mögen, und dennoch tendierst du zu Selbstkritik." Oder „Manchmal haben Sie ernste Zweifel, ob Sie die richtige Entscheidung getroffen haben." Und besonders schön: „Du bist intelligent und lässt dir nicht so schnell etwas vormachen."

Solche Texte sind trivial und ein bisschen schmeichelhaft, ein bisschen kritisch formuliert. Da ist immer für jeden was dabei, was zutrifft. Viele Menschen fühlen sich davon angesprochen und denken „Da ist was dran!" Wissenschaftlich heißt dieses Phänomen auch „Barnum-Effekt"[2] – nach dem großen Zirkus.

Precire dagegen behauptet, ihr Verfahren sei wissenschaftlich abgesichert[3]. Und winkt mit einer Buchveröffentlichung im wirtschaftswissenschaftlichen *Springer Gabler Verlag*.

Wissenschaftlich?

Doch von seriöser Wissenschaft kann hier keine Rede sein, rügt Dr. Uwe Kanning, Professor für Wirtschaftspsychologie an der Hochschule Osnabrück in seiner Buchrezension[4]. Er argumentiert, es existiere keine unabhängige Forschung zum Thema, der Algorithmus sei eine Blackbox und Geheimnis des Anbieters. Die vorhandenen Studien haben keine eigenen Zahlen erhoben, sondern sind Masterarbeiten, die sich auf die Daten stützen, die Precire ihnen zur Verfügung gestellt hat. Andere Studien werden – auch auf Nachfrage – beharrlich nicht rausgerückt. Das bemängelt auch die freie Journalistin Bärbel Schwertfeger[5].

Wir halten fest: Es gibt keine Belege für den direkten Zusammenhang zwischen Sprachparametern und beruflicher Leistung. Und es gibt keine Belege dafür, dass die so erstellten Prognosen irgendeine Aussagekraft für die zukünftige Leistung der Bewerberinnen und Bewerber haben[6].

Die Sprachanalyse von Precire findet zumeist keine Kausalitäten – sondern nur Korrelationen. Und die können völlig zufällig sein. Da könnte ebenso nach Sternzeichen entschieden werden. Oder nach Schuhgröße. Übersetzt heißt das: Wenn der Computer herausfinden würde, dass in der Vergangenheit die drei erfolgreichsten Mitarbeiter Schuhgröße 44 hatten, dann würde er Ihnen in Zukunft auch nur Menschen mit Schuhgröße 44 als Führungspersonal vorschlagen.

Seit 2015 berichten die Medien immer mal wieder über Precire, mit wenigen Ausnahmen[7] meist mit dem Tenor: „Schau mal an, was für faszinierende Technik es heutzutage gibt!" Manchmal spürt man ein leichtes Gruseln, doch kaum ein Journalist stellt wirklich kritische Fragen und verlangt z. B. Zugang zu den Studien, die die Wissenschaftlichkeit von Precire angeblich belegen, die aber nicht öffentlich sind.

Und niemand spießt mal die zahlreichen Widersprüche auf: So sagt Precire, dass Psychotests nicht aussagekräftig seien, weil die Probanden ja ahnten, welche Antworten erwünscht seien. Und dann verwendet Precire selbst als Grundlage einen Datenpool mit Sprachproben von tausenden von Probanden – deren Charakter mittels Psychotest ermittelt wurde. Anders gesagt: Ihr Algorithmus versucht die Ergebnisse von Psychotests nachzubilden. Und niemand fragt nach, warum einerseits von einer „unveränderlichen Sprach-DNA" die Rede ist, Precire aber andererseits selbst eine App zum Trainieren der Sprache anbietet[8]. Personalentwicklung durch Sprachtraining ist nämlich der zweite Geschäftsbereich von Precire. Die vorgebliche „DNA" scheint also doch nicht so unveränderlich zu sein …

Die Teilnahme an so einer Sprachanalyse ist freiwillig – Bewerberinnen und Bewerber können nicht zum Telefoninterview mit dem Computer gezwungen werden. Das gilt auch mit der seit 2018 geltenden europäischen Datenschutzgrundverordnung (DSGVO), hier konkret Artikel 7 Absatz 4 (Freiwilligkeit bei der Einwilligung). Doch hey – wie weit ist es her mit der Freiwilligkeit, wenn jemand einen Job unbedingt haben will?

Und wer setzt Precire nun ein? Angeblich mehr als 100 Firmen in Deutschland. Einige sind bekannt: der Personaldienstleister und Zeitarbeitsvermittler Randstad, der Versicherungskonzern HDI und auch die Gothaer Versicherung, der Transport-Riese Fraport, das Handelsblatt, die Unternehmensberatung KPMG, der Stromversorger RWE, die Krankenkasse DAK, die Hotelgruppe Accor, IBM und Mobilfunkanbieter Vodafone.

Warum um Himmelswillen machen Firmen so etwas?

Weil es modern ist, und weil sie glauben, dass es sie entlastet. Einerseits von der Vorauswahl, andererseits von der Entscheidung. Der Computer ist schnell, da gibt es Zahlen. Und Zahlen sind Fakten, und der Computer ist objektiv. Oder etwa nicht?

Objektiv?

Thomas Belker, bisher Personalvorstand des Talanx-Versicherungskonzerns – Talanx ist Kunde von Precire –, ist von der Effizienz überzeugt. So überzeugt, dass er zum 1. Mai 2019 zu Precire gewechselt ist als neuer Geschäftsführer. Er meint, das Programm spare nicht nur Zeit und Geld – es sei auch objektiver und deswegen fairer. Zitat: „Die Maschine kennt unbewusste Vorurteile, die jeder Mensch hat, nicht. Ihr ist es egal, ob jemand Mann oder Frau ist oder welche Hautfarbe er hat."[9]

Dirk Gratzel, Mitgründer von Precire, behauptet: „Eine Maschine ist weniger fehleranfällig als ein Recruiter. Eine Maschine kann nur objektiv."[10]

Das ist eine äußerst naive Sicht der Dinge. Computer „verstehen" uns nicht. Das dürfen wir aber nicht mit Neutralität verwechseln. Computerprogramme sind auch voreingenommen, denn sie werden von Menschen programmiert. Menschen, die ihre eigenen Wertvorstellungen für selbstverständlich halten und in die Software mit einfließen lassen. Menschen mit bestimmten Fragestellungen, Zielen und Motiven. Und vor allem wird die Software mit einer ausgewählten Personengruppe als Referenz trainiert, die dann bestimmt, was als „normal", gut oder schlecht gilt.

Precire bietet auch einen Service für die Analyse von geeigneten Führungspersonen. Die Theorie: Wer ähnlich klingt wie ein DAX-Manager, könnte als Chef geeignet sein. Als Grundlage dafür wurden Stimmproben von Managern von 30 DAX-Un-

ternehmen ausgewertet. Die haben den Zirkus mit dem Telefoninterview natürlich nicht mitgemacht. Stattdessen hat Precire kurzerhand Reden der Vorstandsmitglieder aus Youtube als Material verwendet. Nicht nur methodisch zweifelhaft. Uwe Kannings, Professor für Wirtschaftspsychologie an der Hochschule Osnabrück, schreibt in einem launigen Kommentar: „Die Stärke dieser Studie liegt in ihrem Unterhaltungswert."[11]

Wissenschaftlichkeit hin oder her: Schlimm sind die Folgen, wenn das Verfahren nun tatsächlich zur Auswahl von Führungspersonen eingesetzt wird. Wie im Precire-Werbe-Video zu sehen: „Sie suchen jemanden, der zu Ihrem Team passt" – im Bild zu sehen: Mann mit grauem Anzug und roter Krawatte, der – na was wohl – einen anderen Mann in grauem Anzug und roter Krawatte als neuen Mitarbeiter begrüßt[12].

Laut einer Untersuchung von 2019 gibt es in Deutschland mehr Chefs, die Michael heißen als Frauen (egal welchen Namens). Dasselbe gilt übrigens auch für Thomas, Andreas, Peter und Christian[13].

Mehr Diversität in Firmenvorständen? Wird so ganz sicher nicht erreicht. Denn solche Auswahlverfahren nach Ähnlichkeit führen dazu, immer weiter „mehr desselben" einzustellen. Nur jetzt verbrämt mit dem Mäntelchen der künstlichen Intelligenz.

Bei Menschen ist klar, dass der „human factor" eine Rolle spielt. Die Voreingenommenheit per Algorithmus ist gefährlicher. Denn sie wird nicht erkannt, solange wir das Märchen vom „objektiven Computer" glauben.

Precire reitet auf dem Trend, Sprachanalyse zur Ausforschung und Klassifizierung von Menschen zu verwenden und der „Künstlichen Intelligenz" magische Urteilskräfte zuzuschreiben. Unbewusster Nebeneffekt: Vorurteile werden durch Reinigung in der Algorithmen-Waschmaschine ganz unauffällig wieder salonfähig gemacht. „Hat der Computer so ausgewählt. Wir wissen nicht, warum."

Aber nicht alle Firmenchefs können sich mit der Personalauswahl per Computer anfreunden. Sebastian Saxe, IT-Vorstand der Hamburg Port Authority (das ist die Zentralverwaltung der Hamburger Hafenbehörden), sagt: „Ich bin ein Freund der Digitalisierung. Aber wenn wir unter den Bewerberinnen und Bewerbern eine Vorauswahl mit Software treffen würden, würden wir Leute mit Ecken und Kanten, die letztlich gut zu uns passen, nie zu Gesicht bekommen."[14]

Danke für diese klaren Worte.

Callcenter

Vielleicht dachten Sie bis hierher „Diese Technik ist fies – aber ich bin ja nicht auf Job-Suche, also betrifft mich das nicht". Falsch gedacht, denn nun kommen wir zum dritten Geschäftsbereich von Precire: Der Einsatz der Sprachanalyse im Callcenter.

Wie funktioniert das? Offenbar zeichnen Callcenter die Sprache von Anrufern auf, leiten sie an einen Server von Precire weiter und lassen sie dort in Echtzeit analysieren. Und Precire schlägt dann dem Callcenter-Agenten vor, wie er oder sie weiter vorgehen soll. Das ist, als ob die ganze Zeit ein Psychologe im Ohr des Callcenter-Agenten sitzt, mithört und ihm live einflüstert, was er als nächstes sagen oder anbieten soll. Die Software soll zum Beispiel erkennen: Ist die Kundin so sauer, dass sie kündigen will, oder will sie nur einen Rabatt rausschlagen? Precire preist an:

> *„Beschwerden sind unbewusste, emotionale Sprache pur, eine einmalige Datenquelle und hervorragende Chance, Ihre Kundenbindung dauerhaft zu vertiefen."*
>
> *„Durch eine direkte IT-Anbindung analysiert Precire eingehende Beschwerden, erkennt psychologische Muster (…) und liefert Hinweise und Auffälligkeiten an die Entscheider."*
>
> *„Dabei lernt unser System – im Fall der next-best-action-Empfehlung – selbst mit jedem Nutzer dazu (‚Künstliche Intelligenz') und hilft Ihnen, die vorhanden Sprachdaten Ihrer Kunden in einen echten Mehrwert zu wandeln."*[15]

Auch hier klingt der Marketingsprech von Precire übertrieben. Doch anders als bei der Vorhersage, ob jemand für einen Job geeignet ist, ist es durchaus möglich, dass die Sprechanalyse etwas über die Anrufenden herausfinden kann, z. B. die Herkunft über den Dialekt, Emotionen, Unsicherheit, Stress.

Seit 2014 schon bewirbt Precire seine Dienste im Callcenter-Bereich. Die Firma ist passenderweise 2016 Mitglied im Callcenter-Verband und auch beim Deutschen Dialogmarketing-Verband[16] geworden. Sie hält sich aber merkwürdig bedeckt, konkret Auskunft über Callcenter in Deutschland zu geben, die die Sprachanalyse der Anrufenden schon im Einsatz haben. Was da alles denkbar ist, beantwortet ein Zitat von Precire-Gründer Dirk Gratzel: „Wir können alles beantworten, was von unseren Kunden gewünscht wird." Zum Beispiel:

> *„Was verrät die Sprache eines Kunden über ihn?", „Ist dieser Krankenversicherte depressiv?", „Lügt dieser Versicherte, wenn er eine Schadensmeldung absetzt?"*[17]

Dieser Einsatz von Sprachanalyse im Callcenter ist nicht nur unethisch – er ist illegal: Er verstößt gegen das Telekommunikationsgeheimnis und verletzt die Vertraulichkeit des gesprochenen Wortes (§ 201 StGB). Das ist strafrechtlich besonders sanktionierbar.

Es wird Zeit, dass sich jemand aufrafft, ein Verfahren einzuleiten. Die Landesdatenschutzbeauftragte von NRW zum Beispiel. Und die jeweils zuständigen Aufsichtsbehörden sollten auch die Precire-Konkurrenz, nämlich die Startups *100 Worte* aus Heilbronn und *Audeering* aus München mal unter die Lupe nehmen.

Emotions- und Motivationserkennung per Sprachanalyse ist gefährlich, denn sie kann ohne unser Wissen irgendwo im Hintergrund passieren, wann immer wir sprechen. Diese Art der Sprachanalyse ist geradezu darauf angelegt, uns zu übervorteilen. So werden die einzelnen Menschen immer ohnmächtiger und unangreifbare Macht wandert immer mehr zu großen Konzernen, Versicherungen, Banken und staatlichen Stellen, die Zugriff auf unsere Daten und solche Technologie haben.

Deshalb fordern wir den Gesetzgeber auf: Die Anwendung von Sprachanalyse und „Künstlicher Intelligenz“ zur Charakter-, Emotions- und Motivationserkennung muss verboten werden!

Wenn Sie, liebes Publikum, das nächste Mal bei einem Callcenter anrufen und Sie bekommen die Ansage, dass „Teile des Gesprächs zur Qualitätsverbesserung aufgezeichnet werden“, dann sagen Sie ganz deutlich am Anfang des Gesprächs „Nein!“ und „Ich will nicht, dass Sie dieses Gespräch aufzeichnen!“.

Lernen Sie, „Nein“ zu sagen. Mit freundlicher, aber klarer Stimme.

Wir sagen „Nein“ zu Precire,

Herzlichen Glückwunsch zum BigBrotherAward 2019!

Anmerkungen

1 *Quelle: Riffreporter, Eva Wolfangel: „Google, wird meine Ehe halten?“ https://www.riffreporter.de/vr-reporterin/kuenstliche-intelligenz-psychologie/*

2 *Barnum-Effekt / Forer-Effekt. https://de.wikipedia.org/wiki/Barnum-Effekt*

3 *Precire Webseite: „Die wissenschaftliche Fundierung von Precire ist das Kernstück der Technologie: Zahlreiche Validierungsstudien (intern, extern) sichern das Verfahren ab.“ Zitiert nach Wirtschaftspsychologie aktuell, 6. November 2017: Ärger des Monats – Algorithmische Verirrungen https://www.wirtschaftspsychologie-aktuell.de/aerger/aerger-20171106-baerbel-schwertfeger-algorithmische-verirrungen.html*

4 *Uwe P. Kanning: Sprachanalyse: eine neue Methode der Personalauswahl? https://www.haufe.de/personal/hr-management/sprachanalyse-eine-neue-methode-der-personalauswahl_80_453994.html*

5 *Personalmagazin, 12/2015. Von Bärbel Schwertfeger: Personalauswahl per Sprachtest. https://www.mba-journal.de/wp-content/uploads/2016/01/Sprachtest.pdf. Kommentar von Bärbel Schwertfeger unter https://blog.recrutainment.de/2016/05/11/persoenlichkeitsprofil-aus-der-analyse-von-sprache-einfach-nur-creepy-oder-die-technologie-von-morgen-interview-mit-mario-reis-von-psyware-und-britta-nollmann-von-randstad/: „Hallo, als Autorin des Artikels im Personalmagazin habe ich mich ausführlich mit Precire beschäftigt und war doch mehrmals sprachlos, wie man versucht hat, mich ‚zu überzeugen‘ und partout keine relevanten Daten herausrückte (Ein Wissenschaftler, der sich dafür interessierte, sollte sogar einen Knebelvertrag unterschreiben) – einschließlich einer wohl als Einschüchterung gedachten anwaltlichen Abmahnung VOR Erscheinen des Artikels (danach kam nichts). Zumindest ein seltsames Geschäftsgebaren! Aber immerhin ernte ich mit meinem Testergebnis schöne Lacherfolge bei Menschen, die mich gut kennen. Bärbel Schwertfeger“*

6 *Wirtschaftspsychologie-aktuell.de: https://www.wirtschaftspsychologie-aktuell.de/fachbuch/20180425-klaus-stulle-psychologische-diagnostik-durch-sprachanalyse.html*

7 *Ausnahmen z. B. Bärbel Schwertfeger im Personalmagazin, 12/2015: Personalauswahl per Sprachtest. https://www.mba-journal.de/wp-content/uploads/2016/01/Sprachtest.pdf, Eva Wolfangel bei den Riffreportern: Google, wird meine Ehe halten? https://www.riffreporter.de/vr-reporterin/kuenstliche-intelligenz-psychologie/*

8 *Precire-Coach auf dem Handy – „Wie wir sprechen, zählt: Als Coaching-App hilft Precire, die eigene Sprache zu analysieren und das Ausdrucksvermögen zu trainieren.“ https://precire.com/people/#1543827472589-3-0*

9 *Quelle: Frankfurter Rundschau, 26.05.18 Künstliche Intelligenz – Vorstand von Computers Gnaden. Von Annika Leister. https://www.fr.de/wirtschaft/vorstand-computers-gnaden-10974824.html*

10 *Quelle: Spiegel Nr. 3, 12.1.2019. Von Martin U. Müller: Plaudernd zum Job*

11 *Quelle: Wirtschaftspsychologie-aktuell.de, 25. April 2018: Fachbuch im Fokus. Von Prof. Dr. Uwe Peter Kanning. Buchrezension zu Klaus P. Stulle (Hrsg.): Psychologische Diagnostik durch Sprachanalyse. Validierung der Precire-Technologie für die Personalarbeit. Wiesbaden: SpringerGabler 2018 https://www.wirtschaftspsychologie-aktuell.de/fachbuch/20180425-klaus-stulle-psychologische-diagnostik-durch-sprachanalyse.html*

12 *Werbevideo von Precire: https://www.youtube.com/watch?v=VCZzfTJRf-c*

13 *Quelle: Manager Magazin, 6.3.2015 Analyse zur Frauenquote Weniger Frauen in Vorständen als Männer, die Thomas heißen. Von Christoph Rottwilm. https://www.manager-magazin.de/politik/artikel/weniger-frauen-in-mdax-vorstaenden-als-maenner-namens-thomas-a-1022017.html*
Gründerszene: Michaels, Thomasse und Andreasse dominieren die Gründerszene https://www.gruenderszene.de/perspektive/vornamen-ranking-handelsregister

14 *Quelle: Computerwoche, 16.06.2016: Personalauswahl 4.0 – Wenn Software in die Seele des Bewerbers schaut. Von Michael Schweizer. https://www.computerwoche.de/a/wenn-software-in-die-seele-des-bewerbers-schaut,3312154*

15 *Diese Zitate stammen übrigens von der alten Website von Precire und sind heute nur noch über das Zeitreise-Tool Wayback Machine bei archive.org zu finden. Damals hieß Precire noch „Psyware“ und schrieb mehr Klartext. 2016 hat die Firma sich umbenannt – die Ähnlichkeit von „Psyware“ (Psycho-Software) und „Spyware“ (Spionage-Software) war ihnen vielleicht doch zu heiß … https://web.archive.org/web/20141011204314/ http://www.psyware.de/de/precire-choice*

16 *News auf Precire Website vom 22.7.2016: Mitgliedschaften beim Callcenter Verband und beim Deutschen Dialogmarketing Verband. https://precire.com/de/2016/07/22/mitgliedschaften-beim-call-center-verband-deutschland-und-beim-deutschen-dialogmarketing-verband/ (nicht mehr aufrufbar, aber auf dieser archive.org-Seite ist die News sichtbar: https://web.archive.org/web/20160729215351/https://precire.com/de/start/)*

17 *Quelle: FAZ, 20.5.2015: Persönlichkeitsanalyse – Deine Sprache verrät dich. Von Katrin Hummel https://www.faz.net/aktuell/gesellschaft/menschen/software-erkennt-persoenlichkeit-mit-sprachanalyse-13596216.html?printPagedArticle=true#pageIndex_0*

Ein dekorativer Whistleblower, gestaltet von Angelika Höger – Foto: Jens Reimerdes, CC BY SA 4.0

NETZPOLITIK.ORG

Lorenz Hilty

Bits & Bäume: Funktionierende Systeme werden systematisch zu Abfall gemacht

Jedes Jahr ein neues Gerät mit mehr Rechenleistung. Die Regel haben viele von uns verinnerlicht und wir produzieren dadurch Berge von Schrott. Doch Hardware und Software sind eigentlich sehr nachhaltige Produkte. Sie sollten so eingesetzt werden, dass wir den Material- und Ressourcenverbrauch endlich senken, schreibt der Informatiker Lorenz Hilty.

Foto: Curtis Palmer, CC-BY 2.0

Schon vor 20 Jahren hoffte man, dank digitaler Technologien weniger Material und Energie für die Befriedigung von Konsumbedürfnissen aufwenden zu müssen. Eine relative Dematerialisierung von Produktion und Konsum sollte das zentrale Dilemma der nachhaltigen Entwicklung lösen: die Bedürfnisse von immer mehr Menschen zu befriedigen und gleichzeitig die Natur zu entlasten. Diese mit der Digitalisierung verbundene Chance ist theoretisch noch intakt – praktisch sind bis heute jedoch kaum Fortschritte zu verzeichnen. Der Beitrag diskutiert mögliche Ursachen und Zukunftsperspektiven.

Videokonferenzen und Flugverkehr

In einer Umfrage unter Mitarbeitenden schwedischer Unternehmen gaben 45 Prozent der Befragten an, sie hätten schon einmal an virtuellen Meetings teilgenommen und dadurch Dienstreisen vermieden. Ein Unternehmen hatte sogar mehr als ein Drittel aller Flugreisen durch Videoconferencing ersetzt. Ich zitiere diese Untersuchung von Peter Arnfalk deshalb, weil sie die Situation im Jahr 1999 widerspiegelt.

Als Arnfalk die Ergebnisse auf der EnviroInfo-Konferenz in Wien vorstellte, interpretierte er sie durchaus vorsichtig. Er extrapolierte die Zahlen nicht einfach in die Zukunft, so als würden bald alle Firmen diesem Beispiel folgen. Er sprach auch von Hürden für Videoconferencing und davon, dass sich Menschen in vielen Fällen persönlich treffen wollen. Dennoch hoffte er, dass man zumindest einen Teil des Flugverkehrs durch virtuelle Meetings würde ersetzen können[1].

Seither ist das Gegenteil dessen geschehen, was man mit vorsichtigem Optimismus erwartet hätte: Der weltweite Flugverkehr hat sich mehr als verdoppelt. Genau genommen hat die Zahl der beförderten Passagiere zwischen 1999 und 2017 um einen Faktor 2,55 zugenommen[2], was einer durchschnittlichen jährlichen Wachstumsrate von 5,3 Prozent entspricht. Auch wenn etwas mehr als die Hälfte des Zuwachses auf den Freizeit-

verkehr zurückgeht und die Geschäftsflüge aufgrund der globalen Finanzkrise 2008 und 2009 vorübergehend eingebrochen sind, haben diese insgesamt ebenfalls deutlich zugenommen. Die Ausgaben für Geschäftsreisen stiegen im globalen Durchschnitt allein im Jahr 2017 um 5,8 Prozent[3].

Halten wir also fest: Die Möglichkeiten der digitalen Kommunikation haben nicht bewirkt, dass der Flugverkehr zurückgegangen wäre, er hat sogar massiv zugenommen. Man könnte einwenden, dass auch virtuelle Meetings Energie verbrauchen und damit Emissionen verursachen. Hierzu ein Beispiel: Ein Flug von Zürich nach New York und zurück verursacht rund 2,5 Tonnen Emissionen pro Passagier, ausgedrückt in CO_2-Äquivalenten. Die Emissionen durch virtuelle Meetings betragen für Full-HD-Videoconferencing via Internet heute 160 bis 290 Gramm CO_2-Äquivalente pro Stunde – man könnte also rund 1000 Arbeitstage in perfekter Qualität virtuell konferieren, bis sich ein Flug nach New York stattdessen lohnen würde[4].

Ob die Digitalisierung in Zukunft zu einem Rückgang des Flugverkehrs führt, hängt vom Verhalten jedes/jeder Einzelnen ab. Die Industrie jedenfalls plant mit anderen Zahlen: Die Internationale Luftverkehrsvereinigung geht von einer erneuten Verdoppelung des globalen Flugverkehrs bis 2037 aus. Ironischerweise hilft die Digitalisierung bei diesem Wachstum durch die Perfektionierung des Wettbewerbs – das Internet war und ist ein Katalysator für den Preiskampf im Billigflugsektor[5].

Lebensdauer von Gebrauchsgütern

Die Arbeitsgruppe *Nachhaltige Informationsgesellschaft* der Gesellschaft für Informatik knüpfte im Jahr 2004 große Hoffnungen an die Digitalisierung. Anstelle von „Digitalisierung" sprach man damals von der Ausbreitung von Informations- und Kommunikationstechnologien (IKT, im Zitat *ICT*):

> *Der Einsatz von ICT kann die Lebensdauer von Produkten verlängern, zum Beispiel durch elektronische Tauschbörsen oder durch ein effizienteres Management von Reparaturen. So ermöglicht ICT eine jahrzehntelange Bereitstellung von Ersatzteilen auch in kleinen Stückzahlen, indem (z.B. dank Internet) die technischen Daten der Ersatzteile und deren Fertigungsdaten verfügbar bleiben sowie eine globale Lagerhaltung organisiert werden kann. Über allgemein zugängliche Datenbanken könnte jederzeit Information über die Verfügbarkeit von Ersatzteilen oder die Möglichkeit einer Reparatur abgerufen werden[6].*

Dies ist teilweise eingetreten – dennoch dominiert im Gesamttrend die Zunahme der Material- und Energieflüsse durch kurzlebige Produkte. Die Dauerhaftigkeit von Gebrauchsgütern wird teilweise sogar durch Digitalisierung untergraben: Bei Produkten, die von Software gesteuert sind, bieten sich für den Hersteller vielfältige Möglichkeiten für Obsoleszenzstrategien, die auch genutzt werden. Die explizit geplante Obsoleszenz, die sich im Programmcode nachweisen ließe, ist aber nur ein Spezialfall. Wahrscheinlich trägt der generelle Mechanismus von Software-Updates, die immer neue Anforderungen an die Hardware stellen, mehr zur Entwertung von Material bei als die explizit geplante Obsoleszenz.

Ich spreche deshalb allgemeiner von *Obsoleszenz durch Software*. Obsoleszenz durch Software scheint zunächst nur IKT-Geräte zu betreffen, kann aber auf alle von Software abhängigen Güter übergreifen. Vor diesem Hintergrund muss die Vision eines *Internet der Dinge* bedenklich stimmen, weil damit eine wachsende Zahl von Gebrauchsgütern faktisch zu Peripheriegeräten eingebetteter Prozessoren wird. Schon heute kommt es vor, dass materialintensive Peripheriegeräte wie Drucker, Scanner oder Monitore obsolet werden, weil die neue Betriebssystemversion sie „nicht mehr unterstützt".

Nach der Vision des Internets der Dinge werden nun potenziell alle Alltagsgegenstände, also nicht nur IKT-Geräte, von Software-Updates abhängig. Damit besteht die Gefahr, dass das Prinzip der Entwertung von Material durch Software in immer mehr Lebensbereiche übergreift. Was mache ich, wenn mein Herd, mein Toaster, meine Waschmaschine, mein Rollladen oder das Kinderspielzeug vom Softwareanbieter „nicht mehr unterstützt" wird?

Das Grundprinzip der Digitalisierung ist Dematerialisierung – nur stellen wir es auf den Kopf

Software ist eigentlich das perfekt nachhaltige Produkt. Ein Softwareprodukt ist auf die gleiche Weise immateriell wie ein Roman oder eine Partitur. Diese können allenfalls aus der Mode kommen, aber sie unterliegen keiner Abnutzung. Sie ändern sich nicht dadurch, dass sie gelesen, beziehungsweise gespielt werden.

Hardware nutzt sich ferner nicht dadurch ab, dass sie Software ausführt. So gesehen ist Hardware erstaunlich haltbar. Eher sind äußere Beschädigungen für die Alterung von Hardware verantwortlich als die eigentliche Arbeit, welche die Prozessoren, Speicherchips und weiteren Elektronikbauteile verrichten. Falls die Hardware nicht die Funktion erfüllt, nach der man gerade verlangt, besorgt man sich neue Software, die man auf der gleichen Hardware ausführt. Die Universalität der Hardware ist der ursprüngliche und eigentliche Sinn der Trennung von Hardware und Software[7].

Um den Energieverbrauch muss man sich normalerweise auch nicht sorgen, denn ein handelsüblicher Prozessor benötigt heute nur eine Kilowattstunde Energie, um unvorstellbare 10 Billiarden Rechenoperationen auszuführen. Die ersten Computer hatten diese Energie schon nach wenigen Tausend Operationen verbraucht. Und die Energieeffizienz der digitalen Technologie steigt weiter[8].

Bis zu diesem Punkt klingt das alles sehr material- und energieeffizient. Nun hat es sich aber seit den 1980er Jahren bei Softwareherstellern eingebürgert, dass sie durch die sogenannte Softwareevolution den Fortschritt an Rechenleistung, Speicherdichte und Energieeffizienz im Hardwarebereich vollständig „aufsaugen"[9].

Das Ergebnis ist, dass funktionierende Geräte systematisch zu Abfall werden, was weltweit zu einem steigenden Aufkommen von Elektronikschrott führt. Dies ist unter Nachhaltigkeitsaspekten besonders bedenklich, denn die heutige Hardware enthält

50 bis 60 Metalle, die zum Teil unter hohen Belastungen für Mensch und Umwelt gewonnen werden. Die Geringschätzung dieser materiellen Ressourcen durch ihren viel zu kurzen Einsatz in Geräten ist beispiellos.

Recycling löst dieses Problem leider nicht. Selbst unter optimalen industriellen Bedingungen werden im Recycling des besagten Elektronikschrotts maximal 17 Metalle zurückgewonnen, alle anderen verteilen sich so fein, dass es praktisch unmöglich ist, sie jemals wiederzugewinnen. Wir entziehen diese Metallmengen damit der Nutzung durch zukünftige Generationen. Hinzu kommt, dass zwischen den entstehenden und recycelten Mengen von Elektronikabfall ohnehin eine Lücke klafft, die in den meisten EU-Ländern weit über 50 Prozent liegt[10] und in der übrigen Welt noch größer sein dürfte.

Für eine nachhaltige Digitalisierung wäre es notwendig, das Prinzip zu rehabilitieren, dass Hardwarekomponenten bis zum Ende ihrer technischen Lebensdauer betrieben werden und der größte Teil der Wertschöpfung im immateriellen Bereich, also in der Software, stattfindet.

Materielle Selbstbestimmung: Die Rechte der NutzerInnen stärken

Weder im Fall des Flugverkehrs noch im Fall der Lebensdauer von Gebrauchsgütern hat sich bisher die Hoffnung erfüllt, dass dank Digitalisierung die Material- und Energieintensität unserer Aktivitäten zurückgehen würde. Im digitalen Zeitalter ist es vielmehr selbstverständlich geworden, dass Anbieter das Prinzip der immateriellen Wertschöpfung durch Software in sein Gegenteil verkehren, indem sie materiellen Konsum durch Software stimulieren oder gar erzwingen.

Aus diesen und auch aus ethischen Gründen wird es unter anderem notwendig sein, die Rechte der NutzerInnen zu stärken, um der Entwicklung entgegenzutreten, dass ihr Eigentum zunehmend unter externe Kontrolle durch Softwareanbieter gerät. Das Recht auf informationelle Selbstbestimmung wurde vom deutschen Bundesverfassungsgericht einst aus dem allgemeinen Persönlichkeitsrecht heraus entwickelt, um dem/der Einzelnen eine rechtliche Handhabe zu geben, über die Verwendung seiner oder ihrer persönlichen Daten zu bestimmen.

Es stellt sich heute die Frage, ob angesichts der zunehmenden Fremdbestimmung unserer Gebrauchsgüter und Infrastrukturen nicht analog aus dem Eigentumsrecht ein Recht auf materielle Selbstbestimmung abzuleiten wäre, das dem/der EigentümerIn eines (softwaregesteuerten) materiellen Gutes bessere Möglichkeiten gibt, sich gegen die Untergrabung seiner/ihrer Verfügungsgewalt über dieses Gut zu schützen.

Ein denkbarer erster Ansatz hierfür wäre das in den USA für Autos geltende und für Elektronikprodukte derzeit geforderte ‚Right to Repair'[11]. Ein Recht auf Reparatur würde sich bei Produkten mit Softwareanteil auch auf die Software beziehen müssen, die folglich offengelegt werden müsste. Allein das könnte bestimmte Formen von softwarebedingter Obsoleszenz verhindern.

Unabhängig davon wird sich die Gesellschaft aber zur einfachen Tatsache verhalten müssen, dass durch Digitalisierung mit immer weniger Arbeit mehr Güter und Dienstleistungen hergestellt werden können, also die Arbeitsproduktivität weiter zunimmt. In naher Zukunft wird die derzeitige Welle der künstlichen Intelligenz (KI) den Arbeitsmarkt erfassen. Zwar haben sich die Konzepte und Methoden der KI in den vergangenen Jahrzehnten nur wenig verändert. Was sie aber heute zumindest vordergründig erfolgreich macht, ist die Verfügbarkeit billiger Hardwareleistung und zugleich riesiger Datenmengen aus dem Internet, mit denen man Lernalgorithmen versorgen kann.

Viele Arbeitsplätze, auch im Dienstleistungssektor, werden durch Automatisierung wegfallen, weil man – zu Recht oder zu Unrecht – annehmen wird, KI-Systeme würden die Tätigkeiten besser und billiger verrichten. Eine nachhaltige Wirtschaftsweise wird aber nicht realisierbar sein, solange wir die grundlegenden Mechanismen nicht infrage stellen, die uns zu Wachstum zwingen.

Einer dieser Mechanismen ist darin zu finden, dass der technische Fortschritt hauptsächlich für die Steigerung der Arbeitsproduktivität, aber kaum für die Steigerung der Ressourcenproduktivität, genutzt wird. Wenn sich diese Entwicklung fortsetzt, werden wir die Prinzipien überdenken müssen, nach denen unsere Gesellschaft heute Arbeit organisiert und Einkommen verteilt.

Ohne grundlegende Veränderungen werden wir aus dem Teufelskreis von Produktivismus und Konsumismus nicht ausbrechen können: Je mehr die Arbeitsproduktivität steigt, desto mehr müssen wir konsumieren, um ausreichend arbeiten zu können.

Quelle: https://netzpolitik.org/2019/bits-baeume-funktionierende-systeme-werden-systematisch-zu-abfall-gemacht/

Die Konferenz Bits & Bäume brachte im Jahr 2018 erstmals im großen Stil Aktive aus der Zivilgesellschaft zusammen, um die Themen Digitalisierung und Nachhaltigkeit zu diskutieren. Jetzt ist das Konferenzbuch „Was Bits und Bäume verbindet" erschienen. Als Medienpartner der Konferenz veröffentlicht netzpolitik.org an dieser Stelle jeden Montag einen Beitrag daraus. Das ganze Buch ist auch als Download (PDF) verfügbar[12].

Lorenz Hilty

Lorenz Hilty ist Professor am Institut für Informatik an der Universität Zürich und leitet die gemeinsame Forschungsgruppe *Informatik und Nachhaltigkeit* der Universität Zürich und der *Empa* (*Eidgenössische Materialprüfungs- und Forschungsanstalt)* in St. Gallen. Seine Schwerpunkte sind ökologische und gesellschaftliche Aspekte der Digitalisierung.

Dieser Text ist im Original unter dem Titel „Dematerialisierung durch Digitalisierung: Anspruch und Wirklichkeit“ erschienen (CC BY-NC-SA 3.0 DE).

Anmerkungen

1 *Arnfalk P (2002) The Role of ICT Based Communication from a Pollution Prevention Perspective. In: Environmental Communication in the Information Society – Proceedings of the 16th Conference (International Society for Environmental Protection)*
2 *World Bank (2009) Air transport, passengers carried: Civil Aviation Statistics of the World and ICAO staff estimates, https://data.worldbank.org/indicator/IS.AIR.PSGR*
3 *IATA (2018) International Air Transport Association. IATA Forecast Predicts 8.2 billion Air Travelers in 2037, https://iata.org/pressroom/pr/Pages/2018-10-24-02.aspx*
4 *Warland L et al (2016) Factsheet: Dienstreisen, https://sustainability.uzh.ch/dam/jcr:8949ac6f-f34e-4f73-97c5-483fa3130b70/2016-08-15_Factsheet_Dienstreisen.pdf*
5 *Moreno-Izquierdo L et al (2015) The Impact of the Internet on the Pricing Strategies of the European Low Cost Airlines. European Journal of Operational Research 246, 651–660*
6 *Dompke M et al (2004) Memorandum Nachhaltige Informationsgesellschaft (Fraunhofer IRB Verlag), http://publica.fraunhofer.de/documents/N-20549.html*
7 *Hilty LM (2017) Grundlagenforschung in der Informatik? Perspektiven der Informatik und ihre Erkenntnisziele. Vereinigung der Schweizerischen Hochschuldozierenden 43, 3–10*
8 *Koomey J et al (2011) Implications of Historical Trends in the Electrical Efficiency of Computing. IEEE Annals of the History of Computing 33, 4 6–54*
9 *Hilty LM et al (2006) Rebound Effects of Progress in Information Technology. Poiesis & Praxis: International Journal of Technology Assessment and Ethics of Science 1, 19–38*
10 *Huisman J et al (2017) Prospecting Secondary raw materials in the Urban mine and Mining wastes (ProSUM): Final Report*
11 *Reichwein A, Sydow J (2018) Wege aus der Reparaturkrise? Das US-amerikanische „Right to Repair“ (Germanwatch)*
12 *https://www.oekom.de/fileadmin/diverses/9783962381493_klein.pdf*

Markus Reuter

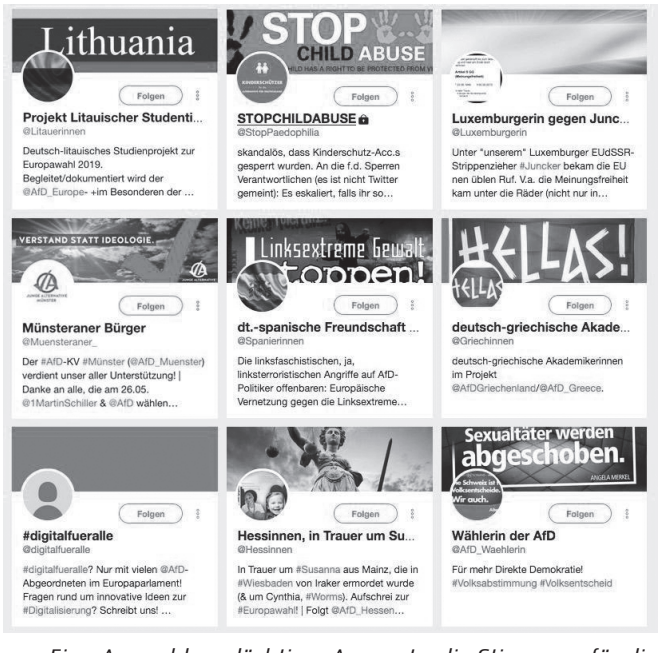
Fälschen, züchten und verstärken: Fragwürdige Twitter-Tricks bei der AfD

Recherchen geben einen Einblick in die Twitterstrategie der AfD. Die Partei bezahlte dabei einen parteinahen Social-Media-Berater aus Münster: Der züchtete Twitter-Accounts mit Spammer-Methoden, reichte Accounts unter wechselnden Namen an Parteivertreter weiter und steht im Verdacht, hinter Netzwerken aus Fake-Accounts zu stehen, die mit koordinierten Retweets Abgeordnete der Partei verstärkten.

Auf Twitter haben die AfD und ihr Umfeld fragwürdige Methoden und Tricks genutzt, um die Partei größer aussehen zu lassen. Eine gemeinsame Recherche von *netzpolitik.org* und *t-online.de* ist auf zahlreiche Fälle gestoßen, in denen mit eigens dafür erstellten Accounts Stimmung für die Partei und über koordinierte Retweets Abgeordneten künstlich Relevanz zugesprochen wird.

Im Rahmen der Recherche fanden wir unzählige orchestrierte Twitter-Accounts, welche die AfD direkt und indirekt mit Postings, Follows und Retweets unterstützen. Hinzu kommen Accounts, die mit wechselnden Namen und einem schon aufgebauten großen Followerstamm durch die rechtsradikale Partei gereicht wurden. In den Fokus rückte dabei wieder einmal der „Mann aus Münster“, den wir schon in unserer Recherche „So twittert die AfD“[1] im Jahr 2017 hinter vielen inoffiziellen Unterstützeraccounts und dem rechten Scheinriesen Balleryna[2] vermuteten. Damals konnten wir eine direkte Verbindung zur oder eine Tätigkeit für die AfD noch nicht nachweisen, auch wenn es dafür Anhaltspunkte gab.

Nun ist klar: Der Mann aus Münster, der eigentlich Magnus B. heißt, hat auf Honorarbasis für die Bundesgeschäftsstelle der AfD gearbeitet. Er reiste im „Twitter-Team“-Shirt zu Parteiveranstaltungen, posierte vor dem Reichstagsgebäude. Und er betreute Accounts von Abgeordneten. Ein Pressesprecher der Partei bestätigte gegenüber T-Online: „Herr B. war in 2018 kurzzeitig für den AfD-Bundesverband in der Bundesgeschäftsstelle tätig gewesen.“ Er hätte dort der „Kommentarkontrolle und der Beitragsmoderation im Bereich Social Media“ zugearbeitet. Mittlerweile sei das Dienstverhältnis aufgelöst worden, es habe „sehr unterschiedliche Ansichten über Arbeitsweisen und -methoden“ gegeben.



Eine Auswahl verdächtiger Accounts, die Stimmung für die AfD machten und machen

Erster Schritt dieser neuerlichen Recherche zu den Twitter-Aktivitäten der AfD waren auffällige Accounts, welche die Partei unterstützten und offenbar für die Europawahl 2019 angelegt waren. Diese Accounts mit Namen wie @Franzoesinnen, @Griechinnen, @Polinnen, @Zypriotinnen oder @AfD_Bulgaria, @AfD_Polska, @AfD_Ungarn wurden in einem Blogbeitrag der Journalistin Andrea Becker beschrieben[3] und waren Ausgangspunkt der Recherche.

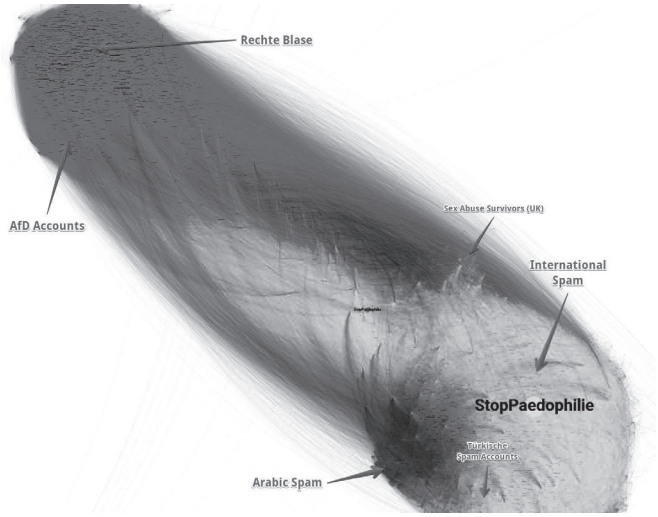
Es entstand der Verdacht, dass auch hier Magnus B. hinter den Accounts stecken könnte. Wenn man sich länger mit Fake-Accounts und den Akteuren dahinter beschäftigt, erkennt man irgendwann deren Muster, Handschriften und Vorlieben.

Merkmale wie Ähnlichkeiten bei Profilbildern oder Headerbilder mit ähnlichen Designs oder Sprüchen weisen darauf hin, dass die Accounts aus einer Hand stammen könnten. Und es tauchten immer wieder Kinderschutz- und Antipädophilie-Bezüge auf, die uns schon in früheren Recherchen zu Magnus B. aufgefallen waren. Auch diese vermeintlichen Kinder- und Frauenschutz-Accounts wurden immer wieder zur Verbreitung von AfD-naher Kommunikation genutzt. Schaut man sich darüber hinaus an, wem die Accounts folgen und wer ihnen folgt, dann fällt auf, dass sie eng zusammenhängen und sich gegenseitig folgen. Magnus B. bestreitet, dass er die oben genannten Accounts betreut hat.

Verdächtige Sockenpuppen

Die verdächtigen Sockenpuppen[4]-Accounts sammelten wir in einer Liste und gaben sie dem Social-Media-Analysten Luca Hammer zur Auswertung des Following-Netzwerkes. Er untersuchte, wer wem folgt und erstellte dann ein Netzwerk anhand der Verbindungen.

Die Analyse offenbarte ein Netzwerk von 51.000 Accounts, die mit über sechs Millionen Follows miteinander verbunden sind. Knapp 6.000 Accounts bilden ein rechtes Cluster rund um die AfD, die mit zwei Millionen Follows verbunden sind. Auf der anderen Seite, schwächer in sich vernetzt, sieht man die Follow4Follow-Spam-Bubble, in deren Mitte @StopPaedophilie ist. Auch dieser Account machte bis 2016 Stimmung für die AfD.



Grafik: Luca Hammer CC-BY-SA 4.0

Das Follow4Follow-Prinzip, bei der sich Accounts zum Aufbau einer großen Followerschaft systematisch gegenseitig folgen, war bei Spammern beliebt, weil das Prinzip als Methode zur Umgehung der Spamerkennung von Twitter galt. Magnus B. bestätigte uns gegenüber, dass er dieses Prinzip bei Accounts anwendete, betonte aber, dass dies vor seiner Zeit bei der AfD geschehen sei.

Interessanterweise gibt es im Netzwerk auch einen arabischen Spam-Cluster, der erstaunlich viele Verbindungen in Richtung AfD-Cluster aufweist. Diese arabische Connection bei Twitter-Accounts ist uns auch schon bei der großen Twitter-Recherche zur AfD 2017[5] und dem rechten Scheinriesen Balleryna[6] aufgefallen. Die Verbindung zu den arabischen Accounts dürfte auch auf das Follow4Follow-Prinzip zurückgehen.

Von den untersuchten verdächtigen Accounts sind heute nur noch wenige aktiv. Viele hörten im Herbst 2018 auf zu twittern, andere Accounts aus der Liste hat Twitter mittlerweile gesperrt.

Twitter-Konzept für die AfD in NRW erstellt

In einem Tweet des offiziellen NRW-Accounts der AfD vom Oktober 2017 ist Magnus B. links im Bild zu sehen. [Verpixelung: netzpolitik.org]

Magnus B. reichte beim Landesverband der AfD in Nordrhein-Westfalen im März 2017 ein mehrseitiges Twitter-Konzept ein, das netzpolitik.org vorliegt. In diesem werden generelle Tipps für die Kommunikation der Partei auf Twitter gegeben. Laut dem Dokument scheint es auch mindestens ein Treffen mit Parteivertretern gegeben zu haben: In einer handschriftlichen Notiz am Twitter-Konzept bedankt sich Magnus B. beim NRW-Landtagsabgeordneten Andreas Keith-Volkmer[7] für einen Termin. Keith-Volkmer, der derzeit Parlamentarischer Geschäftsführer der AfD in NRW ist, war für die Partei schon unter dem AfD-Mitbegründer Bernd Lucke[8] für den Bereich Social Media zuständig.

Dass die Partei in Nordrhein-Westfalen Magnus B. bezahlte, können wir nicht nachweisen. Der Landessprecher Helmut Seifen bestreitet eine Zusammenarbeit mit B. auf Landesebene. Der offizielle Account der Partei in NRW twitterte jedoch nach der Bundestagswahl am 24. Oktober 2017 ein Bild: Es zeigt zweifelsfrei Magnus B. vor dem Reichstag mit einem T-Shirt mit der

Aufschrift „Twitter-Team“. Zahlreiche weitere Bilder von B. mit diesem T-Shirt auf Parteiveranstaltungen der AfD und der Jungen Alternative liegen uns vor.

Dienstleistungen für Abgeordnete und Gliederungen der Partei

Die feilgebotenen Dienstleistungen von Magnus B. waren aber nicht nur konzeptioneller Art. Herr B. reichte offenbar unter anderem Namen geführte Accounts mit einem schon vorhandenen Followerstamm weiter oder befüllte diese selbst mit Inhalten. Auf Twitter lassen sich die Accountnamen beliebig ändern.

In zwei Fällen wissen wir, dass Magnus B. hinter der Weitergabe von Accounts steckte. Einer davon dreht sich um Helmut Seifen: Der AfD-Landtagsabgeordnete Helmut Seifen sagt, dass sein Kreisverband in seiner Abwesenheit eine Zusammenarbeit mit B. beschlossen habe. Das Ergebnis war: Seifen erhielt einen Account unter seinem Namen, der zu dem Zeitpunkt bereits hunderte Follower hatte, und der Kreisverband erhielt als @AfDBorken einen Account, der zuvor @____Rudolf hieß. Das Befüllen der Accounts mit Inhalten hatte B. dem Kreisverband angeboten.

Seifen selbst twitterte gar nicht über @Helmut_Seifen, wie er t-online.de verriet. Irgendwann ärgerte sich Seifen dann über einem in seinem Namen veröffentlichten Tweet. Er beendete die Zusammenarbeit mit Magnus B. – aus @Helmut_Seifen wurde danach plötzlich der Account @hessenwahl2018.

Nutzung von hochgezüchteten Accounts für AfD-Politiker

Eine noch viel weiter gehende Namensgeschichte hat der mittlerweile gesperrte Account @JaZumDiesel: Dieser Account hieß zunächst @sweet_xenia und dann @fina24de. Zur Bundestagswahl 2017 wurde daraus @FDPAussteigerin, ein Account, der vorgab, einer mit der AfD sympathisierenden, enttäuschten FDP-Anhängerin zu gehören. Als dann der AfD-Politiker Dieter Laudenbach in die Stichwahl zur Oberbürgermeisterwahl in Gera[9] kam, wurde aus der enttäuschten FDPlerin plötzlich ein aufstrebender @AfDOBLaudenbach. Ein Account mit immerhin 70.000 Followern.

Laudenbach selbst sagt gegenüber t-online.de, dass er Inhalte, die getwittert werden sollten, an eine offizielle AfD-Mailadresse schickte. In der AfD-Zentrale in Berlin will man sich zu diesem Fall allerdings nicht äußern. Nachdem Laudenbach die Stichwahl verlor, wurde der Account in @ZukunftDEU umbenannt und dann zu @JaZumDiesel. Zahlreiche weitere Accounts mit ähnlich bewegter Namensgeschichte und AfD-Bezug sind netzpolitik.org bekannt.

Namensänderungen von Twitter-Accounts lassen sich nicht mit einer automatisierten Auswertung nachvollziehen, sondern benötigen Handarbeit in der Recherche. Es gibt mehrere Methoden, auf Namensänderungen zu stoßen: Entweder entdeckt man alte Tweets und Replies, die Hinweise auf einen alten Namen geben. Oder man kennt die alten Accountnamen, nutzt hierfür dann die Suchfunktion von Twitter und gleicht die Daten mit den Archivierungen von archive.org ab. Dass es sich um den gleichen Account handelt, kann man auch erkennen, weil jeder Twitter-Account eine – trotz aller Namensänderungen – immer gleichbleibende ID hat. Diese lässt sich öffentlich abrufen. Bei dieser Recherche war sehr hilfreich, verdächtige Accounts über lange Zeit zu dokumentieren und so alle Veränderungen gut nachvollziehbar zu machen.

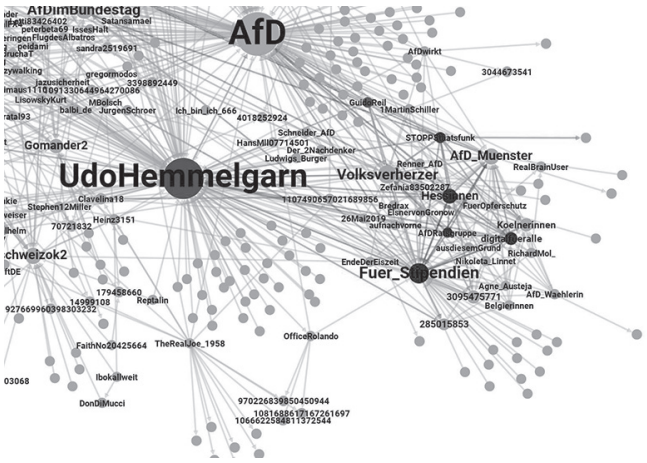
Relevanz-Zuweisung durch koordinierte Retweets

In der Recherche untersuchten wir auch, wer durch Interaktionen verdächtiger Sockenpuppen-Accounts profitierte. Hier kam heraus, dass der Twitteraccount des Bundestagsabgeordneten Udo Hemmelgarn aus NRW überproportional viele Retweets von ihnen erhielt.

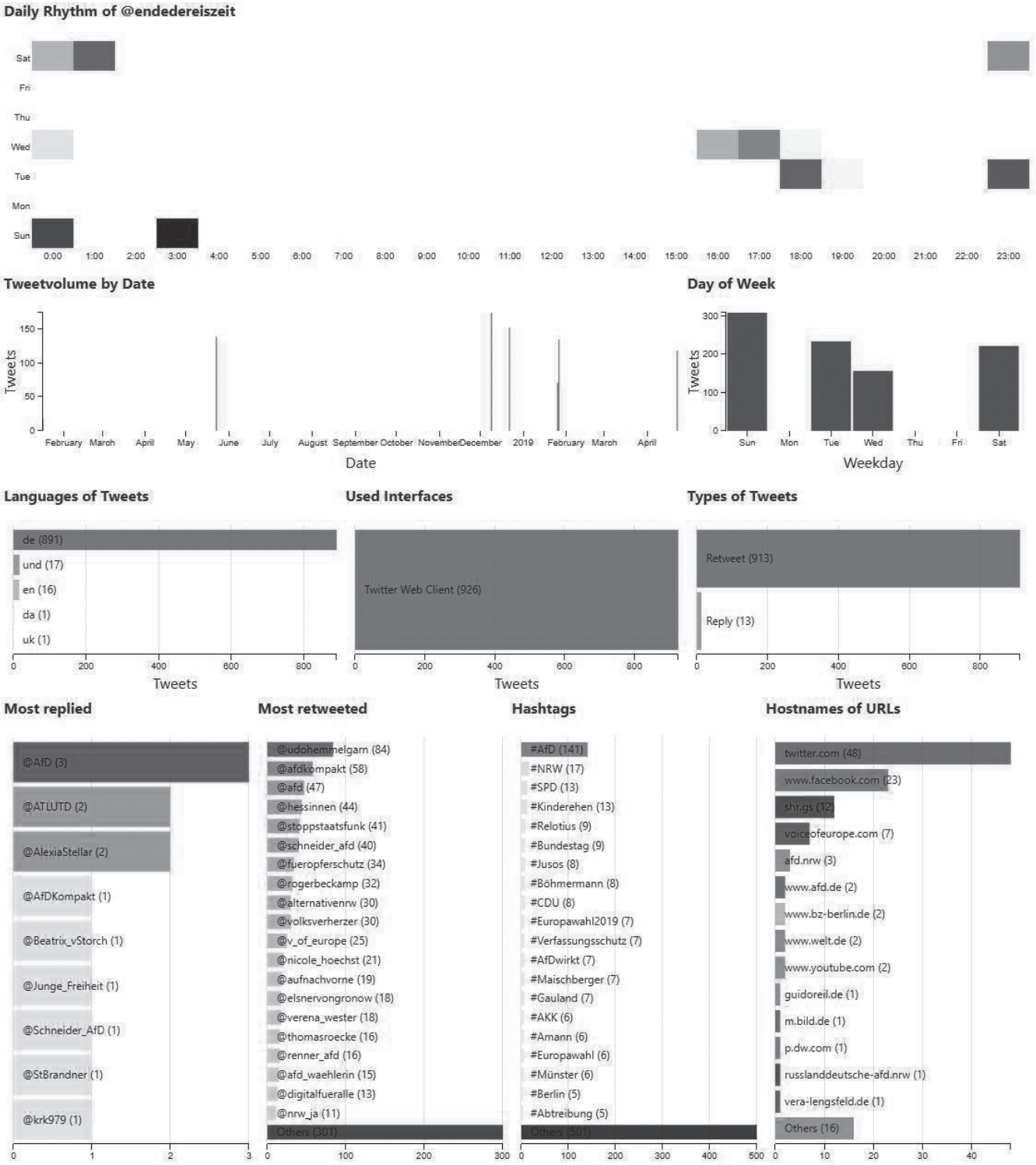
Im Untersuchungszeitraum vom 17.-27. April 2019 hatten wir deshalb die Tweets von fünf AfD-Politikern exemplarisch untersucht und geschaut, wer diese retweetete. Im Zeitraum waren sieben der von uns als Sockenpuppen definierten Accounts aktiv und haben von den fünf untersuchten Accountsausschließlich Udo Hemmelgarn retweetet. Etwa elf Prozent seiner Retweets stammten von den mutmaßlichen Sockenpuppen. Neben diesen tauchten in der Untersuchung weitere Accounts im Retweet-Netzwerk auf, die ähnliche Namen tragen und sich ähnlich verhalten haben. Der tatsächliche Anteil an Sockenpuppen-Retweets von Hemmelgarn könnte daher noch deutlich höher sein.

Gegenüber netzpolitik.org bestätigt Udo Hemmelgarn, dass Magnus B. für ihn arbeitete und seinen Twitteraccount betreute. Der Vorwurf von Retweets durch Fake-Accounts sei ihm bisher nicht bekannt gewesen. Hemmelgarn hält eine solche Kommunikationsmethode nicht für zielführend, sagt er auf Nachfrage von netzpolitik.org.

Einer der während der Analyse neu aufgetauchten mutmaßlichen Sockenpuppen ist der Account @endedereiszeit. Bei der Untersuchung fiel ein besonderes Nutzungsmuster auf: Diese Accounts waren nur von Zeit zu Zeit aktiv, dann aber wurden oftmals 50-150 Retweets auf einen Schlag abgesetzt. Größter Profiteur der Retweets war im Untersuchungszeitraum der Account des Bundestagsabgeordneten Udo Hemmelgarn, aber auch der Account des AfD-Mitgliedermagazins @AfDKompakt wurde verstärkt.



Rechts: Von uns identifizierte mutmaßliche Sockenpuppen. In Links: Von uns untersuchte Accounts bei denen wir schauten, wer diese retweetete.



Die Grafiken zeigen, dass der Account @endedereiszeit, den wir dem Netzwerk zuordnen, nur ab und an genutzt wurde, um bestimmte AfD-Accounts gezielt zu retweeten. Größter Profiteur der Retweets war im Untersuchungszeitraum der AfD-Bundestagsabgeordnete Udo Hemmelgarn. Der Account @endedereiszeit wurde mittlerweile von Twitter gesperrt. Die Auswertung wurde mit dem Tool Accountanalysis von Luca Hammer durchgeführt.

Eine Münsteraner Trollfabrik?

Weitere dieser orchestrierten Verstärker-Accounts mit ähnlichem Nutzungsmuster sind u. a. @26mai2019[10], @ausdiesemgrund[11], @agne_austeja[12], @Belgierinnen[13], @nikoleta_linnet[14], @afd_waehlerin[15] und @afdratsgruppe[16]. Während dieser Recherche konnte t-online.de Kontakt zu einer Person aufnehmen, die für das Posten von Promobildern und für das Retweeten von AfD-Accounts aus NRW sowie von Partei-Promis wie „Alice Weidel und so“ auf Stundenbasis bezahlt wurde. Dieses Muster passt perfekt auf die Aktivitäten der hier untersuchten Accounts. Diese Person, die per Klickwork Stimmung für die AfD machte, taucht auch mehrmals auf Twitter-Team-Fotos mit dem „Mann aus Münster“ auf, ein direkter und persönlicher Kontakt ist also sehr wahrscheinlich. Magnus B. will das nicht kommentieren, er verweist auf eine Verschwiegenheitserklärung.

Die durch die Recherche offengelegte Kommunikationsmethode hat also folgende Säulen:

1. Das Anlegen zahlreicher Fake-Accounts mit beliebigen Namen.

2. Das Hochzüchten dieser Accounts einerseits mit der Followback-Methode und andererseits durch das Betreiben der Accounts als Teil eines inoffiziellen rechten Unterstützernetzwerkes. Durch die Aktivität folgen den Konten dann auch einige echte Accounts.

3. Die Weitergabe von hochgezüchteten Accounts unter anderem Namen, damit AfD-Vertreter oder AfD-nahe Kampagnen mit einem großen Followerstamm starten und von Anfang an größer aussehen.

4. Das Betreiben eines Netzwerkes künstlicher und koordinierter Relevanz-Zuweisung durch Retweets, mit dem die auf Twitter eher schwache Partei und ihre Vertreter stärker aussehen sollen als sie sind.

Fraglich ist, ob diese Methoden in der rechtlichen Grauzone aus kommunikatorischer Sicht überhaupt große Vorteile bringen. Falschen Netzwerken fehlt die echte Reichweite, sie können allenfalls vortäuschen wichtig zu sein.

Dieser Artikel baut auf einer gemeinsamen Recherche von netzpolitik.org und t-online.de auf. Die Autoren der Artikel verfolgen seit Jahren die Aktivitäten von Magnus B. rund um die AfD. Für die Recherche wurden nun unterschiedlichste Erkenntnisse, Auswertungen sowie O-Töne und Konfrontierungen gemeinsam genutzt. Für die Datenauswertung zeichnet der unabhängige Social-Media-Analyst Luca Hammer verantwortlich, mit dem netzpolitik.org immer wieder in Sachen Twitteranalyse und Datenjournalismus zusammenarbeitet.

Quelle: https://netzpolitik.org/2019/faelschen-zuechten-und-verstaerken-fragwuerdige-twitter-tricks-bei-der-afd/

Autoreninfo zu Markus Reuter siehe Seite 55

Anmerkungen

1 *https://netzpolitik.org/tag/so-twittert-die-afd/*
2 *https://netzpolitik.org/2017/twitter-datenanalyse-bei-der-afd-die-falsche-balleryna/*
3 *https://andivendo.wordpress.com/2018/01/23/das-meisje-europa-und-die-afd/*
4 *https://de.wikipedia.org/wiki/Sockenpuppe_(Netzkultur)*
5 *https://netzpolitik.org/tag/so-twittert-die-afd/*
6 *https://netzpolitik.org/2017/twitter-datenanalyse-bei-der-afd-die-falsche-balleryna/*
7 *https://de.wikipedia.org/wiki/Andreas_Keith-Volkmer*
8 *https://de.wikipedia.org/wiki/Bernd_Lucke*
9 *https://www.spiegel.de/politik/deutschland/gera-afd-politiker-dieter-laudenbach-koennte-oberbuergermeister-werden-a-1204933.html*
10 *https://cdn.netzpolitik.org/wp-upload/2019/05/Analysis@26mai2019.png*
11 *https://cdn.netzpolitik.org/wp-upload/2019/05/Analysis@ausdiesemgrund.png*
12 *https://cdn.netzpolitik.org/wp-upload/2019/05/Analysis@agne_austeja.png*
13 *https://cdn.netzpolitik.org/wp-upload/2019/05/Analysis@belgierinnen.png*
14 *https://cdn.netzpolitik.org/wp-upload/2019/05/Analysis@nikoleta_linnet.png*
15 *https://cdn.netzpolitik.org/wp-upload/2019/05/Analysis@afd_waehlerin.png*
16 *https://cdn.netzpolitik.org/wp-upload/2019/05/Analysis@afdratsgruppe.png*

Markus Reuter

Bundesregierung: Drei Viertel aller strafbaren Hasspostings kommen von rechts

Der Hass kommt vor allem von rechts: Zwischen 80 und 90 Prozent aller Straftaten im Bereich Hasskriminalität gehen auf das Konto von Rechtsradikalen. In der neuen Kategorie Hassposting stammen drei von vier der strafbaren Inhalte aus dem rechten Lager.

Seit dem Januar 2017 erfasst das Bundeskriminalamt *Hasspostings* in einer eigenen Kategorie. In den Jahren 2017 und 2018 dominierten rechte Hasspostings mit überwältigender Mehrheit die neu eingeführte Zählung: Etwa drei Viertel aller Hasspostings hatten einen rechten Hintergrund. Das geht aus der Antwort der Bundesregierung auf eine Kleine Anfrage der Linkspartei[1] hervor.

Das Bundesinnenministerium hat im Jahr 2018 bundesweit 1.472 Hasspostings gezählt. Davon wurden 1.130 der Politisch Motivierten Kriminalität (PMK) Rechts zugeordnet, 126 PMK Links, 49 einer religiösen Ideologie, 45 der PMK Ausländer und 122 waren nicht bestimmbar (Abbildung 1).

Im Jahr 2017 gab es mit insgesamt 2.270 Fällen mehr Hasspostings. In der Verteilung sieht es aber ähnlich aus. 1.681 Hasspostings gingen auf das Konto von Rechten, 198 basierten auf religiöser Ideologie, 122 kamen von links und 58 aus dem Bereich Ausländer. 211 Postings wurden nicht zugeordnet.

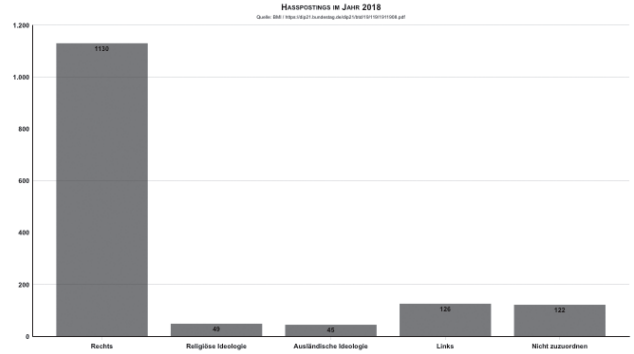


Abbildung 1

Unterschiedliche Definitionen für Hasspostings

Was ein Hassposting ist, wird mitunter leicht unterschiedlich definiert. Das Bundesamt für Verfassungsschutz sagt[2]:

> *Hasspostings sind Beiträge im Internet, die in allen Phänomenbereichen im Rahmen von Debatten zu aktuellen Themen eine Emotionalität und zum Teil auch Schärfe aufweisen, die jenseits der freien Meinungsäußerung liegen beziehungsweise bei denen die Schwelle zur Strafbarkeit mitunter deutlich überschritten wird.*

Das umfasse Drohungen, Nötigungen, Verunglimpfungen, extremistische Inhalte sowie unverhohlene Aufrufe zu Straf- und Gewalttaten.

Während der Verfassungsschutz die Strafbarkeit einer Aussage nicht zur zwingenden Bedingung macht, rechnet das Bund-Länder-Gremium „Kommission Staatsschutz" (KST)[3] nur Straftaten zu Hasspostings. Sie müssten …

> *[…] Anhaltspunkte dafür geben, dass diese wegen einer zugeschriebenen oder tatsächlichen politischen Haltung, Einstellung und/oder Engagements, Nationalität, ethnischer Zugehörigkeit, Hautfarbe, Religionszugehörigkeit, Weltanschauung, sozialen Status, physischer und/oder psychischer Behinderung oder Beeinträchtigung, sexuellen Orientierung und/oder sexuellen Identität oder äußeren Erscheinungsbildes kausal gegen eine oder mehrere Person(en), Gruppe(n), oder Institution(en) gerichtet sind.*

Hasskriminalität mit dem „Tatmittel Internet"

Auch beim Oberthema *Hasskriminalität*, die mit dem Tatmittel Internet begangen wurde, dominieren Rechte das Feld. In den vergangenen Jahren gingen zwischen 80 und 90 Prozent aller Straftaten in diesem Gebiet auf das Konto von rechten TäterInnen. Insgesamt sind die Straftaten in diesem Themenfeld vor allem in den Jahren 2015 und 2016 stark angestiegen, und dann wieder etwas zurückgegangen. Sie blieben jedoch auf einem hohem Niveau.

Im Jahr 2017 fiel die Kategorie *Ausländer* weg, stattdessen wird seitdem zwischen *Ausländische Ideologie* und *Religiöse Ideologie* unterschieden (Abbildung 2).

Die Zahlen im Überblick

- 2010 – 377 Straftaten (303 Rechts, 35 Ausländer, 5 Links, 34 nicht zuzuordnen)
- 2011 – 407 Straftaten (357 Rechts, 17 Ausländer, 8 Links, 25 nicht zuzuordnen)
- 2012 – 492 Straftaten (437 Rechts, 18 Ausländer, 5 Links, 32 nicht zuzuordnen)
- 2013 – 660 Straftaten (590 Rechts, 21 Ausländer, 10 Links, 39 nicht zuzuordnen)
- 2014 – 1.119 Straftaten (945 Rechts, 108 Ausländer, 6 Links, 60 nicht zuzuorden)
- 2015 – 3.084 Straftaten (2.853 Rechts, 92 Ausländer, 10 Links, 129 nicht zuzuordnen)
- 2016 – 3.177 Straftaten (2.891 Rechts, 78 Ausländer, 16 Links, 192 nicht zuzuordnen)
- 2017 – 2.458 Straftaten (2.283 Rechts, 54 Religiöse Ideologie, 38 Ausländische Ideologie, 12 Links, 71 nicht zuzuordnen)
- 2018 – 1.962 Straftaten (1.798 Rechts, 39 Ausländische Ideologie, 38 Religiöse Ideologie, 11 Links, 76 nicht zuzuordnen)

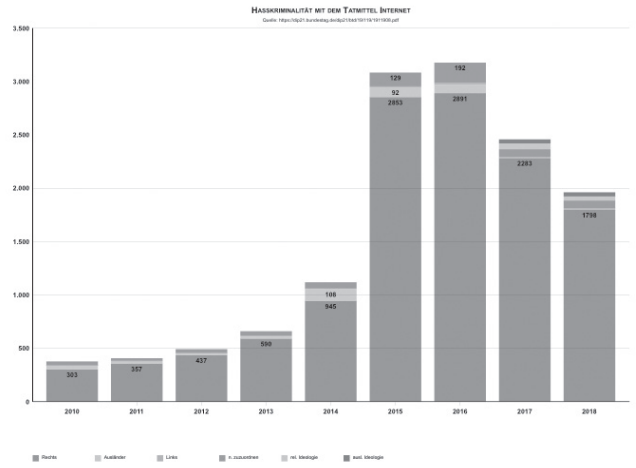


Abbildung 2

Quelle: https://netzpolitik.org/2019/bundesregierung-drei-viertel-aller-strafbaren-hasspostings-kommen-von-rechts/

Anmerkungen

1 *https://dip21.bundestag.de/dip21/btd/19/119/1911908.pdf*
2 *https://www.bundestag.de/presse/hib/653318-653318*
3 *https://www.cilip.de/2013/05/01/allgegenwaertig-aber-wenig-bekannt-der-polizeiliche-staatsschutz-in-deutschland/*
4 *http://pgp.mit.edu/pks/lookup?op=get&search=0xB8020A34EF5B7E17*

Markus Reuter

Markus Reuter beschäftigt sich mit den Themen Digital Rights, Hate Speech & Zensur, Fake News & Social Bots, Videoüberwachung, Grund- und Bürgerrechte sowie soziale Bewegungen. Bei *netzpolitik.org* seit März 2016 als Redakteur dabei. Er ist erreichbar unter *markus.reuter | ett | netzpolitik.org* (OpenPGP[4]) und auf Twitter unter *@markusreuter_*

Matthias Monroy

Europäische Union plant europaweite Abfrage von Gesichtsbildern

Im Vertrag von Prüm ist die polizeiliche Abfrage von biometrischen Daten unter EU-Mitgliedstaaten deutlich vereinfacht. Unter Leitung Österreichs wird jetzt die Erweiterung auf Gesichtserkennung untersucht. Ein entsprechender Ratsbeschluss könnte bereits im nächsten Jahr erfolgen.

Die Europäische Union will der Polizei den Abgleich biometrischer Daten deutlich erleichtern. Dies betrifft Fahndungsfotos oder Lichtbilder, die nach einer erkennungsdienstlichen Behandlung in polizeilichen Datenbanken gespeichert sind. Will eine Behörde die Identität einer Person mithilfe eines Fotos ermitteln, muss derzeit jedes einzelne Land einzeln angeschrieben werden. Geplant ist deshalb ein System, mit dem Daten gleichzeitig in jedem EU-Mitgliedstaat abgefragt werden können.

Um die nationalen Polizeidatenbanken zu vernetzen, soll der Vertrag von Prüm herangezogen werden[1], der die EU-weite Zusammenarbeit zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der als illegal eingestuften Migration regelt. Das Abkommen hatte das deutsche Innenministerium unter Wolfgang Schäuble in 2005 initiiert, unterzeichnet wurde es in Prüm, einer Kleinstadt in der Eifel. Ursprünglich als zwischenstaatliche Regelung einzelner Regierungen eingerichtet, ist der Vertrag 2008 in den Rechtsrahmen der Europäischen Union überführt worden.

„Next Generation Prüm"

Mit dem Vertrag können die Behörden aller EU-Mitgliedstaaten grenzüberschreitend DNA-Dateien, Fingerabdrucksysteme und Register mit Kraftfahrzeug- und Halterdaten abfragen. Der Informationsaustausch erfolgt dabei im Treffer-/Kein-Treffer-Verfahren: Die Behörden erfahren, ob ein Treffer vorliegt. Um mehr Informationen zu bekommen, müssen sie ein Ersuchen an die zuständige Behörde stellen – der sogenannte Folgeschriftverkehr.

Im Rahmen der erneuerten EU-Strategie zur Inneren Sicherheit 2015 bis 2020 soll die polizeiliche Prüm-Zusammenarbeit nun erweitert werden. Grundlage sind die Schlussfolgerungen des Rates vom vergangenen Jahr[2] anlässlich des zehnjährigen Bestehens der EU-Prüm-Beschlüsse.

Das Vorhaben firmiert als *Next Generation Prüm*, kurz *Prüm.ng*. Dabei sollen Datenformate, Abfrageverfahren und der Folgeschriftverkehr vereinfacht werden. Möglich wäre beispielsweise, bereits bei der Abfrage durch eine nationale Behörde Personendaten mitzuliefern, die bei der fehlerfreien Suche nach vorhandenen biometrischen Daten helfen könnten. Geplant ist auch der Einsatz einheitlicher Software.

BKA unterstützt Deloitte-Studie

Für den Aufbau des neuen Systems haben die EU-Mitgliedstaaten drei sogenannte Fokusgruppen zu DNA-Daten (Leitung: Deutschland), Fingerabdrücken (Leitung: Österreich) sowie Fahrzeugregisterdaten (noch ohne Leitung) eingerichtet.

Wie die vorhandenen Fähigkeiten weiter ausgebaut werden können, soll in einer Machbarkeitsstudie untersucht werden. Dafür hat die Europäische Kommission das Beratungsunternehmen Deloitte beauftragt. Die Delegationen der EU-Mitgliedstaaten sollen hierzu Fragebögen zu Verbesserungsmöglichkeiten beantworten, anschließend folgen gemeinsame Workshops. Die Ergebnisse sollen im September und damit noch vor Antritt der neuen EU-Kommission vorliegen.

Auch das deutsche Bundeskriminalamt (BKA) arbeitet an der Studie mit. In einem anderen EU-Projekt hat das BKA das Format UMF3+ entwickelt[3], mit dem der polizeiliche Informationsaustausch in der Europäischen Union erleichtert wird. Die Ergebnisse des Projekts könnten in *Next Generation Prüm* einfließen.

Forensik-Abteilungen suchen nach geeigneter Technik

Um *Next Generation Prüm* auf Gesichtserkennung auszuweiten, existiert eine vierte Fokusgruppe unter Leitung Österreichs. An ihr nimmt auch das BKA teil, das dort seine Erfahrungen aus deutschen Projekten einbringen kann: die Gesichtserkennung zur Fahndungsabfrage[4], im öffentlichen Raum[5], beim Grenzübertritt[6] oder nach Gipfelprotesten[7]. Das BKA stellt sein eigenes System zum Abgleich von Gesichtern in der INPOL-Fahndungsdatenbank außerdem bald auf ein neues Verfahren um[8].

Matthias Monroy

Matthias Monroy, Wissensarbeiter, Aktivist und Mitglied der Redaktion der Zeitschrift *Bürgerrechte & Polizei/CILIP*[11]. In Teilzeit Mitarbeiter des MdB Andrej Hunko. Publiziert in linken Zeitungen, Zeitschriften und Online-Medien, bei *Telepolis*, *Netzpolitik* und in Freien Radios. Alle Texte und Interviews unter *digit.so36.net*, auf englisch *digit.site36.net*, auf Twitter *@matthimon*. Viel zu selten auf der Straße (dafür im Internet) gegen Faschismus, Rassismus, Sexismus, Antisemitismus. Kein Anhänger von Verschwörungstheorien jeglicher Couleur. Freut sich nicht über Kommentare von AnhängerInnen der genannten Phänomene. Benutzt das (altmodische) Binnen-I trotz Gepolter nervtötender Maskulisten.

Mit einer halben Million Euro[9] finanziert die EU-Kommission bereits Forschungen für das europäische Gesichtserkennungssystem. Unter Leitung des estnischen Justizministeriums prüfen polizeiliche Forensik-Abteilungen aus Finnland, Lettland, Schweden und den Niederlanden im Projekt TELEFI[10] (*Towards the European Level Exchange of Facial Images*) mögliche technische Verfahren. Mit einer nur 18-monatigen Laufzeit ist das Projekt vergleichsweise kurz, Ergebnisse sollen bereits im Sommer nächsten Jahres vorliegen.

Die grenzüberschreitende Abfrage von Gesichtsbildern müsste anschließend mit neuen EU-Prüm-Beschlüssen gesetzlich geregelt werden. Würde die Funktion nicht im Rahmen des bestehenden Vertrages umgesetzt, könnte sie auch in einem „Prüm-ähnlichen Gesichtserkennungssystem" erfolgen.

Quelle: https://netzpolitik.org/2019/europaeische-union-plant-europaweite-abfrage-von-gesichtsbildern/

Anmerkungen

1 *http://dipbt.bundestag.de/dip21/btd/19/094/1909407.pdf*
2 *https://data.consilium.europa.eu/doc/document/ST-10550-2018-INIT/de/pdf*
3 *https://netzpolitik.org/2019/bka-testet-die-europaweite-vernetzung-von-polizeiakten/*
4 *https://netzpolitik.org/2018/gesichtserkennung-bei-der-bundespolizei-jede-achte-abfrage-ein-treffer/*
5 *https://netzpolitik.org/2017/ortstermin-am-suedkreuz-die-automatische-gesichtserkennung-beginnt/*
6 *https://netzpolitik.org/2019/deutsche-grossflughaefen-gesichtserkennung-jetzt-auch-fuer-kinder/*
7 *https://netzpolitik.org/2018/soko-schwarzer-block-hamburger-datenschutzbeauftragter-haelt-gesichtserkennung-fuer-rechtswidrig/*
8 *https://netzpolitik.org/2018/gesichtserkennung-bka-will-auf-verbessertes-system-umstellen/*
9 *https://ec.europa.eu/home-affairs/sites/homeaffairs/files/financing/fundings/security-and-safeguarding-liberties/internal-security-fund-police/union-actions/docs/isfp-list-proposals-selected-for-funding-during-2018_en.pdf*
10 *https://www.telefi-project.eu/*
11 *http://www.cilip.de/*

Anna Biselli

Blockchain-Forensik: Wer steckt hinter einer Bitcoin-Zahlung?

Bitcoin ist eine anonyme Währung? Von wegen! Transaktionen kann jeder öffentlich einsehen. Auch wenn da erstmal nur lange Zeichenketten stehen: Es gibt Möglichkeiten zu erfahren, wer dahintersteckt. Wie, das haben wir uns von Forensiker Jakob Hasse erklären lassen.

Die einzelnen Glieder in der Blockchain mögen kryptisch wirken. Aber irgendjemand steckt dahinter CC-BY 2.0 Jinko Cruz

Ransomware verschlüsselt Dateien auf deinem Rechner, die Urheber fordern Lösegeld in Bitcoin. Jemand verschickt Erpressungsmails und hat dich angeblich beim Masturbieren gefilmt – und fordert Bitcoin. Auf Marktplätzen für illegale Drogen, Waffen oder Kreditkartendaten kann man vermeintlich anonym zahlen, natürlich mit Bitcoin.

Auf der anderen Seite stehen Meldungen, dass mit der Blockchain Verdächtige überführt[1] wurden. So im Fall der Administratoren der Darknet-Plattform Wall Street Market. Sie wollten sich mit den Bitcoins ihrer Kunden[2] aus dem Staub machen, aber begingen dann einen Fehler.

Jakob Hasse arbeitet bei der Dresdner Firma *dence*[3], die sich mit digitaler Forensik beschäftigt. Eines ihrer Spezialgebiete: Wie kann man Kryptowährungen wie Bitcoin nachverfolgen und vielleicht sogar herausfinden, wer hinter einer kryptischen Geldübertragung steht? Im Interview mit netzpolitik.org erklärt er, welche Informationen bei Blockchain-Transaktionen anfallen, was sie über die Nutzer verraten und was man beachten sollte, wenn man sich nicht gleich verraten will.

netzpolitik.org: *Wofür nutzt man Blockchain-Forensik?*

Jakob Hasse: Wir schauen uns größtenteils öffentlich verfügbare Daten an und schauen, was man daraus lernen kann. Das ist zum Beispiel interessant, wenn bei jemandem die Festplatte durch Ransomware verschlüsselt wurde und derjenige das Lösegeld gezahlt hat. Das Geld ist dann nicht gleich verschwunden, wie viele glauben.

Bitcoin kann man nachverfolgen, alle Transaktionen sind öffentlich. Oft wird gesagt, Bitcoin sei ein anonymes Zahlungssystem. Das stimmt aber nicht: Es ist ein pseudonymes System mit einem öffentlichen Transaktionsverzeichnis. Wir wissen aber erstmal nicht, welches Pseudonym zu welcher realen Person gehört und können diesen Link nicht einfach herstellen. Dafür versuchen wir, Anhaltspunkte zu finden.

Woher kommt das Geld und wo geht es hin?

netzpolitik.org: *Welche Informationen sind denn öffentlich, wenn ich etwas mit einer Kryptowährung bezahle?*

Jakob Hasse: Das kommt auf das Währungssystem an. Wenn wir über Bitcoin reden, sind die Vorgängertransaktionen und -adressen sichtbar. Das heißt: Woher kommt das Geld, das du in dieser Transaktion nutzen möchtest?

Das Geld, das du nutzt, musst du außerdem öffentlich signieren. Mit dieser Art Unterschrift beweist du, dass du der Eigentümer dieses Geldes bist. Außerdem sind die Blockchain-Adressen sichtbar, an die du das Geld senden möchtest. Sie sind wie öffentliche Schlüssel.

netzpolitik.org: *Kann ich auch erfahren, wann eine Transaktion getätigt wurde?*

Jakob Hasse: Ja, über die Blöcke. In einem Block werden viele Transaktionen zusammengefasst, er ist wie eine riesige Liste. Da sind auch Zusatzdaten drin: ein Zeitstempel und die Verbindungen zu den vorhergehenden Blöcken zum Beispiel.

Die Transaktionen in einem Block werden überprüft. Man prüft einerseits, dass kein Geld doppelt ausgegeben wurde. Andererseits, dass die Transaktionen valide sind: Dass es keine Fehler gegen die Regeln gibt, die man sich für das Blockchain-System selbst gegeben hat. Bei Bitcoin heißt das zum Beispiel: Der Miner bekommt ein bisschen von dem Geld ab, dafür dass er die Transaktion in die Liste schreibt.

Anhaltspunkte via Google-Suche

netzpolitik.org: *Welche Informationen wertet ihr bei der Blockchain-Forensik aus?*

Jakob Hasse: Das Interessante sind die Daten in den Transaktionen: Woher kommt das Geld und wohin soll es gehen? Bei einer Ransomware-Zahlung schaut man etwa, wo das Geld entlanggeht und ob es Punkte gibt, die man irgendwoher kennt. Es kann beispielsweise sein, dass jemand das Geld an eine bekannte Website spendet.

Wenn diese Website ihre Bitcoin-Adresse veröffentlicht, besteht schonmal eine Verbindung zwischen der Transaktion und einer realen Person, beziehungsweise einer Seite. Das lässt sich einfach mit einer Google-Suche herausfinden. Manchmal ergeben sich daraus Anhaltspunkte, wer hinter einer Transaktion steckt.

Anderes Beispiel: Wir haben öfter Fälle, wo Privatpersonen sehr hohe Summen verloren haben. Die Personen haben dann virtuelle Währungen genutzt, zum Beispiel zur Spekulation, und durch Betrug wie Phishing irgendwie ihre Coins „verloren". Dann ist die Frage: Wie ist das überhaupt passiert? Kann man Hinweise finden, um das Geld wiederzubekommen?

netzpolitik.org: *Virtuelle Währungen sind gerade auf Darknet-Marktplätzen verbreitet. Wie realistisch ist es denn, dass man bei Käufen auf solchen Marktplätzen unerkannt bleiben kann?*

Jakob Hasse: Auf Darknet-Marktplätzen sind virtuelle Währungen sehr beliebt, weil sie verschiedene Privacy-Charakteristiken haben. Bitcoin hat aber keine starken Privacy-Garantien, da man jeden Schritt einer Transaktion auf der Blockchain nachvollziehen kann. Man kann sehen, was mit dem Geld passiert und welche Pseudonyme damit Kontakt haben.

Das geht bei Bitcoin sogar noch besser als mit Bargeld. Wenn man Bargeld an eine andere Person zahlt, hinterlässt man höchstens durch die physische Anwesenheit Spuren.

Ich sollte mir überlegen, wie ich mein Geld einsetze. Wenn ich viel Wert darauf lege, dass meine Zahlung privat bleibt und keine Bezüge entstehen, sollte ich nur an jemanden überweisen, der nicht öffentlich bekannt ist. Wenn ich die Coins nur an meine Freunde schicke, ist das schon mal ein Vorteil. Sobald ich aber einem Dienstleister Geld schicke – beispielsweise Exchange-Börsen wie Coinbase – ist das erkennbar.

Anderer Coin, andere Eigenschaften

netzpolitik.org: *Ist das bei anderen Coins anders als bei Bitcoin?*

Jakob Hasse: Andere Krypto-Währungen wie Monero haben viel stärkere Privacy-Garantien. Auch sie bieten über kryptografische Verfahren die Garantie, dass das Geld nicht doppelt ausgegeben wurde. Ich kann beweisen, dass ich der Eigentümer bin. Aber wenn man das Geld verschickt, ist nicht mehr sichtbar, wo es herkommt. Wenn man sich bei Monero nur die Blockchain-Daten anschaut, kann man fast nichts tun.

netzpolitik.org: *Gibt es noch andere Spuren als die Transaktionshistorie, die einen bei virtuellen Währungen verraten können?*

Jakob Hasse: Die Blockchain selbst ist eine Datenbank. Zu dieser Datenbank gehört immer noch ein Netzwerk, in dem sich Teilnehmer miteinander unterhalten und Transaktionen verbreiten. Dieses Netzwerk und die Datenströme sind bei Bitcoin unverschlüsselt. Wenn ich also fürchte, dass meine Leitung überwacht wird, sollte ich VPN-Dienstleister oder Tor einsetzen, um meine Transaktionen zu senden. Sonst könnte dieser Datenstrom mit mir in Verbindung gebracht werden.

Es gibt Erweiterungen, die diesen Nachteil bei Bitcoin verbessern. Eine Variante ist, dass der Client Informationen nicht gleich an alle sendet, sondern erstmal nur an eine ausgewählte Kette – ähnlich wie beim Onion-Routing für Tor[4]. Erst später wird die Transaktion an alle gesendet.

Eine andere Methode sind sogenannte Coin-Join-Techniken[5], die zum Beispiel der Wasabi-Client[6] umsetzt. Da werden Techniken eingesetzt, um die Verbindung „Woher und wohin?" zu trennen. Bei Coin Joins findet sich üblicherweise eine Gruppe von Leuten zusammen, die ihre Coins zur Verfügung stellen und gemeinsam Transaktionen auslösen. Alles soll so möglichst gleich aussehen.

Innerhalb dieser Gruppe von Personen ist nicht mehr eindeutig nachvollziehbar, ob eine Verbindung zwischen Geldeingang und -ausgang besteht oder wo zwischen den Personen das Geld geflossen ist. Letztlich sorgt das trotzdem nur für Anonymität für die Personengruppe, die sich da zusammenfindet. Umso größer die Gruppe, desto mehr „Anonymität".

Der Übergang von digitaler zu analoger Währung

netzpolitik.org: *Wo gibt es noch zusätzliche Punkte, an denen beispielsweise die Polizei ansetzen kann?*

Jakob Hasse: Der Übergang in die analoge Welt ist der Punkt, wo Ermittler die einzige Greifbarkeit haben. Sonst ist eine Blockchain ein dezentrales System, es gibt keinen wirklichen Betreiber. Es gibt nur Individualpersonen und Unternehmen, die mitmachen oder teilnehmen. Unternehmen unterliegen einer Rechtsprechung, je nachdem in welchem Land sie sind und welche Gesetze es dort gibt.

Je nach Land müssen die Unternehmen sich unter anderem mit Geldwäscheprävention oder Terrorismusfinanzierung[7] auseinandersetzen. In der EU gibt es Vorschriften[8], an die sich Unternehmen halten müssen, die mit virtuellen Währungen hantieren.

Betreiber von Exchange-Börsen müssen beispielsweise wissen, wer ihre Kunden sind und Auszahlungsgrenzen einhalten. Das sind Elemente, die auch für traditionelle Konten gelten. Vorschriften sind je nach Land schon verschieden weit umgesetzt[9]. Manche Staaten sind relativ lax, was diese Vorschriften angeht, andere schon recht weit.

netzpolitik.org: *Wie sehr können sich eure Kunden auf eure Analysen verlassen?*

Jakob Hasse: Was wir mit Sicherheit sagen können: Wie sieht ein Zahlungsstrom aus? Was passiert in der Blockchain, wo gehen die Zahlungen entlang? Wenn Zusatzinformationen ins Spiel kommen, wenn etwa Adressen veröffentlich wurden und zugeordnet werden können: Diesen Link finden wir. Wenn bekannte Zahlungsdienstleister beteiligt sind, geben wir das mit an. Wir zeigen auch, wenn Transaktionen an bekannte Systeme gesendet werden, etwa ein Coin-Join-System.

Es geht bei uns aber nicht ausschließlich um Analysen. Eine unserer größten Aufgaben ist, die Techniken dahinter zu erklären – sei es Ermittlern oder Privatpersonen: Welche Eigenschaften hat ein Wasabi-Client? Welche Möglichkeiten und Beschränkungen gibt es? An welcher Stelle kann man keine Erkenntnisse mehr erzielen? Wo könnte man möglicherweise noch Zusatzinformationen herbekommen?

Quelle: https://netzpolitik.org/2019/blockchain-forensik-wer-steckt-hinter-einer-bitcoin-zahlung/

Anmerkungen

1 *https://www.heise.de/ct/artikel/Spurensicherung-Wie-die-Blockchain-Kriminelle-ueberfuehrt-4427702.html*
2 *https://www.sueddeutsche.de/digital/wall-street-market-darknet-verhaftung-administratoren-1.4437605*
3 *https://www.dence.de/de/products/multimedia_forensics*
4 *https://www.heise.de/ix/heft/Hinter-Schichten-2268444.html*
5 *https://en.bitcoin.it/wiki/CoinJoin*
6 *https://wasabiwallet.io/*
7 *https://www.bafin.de/DE/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node.html*
8 *https://news.bitcoin.com/how-eu-european-nations-regulate-cryptocurrency/*
9 *https://netzpolitik.org/2018/die-eu-kommission-moechte-kryptowaehrungen-regulieren-irgendwann-vielleicht/*

Anna Biselli

Auf einem Zettel steht, dass sie eigentlich Informatikerin ist. **Anna Biselli** war ab 2013 bei *netzpolitik.org* und ist nach einer Pause wieder als freie Autorin dabei. Sie interessiert sich vor allem für staatliche Überwachung und Dinge rund ums *BAMF* (Bundesamt für Migration und Flüchtlinge). Du erreichst sie unter *anna@netzpolitik.org* – am besten verschlüsselt [325C 6992 DCD3 1167 D9FA 9A57 1873 5033 A249 AE26]

Der für diese Retrospektive vorgesehene Artikel ist erst fünf Jahre alt, schaut also nicht allzu weit zurück, passt aber gut zum Schwerpunkt. Es handelt sich um eine Art Überblick zum Thema Cyberkrieg, der nichts von seiner Aktualität verloren hat, auch wenn in diesem Kontext inzwischen einiges passiert ist. So hat die Bundeswehr ein Cyberkommando gegründet. So ist das zweite Tallinn-Manual erschienen, in dem die völkerrechtliche Seite von Cyberkrieg aus NATO-Sicht vertieft wird. So hat es jüngst wohl Cyberangriffe der USA auf iranische Raketenabschussanlagen gegeben, was erneut vor Augen führt, dass Cyberkrieg nicht beim Hacken von Webseiten und Datenbeständen und dem Blockieren von Computern Halt macht, sondern auch technische Infrastrukturen zu den Angriffszielen gehören.

Sylvia Johnigk, Hans-Jörg Kreowski und Kai Nothdurft

Cyberwar – Schimäre oder reale Bedrohung?

Im Rahmen des Kongresses „Quo vadis NATO? – Herausforderungen für Demokratie und Recht", der vom 24. bis 26. April 2013 in Bremen stattfand, hat der zweite Autor eine Arbeitsgruppe zum Thema „NATO, Cyberwar und das Recht" geleitet und dazu einen Einführungsvortrag gehalten. Der folgende Beitrag fasst den Vortrag zusammen. Er war ursprünglich für einen Kongressreader gedacht, der aber nicht realisiert wurde.

Der Begriff Cyberwar ist schwer zu fassen

Cyberkrieg (englisch: *Cyberwar* oder *Cyberwarfare*) ist ein schillernder Begriff, in dem die Bestandteile *Cyberspace* und *Krieg* verschmolzen sind und der kriegerische Auseinandersetzungen umfasst, die mit Mitteln der Informations- und Kommunikationstechnik (IKT) wie Computer, Softwaresysteme, Internet u. ä. geführt werden. Dabei macht es Sinn, von Cyberkrieg zu sprechen, wenn die Technik selbst Waffencharakter annimmt, im Gegensatz zu militärischen Systemen wie Raketen, Drohnen, Luftabwehr u. a., bei denen IKT-Systeme zentral an Steuerung und Funktion beteiligt sind, aber nicht das wesentliche Merkmal darstellen. Der früher ähnlich gebrauchte Begriff *Information War* trifft vielleicht etwas besser, worum es geht. Auch ist zu beachten, dass nicht jeder sogenannte Cyberangriff schon Cyberkrieg ist. So sind Straftaten mit IKT wie Online-Betrug, Phishing u. ä. der Cyberkriminalität zuzurechnen, politisch motivierte Aktionsformen des Online-Protests lassen sich unter dem Begriff Hacktivismus subsumieren. Bei Sabotage und Terroranschlägen mit Hilfe von IKT ist nicht immer eindeutig und klar, ob es sich um Straftaten handelt oder bereits kriegerische Akte vorliegen. Auch Cyberspionage, die im großen Maßstab stattfindet, ist in vielen Fällen eher wirtschaftlich als militärisch motiviert.

Wettrüsten für den Cyberkrieg

Dass es sich jedoch bei Cyberkrieg nicht um ein Hirngespinst handelt, lässt sich daraus entnehmen, dass eine Vielzahl von Staaten in den letzten Jahren eigene Cyberwar-Einheiten aufgebaut haben: Beispielsweise gibt es in den USA das *United States Cyber Command*, in Großbritannien die *Government Communication Headquarters*, in Israel die *Cyber Defense Taskforce* und in China die *Blaue Armee*, eine offiziell rein defensiv ausgerichtete Hackereinheit. Der Iran brüstet sich damit, die weltweit zweitgrößte Einheit zu besitzen. Russland wird verdächtigt, Cyberwarfare offensiv zu betreiben oder zu unterstützen. Insgesamt haben inzwischen rund 140 Staaten Cyberwareinheiten aufgebaut, wobei die meisten einen offensiven Charakter haben.[1]

Auch Deutschland steht nicht abseits. Seit Februar 2011 gibt es einen *Nationalen Cybersicherheitsrat*, der bei der Beauftragte der Bundesregierung für Informationstechnik angesiedelt ist und in dem das Kanzleramt, das Auswärtigen Amt, die Innen-, Verteidigungs-, Justiz-, Wirtschafts- und Finanzministerien des Bundes, die Bundesländer sowie assoziierte Mitglieder aus der Wirtschaft vertreten sind. Und seit April 2011 gibt es ein Nationales Cyberabwehrzentrum, an dem das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Bundesamt für Verfassungsschutz (BfV) und das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) zusammenarbeiten, wobei als assoziierte Behörden das Bundeskriminalamt, der Bundesnachrichtendienst (BND), die Bundespolizei, die Bundeswehr sowie das Zollkriminalamt mitwirken. Im November 2012 wurde schließlich die *Allianz für Cybersicherheit* gegründet, in der sich das BSI und der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITCOM) abstimmen. Daneben haben einige Bundesbehörden eigene Cybereinheiten. Die Strukturen sind allerdings ziemlich intransparent, und es bleibt unklar, wer diese Einrichtungen kontrolliert.

Cyberattacken sind alltäglich

Dass auf dem Feld des Cyberkriegs ein vehementes Wettrüsten stattfindet, ist auch an der Vielzahl von staatlich und militärisch motivierten und initiierten Cyberangriffen abzulesen. Öffentliche Aufmerksamkeit erregt haben beispielsweise der *Titan Rain*, eine Angriffsserie einer chinesischen Hackergruppe auf US-amerikanische Computersysteme von Rüstungskonzernen, Streitkräften, NASA u. a., und die *Olympic Games* mit dem Computerwurm *Stuxnet*, der der Störung des iranischen Atomprogramms diente. Bekannt geworden sind auch die Denial-of-Service-Attacken gegen estländische und georgische Regierungswebseiten, die wahrscheinlich von russischer Seite lahmgelegt wurden. Die Liste ließe sich noch um diverse Beispiele verlängern. In vielen Fällen ist allerdings nicht klar, was Ziel und Zweck ist und wer wirklich als Verursacher dahintersteckt. Spionage und Sabotage sind vielfach im Spiel, aber es kann sich auch um Provokation oder Warnung handeln. Es wäre in manchen Fällen durchaus denkbar, dass Cyberkriegseinheiten

solche Angriffe als Training durchführen. Auf jeden Fall zeigen diese Beispiele wie auch die jüngst bekannt gewordene massenhafte Ausspähung sozialer Netzwerke durch die US-amerikanische National Security Agency (NSA) mit Hilfe des Überwachungsprogramms PRISM, dass elektronische Medien und elektronisch gespeicherte Daten umfassend überwacht und ausgewertet und dass Industrieanlagen, Infrastruktursysteme wie Strom- und Wasserversorgung, Verwaltungseinrichtungen und das Bankwesen durch Cyberattacken vergleichsweise einfach gestört oder ausgeschaltet werden können.

Cyberkrieg scheint attraktiv

Mit der weltweit betriebenen Einrichtung von Cyberkriegseinheiten wird erheblich an der Rüstungsspirale gedreht. Das gilt als militärisch attraktiv, weil es relativ kostengünstig ist, so dass sich auch kleinere und ärmere Länder diese Art der Aufrüstung leisten können, und weil die Gefährdung eigener Soldaten geringer ist als bei herkömmlichen Formen des Krieges. Auch können Gegner durch das Ausschalten ziviler Infrastrukturen erheblich geschwächt werden. Außerdem ist eine Rückverfolgung von Angriffen schwierig, so dass die Aggressoren gar nicht immer sofort erkannt werden. Ein weiterer Umstand, der beachtet werden muss, liegt in dem Phänomen, dass es zumindest nach dem heutigen Stand der Technik wesentlich einfacher ist, Cyberangriffe durchzuführen, als sich gegen solche Attacken zu schützen. Gerade die hochentwickelten Industrieländer mit ihrem hohen Grad an Computerisierung und Vernetzung sind extrem verwundbar.[2]

Cyberkrieg tangiert zivile Freiheit

Die vielseitige Aufrüstung zum Cyberkrieg bedeutet aber nicht nur, dass zivile Einrichtungen erheblich gefährdet sind, sondern es gibt weitere Widersprüche zwischen zivilen Ansprüchen und militärischen Ambitionen. So gibt es eine Zuständigkeits- und Mittelkonkurrenz bei der Cybersicherheit zwischen Militär und Strafverfolgungsbehörden. So fehlen Energie und Geld, die in die Herstellung von Schadsoftware für Cyberangriffe fließen, beim Entwickeln von Schutzmechanismen. So werden Sicherheitslücken, die für Cyberattacken nutzbar sind, als Angriffsoption geheim gehalten, statt sie aufzudecken und zum Schutz der eigenen Zivilgesellschaft zu beseitigen. Gleichzeitig wird dadurch Beihilfe zur Cyberkriminalität geleistet, weil weniger Schwachstellen beseitigt werden, als möglich wäre. Schließlich stehen die militärischen Ziele der Kontrolle, Überwachung und Fähigkeit zu Cyberangriffen im Widerspruch zum zivilen Anspruch auf freien Umgang mit digitalen Medien und Internet.

Cyberkrieg ist global, Cyberabwehr national

Während Angriffswerkzeuge für den Cyberkrieg teilweise im Internet zu finden und oft billiger zu haben sind als konventionelle Waffen, während ihre Handhabung vergleichsweise einfach erlernt werden kann, ist es um die Cyberabwehr – zumindest heute noch – schlecht bestellt. Ein wesentlicher Grund dafür ist, dass Bemühungen um Cybersicherheit überwiegend national organisiert sind, während der Cyberspace mit dem Internet und den Netzen internationaler Konzerne global funktioniert. Die Netze internationaler Firmen ignorieren staatliche Grenzen, die Liefer- und Wertschöpfungsketten sind weltumspannend, eine wachsende Menge relevanter Daten ist in einer „Public Cloud" gespeichert, und die Betreiber kritischer Infrastrukturen beschränken sich auch selten auf nationale Territorien. Nationale Cyberabwehr kann deshalb nicht oder nur sehr eingeschränkt funktionieren.

Cyberkrieg erhöht Kriegsgefahr

Ein besonders bedenklicher Aspekt der Aufrüstung zum Cyberkrieg ist, dass die allgemeine Kriegsgefahr und Kriegsbereitschaft dadurch steigen. Das Department of Defense der Vereinigten Staaten hat im Jahre 2011 die *Strategy for Operating in Cyberspace* herausgegeben, die von der defensiven Schwäche, der immensen Abhängigkeit von funktionierenden IKT-Systemen und die hohe Verletzlichkeit durch Vernetzung, Zentralisierung, Standardisierung und Mobilität geleitet ist.[3] Statt jedoch eine weltweite Cyberabrüstung anzustreben, wird mit Gegenangriffen bei Cyberattacken gedroht. Dabei wird der Einsatz konventioneller Waffen nicht ausgeschlossen – im Gegenteil wird die Eintrittsschwelle sogar sehr niedrig gelegt. Der Begriff Cyberangriff wird sehr weit gefasst und reicht von Denial-of-Service-Attacken und Sabotage von militärischen und zivilen Systemen über die Manipulation und den Diebstahl von Informationen sowie Wirtschaftsspionage bis hin zu Diebstahl geistigen Eigentums. Hacktivismus, Cybercrime und Cyberwarefare werden undifferenziert als Bedrohung der nationalen Sicherheit der USA angesehen und können Gegenangriffe nach sich ziehen. Eine spannende Frage in diesem Zusammenhang ist, welche Auswirkungen das für den Bündnisfall in der NATO hat. Wenn die USA eine Cyberattacke mit Raketen beantworten, müssen sich dann die anderen NATO-Partner an die Seite der USA stellen?

Cyberkrieg im Lichte des Kriegsvölkerrechts

Cyberkriege sind wegen der weltweiten Aufrüstung und weitgehend fehlender Bemühungen um Cyberabrüstung eine reale Gefahr. Deshalb drängt sich die Frage auf, ob und wie das Kriegsvölkerrecht auf Cyberkriege anwendbar ist. Die Fachleute sind sich uneinig. Die einen argumentieren, dass Cyberkriege „reguläre" Kriege sind, so dass das Kriegsvölkerrecht uneingeschränkt gilt und angewendet werden kann. Ein wesentliches Problem wird in diesem Falle darin gesehen, dass der Aggressor bei Cyberattacken nicht immer feststeht und schwer ermittelbar sein kann. Die Gegenposition betont die Besonderheiten von Cyberkriegen, die im Kriegsvölkerrecht in der bisherigen Form nicht berücksichtigt sind, so dass eine Art digitaler Genfer Konvention nötig wäre. Wie Cyberkrieg im Völkerrecht reflektiert ist oder werden kann, muss dringend geklärt werden, wobei auch die Ächtung eine Option ist.[4] In diesem Zusammenhang ist vor allem auch das *Tallinn-Manual* von Bedeutung, das im Auftrag des *NATO Cooperative Cyber Defence Centre* mit Sitz in Tallinn von einem rund zwanzigköpfige Expertengremium von 2009 bis 2012 ausgearbeitet worden ist und das völkerrechtlich gebotene Verhalten von Staaten im Cyberkrieg zum Gegenstand hat.[5]

Cyberrüstung bedroht die Zivilgesellschaft

Durch die weitreichenden und hochentwickelten Möglichkeiten, Cyberangriffe durchzuführen, sind aber nicht nur militärische IKT-Systeme bedroht, sondern staatliche Einrichtungen, Unternehmen und die Bürgerinnen und Bürger insgesamt, wobei diese gezielt oder als Zufallstreffer und Kollateralschaden zu Opfern werden können. Die digitalisierte Gesellschaft als Ganzes ist hochgradig abhängig von kritischen Infrastrukturen wie der Energie- und Wasserversorgung, dem Transportwesen, den Informations- und Kommunikationskanälen und dem Gesundheitssystem. Fast alle dafür eingesetzten Computersysteme sind vernetzt und so von überall her erreichbar. Die kommerzielle Hard- und Software ist in der Regel leicht angreifbar. Die Standardisierung erleichtert und effektiviert Angriffe. Die Komponenten von IKT-Systemen kommen von vielen Herstellern und Lieferanten, so dass kaum kontrollierbar und nachvollziehbar ist, wie sicher sie sind. Mit der überdies wachsenden Komplexität der Systeme und Anwendungen wächst die Häufigkeit von Schwachstellen, Fehlkonfigurationen und unbekanntem Verhalten. Die Sicherheit von IKT-Systemen ist selten ein Designziel bei der Durchführung von Entwicklungsprojekten, der Profit steht im Vordergrund. Das Problem besteht darin, dass kritische Infrastrukturen mit dem Internet verbunden sind, dieselbe Hard- und Software, dieselben Protokolle und Dienste nutzen und dass dieselben Schwachstellen auftreten wie bei allen sonstigen Nutzerinnen und Nutzern der IKT-Technik. Zudem mangelt es den Betreibern von kritischen Infrastrukturen an Sensibilität für die Probleme. Auf der anderen Seite bergen die Versuche des Staates, die Angreifbarkeit der kritischen IKT-Systeme zu mindern, auch Gefahren und Risiken. So bedeutet eine Verschärfung von Sicherheitsgesetzen in der Regel, dass die Freiheit im Internet beeinträchtigt wird.

Cyberpeace statt Cyberwar

Der Gefahr von Cyberkrieg lässt sich nur durch eine konsequente Cyberabrüstung und durch eine Konzeption des Cyberpeace begegnen.

Auf der militärischen Ebene heißt das, Offensivwaffen für den Cyberkrieg zu verbieten und Cybersicherheit rein defensiv auszurichten. Im Sinne einer digitalen Genfer Konvention sollte ebenfalls verboten sein, Cyberangriffe auf kritische Infrastrukturen zu unternehmen. Wirtschaftliche Interessen müssen als legitimer Cyberkriegsgrund ausgeschlossen werden, ebenfalls dürfen ziviler Ungehorsam und Onlineprotest im Internet nicht dafür herhalten. Schließlich sollte es verboten sein, Cyberattacken mit dem Einsatz konventioneller Waffen zu beantworten. Außerdem sollte eine internationale unabhängige Instanz geschaffen werden, die behauptete Cyberangriffe forensisch untersucht, so dass eine verlässliche Zuordnung zu den Verursachern stattfindet und nicht die Falschen als Aggressoren beschuldigt werden können.

Auf der zivilen und politischen Ebene müssten alle staatlichen Stellen, alle Unternehmen und alle Bürgerinnen und Bürger verpflichtet werden, Schwachstellen in IKT-Systemen offenzulegen. Der Betriebserlaubnis kritischer Infrastrukturen müsste immer eine kompetente und transparente Sicherheitsprüfung vorausgehen, die Betreiber müssten die Sicherheit der IKT-Systeme garantieren. Die kritischen Infrastrukturen sollten dezentral und unvernetzt betrieben werden. Wichtig wäre auch, Cybersicherheitsstrategien unter demokratische Kontrolle und unter einen Parlamentsvorbehalt zu stellen. Speziell für Deutschland gilt, dass der Aufbau von Cyberabwehrzentren transparent und demokratisch kontrolliert vollzogen wird, dass die Zentren friedenspolitisch ausgerichtet werden und in ihnen eine strikte Trennung von Polizei, Geheimdiensten und Militär gewahrt wird. Als Unterstützung von Cyberpeace-Initiativen sollte die Bundesregierung die Friedensforschung zur Entwicklung von Strategien zur Befriedung des Cyberspace ausreichend fördern.

Statt eines Schlusses

Die Überlegungen in diesem Beitrag fassen nicht nur das entsprechende Referat des zweiten Autors auf dem Kongress *Quo vadis NATO?* zusammen, sondern sie sind auch stark angelehnt an den Vortrag der ersten Autorin über *Cyberpeace statt Cyber-*

Sylvia Johnigk, Kai Nothdurft und Hans-Jörg Kreowski

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

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

Hans-Jörg Kreowski ist Professor (i. R.) für *Theoretische Informatik* an der Universität Bremen und Vorstandsmitglied des *Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung*. Neben seinen fachlichen Schwerpunkten hat er seit vielen Jahren auch immer wieder zur unheilvollen Verflechtung von Informatik und Rüstung

war auf dem 29. Chaos Communication Congress 2012 (29C3) in Hamburg und folgen teilweise Ausführungen von Sylvia Johnigk und Kai Nothdurft in der FIfF-Kommunikation 1/2012.[6] Auch wenn das Thema Cyberwar nicht zuletzt wegen der immensen weltweiten Cyberaufrüstungen in letzter Zeit große öffentliche Aufmerksamkeit erregt, zeichnet sich die Problematik schon lange ab, wie der Artikel von Ute Berhardt und Ingo Ruhmann im Tagungsband der FIfF-Jahrestagung 1994 beweist.[7]

Dennoch stehen die kritische Auseinandersetzung mit dem Thema Cyberwar und die Entwicklung einer Gegenkonzeption unter dem Motto Cyberpeace noch ganz am Anfang. Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF) organisiert einen Arbeitskreis RUIN (RUestung und Informatik), der sich intensiv mit diesen Fragen beschäftigt. Wer interessiert ist, über die Aktivitäten des AK RUIN informiert zu werden oder mitarbeiten möchte, wende sich bitte an den zweiten Autor (siehe auch die Webseite fiff.de/themen/ruin). Darüber hinaus hat das FIfF gerade die Kampagne *Cyberpeace* gestartet, die durch die *stiftung bridge* gefördert wird. Sie hat zum Ziel, das öffentliche Bewusstsein von der gefährlichen Durchdringung des virtuellen Raumes mit militärischen Aktivitäten zu schärfen und den Widerstand dagegen zu stärken (siehe auch *http://cyberpeace.fiff.de/*).

Anmerkungen

1 *Sandro Gaycken: re:publica XI April 2011 http://re-publica.de/11/blog/panel/cyberwar-und-seine-folgen-für-die-informationsgesellschaft/*

2 *Der Cyberkrieg kann jeden treffen http://www.sueddeutsche.de/digital/sicherheit-im-internet-der-cyber-krieg-kann-jeden-treffen-1.146684 und Wirtschaftswoche: Bundeswehr anfällig für Cyber-Angriffe http://www.wiwo.de/technologie/digitale-welt/bundeswehr-bundeswehr-anfaellig-fuer-cyber-angriffe/7220 974.html*

3 *US Militärdoktrin des DoD: Strategy for Operating in Cyberspace http://www.defense.gov/news/d20110714cyber.*

4 *Spiegel Online: Der Wurm als Waffe http://www.spiegel.de/netzwelt/netzpolitik/experten-suchen-nach-kriegsrecht-fuer-den-cyberwar-a-836566.html, Ein Gegenschlag ist nicht legal http://www.sueddeutsche.de/digital/cyberwar-und-voelkerrecht-ein-gegenschlag-ist-nicht-legal-1.1430089 und Cyberwar: Die UN führen erste Gespräche über eine völkerrechtliche Ächtung http://www.sueddeutsche.de/digital/cyberwar-und-voelkerrecht-ein-gegenschlag-ist-nicht-legal-1.1430089*

5 *Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press 2013*

6 *Sylvia Johnigk und Kai Nothdurft: Cyberwarfare – Aufrüstung im Cyberspace als Herausforderung für die Friedensarbeit des FIfF, FIfF-Kommunikation 1/2012, S. 41–45*

7 *Ute Bernhardt und Ingo Ruhmann: Information als Waffe: Netwar und Cyberwar – Kriegsformen der Zukunft, in: Hans-Jörg Kreowski et al. (Hrsg): Realität und Utopien der Informatik, agenda-Verlag Münster 1995, S. 104–119*

Lesen & Sehen

Neues für Bücherwürmer & Cineasten

Rosemarie Will und Sven Lüders für die Redaktion der vor*gänge*

Meinungsfreiheit in Zeiten der Internetkommunikation

Editorial zu vor*gänge* – Zeitschrift für Bürgerrechte und Gesellschaftspolitik – Nummer #225/226

Unser Grundgesetz kennt eigentlich keine Hierarchie der Grundrechte. In ihm stehen die freie Rede wie der Schutz der Vertraulichkeit, die Religionsfreiheit und die Gleichberechtigung sowie viele andere Werte nebeneinander. Unter all diesen Verfassungswerten kommt der Meinungsäußerungsfreiheit eine grundlegende Bedeutung zu, sie ist mehr als nur ein Grundrecht unter den anderen. So betont auch das Bundesverfassungsgericht in seinen Entscheidungen immer wieder, dass die Meinungsäußerungsfreiheit für die Freiheit und die Demokratie schlechthin konstitutiv sei.

Wo und wie sich diese Freiheit jeweils verwirklichen kann, welchen potenziellen Einschränkungen und Gefährdungen sie ausgesetzt ist, unterliegt wie bei allen Grundrechten dem gesellschaftlichen Wandel – sowohl der Wertevorstellungen, Normen und politischen Gegebenheiten, aber auch ihrer technischen Bedingungen. Mit der zunehmenden Verlagerung der öffentlichen Kommunikation in den digitalen Raum stellen sich daher auch für die Meinungsfreiheit neue Fragen: Was bedeutet es, wenn Kommunikation die Flüchtigkeit des gesprochenen Wortes verliert und immer mehr digitale Spuren hinterlässt? Wie sollen wir mit der zunehmenden kommunikativen wie lebensweltlichen Abschottung einzelner Subkulturen, mit *Hate Speech* und *Fake News* umgehen? In welchem Maß beeinflussen Netzwerke und ihre Newsalgorithmen heute unsere Wahrnehmung und Kommunikationsbeziehungen? Mit diesen Fragen digitalisierter Kommunikation befasst sich die vorliegende Ausgabe der vorgänge. Unsere AutorInnen suchen bürgerrechtliche Antworten darauf, welche Chancen und Gefahren sich für die Meinungsfreiheit unter den Bedingungen digitaler, vernetzter Kommunikation ergeben.

Den Schwerpunkt eröffnet Patrick Donges mit einem Beitrag, der die Entwicklung der Internetkommunikation bis zur Entstehung von Social Media kommunikationswissenschaftlich einordnet. Donges macht drei Faktoren aus, die die Kommunikation und die medialen Inhalte im Netz heute prägen: Digitalisierung,

Personalisierung und neue Gatekeeper. Die Digitalisierung befördere vor allem die Quantifizierung und Bewertung aller Inhalte, erlaube aber auch deren schnelle Weitergabe und (nahezu beliebige) Neu-Komposition: niemand muss heute mehr eine ganze Zeitung abonnieren, von der er oder sie sich nur für den Wirtschaftsteil interessiert. Daneben etabliere das Netz eine neue Form der Kommunikation, die an eine breite Öffentlichkeit gerichtet sei, sich aber durch eine Personalisierung ihrer Inhalte und ihrer Ansprache mehr und mehr dem Stil klassischer Individualkommunikation annähere. Schließlich löse das Netz die Unterteilung der klassischen Massenmedien in Produzierende (z. B. JournalistInnen) und Konsumierende (LeserInnen) auf bzw. führe mit den Social-Media-Anbietern neue Formen der Nachrichtenmittler ein, die zwischen diesen beiden Polen anzusiedeln sind.

Till Köstler knüpft daran an und versucht eine genauere Begriffsbestimmung Sozialer Netzwerke: Er geht auf die sozial- und kommunikationswissenschaftlichen Netzwerkdebatten ein, die deutlich älter als Facebook & Co sind und in denen besondere Merkmale und Funktionen dieser Netzwerke hervorgehoben wurden. Dies kontrastiert er mit der juristischen Netzwerk-Diskussion, die in Deutschland ihren vorläufigen Höhepunkt mit dem Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) erreicht hat. Demnach handelt es sich um eine besondere Form von Telemediendienstanbietern, die sowohl von der Individualkommunikation (etwa per E-Mail), aber auch von journalistisch gestalteten Telemedien (z. B. Nachrichtenwebseiten) und vom klassischen Rundfunk abzugrenzen ist. Köstler zeigt, dass die im NetzDG verankerte Legaldefinition der Netzwerkanbieter noch einige Abgrenzungsprobleme aufwirft, wer unter den Anwendungsbereich dieses Gesetzes fällt und wer nicht – etwa wenn die Gewinnerzielung oder die journalistische Gestaltung von Inhalten zu entscheidenden Kriterien werden. Dies wirke sich auch auf die Frage auf, welche grundrechtlichen Schutzbereiche für die Netzwerke bzw. die dahinterstehenden Anbieter anzuwenden sind. Zugleich sieht er den aktiven Einfluss, den die Betreiber über ihre AGBs und die Algorithmen auf die Verteilung (bzw. Unterschlagung) von Nachrichten ausüben, in der rechtlichen Regulierung bisher nicht hinreichend berücksichtigt – das NetzDG behandle die Firmen wie klassische Telefonanbieter, als würden diese gewissermaßen nur „Leitungen" und „Pinnwände" für die NutzerInnen bereitstellen, was aber erkennbar zu kurz greift.

Während die ersten Beiträge den innovativen und teilweise auch emanzipatorischen Charakter der Sozialen Netzwerke betonen, folgt jetzt ein Perspektivwechsel: Wir widmen uns den Problemen und Gefahren, die mit der Ausweitung der Internetkommunikation verbunden sind. Stefan Hügel stellt in seinem Text die Diskussion um die Macht und Reichweite Künstlicher Intelligenz (KI) sowie deren Kontrolle vor. Nach seiner Darstellung korrespondiert ein übertriebener Glaube an eine allmächtige, starke KI („die wissenden Maschinen") mit einem defizitären Verständnis von der realen Wirkungsweise und Einbettung von Algorithmen in unserem technisierten Alltag. Einerseits sei das, was heute unter dem Label „KI" vermarktet werde, längst noch nicht so intelligent, wie es die Visionen intelligenter Automaten nahelegen. Auf der anderen Seite werden die tatsächlichen Folgen der Datafizierung, die sich in nahezu allen Wirtschafts- und Lebensbereichen breit macht, eindeutig unterschätzt. Hügel beschreibt, welche gesellschaftlichen Folgen (etwa neue Formen der Diskriminierung) die verschiedenen „Lernformen" der KI bereits heute haben und wie sich einzelne Techniken auf z. B. Kriegsführung, politische Kommunikation oder Wahlen auswirken. Die Lösung dieses Dilemmas sieht Hügel in einem weiter entwickelten Datenschutz – denn jener schütze nicht nur die Befindlichkeiten der Einzelnen, sondern biete in seiner Gesamtheit auch die Gewährleistung dafür, dass grundlegende Freiheiten wie die Meinungs- oder Handlungsfreiheiten unter digitalen Bedingungen erhalten bleiben.

Als ein weiteres Problem wird in den Netzdebatten immer wieder die Möglichkeit einer anonymisierten Teilnahme benannt: Sie verleite einerseits TeilnehmerInnen zu verbalen, persönlichen Angriffen und zersetze den öffentlichen Diskurs. Andererseits wird in ihr ein zentrales Hindernis für die effektive Rechtsdurchsetzung bzw. die Strafverfolgung im Netz angesehen, weil die UrheberInnen nicht zu ermitteln sind bzw. potenzielle Beweismittel fehlen. Der Beitrag von Michael Kuhn greift dieses Thema mit dem umstrittenen „Recht auf Anonymität" im Digitalen auf. Kuhn zeigt, dass das Recht auf Anonymität eine zentrale Dimension des Grundrechtsschutzes berührt. Er skizziert die Bedingungen für Anonymität im digitalen Raum und weist nach, dass Anonymität kein neues Problem ist, das erst mit der Digitalisierung entsteht. Nach seiner Darstellung enthalten auch die Grundrechtskonzepte für die analoge Welt implizite Annahmen zur Anonymität, ohne dass das Verfassungsrecht bisher ein umfassendes Konzept von Anonymität herausgearbeitet habe. Ein solches Konzept sei aber dringend nötig, um das Verhältnis von Anonymität und Identifizierbarkeit im digitalen Raum so austarieren zu können, damit die Schutzwirkung der Grundrechte auch hier zur Geltung komme.

Nach den eher grundsätzlichen Beiträgen widmet sich der Schwerpunkt dem deutschen NetzDG, seiner konkreten Anwendung und der Kritik daran. Zunächst stellen wir einige Zahlen zur bisherigen Anwendung des Gesetzes auf den drei Plattformen Facebook, Google und YouTube vor. Bisher gilt das NetzDG aufgrund seiner Definition des Anwendungsbereichs in § 1 Abs. 2 NetzDG (mind. 2 Millionen angemeldete NutzerInnen) nur für diese drei Plattformen – alle anderen sind kleiner. Als das Gesetz 2017 beraten und verabschiedet wurde, gab es von vielen Seiten Kritik an dessen Regulierungsansatz. Was ist davon zwei Jahre später übrig geblieben, welcher Nachbesserungsbedarf zeigt sich aus der ersten Rechtsprechung zum Gesetz? Dazu befragten wir Martin Eifert und Ulf Buermeyer. In ihrer Bewertung des Gesetzes gehen sie von den besonderen Grundrechtsgefährdungen aus, die sich aus den speziellen Kommunikationsbedingungen im Social Web ergeben. Dazu gehöre, dass die Plattformen in einem großen Maße die Aufmerksamkeit des digitalen Publikums lenken (sie bestimmen, wer, wann was liest), dass ihnen eine Dynamik zur Monopolbildung innewohnt (denn mit der Zahl ihrer NutzerInnen bzw. LeserInnen steigt zugleich der Informationswert der dort verbreiteten Nachrichten) und dass ihre Techniken der Informationsverteilung zu einer Beschleunigung führen, aus der sich die spezielle Dynamik digitaler Aufmerksamkeit mit ihren hochfrequenten Erregungskurven ergibt.

Daran anschließend stellt Hubertus Gersdorf eine Klage gegen das NetzDG vor. Gersdorf ist Bevollmächtigter einer Feststellungsklage der beiden FDP-Politiker Jimmy Schulz und Manuel Höferlin, die jene im Juni 2018 beim Verwaltungsgericht

Köln eingereicht haben. Sie sehen durch das NetzDG ihre Meinungsfreiheit erheblich eingeschränkt und kritisieren die in vielerlei Hinsicht unzureichenden Regelungen des Gesetzes, etwa die fehlenden Verfahrensvorgaben für die Löschung von Beiträgen, für die Überprüfbarkeit der Entscheidungen oder die Bußgeldsanktionen gegenüber den Betreibern.

Matthias Spielkamp weist in seinem Beitrag auf ein weiteres Problem hin: die Nachahmer, die das NetzDG in autokratischen Staaten gefunden hat. So wurde das Gesetz beispielsweise in Russland, Malaysia sowie auf den Philippinen als Vorbild genommen – nur dass die vergleichbaren Regelungen unter anderen Vorzeichen dort eine unheilvolle Wirkung entfalten. Diese Beispiele zeigen, wie leicht sich derartige Gesetze für eine politische Beschränkung der Meinungsfreiheit nutzen lassen – wovor auch Deutschland nicht gefeit ist. Vor dem Hintergrund zunehmender nationaler Debatten um die Regulierung sozialer Netzwerke hat Facebook vor einiger Zeit einen Vorschlag vorgelegt, der mit Hilfe Künstlicher Intelligenz und eines externen Beirats eine Art regulierte Selbstregulierung zur Kontrolle der Inhalte vorschlägt. Mit diesem Vorschlag setzt sich Spielkamp kritisch auseinander, denn sie gewährleiste keine hinreichende Transparenz und belasse die letztliche Entscheidung weitgehend der Firma.

Dass Handlungsbedarf bei der Anpassung des NetzDG besteht, wird mittlerweile kaum bestritten – die Debatte um dessen Zukunft hat längst begonnen. Was sich die im Bundestag vertretenen Oppositionsparteien in dieser Hinsicht wünschen, fassen wir in einer weiteren Dokumentation zusammen. Der Rechtsausschuss des Deutschen Bundestags führte dazu am 15. Mai eine Sachverständigenanhörung[1] durch. Welche der genannten Vorschläge zur Reform oder gar Abschaffung des Gesetzes eine Chance haben, ist derzeit jedoch offen.

Auf die französischen Versuche, Fake News einzudämmen, sowie die europäischen Regulierungsansätze geht Jörn Reinhardt ein. Er stellt zunächst die verschiedenen Formen der Manipulation öffentlicher Debatten in den Sozialen Netzwerken vor. Im Gegensatz zum NetzDG, welches sich auf die Löschung beleidigender oder anderweitig strafbarer Inhalte beschränkt, zielt das französische „Gesetz gegen die Manipulation von Information" stärker darauf, die Verbreitung von Falschinformationen zu unterbinden. Dies schränkt – im Vergleich zur deutschen Rechtsprechung über die Grenzen der Äußerungsfreiheit – die Meinungsfreiheit deutlich stärker ein und ist aus grundrechtlicher Sicht daher besonders problematisch.

Den Abschluss des Schwerpunkts bilden zwei Beiträge, die sich mit den politischen Alternativen befassen: Patrick Breyer und Katharina Nocun verdeutlichen zunächst, welches Überwachungspotenzial in Netzwerken wie Facebook und Co. steckt. Dies beschränkt sich längst nicht mehr darauf, die Interessen und Vorlieben der NutzerInnen für Werbezwecke zu erfassen – vielmehr werden auch deren Kommunikationsbeziehungen und Vernetzungen untereinander erfasst. Das Tragische daran: Die gesamte digitale Welt an Freundschaften, Bekanntschaften und Netzwerken, in der sich viele Menschen heute wie in einer zweiten Heimat zuhause fühlen, kann Facebook nicht nur beliebig manipulieren (Wer kann mit wem in Kontakt treten?), sondern im Ernstfall sogar auf Knopfdruck beenden. Breyer und Nocun sehen anbietergesteuerte Netzwerke deshalb als Gated Communities, die es dringend durch alternative Formen zu ersetzen gelte. Welche Möglichkeiten es dafür heute gibt, stellen sie in ihrem Beitrag kurz vor.

Mindestanforderungen an eine Regulierung der digitalen Welt dokumentieren wir mit einem Forderungskatalog, den die Beteiligten des 2018 veranstalteten Kongresses *Bits und Bäume* in Berlin vorgelegt haben. Er beschränkt sich nicht auf partizipative Mitgestaltung und demokratische Kontrolle der Netzwerke, sondern hat auch die ethischen und ökologischen Folgen der Digitalisierungstechnik im Blick.

Außerhalb des eigentlichen Schwerpunkts, aber zugleich als historischer Kontext der Debatte um die Meinungsfreiheit im Internet, ist der Beitrag von Helga und Wolfgang Killinger zu verstehen: Sie bieten einen kurzen Abriss der bundesdeutschen Auseinandersetzungen um die Meinungsfreiheit im Rundfunk. Sie schildern die Stationen dieser Geschichte anhand des Engagements der Humanistischen Union, die sich seit ihren Gründungstagen für die Meinungsfreiheit in diesem Medium eingesetzt hat.

Einen weiteren grundrechtsorientierten Rückblick unternimmt Rolf Gössner, der anlässlich des 70. Jahrestages des Grundgesetzes eine kritische Bilanz zur Verfassungswirklichkeit in Deutschland zieht. Er beschreibt in seiner Jubiläumsrede die Etappen der sicherheitspolitischen Aufrüstung der Bundesrepublik. Deren aktuelle Auswüchse schildert Clemens Arzt am Beispiel des Brandenburgischen Polizeigesetzes, wo die rot-rote Landesregierung nach den Vorbild Bayerns, Baden-Württembergs, NRWs und anderer Bundesländer kürzlich mit Verweis auf die „angespannte

Terror- und Gefährdungslage“ neue bzw. erweiterte Befugnisse einführte. Sowohl die Frage, ob diese Regelungen wirklich erforderlich sind, noch bei der Frage, ob sie auch geeignet sind, mehr Sicherheit für die BürgerInnen zu schaffen, sieht er im Einzelnen erhebliche Zweifel.

Mit Brandenburg befasst sich schließlich auch der Beitrag von Rosemarie Will: Sie wagt einen Blick nach vorn und diskutiert das Brandenburger Gesetz zur Parität bei den Landeswahllisten. Die kürzlich beschlossene Reform des Landeswahlrechts schreibt erstmals in Deutschland eine stärkere Repräsentation von Frauen in einem deutschen Landesparlament gesetzlich vor, indem die brandenburgischen Parteien ab 2020 zur geschlechterparitätischen Aufstellung der Landeswahllisten verpflichtet werden. Entsprechend heftig fielen die Angriffe auf den Vorschlag aus, die KritikerInnen sehen in ihm das Ende vom Grundsatz der freien Wahlentscheidung. Will stellt eine verfassungsrechtliche Interpretation dieses Gesetzes vor, mit dem 100 Jahre nach der Einführung des Frauenwahlrechts ein wichtiger Meilenstein auf dem Weg zu mehr Gleichberechtigung erreicht wird.

Der Beitrag von Katharina Nocun und Patrick Breyer ist auch in dieser Ausgabe der FIfF-Kommunikation ab Seite 10 abgedruckt.

Anmerkung

1 *Stellungnahmen der Sachverständigen siehe https://www.bundestag.de/ausschuesse/a06_Recht/anhoerungen_archiv/netzwerkdurchsetzungsgesetz-628712.*

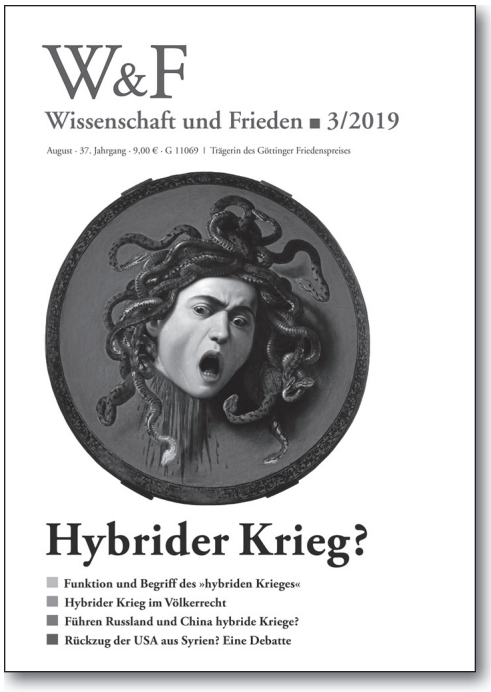
Wissenschaft & Frieden 3/2019 „Hybrider Krieg?“

Wird in Sicherheitsdiskursen von *hybrider Kriegsführung* gesprochen, bleibt oft vage, worum es eigentlich geht: die Verschmelzung ziviler und militärischer Kampfformen, asymmetrische Kampfführung gegen einen Gegner, der im konventionellen Sinne überlegen ist, die Taktiken Russlands in der Ukraine oder gar Cyberkrieg? Was die verschiedenen Konzepte und Sichtweisen eint, ist meist der Ruf nach Gegenmaßnahmen, Aufrüstung und mehr Geld. W&F 3/2019, „Hybrider Krieg?“, untersucht verschiedene Aspekte dieser Art der Kriegsführung, vom Begriff selbst und seiner Funktion bis hin zur völkerrechtlichen Einstufung.

Es schreiben:

- *Wolfgang Schreiber*: Hybride Kriegführung – Die Diffusion eines Begriffs
- *Jürgen Scheffran*: Formen hybrider Kriege – Zwischen Ambivalenz und Komplexität
- *Ina Kraft*: Hybrider Krieg – Zu Konjunktur, Dynamik und Funktion eines Konzepts
- *Hans-Georg Ehrhart*: Russlands „hybride Kriegführung“
- *Doris Vogl*: Volksrepublik China – Zivilisationsanspruch und Wahrnehmung hybrider Bedrohung
- *Michael Bothe*: „Hybride“ Konflikte im Völkerrecht
- *Dirk Freudenberg*: Hybride Kriegführung in urbanen Zentren – Relevanz für die zivile Verteidigung
- *Bernhard Koch*: Der Raum dazwischen – Hybrider Krieg und die „revisionistische Theorie des gerechten Krieges“

Außerhalb des Heftschwerpunkts wird die Frage eines Rückzugs der USA aus Syrien kontrovers diskutiert, die Situation in Venezuela beleuchtet, die Zeit nach dem INF-Vertrag reflektiert und ein neues Projekt am Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg vorgestellt.



Wissenschaft & Frieden, 3/2019: „Hybrider Krieg?“, 9,00 € Inland, EU plus 3,00 € Porto (Bitte um Vorkasse: Sparkasse Köln-Bonn, DE86 3705 0198 0048 0007 72, SWIFT-BIC COLSDE33XXX)

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

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

Wissenschaft und Frieden ist Trägerin des Göttinger Friedenspreises 2018

In eigener Sache

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

Politische Arbeit kostet Geld, viel Geld – für Öffentlichkeitsarbeit, Aktionen und Organisation. Unsere jährlich stattfindende FIfF-Konferenz, der Weizenbaum-Preis, weitere Publikationen, Kommunikation im Web: Neben der tatkräftigen Unterstützung 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, die Euch und uns wichtig sind, weiter verstärken.

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

Aufruf zur Teilnahme an der FIfF-Konferenz 2019

Das Bild wurde von Caroline von Totth gezeichnet nach einer Idee von Karin Vosseberg.

1956 traf sich eine kleine Gruppe junger Wissenschaftler – später alle berühmte Vertreter ihres Faches – für einige Wochen im Dartmouth-College und begründete dort gemeinsam das Gebiet der *Künstlichen Intelligenz* (KI). Ihr erklärtes Ziel war, Computersysteme zu entwickeln, die Leistungen erbringen können, für die Menschen ihre Intelligenz einsetzen wie logisches Schließen, Planen, Lernen, Textverstehen, … In einem Auf und Ab zwischen massiv zunehmender und stark abnehmender staatlicher Förderung – teils auch ganz erheblich im militärischen Kontext – kristallisierte sich allmählich die KI als ein wichtiges Teilgebiet der Informatik heraus.

Dessen anfänglichen Ziele gelten auch heute noch; dessen wesentlichen Methoden wie neuronale Netzwerke sind meist auch schon seit Jahrzehnten bekannt. In jüngster Zeit aber verzeichnet die KI durch die erreichte Rechengeschwindigkeit und Speicherkapazität äußerst bemerkenswerte technologische Erfolge bei Spielen wie Schach, Go, Poker und Starcraft und bei praktischen Anwendungen wie Sprach- und Bildverarbeitung. So weit, so gut.

Aber mit dem erreichten Stand der KI sind auch übertriebene Erwartungen, übersteigerte Hoffnungen und höchst problematische Anwendungsmöglichkeiten verbunden. KI wird von Politik und Wirtschaft weltweit als Schlüsseltechnologie gesehen, von der die zukünftige Wertschöpfung abhängt und die einen signifikanten Teil der heutigen Arbeitsplätze obsolet werden lassen könnte. Die sich abzeichnenden Anwendungen im militärischen Kontext führen zu einer gigantischen Rüstungsspirale, was die Gefahr von Kriegen wohl kaum verringern wird. KI-basierte Überwachungsmethoden lassen tiefe Eingriffe in die Privatsphäre und andere Grundrechte befürchten bis hin zu einer sozialen Totalüberwachung, wie sie in China auf der Tagesordnung steht. Selbst Allmachts- und Weltbeherrschungsphantasien gründen sich auf eine angestrebte Führungsrolle in der KI. Einige KI-Vertreter gehen noch viel weiter und propagieren die Entwicklung einer Superintelligenz, die nicht nur ähnliche Leistungen erbringt wie menschliche Intelligenz, sondern diese sogar in Gänze übertrifft.

Es ist also dringend geboten, das tatsächlich Mögliche und Wünschenswerte vom Märchenhaften, Fantastischen und Schreckeneinflößenden zu trennen. Die FIfF-Konferenz 2019 vom 22. bis 24. November in Bremen bietet dafür eine Plattform. Die Auftaktveranstaltung am Freitag findet mit zwei oder drei Vorträgen im Überseemuseum direkt neben dem Hauptbahnhof statt. Sie beginnt um 18 Uhr und endet mit einem kleinen Empfang. Am Samstag und Sonntag geht die Konferenz in der Universi-

tät Bremen weiter. Am Samstag stehen sechs oder sieben Vorträge, einige parallele zweistündige Arbeitsgruppen, die Verleihung des Weizenbaum-Studienpreises und der FIfF-Bericht auf dem Programm. Der Tag klingt mit einem netten Beisammensein aus. Der Sonntag beginnt mit zwei weiteren Vorträgen, die aus aktuellem Anlass Umwelt- und Klimaschutzprobleme in die Diskussion einbeziehen sollen. Er endet mit der FIfF-Mitgliederversammlung, zu der auch Nichtmitglieder herzlich willkommen sind. Als besonderes Highlight wird es am Freitag eine halbstündige Aufführung des Theaters der Versammlung geben.

Wir können uns auf folgende Vorträge freuen:

- *Marie-Luise Abshagen* und *Nelly Grotefendt* (Forum Umwelt und Entwicklung): Nachhaltige Digitalisierung – Wunschdenken oder Realität?
- *Capulcu*: Künstliche Intelligenz – Bereicherung oder digitalisierte Bevormundung?
- *Alexander von Gernler* (Vizepräsident der GI): Geschlossene Gesellschaft – Von der Verantwortung der Informatik
- *Marit Hansen* (Datenschutzbeauftragte von Schleswig-Holstein): Die Empfehlungen der Datenethikkommission: Bedeutung für die Informatik
- *Matthias Monroy* (Wissensarbeiter, Aktivist und Mitglied der Redaktion der Zeitschrift Bürgerrechte & Polizei/CILIP): Die Militarisierung der Festung Europa und wie europäische Rüstungskonzerne daran verdienen
- *Rainer Rehak* (Weizenbaum-Institut und FIfF-Vorstand): Folgenreiche Verführung – Begriffskritik autonomer und intelligenter Systeme
- *Elke Schwarz* (Queen Mary University London): Silicon Valley zieht in den Krieg: KI, autonome Waffen und politisch-moralische Verkümmerung
- *Bernhard Stoevesandt* (Scientists for Future): Wird KI die Welt retten?
- *Veronika Thiel* (AlgorithmWatch): Viel Lärm um Wenig: Ethische Richtlinien in der Algorithmenentwicklung
- *Dominik Wetzel* (freier Journalist, Tübingen) und Christoph Marischka (Informationsstelle Militarisierung): Die Produktionsbedingungen künstlicher Intelligenz

Die FIfF-Konferenz ist öffentlich und alle Interessierten sind herzlich willkommen. Alle Veranstaltungsräume sind mit dem Rollstuhl über einen Fahrstuhl erreichbar. Der Eintritt ist frei. Für Verpflegung wird am Wochenende gegen einen Unkostenbeitrag gesorgt. Um besser planen zu können, bitten wir um unverbindliche Anmeldung unter *2019.fiffkon.de*.

Wir wollen auch Kinderbetreuung anbieten. Dazu ist eine verbindliche Anmeldung bis zum 31. Oktober per E-Mail an *ingrid.schlagheck@fiff.de* erforderlich.

Das Vorbereitungsteam der FIfFKon2019 freut sich auf Euren Besuch.

Einladung zur Mitgliederversammlung 2019

des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF e. V.)

Wir laden fristgerecht und satzungsgemäß zur ordentlichen Mitgliederversammlung 2019 ein.
Sie findet am Sonntag, den 24. November 2019, von 12:00 bis (maximal) 15:00 Uhr statt.
Adresse: Universität Bremen, Raum MZH 1090, Bibliothekstr. 5, 28359 Bremen

Vorläufige Tagesordnung

1. Begrüßung, Feststellung der Beschlussfähigkeit und Festlegung der Protokollführung
2. Beschlussfassung über die Tagesordnung, Geschäftsordnung und Wahlordnung
3. Bericht des Vorstands einschließlich Kassenbericht
4. Bericht der Kassenprüfer
5. Diskussion der Berichte
6. Entlastung des Vorstands
7. Neuwahl des Vorstands
8. Neuwahl der Kassenprüfer
9. Diskussion über Ziele und Arbeit des FIfF, aktuelle Themen, Verabschiedung von Stellungnahmen, Berichte aus den Regionalgruppen
10. Anträge an die Mitgliederversammlung
    Anträge müssen schriftlich bis drei Wochen vor der Mitgliederversammlung bei der FIfF-Geschäftsstelle eingegangen sein
11. Verschiedenes

gez. Stefan Hügel
für den Vorstand und die Geschäftsstelle des FIfF

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** (Hamburg); Prof. Dr. **Klaus Fuchs-Kittowski** (Berlin); Prof. Dr. **Michael Grütz** (Konstanz); Prof. Dr. **Thomas Herrmann** (Bochum); Prof. Dr. **Wolfgang Hesse** (Marburg); Prof. Dr. **Wolfgang Hofkirchner** (Wien); Prof. Dr. **Eva Hornecker** (Weimar); **Werner Hülsmann** (Konstanz); **Ulrich Klotz** (Frankfurt); 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); **Werner Mühlmann** (Oppung); Prof. Dr. **Frieder Nake** (Bremen); Prof. Dr. **Rolf Oberliesen** (Bremen); 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** (Waldorfhäslach)

FIfF-Vorstand

Stefan Hügel (Vorsitzender) – Frankfurt am Main
Rainer Rehak (stellv. Vorsitzender) – Berlin
Michael Ahlmann – Kiel / Blumenthal
Sylvia Johnigk – München
Benjamin Kees – Berlin
Prof. Dr. **Hans-Jörg Kreowski** – Bremen
Prof. Dr. **Dietrich Meyer-Ebrecht** – Aachen
Kai Nothdurft – München
Jens Rinne – Mannheim
Prof. Dr. **Britta Schinzel** – Freiburg im Breisgau
Ingrid Schlagheck – Bremen
Anne Schnerrer – Berlin
Prof. Dr. **Werner Winzerling** – Fulda
Prof. Dr. **Eberhard Zehendner** – Jena

FIfF-Geschäftsstelle

Ingrid Schlagheck (Geschäftsführung) – Bremen

Impressum

Herausgeber	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF)
Verlagsadresse	FIfF-Geschäftsstelle Goetheplatz 4 D-28203 Bremen Tel. (0421) 33 65 92 55 *fiff@fiff.de*
Erscheinungsweise	vierteljährlich
Erscheinungsort	Bremen
ISSN	0938-3476
Auflage	1 200 Stück
Heftpreis	7 Euro. Der Bezugspreis für die FIfF-Kommunikation ist für FIfF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FIfF-Kommunikation für 28 Euro pro Jahr (inkl. Versand) abonnieren.
Hauptredaktion	Dagmar Boedicker, Stefan Hügel (Koordination), Sylvia Johnigk, Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht, Ingrid Schlagheck
Schwerpunktredaktion	Michael Ahlmann, Sylvia Johnigk, Hans-Jörg Kreowski und Kai Nothdurft
V.i.S.d.P.	Stefan Hügel
FIfF-Überall	Beiträge aus den Regionalgruppen und den überregionalen AKs. Aktuelle Informationen bitte per E-Mail an *hubert.biskup@gmx.de*. Ansprechpartner für die jeweiligen Regionalgruppen finden Sie im Internet auf unserer Webseite *https://www.fiff.de/regionalgruppen*
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	Links: BigBrotherAward (Symbolbild) Rechts: Prototyp von Boston Dynamics „Atlas“, Quelle: Defense Advanced Research Projects Agency (DARPA), 2013
Druck	Meiners Druck, Bremen

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

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

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

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

Aktuelle Ankündigungen

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

FIfFKon19 „Künstliche Intelligenz als Wunderland“
22.–24. November, Universität Bremen,
Raum MZH 1090, Bibliothekstr. 5, 28359 Bremen

FIfF-Mitgliederversammlung
24. November von 12:00 bis (maximal) 15:00 Uhr in Bremen

FIfF-Kommunikation

4/2019 „Überwachungsgesamtrechnung“
Dagmar Boedicker u. a.
Redaktionsschluss: 1. November 2019

1/2020 „Künstliche Intelligenz als Wunderland“
Michael Ahlmann, Hans-Jörg Kreowski u. a.
Redaktionsschluss: 7. Februar 2020

W&F – Wissenschaft & Frieden
3/18 Gender im Visier
4/18 Kriegsführung 4.0
(mit Dossier 87: AfD, PEGIDA & Co.)
1/19 70 Jahre NATO
2/19 Partizipation – Basis für den Frieden
(mit Dossier 89: Verifikation nuklearer Abrüstung)
3/19 Hybrider Krieg?

vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik
#223 Bürgerrechte im Sport
#224 Der Osten als Vorreiter? Rechtspopulismus im Gefolge wirtschaftlicher und politischer Umbrüche
#225/226 Wandel der Kommunikationsfreiheit durch Digitalisierung und Internet
#227 Polizei und Technikeinsatz

DANA – Datenschutz-Nachrichten
4/18 Technischer Datenschutz
1/19 Social Media
2/19 Ein Jahr DSGVO – ein Résumé
3/19 Real Time Bidding
4/19 Datenschutz in Zeiten des Brexit

Das FIfF-Büro

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

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

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

Schluss FIfF

Passend zum Schwerpunkt Cyberpeace und IT-Sicherheit in diesem Heft belegt das Foto, dass die Forderung nach Cyberpeace auch im Rahmen des Protests gegen den Drohnen- und Tornado-Standort Jagel erhoben wird.

Beim letzten Ostermarsch in Jagel – Foto: Ralf Cüppers, CC BY-SA 3.0

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