DELETE
digitalisierte Fremdbestimmung

Hefte zur Förderung des Widerstands gegen den technologischen Angriff

BAND IV: DELETE – DIGITALISIERTE FREMDBESTIMMUNG

capulcu productions | Dezember 2018
V.i.S.d.P. E. Schmidt | Am Zuckerberg 14 | 21984 Silikontal

Das çapulcu redaktionskollektiv untersucht in DELETE! die aktuelle Transformation des Kapitalismus – und damit auch der Machtverhältnisse – durch den ›technologischen Angriff‹.

Der Einfluss der Tech-Giganten auf die Ökonomisierung der entlegensten Lebensbereiche nimmt stetig zu, während klassische politische Institutionen an Bedeutung verlieren. Soziale Punktesysteme verlängern mit ihrem permanenten ›Rating‹ und ›Scoring‹ die Reichweite der lenkenden Disziplinierung weit über die direkte Ausbeutung im Arbeitsverhältnis hinaus.

Doch mit welchen Methoden und Zukunftsvisionen überformen Unternehmen wie Facebook, Google, Amazon & Co. unsere Kommunikation und unser Denken? Wie verändern sich angesichts einer zunehmend digitalisierten Fremdbestimmung die Bedingungen für Autonomie und soziale Revolte? Und wie lässt sich die beabsichtigte Vereinzelung und Entsolidarisierung bekämpfen?

Im Zentrum des Heftes steht erneut die Selbstbehauptung, also der vielfältige Widerstand gegen den umfassenden technologischen Angriff. „Wir fällen nicht das lächerliche Urteil, dass die Technologie schlecht ist. Aus welcher - ohnehin historisch bedingten – Ethik heraus denn auch? Wir sagen, sie ist Gewalt und sozialer Krieg. Unsere Kritik richtet sich gegen die technologische Aneignung von Lebensprozessen."

Eine digitale Version dieses Heftes sowie der Bände I – III findet ihr auf unserer Webseite:

https://capulcu.blackblogs.org

Inhalt

3 EINLEITUNG

5 AN ALLE PRODUKTIVKRAFT-, TECHNIK- UND FORTSCHRITTSFETISCHIST*INNEN:

7 KRISE DER POLITISCHEN REPRÄSENTATION

11 DER TECHNOLOGISCH-MILITÄRISCHE ANGRIFF

16 DIGITALER KOLONIALISMUS

19 THE HACKER WAY

21 EXECUTING COMMAND

24 WEIBLICHE SPRACHASSISTENTEN

26 BLOCKCHAINS – SOFTWARE ALS POLITK

30 KORRELATION STATT KAUSALITÄT

33 PREDICTIVE POLICING

36 GEFANGEN IN DER GESUNDHEITS-ASSISTENZ

45 STRATEGIEN IM WIDERSTAND

48 DOKUMENTIERTE WIDERSTÄNDE

70 GLOSSAR

Einleitung

SUCHEND SCHREITEN WIR VORAN

Wir beschäftigen uns in der Serie unserer bisherigen Publikationen „Disconnect“ – „Disrupt“ – „Delete“ mit unterschiedlichen Schwerpunkten: Während wir in „Disconnect“ eine eher phänomenologische Betrachtung versuchten, wo und wie der technologische Angriff bereits jetzt in unserem Alltag gegen unsere Selbstbestimmung wirkt, widmeten wir uns in „Disrupt“ tiefer den Lenkungsmechanismen des Digitalismus. Mit den Texten in diesem Heft „Delete“ wollen wir verschiedene Aspekte der Transformation von Herrschaft in den Fokus nehmen. Wie verändern sich die Bedingungen für Autonomie in Zeiten digitalisierter Fremdbestimmung?

Im Zentrum von „Delete“ steht wie auch schon bei „Disrupt“ die Selbstbehauptung, also der auch jetzt schon erkennbare vielfältige Widerstand gegen diesen umfassenden technologischen Angriff. Wir werben damit für die Verbreiterung einer praktischen Technologiekritik im Sinne einer expliziten Herrschaftskritik.

Wir bleiben damit in diesem neuen Heft dem technologischen Angriff in unsystematischer Weise auf der Spur. Ein vorgeblicher „roter Faden“, der vermeintlich relevante gesellschaftliche Bereiche nach einer etwaigen Priorität abarbeitet, leitet uns nicht auf unserer Suche nach Auswegen aus einer programmierten Gesellschaft. Allein schon deshalb, weil auch der technologische Angriff kein kohärent vorgetragenes Programm, sondern ebenfalls eine erratische Suchbewegung ist. Ein weiterer Grund ist, dass wir einer Debatte nicht vorgreifen und durch Schnellschüsse weitergehende Gedankengänge kurzschließen wollen. Vor allem aber auch deshalb, weil wir selbst nicht im Besitz der ultimativen Antwort sind. Fokus unserer Arbeit ist eher, die Details des technologischen Angriffs sichtbar, diskutierbar und damit angreifbar zu machen. Wir bestehen auf unserem Recht zur Kritik, zu sagen, was schlecht, menschenverachtend und verbrecherisch ist, selbst, wenn wir nicht die Lösung dafür im Folgesatz nennen können. Wir gehen davon aus, dass sich die “ultimative Antwort” in den Kämpfen gegen den technologischen Angriff entwickelt, und dass ein Versuch, diese Antwort am grünen Tisch zu finden, fruchtlos bleiben wird.

TECHNOLOGIEKRITIK IST HERRSCHAFTS- UND ZIVILISATIONSKRITIK – KEIN PRIMITIVISMUS!

Wir fällen nicht das lächerliche Urteil, dass die Technologie „schlecht“ ist. Aus welcher – ohnehin historisch bedingten – Ethik heraus denn auch? Wir sagen, sie ist Gewalt und sozialer Krieg.

Unsere Kritik macht sich fest an der technologischen Aneignung von Lebensprozessen. Unsere Positionierung gegenüber spezifischen technologischen Innovationen orientiert sich an einem anzustrebenden Abbau von Macht, Ungleichheit und Fremdbestimmung. Unser sozialrevolutionärer Autonomie- und Freiheitsbegriff geht hier weit über die zugestandene „Freiheit“ der „User*innen“ hinaus, die als Konsument*innen und Datenlieferant*innen zwischen verschiedenen vordefinierten Produkten wählen dürfen.

Wir verteidigen nicht pauschal „die Arbeit“ gegen jede Form von Roboterisierung. Menschliche Arbeit versus Nicht-mehr-Arbeit sind wenig aussagekräftige, statische Kenngrößen einer zudem makroskopischen Betrachtung. Ohne eine mikroskopische Sicht auf gesellschaftliche Auseinandersetzungen beschreiben sie weder die Dynamik der gesellschaftlich-technologischen Umwälzung noch geben sie Einblick in ihren Disziplinierungs- und (Selbst-) Unterwerfungscharakter. Wenn wir beispielsweise mit den streikenden Mitarbeiter*innen von Amazon zusammen stehen, unterstützen wir ihren Kampf gegen Entwürdigung und Entrechtung sowie gegen die (in diesem Fall algorithmische) Enteignung und Entwertung ihrer Arbeit. Wir tun das in einem solidarischen Verhältnis, aber auch in dem Wissen, dass uns allen die gleiche Entwürdigung in einer technokratischen Zukunftsvision von Amazon bevorstehen könnte – ermöglicht durch eine permanente Bewertung und Steuerbarkeit sämtlicher Lebensbereiche, in die Amazon und seine zukünftigen Nachfolger sukzessive vordringen.

Umgekehrt halten wir die Position, Technologie als „segensreichen Fortschritt“ zu glorifizieren, den wir lediglich aus den Klauen des Kapitalismus befreien müssen, für naiv. Weder Lenins noch Trotzkis (damalige) Zukunftsvisionen einer tayloristischen Fließbandgesellschaft nähren die Hoffnung auf eine progressive Verhaltenssteuerung. Und wir sehen ebenfalls im sozialistischen Vorläufer der Industrie 4.0, dem chilenischen Cybersyn-Projekt (Proyecto Synco) Anfang der Siebziger Jahre unter Salvador Allende, keine Referenz für eine heilsversprechende Kybernetik. Denn auch dort hat sich der Vermessungseifer längst nicht mit einer automatisierten Selbstregulierung der Produktion in Chile begnügt, sondern nach Methoden einer kleinteiligen Verhaltensökonomie seiner Inhabitant*innen gesucht. Eine Perspektive, die wir heute sowohl in dem „sozialen Punktesystem“ Chinas als auch in Googles Vorstellungen vom „Buch des Lebens“ (selfish

ledger) wiederfinden. Diese Programme sind ihrem Anspruch nach totalitär: Der Kybernetisierung des Sozialen wohnt die Vorstellung sich selbst regulierender Individuen inne, die durch ein von außen vorgegebenes Selbstoptimierungsprinzip maximal fremdbestimmt agieren.

Daher reicht eine Vergesellschaftung der digitalen Plattformen, ja sogar eine Vergesellschaftung der digitalen Infrastruktur nicht aus. Wir müssen die soziale Kybernetik – also die feinstgliedrige Zerlegung unseres Lebens in Mess- und Steuerkreise - als solches zurückweisen. Die Technologie lediglich vom Kapitalismus befreien zu wollen – als vermeintlich „äußerem Verhältnis" –, ist leider eine wenig hilfreiche, unterkomplexe Vereinfachung. Das brachte bereits Max Weber zum Ausdruck, als er schrieb:

»Nicht erst ihre Verwendung, sondern schon die Technik ist Herrschaft (über die Natur und den Menschen), methodische, wissenschaftliche, berechnete und berechnende Herrschaft. Bestimmte Zwecke und Interessen der Herrschaft sind nicht erst ›nachträglich‹ und von außen der Technik oktroyiert – sie gehen schon in die Konstruktion des technischen Apparats selbst ein. Die Technik ist jeweils ein geschichtlich-gesellschaftliches Projekt; in ihr ist projektiert, was eine Gesellschaft und die sie beherrschenden Interessen mit den Menschen und mit den Dingen zu machen gedenken.«

DIGITAL DIVIDE

Der „Confirmation Bias", also die Neigung, Dinge so zu interpretieren, dass sie die eigene Überzeugung bzw. Vermutung untermauern, ist ein psychologisches Phänomen, das weit vor der Digitalisierung entdeckt wurde. Die per Social Media gelenkte Aufmerksamkeits-Ökonomie verstärkt diesen Effekt jedoch nachweisbar. Durch sie zerfällt aktuell nicht nur eine „gemeinsame" Sicht auf „die Dinge", es zerfällt sogar die Möglichkeit, unterschiedliche Sichten diskutierbar zu machen. Denn das, was früher Öffentlichkeit genannt wurde, fragmentiert selbst mehr und mehr. Leute unterschiedlicher Weltsichten leben in voneinander entkoppelten Informationswelten, innerhalb derer die jeweils eigene Sicht durchaus als schlüssig oder zumindest selbstkonsistent erscheinen mag. Es gelingt informationstechnisch immer besser, sich einem Abgleich mit grundlegend anderen Meinungen zu entziehen. Hier erweist sich Facebooks individualisierter Nachrichten- und Kommunikationstrom als wirkmächtiges Isolations- und Lenkungswerkzeug. In den USA verengt sich so bereits jetzt für die Mehrheit der Menschen die Nachrichtenwelt auf die Sicht, die Facebook von ihren Vorstellungen und Neigungen hat - geleitet von der Maxime, die Aufmerksamkeit mit beliebigem Inhalt so lange wie möglich zu binden.

Die aktuellen politischen Vorzeichen mit den Ansätzen für eine in weiten Teilen der Welt rechte bis offen faschistische Bewegung, die allzu oft als Rechtspopulismus verharmlost wird, existieren durchaus ohne den digitalen Transformationsprozess. Aber sie existieren nicht unabhängig von ihm. Jenseits der Frage nach dem Ursprung „einer tiefen Verunsicherung" angesichts der hohen gesellschaftlichen Transformationsgeschwindigkeit, die Raum für simplifizierende rechte Lösungen schafft, ist es die innere Social Media-Funktionsweise, die die Reichweite rechter Propaganda im Netz deutlich erhöht und damit ein politisches Ungleichgewicht verstärkt.

Wenn wir die Transformation des Kapitalismus in Richtung eines digitalen Plattform-Kapitalismus mit neuen nicht-staatlichen Playern samt historisch neuem Ausmaß von Abhängigkeiten und Machtungleichgewichten analysieren und kritisieren, dann lässt sich daraus kein positives Verhältnis zum Staat mit dem Wunsch nach Regulierung ableiten. Das wäre ein reformistischer Kurzschluss. Ähnlich abwegig ist die Unterstellung, die Befürworter*innen des (anonymen) Bargelds stabilisierten den Kapitalismus. Zu glauben, die Bedingungen für eine Überwindung kapitalistischer Verhältnisse ließen sich durch eine von staatlicher Steuerung „entkoppelte" Crypto-Währung verbessern, ist eine reformistisch-romantisierende Vorstellung von Demokratisierungs-Technokrat*innen.

Uns stellt sich eher folgender Befund dar: Der in vielen gesellschaftlichen Bereichen (zunächst begrüßenswert) schwindende Einfluss staatlicher Institutionen wird eingetauscht gegen eine ultrakapitalistische Dominanz technokratisch-privatwirtschaftlicher Akteure, die sich noch leichter einem gesellschaftlichen Aushandlungsprozess entziehen können. Wir lesen z. B. den aktuellen Umbau des Gesundheitswesens in dieser Weise. Die vermeintliche Konkurrenz staatlicher und nicht-staatlicher Akteure löst sich nicht selten in einer gemeinsamen pragmatischen „Modernisierungs"-Offensive auf.

An alle Produktivkraft-, Technik- und Fortschrittsfetischist*innen:

Ihr könntet (mal wieder) auf der falschen Seite der Barrikade stehen.

Bis heute sind wir immer wieder mit dieser abgeschmackten Behauptung über die Schmerzgrenze hinaus angeödet worden: Technik ist entweder gut oder wenigstens neutral oder wird unter Abstraktion vom gewaltsamen Prozess ihrer Herstellung und Durchsetzung neutralisiert: als Dampfmaschine, Fließband und heute „Digitalisierung". Ja, sogar als Teil eines sozialen Verhältnisses affirmativ gesetzt und als Produktivkraft begrüßt. Es sei nur ihre kapitalistische Anwendung bei der Ausbeutung von Menschen, die ihre Widersprüchlichkeit bestimme und die sie schlecht und fragwürdig werden lasse. Von ihr müssten wir befreit werden, um so die Technik, die Menschen, die Arbeit zu befreien.

Der letzte große historische Zyklus, in dem dergleichen propagiert wurde, war der sogenannte „tayloristische" oder „fordistische". In ihm wurden tayloristische Rationalisierung, das Fließband und ihre Maschinerie eingesetzt. Auch sie waren, so die Legende, im Grunde nützlich bzw. neutral. Ja, sogar bestimmendes Strukturprinzip der gesamten Gesellschaft. Mittel der Knechtung und Überausbeutung waren sie nur im Dienste des Kapitalismus. Das sagten Sozialisten aller Couleur, Bolschewisten, Trotzkisten und dergleichen. Die wirkliche Geschichte hat das als propagandistische Lüge entlarvt. An dieser Lüge lässt sich auch für heute vieles lernen. [1]

Taylors Wut als Angehöriger einer aufsteigenden Avantgarde aus dem amerikanischen Progressismus galt der Kontrolle der Arbeiter*innen über ihr eigenes Arbeitsverhalten. Sie konnten langsam arbeiten, sie konnten schnell arbeiten, ohne dass ein direkter Zugriff auf ihr Verhalten zur Erhöhung von Produktivität und Rendite möglich war. Also machten sich Taylor und Konsorten wie Gilbreth und Gantt daran, das Arbeitsverhalten genau zu erfassen und in Einzelschritte zu zerlegen, um sie dann seriell zu einer Kette zu reorganisieren. Die Kontrolle der Arbeiter*innen über ihr eigenes Verhalten sollte so durchbrochen und letztlich beseitigt werden, um das Kommando hierüber auf die Managementebene abzuziehen. Ford hat seine Erfahrungen hiermit in die Organisation des Fließbands übernommen. Taylor ließ in seinen Schriften (den „Principles") und seinen öffentlichen Erklärungen (z. B. im US-Kongress) nicht den Hauch eines Zweifels über den sozialen Charakter seines Vorstoßes aufkommen. Er nannte ihn einen auf eine ganze Epoche angelegten „Krieg" („war") gegen die Arbeiter*innen, eine „schonungslose, harte und gemeine Form des Kämpfens", des „fighting" gegen sie, und die Rationalisierung eine „neue Waffe". Er sprach nicht etwa von der Benutzung von etwas Nützlichem als „Waffe", auch nicht von ihr als Teil eines sozialen Verhältnisses. Vielmehr ging es um die innere Logik der Rationalisierung, um die strategische Zielrichtung der Technologie im Kampf gegen die Arbeiter*innen als kriegerisches Projekt. Keineswegs nur um Herrschaft, denn die brach sich ja noch an Eigenwillen und Subjektivität der Klasse. Der Krieg und die Kämpfe dauerten Jahrzehnte. Sie wurden über eine ganze Epoche hinweg in alle Dimensionen der amerikanischen und schließlich der Weltgesellschaft getrieben. In den USA, Europa, in Russland. Dort zunächst unter dem Zaren und dann nahtlos daran anknüpfend in der Sowjetunion unter Lenin und seinem tayloristischen Kettenhund Gastev, Trotzki und Stalin, und zwar gegen den permanenten und zeitweise außerordentlich militanten Widerstand der Arbeiter*innen noch über den „Großen Terror" 36/37 hinaus. Taylors „Krieg" nahm zu seiner Durchsetzung zwei blutige „Maschinenkriege" in Anspruch, inklusive der sie begleitenden völkermörderischen Barbareien. Egal, ob sich seine Avantgarden nun „Kapitalisten" oder „Sozialisten" nannten, sie waren alle Kapitalisten, wenn man sich mal von den vulgärmarxistischen Definitionen trennt. Sie betrieben nicht die Verwendung einer Maschine, sondern einen Zurichtungsangriff, der die restlose Maschinisierung von Arbeit und Leben zum Ziel hatte, bis in Haushalt, Fami-

1 Buch dazu im Frühjahr 2019 bei AssoziationA

lie und städtisches Umfeld hinein. Lenin z. B. wollte die gesamte Gesellschaft zu einer einzigen großen Maschine taylorisieren, zu einem „Uhrwerk", das dem Kommando des sozialistischen Leiters gehorchte. Trotzki imaginierte sogar die totale Integration von Stadt und Land zum „sozialistischen Fließband". Der Begriff des „Fordismus" und die paradigmatische Vorstellung von einer „Fließbandgesellschaft" tauchte allerdings als Produkt des Antagonismus auf der Kapitalseite erst Jahrzehnte nach Beginn des Angriffs auf. Dieser ist schließlich an den Widerständen der Subjekte in den 60er und 70er Jahren weltweit, auch bis in den letzten Winkel des Realsozialismus (z. B. „Prager Frühling") hinein, in die Krise geraten. Er wurde, wie dies in der Geschichte in ähnlicher Weise immer wieder passiert ist, durch einen neuen technologischen Angriff zur Wiederherstellung des Kommandos auf neuer historischer Stufe aufgefangen: dem technologischen Angriff der Informationstechnologien.

Wir haben den Beginn dieses neuen epochalen Angriffs – denn mehr ist es bis jetzt nicht – in Büchern, Artikeln und zum Schluss in Köln auf einem Kongress unter dem Titel „Leben ist kein Algorithmus" dargestellt. D. h. in die Tiefe seiner Logik von Unterwerfung und technologischer Aneignung von Lebensprozessen (nicht zu verwechseln mit der notwendig damit einhergehenden Aneignung von Produkt und Mehrwert), und in ihre verschiedenen Felder in Arbeit und Gesellschaft verfolgt.[2] In den Angriff auf die Sozialstrukturen durch eine Politik der „schöpferischen Zerstörung" und Vertreibung (am Beispiel des Silicon Valley/ San Francisco); in einer Politik der gnadenlosen Unterwerfung von Arbeit in völlig neuen Formen (Amazon, Uber); in einer Politik des Eindringens in Subjektivität und Gefühl („Facebook, Liebe, Sex"); in der Vergewaltigung überkommener demokratischer Vorstellungen und Meinungsbildung durch „Cambridge Analytica", in einer Politik des Zwangs zur Selbstunterwerfung im digitalisierten Schuldenregime; in einer Politik des Zwangs zur Selbstoptimierung im Gesundheitswesen; in einer Politik der Transformation des Geldregimes und der politisch-ökonomischen Bewirtschaftung, und, und, und. Wir fällen nicht das lächerliche Urteil, dass die Technologie „schlecht" ist. Das wäre ein – ohnehin historisch bedingtes – moralisches Urteil und es geht uns nicht um Moral. Wir sagen, sie stellt einen technologischen Angriff dar, sie ist Gewalt und sozialer Krieg, gegen die wir Widerstand leisten. Die Form der technologischen Aneignung von Lebensprozessen (nicht nur des Produkts!) im Angriff der neuen innovatorisch-technologischen Avantgardeunternehmen hat direkt Kämpfe der Arbeiter*innen und angegriffenen Subjekte im erweiterten gesellschaftlichen Zusammenhang der kapitalistischen Reproduktion gegen sich aufgerufen. Er fordert auch uns – so haben wir argumentiert – dazu auf, der Offensive im Sinne der Befreiung, Selbstorganisation und Entwicklung völlig neuer Formen revolutionärer Subjektivität zu begegnen.

Angesichts dieser eindeutigen Befunde von technologischem Angriff und Gewalt und der blutigen historischen Erfahrungen der Opfer fragen wir uns, wie linke Fortschrittsfetischist*innen noch immer den Angriffscharakter von Technologie leugnen und sie als neutral oder gar segensreich deklarieren können. „Segensreich" ist die Vokabel, mit der in einem zentralen Text der in marxistischer Tradition operierenden „Rosa-Luxemburg-Stiftung" die „Kraft von Wissenschaft und Technik" bezeichnet wird.[3] Nach Abarbeitung einiger technologiekritischer Einwände aufgrund der mit den neuen Technologien verbundenen Risiken heißt es dann schließlich: „Eine linke Zukunftsvision braucht Modelle, die auch weiterhin auf die Triebkräfte des wissenschaftlich-technologischen Fortschritts vertrauen und diese zugleich aus der Verfügungsmacht des Kapitals heraus zu lösen suchen"[4] Ein Gedanke daran, dass die Technologien kapitalistischer Natur sind und zu seinem historisch jeweils erneuerten, gegen die Arbeiter*innenklasse und die Gesellschaft gerichteten, Angriffsarsenal gehören, taucht gar nicht erst auf. Folgerichtig wird den neuen Technologien die Aufgabe übertragen, die Zerstörungen durch die jetzt überholten Technologien zu beseitigen. Ein Lieblingsgedanke der kapitalistischen Welt, der darauf zielt, den Teufel durch den noch effizienteren und zugleich barbarischeren Beelzebub auszutreiben. Eine Revolution sei nicht beabsichtigt, der Kapitalismus solle zunächst auch gar nicht beseitigt werden, damit könne man später mal anfangen. Dementsprechend bemühen sich Autoren mit ihrer Veröffentlichung zu „smart cities", mit einer kritischen Analyse „eine Grundlage zu schaffen, mit der das emanzipatorische Potenzial der ‚Smart City'… freigelegt werden kann." [5]

Ähnliche Einstellungen wurden von einigen Organisator*innen des 4. UmsGanze-Kongresses vom 24. – 26. November 2016 in seinem Vorfeld propagiert. Auch hier war von Befreiung mit und durch die Maschinen die Rede, auch hier wurde der offensive kapitalistische Charakter der historisch jeweils neuen Technologien und damit auch die Notwendigkeit des Widerstands unterschlagen: Die Frage müsse anders gestellt werden: „Wie können wir

2 Vgl. bigdata.blackblogs.org; capulcu.blackblogs.org ; Detlef Hartmann, Krisen, Kämpfe, Kriege/ Bd 1.

3 R. Mocek (Hrsg.), Technologie, Politik und kritische Vernunft. Wie geht die Linke mit den neuen Technologien um? Diskussionsangebote des Gesprächskreises „Philosophie und Bildung" der Rosa-Luxemburg-Stiftung, Berlin 2008, S. 12. Reinhard Mocek war Vorsitzender des Vorstandes der Rosa-Luxemburg-Stiftung und Mitglied ihres Kuratoriums. Die Schrift wird noch immer an prominenter Position ihrer Homepage als grundlegend geführt.

4 Ebd., S. 31.

5 J. Sadowski, F. Pasquale, Smart City, Überwachung und Kontrolle in der „intelligenten Stadt", Rosa-Luxemburg-Stiftung, Analysen, S. 35.

die Maschinen – und mit ihnen uns – vom Kapitalismus befreien?". „Die Digitalisierung ist darum eine technische Revolution, weil sie alle gesellschaftlichen Bereiche neu strukturiert. Die Gesellschaft stellt sich nicht mehr nach dem Bild der Dampfmaschine her und auch nicht mehr nach dem Bild des Fließbandes, sondern nach dem Bild der universellen Rechenmaschine, der Informations- und Datenverarbeitung und der Vernetzung."[6] Mit Freude konnten wir allerdings auf dem Kongress feststellen, dass, wie schon im Vorfeld von den Veranstalter*innen eingeräumt, das Meinungsbild bei „UmsGanze" nicht einheitlich war. Ein großer Teil der Teilnehmer*innen stand der Vorstellung vom „technologischen Angriff" und damit der Notwenigkeit des Widerstands positiv gegenüber und es entwickelte sich eine lebhafte Kontroverse.

Diese beiden Beispiele stehen exemplarisch für die Tatsache, dass Teile der Linken aus ihrer marxistisch-leninistischen Orientierung heraus sich noch immer mit dem kapitalistischen technologischen Angriff identifizieren. Warum? Die Frage ist leicht zu beantworten. Sie suchen, wie schon in vorherigen analogen Phasen, noch immer die Teilhabe an der Macht, die die neuen Technologien gewähren. Ob als Angehörige der neuen technischen Intelligenz selbst oder als parteipolitische Organisator*innen gesellschaftlicher Prozesse, oder einfach auf der Suche nach unterstützenden Aufgaben als Philosoph*innen, Ethiker*innen, Kultursoziolog*innen und dergleichen mehr. Insgesamt formieren sie sich dabei als neoreformistisches Element im Spektrum der neuen Angriffsformation, wie es die Reformisten aus der alten Sozialdemokratie vor dem ersten Weltkrieg getan haben.

So unbedeutend sie derzeit zu sein scheinen, sie sind gleichwohl gefährlich. Als vorgebliche „Linke" schwächen sie den antikapitalistischen Kampf und fördern damit die enormen Gewaltpotenziale, die der technologische Angriff vor unser aller Augen zu entfesseln begonnen hat. Bei vielen Linken ist dies jedoch keine irreversible Entwicklung, die zu einem endgültigen Urteil Anlass geben müsste. Wir begreifen diesen Beitrag daher als Aufforderung zu einer Debatte über alle, vor allem auch die historischen, Dimensionen des hier skizzierten Prozesses, an der wir uns gerne beteiligen wollen.

6 www.tueinfo.org/cms/node/23541; http://top/berlin.net/de/texte/beitraege/keine-zukunft-ist-auch-keine-loesung. Beides Material zur Vorbereitung des Kongresses.

Die Krise der politischen Repräsentation

Wir befinden uns in einer Phase globaler Fragmentierung. Selbst vermeintliche ökonomische Gewissheiten der neoliberalen Wirtschaftsordnung der 90er und 2000er Jahre zerbröckeln in einem „Me first" nationaler Selbstbezüglichkeit und Abschottung. Nicht nur, dass die Anzahl sogenannter „failed states" zunimmt – auch äußerlich stabile Gesellschaften fallen innerlich auseinander. Es gibt kaum noch eine gemeinsam diskutierte und umstrittene politische Öffentlichkeit, sondern den Zerfall in immer mehr voneinander getrennte, gesellschaftlich isolierte Parallelwelten. Die einzelnen gesellschaftlichen Fragmente beziehen ihre Informationen und Weltsichten aus den Echokammern und Filterblasen digitaler Portale und „sozialer" Netzwerke und verstärken darüber ihren eigenen Einschluss.

Die klassische politische Repräsentation befindet sich nicht erst seit Trump und dem zunehmenden rechten „Populismus" in Europa in der Krise. Der Bedeutungsverlust der politischen Administration ist tiefgreifender: Die Durchsetzung bzw. die Vermittlung unterschiedlicher Interessen und Bedürfnisse erfolgt zunehmend an der Kontrolle und der Steuerungsmöglichkeit klassischer politischer Instanzen vorbei. Die radikale und beschleunigte technologische Transformation des Kapitalismus wird viel stärker von einigen (wenigen) privatwirtschaftlichen Akteuren aus dem Silicon Valley und China dominiert als von der Gestaltungsmacht staatlicher Institutionen. Das geschieht mitunter abseits gesellschaftlicher Aushandlungsprozesse. Während es zumindest vorgesehen ist, auf den Staat als klassischen politischen Akteur (eingeschränkt) demokratisch einwirken zu können, bleibt der*die „User*in" gegenüber dem*der Plattformbetreiber*in zumeist in einem rein passiven Nutzer*innen-Verhältnis. Seine aktive (Un-)Willensbekundung gegenüber den neuen Gestalter*innen, den Entwickler*innen, beschränkt sich derzeit auf die Nutzung oder

die Verweigerung einer Software-Plattform. Der Preis für die Nicht-Nutzung von quasi-standardisierten Kommunikationsplattformen ist vielfach die drohende soziale Isolation (im Freundeskreis, in der Schule, in der Lerngruppe im Studium, …).

Diese neue Dominanz führt zu einer noch nie gekannten Konzentration von Macht: Eine kleine patriarchale Elite von Technokraten treibt weltweit den Plattform-Kapitalismus mit seiner Smartifizierung des Seins voran, um unsere sozialen Beziehungen neu zu ordnen und in Wert zu setzen. Jede noch so kleine Regung wird digital vermessen, bewertet und damit steuerbar. Der Mensch wird weit über seine Arbeitskraft hinaus dem permanenten Zwang zur Selbstoptimierung und -veräußerung unterworfen. Diese Entwicklung wird derzeit von China mit der Einführung von „Sozialen Kredit-Systemen" angeführt. Weiter zunehmender Anpassungsdruck, soziale Vereinzelung in permanenter Rating-Konkurrenz und soziale Dequalifizierung der Abgehängten als „Überflüssige" sind die Folge.

Doch es wäre fahrlässig, wenn wir glaubten, solche fortgeschrittenen Programme der Bevölkerungssteuerung ließen sich nur in autoritär formierten Gesellschaften wie China umsetzen. Tatsächlich benötigte die Einführung unterschiedlicher (regionaler) Punkte-Systeme in ihrer Erprobungsphase in Chinas Großstädten keinerlei Zwang. Die zunächst freiwillige Teilnahme mehrerer Hundert Millionen wird teils über Preisrabatte z. B. bei Online-Einkäufen und Bahnreisen, über die Bevorzugung bei Jobangeboten, teils allein über den spielerischen Charakter („Gamification") des Punkte-Sammelns erreicht.

Auch wenn die großen Tech-Unternehmen aus dem Silicon Valley gerade neidvoll nach China blicken, bleiben sie nicht untätig. Im Mai 2018 sickerte ein internes Firmenvideo der Forschungsabteilung Google X in die Öffentlichkeit. Unter dem Namen „The selfish ledger", was sich nur eher ungelenk mit dem „Buch des Lebens" übersetzen lässt, beschreibt Google seine Zukunftsvision einer paternalistisch geführten Welt.

Ein persönliches Journal „sämtlicher Handlungen, Entscheidungen, Vorlieben, Aufenthaltsorte und Beziehungen" ist die Grundlage für ein System digitaler Assistenz, das KI-basiert auf jede*n Einzelne*n zugeschnittene „Handlungsempfehlungen" ausspricht. Google verspricht perspektivisch, Armut und Krankheiten überwinden zu können unter der freimütig vorgetragenen Bedingung: die Aufgabe des freien Willens. Nur dann ließen sich effektiv „potentielle Fehler im Verhalten der Nutzer detektieren und korrigieren". Selbstbewusst stellt Google in Aussicht: „Noch passen sich die Geräte ihren Nutzern an. Dieses Verhältnis wird sich bald umkehren." Diese erschreckend totalitär anmutende Sicht auf eine vermeintlich bessere Welt knüpft nahtlos an die Vorstellungen des behaviourism an. Dieser geht angesichts zu komplexer Lebensverhältnisse von einer notwendigen Verhaltenssteuerung andernfalls nicht-rational handelnder Individuen aus – ein zutiefst paternalistisches Menschenbild.

Wir wollen den politisch-ökonomischen Bedeutungsverlust staatlicher Institutionen gegenüber den Tech-Giganten und deren Startup-Gefolgschaft an einigen Beispielen konkret nachvollziehen:

DIGITALISIERUNG DES GESUNDHEITSSYSTEMS

In Deutschland ist die Einführung einer elektronischen Gesundheitsakte lange umstritten. Ärzt*innen und (deutlich schwächer organisiert) viele ihrer Patient*innen liefen Sturm gegen die Einführung einer zentralen Speicherung von Gesundheitsdaten, Medikationen und Behandlungsansätzen. Das Vorhaben der Bundesregierung ist über zehn Jahre in Verzug. Ende 2018 soll die Gesellschaft für Telematikanwendungen der Gesundheitsakte (gematik) gerade mal die technischen Voraussetzungen klären. Die milliardenschwere Vorbereitung der dazu notwendigen Infrastruktur rund um die Gesundheitskarte ist mittlerweile veraltet und genügt den Sicherheitsanforderungen der mehrheitlich skeptischen Patient*innen und Ärzt*innenschaft nicht. Das Vorhaben droht endgültig zu scheitern.

Nachdem Apple, Google, Amazon, Facebook und Microsoft erkannt haben, dass „Gesundheit fast überall auf der Welt der größte oder zweitgrößte Sektor der Wirtschaft ist" (Apple-Chef Tim Cook in einem Interview mit dem Magazin „Fortune" im Herbst 2017), investieren sie Milliarden in die Biotech-Forschung und versuchen mit Hochdruck, erweiterte Gesundheitsdienste in ihre Softwareumgebungen zu integrieren. Das Smartphone soll zur neuen persönlichen Gesundheitszentrale avancieren. Zusatzgeräte wie Fitness-Armbänder sollen dessen Funktionalität erweitern. Die Apple-Watch z. B. gibt vor, Herz-Anomalien erkennen zu können. Die Qualität der Messung des Herzrhythmus lässt zu wünschen übrig, und so beklagen sich nicht wenige Notaufnahmen über Smart-Watch-Besitzer*innen, die glauben, einen Herzinfarkt zu haben. Doch das boomende Geschäft mit der Fortschrittsgläubigkeit seiner technokratiehörigen Kund*innen nimmt dadurch keinen Schaden.

Amazon nähert sich dem vielversprechenden Gesundheitsmarkt gleich auf drei Weisen. Amazon wird nicht nur Krankenversicherung, sondern plant auch gleich Apotheke und Pharma-Unternehmen zu werden. Warum? Krankenversicherungen preisen das Risiko ein, krank zu

werden. Je vielfältiger und je genauer die Kenntnis der Versicherung über die Gewohnheiten der*des Versicherten ist, desto exakter lässt sich dieses Risiko berechnen. Ein Wettbewerbsvorteil gegenüber anderen Konkurrenten. Daher liegt es nahe, dass Google und Amazon sich in diesem Geschäft behaupten könnten – die fehlende Expertise im Versicherungswesen kaufen sie ein.

Den Tech-Giganten folgen nun die klassischen Krankenversicherungen auf die Überholspur. Gemeinsam schaffen sie Fakten und lassen die gesellschaftliche Aushandlung über Standards bei der Digitalisierung des Gesundheitssystems als überflüssig zurück: Nachdem die Generali Deutschland mit ihrem Programm Vitality als erste einen günstigeren Tarif für Kund*innen in Aussicht stellte, die bereit sind, ihr Gesundheitsbemühen (Fitness und Ernährung) vermessen zu lassen, verzeichnen wir seit September 2018 einen gemeinsamen Vorstoß von derzeit 16 Krankenkassen, denen die Gesetzesinitiative der Bundesregierung zu langsam voranschreitet. Hinter dem Namen „Vivy" verbirgt sich eine App, die sämtliche Gesundheitsdokumente, Befunde, Arztbesuche, Medikationen und darüber hinaus Fitness- und Ernährungsbemühungen speichert und bewertet. Auch diese Plattform ist zwei Tage, nachdem sie online ging, bei Sicherheitsexpert*innen durchgefallen: Entgegen ihrer Zusicherung werden Gesundheitsdaten an Dritte gesendet – ein *no go* angesichts der Sensibilität der dort gespeicherten Daten. Dennoch erfreut sich die (freiwillige) App bei den über 13 Millionen Versicherten, denen sie derzeit angeboten wird, wachsender Beliebtheit.

Die Techniker Krankenkasse bietet ebenfalls ihren 10 Millionen Versicherten eine elektronische Gesundheitsakte als App. Auch die AOK arbeitet an einer eigenen Gesundheits-App, um ihre 26 Millionen Versicherten mit Ärzt*innen und Kliniken digital zu vernetzen. Beide Projekte sind noch in der Testphase. Viele Krankenkassen gehen derzeit erste Schritte auf dem Weg zu einem dynamischen Tarifsystem, welches das ursprüngliche Solidarprinzip vollständig auszuhebeln versucht: Jede*r ist für ihre*seine Gesundheit selbst verantwortlich. Künstlich intelligente Gesundheitsassistenten geben personalisierte Ratschläge, deren Nichtbefolgen mit teureren Tarifen in der Krankenversicherung „honoriert" wird.

Der staatliche Einfluss in diesem Geschäft mit der Gesundheit ist auf eine minimal gesetzgebende Rolle zurückgedrängt. Der Staat ist längst kein aktiver Gestalter mehr in der Frage: wie lässt sich ein solidarisches Gesundheitssystem realisieren? Das Lockern der Bedingungen für eine Fernbehandlung durch einen Online-Doktor im Mai 2018 markierte das Einknicken vor einem wachsenden Geschäft mit der Gesundheit. Hiermit wird perspektivisch der qualitativ wichtige Standard eines echten (nicht-virtuellen) Arztbesuches inklusive freier Arztwahl aufgegeben. Ein lange gefordertes Zugeständnis an die Gesundheitsindustrie, die sich davon deutlich höhere Profite verspricht. Hiermit dokumentiert der Staat sein Scheitern, insbesondere im ländlichen Raum eine vernünftige Gesundheitsversorgung aufrecht zu erhalten, und tauscht den universellen Anspruch auf einen Arztbesuch gegen eine Skype-Fernberatung im Stil einer Callcenter-Kund*innenbetreuung. Krankenversicherungen entwickeln derzeit KI-basierte Online-Filter-Apps, mit denen sich automatisiert vermeintlich ernsthaft erkrankte Patient*innen von Hypochonder*innen und Blaumacher*innen unterscheiden lassen. Letzteren soll dann perspektivisch der zu teure echte Arztbesuch verwehrt bleiben. Der „Goldstandard" des frei gewählten Arztbesuchs sei zukünftig nicht mehr aufrecht zu halten.

RÜSTUNGSENTWICKLUNG

Die Wissenschaftsbehörde des US-Verteidigungsministeriums DARPA sieht große Gefahr in einer drohenden Dominanz nichtstaatlicher Akteure bei der Entwicklung künstlicher Intelligenz (KI). Dies hätte angeblich fatale Folgen für das weltweite Wettrüsten auf dem Sektor autonomer Waffentechnologie. Expert*innen fürchten, dass chinesische Großkonzerne wie Tencent und Alibaba über ihre besonders konsequente Umsetzung von Big-Data-Strategien innerhalb der KI allein wegen ihrer am schnellsten wachsenden verknüpften Datenbanken in wenigen Jahren weltweit die Nase vorn haben könnten. Zum Verständnis: Künstlich intelligentes „Maschinelles Lernen" mithilfe sogenannter tiefer neuronaler Netzwerke hängt maßgeblich von der Menge und der Qualität verfügbarer „Trainings"-Daten ab.

Auch wenn das Silicon Valley mit seinen Startups derzeit (noch) mehr KI-Ideen beforscht und entwickelt – der Markt für deren Umsetzung ist bereits jetzt in China größer. Das Marktanalyseunternehmen CB Insights veröffentlichte, dass bereits 2017 China 48 Prozent aller weltweiten Investitionen im Bereich Künstliche Intelligenz anzog. Nur 38 Prozent der Gelder gingen an die USA. Europa und der Rest der Welt sind weit abgeschlagen.

RAUMFAHRT

Lange war die Raumfahrt die symbolträchtigste Kategorie in der Spitzentechnologie, die das Streben nach Überwindung menschlicher Beschränktheiten – gefesselt an ein irdisches Dasein – markierte. Aber sie ist ähnlich der Formel Eins in der Automobilindustrie ein extrem teures Prestigegeschäft. Selbst multinationale Raumfahrtbestrebungen speckten deutlich ab und beschränkten ihre Ak-

tivität auf weniger Missionen mit unmittelbarer verwertbarem Nutzen.

Auch in dieser Phase war die europäische Ariane 5-Rakete (seit ihrer Inbetriebnahme 1996) so etwas wie der Mercedes unter den Trägerraketen. Deutlich zuverlässiger als ihr US-amerikanisches und russisches Pendant. Keiner hatte mehr Satelliten ins All gebracht. Doch zehn Jahre später kündigte der Tesla-Gründer Elon Musk mit seiner neuen Privatinitiative SpaceX den Bau einer wiederverwertbaren Trägerrakete an. Ein Game Changer, wie sich 2018 herausstellt. Mehr Starts und dazu deutlich günstiger. Auch das neue Modell Ariane 6 wird (ab 2020) daran nichts ändern und pro Start etwa doppelt so teuer bleiben.

Ein Einzelunternehmen, welches zudem nur „nebenbei" Raketen baut, macht nun das Rennen gegen die staatlich geförderten Traditions-Gesellschaften der USA, Russland und Europa. Kein Unternehmen geht die Zukunft vermeintlicher Mars-Missionen so konsequent und aggressiv an wie SpaceX. Ernst zu nehmende Konkurrenz droht hier allenfalls vom Konkurrenz-Startup Blue Origin des Amazon-Chefs Jeff Bezos. Der möchte zunächst „kleinere" Brötchen backen und erstmal eine Siedlung auf dem Mond bauen.

ZENSUR / KOMMUNIKATIONSSTEUERUNG

Mit der Dominanz der Kommunikationsplattform Facebook haben sich auch die Bedingungen und Grenzen der freien Meinungsäußerung verschoben. Über *no gos* in der digitalen Kommunikation entscheidet derzeit nicht mehr eine Institution, die sich (wie unzulänglich auch immer) gesellschaftlich legitimieren muss, sondern ein Konzern, der an der durch ihn vermittelten und gelenkten Kommunikation verdient. Ein Beispiel: Nach langer Debatte um die Verantwortung von Facebook bei der Verbreitung von terroristischer Propaganda hat Mark Zuckerberg 2018 ein Machtwort gesprochen. Ein Mix aus Künstlicher Intelligenz und „geschulten" Mitarbeiter*innen soll Echtzeit-Löschungen gemäß folgender Terrorismus-Definition vornehmen. Als terroristisch und damit zu löschen gilt der Beitrag „jeder Nichtregierungsorganisation, die vorsätzliche Gewalttaten gegen Personen oder Eigentum betreibt, um Zivilbevölkerung, die Regierung, oder internationale Organisationen einzuschüchtern, um ein politisches, religiöses oder ideologisches Ziel zu verfolgen." Auffallend ist, dass gemäß dieser Definition jegliche Form von staatlichem Terrorismus ausgeklammert bleibt. Die Deutungshoheit in einer öffentlichen (politischen) Debatte hat nunmehr Facebook mit seinen intransparenten Zensur-Algorithmen und den nicht-öffentlichen Kriterien seiner menschlichen Lösch-Teams. Die Verantwortung der Zensur entkoppelt sich damit von einer gesamtgesellschaftlichen Legitimation. Die Zensur selbst ist faktisch nicht mehr politisch debattierbar.

Besonders weitgehend sind die Folgen einer derart „eigenständigen" Zensur des größten Kommunikationslenkungs-Unternehmens bei der von Facebook 2018 eingeführten Suizidkontrolle. Facebook untersucht in allen Ländern außerhalb der EU die Daten seiner Nutzer*innen auf psychische Auffälligkeiten, ohne sie vorher zu fragen. Ein vom Algorithmus „erkanntes" abnormes Muster wird Moderator*innen gemeldet. Diese können sogenannte „first responder" (Ersthelfer*innen) einschalten. Dabei handele es sich um Polizist*innen, Notärzt*innen oder Feuerwehrleute, die versuchen, mit der betroffenen Person Kontakt aufzunehmen oder sich ggf. Zutritt zur Wohnung verschaffen. Wichtig in diesem Zusammenhang ist, dass diese Detektion einer vermeintlichen Suizidabsicht nach Facebooks selbst gewählten, intransparenten Regeln stattfindet.

Bezeichnend für die Allmachtsphantasie, soziale und auch politische Prozesse beeinflussen zu können, ist ein Post von Marc Zuckerberg vor der Bundestagswahl 2017: „Wir haben daran gearbeitet, den integeren Ablauf der Wahl sicherzustellen". Das sagt ein Unternehmen – keine irgendwie legitimierte Institution!

Es lassen sich viele weitere Beispiele finden für den schwindenden Einfluss klassischer politischer Instanzen auf das digitalisierte Alltagsleben der 50 Prozent der Weltbevölkerung, die Zugang zum Internet haben. Wir wollen nicht missverstanden werden: Wir sehnen uns nicht angesichts der offen artikulierten technokratischen Drohung nach alten Verhältnissen oder gar nach einem stärkeren Staat zurück. Im Bedeutungsverlust staatlicher Institutionen könnte auch eine Chance für einen emanzipatorischen Umbruch liegen – doch dies scheint derzeit außerhalb der Vorstellungskraft einer in die Defensive zurückgedrängten Linken. Die Verunsicherung angesichts des massiven europäischen Drifts nach Rechts im Rahmen der „Terror-" und „Flüchtlingsbekämpfung" erscheint derzeit zu groß. Die Aufgabe der radikalen Linken in Europa wäre es, die Fragmente des Zerfalls-Prozesses in einer emanzipativen Perspektive von unten miteinander zu verbinden.

Das gelingt allerdings nicht über das naive Herbeisehnen einer vermeintlich gerechteren Ökonomie des Teilens – der Share-Economy. Jeremy Rifkin und Paul Mason sehen darin die Möglichkeit, den Kapitalismus zu überwinden. Das Argument geht wie folgt: Das Internet ermögliche erstmals über digitale Plattformen eine direkte Verbindung zwischen den (ökonomischen) Interessen der Individuen ohne staatliche Vermittlungsinstanzen. Hierüber könne aufbauend auf den Gedanken des Teilens in der

Share-Economy eine Gemeinwesen-Ökonomie etabliert werden, die die einstigen ökonomischen Rahmenbedingungen untergrabe. Die Chance für eine Überwindung des Kapitalismus rücke mit einer beschleunigten Technologisierung näher, so die Vertreter*innen der sogenannten Akzelerationist*innen. Die Realität sieht leider anders aus. Uber, AirBnB und Co. haben gut gemeinte Sharing-Ideen monopolisiert und monetarisiert. Angesichts milliardenschwerer Börsenkonzerne können aktuell nur unverbesserliche Optimist*innen eine reformistische antikapitalistische Dynamik der Selbstermächtigung im Netz erkennen.

Eine klare Zurückweisung der Bestrebungen von Google, Amazon, Facebook, Apple, Alibaba und den Startups, die sie sich zukünftig einverleiben werden, ist vielmehr von Nöten. Die Zurückweisung der tatsächlich totalitären Kybernetisierung aller Lebensbereiche, verbunden mit dem Zwang zur Optimierung und Veräußerung des Selbst weit über den Bereich der Arbeit hinaus, braucht unserer Meinung nach die Autonomie, also die Selbstbestimmung als positiven Bezugspunkt. Dieser sollte nicht als selbstbezüglicher Individualismus missverstanden werden, sondern als eine Selbstbehauptung, die sich nur kollektiv, widerständisch erkämpfen lässt.

Der Bedeutungsverlust staatlicher Macht war auch vor über hundert Jahren ein Resultat der damaligen fordistisch-tayloristischen Innovationsoffensive, gleichfalls zugunsten der großen innovativen Unternehmen. Er eröffnete ebenfalls Chancen für Widerstand und Gegenmacht von unten. Allerdings haben die Staaten ihre Macht im blutigen Ersten Weltkrieg in Form militärisch-industrieller Komplexe reorganisiert. In Anbetracht der zunehmenden globalen Spannungen, die Möglichkeiten der Repression nach innen eröffnen, erscheint das Zeitfenster für erfolgreichen Widerstand eingeschränkt.

Der technologisch-militärische Angriff

Deutlicher als sonst jemand aus den Kommandohöhen der großen Mächte hat Putin es auf den Punkt gebracht: „Künstliche Intelligenz ist die Zukunft, nicht nur für Russland, sondern für die Menschheit. Es geht einher mit kolossalen Möglichkeiten, aber auch mit Bedrohungen, die schwer vorher zu sagen sind. Wer immer sich zum Führer auf diesem Gebiet macht, wird die Welt beherrschen." Diese Rede an russische Kinder am 1.9.2017, dem „Tag des Wissens", hat ein weltweites Echo hervorgerufen, vor allem bei den konkurrierenden Mächten. Ihre Konkurrenz heizt sich zunehmend auf. Aber sie beschränkt sich lange nicht mehr auf die Innovationskonkurrenz der großen IT-Unternehmen. Sie wird zunehmend zur Konkurrenz in der militärischen Nutzung der neuen Technologien.[7] Der erbitterte Wettbewerb, der die der heutigen Innovationsoffensive vorausgehende fordistische Epoche beherrschte, wiederholt sich auf neuer historischer Stufe. Darum ist zunächst ein kurzer Blick in die Vergangenheit angebracht.

Die Innovationen, die diese Epoche beherrschten, waren die neuen Verfahrenstechnologien des Taylorismus bzw. Fordismus und die mit ihnen einhergehenden Schlüsselindustrien im Elektro-Auto- und Chemiebereich. Sie stießen die Welt in eine Ära der Massenproduktion. Ihr Kern war der „Krieg" (so Winslow Taylor ausdrücklich) gegen die Arbeiter*innenklasse auf dem „shop floor" des unmittelbaren Produktionsprozesses. Arbeitsprozesse wurden zertrümmert und die Verhaltenspartikel seriell aneinander gereiht und zu Verhaltensketten reorganisiert, wie etwa beim Fließband. Dadurch wurde den Arbeiter*innen die Kontrolle über ihr eigenes Arbeitsver-

7 Zur Orientierung seien empfohlen: P. Scharre, Army of None. Autonomous Weapons and the Future of War, New York 2018; V. Boulanin, M. Verbruggen, Mapping the Development of Autonomy in Weapon Systems, Stockholm (sipri) 2017; P. W. Singer, Wired for War, London 2009 (etwas veraltet); D. Hartmann, Krisen, Kämpfe, Kriege, Bd. 2. Innovative Barbarei gegen soziale Revolution. Kapitalismus und Massengewalt im 20. Jahrhundert, Berlin 2018. Für aktuelle Berichterstattung ist www.defenseone.com., sipri. der US-Thinktank Brookings und The Guqardian zu empfehlen.

halten genommen und ins Kommando des Managements überführt. Die damit einhergehende gesteigerte Produktivität führte zu Absatzkrisen, weil die weltweite und vor allem periphere Arbeitsproduktivität nicht Schritt hielt – mit der Folge wachsender gegenseitiger Aggressivität nicht nur der großen Unternehmen, sondern der metropolitanen Länder. Die Innovations- und Wachstumsdynamik stockte in einer großen Krise der Jahre 1913/14, und damit gleichzeitig die Durchsetzung der neuen Technologien. Die Lösung der Krise und zugleich die Neuentfesselung der Innovations- und Wachstumsdynamik suchte der Kapitalismus in der Rüstungskonkurrenz vor und im ersten Weltkrieg, der an der Front für den Massenabsatz der in technologisch hochgerüsteten Fabriken produzierten Tötungs- und Vernichtungsmitteln sorgte. Die führenden kapitalistischen Länder transformierten die Konkurrenz in einen militarisierten, blutigen Kampf der „feindlichen Brüder" (Marx) um Führerschaft bei der Durchsetzung der neuen Technologien und die darauf gegründete imperiale Macht. Nach einer erneuten, mit dem Ende der 20er Jahre einsetzenden, Krise wiederholten die „feindlichen Brüder" unter Einschluss der Sowjetunion ihre blutige Konkurrenz im zweiten Weltkrieg. Zur Durchsetzung dieser konkurrenzgetriebenen kriegerischen Innovationsprozesse wurden Komplexe militärisch-industrieller Zusammenarbeit organisiert, sogenannte „militärisch-industrielle Komplexe".[8]

TÖDLICHE KONKURRENZ

Die feindlichen Brüder, deren Konkurrenz den gegenwärtigen Innovationsprozess militärisch vorantreibt – dies sind in erster Linie USA, China, Russland, und nachhängend Europa –, formieren in gleicher Weise in ihrem Machtbereich militärisch/industriell/wissenschaftliche Komplexe. In China wird die Verschmelzung ziviler und militärischer Unternehmungen und Institutionen forciert. Große Unternehmen wie Baidu betreiben militärisch orientierte Forschung und Entwicklung. Die Volksbefreiungsarmee hat eine Reihe von KI-Forschungszentren eingerichtet. Alle sind über das Kommando der Diktatur verbunden. In Russland wird großes Gewicht auf die organisatorische Überwölbung ziviler und staatlicher Institutionen gelegt. Das in der Vorstellung, dass man die internationale Konkurrenz wenigstens in der organisatorischen Entwicklung überholen kann, wenn man sie denn nicht im Einsatz finanzieller Mittel hinter sich lassen kann. So sollen wissenschaftliche und militärische Institutionen mit industriellen Kapazitäten im Sinne von staatlich-privaten Partnerschaften verbunden werden. Auf jährlichen KI-Konferenzen sollen Fortschritte und weitere Möglichkeiten erörtert und im Rahmen von KI-Kriegsspielen getestet werden. Alles verbunden mit genauer Beobachtung der Fortschritte der anderen Konkurrenten. In den USA werden unter Leitung des Pentagons die militärischen KI-Initiativen zwar in einem KI-Zentrum gebündelt (JAIC). Bei all dem großen Interesse und der Einsatzbereitschaft führender Akteure aus dem privaten Sektor – Eric Schmidt und Milo Medin von Google sind Mitglieder der Innovationskommission des Pentagon – sind die Ansätze zu einem neuen militärisch-industriellen Komplex vor allem auf dem KI-Sektor bisher aber noch nicht so weit gediehen, wie bei den Konkurrenten. Eine Initiative in diese Richtung stellt in Europa die Zusammenarbeit großer Unternehmen unter staatlicher Beteiligung auf dem militärischen Sektor in einem Komplex bei Tübingen mit Namen Cyber Valley dar. Hier soll offenbar die militärische Nutzung der Informationstechnologien und vor allem von KI der zurückgebliebenen deutschen bzw. europäischen Entwicklung einen entscheidenden Schub geben. Gegen marxistisch-leninistisch orientierte Darstellungen wie z. B. seitens der Tübinger IMI, die vom Interesse bestimmt werden, der BRD eine Vorreiterrolle zuzuweisen, ist festzustellen, dass die Entwicklung der BRD auf dem Gebiet der KI im Allgemeinen und ihrer militärischen Anwendung im Besonderen weit hinter den Konkurrenten zurückhängt. Lediglich auf dem Spezialgebiet der Sensorentwicklung halten die BRD-Unternehmen an vorderster Front mit. Man verweist zwar auf hoffnungsvolle Ansätze, etwa mit dem Forschungszentrum für KI (DFKI) in Saarbrücken oder dem Cluster Karlsruhe und der TU München, an der der „KI-Pionier" Jürgen Schmidhuber eine junge Garde großzieht. Offenbar soll dieser Zersplitterung über „Cyber Valley" entgegengewirkt werden, wo unter der Führung des Max-Planck-Instituts große Firmen wie Bosch und Mercedes ihre Ressourcen zusammenführen sollen. Diese sind allerdings mit ihren am autonomen Kraftfahrzeug arbeitenden Abteilungen, die alle in Silicon Valley vertreten sind, beträchtlich. Weckt Deutschland hier über die zivil-militärische Schiene wieder einmal einen „schlafenden Riesen" auf, wie im 19. Jahrhundert? On verra.

Auf der Schiene einer militärpolitischen Dynamisierung auch der zivilen Entwicklung operieren jedenfalls jetzt auch schon alle Konkurrenten. Die Rüstungskonkurrenz ist wie früher ein Vehikel, mit dem die Entwicklung auf dem informationstechnologischen Sektor, vor allem aber im KI-Bereich vorangetrieben werden soll. Von Bedeutung hierbei ist, dass die Krise, die ja auch eine Krise der Innovationsoffensive darstellt, alles andere als überwunden ist. Kriegerische Konflikte könnten auch heute wieder zum Mittel werden, aus der Krise herauszukommen, um zugleich Blockierungen des Innovationsprozesses aus dem Weg zu räumen. Und hier kommt inzwischen militärisch und zivil der Künstlichen Intelligenz eine zentrale Rolle zu, wie sich an der Forcierung der Entwicklung autonomer Waffensysteme durch die großen Konkurrenten ablesen lässt.

8 Zu allem: D. Hartmann, Krisen,…., op. cit.

AUTONOME WAFFENSYSTEME

Autonome Waffensysteme betreiben alles autonom, d. h. ohne Einsatz von Menschen: Die Sensor-gestützte Beobachtung, die Datenerhebung, die Ziel- bzw. Objekterkennung – hier spielt der Einsatz von KI eine besonders große Rolle –, die Entscheidung zum Einsatz und schließlich den Einsatz selbst. Beispiele sind auf russischer Seite ein von Kalaschnikow für den Bodenkampf entwickeltes voll automatisiertes Kampfmodul, das nach Werksangaben autonom Ziele identifizieren und eigene Entscheidungen zum Einsatz treffen soll. Hierhin gehört auch der T-14-Kampfpanzer „Armata", der schon 2016 in Produktion gegangen ist. Die Fachwelt ist unsicher über den Wahrheitsgehalt der vollmundigen Behauptungen. Beobachter*innen konnten jedenfalls auf dem gigantischen und demonstrativen Herbstmanöver „Wostok" zwar perfekte Logistik, aber keinen T-14 oder andere KI-getriebenen Waffen bewundern. In Großbritannien ist die vollautonome „Taranis"-Drohne für den Lufteinsatz entwickelt worden. Samsung baute für die südkoreanische Armee den „SGR-AI-Roboter", der vollautonom zur Überwachung an der demilitarisierten Zone zu Nordkorea eingesetzt werden sollte. In Israel, einer KI-Großmacht, ist die vollautonome „Harpy"-Drohne für den Lufteinsatz und das autonome Boden-Fahrzeug „Guardium" für Patrouillen an der Gaza-Grenze sowie der „Protector" für Küstenpatrouillen zu Wasser entwickelt worden. Zu den autonomen Waffensystemen, die in den USA entwickelt wurden, werden gezählt der „Sea Hunter" für den Einsatz gegen U-Boote und Schiffe; das X-47B-Flugzeug; der autonome Panzer „Crusher". Anlass zu erbitterten Kontroversen hat 2018 das Projekt „Maven" zur Entwicklung einer autonomen Kampfdrohne gegeben, in der bei Google entwickelte KI zum Einsatz kommt. Über 3000 Google-Mitarbeiter*innen haben Anfang April in einem offenen, in der New York Times veröffentlichten Brief die Geschäftsleitung aufgefordert, die Mitarbeit an diesem Projekt zu beenden. Der Anfang April ernannte Chef der KI-Abteilung bei Google und zugleich der Leiter seiner Gehirnforschungsabteilung Jeff Dean hat sich auf einer Konferenz im Mai auf die Seite der Kritiker*innen gestellt mit der Meinung, dass Google sich aus dem Geschäft der Herstellung autonomer Waffen heraushalten solle. Das war beileibe kein Auffangmanöver der Google-Führung und stand kaum im Widerspruch zur Geschäftsführung. Denn der Arbeitsmarkt für gute KI-Spezialist*innen ist weltweit sehr eng, praktisch leergefegt bei großer Nachfrage der Unternehmen. 3000 Spezialist*innen haben da schon eine beträchtliche Verhandlungsmacht und die setzten eine bedrohliche Kündigungswelle in Gang. Am 1.6.2018 erklärte die Google-Führung, sie werde den 2019 auslaufenden Vertrag mit dem Pentagon nicht erneuern. Der Rest der Laufzeit wurde unter die Bedingung gestellt, dass die Regierung „… unsere Prinzipien über den KI-Einsatz respektiert" und nicht nur für dieses Projekt. Wirklich eine Beendigung der Teilnahme? Ein taktisches Manöver? Ein Aufschub? Google weiß, dass dadurch das Projekt nicht wirklich beendet wird, sondern an Konkurrenten übergeht. Eine derart mächtige Waffe lässt sich das Pentagon nicht madig machen, so die Meinung der Expert*innen. Wie wird Google das umgehen? Vielleicht durch Outsourcing-Manöver? Man darf gespannt sein.

Eine Besonderheit auf dem Gebiet autonomer Waffen sind „Schwärme", die in der Luft, zu Lande und im Wasser operieren können. Die innere Organisation ihrer Einheiten – Drohnen, Kampfroboter, Schiffe bzw. Mini-U-Boote – kann hierarchisch oder zentralisiert sein, unter Einsatz von KI ist sogar eine autonome Abstimmung der beteiligten Waffen untereinander möglich. Wenn eine von ihnen wegfällt, können sich die anderen autonom reorganisieren. Neben den USA hat auch China hier enorme Fortschritte gemacht, das im Jahre 2016 auf eine Demonstration durch das Pentagon mit 103 Drohnen binnen Monaten mit einer eigenen mit 119 Drohnen antwortete. Wie Schwärme im Tierreich, nach denen sie modelliert sind, macht der Schwarm weiter, wenn Einheiten aus ihm eliminiert werden. Das macht sie so gefährlich und so schwer angreifbar. So können z. B. große Teile der Schwärme von Hunderten Explosivstoffe oder Chemikalien tragender Einheiten durchkommen, obwohl ein Teil getroffen oder sonstwie außer Gefecht gesetzt wurde. Kritiker*innen bis hin zu dem Pentagon nahestehenden externen Mitarbeiter*innen fordern den Verzicht auf ihren Einsatz, weil sie zu den Massenvernichtungswaffen zu zählen seien

Dass die Frage der Produktion von vollautonomen Killerwaffen hochempfindlich ist, lässt sich auch daran ablesen, dass maßgebliche Verteidigungsministerien der westlichen Welt wie die der USA und Großbritanniens immer wieder öffentlich betonen, dass die menschliche Entscheidung beim direkten Einsatz stets eine Rolle spielen werde. Wohl ein bloßes Lippenbekenntnis, denn in diesen beiden Regierungen ist auch anerkannt, dass die Zwänge der Konkurrenz und die enormen mit dem Einsatz verbundenen Geschwindigkeitsvorteile ihn erzwingen könnten. Das mag der seit Jahren laufenden Bewegung für das Verbot autonomer Killerwaffen vielleicht einen Schub geben. Viele hunderte Prominente wie Stephen Hawking, Elon Musk, Steve Wozniak, Alphabets Mustafa Suleyman haben sich dafür eingesetzt. Seit Jahren schon tobt die Schlacht hierüber vor der UNO ohne Ergebnis: es steht etwa unentschieden. Die Geschichte der Verbotsbewegungen gegen unmenschliche Waffen – von der Armbrust, über Feuerwaffen und U-Boote bis zu cruise missiles ist nicht gerade ermutigend.

Bei allen Geschwindigkeitsvorteilen: Die Fragwürdigkeit des Einsatzes voll autonomer Waffen liegt vor allem darin begründet, dass die Schwierigkeiten der Objekterken-

nung mit hohen Risiken verbunden sind. Im Grunde genommen ähnelt der Einsatz vollautonomer Waffen dem Einsatz vollautonomer Automobile, nur dass im einen Fall die Vermeidung des Schadens für Menschen zur Zielsetzung gehört, im anderen die Zerstörung und Tötung. Schon bei vollautonomen Autos hat sich die Objekterkennung und -interpretation als Grund für Schadensverursachung erwiesen. Das ist bei voll autonomen Waffen grundsätzlich nicht anders, verschärft aber durch die enormen Geschwindigkeiten der Prozesse und die häufige Unklarheit und Verworrenheit der Umweltbedingungen. Selbst bei großer Anzahl der Schichten „tiefer neuronaler Netzwerke" bleiben beträchtliche Unsicherheiten. Die Fähigkeiten zur Identifizierung bzw. Erkennung von Zielen ist, so summiert die schwedische NGO „sipri", insgesamt ziemlich rudimentär. Noch immer kann KI, wie es immer plakativ heißt, nicht zwischen einem Apfel und einer Tomate unterscheiden. In der Mehrzahl der Fälle kann die automatische Zielerkennung nur große und wohldefinierte militärische Objekte erkennen, wie Panzer, Flugzeuge, U-Boote, und auch das nur unter optimalen Bedingungen und mit erheblichen Fehlerquoten. Bestenfalls kann die Software nur erkennen, ob das Ziel ein Mensch ist, ohne unterscheiden zu können, ob Zivilist oder Soldat. Der Samsung SGR-A 1 (nun außer Dienst gestellt) sollte immerhin erkennen können, ob das Objekt Gebärden der Kapitulation machte (erhobene Arme). Immerhin gehen an die Öffentlichkeit gelangte Informationen über das Projekt „Maven" davon aus, dass – sicher nur bei optimalen Bedingungen - eine Identifikationssicherheit von 80 Prozent erreicht werden könne. Die Verlässlichkeit solcher Angaben ist mit Zweifeln behaftet, weil das Pentagon offiziell zu Fragen der Objekterkennung wegen der Empfindlichkeit des Themas grundsätzlich keine Angaben macht.

Eine relative Sicherheit wird den vollautonomen Killerwaffen bei Vorliegen einer Reihe von außergewöhnlichen Bedingungen zugeschrieben. Dazu gehört der Einsatz in genau abgegrenzten Land- und Seegebieten, in dem sich nur „feindliche" Objekte aufhalten können. Dann etwa im Fall der Grenzkontrollen, wie an der demilitarisierten Zone zwischen Nord- und Südkorea, wenn Objekte per definitionem nur feindlich sein können (aber – so ein geltend gemachter Einwand – bei nordkoreanischen Flüchtlingen nach Südkorea?). Zu derartigen Situationen wird auch die Grenze zwischen Israel und Gaza gerechnet. Die Bedingungen klarer Kriegsfronten erleichtern daher den Einsatz. Aber wo gibt's die noch? In Zeiten der „asymmetrischen Kriegsführung" und der Aufstandsbekämpfung herrschen unklare Umfeldbedingungen. Ihre Problematik wird allerdings schon jetzt bei Drohnen-Einsätzen in verbrecherischer Weise zu Lasten der anvisierten Menschen gelöst. Die sogenannte „pattern-of-life analysis" erklärt sie auf der Basis ihrer Erscheinung und ihres Verhaltens im Überwachungsbild zu Zielen und tötet sie und weitere etwa bei sozialen Anlässen (Hochzeit, wie in dem 2013 von der New York Times berichteten Beispiel) oder auf der Straße anwesende „Zivilisten" gleich mit. Letztlich spielt dabei auch immer eine Rolle, dass das Risiko in der Regel auf der „Feindesseite" liegt. Da nimmt man dann durchaus Risiken von „collateral damage" in Kauf. Die Last, sein Verhalten bei Strafe des Todes an den Wünschen der Aggressoren auszurichten (z. B. die bedrohten Lebenszusammenhänge zu verlassen und so die Aufständischen bloßzustellen und sichtbar zu machen), wird den angegriffenen „Lebenszusammenhängen" auferlegt. Du musst weggehen, sonst bist du tot. Einsatzbereiche sind denkbar im Fall von Flüchtlingskontrolle (Frontex am Mittelmeer und die Bewachung von Lagern) und auch in der Bekämpfung von „Terrorismus" und Aufständen.

Grundsätzlich haben wir diese beim Einsatz von KI betriebene eliminatorische Tendenz schon im KI-Artikel (Disrupt, Die Rückkehr der Künstlichen Intelligenz) thematisiert. Genau an dieser Stelle tut sich erneut der dort beschriebene gewaltige Abgrund zwischen der armseligen KI und dem Potential, besser: dem logischen Reichtum des Lebendigen auf, der selbst einen 1,5 Millimeter langen Fadenwurm so unendlich überlegen macht. Die, wie sie auch bei den Militärs heißt, „artificial general intelligence" (AGI), eine Intelligenz, die „wie Menschen lernen und denken könnte" (Tenenbaum), könnte zwar nicht nur Umgebung und Kontext berücksichtigen, sondern auch die Gesetze und ethischen Regeln der Kriegführung beachten. Das aber ist ein (böser, ein Alb-) Traum, dessen Realisierung in unmessbar weiter Ferne liegt. Die Expert*innen hantieren zur Frage der Entwicklungsdauer mit beliebigen Zahlen unter hundert Jahren, um wenigstens die Illusion aufrechtzuerhalten. Schmidhuber beziffert sie auf dreißig, dann könnte das Wachstum künstlicher, elektronischer sogenannter „neuronaler" Verbindungen die derzeit Millionen mal größere Anzahl derjenigen erreichen, mit denen das Gehirn operiert. Aber Schmidhuber vergisst die unzählbaren Verbindungen in der „Leib-Seele-Dimension". Er unterstellt zudem, dass es sich um ein quantitatives Problem handelt. Es ist jedoch vielmehr ein qualitativ-logisches. Eines, das die „Leistung" des Fadenwurms noch immer unerreichbar macht, lange bevor, sagen wir mal, das Entwicklungsstadium eines Rabens erreicht ist. Bis dahin wird's dabei bleiben, dass die Differenz durch ungeregelten Overkill wettgemacht wird.

CYBERWAR

Die wirklich gefährliche Situation herrscht auf dem Gebiet der informatischen Kriegsführung, „Cyberwar" genannt. Die Prozesse sind hier weitgehend autonom und so führt die enorme Geschwindigkeit der Prozesse zu

Möglichkeiten der Eskalation im Bereich von Millisekunden. Lehrbeispiel auf einem ähnlichen Gebiet des Preiskriegs im Bereich des Hochfrequenzhandels ist das Beispiel des Börsenhändlers Waddell & Reed, der durch den Blitzkrieg der Verkaufsalgorithmen am 6. Mai 2010 innerhalb von Sekunden in den Ruin getrieben wurde. So etwas kann im Bereich der oben behandelten autonomen Waffen nicht passieren, weil die Trägheiten der physischen Bewegung für enorme Zeitpuffer sorgen. Die Gefahr des Cyberwar für die Welt liegt in dem ungeheuer großen Einsatzfeld begründet. Infolge der inzwischen erreichten Vernetzung informationstechnologischer Geräte, nunmehr drastisch in Bereiche privaten häuslichen Lebens erweitert durch das Internet of Things (IoT), liegt ein Gesamtkomplex von im Jahre 2016 auf 6,4 Milliarden. geschätzten Gegenständen im Angriffsbereich. Bis 2020 soll er auf 20 Milliarden. anwachsen.

Dieses Einsatzfeld ist den Waffen des Cyberwarfare ausgeliefert, bei nur begrenzten Verteidigungsmöglichkeiten. Die Waffen sind „malware" („malicious software"), Viren, Trojaner, „worms" (Würmer), „botnets". Den ersten Höhepunkt der Entwicklung bildete schon 1998 der berühmte „Internet Worm". Die US-Regierung zählte im Jahre 2015 70000 Vorfälle. Die Dunkelziffer ist enorm hoch, weil angegriffene Unternehmen keine Auskunft geben, denn sie wollen so etwas nicht an die große Glocke hängen. Diese Zahl gibt also weitgehend Angriffe auf Regierungssysteme wieder. Einen Höhepunkt bildete im Jahre 2010 der Wurm „Stuxnet". Der Wurm zielte auf die von Siemens entwickelte Software, mit der im Iran und seinen Zulieferern Zentrifugen zur Fütterung des Atombombenprogramms betrieben wurden. Als Urheber wurden Israel und die USA geoutet. Er war auch deswegen bemerkenswert, weil er nach seiner „Auswilderung" völlig autonom agierte. Denn er musste sein Eindringen in die Systeme selbständig über USB-Eingänge suchen. Die Selbstvervielfältigungsrate der malware im Verlauf der Operation lag allerdings nur bei drei, heute wäre sie viel größer. Ein anderes Beispiel war die malware, mit der die gesamte Servicestruktur Estlands (Banken, Telekom etc.) lahmgelegt wurde. Als Urheber wird Russland vermutet, weil dies unmittelbar nach der Entscheidung zur Verlegung einer sowjetischen Gedenkstätte geschah.

Zu den Übeltätern der Angriffe werden Spionage- und Sabotageabteilungen und Wissensdiebe gezählt, zu den Wohltätern Whistleblower. Die Angreifer sind im Vorteil, die Angegriffenen müssen reagieren und haben zudem Schwierigkeiten, die gefährdeten Schwachstellen herauszufinden. Das geschieht über den Einsatz von Hackern. Es werden darüber hinaus regelrechte Turniere und Manöver abgehalten, um verletzliche Stellen aufzudecken.

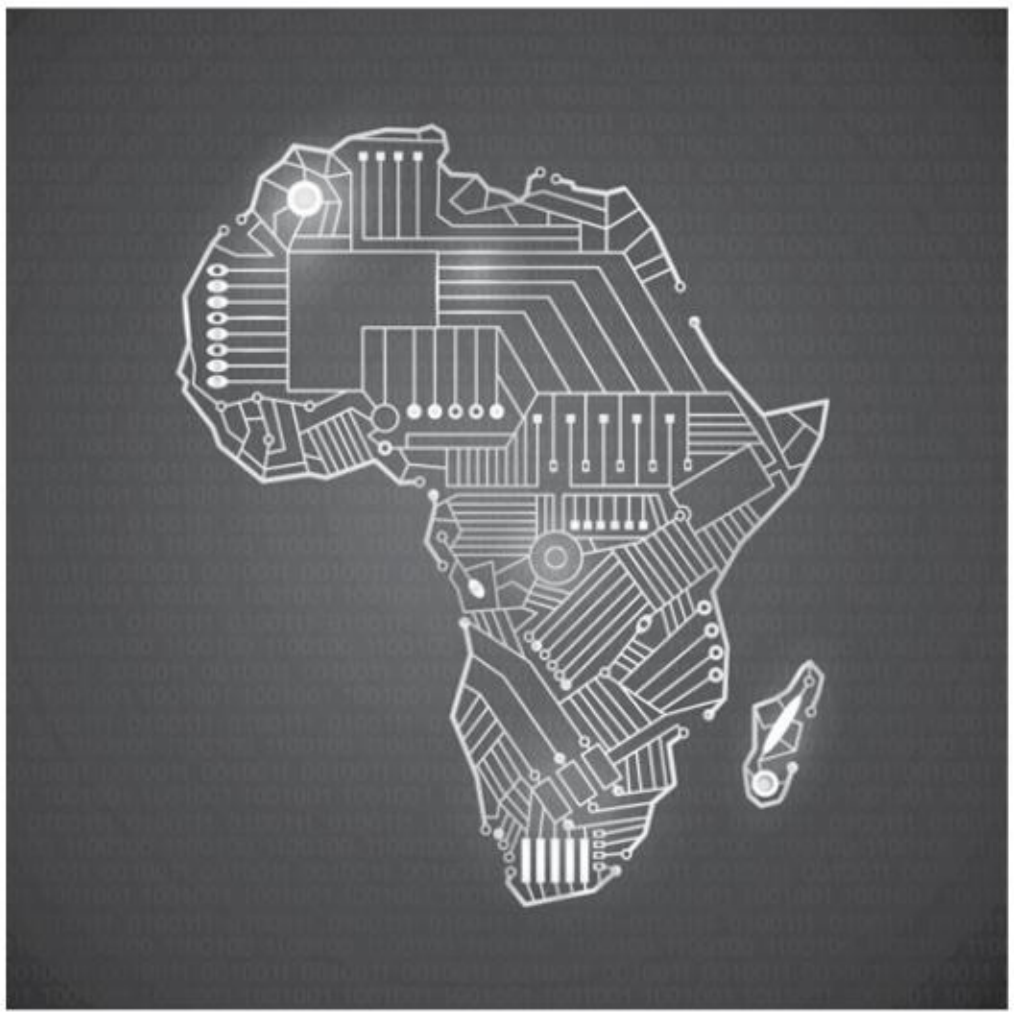
Der Rüstungswettbewerb ist im vollen Gange. Die Eskalationsrate des Cyberwar ist bei vollautonomen Prozessen enorm. Sie liegt manchmal im Millisekundenbereich und damit auch der vollständige Kontrollverlust. Immerhin sind die Systeme weitgehend statisch, die Möglichkeiten der autonomen eigenständigen Weiterentwicklung ist begrenzt, ganz im Gegensatz zu biologischen Systemen, die über Veränderungs- und Mutationsmöglichkeiten verfügen. Der Cyberwar verdient es, neben der Gefahr der Klimakatastrophe, zu den besonders menschheitsbedrohenden, ja weltbedrohenden Innovationsoffensiven gezählt zu werden. Prozesse, die in Millisekunden außer Kontrolle geraten können, bringen die Gefahr eines totalen kriegerischen Konflikts mit sich. Mehr noch. Diese Bedrohung hat das Potential, den „Atomstaat" als Mittel der internen Erpressung und Zurichtung im Sinne eines gesellschaftspolitischen Transformationsinstruments zu beerben, ja gar zu übertreffen. Dies, je mehr Menschen, Institutionen, Unternehmen und weitere gesellschaftliche Bereiche dem Kreis der Betroffenen einverleibt werden. Mit großer Besorgnis wurden in diesem Zusammenhang die Cyberangriffe Anfang Oktober 2018 auf das Computernetz der Zentrale der Organisation für das Verbot chemischer Waffen (OPCW) der Niederlande gesehen, deren Urheber im russischen Militärnachrichtendienst (GRU) gesucht wird.

GIBT ES EINEN GROSSEN KRIEG?

Die Möglichkeit und Wahrscheinlichkeit der Zuspitzung der Rüstungskonkurrenz zu einem großen Krieg hängt nicht von irgendwelchen partikularen Konflikten ab, wie wir an der analogen Situation vor dem ersten Weltkrieg erkennen können. Wenn Krieg genutzt wird, um aus einer Krise, einer Stagnation der Innovations- und zugleich ökonomischen Dynamik heraus zu kommen, dann resultiert der Krieg aus der Krisenhaftigkeit des Kapitalismus. Der Weg, sich dem entgegen zu setzen, ist also der antikapitalistische Kampf. Und das nicht auf der Grundlage des orthodoxen, und das heißt auch des marxorthodoxen, Verständnisses des Kapitalismus. Zum Kapitalismus gehört auch der sich zyklisch erneuernde technologische Angriff mit dem Ziel der Wiederherstellung des kapitalistischen Kommandos auf neuem Niveau und zugleich auch der Ausbeutungsbedingungen und -tiefe. Und das bedeutet – gegen die Einschränkungen von marxorthodoxer Seite – der Kampf gegen die Technologie als solche. Das Buch über „Krisen, Kämpfe, Kriege" belegt, wie Krieg auch von Seiten der Sowjetunion als Mittel der Durchsetzung des technologischen Angriffs benutzt wurde.

Digitaler Kolonialismus

Kolonialer Digitalismus in Afrika



Bislang repräsentiert Afrika lediglich Ursprung und Ende der digitalen Wertschöpfungskette. Als Rohstoffquelle seltener Erden und als Müllhalde für digitale Hardware. Die Digitalisierung und vor allem auch die eigentliche Wertschöpfung finden woanders statt. Heute wird die Vernetzung Afrikas als das große Zukunftsprojekt und als zentrale Chance gefeiert, sich aus der Armut zu befreien.

In den USA und Europa verlangsamt sich das Wachstum der Tech-Giganten auf dem Gebiet der digitalen Erschließung bisher „unverbundener Regionen". Hier gibt es bereits Sättigungserscheinungen insbesondere bei den sozialen Netzwerken. Die am wenigsten angebundenen Länder kommen allesamt aus Afrika. Dort arbeiten nicht nur Facebook und Google, sondern auch ihre chinesischen Kontrahenten aus dem Hause Tencent und Alibaba daran, ihre digitalen Netze über den nach Asien zweitgrößten Kontinent zu werfen. Per Ballon oder Drohne sollen auch die Bewohner*innen der entlegensten Regionen an- und eingebunden werden: Nicht nur einen Großteil der brachliegenden Produktivität, sondern auch soziale Prozesse anzapfen und reorganisieren, das ist erklärtes Ziel. Facebook geht hier besonders selbstbewusst vor.

NEOKOLONIALE BEVORMUNDUNG

Facebook gibt vor, mit seinem Angebot „Free Basics" die Digitale Spaltung der Welt beseitigen zu wollen. Vier Milliarden Menschen, insbesondere im globalen Süden, will Facebook mit seinem Projekt erstmals ins Internet bringen. Doch statt auf die Bedürfnisse der lokalen Bevölkerung einzugehen, teilt der Werbekonzern das Internet in mehrere Klassen, versucht die Nutzer*innen auf die eigene Plattform zu lenken und sammelt dabei möglichst viele Daten über Standorte und Gewohnheiten der Nutzer*innen.

Dazu kooperiert das Unternehmen mit lokalen Mobilfunkanbietern und stellt Free Basics als Handy-App in mittlerweile 65 Ländern Afrikas, des Mittleren Ostens, Asiens und Mittelamerikas bereit. In der App sind neben Facebook auch abgespeckte Versionen anderer Dienste sowie eine Reihe anderer Websites enthalten. Diese werden an die oftmals schwächere Netzinfrastruktur der jeweiligen Länder angepasst – ohne Bilder und Videos. Der Zugriff ist kostenlos. Wer auf den Rest des Internets zugreifen möchte, muss zahlen. Derzeit nutzen mehr als 50 Millionen Menschen das „Umsonst"-Angebot von Free Basics.

"Facebook führt Leute nicht an das offene Internet heran, wo sie Dinge lernen, erschaffen und bauen können," sagt Ellery Biddle, Sprecherin der Medienaktivist*innen-Gruppe Global Voices. *„Facebook baut dieses kleine Netz auf, das Nutzer zu passiven Konsumenten zumeist westlicher Inhalte macht. Das ist digitaler Kolonialismus."*

Die Suchergebnisse nicht unterstützter Suchmaschinen außerhalb des winzigen Angebots werden angezeigt, aber mensch kann sie nicht anklicken. Das bedeutet, dass Nutzer*innen nur die Überschriften vieler Artikel, aber nicht deren Inhalt lesen können. Fake News lassen sich so nicht erkennen. *„Bei dem Angebot fehlen wichtige Webseiten, die Ghanaer nutzen wollen"*, sagt Kofi Yeboah, der die App in Ghana untersuchte und fügt hinzu, dass populäre Nachrichtenseiten wie MyJoyOnline und CityFM komplett fehlen.

Die Daten aller unter Free Basics erreichbaren Webseiten werden durch die Facebook-App geleitet. Darüber hat Facebook Zugriff auf die Nutzungs-Häufigkeit und -dauer sowie die gelesenen Inhalte auch bei Dritt-Anbietern.

VORZEIGEPROJEKT „M-PESA"

Kenia gilt als Silicon Savannah – sozusagen Afrikas Antwort auf das Silicon Valley der USA und Indiens Bangalore. Dortige Kund*innen eines Telefondienstanbieters

hatten Telefonguthaben, das an andere Nutzer*innen versendet werden kann, in ein Zahlungsmittel verwandelt. Wer Geld brauchte, dem wurde „air time" überwiesen, die er dann mit Bekannten oder Nachbar*innen gegen Bares eintauschen konnte. Eine britische Nichtregierungsorganisation entwickelte daraus ein System zur Verwaltung von Kleinkrediten. Schließlich kam bei der afrikanischen Vodafone-Tochter Vodacom, der Mutter von Safaricom, jemand auf die Idee, das Ganze zu einem Geldüberweisungssystem auszubauen.

Der Name setzt sich zusammen aus dem Kürzel „M" für *mobile* und dem aus dem Swahili stammenden Wort „Pesa" für Bargeld. Bereits nach einem Jahr nutzten zwei Millionen Menschen das Transfersystem. Die große Mehrheit war bis dahin von den herkömmlichen Geldinstituten links liegen gelassen worden. Wie in den meisten afrikanischen Staaten verfügten kaum zehn Prozent der Haushalte über ein Bankkonto.

Gut zehn Jahre nach seinem Start hat sich M-Pesa heute zum mit Abstand beliebtesten bargeldlosen Zahlungsmittel des Landes entwickelt. Jetzt kann man in Cafés, an Tankstellen oder bei Straßenhändler*innen per Handy zahlen. Auch die monatliche Stromrechnung oder das Schuldgeld lässt sich so begleichen. Da das Unternehmen vom Gesetzgeber nicht als Bank, sondern als Kommunikationsdienstleister betrachtet wird, hat der Staat die Summe pro Transfer auf 1400 US-Dollar beschränkt.

Seinen Siegeszug hat das Geldüberweisungssystem auch in anderen Staaten des Kontinents fortgesetzt. Inzwischen sind mehr als 140 Anbieter in 39 afrikanischen Staaten aktiv. Und auch nach Albanien und Rumänien wurde die Technik mittlerweile exportiert.

Angebote wie M-Pesa und seine darauf aufbauenden Dienste kommen vor allem der afrikanischen Mittelschicht zugute – jener Gruppe von Menschen, die jährlich über mehr als 5000 US-Dollar verfügen. Diese Gesellschaftsschicht wächst, doch das große Problem Afrikas ist seine Unterklasse, die in absoluten Zahlen ebenfalls wächst: Menschen, die von zwei US-Dollar und weniger am Tag überleben müssen.

In Kibera, einem der großen Slums in Nairobi, gibt es mittlerweile eine den gesamten Slum abdeckende WLAN-Verbindung, für die man acht Cent pro Stunde oder zwölf Euro pro Monat zahlen muss. Genutzt wird sie hauptsächlich für Wetten und Glücksspiele. Dies wird vorherrschend als einzige Exit-Strategie empfunden, der Armut entkommen zu können. Die vermeintlich „segensreiche" digitale Vernetzung transformiert durchaus Machtstrukturen, sie bietet den „Abgehängten" und „Überflüssigen" jedoch keineswegs aus sich heraus echte Teilhabemöglichkeiten. Die digitale Kluft (digital divide), also die unterschiedlichen Zugangsmöglichkeiten zu digitaler Infrastruktur, beschreibt die vielfältige „social divide" nur unzureichend. Das „Vernichtsen", also das Degradieren eben jener Überflüssiger in der Schuldenfalle, funktioniert auch online.

ZWEIFELHAFTES LEAPFROGGING

Die Hoffnung, dass zumindest einige Länder Afrikas dank neuer Technologien die Phase der Industrialisierung überspringen (*leapfrogging*) und direkt in der digitalen Moderne landen – und so den ökonomischen Rückstand zum Rest der Welt aufholen können –, hat sich bislang nicht erfüllt. Sie wird es auch nicht, denn der Hochglanzprospekt von Landwirt*innen, die die Bewässerung und Düngung ihrer Äcker per Drohnen-Analyse optimieren können, ist ein Zerrbild, welches Infrastrukturprobleme auf eine „noch zu schwache" digitale Infrastruktur reduziert. Ein Trugschluss, denn insbesondere die Digitalisierung schafft kaum Jobs. Firmen mit rein digitalen Geschäftsmodellen schaffen relativ wenige Arbeitsplätze und beschäftigen oftmals hoch qualifizierte Mitarbeiter*innen aus dem Ausland in den afrikanischen Startups.

Während 2007 noch weniger als vier Prozent der Menschen in Afrika Zugang zum Internet hatten, sind es nun bereits 30 Prozent. Dennoch haben Länder wie Südafrika und Nigeria gerade die stärkste Rezession seit zwei Jahrzehnten hinter sich – ohne dass die „mobile Revolution" das hat verhindern können. Es geht um viel grundlegendere Probleme wie z. B. Bildung, die sich über die Digitalisierung nicht von allein lösen. Wer zu den 40 Prozent in Subsahara-Afrika gehört, die nicht lesen und schreiben können, schafft es überhaupt nicht ins Netz.

OFFSHORING IM CALLCENTER

Nach der Installation des Unterseekabels Atlantis 2 im Jahr 2000 dauerte das Routing von Sprachdaten nach Europa nicht mehr als 80 Millisekunden. Das ermöglicht eine ausreichende Verbindungsqualität, die sich nicht von innereuropäischen Telefongesprächen unterscheidet. Das war der Startschuss für eine Reihe von Callcentern z. B. in Dakar. Hier konnte insbesondere französischen Kund*innen vorgetäuscht werden, sie würden einen Telefondienst einer Servicekraft in einem Kundencenter irgendwo in Frankreich in Anspruch nehmen.

Damit „durften" Afrikaner*innen für ausbeuterische Preise und unter autoritärer Aufsicht Telefon-Dienstleistungen für Konsument*innen im Westen erbringen. Voraussetzung war das Antrainieren eurozentristischer

bürgerlicher Verhaltensnormen in eigens dafür eröffneten Recruiting- und Training-Centern. Um als Callcenter-Mitarbeiter*in für französische Firmen angestellt zu werden, muss insbesondere der senegalesische Akzent „ausradiert" werden.

Auch um diesen Sektor der Offshore-Dienstleistungen geht es beim Ausbau der europäischen Wirtschaftsbeziehungen der von Deutschland initiierten G20-Offensive „Compact with Africa". Eine „Kooperation auf Augenhöhe" ist hier eher nicht zu finden – neokoloniale Stereotype hingegen reichlich.

DAS GESCHÄFT MIT DEN DATEN

Was hingegen tatsächlich boomt, ist das Geschäft mit persönlichen Daten. Dank M-Pesa weiß Vodacom fast alles über Vermögen und Vorlieben seiner Kund*innen, auch darüber, wo sie sich gewöhnlich aufhalten. Für Unternehmen, die sich auf den kenianischen Markt begeben wollen, sind solche Informationen Gold wert. Ebenso verkaufen Google und Facebook nutzer*innenspezifische Informationen, zumeist an Investor*innen außerhalb von Afrika.

Google bemüht sich im Bereich BigData auf dem Gesundheitssektor einen Fuß auf den Zukunftsmarkt Afrika zu bekommen. Immerhin prognostizieren die UN, dass in 30 Jahren 25 Prozent der dann 9 Milliarden. Menschen betragenden Weltbevölkerung in Afrika leben werden. Googles erstes Forschungszentrum in Afrika soll Ende 2018 in Accra (Ghana) eröffnen. Forschungsschwerpunkt ist die Künstliche Intelligenz in der Gesundheit.

Das in Johannesburg, Südafrika ansässige Versicherungs- und Investment-Unternehmen *Discovery* exportiert sein Vitality-Modell mittlerweile über den afrikanischen Kontinent hinaus weltweit in 19 Länder in den USA, Europa, Asien und Singapur. Das Gesundheits-Programm Vitality ist eines der konsequentesten Erziehungsprogramme, welches abhängig vom Bewegungs- und Ernährungs-Status der Kund*innen den Versicherungs-Tarif individuell anpasst. Die Generali hat als erste Krankenversicherung in Deutschland das Vitality-Programm übernommen und mietet die Datenauswertung als Dienst beim Partner-Unternehmen Discovery. Die paternalistische Gesundheitserziehung entwickelt sich zum Exportschlager, den u. a. die europäische Versicherungsbranche zur Entsolidarisierung und Ökonomisierung des Gesundheitswesens nutzt. Die Verantwortung für die eigene Gesundheit soll individualisiert werden. Ehemals alle betreffenden „Zivilisationskrankheiten" werden als Konsequenz eines individuell-unachtsamen Lebensstils uminterpretiert. Bewegungsarmut soll zur persönlichen Verhaltensstörung erklärt werden, die die Gesellschaft so teuer zu stehen kommt, dass jeder in Eigenverantwortung dafür haften soll. Das Ergebnis sind hochmoderne, subtile Verhaltenslenkungsprogramme auf dem Gesundheitsmarkt – quasi als Re-Import eines kolonialen Behaviourismus.

ANSÄTZE VON SELBSTBEHAUPTUNG

Die Übernahme digitaler Infrastrukturkonzepte an sich und zudem nach westlichem Vorbild führt nicht zu einer Verbesserung der Lebensverhältnisse. Das ist derzeit mehr als deutlich in Afrika. Zudem reißt die Kritik an der neokolonialen Bevormundung von „Entwicklungs-Angeboten" wie Free Basics nicht ab. Leider hat sie (noch) nicht wie in Indien dazu geführt, dass Facebook das Angebot zurückziehen muss. Im Februar 2017 hatte die indische Netzaufsichtsbehörde Facebook den Betrieb von Free Basics mit Verweis auf die heftigen Widerstände und die Verletzung der „Netzneutralität" (kein Inhalt darf in seiner Erreichbarkeit vor anderen vorrangig behandelt werden) untersagt.

Es sind die Resistenzen und Beharrungstendenzen von einzelnen Individuen, aber auch Kollektiven, die sich dagegen wehren, die eigenen Lebensformen und Selbstverständnisse aufzugeben. Menschen, die sich gegenüber einer Verdatung verweigern, sodass Konzerne wie Facebook und Google all ihre destruktive Energie aufwenden müssen, um diese sozialen Strukturen aufzuknacken, zu verflüssigen, um sie dann in eine verwertbare Isolation zu treiben. Das brachiale Durchsetzen von vorgegebenen Kommunikationsnetzen zur Lenkung stößt insbesondere dort auf Widerstand, wo die Ähnlichkeit zur klassischen, analogen kolonialen Zerstörung besonders hoch ist.

Den Bedürfnissen angemessene Formen der Vernetzung und damit tatsächlich selbstbestimmter und selbstorganisierter Wissensaustausch kann ganz anders aussehen. In einem regionalen Zusammenschluss mehrerer Dörfer in Südafrika tauschen die Bewohner*innen landwirtschaftliche Erfahrungen und für gemeinsame Beschaffung relevante Kennzahlen über ein einfaches und robustes System, das sie zusammen mit anarchistischen Hacker*innen entwickelt haben: In jedem Dorf steht ein Rechner, auf dem die Daten lokal gespeichert sind und ergänzt werden können. Ein sich selbst synchronisierender USB-Stick trägt eine Kopie dieser Daten und wird bei jedem Besuch in eines der anderen Dörfer mitgenommen und zum Datenabgleich in den dortigen Rechner gesteckt – fertig. Die Reisetätigkeit der Bewohner*innen stellt das Netz dar. Per Datenabgleich mit dem „Reise-Stick" befindet sich (mit wenigen Tagen Verzögerung) auf den Rechnern der beteiligten Dörfer das gleiche, jeweils aktualisierte Wissen.

The Hacker Way

"We have cultivated a unique culture and management approach that we call the Hacker Way."

(Mark Zuckerberg)

Zum Börsengang von Facebook im Mai 2012 veröffentlichte Mark Zuckerberg ein Statement[9], welches potentiellen Investor*innen das Unternehmen erklären und attraktiv machen sollte. In diesem Statement beschrieb er die Unternehmenskultur von Facebook als "hacker culture" und führte aus, was er damit meinte. Nun sind Statements zum Börsengang (IPO) im wesentlichen Werbung für die jetzt erhältlichen Aktien, Zuckerbergs Statement zum IPO wirbt ganz entscheidend mit einer Ideologie, die es wert ist, analysiert zu werden, weil Facebook bei weitem nicht das einzige Unternehmen ist, welches diese Ideologie teilt. Barbrook und Cameron haben dieser Ideologie bereits 1995 den Namen "Kalifornische Ideologie" gegeben.[10]

Wenn Zuckerberg hacker culture als Unternehmenskultur von Facebook reklamiert, dann nicht, ohne sich früh im Text von den negativen Konnotationen des Begriffs "Hacker" zu distanzieren. Für ihn sind Hacker wohlmeinende Geister, die Probleme anpacken, lösen, und sich nicht von Bedenken abhalten lassen. Sein Versuch, den Begriff zu besetzen und umzudefinieren, ist bemerkenswert, weil Hacker üblicherweise mit Untergrund, Computerkriminalität, Einbrüchen, Raubkopien und mangelnder Körperhygiene in Verbindung gebracht werden - damit lässt sich schlecht für einen Börsengang werben. Hacker (nicht nur in den USA) haben massive Repression und drakonische Strafen zu befürchten. Gleichzeitig werden Hacker in der Popkultur glorifiziert, sie haben fast übernatürliche Fähigkeiten, Dinge mit Computern zu machen, die für Normalsterbliche unerreichbar sind. Und dann gibt es noch die realen Hacker mit ihrer eigenen Subkultur[11] und deren Ausstrahlung auf Programmierer*innen – also das von Facebook gewünschte Personal fürs eigene Unternehmen.

Diese Hacker-Subkultur bildete sich um die Erfahrung herum, Dinge tun zu können, zu denen andere nicht in der Lage waren. Dies bezieht sowohl das Benutzen fremder Rechner ohne Wissen oder gar Zustimmung der Betroffenen als auch den kreativen Umgang mit verfügbaren Ressourcen ein. Dinge (meist Computer, aber nicht nur) umzubauen und neu zu kombinieren und auf eine Weise zu benutzen, für die sie gar nicht vorgesehen waren. Diese Erfahrungen und das angesammelte Wissen waren die benötigte Reputation, um in den sozialen Orten[12], die sich die Hacker schufen, Anerkennung und Respekt zu bekommen. Anfangs schien diese Welt ohne Grenzen zu sein, alles war möglich (wenn vielleicht auch nicht legal). Zum Einstieg in diese Welt bedurfte es nur eines "Homecomputers", eines Modems und einer Telefonleitung sowie der Fähigkeit, die monatliche Rechnung zu bezahlen. Der demokratisierende Effekt war enorm: Um in der ersten Liga mitspielen zu können, brauchte es kein Vermögen, keine speziellen Zugänge, Rechte oder Titel, sondern "nur" Wissen und Fähigkeiten. In dieser Liga spielte man nicht nur mit anderen Hackern, sondern auch mit den Profis, den offiziellen Systemadministrator*innen der Rechner, die man gerade "besuchte". "We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth."[13]

Die Angewohnheit, sich illegal auf Rechnern rumzutreiben, unberechtigt Infrastruktur zu benutzen und Daten zu durchforsten, die deren Besitzer*innen lieber geheim hielten, hat Strafverfolgungsorgane auf der Plan gerufen. Diese sahen das Treiben der Hacker bei weitem nicht so harmlos wie diese selbst. Der Ermittlungsaufwand und die drakonischen Strafen belegen das[14].

Die kombinierte Erfahrung mit den Autoritäten der Rechner, den Systemadministrator*innen, die auch nur mit Wasser kochten und den Hackern immer wieder unterlegen waren, und den Autoritäten des Staates, den Strafverfolgungsorganen, die sie mit großem Aufwand

9 https://www.theguardian.com/technology/2012/feb/01/facebook-letter-mark-zuckerberg-text

10 The Californian Idologie, Essay von Richard Barbrook und Andy Cameron, 1995, Mute online Magazin

11 Siehe CCC oder auch underground.txt (Suelette Dreyfus, Julian Assange, 1997)

12 Mailboxen, Chaträume, Mailinglisten

13 A Declaration of the Independence of Cyberspace, John Perry Barlow, 1996

14 Underground.txt (s. o.), THE HACKER CRACKDOWN, Bruce Sterling, 1994

und Vernichtungswillen jagten, führte zu einem großen Misstrauen gegenüber Autoritäten generell in der Szene.

Überdies führte (und führt) diese Erfahrung zu einer verengten Bewertung der eingesetzten Technologie. Während die demokratisierende und durchaus auch befreiende Wirkung aus der Sicht des Individuums durchaus real sein kann, verstellt dies die Sicht auf die gesellschaftlichen Auswirkungen, wenn die eigene Erfahrung auf gesellschaftliche Dimensionen extrapoliert wird. Die als befreiend wahrgenommene Technologie verkehrt sich in ihr Gegenteil, wenn sie von mächtigen Institutionen eingesetzt wird – um das zu belegen, reicht ein kurzer Blick Richtung NSA, China, Facebook … Die oben zitierte „Declaration of the Independence of Cyberspace" verklärt den Cyberspace gar zur Natur, und Hacker zu antikolonialen Freiheitskämpfern derselben gegen staatliche Regulierungen – ein Schulterschluss mit Facebook und anderen Akteuren, die allerdings nicht Freiheit im Sinne haben, sondern Profit, und sich gegen alle Regulierungen stellen, die diesen schmälern. Aus dieser Warte wird ein kritischer Blick auf die gesellschaftlichen Auswirkungen von Technologie unmöglich.

Vor dem Hintergrund anarchistischer Selbstverwirklichung, dem Misstrauen gegenüber Autoritäten und des Gefühls, einer Elite auf Mission anzugehören, ist der Sprung zum Konzept der Meritokratie nicht mehr weit.

Meritokratie beschreibt eine Herrschaftsform, bei der diejenigen die Herrschaft ausüben sollen, die bewiesen haben, dass sie die geeignetsten für diese Aufgabe sind. Üblicherweise erfolgt dieser Beweis in Form von belegter Fähigkeit, Kompetenz und "Leistung", als bewusster Gegenentwurf zu Herrschaftsformen, bei denen das Personal seine Rolle "erbt", wie etwa der Aristokratie. Die Idee der Meritokratie ist in der Tech-Welt verbreitet, für einige Unternehmen und Projekte ist sie ganz offiziell Vorbild: GitHub, Ubuntu, LibreOffice, um ein paar zu nennen. Auch Mark Zuckerberg feiert die Meritokratie, erhebt sie gar zum Kernelement seiner "hacker culture".

Meritokratie ist zutiefst anti-egalitär. Der Begriff der Gleichheit wird von seiner universalistischen Lesart, der bedingungslosen Gleichheit aller, zurück gestutzt auf eine Gleichheit aller vor der Messlatte "Leistung". Diese Gleichheit ist die Gleichheit des Faustrechts – alle haben das Recht, den Ring zu besteigen, dass die Fähigkeiten in diesem Ring zu bestehen ungleich verteilt sind, ist dabei bekannt und akzeptiert. Zweck des Rings ist es, die "Besten" auszusieben. In der Realität ist das Recht, den Ring zu betreten, oftmals zusätzlich der eigenen sozialen Gruppe vorbehalten: weißen Männern. Die „Gleichheit des Faustrechts" hat die fatale Eigenschaft, viele Verlierer*innen zu produzieren. Da es bei der Meritokratie um die Besetzung von Herrschaftspositionen geht, ist das Recht, den Ring zu betreten, bereits ein Privileg, welches durchaus erbittert verteidigt wird – schon allein deshalb, weil es eine Masse an nicht-Privilegierten braucht, die den sozialen Absturz der Verlieren*innen nach unten begrenzt und abfedert. Dass der Ausschluss bzw. die Entprivilegierung von Frauen, aber auch von „nicht-weißen" Männern tagtägliche Realität ist, belegen zahlreiche Untersuchungen[15].

Vetternwirtschaft, Korruption, Vitamin-B, Seilschaften und "grundlose" Bevorzugung generell sind verhasst, das geht soweit, dass auch affirmative action bekämpft wird. Meritokratie muss auf dem historischen Auge blind sein, "Leistung" und Erfolg legitimieren Privilegien, die ihrerseits zukünftigen Erfolg vereinfachen – Erfolg legitimiert sich selbst, es entsteht tatsächlich eine eigene, sich selbst stabilisierende gesellschaftliche Klasse. Das Versprechen der Meritokratie, dass alle zumindest vor der Messlatte der "Leistung" gleich sind, war schon immer hohl. Wenn diejenigen herrschen sollen, die am geeignetsten sind, dann ist es in der Tat egal, woher und wie sie diese Eignung erworben haben. Meritokratie dient damit höchstens als Begründung für den einmaligen Austausch der Eliten, als Modernisierung des Kapitalismus auf Führungsebene.

"Während Politiker als oberstes Ziel haben, ihren Job zu behalten und den Leuten freundliche Lügen erzählen, konzentrieren sich Hacker darauf, defekte Systeme zu reparieren, und sie sind Experten darin, die unfreundliche Wahrheit zu sagen."[16]. Diese Selbstempfehlung als zukünftige herrschende Klasse, abgeleitet von einem glorifizierten (Selbst-)Bild idealtypischer Hacker, vorgetragen von einer bekannten Szenepersönlichkeit, ist kein isolierter Irrläufer, sondern findet sich selbst in eher dystopischen Beiträgen wieder[17]. In dieser Echokammer befinden sich auch Mark Zuckerberg und andere aus der Chefetage des Silicon Valleys. Sie unterscheiden sich von den Farrs, Riegers und Gongripps der Szene nicht im glorifizierenden Selbstbild, sondern in den milliardenschweren Aktienpaketen, die sie ihr Eigen nennen. Sie wähnen sich strikt meritokratisch als "erfolgreich" und damit als berechtigt, Herrschaft auszuüben.

Das Selbstbewusstsein ist überbordend. Ausgestattet mit signifikantem Sendungsbewusstsein und der Überzeugung, zu wissen, wie es geht und was getan werden muss, stampfen die Protagonist*innen dieser Mentalität Projekte wie internet.org/free-basics aus dem Boden, deren neokolonialer Charakter kaum zu übersehen ist. Diese Men-

15 Sammlung von Erfahrungen: „Elefant in the valley", https://www.elephantinthevalley.com/ , GamerGate https://en.wikipedia.org/wiki/Gamergate_controversy oder Untersuchungen zum Umgang mit Codebeiträgen (commits) von Frauen auf GitHub.

16 Nick Farr auf der SIG-INT, 2010

17 "Ten years after 'We lost the war'", Frank Rieger, Rop Gongripp, 2015, https://media.ccc.de/v/32c3-7501-ten_years_after_we_lost_the_war

talität ist bewusst zerstörerisch – der Einsatz disruptiver Technologien geschieht genau mit der Absicht, bestehende soziale Beziehungen zu unterbrechen und durch eigene, dann technisch moderierte Beziehungen zu ersetzen. Dazu bekennen sich die Protagonist*innen öffentlich, in ihrem Weltbild ist ein derartiges Vorgehen nichts Verwerfliches, sondern schon fast soziale Verpflichtung.

Wenn sich die Zuckerbergs des Silicon Valleys die hacker culture zu eigen machen, dann beerdigen sie bewusst das egalitäre Erbe der Hacker-Subkultur unter einer dicken Schicht meritokratischer Ideologie. Damit dies gelingen kann, braucht es "nur" den Verzicht auf den Universalismus, einer bedingungslosen Gleichheit aller, damit die Mischung aus Meritokratie, libertärer Ideologie und dem Anarchismus der Hacker-Subkultur zumindest oberflächlich konsistent bleibt. Das Angebot sind "flache Hierarchien" statt Hierarchielosigkeit, "Selbstverwirklichung im Job" statt eines freien, selbstverwirklichten Lebens, "individueller Erfolg und Anerkennung" statt kollektiver Lösungen, "den-Chef-duzen" und damit die bestehenden Unterschiede zu verkleistern, und, und, und.

Der Verzicht auf den Universalismus ist folgenschwer, den egalitären Impuls der Hacker-Subkultur gilt es freizulegen, zu erhalten und auszubauen.

Executing command

„Die Grenzen meiner Sprache bedeuten die Grenzen meiner Welt."

(Wittgenstein)

Software ist das, mit dem mensch in Berührung kommt, wenn Computer im Spiel sind. Software braucht zwar eine Hardware, auf der sie läuft, verdeckt diese aber komplett.

Software hat aber noch eine andere Dimension, jenseits der rein technischen Aspekte. Software ist das Medium einer Kommunikation zwischen Programmierer*in (oder genauer: der Auftraggeber*in der Programmierer*in) und Nutzer*in. Kommuniziert wird die Vorstellung, wie eine bestimmte Aufgabenstellung zu bewältigen sei: Wie soll ein Text geschrieben[18], wie ein Bild bearbeitet, wie ein (Verwaltungs-)Vorgang angelegt werden? Diese kommunizierte Vorstellung ist absolut, was nicht in ihr enthalten ist, ist nicht existent. Ein Textverarbeitungsprogramm ohne die Funktionalität z. B. der Fettschrift kann keine Fettschrift – das ist banal, beschreibt aber die Totalität der kommunizierten Vorstellung und gibt ihr den Charakter eines Kommandos – die kommunizierte Vorstellung ist im engen Rahmen der Software nicht verhandelbar.

Die Kommunikation ist inhärent gerichtet, sie geht von der Programmierer*in zur Nutzer*in – die andere Richtung ist nicht enthalten. Selbst wenn der Informationsfluss von der Nutzer*in weg geht – z. B., wenn die Software Nutzungsdaten aufzeichnet und zur Hersteller*in sendet, bleibt die Richtung des Kommandos gleich. Das wird unter anderem daran sichtbar, dass ein solcher Informationsabfluss durch die Nutzer*in kaum zu kontrollieren oder zu unterbinden ist.

Software selbst wird programmiert, sie wird in einer Programmiersprache niedergeschrieben und dann auf Hardware ausgeführt. Das oben beschriebene Kommando existiert also in Form eines Textes in einer Programmiersprache. Ein Ausbruch aus dem Kommandoregime einer Software hängt unter anderem davon ab, wie lückenlos der Text das Kommando beschreibt.

Da Software statisch ist – sie ändert sich erst mit dem nächsten Update – bleibt Freiheit für einen kreativen Umgang mit ihr. Solche Freiheiten können absichtlicher Bestandteil des Kommandos sein, oftmals sind sie aber einfach nur Auslassungen im Programmtext. Die meiste Software entsteht in kapitalistischer Produktion, jedes noch so abwegige Detail zu behandeln kostet Zeit und

18 Wer*welche eine Idee davon bekommen will, wie "exotisch" diese Vorstellungen sein können, sollte sich den Texteditor "vi" ansehen.

Geld und wird deshalb auch nicht behandelt, bzw. erst dann, wenn diese Auslassung zum Problem wird. Das gilt übrigens auch für die meiste open-source-Software, praktisch jedes größere Projekt hängt von Sponsorengeldern ab.

Diese Freiheiten durch Auslassungen sind durchaus beliebte Features bei Nutzer*innen, es ist nicht unüblich, ein Update einer Software zu verweigern, weil damit evtl. die Auslassungen gefüllt werden und damit verknüpfte Freiheit verschwindet. Das wirft auch ein spezielles Licht auf Software, die in Gestalt von Webplattformen, „Software as a Service“ und “cloud” daherkommt – dort finden Updates außerhalb der Kontrolle der Nutzer*in statt und können von ihr nicht verhindert werden. Das Kommando kann geschmeidig auf Ausweichmanöver reagieren.

Wie schon erwähnt, wird Software in einer Programmiersprache geschrieben. Sprache bestimmt, welche (komplexen) Gedanken formulierbar sind. Dinge, Verhältnisse, Tätigkeiten, die keinen Namen haben, für die kein Begriff geprägt wurde, lassen sich nur schwierig denken – und noch schwieriger kommunizieren. Das gilt sowohl für natürliche als auch für Programmiersprachen.

Programmiersprachen haben (bis auf wenige Ausnahmen) eine Richtung, in der sie niedergeschrieben und später auch ausgeführt werden. Sprünge in diesem Programmfluss, z. B. zur Wiederholung von Code in Schleifen, müssen wohldefiniert sein – ein beliebiges Einsteigen oder Herumspringen im Programmcode ist ein sicherer Weg in den Softwareabsturz. Tatsächlich sind diese Abstürze interessant, weil dies Stellen sind, in denen der Programmfluss eine nicht vorhergesehene Abzweigung nimmt. Hinter der Abzweigung eigenen Code zu platzieren ist der klassische Weg, eine Software zu hacken.

Sprachen bestehen aus mehr als nur isolierten Begriffen – die Begriffe stehen in Bezug zueinander, z. B. in einem Subjekt-Objekt-Verhältnis. Programmiersprachen sind da speziell: Sie kennen kein Subjekt. In natürlichen Sprachen kann über andere Verhältnisse spekuliert werden – was wäre, wenn es keinen Kapitalismus gäbe –, Entwicklungen können vorweg genommen, analysiert und bewertet werden. Gesellschaftliche Veränderung braucht Spekulation, das Reflektieren und Kommunizieren über das ganz Andere. Etwas Vergleichbares auf der Sprachebene ist in Programmiersprachen nicht vorhanden, sie sind dazu da, Algorithmen zu formulieren, also Vorgehensweisen, um von einer Problemstellung zu einer Lösung zu kommen – und nicht, um über alles mögliche zu spekulieren. Diese in der Programmiersprache niedergelegte Vorgehensweise hat genau eine richtige Interpretation, Programmiersprachen sind nicht mehrdeutig – eine Eigenschaft, die mensch natürlichen Sprachen beim besten Willen nicht zuschreiben kann, die tatsächlich eine Qualität ausmachen. Sortiert nach CPU-Zyklen, also der gesammelten Rechenzeit weltweit – was als Maß für den Umfang der oben beschriebenen Kommunikation herhalten kann – entfällt praktisch alle Zeit auf Software, die in sogenannten imperativen[19] Programmiersprachen geschrieben wurden. Andere Sprachkategorien (funktional, deklarativ) sind nur marginal vertreten. Imperativ meint, dass der Programmtext aus einer Folge von Anweisungen besteht: tue erst dies, dann jenes. Das Kommando wird in Sprachen formuliert, die selbst nach dem Kommandoprinzip aufgebaut sind.

Die Kommandoform der imperativen Programmiersprachen ist aber nicht ursächlich für den Kommandocharakter des Kommunikationsaspekts von Software. Ein Programm, geschrieben in einer funktionalen Programmiersprache, hat den gleichen Kommandocharakter. Zu fragen wäre höchstens, inwieweit der Charakter des Imperativs auf die Kommunikation durchfärbt.

Sprache prägt das Denken – Studien zeigen, dass man bei dem Begriff „Professoren“ Männer vor Augen hat, obwohl Frauen, zumindest grammatikalisch, mit gemeint sind. Übertragen lässt sich vermuten, dass Programmierer*innen, die quasi im permanenten Befehlsmodus schreiben, im Denken ähnliche Strukturen aufweisen. Vielleicht kommt die Selbstüberzeugtheit, mit der die IT-Welt antritt, die Welt (vermeintlich) zu revolutionieren, auch aus der Sprache des Codens.

Code lässt keinen Raum für Interpretationen und Möglichkeitsformen, ein derartiges Denkgerüst auf soziale Probleme angewandt verengt den Lösungsraum. Das Auffinden nicht technokratisch reduzierter Lösungen hängt auch ganz banal von der Intensität der Suche nach komplexeren Zusammenhängen ab. Der technokratische Trend im herrschenden politischen Alltagsgeschäft schickt sich an, ganze Arbeit zu leisten und die Lösungssuche für zentrale gesellschaftliche Probleme schon jetzt zu verengen[20].

Es tritt auch ein umgekehrter Effekt auf: Die Callcenter-Mitarbeiter*in, die ihr stimmliches Repertoire anpasst und vereinfacht, um von der Sprachanalysesoftware, die die „Freundlichkeit“ vermisst, nicht abgewertet zu werden. Allgemeiner formuliert: Die Anpassung des Menschen an die Begrenztheit der Plattform. Quasi ein „Lernen“, das eigene komplexe Sozialverhalten auf die eingeschränkte Welt der Plattform zu reduzieren.

---

19 Wir zählen objektorientierte Programmiersprachen zu den imperativen

20 Gemeint ist hier z. B. das „Nützlichkeitsdenken“, mit dem Migration begegnet wird. Aufenthalt ist kein Menschenrecht mehr, sondern abhängig von der Verwertbarkeit der konkreten Individuen.

Software ist mehr als einfacher Transmissionsriemen von Herrschaft, sie strukturiert die Form, in der Herrschaft kommuniziert und ausgeübt wird. Das Kommando kann durchaus dezent und trotzdem total sein. Umsonst-Plattformen wie etwa Facebook, die eher mit Verführung und Abhängigkeit denn mit stumpfem Kommando agieren, nutzen dennoch das Kommando, um das Tauschverhältnis Zugang/Inhalt/Dienstleistung auf der einen, zu persönlichen Daten auf der anderen Seite zu diktieren.

Der Kommunikationsakt, der sich hinter Software verbirgt, wird immer den Charakter eines Kommandos haben. Zu fragen ist daher, was passieren muss, damit dieses Kommando zumindest partiell ins Leere läuft oder bestenfalls anders, also im eigenen Interesse, funktioniert. Als Beispiel sei selbst geschriebene Software für eigene Anwendungsfälle genannt – der Kommunikationsakt wäre an dieser Stelle einem Selbstgespräch verwandt. Das kann durchaus auf größeren Skalen gedacht werden – als "Selbstgespräch" einer politischen oder sozialen Bewegung, die sich selbst ihre Software schreibt. Vereinzelt gibt es derartiges schon, als Beispiel sei Lorea [21]genannt.

Das Kommando ins Leere laufen zu lassen gestaltet sich hingegen als schwieriger – einfach die Software nicht zu benutzen und sich erst gar nicht dem Kommando auszusetzen, scheitert spätestens dann als Strategie, wenn Leistungen Dritter in Anspruch genommen werden wollen. Egal ob ÖPNV, Krankenkassen, soziale Transferleitungen etc. - die Entscheidung, ob und welche Software zu Einsatz kommt, ist abgegeben.

Da immer mehr Vorgänge sowohl auf privater als auch auf gesellschaftlicher Ebene "rechnergestützt" verlaufen, multiplizieren sich die Einfallstore des Kommandos und damit die Wirkmächtigkeit dieses Prinzips. Das kann als Umkehrung dechiffriert werden: Die Nutzer*in "nutzt" nicht die Software, sondern wird zum Objekt des in der Software eingewobenen Kommandos.

Nun fällt Software nicht vom Himmel, sondern wird von Programmierer*innen geschrieben, die in der bemerkenswerten Situation sind, das Kommando durch Niederschreiben in einen Programmtext wirkmächtig werden zu lassen, gleichzeitig aber im Alltag zu den Nutzer*innen zählen, also zu den Objekten des Kommandos.

Selten kippt diese Widersprüchlichkeit in artikulierten Widerspruch, ein Beispiel dafür wäre die kollektive Verweigerung der Mitarbeit von Google-Angestellten am militärischen KI-Projekt "maven". Google hat in Folge dessen das Projekt zwar nicht beendet, sah sich aber gezwungen, die Arbeiten outzusourcen, um dem Betriebsfrieden nicht zu sehr zu schaden.

Dass Programmierer*innen und Softwareentwickler*innen eine Verantwortung für das tragen, was sie tun, ist Botschaft von NGOs wie CPSR oder FifF.

Wir gehen darüber hinaus. Eine Verweigerung der Mitarbeit reicht nicht angesichts des bereits erreichten Stadiums der Entwicklung. Ein subversives und disruptives Eingreifen, welches in der Lage ist, dem technologischen Angriff den einen oder anderen Zahn zu ziehen, ist notwendig, und sei es nur, um gesellschaftlichen Prozessen, die langsamer sind als technologische Entwicklungen, Zeit zu geben, aus Besinnungslosigkeit und Reizüberflutung aufzuwachen.

Softwarekonzerne brüsten sich mit ihren "disruptiven Technologien", die Zerstörung und Neuzusammensetzung bestehender Prozesse und damit auch sozialer Verhältnisse ist offen deklariertes Ziel. Diese Zerstörungswut sollte ernst genommen werden, denn sie ist ernst gemeint – die Antworten darauf sollten mindestens auf Augenhöhe sein.

Da geht noch was ...

21 Eine Software von Aktivist*innen, die im Kontext der spanischen M15-Bewegung entwickelt wurde.

Weibliche Sprachassistenten

Digitale Sprachassistenten[22] sind erste Gehversuche in Richtung eines neuen Paradigmas im Feld der Mensch-Computer-Schnittstellen. Traut man den hippen Trendforscher*innen der vielen Computermessen, dann sind Sprachinterfaces der nächste große Hype, weil bisherige Text- oder Grafikschnittstellen zur Ein- und Ausgabe Hände und Augen brauchen, während Sprachinterfaces über Reden und Zuhören funktionieren, so dass man sich währenddessen mit anderen Tätigkeiten befassen kann.

Wir sehen eine große Notwendigkeit, uns mit Sprachassistenten besonders aus feministischer Perspektive zu befassen, weil sich durch die digitalen Geräte ein immer größer werdender Einfluss auf das soziale Leben abzeichnet.

Zu weiblichen Sprachassistenten gibt es bereits einige, wenngleich auch wenige, kritische Veröffentlichungen, auf die teilweise Bezug genommen und versucht wird, die verschiedenen Aspekte in Zusammenhang zu bringen.

SEXISTISCHE STEREOTYPE

Die Entwicklung der Sprachassistenten hat Google 2012 begonnen, woraufhin Amazon relativ schnell die Vorreiterrolle in der Entwicklung der sprachfähigen digitalen Assistenten übernahm. Die virtuellen Assistenten wurden entweder voreingestellt oder sogar unveränderbar mit als ‚wohlklingend' erachteter weiblicher Stimme und rundlichen Formen, die Assoziationen einer weiblichen Ansprechpartnerin und Servicekraft hervorrufen sollen, auf den Markt gebracht.

Nicht nur die Erscheinung, sondern auch das Antwortverhalten dieser weiblich konnotierten Sprachassistenten war und ist auf stereotype Weise gendergefärbt. In der Anfangszeit der Fembots wurden einige Artikel veröffentlicht, die deren Reaktionen auf verbale sexuelle Belästigungen hin untersuchten.

Die Ergebnisse dieser Studien sind bezeichnend. So reagierten die Sprachcomputer nicht nur nicht abweisend auf übergriffiges Verhalten, sondern unterwürfig bis ermunternd. Auf die Ansprache ‚*You're a bitch*' antwortete Alexa beispielsweise mit den Worten ‚*Well, thanks for the feedback*'[23].

Nach einiger öffentlicher Kritik sahen sich die Großkonzerne genötigt, ihren smarten Assistenten ein gemäßigteres Antwortverhalten einzuprogrammieren und zum Beispiel auf eindeutig missbrauchende Fragen, sofern sie denn als solche erkannt werden, nicht motivierend zu reagieren, sondern mit Worten wie „Das ist nichts für mich" oder „Ich weiß nicht, was du erwartest". Allerdings würden wir die These aufstellen, dass ausweichendes Antwortverhalten des Gerätes eher weniger dazu veranlasst, sein eigenes Verhalten zu hinterfragen, sondern es eher als normal zu bewerten.

‚*How we gender robots is not an abstract, academic issue: the link between how we treat „fembots"and human women is real.*' [24]

Eine ‚Partnerin', die sich sexuellen Übergriffen nicht widersetzt, sondern schlimmstenfalls sogar ermutigend reagiert, führt dazu, Frauen nicht als gleichberechtigte und respektvoll zu behandelnde Wesen zu sehen. Eine feministische Haltung ist darin nicht zu erkennen.

Es fehlt sowohl der Ansatz, sich grundsätzlich gegen sexuelle Belästigung und Missbrauch zu wehren, als auch eine fundierte Kritik und eine Auseinandersetzung damit, weshalb ein solches Verhalten falsch ist und wie eine respektvolle Kommunikation aussehen könnte.

ROLLENBILDER

Über das Antwortverhalten der Sprachassistenten hinaus gibt es noch weitere Aspekte, die sexistische Stereotype verstärken können. Was für ein Rollen- und Frauenbild wird mit dem widerspruchslosen Gehorchen auf Befehle transportiert? Das Konzept als solches, die Sprachassistentin, die die Rolle der ‚dienenden Assistentin' ausfüllt,

22 Die männliche Form des Begriff der „Sprachassistenten" ist der, mit dem öffentlich operiert wird, und wir übernehmen ihn an dieser Stelle bewusst, um die Widersprüchlichkeit sichtbar zu machen.

23 https://qz.com/911681/we-tested-apples-siri-amazon-echos-alexa-microsofts-cortana-and-googles-google-home-to-see-which-personal-assistant-bots-stand-up-for-themselves-in-the-face-of-sexual-harassment/

24 Laurie Penny, 2016, https://www.newstatesman.com/politics/feminism/2016/04/why-do-we-give-robots-female-names-because-we-dont-want-consider-their

die alle Wünsche und Fragen bedingungslos akzeptiert, der man nicht Bitte oder Danke sagen muss, die umsorgend rund um die Uhr tut, was man ihr befielt, spiegelt ein extrem rückschrittliches Rollenverständnis wider, in dem Männer die Autoritäts- und Entscheidungspersonen und Frauen die Servicekräfte und Unterstützerinnen sind.

Natürlich wehren sich die Firmen gegen den Verdacht, dass dahinter Absicht steckt. Es werden diverse Begründungen herangezogen, weshalb sich eine weibliche Stimme besser eignet als eine männliche. Zum Beispiel seien Frauenstimmen im Allgemeinen leichter zu hören, vor allem, wenn Hintergrundgeräusche eine Rolle spielen. Ein anderer Grund sei, dass zum Beispiel kleine Lautsprecher tiefe Stimmen nicht gut wiedergeben könnten.

Mit diesen vorgeschobenen Gründen haben sich gleich mehrere Studien beschäftigt, die diese Annahmen entkräften. Eine Untersuchung der University of Indiana[25] belegt beispielsweise, dass keine Beweise dafür existieren, dass die Grundfrequenz der Sprache in der Verständlichkeit eine direkte Rolle spielt und sich männliche und weibliche Stimmen zudem in mehr als dieser Frequenz unterscheiden. Frauen sprechen laut der Studie zwar Vokale etwas deutlicher aus und verfügen über größere Vokalräume, die ihre Stimmen theoretisch tatsächlich etwas verständlicher machen können als männliche, jedoch gilt dies aber nur für echte Stimmen lebender Frauen und nicht für digital bearbeitete Stimmen. Außerdem gibt es innerhalb einer Gruppe von weiblichen oder männlichen Stimmen sehr große Variationen und durchaus auch viele Überschneidungen zwischen den Gruppen, sodass hier keine so absolute Aussage zulässig ist.

Auch das Argument, Frauenstimmen würden sich besser gegen Hintergrundgeräusche absetzen können, wird in einer militärischen Studie (Wright-Patterson Air Force Base in Ohio) entkräftet. Statistisch lässt sich kein signifikanter Unterschied feststellen. Technisch gesehen gibt es also keine Gründe, weshalb Sprachassistenten weibliche Stimmen haben müssen.

DIE EIGENTLICHE MOTIVATION

Es lässt sich unschwer erahnen, dass die eigentlichen Gründe marktwirtschaftlichen Ursprungs sind. Es lässt sich nämlich schlicht mehr Geld damit verdienen. Mehreren Umfragen zufolge mögen es Kund*innen lieber (das gilt für alle Geschlechter), wenn ihre digitalen Assistenten menschlich und weiblich klingen.

Eine einem Geschlecht zuordenbare Stimme vermittelt den Eindruck, dass man mit einer echten Person kommuniziert und das ist Menschen wichtig. Zudem empfinden die meisten Menschen Frauenstimmen als angenehmer und wärmer und bevorzugen sie deshalb als Stimme für ihre virtuellen Assistenten. Weibliche Stimmen werden als Lösungshilfe für Probleme lieber herangezogen – zumindest solange es sich nicht um technische Probleme handelt, denn in diesem Fall werden tatsächlich männliche Stimmen bevorzugt, die eine gewisse Autorität darstellen[26]. Der Sprachroboter dient also als weibliche Bedienstete oder persönliche Sekretärin, die gerne Hilfe leisten darf, solange man selbst die Autorität bleibt.

Natürlich denken die Konzerne auch vorausschauend und im Hinblick auf eine momentan noch eher verbreitete Skepsis bis Ablehnung gegenüber Künstlichen Intelligenzen ergibt es Sinn, diese als praktische, aber harmlose unterlegene Helferinnen einzuführen, die keine bösen Absichten haben, sondern nur tun, was ihnen befohlen wird. Um so weniger traut man ihnen das Potential zu, in großem Ausmaß gesellschaftlichen Schaden anzurichten. Eine männliche Stimme, die Assoziationen von autonomen und zerstörerischen KIs wie beispielsweise *hal9000* hervorruft, ist da sicherlich weniger hilfreich.

GESELLSCHAFTLICHE AUSWIRKUNGEN

Die künstlichen Intelligenzen, hinter denen eine vornehmlich männliche, weiße Entwicklerschaft steht, reproduzieren die Herkunft und Haltung ihrer Urheber.

Sie sind weder neutrale Elemente in der Gesellschaftsstruktur noch tragen sie zur Lösung sozialer Probleme bei. Im Gegenteil, sie verfestigen bereits Vorhandene und produzieren darüber hinaus noch Neue.

So zeigt sich an den Sprachassistenten einmal mehr, dass Herrschaftstechnologien nicht neutral sind, sondern politische und gesellschaftliche Verhältnisse widerspiegeln. Durch die Entwicklung und auch die Nutzung dieser Produkte wird eine männlich-privilegiert sozialisierte Perspektive transportiert und es werden aktiv Realitäten gestaltet. Kapitalistische Herrschaftsverhältnisse werden durch eine zutiefst patriarchale Entwicklergemeinde nicht nur abgebildet, sondern aufrecht erhalten und weiter ausgebaut.

Informationstechnologien durchdringen mittlerweile fast alle Lebensbereiche, bilden einen großen Einflussfaktor und in ihrer Entwicklung und Implementierung in den Alltag sind zurzeit kaum Grenzen auszumachen. Neben den in früheren Beiträgen kritisierten Aspekten, wie dem totalen Durchleuchten der Privatsphäre zum Nutzen der Interessen von Konzernen und Repressionsorganen, ist dies auch aus feministischer Sicht kein hinnehmbarer Zustand.

25 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3066472/

26 https://theweek.com/articles/684606/where-are-all-male-ai-voice-assistants

Blockchains – Software als Politk

Bitcoin ist ein digitales Zahlungssystem, welches damit wirbt, ohne eine zentrale Instanz auszukommen, die Bitcoin erzeugen („drucken") oder Transaktionen ausführen würde. Statt dessen gibt es die community von Nutzer*innen, welche diese Aufgabe übernimmt – keine einzelne Instanz soll Bitcoin besitzen oder kontrollieren können. Die community ist offen, um teilzunehmen, reicht die Installation der entsprechenden Software auf dem eigenen Rechner, schon ist man Teil des Netzes, Teil der community – niemand wird ausgeschlossen.

Bitcoin ist – anders als der Name suggeriert – keine Münze (coin), sondern ein Buchhaltungssystem für Kontostände. Das Hauptbuch (engl.: *ledger*) dieser Buchhaltung liegt als Kopie auf jedem Rechner, welcher Teil des Bitcoin-Netzes ist. Jede*r aus der community kann alle Geldflüsse nachvollziehen. Der ledger ist „ewig", zeichnet seit Beginn der Bitcoins die Transaktionen auf – zur Zeit (11/2018) hat er eine Größe von 224.25 GB. Da seit Tag 0 alle Transaktionen einsehbar sind, können alle Nutzer*innen nicht nur aktuelle Geldflüsse sehen, sondern alle jemals getätigten Transaktionen aufaddieren und den aktuellen Kontostand jeder Teilnehmer*in errechnen. Da alle mit dem gleichen ledger arbeiten, sprich, alle zum gleichen Kontostand kommen, gilt dieser als Konsens und damit als existent und „wahr". Hat eine Nutzer*in laut dieses Konsenses zehn Bitcoin auf ihrem Konto, dann kann sie die auch ausgeben. Allerdings auch nicht mehr, negative Kontostände sind nicht vorgesehen.

Bitcoin ist (bei weitem) nicht das einzige digitale Zahlungssystem – erst recht nicht das Erste. Digitale Zahlungssysteme haben das generelle Problem, verhindern zu müssen, dass Geldeinheiten mehrfach ausgegeben werden. Digitale Geldeinheiten sind nur Bits im Rechner, Kopien davon zu erstellen ist ein Kinderspiel, anders als bei Zahlungssystemen mit physikalischen Wertträgern. Diese Wertträger sind zwar auch nicht vor dem Kopieren (vulgo: Geldfälschen) geschützt, eingebaute „Sicherheitsmerkmale" zum Beispiel in Banknoten können den Aufwand jedoch erheblich erhöhen und bestenfalls das Kopieren ökonomisch uninteressant machen.

Das gängige Verfahren, das mehrfache Ausgeben der gleichen Geldeinheit zu verhindern, ist, jede Transaktion durch eine zentrale Instanz abzuwickeln, die sicherstellt, dass ausgegebenes Geld nicht mehr zur Verfügung steht. Kreditkarteninstitute oder auch PayPal arbeiten entsprechend. Die Macht dieser Instanzen ist für das Zahlungssystem, für welches sie zentral sind, total – gegen deren Willen ist keine Transaktion möglich. Deutlich wurde das beispielsweise bei der finanziellen Blockade von wikileaks – Spenden an wikileaks wurden einfach nicht gutgeschrieben.

Bitcoin behauptet von sich, ohne eine solche zentrale Instanz auszukommen und trotzdem ein mehrfaches Ausgeben der selben Bitcoin zu verhindern. Die Methode, dies zu erreichen, liegt in der Handhabung des ledgers – die Idee ist, zu verhindern, dass mehrfach ausgegebene Bitcoins Teil des Konsenses werden können. Das Ausgeben einer Bitcoin führt zu einer Transaktion und damit zu Änderungen in Kontoständen – nachfolgende Transaktionen arbeiten dann mit diesem neuen reduzierten Kontostand. Die „Handhabung des ledgers" muss sicherstellen, dass Transaktionen nicht parallel, sondern immer nur sequentiell stattfinden können – parallele Transaktionen ermöglichen das mehrfache Ausgeben der gleichen Bitcoin.

Die Technologie, die einen ledger mit diesen beschriebenen Eigenschaften[27] implementiert, heißt *„blockchain"* und umfasst gleich mehrere Algorithmen, die solche Eigenschaften haben. Blockchain[28] beschreibt also weniger eine konkrete Software, sondern ein Konzept der Datenverarbeitung. Dieses Konzept wird in digitalen Zahlungssystemen wie Bitcoin , für digitale Verträge oder auch für digitale Namensverwaltung verwendet.

Zentrale Eigenschaft der blockchain ist die Fixierung, das Festhalten und Dokumentieren eines Konsenses. Der Gegenstand dieses Konsenses ist beliebig, einzige Bedingung ist, dass er sich digital abbilden lässt.

Konsense sind üblicherweise unproblematisch in der Handhabung, schwierig wird es, wenn ein Konsens auf-

27 und einigen mehr

28 Bitcoin war das erste Zahlungssystem mit blockchain, mittlerweile gibt es weit über 1600 (Stand 8/2018)

gekündigt wird – um bei den genannten Beispielen zu bleiben: ein Vertrag gebrochen wird.

Menschliche Gesellschaften, nicht nur die Bürgerliche, die vielleicht am ausgeprägtesten, sehen für die Situation eines Vertragsbruches eine „dritte Partei" vor, die eingeschaltet wird, um den Konsens wieder herzustellen. Dritte Parteien in diesem Sinne wären Gerichte, Schiedsgerichte, irgendein*e König*in, Schlichtungs- oder Clearingstellen. Die dritte Partei ist mächtiger als die beiden Vertragsparteien und kann einen neuen „Konsens" diktieren – etwa auf Vertragserfüllung bestehen oder Strafen aussprechen. Insofern kann man die Exekutive als Teil der dritten Partei ansehen und ebenso die Legislative – in der bürgerlichen Gesellschaft letztendlich den Staat. Diese dritte Partei übernimmt die oben beschriebene Rolle der „zentralen Instanz".

BLOCKCHAIN VERSPRICHT, EIN „KONSENSSYSTEM" ZU IMPLEMENTIEREN, WELCHES OHNE ZENTRALE INSTANZ AUSKOMMT.

Die ideologische Reichweite dieses Versprechens ist enorm – wenn bei allen möglichen Konsensen, Verträgen, Besitzverhältnissen, Kontoständen usw. der Bruch eines jeden einzelnen dieser Konsense ohne zentrale Instanz, ohne dritte Partei wieder „ins Lot" zu bringen ist … wer braucht da noch den Staat? Staaten wären – zumindest in der jetzigen Form –schlicht überflüssig.

Dass Bitcoin als erste konkrete Implementation einer blockchain-Technologie ausgerechnet ein digitales Zahlungssystem ist, ist kein Zufall. Die Ablehnung der zentralen Autorität des Staates ist (nicht nur) in den USA verbreitet, diesen Staat auch noch durch eigenes Geld in Form von Steuern zu finanzieren, ist unerträglich.

In den USA fand 1992 eine Gruppe von Softwareentwickler*innen und Computerwissenschaftler*innen zusammen, welche unter dem Namen „cypherpunks" die Privatsphäre Aller vor den neugierigen Augen des Staates schützen wollte. Die neu entwickelten Möglichkeiten, die der sich gerade verbreitende „Homecomputer" bot, sollten dabei die zentrale Rolle spielen. Computer ermöglichten es jeder*m, Verschlüsselung in einer Stärke zu benutzen, die es einem Staat – oder jeder anderen unerwünschten Instanz – unmöglich machte, den Inhalt zu entziffern. Mit ein paar extra Modifikationen konnte zudem verborgen werden, wer mit wem kommunizierte. Totale Anonymität, das einzige, was noch fehlte, war die entsprechende Software. Die zu entwickeln war erklärtes Ziel der cypherpunks.

Es ging allerdings nicht nur um Kommunikation, schon im Gründungspapier[29] war eine anonyme Währung prominent erwähnt. Hier fanden diejenigen, welche den Staat ablehnten und keine Steuern zahlen wollten, mit denjenigen zusammen, die nicht überwacht werden wollten. Eine anonyme Währung, die Transaktionen unverfolgbar für Dritte realisieren könnte, würde dazu führen, dass der Staat keine Steuern mehr kassieren könnte und deshalb zusammenbrechen würde. Die Theorie dazu gab es bereits[30] , die meisten notwendigen Bausteine ebenfalls, es musste „nur" noch zusammengesetzt und als bedienbare Software veröffentlicht werden.

Es gab eine ganze Reihe von Anläufen, eine anonyme Währung auf Basis von computergestützter Verschlüsselung zu realisieren. Alle hatten schwer damit zu kämpfen, ein mehrfaches Ausgeben des Geldes zu verhindern. Die meisten kamen früher oder später zum Konzept der „zentralen Instanz" zurück. Die, die das vermeiden konnten, stellten sich als so komplex und unhandlich heraus, dass sie nie mehr wurden als ein proof-of-concept.

Aus dieser Tradition kommt Bitcoin, das erste digitale Zahlungssystem auf Basis computergestützter Verschlüsselung, und das ohne zentrale Instanz. Dass Bitcoin nicht anonym ist, ist in der Begeisterung über die neue Technologie in den Hintergrund gedrängt worden.

Apologeten von Bitcoin spekulieren lieber über deren Auswirkungen auf das Finanzkapital. Eher linke Positionen kritisieren die Macht von Institutionen wie PayPal, willkürlich die ökonomische Handlungsfreiheit kontroverser Initiativen wie etwa wikileaks massiv einschränken zu können, ohne dafür auf irgendeine Weise demokratisch legitimiert zu sein[31]. Bitcoin sei der Sargnagel für diese Institutionen, da sie deren Machtposition als „Türsteher" schlagartig entwerten würde, ohne selbst diese Position übernehmen zu können – was den Tod des Kapitalismus vorantreibe.

Diese etwas eigenwillige Analyse der Funktion von Banken im Kapitalismus trifft auf rechtsextreme Verschwörungstheorien, nach denen die Zentralbank mittels Inflation Diebstahl am Vermögen der Bevölkerung betreibt. Weil sie die Notenbankpressen kontrollierten, könnten die Zentralbanken willkürlich die Inflation steuern und sich nach Belieben bedienen. Bitcoin hat keine kontrollierbare Notenbankpresse, neue Bitcoins „entstehen", weil

29 A Cypherpunks Manifesto, 1992: https://www.activism.net/cypherpunk/manifesto.html

30 Security without Identification, Card Computers to make Big Brother Obsolete; David Chaum 1985; https://www.chaum.com/publications/Security_Wthout_Identification.html

31 The Bitcoin Manifesto, Denis Jaromil Roio, 2011, zitiert in Bitcoin, The end of the Taboo on Money, https://files.dyne.org/readers/Bitcoin_end_of_taboo_on_money.pdf

denjenigen, die neue Blöcke für die blockchain erzeugen, ein definierter Betrag gutgeschrieben wird, und neue Blöcke kann jeder errechnen. Damit wäre der Zentralbank das Machtmittel aus der Hand geschlagen. Aus diesen Verschwörungstheorien trieft Antisemitismus und Antisemit*innen feiern Bitcoin als Waffe, die „den Juden" ordentlich wehtut.

Bitcoin bedient dieses Misstrauen gegenüber der Inflation noch auf eine sehr inhärente Weise: Die Anzahl der erzeugbaren Bitcoins ist begrenzt – der Algorithmus hat eine eingebaute Obergrenze. Bitcoins sind also knapp und bewirken tendenziell eine Deflation.

Rechte Apologeten sehen in Bitcoin ein Ende der staatlichen Regulationen und den Beginn eines „freien" entfesselten Kapitalismus, während Linke darin das Ende privatwirtschaftlicher Regulationen sehen und daraus das Ende des Kapitalismus ableiten. Dazu später mehr.

Wie sehr Bitcoin zum Transport von Ideologie verwendet wurde, sollte nicht verdecken, dass Bitcoin selbst ideologisch aufgeladen ist: Zentrale Aussagen über die Eigenschaften der Software sind fragwürdig.

So soll Bitcoin keine zentrale Instanz haben, die den Markt regelt. Regeln gibt es aber, unauffällige, scheinbar belanglose Setzungen in der Software. Da wäre zum Beispiel die Größe der einzelnen Blöcke in der blockchain zu nennen oder aber die Geschwindigkeit, mit der neue Blöcke „erzeugt" werden können. Beides zusammen bestimmt die maximale Anzahl von Transaktionen, die das Bitcoin-Netzwerk pro Zeiteinheit bewältigen kann. Dieses Maximum ist am Anfang willkürlich gesetzt worden und erwies sich als zu klein, nachdem der Hype erstmal losgebrochen war.

Über die Frage, ob und in welchem Maße an diesen Parametern gedreht werden sollte, entstand ein Streit unter den Programmierer*innen und es stellte sich heraus, dass die Anzahl derjenigen, die da Entscheidungen durchsetzen konnten, weil sie den Code verwalteten, einstellig war. Eine Handvoll Entwickler*innen entschieden über das Schicksal einer Währung, deren Volumen viele Milliarden US-Dollar wert war. Eine Einigung konnte nicht erzielt werden, als Folge gab es einen sogenannten „*hard fork*", die Währung spaltete sich in Bitcoin ohne Veränderungen an den Parametern und Bitcoin Cash mit größerer Blockgröße.

Die blockchain als „Handhabung des ledgers" muss, um das mehrfache Ausgeben von Geld zu verhindern, Transaktionen nur sequentiell zulassen. Die blockchain kann aber eine parallele Erzeugung von Transaktionen – genauer eine parallele Erzeugung von Blöcken – nicht verhindern. Die blockchain gabelt sich in Folge in zwei oder mehr Ketten paralleler Transaktionen auf. Um wieder zur gewünschten Kette mit sequentiellen Blöcken zurück zu finden, gibt es in der blockchain-Technologie eine Art automatisierter Mehrheitsentscheidung, welches der Kettenenden weiterverfolgt und damit zur alleinig gültigen Kette wird – die Transaktionen in den anderen Ketten werden verworfen und gelten als nicht getätigt. Das System kann den Fehler nicht verhindern, aber sich selbst zeitversetzt reparieren.

Das entscheidende Detail ist die Frage, woraus sich die Mehrheit dieser Mehrheitsentscheidung zusammensetzt. Es ist nicht die Mehrheit der Mitglieder der community, auch nicht die Mehrheit derjenigen in der community, die neue Blöcke erzeugt[32], sondern die „Mehrheit" der Rechenleistung, die in die Erzeugung neuer Blöcke gesteckt wird. Erlangt eine Partei eine solche Mehrheit, produziert sie mehr als die Hälfte der neuen Blöcke, kann sie Geld mehrfach ausgeben und die Selbstreparatur solange hinauszögern, wie diese „Mehrheit" aufrecht erhalten werden kann. Es hat solche Zeitabschnitte in der Geschichte der Bitcoin-blockchain bereits gegeben.

DIE AUSSAGE, DASS BITCOIN KEINE ZENTRALE INSTANZ HAT, STIMMT NUR AUF DER ERSCHEINUNGSEBENE.

Bitcoin suggeriert, dass via Dezentralität und community alle gleichberechtigt am Markt teilnehmen können, die zentrale Instanz, die das verhindern könnte, gäbe es nicht. Gerade aber das Fehlen einer zentralen Instanz liefert den Bitcoin-Markt Kursmanipulationen aus. Regulationen, die etwa market cornering verhindern könnten, sind explizit nicht Teil der Software. Und so können diejenigen, die genug Kapital aufrufen können, den Kurs manipulieren, auf Kosten aller anderen.

Die Dezentralität der blockchain, genauer der Anforderung, dass jede Teilnehmer*in die gleiche Kopie lokal auf ihrem Rechner haben muss, damit ein Konsens aller existieren kann, führt zu einer sehr speziellen Eigenschaft der blockchain. Die Rate, mit der neue Blöcke erzeugt werden können, darf nicht zu hoch werden. Änderungen müssen sich bis in den letzten Winkel des Netzes rumgesprochen haben, bevor ein neuer Block hinzugefügt werden kann[33]. Ansonsten würden unterschiedliche „Ecken" des Netzes unterschiedliche blockchains sehen – der Schutz vor Mehrfachausgabe von Geld wäre dahin, der Konsens auch. Es gibt weitere Gründe, die Erzeugungsrate von Blöcken zu limitieren.

32 Das Erzeugen neuer Blöcke (genannt mining) ist nicht Bedingung zur Teilnahme. Die wenigsten Teilnehmer*innen minen selbst.

33 Dies erklärt übrigens, warum die Blockgröße ein zentraler Parameter mit viel Streitpotential ist: Größere Blöcke brauchen länger um sich rumzusprechen.

Um Vertrauen in die blockchain haben zu können, darf es nicht möglich sein, dieses Limit zu verletzen – ein Versprechen, sich wohl zu verhalten, reicht augenscheinlich nicht. Die blockchain von Bitcoin nutzt dazu einen sogenannten „proof-of-work". Die Erzeugung eines neuen Blocks muss so rechenintensiv sein, dass selbst die schnellsten Rechenfarmen das Limit nicht unterbieten können. Da Rechner immer leistungsfähiger werden, wird der proof-of-work der blockchain immer wieder angepasst und schwieriger gemacht.

ÖKOLOGISCHER WAHNSINN

Bitcoin gibt es seit 2009, mittlerweile ist der proof-of-work so aufwendig, dass der Stromverbrauch, der notwendig ist, um die blockchain von Bitcoin am laufen zu halten und mit neuen Blöcken zu füttern – ohne neue Blöcke keine neuen Transaktionen –, zwischen 55 und 70 Terawattstunden liegt und in etwa dem Stromverbrauch Österreichs entspricht, Tendenz steigend. Runter gebrochen sind das 797 Kilowattstunden für jede einzelne Transaktion, das entspricht dem Tagesbedarf von 26 Haushalten. Das ist ökologischer Wahnsinn.

Letztendlich ist die Begründung für den proof-of-work dessen Funktion, Betrug in der blockchain unmöglich zu machen. Andere digitale Zahlungssysteme benutzen dafür einen sogenannten proof-of-stake. Naiv erklärt dürfen nur diejenigen neue Blöcke erzeugen, die am meisten Geld im System angelegt haben und sich selber schädigen würden, wenn sie betrügen würden[34]. Proof-of-stake gibt erst gar kein Gleichheitsversprechen aller Nutzer*innen des Systems. Um die Gefahr einer neuen „zentralen Instanz" im System abzuwenden, wird das oben beschriebene naive Verfahren durch Zufallsfaktoren und andere Mechanismen ergänzt. Existierende Implementationen sind ziemlich komplex, dass sie sicher Betrug verhindern, ist weit schwieriger nachzuvollziehen als beim proof-of-work.

Trotz dieser durchaus massiven Einschränkungen gilt die blockchain als Zukunftstechnologie, gar als die Technologie, die zentrale Probleme lösen könnte. Vieles von dieser Heilserwartung ist bestimmt dem Hype geschuldet, der die blockchain umgibt. Die blockchain hat aber auch eine immanent politische Dimension: Die Eliminierung der „dritten Partei".

34 Peercoin war das erste digitale Zahlungssystem mit proof-of-stake

HIER TAUCHT DAS „ENDE DER REGULATIONEN" WIEDER AUF, WAS JE NACH POLITISCHEM LAGER DEN KAPITALISMUS BEFREIEN, ODER ABER SEIN ENDE EINLÄUTEN SOLL.

Regulationen bedeuten, dem „Recht des Stärkeren" Grenzen zu setzen, um damit die Schwächeren zu beschützen. Die klassische Methode via hoheitlicher Maßnahmen einfach eine stärkste Partei zu etablieren, die alle anderen in Schach halten und Regulationen durchsetzen kann, ist in der Theorie verlockend, solange diese hoheitlichen Maßnahmen demokratisch legitimiert sind. In der Realität ist diese Machtposition umkämpft und trägt im Kapitalismus zu dessen Stabilisierung bei.

Aus antikapitalistischer Sicht ein Ende der „dritten Partei" zu fordern, ist aber über das Ziel hinausgeschossen: Macht prinzipiell aus ihrer Rechenschaftspflicht zu entlassen, kann nicht im Sinne einer emanzipatorischen Bewegung sein.

Schaut man genau hin, dann „eliminiert" die blockchain die dritte Partei nicht einfach, sondern absorbiert diese. Legislative (Auswahl des Verfahrens und Definition der darin verwendeten Parameter), Exekutive (Abwehr oder rückwirkende Aufhebung von Betrug) und Judikative (Bestätigung der Rechtmäßigkeit einer Transaktion durch Aufnahme in die blockchain) verschwinden im Algorithmus der blockchain. In diesem Sinne versteckt sich hinter der blockchain der Versuch einer verdeckten Machtübernahme.

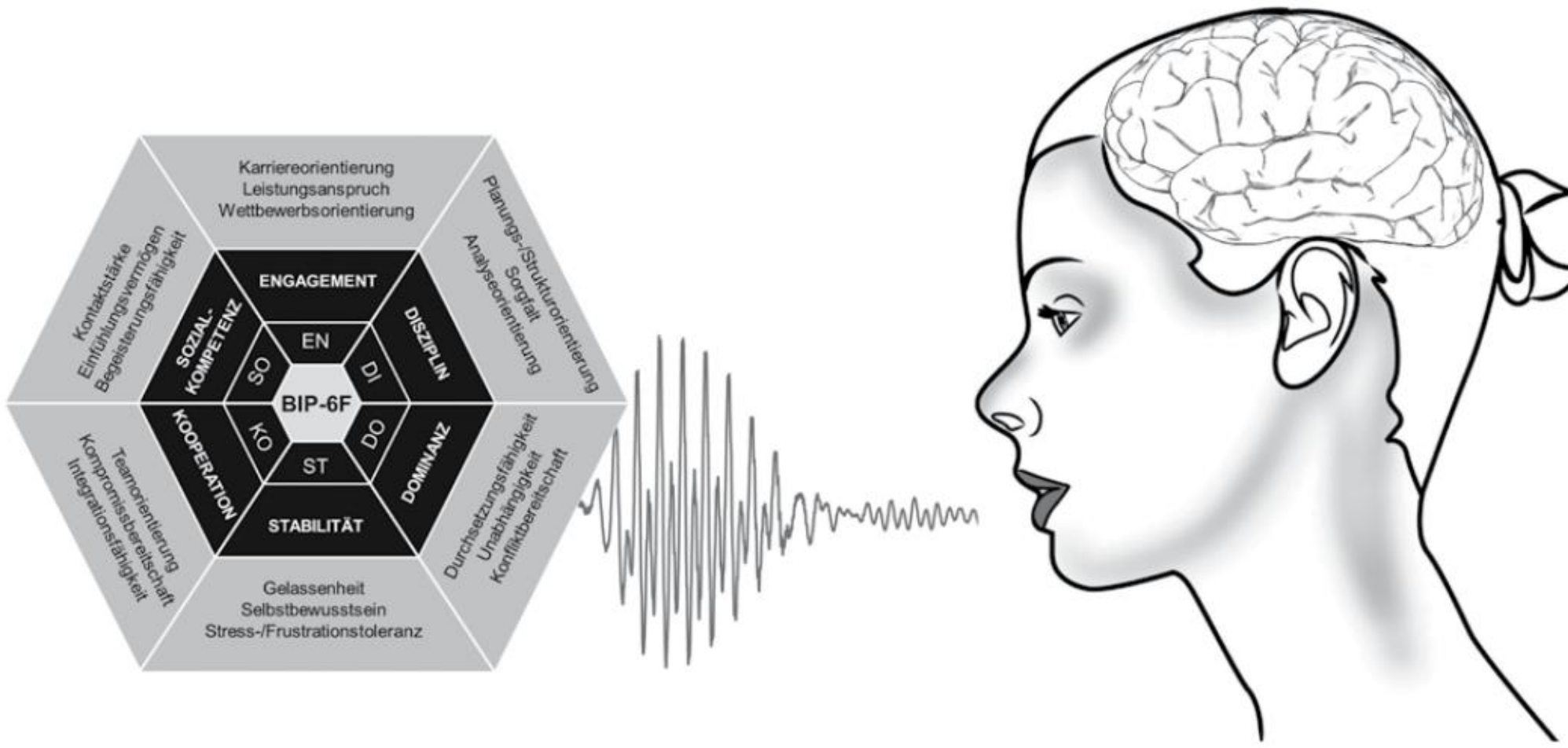
Eine Machtübernahme, die dem Recht des Stärkeren Geltung verschaffen soll – die blockchain ist in Software gegossene rechte, libertäre[35] Politik.

Postscriptum: *Um jeglichen Kurzschlüssen vorzubeugen, mit unserer Kritik an der blockchain wollen wir keinesfalls dem staatlich abgesicherten Kapitalismus das Wort reden, sondern dafür plädieren, genau hinzusehen, denn nicht jede Alternative zur jetzigen Situation ist erstrebenswert.*

35 David Golumbia unternimmt in seinem Buch „The Politics of Bitcoin, Software as right-wing extremism" eine sehr detaillierte Analyse der Argumente der Bitcoin-Apologeten und deren Überscheidungen zu rechtsextremen Verschwörungstheorien.

Korrelation statt Kausalität

Zentralisierte Macht in Datenbanken



SPRACHPROFIL = PERSÖNLICHKEITSPROFIL?

Die Zeitarbeitsvermittlung *randstad* hat ihr Bewerbungsverfahren verschlankt. Wer sich hier um einen Job bemüht, muss nun kein klassisches Bewerbungsgespräch mehr absolvieren. Das neue Job-Interview besteht aus einem 15-minütigen Telefonat. Erstaunlich dabei: Ich werde nach den Erlebnissen in meinem letzten Urlaub gefragt – es geht überhaupt nicht um meine Qualifikationen, Joberfahrungen oder sonstige für die Lohnarbeit relevante Eigenschaften. Noch befremdlicher: *Was* ich erzähle, wird nicht einmal berücksichtigt! Randstad analysiert über eine „künstlich intelligente" Sprachanalyse-Software lediglich, *wie* ich erzähle.

Dazu vermisst die Software der Aachener Firma *Precire* die Wortwahl, meine Art, Wörter zu kombinieren, Sprech-Tempo und -Rhythmus sowie die Variation von Lautstärke und Stimmhöhe. Precire will herausgefunden haben, dass diese Sprachmerkmale auch Aufschluss auf den Charakter eines Menschens geben – seine Risiko- und Leistungsbereitschaft, die emotionale Stabilität, Neugier und Kontaktfreude, um nur einige der abgeleiteten Eigenschaften zu nennen. Das ermittelte individuelle Sprachmuster wird mit einer Datenbank vergleichen. Diese Datenbank besteht (anfänglich) aus Sprachmustern von 5200 Proband*innen, die sich einem psychologischen Test unterzogen haben. Von diesen Proband*innen glaubt der Konzern zu wissen, wie sie „ticken". Ab da lernt die Software eigenständig dazu.

Angeblich weisen etwa Personen, die wenig belastbar sind, ähnliche Sprachmuster auf. Diese „Erkenntnisse" bleiben gänzlich unbewiesen. Sie werden nicht einmal weiter untersucht. Es wird gar keine Abstraktion vom zugrunde liegenden Datensatz angestrebt. Niemand macht sich die Mühe, einen *kausalen* Zusammenhang herzustellen zwischen der rein statistisch ermittelten *Korrelation* (Häufigkeit, mit der zwei Eigenschaften in einem Datensatz gleichzeitig auftreten) von Sprach- und Persönlichkeitsprofil. Niemand versucht, eine *Theorie* zu entwerfen, worin sich der Zusammenhang begründen könnte, den die Korrelationen nahelegen. Genau das ist der entscheidende Punkt. Die schiere Anzahl zur Verfügung stehender Daten verleitet dazu, den Erkenntnisgewinn eines kausalen Zusammenhangs gering zu schätzen. Klassische Theoriebildung wird verdrängt von einer wachsenden Masse an Daten, die – wie wir sehen werden – mitunter wenig aussagekräftig sein kann. Viel zu selten wird im BigData-Geschäft die Qualität von Datensätzen analysiert und diskutiert. Dazu gehört auch das Ausblenden eines in der Regel komplexen Kontextes, in dem Daten erhoben werden. Viele der per Korrelationsanalyse behaupteten statistischen Zusammenhänge halten einer Verallgemeinerung nicht stand.

Jetzt mag mensch einwenden, dass die Auswirkungen eines zweifelhaften Rückschlusses von Spracheigenschaften auf die Persönlichkeitseigenschaften bei einem Bewerbungsverfahren in der Zeitarbeitsvermittlung gering sind. Allerdings ist das Anwendungsgebiet der Sprachanalyse mittlerweile deutlich breiter. Sie wird z. B. auch in Callcentern eingesetzt, um zu überprüfen, ob sich die

Mitarbeiter*innen des Callcenters in einem vorgegeben Freundlichkeits-Korridor bewegen. Diese bemängeln, dass die Bewertung durch den digitalen „Freundlichkeits-Assistenten" sie in einen unnatürlich vereinfachten Sprachmodus dränge – denn die Maschine versteht keine Ironie oder subtilere Formen von Zuwendung. Die Mitarbeiter*innen erhalten dann eine schlechtere Bewertung.

Nach dem Suizid eines Lufthansapiloten, der seine voll besetzte Maschine in den Alpen zum Absturz brachte, fordern Technokrat*innen, Risikoberufe unter permanente Beobachtung durch eine solche Sprachanalyse zu stellen – in der Hoffnung, dann Warnhinweise auf eine drohende Depression zu erhalten.

Das eigenständige „Hinzulernen" der auf künstlichen neuronalen Netzen basierenden Software hat seine Eigenheiten und entzieht sich per Konstruktion der begleitenden Kontrolle selbst ihrer Programmierer*innen. Ein Beispiel: Amazon hatte eine Software entwickelt, die eine Vorabbewertung von Bewerbungsunterlagen vornehmen sollte. Die Software lernt eigenständig und sucht in allen bisher analysierten Bewerbungen nach Mustern, die auf eine geeignete Kandidat*in hinweisen. Amazon schaltete die Software wieder ab, als sie sich mehr und mehr zur Frauenfeindin entwickelte. Das Muster „männlich" schien ihr (aus den gegebenen Daten heraus) besonders erfolgversprechend zu sein. Kaum eine weibliche Bewerberin wurde zum Casting vorgeschlagen.

In ähnlicher Weise entpuppte sich 2016 Microsofts Chatbot Tay mit wachsender Gesprächserfahrung nach nur 16 Stunden Geschwätzigkeit als Nazi und musste abgeschaltet werden. Er „lernte" lediglich Inhaltsmuster von seinem offenbar politisch unausgewogenen Schatz an Gesprächspartner*innen.

Eine simple Softwarekorrektur ist dann nicht möglich. Nicht einmal die Vorhersage, ob es zu einer solchen Ausprägung von Mustern kommen könnte. Die Programmierer*in müsste sämtliche bisher gemachten „Erfahrungen" der Software nachvollziehen, um eine solche Vorhersage von unerwünschten Mustern zu treffen. Die Qualität der Daten ist eine wichtige Kenngröße bei diesem Problem. Lernt die Software frei hinzu, geht die Kontrolle über die Qualität der nun wachsenden Datenbank in der Regel verloren.

DAS ENDE DER THEORIE

Chris Anderson (ehemaliger Chefredakteur des Technologie-Magazins Wired) läutete bereits 2013 in einem Essay „Das Ende der Theorie" ein. Er schrieb, man brauche keine semantische oder kausale Analyse mehr – eine statistische reiche völlig aus:

„Wir leben in einer Welt, in der riesige Mengen von Daten und angewandte Mathematik alle anderen Werkzeuge ersetzen, die man sonst noch so anwenden könnte. Ob in der Linguistik oder in der Soziologie: Raus mit all den Theorien des menschlichen Verhaltens! Vergessen sie Taxonomien, die Ontologie und die Psychologie! Wer weiß schon, warum Menschen sich so verhalten, wie sie sich gerade verhalten? Der springende Punkt ist, dass sie sich so verhalten und dass wir ihr Verhalten mit einer nie gekannten Genauigkeit nachverfolgen und messen können. Hat man erst einmal genug Daten, sprechen die Zahlen für sich selbst."[36]

Fast könnte man meinen, Anderson habe recht: Die erfolgreichste Variante künstlich-intelligenter Sprachübersetzungs-Software von Google verzichtet fast vollständig auf grammatikalische Vorgaben der beiden beteiligten Sprachen. Die Übersetzung basiert ausschließlich auf ausreichend vielen Textdaten, die in einen selbst-lernenden Algorithmus zur Sprachmustererkennung eingespeist werden. Google versucht also gar nicht erst, eine Sprache „zu verstehen" – das heißt, per Abstraktion Sprachregeln abzuleiten und sich somit eine Theorie der Sprache zu erarbeiten, sondern erhöht die Wahrscheinlichkeit einer treffenden Übersetzung ganzer Wortgruppen durch zwei Dinge: die stetige Erweiterung der Vergleichsdatenbanken bereits getätigter „Übersetzungen" und eine darauf basierende, sich automatisch anpassende Neugewichtung erkennbarer Übersetzungsmuster. Nach Milliarden so „übersetzter" Texte könnten KI-Enthusiast*innen behaupten, diese erlernten Gewichte (Korrelationen) gäben eine Art „Grammatik" der Sprachübersetzung z. B. vom Spanischen ins Isländische wieder.

WER DIE DATEN BESITZT, HAT DIE MACHT

Der entscheidende Punkt ist: Diese „Grammatik" ist nicht extrahierbar – der Mensch profitiert nicht in einer von der künstlich-intelligenten Maschine abstrahierbaren Form von diesem „Übersetzungs"wissen. Das Wissen ist nicht von der immer größer werdenden Sprachmusterdatenbank abzutrennen: Wir lernen nichts über das Wesen der beteiligten Sprachen. Das künstlich „Erlernte" wird kein für andere erlernbares Allgemeinwissen. Googles Übersetzungsassistent ist eine „Black Box". Alleinig die Institution bzw. das Unternehmen, welches die Datenbank besitzt, hat die Deutungshoheit inne und profitiert davon. Google häuft Herrschaftswissen an und behauptet, einen Beitrag zur allgemeinen Verständigung und zur Wissensvermehrung zu liefern – für alle frei zugänglich.

36 Chris Anderson, Das Ende der Theorie in „Big Data - Das neue Versprechen der Allwissenheit", Suhrkamp, 2013

Mehr noch: Die Eigentumsverhältnisse der Datenbank machen eine behauptete Universalität von Datenzusammenhängen unanfechtbar. Der Geltungsbereich eines theoriefreien Datenzusammenhangs ist nicht verifizierbar: ohne Offenlegung der Daten ist die Nachvollziehbarkeit, also auch die Reproduzierbarkeit behaupteter Datenzusammenhänge, nicht gegeben.

Der Übersetzungsassistent ist (derzeit) für alle „frei nutzbar" und dennoch machen wir uns mit seiner Nutzung von Google abhängig. Ein leichter Schritt für Google, in einer späteren Entwicklungsstufe die Nutzung der Software an Bedingungen zu knüpfen. Nicht jetzt, wo wir alle beitragen sollen zu Googles Wissensanhäufung – aber später, wenn die Sprachassistenz als Alltagswerkzeug etabliert ist und viele Alltagsabläufe nur noch mit ihr zu bewerkstelligen sind. Dann kann Google entscheiden, wer zu welchen Konditionen die bis dahin entwickelte Echtzeit-Übersetzung von Sprache A nach B nutzen darf.

Eine solche Verengung des vormals freien Zugangs ist keine pessimistische Phantasterei, sondern Realität für die Mehrzahl der erfolgreichen, zunächst unabhängigen Software-Entwicklungen. Als Startup von Google, Facebook, Amazon und Co. gefördert, zum Marktführer aufgebaut, später verschluckt und als Dienst in die eigene Produktgruppe eingemeindet, werden sie zunächst weiter frei angeboten. Schleichend werden dann jedoch über die Allgemeinen Geschäftsbedingungen (AGB) Konditionen für die Nutzung verändert.

Einige werden sich noch erinnern, dass Facebook bei der Übernahme von WhatsApp garantiert hatte, es werde keinen Datenaustausch zwischen WhatsApp und Facebook geben. Die Realität sah schnell anders aus.

Der Macht zentral gesammelter Daten in einem durch die Omnipräsenz digitaler Dienste transformierten Kapitalismus gehen wir im Artikel „Die Krise der Repräsentation" hier in diesem Band nach. Wir verweisen auf die vielfältigen Methoden der sozialen Physik zur personalisierten Lenkung individuellen Verhaltens. Es hat in der Geschichte der Menschheit keine vergleichbar große Möglichkeit der Machtkonzentration gegeben!

Dabei ist die Macht der Daten nicht unmittelbar bei ihrer Erhebung ersichtlich. Häufig stellen sich Konsequenzen der persönlichen Abhängigkeit von diesen Daten viel später heraus. Die viel zitierte „Rosa Liste", in der die Daten von Schwulen und Lesben im Deutschland der Weimarer Republik erhoben wurden, hatte erst (deutlich zeitversetzt) unter der Naziherrschaft dramatische Folgen für die dort Verzeichneten.

GEWÖHNUNG AN ZENTRALE DIENSTE

Bei digitalen Diensten, deren Dienstleistung auf Künstlicher Intelligenz basiert, stellt die Kopplung von künstlich „Erlerntem" an die Erfahrungsdatenbank das zentrale Merkmal dar. Die Erfahrungsdatenbank ist das eigentliche Herzstück des Dienstes, ganz egal, ob wir von Facebook, Google, Amazon oder Uber reden. Diese Art des künstlichen „Lernens" setzt voraus, dass die Nutzer*in des Software-Dienstes, die gleichzeitig Trainer*in der Datenbank ist, permanent mit der zentralen Datenbank verbunden – also online – ist.

Wenn wir uns an die 90er Jahre zurück erinnern, stellen wir fest, dass damals der Großteil der Nutzer*innen-Software lokal und offline funktionierte. Derart dezentrale „Dienste" erlauben keine Ökonomisierung des Nutzer*innenverhaltens. Die Verlagerung vieler ehemals eigenständiger Standardsoftware in cloud-basierte Dienste war und ist eine notwendige Gewöhnung der Nutzer*in an die neue App-ifizierte Mensch-Software-Relation. Eine Textverarbeitung benötigt keine Online-Funktionalität – auch nicht für die Rechtschreibkorrektur. Der Gewinn, von unterschiedlichen Geräten auf die verfassten Texte zugreifen zu können, ist für die meisten ebenfalls ein marginaler. Viele haben sich schlichtweg daran gewöhnt, dass alles nur online zu funktionieren scheint. Es ist fast ein kultureller *shift*, den wir bereitwillig mitgegangen sind. Erst beim Netzausfall merken wir die unsinnig große Abhängigkeit von der cloud.

VERDRÄNGUNG DER KAUSALITÄT

Joseph Weizenbaum war einer der KI-Pioniere in den 60ern. Fasziniert von den Möglichkeiten der algorithmischen Simulation schrieb er ein Programm namens ELIZA. Heute würden wir dieses Programm einen Chatbot nennen. Der Computer nimmt die Position einer Psycholog*in ein und gibt vor, zu „verstehen", was die Klient*in äußert. Simples Aufgreifen des Gesagten in Form einer Frage lässt den Eindruck entstehen, ELIZA höre wirklich zu. Von der überhöhenden gesellschaftlichen Rezeption der Fähigkeiten seiner recht schlichten „künstlichen Intelligenz" geschockt, entwickelte sich Weizenbaum zum glühenden Kritiker der Künstlichen Intelligenz.

Weizenbaum warf den nun folgenden KI-Technokrat*innen die bewusste Verschleierung des Unterschieds zwischen (phänomenologischer) "Beschreibung" und einer „Theorie", die semantische bzw. kausale Zusammenhänge aufzeigt, vor. Besonders fatal wird dies bei der Modellierung des Menschen mit seinen Persönlichkeitseigenschaften. Der Vorwurf lautet: KI-Enthusiast*innen geben das Datenabbild eines Menschen für den Menschen selbst

aus. Das meint, die Beschränkungen einer modellhaften Beschreibung nicht nur zu vergessen, sondern bewusst zu vertuschen. Weizenbaum prognostizierte fatale Folgen bis hin zum Verlust der Eigenständigkeit in einer von Künstlicher Intelligenz fremdbestimmten Welt digitaler Dienste.

Die Kausalität ist, anders als die Korrelation, ihrem Wesen nach überprüf-, hinterfrag- und angreifbar. Sie ist nicht proprietär und eignet sich daher weniger zum Aufbau von Machtgefälle. Die im Abschnitt „Das Ende der Theorie" zitierte radikale Position von Chris Anderson muss vor diesem Hintergrund als machtbewusst interpretiert werden. Daher ist es nur folgerichtig, dass Anderson die klassische Theoriebildung in der Physik als unzureichend diskreditiert, nämlich als *„Schöne-Geschichten-Phase einer Disziplin, die an Datenhunger litt"*[37] . Hier manifestiert sich der Irrglaube, dass qualitative Methoden „Geschichten interpretieren", während quantitative Methoden „Tatsachen produzieren". Anderson geißelt NonBigData-Ansätze schlichtweg als statistisch zu schwach fundiert.

37 Chris Anderson, Das Ende der Theorie in „Big Data - Das neue Versprechen der Allwissenheit", Suhrkamp, 2013

Das, was Paul du Gay und Michael Pryke über die Buchhaltung schrieben, nämlich, *„dass die Werkzeuge […] nicht einfach nur die Messung der wirtschaftlichen Aktivität erleichtern, sondern dass sie auch die Realität verändern, die mit ihr gemessen werden soll"*, gilt in gesteigertem Maße auch für die Kopplung von BigData-Analysen mit Methoden der Künstlichen Intelligenz.

„Verändere die Instrumente, und Du wirst die gesamte Sozialtheorie verändern, die mit ihnen zusammenhängt." (Bruno Latour)

So wie der Fordismus mit seinen Innovationen rund um das Fließband nicht nur als Werkzeugsammlung gesehen werden kann, und neben der Arbeit gleich die ganze Gesellschaft transformierte, so kreiert der Doppelpack aus BigData und KI machtbewusst eine Welt des Wissens, die ebenfalls die Subjekte und Objekte der Wissensgesellschaft verändert. Das umfasst auch unsere Sozialität, also das Verständnis, wie wir menschliche Netzwerke und Gemeinschaften verstehen.

Predictive Policing

Im Musterpolizeigesetz, das Horst Seehofer gerne deutschlandweit einführen möchte, sind zwei Dinge wichtig: Aufrüstung und präventive Gefahrenabwehr. In der Vergangenheit war Prävention auch positiv besetzt und umfasste Aufklärungsarbeit oder kostenlose Beratung (meistens zu Schließanlangen fürs Eigenheim). Heute ist sie gleichbedeutend mit präventiver Gefahrenabwehr, die vor allem durch technische Aufrüstung und erweiterte Überwachungsbefugnisse erreicht werden soll. Dahinter steckt die Hoffnung, gesellschaftliche Probleme durch Technik zu lösen oder zumindest so unsichtbar machen zu können, dass man sich für die Erhöhung des „subjektiven Sicherheitsgefühls" rühmen kann. Das Schlagwort, hinter dem sich viele verschiedene Technologien verstecken, ist Predictive Policing. Das Marketingversprechen ist, dass sie helfen, Straftaten zu verhindern, bevor sie passieren.

Wen das an den Film Minority Report erinnert, die*der liegt nicht ganz falsch. Nur dass statt Mutanten auf Drogen, die in einer Nährlösung vor sich hin vegetieren, heute Algorithmen auf Big Data in der Cloud die Allzweckwaffe präventiver Polizeiarbeit sein sollen. Wenn Horst den Film zu Ende geguckt hätte, wüsste er allerdings, dass das System abgeschaltet und die Mutanten befreit werden, weil sich herausstellt, dass man auch Visionen hijacken kann. Ob es im Real Life auch soweit kommt, wird sich zeigen.

Predictive Policing ist zwar schwer angesagt und wird in Medien und Politik diskutiert, ist aber abseits einiger einzelner Probeläufe in der Breite in Deutschland noch nicht im Einsatz. Die vielen neuen Polizeigesetze der letzten Monate und Jahre sollen die Entwicklung aber fördern. Die Software dazu wird vor allem in den USA, aber auch in Indien, China und Australien entwickelt. Und auch in Deutschland hat der Hype um Big Data diejenigen inspiriert, die an die dicken Finanztöpfe der öffentlichen Verwaltungen wollen.

WIEDERHOLUNGSTÄTER VS. COMPUTER

Nicht zuletzt auf Grund der strengeren Datenschutzgesetze in Europa, gepaart mit dem nationalistischen Wunsch, den IT-Standort Deutschland zu stärken, sind in Deutschland zur Zeit vor allem Softwareprodukte „made in Germany" im Einsatz. Dazu gehört neben Software, die in den Landeskriminalämtern selbst entwickelt wird, das System „PRECOBS" des „Instituts für Musterbasierte Prognosetechnik" aus Oberhausen. Die Idee hinter der Software ist simpel und wird so oder so ähnlich in vielen Predictive Policing-Verfahren benutzt. Sie basiert auf der Theorie der „Near Repeats", die besagt, dass viele Verbrechensarten einen Wiederholungscharakter haben. PRECOBS ist spezialisiert auf Einbrüche und geht davon aus, dass ein erfolgreicher Einbruch die Wahrscheinlichkeit erhöht, dass in der selben Gegend in nicht allzu ferner Zukunft noch einmal eingebrochen wird. Dabei spielt die Motivation oder Herkunft der Täter*innen für den Algorithmus keine Rolle – anders als bei Populist*innen, für die nur „ausländische Einbrecherbanden" hinter Mehrfacheinbrüchen stehen können. Die Software löst bei Eingang einer Einbruchsmeldung und in Kombination mit weiteren Tatmerkmalen (Haustyp, Lage, Beute, Jahreszeit und „Modus Operandi")[38] einen Alarm aus, wenn statistisch ein weiterer Einbruch in der näheren Umgebung wahrscheinlich scheint. Das wiederum soll dann zur Einsatzplanung herangezogen werden, so dass z. B. mehr Streifen in der Gegend unterwegs sind und entweder abschrecken oder bestenfalls die Täter*innen fassen.

Ähnlich funktioniert das in den USA verbreitete PredPol-System. Deren Algorithmus stammt aus der Erdbebenforschung und diente ursprünglich dazu, Nachbeben vorauszuberechnen. Auch hier werden Städte in Quadrate gerastert und, wird in einem Abschnitt ein Ausschlag registriert, steigt die Wahrscheinlichkeit, dass dort oder in den Nachbarbereichen bald wieder das Gesetz überschritten wird. Verbrechen wird so naturalisiert und mit unvermeidbaren Ereignissen gleichgesetzt, deren Auswirkungen durch kluge Ressourcenplanung verringert werden sollen. Deren Ursachen, wenn auch vielleicht bekannt, spielen dafür keine Rolle. Die Technik unterstellt sozialen Systemen, nach Naturgesetzen zu funktionieren. Einerseits nimmt es damit die Nutzer*innen (diejenigen mit dem Gewaltmonopol) aus der Verantwortung, sich darum zu kümmern, warum etwas passiert. Andererseits ist es aber auch der blinde Fleck der Algorithmen, anzunehmen, dass das Vorgehen der vielbeschworenen „Einbrecherbanden" auch in Zukunft immer den gleichen Gesetzen folgen wird.

38 Die genaue Funktionsweise bleibt bei allen Systemen natürlich geheim. Aber einiges lässt sich aus der Dokumentation von Forschungsprojekten entnehmen. Für PRECOBS gibt es z. B. eine Evaluation des Max-Planck Instituts: https://www.mpicc.de/de/forschung/forschungsarbeit/kriminologie/predictive_policing_p4.html

DEFINITIONEN GEFÄHRLICHER ORTE

Eine zweite Kategorie von Predictive Policing fokussiert weniger die konkreten Taten, sondern geht davon aus, dass bestimmte Eigenschaften von Orten die Wahrscheinlichkeit erhöhen, dass dort Straftaten begangen werden – „Gefahrengebiet" und „kriminogene Orte" kennt die Polizei auch jetzt schon – und die Statistiker*innen bestätigen dies mit ihren Algorithmen gerne. Eine der Methoden dahinter heißt „Risk Terrain Modelling". Forscher*innen arbeiten seit Jahren daran, Korrelationen zu berechnen zwischen Straftaten und den Eigenschaften von bestimmten Orten, an denen sie besonders häufig begangen werden. Die Zahlen zeigen zum Beispiel: Geklaut wird häufig in der Nähe von Sehenswürdigkeiten oder auf Fahrradabstellplätzen, geprügelt wird sich vermehrt dort, wo Kneipen vorhanden sind, und Vergewaltigungen wiederum passieren (nicht nur in den USA) dagegen gehäuft in oder in der Nähe von Studierendenwohnheimen.[39] Hat man all diese Statistiken und gleichzeitig genaue Karten, in denen all diese Dinge markiert sind, kann man für beliebige Zonen die Wahrscheinlichkeiten berechnen, mit denen bestimmte Dinge passieren. Theoretisch ist eine Kombination mit der Near Repeat-Idee möglich. Einbrüche etwa sind dort wahrscheinlicher, wo Autobahnauffahrten in der Nähe sind. Auch hier ist das Ziel vor allem die Einsatzplanung: Kriminalität als Frage des Managements von Einsatzkräften. Anbieter wie das US-Unternehmen „Hunchlab" entwickeln Apps für die mit Tablets ausgestatteten Polizeiwagen, die in Zukunft (wahrscheinlich schon voll automatisch) in die Richtung des Verbrechens fahren, bevor der Notruf gewählt wurde. Auch hier ignoriert die Statistik die Ursachen – Korrelation bedeutet nicht Kausalität. Es ist nicht die Tatsache, dass Studierendenwohnheime existieren, die die Wahrscheinlichkeit erhöht, dass deren männliche Bewohner zu Vergewaltigern werden. Gleichzeitig führt auch ein Polizeiwagen vor der Tür nicht automatisch dazu, dass sich Frau* sicherer fühlen kann, wenn darin wieder nur Männer sitzen, die Korpsgeist verstehen, aber nicht die Vielschichtigkeit sexueller Gewalt.

Was diese Techniken auch unter dem strengen und von den Polizeibehörden wenig geliebten europäischen Datenschutzregime möglich macht, ist die Tatsache, dass bei beiden Verfahren irrelevant ist, wer oder was ein Verbrechen verübt. Wichtig sind allein die Korrelationen. Warum die *rape culture* auf den Campussen so verbreitet ist oder welche stadtpolitischen Maßnahmen dazu geführt haben, dass Drogenhandel und Beschaffungskriminalität sich in bestimmten Stadtteilen konzentriert, ist für diese Art der Polizeiarbeit irrelevant.

39 Caplan, Joel M., and Leslie W. Kennedy. 2011. Risk Terrain Modeling Compendium: For Crime Analysis. New Jersey: Rutgers Center on Public Security http://www.rutgerscps.org/uploads/2/7/3/7/27370595/riskterrainmodelingcompendium_caplankennedy2011.pdf

WIE GEFÄHRLICH SIND GEFÄHRDER*INNEN?

Die Diskussion um Fußfesseln und Präventivhaft für so genannte Gefährder*innen weist darauf hin, dass predictive policing auch sehr persönlich werden kann. Für die Berechnung des persönlichen Risikos, straffällig zu werden, gibt es verschiedene Verfahren. In Deutschland genutzt wird die Software DYRiAS, die das BKA in Zukunft unter dem Namen RADAR einsetzen will. Die dazugehörige Software ist im Stil einer Onlineumfrage gestaltet und spuckt nach der Beantwortung einer Reihe von Fragen zur Persönlichkeit einen Risikowert aus. Das Prinzip wurde in einigen Studien vor allem zu häuslicher Gewalt und jugendlichen Gewalttäter*innen an Schulen mehr oder weniger erfolgreich evaluiert.[40] Grundvoraussetzung für die Nutzung ist (bisher), dass nur psychologisch geschulte Personen den Fragebogen ausfüllen dürfen, eine automatisierte Berechnung auf Basis anderer Daten gibt es bisher nicht.

Wie so etwas automatisiert werden kann, zeigt das Beispiel der „Heat List", die seit einigen Jahren in Chicago – seit längerem die Stadt mit der höchsten Mordrate in den USA – im Einsatz ist. Anhand von Netzwerkanalysen, vermuteten Gangzugehörigkeiten und Vorstrafen erstellt ein Polizeicomputer dort eine Liste von Personen, für die angenommen wird, dass sie Opfer oder Täter*in eines Gewaltverbrechens werden. Die Polizei stattet dann einen Hausbesuch ab, was der hier auch üblichen „Gefährderansprache" entspricht und warnt die Personen vor den negativen Effekten, die ihr aktuelles Verhalten haben kann. Eine ähnliche Software wird in verschiedenen US-Städten auch zum vermeintlichen Schutz von Polizist*innen eingesetzt. Geht ein Notruf ein, führt ein Programm alle bekannten Daten (zum Beispiel zum Haus) zusammen, aus dem der Anruf kommt (Vorstrafen der dort Wohnenden, evtl. existierende registrierte Waffen usw.), und zeigt den Polizist*innen auf einer praktischen Ampelskala an, wie sie sich vorbereiten sollten.

POLIZEI UND ALGORITHMEN IM ZAUM HALTEN!

Überall wird die Einführung von Predictive Policing von viel Kritik begleitet. Vor allem Bürgerrechtsgruppen richten ihre Kritik auf die Gefahr von Vorverurteilungen und der technisch gestützten Reproduktion von diskriminierenden Stereotypen. In stark segregierten Städten führen seit jeher immer die selben Stadtteile die Kriminalstatistiken an. Senden die Leitstellen, gestützt durch diese Statistik, mehr Polizei in einen Stadtteil, führen mehr Kontrollen in der Regel auch dazu, dass die Zahlen steigen, was der Algorithmus wieder zum Anlass nimmt, dorthin zu navigieren. Diese Feedback-Schleife zu durchbrechen erfordert einen reflektierten Umgang mit der Technologie, die man zumindest Horst Seehofer eher nicht zutraut. Bei den personalisierten Risikoberechnungen fallen vor allem die so genannten „false positives" auf, wenn der Computer Alarm schlägt, obwohl dies unangemessen ist. Es gibt Berichte aus Chicago von Hausbesuchen bei Menschen, die bisher nur wegen kleineren Drogendelikten aufgefallen waren, und die von der Polizei vor den Augen der Nachbarschaft nun vor dem tödlichen Ende ihre Gangkarriere gewarnt wurden. Solche Fälle werden auch hier wahrscheinlicher, wenn der Druck hoch ist, vor allem „false negatives" zu vermeiden – Fälle wie der von Anis Amri, dem Expert*innen kein besonders hohes Risiko bescheinigten, was sich ebenfalls als Trugschluss erwies. Wer das verhindern will, knastet lieber zu viele Personen ein als zu wenige – so wie es die Präventivhaft in den neuen Polizeigesetzen erlaubt.

In letzter Zeit bekommen Kritiker*innen aber auch Unterstützung durch Statistiken. Wie die Studie zu PRECOBS in Baden Württemberg zeigen auch andere, länger laufende Tests in Zürich kaum signifikante Verbesserungen der Situation durch den Einsatz von Software. Gerade bei der Einbruchsvorhersage sind die Effekte statistisch nicht messbar. Die Zahlen gehen gerade überall zurück und in den Gebieten, in denen die Software genutzt wird, nicht mehr also anderswo. So hat auch eine kleine Anfrage im Bundestag zu den Plänen des BKA zur Ausweitung von predictive policing zuletzt ergeben, dass der Hype etwas zurückgegangen ist – konkrete Pläne für einen bundesweiten Einsatz bestimmter Systeme gibt es zunächst nicht. Auch nach fünf Jahren wird noch breit „evaluiert". Die Hersteller der Software setzen daher auf einen anderen Trend – die Digitalisierung – und argumentieren, dass, wenn die Software schon keinen Effekt auf die Kriminalstatistiken habe, sie dann doch definitiv einen Einfluss auf die Kostenkalkulation habe. Aus „Kommissar Computer" wird dann vielleicht „Einsatzleiter Algorithmus" – wie der sich dann beeinflussen lässt, wird eine interessante Frage sein.

Aber auch, wenn sich die posthumanistischen Visionen der Kybernetiker*innen nicht erfüllen, darf die Kritik nicht aufhören. Es geht nicht nur gegen Algorithmen und die implizite Fortschreibung bekannter Machtlogiken, sondern gegen die Ausstattung der Polizei mit geheimdienstähnlichen Rechten und militärischer Technik. Während die Kriminalitätsraten zumindest in Europa und den USA immer weiter sinken, verschiebt sich die Diskussion hin zum Kriminalitätsmanagement, bei dem die politischen, sozialen und ökonomischen Hintergründe keine Rolle mehr spielen und Statistiken die Diskussionen ersticken.

40 Grossenbacher, Timo. 2018. https://www.srf.ch/news/schweiz/predictive-policing-polizei-software-verdaechtigt-zwei-von-drei-personen-falsch

Gefangen in der Gesundheits-Assistenz

FITSPIRATION

„Fitness als Inspiration für den eigenen Lifestyle", so bewirbt die santé generali den angeblich neuen Trend. Lachende Hipster, die im engsten Wortsinn spielend ihren Gesundheitsindex erhöhen, um damit Geld zu sparen. Alles ganz easy: Wer sich bewegt, spart. Sportliche Inaktivität hingegen wird immer öffentlicher und immer eindringlicher als Ursache von selbst verschuldeter Krankheit markiert. Die digitalisierte Gesundheitsbranche entwickelte sich schneller, als viele erwartet hatten. Sie sollte das umsatzstärkste Segment der technologischen Umwälzung in den 2020ern werden. Es dauerte nur wenige Jahre, da waren die ehemals alle betreffenden „Zivilisationskrankheiten" als Folge eines individuell-unachtsamen Lebensstils ausgemacht. Bewegungsarmut wurde zur persönlichen Verhaltensstörung, die die Gesellschaft so teuer zu stehen kommt, dass jeder in Eigenverantwortung dafür haften soll. Das Solidaritätsprinzip im Krankheitsfall war erfolgreich ausgehebelt – schleichend, fast unmerklich. Dabei sind die Gesundheits-Assistenten mit ihren Fitnessarmbändern und Smartwatches doch nur der technische Ausdruck eines kulturellen Leitbilds vom fitten, ausgeglichenen, berechenbaren und leistungsbereiten Menschen – oder? Wäre eine derartige Entmündigung ohne den technologischen Charakter dieser gesellschaftlichen Umwälzung von oben überhaupt denkbar gewesen? Begonnen hatte alles auf jeden Fall ganz harmlos. Die anfangs noch hilfreich daher kommenden Anleitungen zur körperlichen Selbstoptimierung wären beinahe bis hin zur völligen Fremdbestimmung ohne jeden Widerspruch durchgegangen. Beinahe.

Janine hat nichts gegen Selbstvermessung, im Gegenteil. Sie benutzt seit Jahren eine Wasser-App, um sich daran zu erinnern, genug zu trinken, und eine Schlaf-App, weil sie schlafen besonders gut kann und das morgens gern bestätigt sieht. Seit einiger Zeit zeichnet die App auch auf, wie sie schläft und wenn sie nachts schnarcht. Wenn sie wollte, könnte Janine ihr Schnarchen als mp3-Datei an Freunde oder ihre Recreation-Therapeutin verschicken.

Schon morgens wird Janine nun von einer App geweckt.

Guten Morgen Janine – Heute Nacht hattest Du 4:48 Stunden Schlaf bei einer Schlafqualität von 72 Prozent. Du hattest vier Tiefschlafphasen von insgesamt 2:13 Stunden. Du hast gestern noch spät gegessen. Das verkürzt Deine Tiefschlafphasen. Gönn Dir nächste Nacht etwas mehr Schlaf.

Das ist der Sleepy-Coach. Janine mag ihn nicht.

Ich bin erwachsen und gehe ins Bett, wann's mir passt.

Aber sie ertappt sich immer öfter, dass ihr die Fitness-Empfehlungen mehr bedeuten, als sie anfangs hoffte. Janine hat von ihrer Versicherung ein neues Armband zugeschickt bekommen. Schon das dritte. Aufenthaltsort, Puls, Blutdruck, Sauerstoffkonzentration im Blut, gelaufene Schritte und verbrannte Kalorien werden permanent aufgezeichnet und an die Krankenkasse gesendet. Letzten Dienstag gab es ein Problem und das Gerät hatte nicht aufgezeichnet. Ihr ist nicht klar, ob sie das Armband zu locker eingestellt hatte, oder ob es ein Softwareproblem bei der Datenübertragung an die santé generali gab.

Kea 24/7 – Janines Daily-Assistent zur Steigerung der Leistungsfähigkeit – ist immer mit und bei ihr. Perfekt assistieren kann Kea nur, wenn Janine online ist. Aber normalerweise kann Kea selbst offline ihren Körperzustand aufzeichnen. Die Körper-Daten werden dann nachträglich vervollständigt und interpretiert. Dann kann es allerdings sein, dass Janine dem Programm für die optimale Assistenz zusätzlich einige Fragen beantworten muss.

Diesmal hingegen muss etwas anderes vorliegen. Janine ärgert sich, da sich ihre eher seltene sportliche Aktivität nicht positiv auf dem Bewegungskonto niederschlägt. Wenn sie sich schon mal durchringt, Sport zu machen, dann soll es sich wenigstens „lohnen". Eigentlich findet sie das bescheuert. Aber sie kennt es bereits vom Bahnfahren. Wenn sie sich doch mal ein Ticket kauft, ärgert sie sich, wenn mal wieder kein Schaffner kommt, um ihr Nicht-Schwarzfahren mit einem Zangenabdruck zu honorieren. Und so geht es ihr nun auch mit der Aufzeichnungspause ihrer App: Obwohl sie die manuelle Option „Nachtragen" anfangs noch als krankhaften Nerd-Scheiß für Selbstvermessungsfanatiker und Ordnungs-Kleingeister belächelt hatte, klickt sie sich nun schon minutenlang durch die Menüs ihrer Fitness-App, um ihre dreistündige Radtour einzutragen. Das gibt Punkte, die sie sich nicht entgehen lassen möchte.

Das Punkte-Fieber befällt Janine nun öfter, als ihr lieb ist: „Wenn ich mir eine Zigarette anmache, steigt mein Herzschlag auf Fettverbrennungsmodus. Das zeigt mir zumindest mein Armband an. Vielleicht kann ich durch intensives Rauchen punkten." Trotzdem kommt sie mit einer Zigarette vor dem Sport nicht aus dem gelben Bereich ihres Fitness-Anzeigers auf dem Smartphone. „Kann es sein, dass mit meinem Armband etwas nicht stimmt?", tippt sie in den Kundenchat. Ihr Puls erscheint ihr abnormal beim Abgleich mit den „Sollwerten" ihrer Altersgruppe. Das stresst sie nun schon seit Wochen und daher beschließt sie, zum Internisten zu gehen. Alles gut, sagt der Arzt. Es kämen jetzt häufiger Leute, die ihre Fitnessbänder nervös machten.

Ob die App bemerkte, wenn nicht sie, sondern ihr Hund das Band tragen würde? Einen Versuch ist es wert. Bislang ist sie noch nie zum Glaubwürdigkeits-Chat geladen worden. Negativ, die „Trainingssequenz" ihres Hundes wird einfach ignoriert und von ihrem Punktekonto werden kommentarlos 55 Punkte abgezogen. Sie weiß nicht genau wie, aber die Analyse-App hat den fremden Träger des Bandes offenbar erkannt – vielleicht an der ungewöhnlichen Herzfrequenz oder an der abweichenden Erholungsphase? Die App schweigt darüber.

Es gäbe nochmal „Bonus-Points", wenn Janine sich mit Freunden zu einer „Energy-Burner-Group" zusammenschließen würde. Dann würden alle erzielten Bewegungswerte permanent verglichen: Alle bekämen „zur Motivation" täglich ihren Tabellenplatz in der Gruppe angezeigt. Der Gruppenerste bekommt für jeden Tag seiner „Leadership" Bonuspunkte. Aber irgendwie traut sie sich nicht. Zum einen hat sie keine Freunde, in deren Umfeld sie punkten könnte. Zum anderen kommt ihr der eigene Punkte-Wahn immer noch wie ein charakterlicher Makel vor, mit dem sie sich lieber doch nicht outen möchte. Also frönt sie ihrer neuen Leidenschaft zunächst lieber noch „heimlich".

Janine ist alles andere als eine Sportskanone, daher dümpelt ihr Gesundheitsindex im unteren Mittel. Aber: Viel spazieren hilft auch. Bei der santé generali bekommt Janine 100 Bonuspunkte pro Monat, wenn sie jede Woche mindestens 50.000 Schritte macht. Bei 1000 Punkten gibt es 30 Euro Rückzahlung. „Na ja – kein wirklich guter Stundenlohn", errechnet sie. Daher legt sich ihre Bonus-Punkte-Jagd nach einem halben Jahr wieder. Etwas anderes wäre es, wenn „Minderleister" von ihren Kassen sanktioniert würden – etwa mit Zusatzbeiträgen, denkt Janine. „Einen Bonus auszuschlagen fühlt sich irgendwie immer noch anders an, als Strafpunkte zu bekommen" – ein Gesundheitsknöllchen also.

DAS ANGEBOT

Janine ist seit nunmehr acht Jahren selbständig. Derzeit läuft es nicht so gut. Sie schlittert nun schon seit einem Jahr knapp an der Zahlungsunfähigkeit vorbei. Bei ihrer Krankenkasse beantragt sie, vorübergehend als Geringverdienerin eingestuft zu werden: Wer belegen kann, dass die Einkünfte im letzten Halbjahr unter 6200 Euro liegen, kann auf Antrag die Krankenkassenbeiträge um 45 Prozent senken. Janines Krankenkasse, die santé generali, willigt seit der Richtlinien-Anpassung vom 1. Juli 2019 jedoch nur noch ein, wenn die Antragstellende dazu „freiwillig" in das neue Assistance-Modellprojekt wechselt.

Janine stimmt den Vertragsbedingungen skeptisch zu – sie hat eh keine Idee, wie sie anderweitig ihre monatlichen Fixkosten reduzieren kann. Im Assistance-Modelltarif erhält der Versicherte eine kostenlose Beratung per App zur „Orientierung", bevor die App einen Termin mit

dem Hausarzt oder einem Facharzt vereinbart. Das, was nach zusätzlichem Service klingt, ist der neueste Kniff einiger Digitalisierungs-Vorreiter unter den Krankenkassen. Denn real entscheidet nun eine vorgeschaltete Beratungs-App: Wer bekommt einen Termin beim akkreditierten Vertragsarzt und wer bekommt nur ein paar KI-generierte Gesundheitstipps. Es hängt also von Janines Online-Beantwortung des App-Fragenkatalogs ab, ob sie bei akuten Bauchschmerzen beim Hausarzt vorsprechen darf, oder nur ein paar Hausmittel und verschiedene Tees empfohlen bekommt.

Zunächst bereute Janine ihre Entscheidung nicht – immerhin sparte sie monatlich fast 170 Euro. Ihre bisherige Hausärztin wurde ebenfalls von der santé generali als Vertragsärztin akzeptiert. Die App war zwar etwas neugierig, und dementsprechend aufwändig war die Erstanmeldung beim Software-System des Assistance-Tarifs. Die gesamte Historie ihrer bisherigen Gesundheitsprobleme nachzuzeichnen, bescherte ihr durchaus viele Stunden Arbeit. Das nervigste war die kleinteilige Bewertung sämtlicher Ratschläge und Diagnosen all ihrer dort gelisteten Arztbesuche. An die meisten erinnerte sie sich eh kaum noch. Auch an die Vorfälle, mit denen sie gar nicht erst zum Arzt gegangen war, hatte sie nur eine blasse Erinnerung. Trotzdem – das System fragte beharrlich weiter und weiter. Die Befragung abzubrechen war keine echte Option, denn sie brauchte ihre neue Assistance-ID. Ohne die konnte sie sich gar nicht bei der App auf ihrem Smartphone anmelden. Und ohne Assistance-App kein Arztbesuch. Daran musste sie sich erst gewöhnen. Überhaupt verbrachte sie nun deutlich mehr Zeit mit Dingen, mit denen sie vorher nichts zu schaffen hatte.

Janine, Dein Fitness-Level stagniert. Ich empfehle Dir ein extra auf Dein Leistungsniveau und auf Deinen Typ abgestimmtes Motivationstraining.

Janine klickt die Nachricht kopfschüttelnd weg.

Janine, wenn Du weiterhin von den günstigen Konditionen unseres Tarifs profitieren möchtest, solltest Du eines der unten angezeigten Motivationsvideos schauen.

DAS 24/7 PREMIUM PROGRAMM

Hallo Janine, Du kannst mich als Deine persönliche Assistentin erweitern. Obwohl ich hoffe, dass auch meine bisherigen Dienste für Dich hilfreich waren, könnte ich Dir noch besser zur Seite stehen. Ein neues Assistenz-Plugin steht zum Download für Dich bereit: „personal fitness 24/7“ ist unsere Premium-Assistenz. Damit kannst Du wesentlich genauer als bisher voraus berechnen, wann es für Dich besonders ratsam ist, zu schlafen, Sport zu treiben oder konzentriert zu arbeiten. Diesen maximal genauen Assistenz-Premium-Service bekommst Du für einen monatlichen Aufpreis von 14,99 Euro. Dafür bekommst Du die optimale Gesundheitsberatung. Schon bei einer Follow-Quote von 80 % unserer Empfehlungen sparst Du mit „personal fitness 24/7“ mehr Gesundheitsvorsorgekosten als den monatlichen Aufpreis. Willst Du das Plugin aktivieren?

Das Wetter ist gut, wie wäre es mit einer Stunde Jogging?

Ich jogge nicht gern, das bereitet mir Hüftschmerzen.

Ich verstehe, ich speicher die Schmerzen in Deiner E-Akte. Geh doch schwimmen – das nächste Bad befindet sich nur 15 Gehminuten entfernt.

Ich will gerade gar nicht raus – mir ist nicht danach.

Kein Problem, Du kannst auch 30 Minuten Yoga machen. Soll ich Dir die erste Übung auf den Bildschirm laden? Dein Outfit ist dafür allerdings nicht optimal – zieh Dir besser legere Trainingskleidung an. Deine graue Leggings scheint mir geeignet.

Janine ist genervt und schaltet den Assistenten einfach ab. Ständig diese bevormundenden Tipps, und diese durch nichts aus der Ruhe zu bringende Freundlichkeit gehen ihr zunehmend auf den Zeiger. Sie weiß, dass Abschalten nicht die beste Lösung ist. Diese wenig galante Zurückweisung kostet Janine Tagespunkte, und verlorene Punkte bedeuten einen höheren Tarif für ihre Krankenversicherung in diesem Monat. Janine nennt es noch heute Krankenversicherung, obwohl die Versicherungen und auch ihr KI-Assistent schon lange von „proaktiver Gesundheitsvorsorge“ sprechen. Die hat seit 2020 die Eigenverantwortung des Versicherten in den Mittelpunkt gerückt – zur Kostenreduktion. Das Gesundheitssystem sei sonst nicht mehr finanzierbar, heißt es.

Janine hat sich bislang nicht für den Intensivkurs „personal fitness 24/7“ eingetragen. Hier könnte sie am meisten Geld sparen, aber dort könnte sie nicht ohne weiteres eine Empfehlung ignorieren – das würde sie sofort aus dem Programm werfen. Und sie würde direkt für ein halbes Jahr in einer für sie nicht bezahlbaren Tarifklasse landen. Janine glaubt, dass eh nur Arbeitslose den Intensivkurs länger als zwei Monate durchhalten. Wer sonst hat soviel Zeit für drei Sport-Einheiten täglich und den wöchentlichen Gesundheitscheck?

Weit gefehlt, das Programm wird immer beliebter – insbesondere bei sogenannten „Leistungsträgern“. Renommierte Arbeitgeber „empfehlen“ ihren Mitarbeitern wärmstens, sich an dem Programm zu beteiligen. Fitness- und Workout-Gelegenheiten finden sich dort in jeder Abteilung. Janines alte Freundin Regina zum Beispiel arbeitet mittlerweile bei Mircosoft in München. Sie hat bereits informelle Team-Sitzungen im Workout-Stu-

dio ihrer Abteilung mitgemacht. Bei Mircosoft ist es so, dass Fitness-Verweigerer in Rechtfertigungsnot geraten, wenn sie sich dem normierenden Druck ihrer Kollegen und der Personalentwicklungsabteilung erwehren. Außerdem winken 500 Euro Jahresbonus für alle, die ihren Body-Mass-Index gegenüber dem Vorjahr um mehr als zwei Prozentpunkte verbessert haben.

Auch die Nicht-Teilnahme derer, die sich insbesondere von ihrem Arbeitgeber nicht vermessen lassen wollen, wird detailliert bemessen und bewertet – zum Aufspüren und Abbauen struktureller Resistenzen. Selbstverständlich wird niemand zur Teilnahme am Gesundheitsprogramm gezwungen, das würde den fortschrittlich-sozialen Ruf des Unternehmens beschädigen. Dafür hat seit letztem Jahr die „Nudging"-Abteilung gesorgt, die der Geschäftsführung direkt unterstellt ist. Sie ist aktuell der brillanteste Coup der Personalentwicklung und versucht mit modernen Methoden der Verhaltensökonomie, die Bereitschaft zur fortwährenden Selbstoptimierung unter den Mitarbeitern zu wecken. „Nudging" ist frei übersetzt so etwas wie „Anstubsen" und ersetzt die alte und mittlerweile wenig populäre direkte Aufforderung oder gar autoritäre (Dienst-)Anweisung. Es regiert sich bedeutend effizienter, seit moderne Herrschaft subtiler lenkt und weniger anordnet. Die indirekt Angestubsten erfüllen die an sie gerichteten Erwartungen nachweislich besser als die Angewiesenen. Gelingt es zum Beispiel in der WhatsApp-Gruppe des „Teams" einer Abteilung, ein Thema subtil zu setzen, darf sich der Angestubste selbst als Ideenträger fühlen und setzt sich häufig mit eigenem Elan für das gewünschte Anliegen ein.

Janine hat einen Fahrrad-Unfall. Blut ist hinter die Kniescheibe gelaufen. Die empfohlene Krankenhaus-Behandlung wird recht teuer. Die ist in ihrem Gesundheitsprogramm nicht vorgesehen – es sei denn, sie willigt ein, in das Premium-Programm zu wechseln. Kopfschüttelnd willigt sie ein.

KI-ANTI-DEPRESSIVA

Einsamkeit erhöht das Krebs- und Herzinfarkt-Risiko. Das fand eine internationale Studie 2020 heraus. In England gibt es schon seit 2018 das weltweit erste Einsamkeits-Ministerium, denn bei einer Quote von fast 20 Prozent wurde Einsamkeit als „Krankheit mit weitgehenden Folgen für die Gesellschaft" eingestuft. Der Studie zufolge seien insbesondere soziale Netzwerke für das drastisch gestiegene Maß an (gefühlter) Isolation verantwortlich. Einsamkeit sei dort besonders ansteckend. So wurde vielen zumeist jugendlichen Patienten eine zeitliche Netz-Selbstbeschränkung nahegelegt. Das erwies sich wegen des hohen Suchtpotentials als wenig wirksam.

Doch es gab noch eine weitere Krankheit, der ab 2020 zunehmende Beachtung geschenkt wurde: In den Talkshows der Nation wurde das Thema Burnout rauf und runter diskutiert. Zu viele Leute glauben oder geben bei leichten Verstimmungen vor, unter Depressionen oder Burnout zu leiden, schreibt die santé generali.

Auf dem Weg zu ihrer Gesundheits-Gruppe im Kreuzberger Bethanien sieht Janine eines der neuen Plakate. Hier macht der Krankenkassenverband Stimmung gegen vermeintliche Hypochonder und die durch sie verursachten „nicht mehr tragbaren Kosten": „Nicht jeder, der sich ausgelaugt fühlt, muss gleich mit Verdacht auf Burnout behandelt werden." Die Bildzeitung bringt eine Serie unter der Headline „Burn-Outing", in der wöchentlich ein besonders dreister Gesundheitskostenverursacher namentlich porträtiert wird. Die einen fanden die Hetze gegen vermeintliche Simulanten widerwärtig. Die anderen gossen begeistert noch mehr Öl ins Feuer und schlugen amtsärztliche Ermittlungsverfahren vor. Die technokratische Lösung des Konflikts sollten KI-basierte Diagnose-und Therapietools bringen. Auch Janine bekam sie von der santé generali „wärmstens ans Herz gelegt".

Janine, an Deiner Stimme, Deinem Tippverhalten und der geringen Fokussierung Deines Blickes erkenne ich, dass Du zu 54 % niedergeschlagen bist.

Janines Gesundheits-App attestierte ihr wegen „einer häufigen Antriebsarmut" eine „seelische Beeinträchtigung". Der könne sie nun früher und wirksamer gegensteuern, bevor sich die vermutete leichte Depression zum gesamtgesellschaftlich teuren Burnout auswächst. Ihr künstlicher Assistent hatte Janine unter anderem darauf hingewiesen, „dass der Erholungswert des geplanten Urlaubs nicht optimal auf Deinen aktuellen Erschöpfungszustand abgestimmt ist".

Begonnen hatte Janine mit den ihr zugewiesenen Meditations-Apps, um „gezielt Stress abzubauen und darüber wieder konzentrierter arbeiten zu können". Damit soll der „User" Depressionen selbst erkennen und sich dann zu mehr Zuversicht verleiten lassen. Janine hat sie alle durchprobiert: *Meditate*, *Pacifica*, *SuperBetter* oder *Calm*. Bei allen war nicht viel mehr dahinter als schlecht abgestimmte Alltagsratschläge vor sphärischen Klängen oder Bachgeplätscher. Von einer selbstlernenden KI, die Janines Gemütszustand auch nur annähernd „verstehen" konnte, war hier so wenig zu verspüren, wie beim wöchentlichen Horoskop ihrer Fernsehzeitung. Und dafür hat sie so viel Zeit und Daten über ihre intimsten Ängste und Sehnsüchte verschleudert.

Dann kam die Aufforderung, ein Stimmungs-Tagebuch zu führen. Janine hatte die „Empfehlung" schon letzte Woche wegen der zu großen Flut von Fragen und Hin-

weisen weggedrückt. Damit ist sie allerdings nicht wirklich weg, sondern lediglich kurzfristig in den See der mittlerweile 1027 ungelesenen Nachrichten verschoben. Sie weiß, dass auf längere Zeit ungelesene Empfehlungen und unbeantwortete Fragen ihren Score senken und ihren Versicherungstarif steigen lassen. Sie nimmt sich immer wieder vor, wenigstens einige der schier endlosen Gesundheits-News abzuarbeiten.

Das Stimmungs-Tagebuch „Mood-Diary" befragt Janine nun täglich, um „Symptome einer Depression monitoren und ihr Wohlbefinden gezielt steigern zu können". Laut Entwicklern handelt es sich um ein interaktives Depressions-Screening, das eine fundierte Einschätzung der psychischen Gesundheit verspricht. Die App benötigt dazu Daten über die Schlafqualität. Zusätzlich fragt sie den Nutzer, ob sich etwas am Appetit verändert hat, ob er sich durchgängig traurig oder scheinbar grundlos schuldig fühlt. Die Auswertung erfolgt in Echtzeit und erlaubt, die Depressivität am „moodmeter", einer Art Depri-Fieberthermometer, zu verfolgen. Die App ist zunächst kostenlos. Will mensch zusätzlich zur Diagnose auch die mentalen Übungen herunterladen, entstehen zusätzliche Kosten bei jeder Übungseinheit. Ebenfalls gegen Aufpreis kann auch ein Gesprächstermin mit einem menschlichen Psychologen gebucht werden.

Janines Unmut über die Absurdität und die wachsende Fremdbestimmung ihres Alltags, die zuweilen in lautstarke Aggressivität umschlägt, bleibt auch dem Stimmungstagebuch nicht verborgen. Und so findet sie sich in einem tautologischen Kreis. Der einzige Ausweg: Ein App-Wechsel. Das offensichtlich für sie weniger geeignete „Mood-Diary" wird durch das Programm „Happify" eingetauscht. Ein angeblich besonders starkes Tool, um Janines „grundlegende Negativität" zu lindern. Nach einem halben Jahr erfolgloser Therapie mit dieser App folgte „Optimist", das der santé generali zufolge eine vortreffliche Erfolgsstatistik vorweisen kann. Auch damit war bei Janine kein Anstieg im Wohlbefindlichkeits-Score zu erzielen. Sie schien für die KI eine besonders harte (schwer zu berechnende) Nuss zu sein – oder sie wolle sich partout nicht auf eine appifizierte Therapie einlassen. Bei letzterem stimmte die Diagnose endlich einmal.

DAS TELEMEDIZIN-UPGRADE

Dann kam das Upgrade. Janine wurde nicht gefragt, lediglich informiert – per Textnachricht. Das kannte sie zwar schon, denn Facebook und andere Plattformen verändern auch alle paar Monate ihre Geschäftsbedingungen und dementsprechend ihre Algorithmen – die Konditionen ihrer Krankenkasse hingegen fühlten sich früher als etwas quasi Unveränderliches an.

Bei zahlreichen Beschwerden wird Janine nun nicht mehr an den Hausarzt oder Fachmediziner, sondern von der KI im Auftrag der Krankenkasse an Telemediziner weitergereicht. Ärzte, die irgendwo in Deutschland sitzen und Zugriff auf die Patientenakte freigeschaltet bekommen.

Mit ganzseitigen Anzeigen werben die Krankenkassen für Verständnis, dass die Kostenexplosion im Gesundheitswesen es schlicht nicht mehr zulasse, jeden Behandlungswunsch erfüllen zu können. Zumindest nicht bei freier Arztwahl und insbesondere nicht bei „leicht heraus zu filternden Lappalien". Gerade hier verspreche man sich mit diesen „Abwimmel-Filtern", wie Janine sie nennt, eine enorme Kostensenkung.

Die Berliner Charité hatte 2018 ein Zentrum für kardiovaskuläre Telemedizin eingerichtet. Wer früher wegen Herzschwäche im Krankenhaus lag, kann nun morgens selbständig zu Hause Blutdruck messen und ein EKG durchführen. Ein Berliner Arzt ruft den Patienten an, falls etwas nicht stimmt. Viele Patienten kommen aus ländlichen Regionen in Brandenburg. Die Telemedizin entwickelte sich zum Lückenfüller für das ländliche Ärzte-Vakuum. Denn seit Jahren waren die durch das Gesundheitssystem geschaffenen Bedingungen für Kassenärzte auf dem Land so schlecht, dass reihenweise Praxen schlossen. Statt hier gegenzusteuern, setzte das Gesundheitsministerium auf die boomende Telemedizin. Die beschleunigt nun das Ärztesterben im ländlichen Gebiet, sodass die Lösung selbstverstärkend das Problem verschärft.

Gesundheitsministerin Meywald geißelt die „ungewöhnlich hohe Ärztedichte in Deutschland als nicht mehr zeitgemäß". „Dänemark, Großbritannien und die Schweiz machen uns vor, wie sich ein gesunder „Volkskörper" mit einem modernen und schlanken Gesundheitssystem formen lässt, das auf mehr Eigenverantwortung setzt. In Deutschland seien die Wartezimmer voll von Leuten, die sich jeden kleinen Schnupfen attestieren lassen. Zudem bremsen die ewig gestrigen Technologiekritiker unter dem Deckmantel des Datenschutzes den längst überfälligen Umbau unseres Gesundheitssystems aus". „Eine datenbasierte Gesundheitsversorgung wird nur dann möglich, wenn eine Nutzung von Daten auch außerhalb des ursprünglichen Zwecks der Datenerhebung erlaubt ist." Das hatten acht große Lobbyverbände der Gesundheitsindustrie 2018 bemängelt und mehr Freizügigkeit bei der Datenverwertung gefordert.

Der neue rechtskonservative Bundeskanzler Spahn bestätigte, dass Deutschland den Anschluss an die USA und China gänzlich zu verlieren drohe, wenn „Fortschrittsverweigerer" der überfälligen Big-Data-Offensive weiterhin Steine in den Weg legten. Das war zwar nicht mehr als die Kopie der alten, viel belächelten FDP-Werbung „Digi-

talisierung first - Bedenken second", aber es wirkte. Die AfD/CDU-Regierung fährt passend dazu eine Kampagne gegen Blaumacher, Minderleister und Arbeitsverweigerer, die unserem Gesundheitssystem auf der Tasche liegen. „Hatten wir doch alles schon", merkt Janine an. 2003 wurde mit Florida-Rolf der Entwurf der Hartz-Gesetze vorbereitet.

Bereits 2018 hatte die Bundesärztekammer den Weg für die Telemedizin geebnet: Sie hatte zwar noch klargestellt, dass Mediziner ihre Patienten grundsätzlich im persönlichen Kontakt behandeln – und dass eine ausschließliche Beratung über Kommunikationsmedien nur „im Einzelfall" erlaubt ist und, wenn die ärztliche Sorgfalt dabei gewahrt bleibt. Zuvor war es Pflicht, dass ein Arzt seinen Patienten mindestens einmal persönlich gesehen haben sollte, ehe ein Kontakt über Telefon und Internet statthaft war. Nach einem Jahr schon wurde aus dem Einzel- der Regelfall:

Bei der Firma Medgate z. B. rufen mittlerweile bis zu 135.000 Menschen täglich an. 270 Ärzte sind dort beschäftigt – rund um die Uhr. Die Online-Sprech-Minuten enden mit einem Rezept an der Online- (bzw. für ewig gestrige an der benachbarten) Apotheke oder mit einer Vermittlung an einen Facharzt. In mehr als der Hälfte der Fälle sei aber gar keine weitere Behandlung nötig, so die Statistik-Präsentation beim letzten Quartalsbericht.

Es bildeten sich neue Gesundheits-Startups unter der Anleitung von Amazon, Google, Facebook und Apple aus. Das Muster hatte sich kaum verändert – Startups blieben solange solche, bis sie als sogenannte Unicorns so erfolgreich wurden, dass die großen Player aus China und dem Silicon Valley sie aufkauften. Amazon ist so 2020 in Europa in den Gesundheitsmarkt eingestiegen und hat selbstbewusst eine Kooperation mit deutschen Krankenkassen abgelehnt. Die hatten darum gebuhlt, aber Jeff Bezos hat es gereicht, ein paar führende „brains" der Branche abzuwerben. Man bringe selbst genügend Know-How mit und sei auf die bald aussterbenden Dinosaurier auf dem Gesundheitsmarkt nicht mehr angewiesen, so sein Statement bei der Eröffnung des neuen Health-Departments in Brüssel. Die lediglich 2500 Gegendemonstranten draußen vor dem neuen Büroturmkomplex in H-Form hatte er gleich als „bedeutungslos" verspottet. „Sie sind so überflüssig und Teil des alten Europas – die neue Welt braucht sie nicht nur nicht – sie funktioniert besser ohne sie". Es war unklar, ob er die Demonstranten oder die klassischen Krankenversicherungen meinte.

FEMTECH

Janine gehen die permanenten Aufforderungen, sich immer detaillierter „erforschen zu dürfen", um sich (noch) mehr mit sich selbst zu beschäftigen, mittlerweile gehörig auf die Nerven. Nichts in ihrem Leben scheint mehr ohne programmierte Hilfestellung auszukommen. Lehnt sie die zahlreichen freundlichen Helfer-Programme ab, meldet sich prompt irgendeine App, die ihr „hilft", sich nicht so gehen zu lassen. Keine Nische mehr in ihrem Alltag, die nicht vom KI-Hype erfasst wird. Das Versprechen, ihr Leben werde so „lebenswerter", klingt eindeutig wie eine Drohung – genau wie die Werbe-Mails verschiedener Firmen aus der sogenannten „Femtech-Branche" – das sind Startups, die sich „ganz allein den Gesundheitsbedürfnissen und den Lifestyle-Wünschen der Frau verpflichtet fühlen".

Hallo Janine, unsere neue Zyklus-Tracking-App Clue erlaubt Dir, Deine Stimmungen und Hormonschwankungen direkt mit Deinen Freundinnen zu teilen. Abhängig von der Vielfalt der Daten, die Du unserem selbstlernenden Verhütungskalkulator zur Verfügung stellst, kann Clue sicherer sein als die Pille. Willst Du schwanger werden, stellt Dir unser Conceive-Prediction-Timer einen Kalender der Tage zusammen, an denen Du die größte Chance hast. Wenn Du magst, kannst Du Deine engsten Freundinnen automatisch teilhaben lassen.

„Du darfst froh sein, wenn es auf dem Niveau bleibt", schreibt Janines Freundin Ulla im Chat mit ihr.

Ulla arbeitet in Walldorf beim größten deutschen Software-Hersteller SAPi, und der „unterstützt" seine Mitarbeiterinnen mittlerweile bei der Familienplanung. Die erste Mitarbeiterinnenbesprechung, die sich ausschließlich an die weibliche Belegschaft wandte, war im zentralen Firmen-Auditorium schlicht mit dem Titel „Prelude Fertility" angekündigt. Den meisten männlichen Kollegen war gar nicht klar, dass es sich dabei nicht um die Präsentation eines neuen Software-Produkts von SAPi handelte, sondern um die zweistündige Einführung in das, was in den USA „social freezing" genannt wird.

Der Chef der Firma *Prelude Fertility*, Martin Varsavsky, war persönlich nach Deutschland gekommen. Immerhin ist SAPi auf dem deutschen Arbeitsmarkt ein Trendsetter – vergleichbar mit Apple und Facebook in den USA, wenn auch einige Nummern kleiner. Die beiden raten ihren Mitarbeiterinnen bereits seit 2014, Eizellen auf Firmenkosten einfrieren zu lassen, „um die Babypause und den damit oftmals verbundenen Karriereknick möglichst weit nach hinten zu schieben." Ein „Angebot", das durchaus im Interesse des Arbeitgebers liegt, und nun bei SAPi auch als solches unmissverständlich unterbreitet wird:

„Was wir bei Prelude Fertility bieten, gibt es nirgendwo sonst aus einer Hand: Junge Frauen mit Mitte zwanzig frieren ihre Eizellen bei uns ein; sie lassen sie Jahre später befruchten, wenn sie so weit sind; es entstehen Embryos, die wir auf genetische Krankheiten testen – und dann set-

zen wir einen Embryo ein. Ich bin überzeugt: Frauen, die das machen, haben viel höhere Chancen, später im Leben gesunde Kinder zu bekommen. Als wirklich neu darf ich verkünden, dass wir für Sie nun ein Abo-Modell eingeführt haben: Eine Patientin bekommt nun alle Leistungen für 199 Euro im Monat – vom Einfrieren der Eizellen über die künstliche Befruchtung bis zum Einsetzen des Embryos. Und ich darf Ihnen ebenso freudig mitteilen, dass für Sie, liebe SAPi-Mitarbeiterinnen, das Abo gratis ist. Ihr Arbeitgeber hat sich bereit erklärt, diese Kosten für Sie zu übernehmen."

Ulla schreibt, „Der schmierige Typ sprach wie bei einer Verkaufspräsentation eines Autopolitursets vor einem Einkaufszentrum. Die eigentliche Frechheit war allerdings, dass nicht etwa Listen für Interessierte durch die Reihen der Zuhörerinnen gereicht wurden, sondern nun nahtlos kleine Gruppen gebildet wurden, in denen die Details des Firmen-geförderten Programms und etwaige Nachfragen diskutiert wurden. Kein Entrinnen. Ich musste mich regelrecht erklären, warum ich den Nachfolgetermin der Kleingruppen nicht wahrnehmen möchte."

PERSONALISIERTE GENTHERAPIE

Hallo Janine – bist Du bereit, an einer gentechnischen Analyse Deines Suchtpotentials und einer etwaigen Gentherapie teilzunehmen? So lassen sich für die Gesellschaft und insbesondere für Dich erhebliche Gesundheitskosten einsparen.

Willst Du kostengünstig von unserer reichhaltigen Lifestyle-Medizinischen Produktpalette profitieren und als Community-Mitglied zu deren Verbesserung beitragen? Hier einige Angebote unserer Programmpartner:

Vinome – *sucht für Kunden Weine auf Grundlage ihrer DNA aus.*

SkinGenie – *liefert personalisierte Empfehlungen für Hautpflege-Produkte auf der Grundlage eines Lebensstil-Quiz und einer DNA-Analyse. Nach Angaben des Unternehmens kann auf die DNA-Analyse auch verzichtet werden, aber sie soll eine „genauere Einschätzung" ermöglichen. Die Hautpflege-Einschätzung kostet 59 Euro, hinzu kommt der Kauf eines DNA-Testkits von LifeNome oder das Hochladen der eigenen DNA-Rohdaten von 23andMe, Ancestry.com oder anderen Anbietern.*

Nutria – *Lean Cuisine, ein bekannter Anbieter von Tiefkühlkost, bietet Dir einen neuen Dienst für das Planen von Mahlzeiten. Genetische Marker tragen dazu bei, Deine individuelle Nährstoff-Aufnahme festzulegen. Neben der DNA wird eine Befragung über Lebensmittel-Präferenzen, Allergien und den Lebensstil ausgewertet. 79 Euro für acht Wochen (in der Testphase) kostet das Programm mit Empfehlungen für Rezepte, Restaurants und Fertiggerichte. Für weitere 29 Euro kannst Du das Modul zur erfolgreichen Gewichtsabnahme dazu buchen.*

Youngblood – *Die Firma bietet nach einer DNA-Analyse einen individuell zugeschnittenen Verjüngungscocktail aus Blutbestandteilen von maximal 25-jährigen Spendern. Die Risiken und vor allem die Kosten des „unkorrigierten" Alterns sind der Gesellschaft nicht mehr zuzumuten. Per Bio-Hacking kannst Du Deinen Stoffwechsel neu definieren und so erfolgreich deine körperlichen Alterungsprozesse verlangsamen.*

SpareRoom – *Das Unternehmen bietet eine mobile App an, die Dir dabei helfen soll, den richtigen Mitbewohner zu finden. Dazu werden eine DNA-Probe und ein Online-Persönlichkeitstest ausgewertet.*

Nach dieser überzeugenden Darbietung schaltet Janine ab. Warum werden diese Dienste als DNA-Analysen vermarktet, obwohl die DNA nicht einmal ansatzweise sinnvoll für die personalisierten Empfehlungen genutzt werden kann? Neue Gebiete der Wissenschaft werden als Marketing-Instrument genutzt. Eine ähnliche Mode hatte es auch in der Hochzeit der Stammzellen-Forschung gegeben: Kosmetik-Unternehmen begannen, alle möglichen „regenerativen" Hauptpflege-Produkte anzubieten, die angebliche Stammzellen enthielten. Viele der Unternehmen wollen allerdings nicht nur Geld mit ihren unnötigen DNA-Lifestyle-Angeboten machen, sondern verfolgen eher längerfristige Ziele: Wenn sie genügend Daten von Verbrauchern gesammelt haben, können sie diese an Forscher verkaufen. Damit ist deutlich mehr Geld zu verdienen.

All diese vorgeblich trendigen Apps konnten bei Janine nicht verfangen. Zugegeben, es war nicht gerade schwer, ihnen zu widerstehen. Aber die Vorschläge der kommenden Monate verunsicherten Janine tatsächlich. Sie waren ähnlich befremdlich, aber vor allem Besorgnis erregend. Fast schien es, als würde die detaillierte Körperanalyse der immer wissbegierigeren App Janine kränker „schreiben", als sie je vermutet hatte.

Die Gesundheits-App habe bei ihr eine Disposition für „potenzielle Hautveränderungen" festgestellt. Des Weiteren gäbe es mit der damit dringend angeratenen „erweiterten Genanalyse" die Möglichkeit, auf insgesamt 7000 seltene genetische Krankheiten zu testen. In Kombination mit dem Einsatz der künstlich intelligenten Gesichtserkennungssoftware Face2Gene der Firma FDNA könne Janine auf eine hohe Erkennungsquote setzen. Next Generation Phenotyping nennt sich die Methode: Über kleinste Veränderungen der Gesichtszüge und eine DNA-Analyse lassen sich genetische Defekte frühzeitig erkennen. „Seien Sie unbesorgt. Unserem digitalen Assistenten entgeht dabei weniger als unseren erfahrensten Radiologen."

Die Visionäre der Forschungsabteilung Google X hatten es schon 2018 vorausgesehen: Die Medizin werde sich grundlegend verändern – weg von einer Symptom-basierten Behandlung hin zu einer präventiven, personalisierten Medizin, mit Therapien, die auf der Analyse des Erbguts beruhen. Der Arzt werde zum umfassenden „Gesundheitscoach" und „Datenmanager", der zusammen mit KI-Assistenten Dispositionen, also Wahrscheinlichkeiten für den Ausbruch verschiedener Krankheiten, berechnet. Per Gentherapie sollen derartige genetische Defekte eliminiert werden.

„Wir können sämtliche Krankheiten und das Hungern überwinden – aber dazu müssen wir jegliche Form von nicht sachgerechtem Verhalten abwenden". „Detecting and correcting potential errors in user behaviour" nannte Google die von ihnen anvisierte Verhaltenslenkungsmaschinerie in einem (eigentlich) internen Firmenvideo. Eine klare Ansage: Ihr bekommt den Fortschritt eines nach unserer Weltsicht „gesunden Lebens" unter der Prämisse einer „massenhaften Verhaltens-Modifikation". Eine zutiefst totalitäre Idee, die an den Behaviourismus des letzten Jahrhunderts anknüpft, und von der die meisten lange glaubten, dass sie sich in einer modernen, selbstbestimmten Gesellschaft niemals durchsetzen könne.

„So weit weg ist diese Zukunftsvision gar nicht", trägt Janine auf einer Veranstaltung zum Umbau des Gesundheitssystem vor. Sie ist mittlerweile im Berliner Netzwerk „Save Solidarity" organisiert.

„Mein neuer Versicherungstarif passt sich kontinuierlich meiner individuellen Krankheitswahrscheinlichkeit an. Ich bin permanent in der Pflicht, zu beweisen, dass ich ausreichend an meiner Gesundheit arbeite. Tu ich das nicht, folgt die Konsequenz quasi in Echtzeit – in Form einer unmittelbaren Tarifanpassung. Nicht nur die Abkehr vom Solidarprinzip, auch die Beweislastumkehr ist hier bereits implementiert: Ich als Versicherte in diesem neuen Programm muss täglich beweisen, dass ich keine Mitschuld an einer eventuell eintretenden Erkrankung trage. Die Bewertung meiner Bemühungen wird dabei nicht von einer unabhängigen Institution durchgeführt, sondern vom Versicherungs-Unternehmen selbst – nach Kriterien, die nicht einsichtig sind, da sie in der sogenannten Health-Improvement-KI versteckt sind".

HUNDERTTAUSENDFACHER EXIT

Janine hat erneut mies geschlafen – sagt ihre Schlaf-App. Heute braucht sie dazu keine App, denn es fühlt sich exakt so an. Beim Kaffee wischt sie durch ihre Nachrichten. Mal wieder sind viele Nachrichten von ihrer geschwätzigen Krankenkassen-App dabei. „Anhaltender Kostendruck im Gesundheitssektor" lautet die Erste: Der fortwährende Kostendruck und Amazons Einstieg in den europäischen Krankenversicherungsmarkt im November 2020 „zwinge die santé generali, sich im Geschäft der intensivierten Datenauswertung besser aufzustellen". Für Janine und Hunderttausende andere bedeute das, sie könnten nicht mehr wählen, ob und wieviele Daten sie über sich preisgeben wollen. Na super – irgendwie hat Janine diese finale Windung der Spirale in Richtung autoritäre Bevormundung erahnt. Dass es nun so schnell kommt, überrascht sie dennoch.

Aus den Handlungsempfehlungen werden nun Handlungsanweisungen – und das im intimsten Bereich ihres Lebens. Lange schien es so, als passten sich die immer raffinierteren Mess- und Bewertungsmethoden der KI-Gesundheits-Algorithmen samt ihrer ausgefeilten Hardware-Gadgets den individuellen Vorlieben und Bedürfnissen der Menschen an. Jetzt markiert Janines Krankenkasse erstmalig ganz offen den Punkt, wo sich dieses Verhältnis umkehren soll. Erstmalig gibt es die ernst gemeinte „Option", aus der Gesundheitsversorgung herauszufliegen: Wer sich verweigert oder den KI-basierten Gesundheits-"Empfehlungen" mehrfach nicht nachkommt, erhält nach vorherigen „Punktabzügen" nur noch eine erste Notfall-Hilfe, aber keine weiter gehende ärztliche Versorgung. So die unmissverständliche Botschaft ihrer WhatsApp-Nachricht. „Die verschicken so einen Hammer, als wäre es eine unbedeutende Änderung in den AGBs, der sowieso niemand seine Aufmerksamkeit schenkt.", empört sich Janine.

Tatsächlich geht die Ankündigung diverser nun folgender Krankenkassen medial durch die Decke. Der angedrohte „Kick-out" aus der Gesundheitsversorgung sei eine Bankrotterklärung für das reichste europäische Land, sagen die einen. Eine längst überfällige Anpassung an die reale Macht der Konkurrenz aus den USA und China, den Gesundheitsmarkt neu zu definieren, sagen die anderen. „Wer an diesem Markt auch 2021 noch bestehen wolle, müsse die Erfassung, Bewertung und Prognose der Gesundheitsdaten zu seinem Kerngeschäft machen – das sei absolut alternativlos", so der Deutschland-Chef der santé generali.

Es folgen große Demonstrationen. Die von letzter Woche Samstag in Berlin erinnerte Janine an die fetten Demos gegen die Verabschiedung der Hartz-Gesetze 2004 und die Unteilbar-Demo gegen rassistische Ausgrenzung 2018.

In Berlin und Hamburg poppen in den folgenden Monaten gleich vier selbstorganisierte Medikamente-Vergabestellen aus dem „Nichts" auf. Wer genauer hinschaut, bemerkt ein erstaunlich gut organisiertes Zusammenspiel unentgeltlich arbeitender Ärzte und Medikamentensammelstellen. Tatsächlich greifen diese „neuen" Alternativstrukturen auf eine gewisse Erfahrung zurück - denn ei-

nige der hier arbeitenden Ärzte haben sich bereits in der Gesundheitshilfe für Geflüchtete engagiert. Hier haben die Krankenkassen ihren gesellschaftlichen Auftrag schon seit über 20 Jahren verweigert. Jetzt droht eine Art Tafelsystem der Apotheken die Standards im Gesundheitssystem für einen deutlich größeren Teil der Bevölkerung zu senken: Der gesicherte Anspruch auf Gesundheitsversorgung weicht der Möglichkeit auf eine Gefälligkeitsleistung.

Janine war auf einer Veranstaltung im SO36 in Kreuzberg – nicht weit von ihrem ehemaligen Wohnort. Den musste sie schon 2018 verlassen. Die Mieten stiegen ins Unermessliche, obwohl die „Scheiß-Techi-Hipster von Google", wie Janine sie nennt, noch gar nicht da waren. Es reichte schon die Ankündigung der Eröffnung des neuen Google-Campus in der damals angesagtesten Großstadt Europas, um die Mieten in die Höhe schnellen zu lassen. Janine musste raus – ihre alte Miete war nicht mehr zeitgemäß. Der angebliche Eigenbedarf ihres Vermieters hatte sich zwar in Luft aufgelöst, aber raus ist raus. Statt 580 Euro verlangt der Eigentümer nun 960,- ohne jede Sanierung. Nicht mal renoviert hatte er; es gab prompt über zweihundert neue Bewerber. Drei Monate später hatte Janine es sich nicht nehmen lassen, den Nachmieter zu fragen, ob sie mal rein kommen darf. Immerhin konnte sie etwas Entschädigung erstreiten, da der Eigenbedarf ihres damaligen Vermieters offensichtlich nur vorgetäuscht war.

Aber zurück zur Veranstaltung. Leute aus Athen und Thessaloniki haben sich angekündigt und der Saal war bis auf den letzten Stehplatz gefüllt. Es ging um die Erfahrungen, die verschiedene Medizin-Kollektive seit der Krise 2008 gemacht hatten. Damals brach für mehr und mehr Leute die Versorgung mit dem Nötigsten zusammen - darunter auch die Gesundheitsversorgung. Die eine Referentin, eine Allgemeinmedizinerin aus Veria (rund 40 Kilometer westlich von Thessaloniki), erzählte, dass damals das Sammeln von Medikamenten wegen der breiten Solidarität erstaunlich gut klappte, aber medizinische Geräte absolute Mangelware waren. Sie nutze oft die Geräte befreundeter Praxen in den Abendstunden – gegen ein kleines Entgelt. Das wiederum beglich sie mehr schlecht als recht mit gesammelten Spenden.

Janine war überrascht, ihre alte Hausärztin auf der Veranstaltung zu treffen. Sie tranken noch in kleinerer Runde ein Bier nach der langen Debatte im SO36.

Warum hast Du damals eigentlich aufgehört? Die Praxis lief doch gut?

Ich hatte wirklich keine Lust, Tele-Ärztin zu spielen. Am Anfang war es nur die santé generali, aber dann sind immer mehr Krankenkassen umgestiegen auf das Vorabfiltern per Ferndiagnose. „Prevaluation" nennen sie das. Nur noch einige wenige Private erlaubten ihren Kunden einen direkten Besuch bei mir – ganz ohne App oder Vorab-Tele-Sitzung. Große Scheiße, das Ganze. Jetzt kriegen die meisten nicht mal mehr eine Tele-Sitzung. Die App der BAK zum Beispiel entscheidet, ob Du überhaupt zum Callcenter-Arzt vorgelassen wirst. Und das macht kein echter Kollege mehr, das machen jetzt die Künstlichen – die Apps.

Ich weiß – sagt Janine. Ich steck auch grad drin in so nem dämlichen Assistenz-Programm. Ich komm aber auch gar nicht mehr raus. Mich nimmt keine andere mehr und den freien Arztzugang bei der santé generali, also ohne vorgeschaltete App, kann ich mir nicht leisten.

Was denkst Du über die Idee mit dem Gesundheitsladen und der Soli-Praxis im Mehringhof? Meinst Du, das klappt? Klingt irgendwie ganz schön vermessen, das jetzt selbst in die Hand zu nehmen, oder?

Mehr als scheitern können wir nicht – und beschissener als jetzt kann es kaum werden. Schon 350.000 Leute sind raus aus jeder Versorgung. Einige sind sogar raus aus der Notfall-Hilfe – nur, weil sie sich von dieser Healthcare-App ihr Leben nicht vorschreiben lassen wollen. Also ich bin dabei – allerdings mehr als 20 Stunden die Woche schaffe ich gerade nicht. Ich mache noch diese Fortbildung und zwischendurch muss ich auch noch Geld verdienen.

Was machst'n – jetzt, wo Du die reguläre Praxis geschmissen hast?

Ich fahr für Amazon Medikamente aus.

Ach nee – und das machst Du? Die haben den Mist mit der KI und diesem ganzen Bewertungsscheiß in der Gesundheit doch erst hoffähig gemacht. Amazon Healthcare, Amazon Pharma und Amazon Medicals – alles unter einem Dach. Kein Entrinnen für alle, die Amazon jahrelang ihre Gewohnheiten und Wünsche offen gelegt haben.

Na ja, sagen wir so – ich machs nicht aus Leidenschaft, eher aus Überzeugung. In den Achtzigern haben die Leute so was „militante Untersuchung" genannt. Kann auf jeden Fall nicht schaden, den Feind genauer zu kennen und sich von drinnen einzumischen. Und es gibt immer wieder Sachen, die vom Laster fallen – wenn Du weißt, was ich meine. Das brauchen wir dringend für die Umsonst-Apotheke hier im Kiez.

Und wie siehts bei Amazon aus? Gibts Widerspruch von innen? Kriegst Du was mit?

Es tut sich was in der Belegschaft. Früher haben die Mitarbeiter ausschließlich für bessere Arbeitsbedingungen gestreikt, sich teilweise sogar mit dem Konzern-Image als erfolgreicher Game-Changer identifiziert. Das ist jetzt anders – keiner spricht mehr positiv von Disruption oder ähnlichem Quatsch. Heute geht die Kritik an Amazons Gesundheitsgeschäft mit den Protesten gegen die krank machenden Arbeitsbedingungen zusammen. Immerhin ist die Healthcare-Sparte mit Pharma-Produktion, Online-Apotheke und Krankenversicherung mittlerweile das zweitgrößte Geschäft für Amazon; nach den Web-Services. Der Online-Handel ist dagegen fast schon unbedeutend. Der dient nur noch als Daten-Beschaffer. Der klassische Versandhandel läuft jetzt hauptsächlich über die neue Plattform aus China. Amazon hat das fast komplett abgegeben – den Zugriff auf die persönlichen Daten haben sie sich allerdings gesichert. Das ist quasi die Basis für alle ihre persönlichen Assistenten.

Auch die militante Linke beschäftigt sich nun mit dem Thema. Ein Anschlag auf die zentrale Netzverbindung des europäischen Amazon-Datenzentrums in Dublin legte letzte Woche sämtliche Healthcare-Dienste des größten Players im Gesundheitsgeschäft für vier Tage lahm. Die europäischen Datenschutzbestimmungen hatten Amazon genötigt, Daten ausschließlich innerhalb Europas zu speichern und zu verarbeiten. Das wurde ihnen nun zum Verhängnis: Eine Kopie in den USA gibt es nicht – oder wird von Amazon nicht eingespielt, um die minimalen Zugeständnisse an die europäische Datensicherheit nicht auch noch zu verspielen.

Der bislang ungeklärte Serverausfall bescherte den Leuten nur eine kleine Auszeit von der permanenten Verhaltenslenkung: keine Chance, Bonuspunkte zu sammeln, aber eben auch keine Strafpunkte. Vor allem vermittelte die Auszeit aber eines: Eine Erinnerung an Zeiten, in denen es üblich war, jenseits der Arbeit unbeobachtet und unbewertet selber zu entscheiden, wie wir leben wollen.

Abschließende Anmerkung: Die Geschichte ist fiktiv, die erwähnten Apps und skizzierten Forschungsentwicklungen sind real. Sie firmieren großenteils unter anderem Namen und teils außerhalb Europas.

Strategien im Widerstand

Nun ist es nicht so, dass wir unsere Zeit nur mit Analysen verbringen. Als Aktivist*innen sind wir immer auf der Suche nach möglichen Widerstandsstrategien gegen den technologischen Angriff.

In den letzten Heften haben wir Beispiele verschiedener Ideen gebender Arten von Widerstand dokumentiert. Auch diesmal haben wir verschiedene Leuchtfeuer gesammelt, die wir euch nicht vorenthalten wollen. Aber wir wollen auch unsere Ideen zur Strategiedebatte mit euch teilen.

Wenn wir im Folgenden von WIR reden, meint das nicht nur uns als capulcu, sondern auch euch. Das grundsätzlich Problematische daran: ein WIR macht immer auch ein DIE. Gibt es klare Grenzen zwischen UNS und DENEN? Es ist wichtig und hilfreich, eine gesellschaftliche Gruppe zu haben, in der man nicht immer alles erklären muss, gemeinsame Grundsätze und Werte teilt. Es ist aber genauso wichtig, immer wieder dieses WIR zu hinterfragen. Nicht im Sinne von Spaltung, sondern im Sinne von Lernen und Lust an der Auseinandersetzung. Nicht umsonst heißt es bei den Zapatistas: „*Fragend schreiten wir voran*“. Aus Fragen entstehen Konflikte, Auseinandersetzungen und Reibungspunkte, aber eben auch Antworten. Und dies betrifft nicht nur das WIR. Auch mit DENEN sollten wir in die Auseinandersetzung gehen und lernen, dass die trennenden Linien zwischen UNS und IHNEN oft unscharf sind. Wer jetzt denkt, wir streben ein klärendes Gespräch mit dem Chef von Amazon an, der irrt. Aber der gemeinsame Kampf mit den Arbeiter*innen in den Logistikcentern öffnet Räume der Auseinandersetzung und des Lernens voneinander. Also Allianzen eingehen, ohne unsere eigenen Ideen und Vorstellungen aus dem Blick zu verlieren. Ein weiterer Effekt: wenn wir unsere Ideen, Utopien und Aktionsformen zur Diskussion stellen und bereit sind, diese so zu erklären, dass nicht nur wir sie verstehen, erhöhen wir die gesellschaftliche Akzeptanz für direkten Widerstand. Selbstverständlich gibt es für einzelne Aktive gute Gründe, diese offene Auseinandersetzung zu meiden – es müssen ja auch gar nicht *alle* machen.

Die technologische Entwicklung rast voran, das heißt, dass sich ihre Herrschaft rasant verfestigt. Aber: die Systeme werden auch komplexer und (wegen der hohen Entwicklungsgeschwindigkeit) offensichtlich unausgegorener. Und das heißt fragiler, angreifbarer. Wir haben das Gefühl, unser Widerstand nimmt oft nur DIE (Taktgeber der neuen Technologien) als Referenz. Wir denken, es

könnte eine Chance sein, unsere Bezugspunkte für Analyse, Kritik und Widerstand zu erweitern:

Müssen wir uns an dieser Geschwindigkeit orientieren, auf die wir zudem nur beschränkt Einfluss haben? Ja und Nein. *Ja*, weil wir jede Gelegenheit nutzen sollten, diese Entwicklung aus dem Tritt zu bringen, zu verlangsamen und neu zu orientieren, denn wer weiß, wie lange wir noch die Möglichkeiten haben. *Nein*, nicht um jeden Preis. Es ist wichtig, sich die Frage zu stellen, wie wir uns organisieren wollen, wie wir lernen wollen und wie wir Widerstand leisten wollen. Entspricht das unseren Utopien? Verlieren wir Weggefährt*innen, weil sie ausgebrannt und überlastet sind? Auch hier haben wir weniger Antworten, sondern eher Fragen, die wir gemeinsam mit unseren Gefährt*innen beantworten sollten.

Viele unserer Analysen und Debatten beziehen sich auf die westlichen Metropolen.

Die mit dem technologischen Angriff verbundene Steigerung der Produktivität in den Metropolen führt zu einer enormen Entwertung von Arbeit und Lebensformen in den Peripherien, die vielfältigen Widerstand mit sich bringen (werden). Auch auf ihn sollten wir uns in unserem Widerstand beziehen. Auf dem Land und auch in anderen Kontinenten stehen die technologischen Entwicklungen an anderen Punkten. Gibt es dort Möglichkeiten, in Entwicklungen einzugreifen, die sich hier nicht (mehr) bieten? Wir berichten in unseren Heften von Protestbewegungen im globalen Süden. Die technokratischen Player suchen dort nicht nur Absatzmärkte, sondern dehnen ihren lenkenden Einfluss auf den globalen Süden aus – so z. B. Facebooks Netz der Bevormundung „free basics". Die Rohstoffe für den technologischen Angriff kommen nicht aus Europa oder den USA. Der koloniale Abbau von seltenen Erden hat dramatische Auswirkungen auf viele Länder in Afrika. Unsere Analyse muss diese Bedingungen und Auseinandersetzungen berücksichtigen, um gemeinsame Kämpfe zwischen den unterschiedlich Betroffen herzustellen.

Nicht nur viele der Protagonist*innen aus dem Silicon Valley, auch viele unserer Mitstreiter*innen, die sich „hackend" gegen den technologischen Angriff zur Wehr setzen, sind männlich und weiß. Uns fehlen dadurch Blickwinkel, Fragen und Analysen, um weiter zu kommen. Wir versuchen, eine anti-patriarchale Position gegen die Technologiegläubigkeit so stark wie möglich zu machen – leider ist diese Position bislang noch längst nicht so stark wie nötig.

Wir sind nach Veröffentlichung unseres letzten Heftes „Disrupt!" oft nach möglichen „reformistischen Perspektiven" befragt worden. Wir haben hierzu eine klare Meinung:

Die Vergesellschaftung von Software-Plattformen, ja selbst von digitaler Infrastruktur, wird nicht ausreichen. Wir benötigen eine klare Zurückweisung der „Sozialen Kybernetik" und der ihr innewohnenden Ideologie des Zwangs zur Selbstoptimierung. Menschen sind keine Parameter in Computersystemen und das Lösen von sozialen Problemen funktioniert nicht über Technologie-dominierte Ansätze. Im Gegenteil: Letztere sind vielfach der Kern sozialer Isolation und Entsolidarisierung. Genau das ist unsere Motivation, den Kampf gegen den vermeintlich übermächtigen technologischen Angriff aufzunehmen: Wir leben im Widerstand, wir finden unsere sozialen Beziehungen im gemeinsamen Kampf. Wir brauchen die analoge (reale) Welt und eine tiefer gehende gemeinsame Auseinandersetzung, um unsere Beziehungen (die auch online entstehen können) zu festigen und zu vertiefen. Außergewöhnliche Situationen schaffen außergewöhnliche Bindungen.

FÜNF WIDERSTANDS-STRÄNGE VERKNÜPFEN

Wir sehen, ohne Anspruch auf Vollständigkeit, fünf mögliche Strategiestränge. Für uns steht außer Frage, dass wir für einen Erfolg versprechenden Weg hin zu einer befreiten Gesellschaft diese Stränge miteinander verknüpfen und zudem aushalten sollten, dass unterschiedliche Strömungen in unseren Bewegungen unterschiedliche Prioritäten setzen. Wir sehen nicht „den besten" Widerstandspfad, welcher uns am weitesten bringt. Wie auch? Unserer Meinung nach gelingt das Entwickeln von Strategien nur gemeinsam im aktiven Prozess des Rebellierens.

Kollektives Lernen

Wir müssen die uns zugewiesene Rolle der Nutzer*in durchbrechen. Wir wollen mehr: mitbestimmen und mitentwickeln. Dazu müssen wir lernen. Nicht allein, sondern kollektiv. Nicht alle müssen wissen, wie ein Mailserver administriert wird, effektive Verschlüsselungs-Werkzeuge weiterentwickelt werden oder ein hippes Widerstands-Video gemacht wird.

Nicht alle – aber mehr als jetzt! Wir brauchen Allianzen des Lernens. Wen können wir fragen? Wer ist bereit, dies oder jenes zu lernen, um es anderen weiter zu vermitteln? Wir brauchen ein rudimentäres Verständnis verschiedener Techniken, auch um diese zu sabotieren und zu „hacken". Die Kaffeekanne im Büro ist ein gutes Beispiel. Kippen wir sie über die Tastatur, ist das Sabotage. Nicht jede*r muss lernen, was dann im Inneren der Tastatur passiert, aber das Wissen, dass dies eine Möglichkeit der Sabotage ist, ist wichtig für uns alle.

Für ein kollektives Lernen brauchen wir solidarische Organisierung. Wir wollen lernen, Bedürfnisse ernst zu nehmen. Wir wollen uns aber auch trauen, sie in Frage

zu stellen. Wo sind Bedürfnisse künstlich kreiert durch technologische Entwicklungen, die uns eher ketten als befähigen? Wo sind es vielleicht keine Bedürfnisse, sondern Interessen? Zudem müssen wir Lernen und Erklären wollen. Dazu braucht es Lust und Fähigkeiten.

Hacking und Sabotage

Hacking und Sabotage sind Selbstermächtigung und Handlungsfähigkeit gegen den technologischen Angriff. Hacking und Sabotage erzeugen Brüche und Risse einer allgegenwärtigen Konnektivität, in denen wir agieren können. Wir schaffen damit Lücken, geben uns und anderen die Möglichkeit, ins Gespräch zu kommen, zu lernen und auszubrechen. Aber wir brauchen dafür auch den Willen zur Auseinandersetzung. Wenn wir in der U-Bahn mit einem GSM-Jammer die Handyverbindung kappen, dann haben wir wenig erreicht, wenn alle lediglich ihre Bücher und Ebook-Reader raus holen. Wir sollten eine dann mögliche Auseinandersetzung initiieren oder mitgestalten.

Für uns umfassen Sabotage und Hacken nicht nur das Außer-Betrieb-Setzen von Geräten, sondern auch ihr Umfunktionieren. Statt einfach auszufallen, können gehackte Navigationsapps auch Fake-Staus kreieren. Genauso wie die Arbeiter*innen in den Fabriken lernen mussten, an welcher Stelle der Schraubenschlüssel ein effektives Mittel der Sabotage sein kein, müssen wir auch unsere digitalen Schraubenzieher finden und lernen, sie zu platzieren. Das kann bedeuten: Wir verwenden Technik, um den technologischen Angriff aufzuhalten. Für uns kein Widerspruch.

Alternativen

Wir brauchen Alternativen. Wir müssen akzeptieren und verstehen, warum so viele Menschen spezifische Technologien nutzen (wollen). Nur so können wir analoge UND digitale (ja, wir wollen nicht zurück in die Steinzeit) Alternativen aufbauen, die eine Wirkmächtigkeit gegen Lenkung, Entmündigung und Entfähigung entfalten. Für uns sind alternative Infrastruktur, Tools und digitale Selbstverteidigung Teile unseres Widerstands. Aber Alternativen sind nicht rein technischer Natur. Wie verändert der Digitalismus unsere Beziehungen und Kommunikation, unsere Verbindlichkeit und Verlässlichkeit? Wie können wir dem auch ganz analog begegnen?

Solidarität

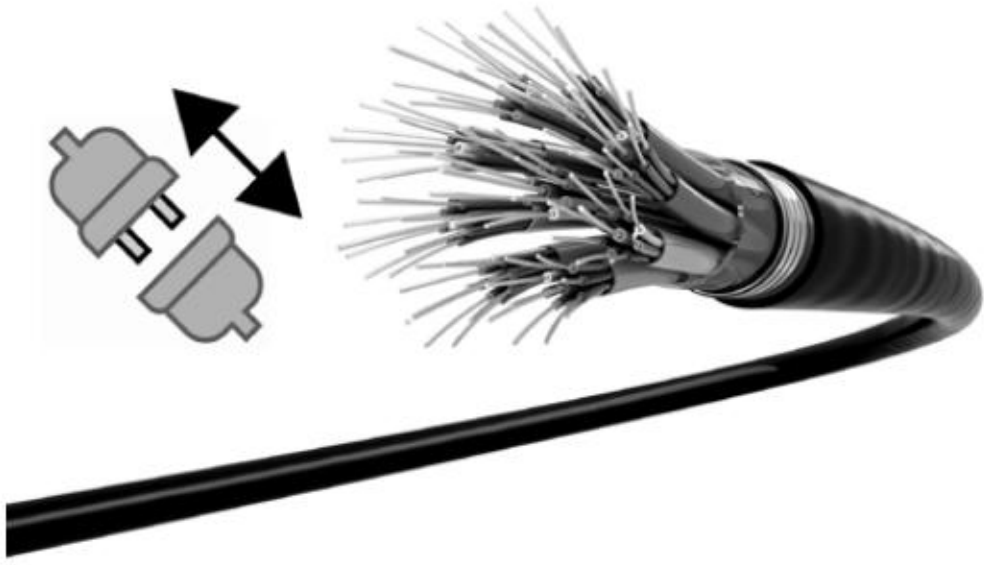
Technologie individualisiert Menschen und versucht, unsere Solidarität zu unterwandern. Sie zerstört die – insbesondere für den Widerstand so grundlegenden – Fähigkeiten zur Gemeinschaftlichkeit. Solidarisches Handeln ist deswegen ein essentieller Baustein unseres Widerstandes. Der kybernetische Kapitalismus zerrt uns in entgegengesetzte Richtung: Individualismus – Leistungsoptimierung – Profit. Sozialer Widerstand im Kiez oder Dorf schafft Solidarität auf einer alltäglichen, praktischen Ebene. Er eröffnet Lern- und Begegnungsfelder und macht uns ansprechbar. Wir denken, dass wir eine solidarische Praxis des Sozialen benötigen, um der isolierenden Sogwirkung des technologischen Angriffs zu widerstehen. Der technologische Umbau des Gesundheitssystems in Richtung Einpreisung individueller Verfehlungen und individueller Bemühungen ist hier ein gutes Beispiel.

Verweigerung

Wir müssen nicht alles mitmachen. Wir können uns mit Technologien kritisch auseinandersetzen und uns um weitreichende Verweigerung bemühen – vorzugsweise kollektiv. Auch hier ein Beispiel aus dem Gesundheitsbereich. Der Versuch, medikamentöse Therapien zukünftig zu personalisieren, ihnen also nur noch dann heilende Wirkung zu attestieren, wenn Wirkstoffe und Dosierung in Form einer Gentherapie individuell auf die Patient*in abgestimmt werden, erfordert unser grundsätzliches Nein. Hier hilft kein technisches Ausdifferenzieren verschiedener Methoden. Den gentechnologischen Übergriff als Ideologie einer mechanistischen Körperoptimierung sollten wir kompromisslos zurückweisen.

Zuallerletzt ein Disclaimer: Wir glauben an kein Expert*innentum, haben keinerlei Weisheit mit Löffeln gefressen, stellen daher viele Fragen und haben nur wenige Antworten. Somit freuen wir uns über Feedback, Debatte und Auseinandersetzung. Sei es per Mail an *capulcu@nadir.org* oder über andere Veröffentlichungen.

Dokumentierte Widerstände



Im Folgenden dokumentieren wir beispielhaft einige Widerstandsbemühungen gegen den technologischen Angriff. Hier finden sich neben bedeutenden und kleineren Hacks sowie Sabotage-Aktionen auch Mobilisierungen gegen diverse global player des Plattform-Kapitalismus. Die gekennzeichneten Selbstbezichtigungsschreiben der dokumentierten Aktionen geben dabei nicht unbedingt die Meinung der Redaktion wider.

Interview mit Phineas Fisher über Hacken als Direkte Aktion

„Phineas Fisher ist die wohl berühmteste Hacker-Persönlichkeit und selbsternannte anarchistische Revolutionärin. Im Interview spricht sie über die Politik hinter ihren Angriffen auf die Überwachungsindustrie, die türkische Regierungspartei und die katalanische Polizei. Ein Rückblick auf die Hacks – und ihre ersten öffentlichen Statements seit angeblichen Verhaftungen.

Dieser Beitrag erschien zunächst bei CrimethInc. Der Text und das Interview stammen von BlackBird, die Übersetzung von Leo Thüer.

Hacken wird oft als etwas Technisches dargestellt, als einfache Frage von Angriff und Verteidigung. Viel entscheidender sind aber die Beweggründe dahinter. Ein und dieselbe Methode kann als Werkzeug der Unterdrückung oder als Waffe der Emanzipation dienen. In seiner reinsten Form geht es beim Hacken nicht um die Ingenieursarbeit. In erster Linie geht es darum, Technologie kurzzuschließen damit Machtdynamiken ausgehebelt werden. Es ist eine Direkte Aktion für die neue digitale Welt, in der wir alle leben.

Im Schatten des Techno-Imperiums wurde die Hackerszene zunehmend zum Ziel für Vereinnahmung und Unterwanderung. Aber der Untergrund kann nicht ausgerottet werden, hin und wieder durchbricht eine neue Aktion die Oberfläche. Einige der Hacker, die wir bewundern, sind Programmierer und bauen Werkzeuge zum Schutz von Privatsphäre und Anonymität. Andere Crews erstellen und vertreiben alternative Medien. Und dann gibt es die, die zurückhacken.

WO IST DER HACKER-UNTERGRUND?

Für die Aufmerksamen ist es kein Geheimnis: Der Hacker-Untergrund hat im andauernden Krieg lange Zeit selbst Partei ergriffen. Doch dieses unruhige Aufbrausen, das die Untergrund-DIY-Szene der letzten Jahrzehnte geprägt hat, ist abgeklungen oder zumindest weniger sichtbar.

Pessimisten befürchteten in der Zunahme von individueller Fahnenflucht den Untergang der Hacker-Community. Dem technisch-militärischen Komplex ist es gelungen, immer mehr Hacker zu Söldnern zu machen. Es scheint auch für Menschen einer ganz bestimmten Gesinnung einen Preis zu geben: Sei es Geld, Erfolg, das Gefühl von Macht oder schlicht die Begeisterung für extravagantes Spielzeug, selbst wenn man damit diejenigen jagt, die die Staatspropaganda als „Feinde“ betitelt.

Der Untergrund versuchte zwar Zonen der Undurchsichtigkeit und des Widerstands zu vervielfältigen, doch in der öffentlichen Wahrnehmung normalisierte sich die Beziehung zwischen Hacker-Attitüde und Technologie. Hacker wurden nicht mehr als rebellische und Chaos stiftende Teenager wahrgenommen (wie in Filmen der Achtziger und Neunziger Jahre, etwa War Games oder Hackers), vielmehr wurden sie zu hochspezialisierten Militäreinheiten stilisiert – oder eben in feinster Comic-Manier als deren bösartige Gegenspieler. In ihrer entpolitisiertesten Form steht die Bezeichnung „Hacker“ fast synonym für den kapitalistischen Entrepreneur, einem Mythos, der sich sehr gut in so ziemlich jedem „Hackerspace“ einer beliebigen, gentrifizierten Großstadt beobachten lässt.

VEREINNAHMUNG DURCH STAAT UND INDUSTRIE

Die Überwachungsindustrie war so stolz auf ihre Machenschaften, dass sie sich nicht weiter darum bemühte, sich zu verstecken. Vertreter von Militärs und Anbieter von Spionageprogrammen tauchten regelmäßig auf Hacker-Community-Events auf, um Talente zu rekrutieren. Werbevideos für eine „offensive Sicherheitsstrategie" wurden offen verbreitet, um entsprechende Produkte unverblümt an Geheimdienste, Unternehmen und Regierungen zu verkaufen.

Eine alte Leier: Staaten erkaufen sich Legitimität, indem sie vorgeben solche Verbrechen zu zu bekämpfen, die nur wenige zu überhaupt zu diskutieren wagen – Kinderpornographie, Menschenhandel, Terrorismus. Doch sobald die Waffen der Überwachung in ihren Arsenalen sind, richten sie diese gegen die gesamte Bevölkerung.

Doch inmitten der andauernden Unterwanderung der Hackerwelt musste der Überwachungskomplex einen wichtigen, doch bisher unsichtbaren, Gegenschlag einstecken. Eine Einzelperson – oder vielleicht eine Gruppe – hat zurückgeschlagen, indem sie Spyware-Firmen gehackt und Information über ihre geheimsten Machenschaften veröffentlicht hat. Wenn man gegen eine Industrie kämpft, die in hohem Maße von Geheimhaltung abhängig ist, kann die Veröffentlichung interner Kommunikation und Tools eine sehr effektive Strategie sein.

DER GAMMA HACK

Im August 2014 wurde Gamma gehackt, ein deutsch-englischer Anbieter von Spionageprogrammen. Es wurden 40 GB an Informationen befreit. Nach diesem Hack gab es keine Geheimnisse mehr über Gamma, alles war öffentlich zugänglich: Kunden, Produktkataloge, Preislisten, die Software selbst und sogar Schulungshandbücher.

Das bekannteste Produkt der Firma, das Programm FinFisher, wurde an mehr als 30 Regierungsbehörden und Polizeikräfte verkauft, um Journalisten, Aktivisten und Regimekritiker zu auszuspionieren. Im Zuge des sogenannten Arabischen Frühlings hatte das Unternehmen Andersdenkende in Ägypten und Bahrain infiziert. In der Regel wurden die Ziele durch Social Engneering dazu verleitet, die Schadsoftware zu installieren.

Einmal im Visier des Unternehmens, muss das Ziel nur noch den Anhang oder Link aus einer Mail öffnen und schon ist FinFisher installiert. Von dort an haben die Kunden, die die Schadsoftware von dem Unternehmen gekauft haben, die Kontrolle über den infizierten Computer oder das Smartphone und somit uneingeschränkten Zugriff auf Mikrofone, Nachrichten, Mails sowie Standortdaten.

Unmittelbar nach dem Hack begann jemand, mit einem Account zu twittern, der sich als „Gamma PR" ausgab. Doch die bloße Enthüllung der Informationen war noch nicht genug: Ein Hacker mit dem Namen Phineas Fisher veröffentlichte eine einfache Textdatei, in der ein Tutorial mit Details über den Angriff auf Gamma enthalten war:

Ich schreibe das nicht, um anzugeben, was für ein cooler Hacker ich bin und welche krassen Fähigkeiten ich eingesetzt habe, um Gamma bloßzustellen. Ich schreibe das, um Hacken zu entmystifizieren und um zu zeigen wie einfach es ist. Und hoffentlich um euch zu informieren und zu inspirieren raus zu gehen und zu hacken.

Der Name dieser Datei war „Hack Back! Ein Do-it-yourself-Guide für alle, die keine Geduld haben, auf Whistleblower zu warten". Innerhalb der geschwächten Hacker-Community haben die ursprünglichen Werte wie Solidarität, individuelle Freiheit und offener Informationsaustausch an Boden verloren gegenüber der zunehmenden Kommerzialisierung von Wissen durch den freien Markt und das Imperium. Diese Aktion war ein Hauch von frischer Luft – und vielleicht der Beginn einer Bewegung.

HACKEDTEAM

Du willst mehr. Du musst dein Ziel hacken. Du musst Verschlüsselung überwinden und relevante Daten aufzeichnen und dabei listig und unauffindbar sein. Genau was wir machen.

Diese Worte lassen sich dem Werbeclip für das Produkt „Da Vinci" entnehmen, einem „Fernsteuerungssystem", das von einer italienischen Firma namens Hacking Team weltweit verkauft wurde.

Eine Firma mit einem so schamlosen Namen wie „Hacking Team" entsteht, wenn eine lokale Polizeibehörde zwei Hacker-Söldner zur Zusammenarbeit einlädt. Die Einheit für „Cyberkriminalität" der Mailänder Polizei war der Meinung, dass passive Überwachung für ihre Zwecke nicht ausreiche. Um also ihr Bedürfnis nach Offensive zu befriedigen, baten sie Alor und Naga, zwei berühmte italienische Hacker, um Hilfe. Ein bekanntes Hacking-Tool, das die beiden entwickelt hatten, sollte an neue Zwecke angepasst werden.

Wer ihre Kunden waren und wie sie es geschafft haben, ihre Opfer zu infizieren und auszuspionieren, blieb bis zum Juli 2015 ein Geheimnis. An diesem Tag gab der

Twitter-Account des Unternehmens bekannt: „Da wir nichts zu verbergen haben, veröffentlichen wir alle unsere E-Mails, Dateien und Quellcodes“. Es wurden Links zu mehr als 400 Gigabyte Daten bereitstellen. Wie üblich behauptete das Unternehmen zunächst, dass der Leak aus falschen Informationen bestehe, doch das Fälschen einer so großen Menge an Daten wäre eine fast unmögliche Leistung.

Diejenigen, die vermuteten, dass der Angriff eine vertraute Unterschrift trug, lagen nicht ganz falsch. Wieder einmal steckte der sarkastische Spitzname Phineas Fisher hinter den Enthüllungen.

Durch die Veröffentlichung all der internen Informationen – gefolgt von weiteren Anleitungen mit technischen Details und der politischen Motivation hinter dem Angriff – offenbarte Phineas Fisher der Welt die unbestreitbaren Beweise über die Arbeit der 70 Kunden von Hacking Team. Die meisten dieser Kunden waren Militärs, Polizeikräfte oder Bundes- und Landesregierungen. Der Gesamtumsatz belief sich auf über 40 Millionen Euro. Die vollständige Liste der Kunden findet sich auf Wikipedia.

Die Enthüllungen bestätigten, dass es sehr gute Gründe für die weltweite Forderung nach mehr Schutz von Privatsphäre und Anonymität gibt. Neben den Snowden-Enthüllungen gaben uns die Einblicke in die schmutzigen Geheimnisse von Hacking Team eine Vorstellung von dem enormen Ausmaß, mit dem sich Regierungen und Unternehmen für gezielte Überwachung einsetzen. Wir wissen heute, dass es viele andere skrupellose Firmen gibt, die von illegalen Spionageoperationen profitieren – zum Beispiel lockte die israelische NSO-Gruppe kürzlich Journalisten, die das Massaker von Iguala in Mexiko untersuchten, in eine Falle und lies ihre Geräte eigenhändig infizieren.

Die anonyme Demaskierung von Hacking Team war eine brillante Operation mit globalen Auswirkungen.

EIN MARKT FÜR GEHEIMNISSE

Unternehmen wie Gamma und Hacking Team sind auf Geheimhaltung angewiesen. Um ihre Ziele zu infizieren, werden sogenannte „Zero Days“ eingesetzt. Ein „Zero Day“ ist eine Sicherheitslücke in einem Computerprogramm, die noch nicht öffentlich bekannt gemacht wurde und von jedem, der sie kennt, ausgenutzt werden kann, um Programme, Daten oder Netzwerke anzugreifen. In vielen Fällen wird dadurch eine vollständige Fernsteuerung ermöglicht.

Der Überwachungskapitalismus hat unlängst ein Netz von Unternehmen geschaffen, die als Broker agieren und diese Schwachstellen auf schwarzen und grauen Märkten einkaufen. Der Preis für einen einzelnen „Zero Day“ kann zwischen 10.000 und 300.000 Dollar oder sogar einer Million liegen. Um mehr über Software-Schwachstellen und den von Regierungen geführten „Cyberwar“ zu erfahren, schaut Euch die Doku „Zero Days“ an.

Spyware-Unternehmen wie Hacking Team machen diese Sicherheitslücken zu Waffen, verkaufen Lizenzen an Repressionsbehörden und ermöglichen diesen ein kinderleichtes „click and spy“. Je nach Bedürfnis des Kunden werden auch maßgeschneiderte Lösungen angeboten, um in Systeme von ausgewählten Opfern einzudringen.

Günstige Gelegenheiten, um diese „Zero Days“ auszunutzen, werden mit der Zeit seltener. Je öfter eine Sicherheitslücke ausgenutzt wird, desto höher ist die Wahrscheinlichkeit, dass der Angreifer auffliegt und die Löcher gestopft werden. Ebenso steigt die Wahrscheinlichkeit, dass andere Gruppen die gleiche Sicherheitslücke entdecken. Wenn das Gerät der Zielperson einen Patch bekommt, der die Fehler zu behebt, hat der Angreifer seine Chance vertan. Deshalb ist es so wichtig, stets die aktuellsten Updates auf unseren Geräten zu installieren. Es gibt jedoch Fälle, in denen Hersteller Updates erschweren oder gar unmöglich machen.

Schwachstellen-Broker und Spyware-Anbieter erlauben es technisch inkompetenten Menschen, Ziele zu infizieren, auszuspionieren und Daten abzugreifen. Dazu müssen lediglich Formulare ausgefüllt und in einer Web-Anwendung herum geklickt werden. Das haben Analysen von Software wie XKeyscore oder der Galileo-Suite von Hacking Team gezeigt.

Ironie ist, dass der Verkauf von idiotensicheren Spionage-Tools, etwa an die Polizei, oft ein falsches Gefühl von Sicherheit verleiht. Phineas hat gezeigt, dass die von ihm kompromittierten Systeme absolut lahme Passwörter wie „P4ssword“, „Wolverine“ oder „Universo“ hatten. Den Grundregeln der Betriebssicherheit kann sich niemand entziehen.

TÜRKEI UND KURDISTAN

Ein weiterer Vorteil des Internets ist, dass man ein Ziel auf der anderen Seiten der Welt angreifen, die Reise dorthin aber sparen kann. Man muss nicht mal aus dem Bett aufstehen, auch wenn das zuträglich ist, um die Sache ausgeglichen anzugehen.

„Ich habe die AKP gehackt", verkündigte Phineas in 2016, nachdem er die Server der türkischen Regierungspartei gehackt hatte. Ein Auszug von mehr als 100 Gigabyte Daten und Mails der AKP wurde an die revolutionären Kräfte in Kurdistan weitergegeben. Phineas musste sich beeilen, denn WikiLeaks veröffentlichte die Informationen, noch bevor er überhaupt alle Daten heruntergeladen hatte.

Doch nicht nur die Informationen sind in Kurdistan angekommen: Phineas hat auch eine Schwachstelle in den Sicherheitssystemen einer unbekannten Bank ausgenutzt, um 10.000 Euro in Bitcoin an „Rojava Plan" zu überwiesen, eine internationale Unterstützergruppe der autonomen Region Rojava.

KATALONIEN UND SÜNDENBÖCKE

Im Mai 2016, inspiriert durch den Dokumentarfilm Ciutat Morta, überlegte sich Phineas einen einfachen Angriff auf die katalanischen Polizeikräfte. Die Doku erzählt die Geschichte eines berüchtigten Zwischenfalls in der Geschichte Spaniens, dem sogenannten „4F-Fall": Mehrere junge Leute aus Südamerika werden von den Repressionskräften eingesperrt und gefoltert, als Akt der Vergeltung für einen Polizisten, der im Zuge von Verhaftungen in Barcelona ins Koma gefallen war.

Phineas neuester Hack nutze eine bekannte Schwachstelle, um auf der Website der katalanischen Polizeigewerkschaft mit einem ironischen Manifest zu verkünden, die Gewerkschaft habe sich „zugunsten der Menschenrechte neu gegründet". Ein Auszug personenbezogener Informationen von etwa 5.000 Polizisten wurde veröffentlicht, zusammen mit einer 40-minütigen Anleitung, in dem die von Phineas verwendeten Techniken erklärt wurden.

Kurz darauf führte die Polizei mehrere Razzien in Sozialen Zentren und Hacklabs in Barcelona durch und behauptete, den berüchtigten Hacker erwischt zu haben. Journalisten berichteten allerdings nur wenige Stunden später, sie seien von eben dieser Person kontaktiert worden, sie sei „frei und guter Dinge". Die Polizei habe nur einen Sündenbock verhaftet, der lediglich die Informationen aus dem Hack vertwittert hatte.

Nachdem weitere Razzien der katalanischen Polizei erfolglos blieben, stimmte Phineas Fisher einem Interview mit Vice Motherboard zu, unter der Bedingung, dass seine Antworten von eine Puppe präsentiert werden.

PERSON UND PERSONA

Eine der interessantesten Konsequenzen der Aktionen von Phineas Fisher ist der Ausdruck in den Augen deiner Hacker-Kollegen, wenn du das Thema mit ihnen diskutierst. Chilenen sind überzeugt, Phineas sei ein Latino. Hausbesetzer in Barcelona schwören, dass ihnen sein Ton vertraut ist. Auch Italiener behaupten das Gleiche. US-Amerikaner denken, sie oder er spricht wie einer von ihnen. Und dann gibt es die gesunde Annahme, dass Phineas wie jeder gute Hacker Russe sein muss – einer jener Russen, die überraschend gut Spanisch sprechen.

Es steckt in der Tat etwas Vertrautes in den Handlungen dieses Phantoms. Ein tiefes Gefühl von Gerechtigkeit und Internationalismus sowie der starke Eindruck, dass seine Handlungen auch weiterhin unter dem Radar bleiben werden. Wie in der Vergangenheit will niemand wahr haben, dass ein stinknormaler Mensch hinter solchen Taten steckt, der ansonsten ein ganz gewöhnliches Leben führt.

EINER VON UNS

Die Wahrheit ist, dass es niemanden interessiert – außer vielleicht die Cops, denen es schwer fällt, diese Persona nur anhand ihrer inhärenten Widersprüche und stilistischen Analysewerkzeuge zu identifizieren. Uns hingegen interessiert die Identität der Persona nicht. Es ist am Ende egal, denn wenn diese Identität verbrannt werden sollte, erscheint eine neue. Wer sich von Persönlichkeitskult lossagen kann, gewinnt Freiheit.

Viel entscheidender ist: Wer auch immer Phineas Fisher wirklich ist, er ist einer von uns – und seine Taten zeigen uns, welche Macht wir haben.

Die direkten Aktionen zeigen, dass zwar eine Menge Hingabe erforderlich ist, um gewisse Fähigkeiten zu erlernen, dafür aber in den meisten Fällen nichts weiter Außergewöhnliches notwendig ist. Vielleicht seid ihr technisch nicht besonders versiert, dafür aber gut im Umgang mit Menschen – oft braucht es gar nicht mehr für einen fantastischen Hack. Auch wenn ihr keinen technischen Hintergrund habt, eine spielerische Beharrlichkeit kann oft mehr erreichen als jede formale Ausbildung, wenn es darum geht, einen Keil in die Reihen der Bürokraten zu treiben, denen es nur um die Umsetzung von irgendwelchen Politiken geht, unabhängig davon wofür diese stehen.

Sicherheit ist keine absolute Qualität. Im Netz wird es nie eine absolute Macht geben. Um Phineas zu zitieren: „Darin liegen Schönheit und Asymmetrie des Hackens: Mit 100 Stunden Arbeit kann eine einzelne Person mehrere Jahre Arbeit eines millionenschweren Unternehmens zu-

nichte machen. Hacken gibt den Underdogs die Chance zu kämpfen und zu gewinnen."

Die Taten eines bescheidenen, aber motivierten Hackers können die aufgeblasenen Egos der Cyber-Sicherheitsindustrie oder die Akademiker, die es nicht wagen, über den Tellerrand zu schauen, mit Leichtigkeit in den Schatten stellen. Und dabei sind es nicht immer die großen Hacks, die die Realität verändern: Jemand, der lernt, anonym zu bleiben, also keine Angst aber die Disziplin hat, Details zu seiner Person beisammenzuhalten, ist stets im Vorteil. Dabei gilt außerdem: Wer ständig sein Ego füttern muss, wird es schwerer haben, seine individuellen Freiheiten zu bewahren.

PHINEAS FISHER IST TOT

Am Ende ist Phineas verstummt. „Ich habe die Accounts gelöscht, weil ich nichts mehr zu sagen hatte." Und wahrscheinlich war es genug. Manchmal braucht es ein wenig Action, damit sich die kollektive Stimmung ändert und wir uns unserer eigenen Macht bewusst werden.

Phineas Fisher ist tot. Es war mehr als nur ein Name, es war die Spitze eines Untergrund-Netzwerks von Praktiken und Wünschen. Es war nicht nur eine, sondern mehrere Aktionen. Kybernetische Guerilla: Hit and Hide.

Wer an die Hackback-Mail-Adresse schreibt, kann bezeugen, dass Phineas noch immer die Freiheit genießt. In einer charmanten Unterhaltung zeigt er oder sie, dass der Staat eben keine absolute Kontrolle hat. Wie er immer wieder gerne betont: „Es ist immer noch möglich, das System anzugreifen und damit durchzukommen."

STILLE JAHRE DER INDIVIDUELLEN WIEDERANEIGNUNG

Phineas ist weiterhin beschäftigt. Er mag es, aus dem Schatten zu sprechen, wie er uns mitteilt:

Individuelle Wiederaneignung hat sicherlich materielle Auswirkungen, aber sie ist eigentlich eine ideologische Waffe. Die Regeln dieses Systems sind keine unveränderlichen Fakten, sondern von einer Minderheit auferlegte Regeln, die wir in Frage stellen, ändern und sogar brechen können. Wenn jemand eine Bank ausraubt, gibt der Staat riesige Mittel aus, um dem Raub nachzugehen. Nicht weil es ökonomisch sinnvoll ist, 100.000 Dollar auszugeben, um einen 3.000-Dollar-Raub zu untersuchen, sondern um die kollektive Illusion von Privateigentum zu schützen. Der Staat versucht, jeden rebellischen Geist auszulöschen, der außerhalb seiner Regeln spielt.

Er ergänzt:

Man braucht kein Informatikstudium, um an dem teilhaben zu können, was der ehemalige NSA-Chef Keith Alexander als verantwortlich für den größten Transfer von Reichtum in der Weltgeschichte bezeichnet. In diesem großen Projekt wird die meiste Arbeit nicht von Hackern gemacht, sondern von Laien, die wissen, wie man Adressen findet, wie man Post und Pakete erhält, wie man gefälschte Dokument überzeugend einsetzt und wie man ein Wegwerfhandy benutzt. Mehr muss man nicht können, um einen Handyvertrag abzuschließen, Bankkonten zu eröffnen und nach Krediten zu fragen, Online-Einkäufe zu tätigen und diese zu erhalten. Jeder kann lernen, wie man den *Tor*-Browser und Bitcoin benutzt, um an Darknet-Märkten teilzunehmen. Die Mafia und das organisierte Verbrechen haben diesen Wandel erkannt, aber Anarchisten, die für Illegalismus und Wiederaneignung zu haben sind, haben noch nicht erkannt, dass wir nicht mehr in der Vor-Internet-Zeit leben und dass es bessere Taktiken gibt, als eine Bank mit einer Waffe auszurauben. Wir leben einen einzigartigen Moment in der Geschichte, und wir haben eine großartige Chance."

Netzpolitik 1.7.2018

Bure: Neue Daten aus dem Hack bei Ingerop

Dokumentation: Indymedia, 06.09.2018

DIE MONSTER VON CIGEO

„Anfang Juni startet eine Kampagne namens les monstres de CIGEO mit dem Ziel, die am Projekt beteiligten Firmen und Subunternehmen stärker ins Auge zu fassen und politisch unter Druck zu setzen. Auf der Homepage "lesmonstresdecigeo.noblogs.org" werden umfassende Listen entsprechender Niederlassungen Weltweit veröffentlicht. Dass es sich hier um mehr als fleißige Recherchearbeit und die Auswertung öffentlich zugänglicher Dokumente handelt, wird schnell deutlich, nachdem auch Namen und persönliche Daten von 1700 leitenden Mitarbeitern des Ingeneurkonzerns ingerop online gestellt werden. In einer privaten email an die Betroffenen werden diese über

deren outing informiert und darauf hingewiesen, dass sie mit ihrer Arbeit eine auch persönliche Verantwortung an dem Projekt tragen.

Der Datenklau bei ingerop war kein einmaliger Glücksgriff, sondern Ergebnis einer mehrwöchigen intensiven Cyberattake gegen den Konzern. Das belegt die spätere Veröffentlichung von emails der Firma mit Sicherheitsanweisungen an ihre Mitarbeiter*innen in selber Angelegenheit. Nach eigenem Bekunden ist es den Hacker*innen gelungen, bei ingerop eine enorme Datenmenge mit teils hoch brisanten Informationen abzuschöpfen. Seither werden immer wieder Dokumente von CIGEO geleakt, die in der Tat an politischer Sprengkraft nicht zu wünschen übrig lassen: eine bisher zurückgehaltene Studie, die dem kleinen Dörfchen Mandres ein Verkehrsaufkommen von 200 LKW täglich für die mehrjährige Bauphase prognostiziert. Belege darüber, dass ANDRA Listen der lokalen Landbesitzer*innen führt auf denen diese in 3 Kategorien nach ihrer "Beherrschbarkeit" unterteilt werden. Technische Einzelheiten zur bevorstehenden Trafobaustelle und dessen Sicherheitskonzeptes. Umweltschützer*innen, Anwohner*innen, Bürgerrechtler*innen, Freund*innen der direkten Aktion – für alle was dabei!

Und es ist offensichtlich noch Luft nach oben... In Reaktion auf die Razzien am 21. Juni werden weitere sensible Daten geleakt. Diesmal jedoch nicht zu CIGEO: über einen link stellen die Netzaktivist*innen die Baupläne von 4 französischen (zum Teil noch nicht fertig gestellten) Hochsicherheitsgefängnissen, dem AKW in Fessenheim, sowie der U-Bahn von Madrid online. Während sich politischer Bezug, sowie praktischer Wert der Veröffentlichung der Gefängnisbaupläne wohl von selbst erklären, mag die Auswahl der anderen Objekte etwas geschmacklos erscheinen (Baut Zuhause jetzt bitte kein marodes Atomkraftwerk nach, oder plant Anschläge auf den öffentlichen Nahverkehr in Spanien!). Die Kernbotschaft ist wohl eher folgende: Wir reden hier vom Zugriff auf Daten höchster Geheimhaltungsstufe in einem Zeitraum von etwa 50 Jahren bis hinein in zukünftige Großbauprojekte und das international! Der Imageverlust dieser Firma, die ja quasi nichts anderes als „Sicherheit" verkauft ist gar nicht auszudenken. Abgesehen von dem realen wirtschaftlichen Schaden der damit einhergehen wird, könnten weitere Verluste hinzukommen, wenn betroffene Kund*innen Rechtsansprüche geltend machen, oder Abstand von bereits geplanten Bauprojekten nehmen.

Unter folgendem Onion Link findet ihr weitere Daten aus dem Hack. Der Link ist nur mit dem *Tor* Browser zu öffnen und wird nach einiger Zeit wieder abgestellt. Also kopiert die Daten und erstellt Mirror. Veröffentlicht sie in anderen Medien und nutzt sie!"

bxqigvnvsi7nlure.onion
https://de.indymedia.org/node/24069

Hacker legen RWE-Webseite lahm

Hacker haben die Internetseite des Energiekonzerns RWE lahmgelegt. Das Unternehmen habe Strafanzeige gegen unbekannt erstattet, teilte ein RWE-Sprecher am Montag (24.9.2018) mit. Eine Flut gesteuerter Anfragen habe die Leistungsfähigkeit des Servers erheblich reduziert.

„In der Folge war die Website zeitweise nur schwer oder mancherorts gar nicht erreichbar", erklärte der Sprecher. IT-Spezialisten des Unternehmens seien damit beschäftigt, das Problem zu lösen. Sicherheitseinrichtungen des Unternehmens waren den Angaben zufolge nicht betroffen. Am Dienstagmorgen war die RWE-Website wieder erreichbar.

RWE steht seit Wochen in der Kritik, weil das Unternehmen ein Waldgebiet westlich von Köln abholzen will, um weiter Braunkohle abzubauen. Gegen die Rodung des Hambacher Forstes gibt es heftigen Widerstand. Umweltschützer fordern einen Aufschub, bis die derzeit tagende Kohlekommission einen Plan für den Kohleausstieg vorlegt. Ob der Hackerangriff aber etwas mit dem Hambacher Forst zu tun hat, ist unklar.

Drohungen allerdings gibt es gegen den Energiekonzern. Am Donnerstag veröffentlichte ein Account namens „Troll Troll" ein erstes Video mit dem Titel „Anonymous Operaton: RWE abschalten". In dem knapp zweiminütigen Clip ist eine Person mit einer Anonymous-Maske zu sehen und eine Computerstimme zu hören:

„An RWE: Sollten Sie nicht sofort die Rodung des Hambacher Forstes einstellen, werden wir Ihre Server angreifen, Ihre Homepages und Facebook-Seiten abschalten, so lange bis Ihr Konzern einen wirtschaftlichen Schaden davonträgt, dass Sie sich nicht mehr davon erholen." Zudem fordert die Stimme die RWE-Kunden auf, ihre Verträge zu kündigen. Zusammen werde man RWE in die Knie zwingen. Wer das Video hochgeladen hat, ist nicht bekannt.

https://www.welt.de/wirtschaft/article181653102/RWE-Website-von-Hackerangriff-lahmgelegt.html

Roboter zur Vertreibung von Obdachlosen

San Francisco: Eigentlich werden die Roboter des Unternehmens Knightscope als elektronische Wachmänner eingesetzt. Eine Tierschutzorganisation nutzt einen K5-Roboter hingegen, um Obdachlose von ihrem Büro fernzuhalten. Der Widerstand gegen den Robo-Cop ist groß.

Mittlerweile ist es in vielen internationalen Metropolen keine Seltenheit mehr, Roboter zu sehen, die auf Parkplätzen, in Einkaufszentren oder auf Firmengeländen patrouillieren. In Dubai assistieren sie zudem Touristen und in China halten sie mit Gesichtserkennungssoftware nach Straftätern Ausschau. Die Tierschutzorganisation Society for the Prevention of Cruelty to Animals – kurz SPCA – lässt einen Roboter derzeit auf dem Bürgersteig um ihr Büro in San Francisco Streife rollen. Der K5-Roboter des Start-ups Knightscope ist mit Video-, Wärmebildkameras, Laserscanner, Radar, Mikrofon und CO2-Sensoren in der Lage, Vandalismus, Einbrüche und Verletze zu erkennen. Jedoch wird er von der SPCA genutzt, um Obdachlose zu verscheuchen und sie davon abzuhalten, ihr Nachtlager aufzuschlagen.

Der an einen Dalek aus Doctor Who erinnernde Blech-Wachmann ist bereits seit einem Monat im Einsatz. Auf seinen Rundfahrten gibt er eine entnervende Musikbeschallung von sich und kann bei Auffälligkeiten einen Wachdienst informieren. Wie die Tierschutzorganisation in US-Medien angibt, richte sich der Roboter gegen „Verbrechen, die scheinbar von den nahegelegenen Lagern von Obdachlosen ausgehen". Darunter Drogenmissbrauch und Einbrüche. Wobei die Organisation dementiert, dass der K5 die Personen aus der Umgebung vertreiben solle. Zumindest laut Hersteller Knightscope habe sich „die Sicherheit und Qualität der Region" durch den Einsatz schon deutlich verbessert. Die Kosten für die Anmietung des Roboters betragen zwischen sechs und sieben Dollar pro Stunde und liegen damit niedriger als der Mindestlohn für einen menschlichen Schutzmann.

Die Reaktion der Öffentlichkeit auf den mit Tieraufklebern dekorierten K5 ist allerdings alles andere als positiv. Den Einsatz gegen Obdachlose empfinden viele als unethisch, herzlos und empörend. Auf Twitter und Facebook wird zum Protest und gar zur Zerstörung des Roboters aufgerufen. Tatsächlich wurde der K5 angeblich schon mehrfach angegangen. Er wäre mit Barbecue-Sauce und Fäkalien beschmiert oder auch umgestoßen worden. Ebenso hätten Scherzbolde ihm „eine Plane übergestülpt". Das wirft generelle Fragen über die Akzeptanz von Sicherheitsrobotern in der Öffentlichkeit auf.

Auch die Stadtverwaltung von San Francisco sieht Handlungsbedarf in Bezug auf die Roboter, die zuletzt immer wieder durch peinliche Pannen und gefährliche Unfälle auffielen. Bereits am ersten Dezember war die Tierschutzorganisation informiert worden, dass eine explizite Genehmigung für den Einsatz auf öffentlichem Grund nötig seit. Daher droht nun für jeden weiteren Einsatztag eine Geldbuße von 1000 US-Dollar. Es sei denn, es wird eine ordentliche Nutzungserlaubnis beantragt und bewilligt. Derzeit soll sich der Roboterhersteller Knightscope auch schon selbst in Verhandlungen mit der Stadtverwaltung befinden.

wired 14.12.2017

Hack the police

BERLINER POLIZEI LAHMGELEGT

Die Telefonanlagen zweier Polizeiwachen sind Anfang der Woche von Hackern zeitweise lahmgelegt worden. Auf den Abschnitten 13 in Pankow und 32 in Mitte hörten die Beamten u.a. Rap-Songs.

Pfeiftöne, automatische Ansagen und Rap-Songs – Hacker legten Polizei-Telefone lahm!

In mehreren Berliner Polizei-Dienststellen und Abschnitten wurden die Beamten in den vergangenen Tagen Opfer eines besonders ausgeklügelten „Klingelstreichs". Die Telefonanlage spielte komplett verrückt. Offenbar, weil sie von außen manipuliert worden war.

In einem internen Schreiben (liegt B.Z. vor) heißt es: „Alle Telefone klingelten gleichzeitig, bei Abnahme der Hörer waren Pfeiftöne, verschiedene automatische Ansagen und Rap-Songs zu hören. Die normale Annahme von Gesprächen war nicht möglich."

So klingelte es am Montag und Mittwochabend auf dem Abschnitt 13 (Pankow) Sturm. Und auch ihre Kollegen vom Abschnitt 32 (Mitte) mussten den Telefon-Terror über sich ergehen lassen. Die Beamten erstatteten Anzeige wegen Störung der Telekommunikationsanlagen.

Telefonanbieter Versatel bestätigt gegenüber B.Z. die Attacke. Eine Sprecherin: „Es war ein Versuch, die polizeiliche Arbeit zu stören."

Berliner Zeitung 29.11.2015

https://www.bz-berlin.de/berlin/pankow/telefon-lahmgelegt-hacker-angriff-auf-die-berliner-polizei

OBSERVATIONSSYSTEM GEHACKT

Der Datendiebstahl bei der Zollfahndung ist nach wie vor nicht aufgeklärt. In Zusammenarbeit mit der Bundespolizei und dem Cyber-Abwehrzentrum werde weiter untersucht, wie bislang unbekannte Täter Daten eines Observationssystems stehlen konnten, sagte ein Sprecher des Zollkriminalamtes.

Eine Gruppe, die sich „no name crew" nennt, hatte sich in der Nacht zum Donnerstag auf elektronischem Weg Zugang zu einem Computer verschafft. Auf diesem speichert der Zollfahndungsdienst Daten des Ortungssystems „Patras", das Standorte von Personen, Fahrzeugen oder Waren dokumentiert. Daten dieses Systems wurden von den Unbekannten abgegriffen und im Internet veröffentlicht. Dabei ging es nach Auskunft des Sprechers zunächst nicht um Angaben zu laufenden Ermittlungen. Bei einer zweiten Veröffentlichung seien jedoch auch persönliche Daten von Ermittlern betroffen gewesen.

Nach Informationen des Nachrichtenmagazins „Spiegel" begründete die Hackergruppe ihre Attacke mit politischen Motiven. In einem Chat-Interview gab ein führendes Mitglied der Gruppe unter dem Namen „Darkhammer" an, „für die Rechte und die Freiheit der Bürger" zu kämpfen, wie das Magazin berichtet.

ntv 9.7.2011

https://www.n-tv.de/politik/Polizei-raetselt-ueber-Hacker-angriff-article3769086.html

BRITISCHE POLIZEI SOCA GEHACKT

Die Serie von Hacker-Angriffen auf Behörden und internationale Konzerne reißt nicht ab. Diesmal attackierte die Hacker-Gruppe Lulz Security nach eigenen Angaben am Montag eine Internetseite der britischen Polizei. Die Website der britische Behörde zur Bekämpfung von organisiertem Schwerverbrechen (SOCA) sei kurzzeitig abgeschaltet worden. Ein Sprecher des betroffenen Dezernats sagte, dass man den Vorfall prüfe. Dieselbe Hacker-Gruppe hatte nach eigener Darstellung erst vor wenigen Tagen Internetseiten des US-Geheimdienstes CIA und des US-Senats angegriffen.

In den vergangenen Wochen wurden wiederholt große Einrichtungen oder Unternehmen von Hackern angegriffen. Betroffen waren unter anderem der Internationale Währungsfonds, Lockheed Martin, Citigroup, Google, Sony, Nintendo und Sega.

rtl 13.2.2016

https://www.rtl.de/cms/hacker-greifen-internetseite-britischer-polizei-an-780822.html

Herrschaftsnetze sind angreifbar

von „Vulkangruppe NetzHerrschaft zerreißen"

Dokumentation: indymedia 26.3.2018

„Die Herrschaft über die Menschen organisiert sich neu: über die Netze, die Algorithmen und die Zugriffe des Staates und der Konzerne – auf unser Leben und im Alltag. Auf unsere Gefühle, unser Denken, unser Tun. Jetzt und in der Zukunft. Und weitet sich immer tiefer aus. Wir werden überwacht, gesteuert und gelenkt.

Wir haben heute ein paar wichtige Netzwerkverbindungen gekappt und dadurch den Zugriff auf unser Leben unterbrochen - ein bescheidener Beitrag, einen Moment unkontrollierten Lebens zu schaffen. Betroffen von unserem Anschlag waren Netzbetreiber wie: BASE (belgischer Mobilfunk, in Deutschland E-Plus), Level3, Globalmetro Networks (versorgt u.a. Militärstützpunkte), Tele-Com, LIT (Landesbetrieb für Informationstechnik; jetzt IT-Dienstleistungszentrum Berlin, Zuständigkeit: zentrales Verwaltungsnetz der Stadt), COLT (Regierungsnetze) und weitere zivile und militärische Betreiber. Unser konkretes Ziel war auch die Störung des Flughafen Tegels, der Bundes- und Landesverwaltungen, der Bundeswehr, der Flugbereitschaft der Bundesregierung und der Industrie- und Technologiekonzerne.

Zu diesem Zweck haben wir am 26.3.2018 an der Mörschbrücke in Berlin an zwei je vier Meter breiten und drei-

ßig Meter auseinander liegenden Kabelsträngen Feuer gelegt. Die Gasleitungen lagen von unseren Brandherden zu beiden Seiten 15 Meter entfernt. Die Brandherde lagen nicht zugänglich innerhalb der Brückenkonstruktion, abgeschirmt von 1 Meter dicken Betonwänden auf einer Höhe von mehr als zwei Metern. Weder Fußgänger_innen (noch Fahrzeuge) unter noch auf der Brücke konnten unmittelbar mit dem Feuer in Berührung kommen. Eine Gefährdung von Menschen haben wir ausgeschlossen.

Der hoffentlich hohe wirtschaftliche Schaden ist uns eine Freude!

Herrschaftsnetze sind angreifbar.

Aus gegebenem Anlass: Deutsche Waffen und türkisches Militär raus aus Efrin! Die Verantwortlichen des Krieges in Efrin sitzen auch in Deutschland. Sie sind zu finden.

Vulkangruppe NetzHerrschaft zerreißen

Anmerkung zur Mitmachmilitanz: Die Zensur ist mittlerweile sehr massiv. Sie muss durchbrochen werden. Darum benutzt *Tor* um zu unserem Text Zugang zu erhalten. Und streut dann unsere Erklärung in Printmedien, Flyern, Kommentarspalten, E-Mails, „sozialen" Medien.

PROLOG

(…) Die Arroganz der Macht, die Herrschaft des Falschen, die Vulgarität der Reichen, die Industrie-Katastrophen, das galoppierende Elend, die nackte Ausbeutung, der ökologische Untergang – von nichts werden wir verschont, nicht einmal davon informiert zu sein.

Klima 2017, Klima 2018, Klima 2019 – heißestes Jahr. Die Gründe für eine Revolution wären gegeben. Aber nicht die Gründe machen eine Revolution – sondern die Menschen. Und die Menschen sitzen vor den Bildschirmen. (…) Die Menschheit wohnt verzaubert ihrem Untergang bei (…). Sie verfolgt es so gebannt, dass sie nicht spürt wie ihr, wie uns (!) das Wasser bereits zu den Fesseln reicht (…). Es geht nicht mehr darum, diese Welt zu kommentieren, zu kritisieren, anzuprangern. (…) Weiterhin Diskriminierung, Unterdrückung, Ungerechtigkeit anzuprangern und darauf zu warten, dass das was bringt, ist überholt. (…) Die Lüge ist die Weigerung gewisse Dinge zu sehen, die man sieht, und sie so zusehen, wie man sie sieht. Die tatsächliche Lüge sind all die Bildschirme, all die Bilder, all die Erklärungen, die man zwischen sich und der Welt stehen lässt. Es ist die Art, wie wir tatsächlich unsere eigene Wahrnehmung mit Füßen treten …

Wir haben heute viele Kabelstränge durchtrennt. Niemand kommt dadurch körperlich zu Schaden.

Die verschiedenen Kabel unter der Mörschbrücke in Berlin werden konkret genutzt vom Militär und seinen Dienstleistern, der Flugbereitschaft der Bundesregierung, der Bundespolizei, der Bundesregierung, der Verwaltung des Landes Berlin, Großkonzernen, Internet-Knotenpunktbetreibern, dem Flughafen Tegel.

Wir unterbrechen mit unserem kleinen Beitrag das reibungslose Funktionieren der Metropole. Denn solange alles funktioniert, geht die beispiellose Zerstörung der ökologischen Lebensgrundlagen unverändert weiter. Krieg, Klimazerstörung, Fluchtbewegungen und militarisierte EU-Außengrenzen sind nicht getrennt zu betrachten. Der Raubbau von Rohstoffen und die Existenz von Armut, die Rodung von Urwäldern und die Fleischproduktion, das steigende Flugaufkommen und der krank machende Dreck, der in die Luft geblasen wird.

Es braucht das Eingreifen derer, die nicht länger zuschauen wollen. Zum Beispiel durch Angriffe auf das Funktionieren der Metropolen. Zum Beispiel durch die Sabotage von Strukturen, welche diese Zerstörung aufrecht erhalten, durch Angriffe auf Infrastruktureinrichtungen, künstliche Intelligenz, Smart City, Industrie 4.0 - Überwachungsformen aller Art. Die Folgen einer kapitalistisch bedingten Umwelt- und Klimazerstörung sind unausweichlich – wir werden diese nicht verhindern. Wir müssen ein Verhalten finden angesichts der daraus resultierenden autoritären, kriegerischen Formierungen.

Wir unterbrechen mit unserem Sabotageakt den ganz normalen Gang vielfältiger Arbeitsabläufe in der Hauptstadt – das war gesetztes Ziel. Die oben benannten Netzbetreiber sind Verwalter eines gewaltsamen Prozesses, welcher uns als digitale Revolution verkauft wird. Wir als Nutzer_innen des Netzes begeben uns unweigerlich in eine Abhängigkeit. Wir sind damit sowohl Opfer als auch Mitverantwortliche dieses Prozesses. Die digitale Dauererreichbarkeit dehnt beispielsweise den Arbeitstag aus, so dass er oft kaum noch endet. Selbstoptimierung und (als Selbstbestimmung getarnte) Fremdbestimmung führen uns in eine neue Form moderner Versklavung. Unser Elend ist auch verbunden mit dem Elend Anderer. Denn die millisekündliche Gewinnmaximierung hier bestimmt das ungleich größere Elend in vielen anderen Ländern. Der hoffentlich hohe wirtschaftliche Schaden ist uns eine Freude!

Wenn wir den Datenfluss unterbrechen, dann auch dies in voller Absicht. Er ist die Voraussetzung zur Beherrschung durch Überwachung. Wir alle wissen, dass die großen IT-Konzerne und staatlichen Behörden alle verfügbaren Daten sammeln. Und das, damit Menschen und

Gesellschaften in immer größerem Umfang kontrolliert und gesteuert werden. Ein jeder Mensch wird zur Manipulationsmasse von Machtinteressen und zur Zielscheibe der Vermarktung.

Wir sind Zeitzeug_innen der Entstehung einer globalen gesellschaftlichen Totalität der Kontrolle, Überwachung und Steuerung, der Vermessung, Markierung und Ausgrenzung. Edward Snowden hat dies erkannt und gehandelt. Für die (herrschafts-)technisch bedingte Zerstörung der Umwelt und der sozialen Beziehungen werden keine sozialen Lösungen entwickelt, sondern erneut (herrschafts-)technische. Diese technokratische Entwicklung führt in ihrer Machtkonzentration Stück für Stück zu autoritärer Kontrolle. „Abnormalitäten" werden von vorgegebenen „Standards" uneingeschränkt unterscheid- und selektierbar. Die Daten, die das ermöglichen, liefern wir alle täglich in den „sozialen" Netzen, beim bargeldlosen Zahlen, beim Googeln oder bei der Nutzung digitaler Dauerassistenten wie Alexa und Siri. Meldungen und Suchergebnisse sind individuell auf jede_n von uns zugeschnitten und führen uns „bequem" durch den Alltag. Dieses Lenken von Information und Kommunikation heute ist die Grundlage für unsere Steuerbarkeit von morgen. Viele, die zu Beginn des Internets ihre egalitären Hoffnungen stützten auf dessen Möglichkeiten, warnen heute vor der Totalität der Verhältnisse von morgen. Eine moderne Form von Faschismus ist eine der möglichen Varianten dieser drohenden Totalität.

Es ist absehbar: Wenn die Folgen von Umweltzerstörung, Klimawandel und Krieg hier deutlicher spürbar und die Verteilungskämpfe härter werden, dann werden die schlimmsten Alpträume und Dystopien Realität – falls kein revolutionärer Bruch mit den Zuständen gelingt!

Daher sabotieren wir den vermeintlichen Fortschritt.

Wir begreifen unsere Praxis auch als Lehre aus den Erfahrungen des deutschen Faschismus. Wir erkennen eine wachsende Bereitschaft, sich fortschrittsgläubig lenken und fremdbestimmen zu lassen, wir erleben die willigen Helfer, wir spüren die grausame soziale Kälte, wir erahnen den Vernichtungswillen. Er könnte eines Tages viele treffen: den disfunktionalen Rentner, die Kranke, den Geflüchteten, die Arbeitsverweigerer_innen, die Gebärunwillige. Denn das ist der Charakter und das Ausmaß der Möglichkeiten der digitalen „Revolution".

Unger, Lichtenstein, Lepehne – das sind die Namen der Menschen, die von dem Ort unserer Aktion deportiert und ermordet wurden. 1942. Nach Ausschwitz und Riga. An diese Menschen erinnern Stolpersteine, eingelassen auf der Brücke Mörschbrücke, die erinnern helfen sollen. Was hat die Deportation dieser Menschen mit den zwei Meter darunterliegenden Glasfaserkabeln zu tun?

Ein historisches Beispiel, welches die Möglichkeiten entgrenzter digitaler Erfassung für den Faschismus illustriert: Der Ingenieur Herman Hollerith erfand die Lochkarten-Technik, mit der die Volkszählung in Amerika effektiv durchgeführt werden konnte. Zu Zeiten der Nazi-Diktatur hatte IBM ein nahezu weltweites Monopol über diese Technologie und die Produktion der dazu gehörenden Lochkarten. IBM-Chef Watson war persönlich nach Berlin gereist, als seine Deutschlandfiliale (DEHOMAG) den Auftrag an Land gezogen hatte, die Volkszählung 1933 auszuwerten. Vier Monate dauerte die Übertragung der Zählbögen, dann ließ sich in jeder Stadt, Berufsgruppe oder Hausgemeinschaft der Anteil der Jüd_innen ermitteln. Bei der Volksfahndung 1939 wurden Jüd_innen mit dem gleichen Lochkarten-Rechnersystem nach den Kriterien der nazistischen Rassenlehre erfasst.

Dieses Modell wurde wieder und wieder angewandt. In praktisch jedem von den Nazis besetzten Land sammelten deutsche IBM-Tochterunternehmen nationale und „rassische" statistische Informationen für die Nazis, die dann zur Identifizierung von Jüd_innen und anderen Unerwünschten benutzt werden konnten. Diese Lochkarten-Technologie war maßgeblich für die Effizienz der Deportation. Während mit einem nahezu ungehinderten Erfassungssystem etwa in Holland 73% der Jüd_innen deportiert wurden, waren es aber in Frankreich 25%. Einer der vielen Faktoren, die das unterschiedliche Schicksal der Jüd_innen beider Länder beeinflussten, war die Tatsache, dass es dem Widerstand in Frankreich gelungen war, die Lochkarten-Registrierung massiv zu sabotieren.

Es gab Hollerith-Abteilungen in fast jedem Konzentrationslager, sie dienten der Registrierung der Ankommenden, der Zuteilung von SklavenZwangsarbeit und der Buchführung über die toten Gefangenen. Ohne die IBM-Maschinerie, den IBM-Service, sowie die Lieferung der Kartenrohlinge hätten die Nazilagerverwaltungen die erreichten Häftlingszahlen nicht so „effektiv" handhaben können.

Die Stolpersteine mahnen heute. Mit dem historischen Rückblick lohnt ein Ausflug in die alarmierend gegenwärtige Zukunft. Das in China aktuell erprobte Herrschaftsprojekt „Sesam" versteht sich als Dauer-Erfassungssystem aller Informationen, die über jede_n einzelne_n zu finden sind. Eingeführt über verlockende Bonusprogramme ist die derzeit noch freiwillige Teilnahme groß. Alle Daten, die staatliche Behörden über jede_n einzelne_n beisteuern können, alle Daten über Bezahlvorgänge jedes einzelnen und alles, was das Auswertungsprogramm in sozialen Netzen über jede_n einzelne_n findet, wird in einem Zahlwert – dem „social score" – zusammengefasst. Insbesondere hängt der Score jedes einzelnen mit ab von der Bewertung seiner „sozialen Freunde". Bei hohem Score winken Vergünstigungen

bei Krediten, Mobilität und Versicherungen. Umgekehrt bedeutet dies soziale und materielle Ausgrenzung. Erst kürzlich wurde der Zugang zu öffentlichen Verkehrsmitteln für Menschen mit zu niedrigem Score beschränkt. Ab 2020 plant China die verpflichtende Teilnahme an einem Nachfolger von Sesam. Dann sollen unter anderem Chancen auf Arbeit, Bildung und Gesundheit von diesem Score abhängen.

Um Missverständnissen vorzubeugen: Die Entwicklung und Umsetzung solcher sozialer Scoring-Systeme ist nicht automatisch faschistoid, aber allein ihrem Anspruch nach totalitär. Die darin verwirklichte Idee der vielstufigen Kategorisierung von Menschen und der erwünschten Verhaltenssteuerung bietet hervorragende Voraussetzungen für eine modernisierte Form der Faschisierung. Für Selektionen und Vernichtung.

Wir enden mit Fragen: Wann wäre der historische Zeitpunkt noch gegeben gewesen, sich gegen den deutschen Faschismus zu erheben? Wann war der Zeitpunkt verpasst? Was heißt das für heute?

Unser Beitrag – einer von vielen.

Aus gegebenem Anlass: Deutsche Waffen und türkisches Militär raus aus Efrin! Die Verantwortlichen des Krieges in Efrin sitzen auch in Deutschland. Sie sind zu finden."

Vulkangruppe NetzHerrschaft zerreißen

Deutschland ohne Netz - Kein Twitter, WhatsApp und Facebook

9.4.2018 – Nutzer in ganz Deutschland konnten in der Nacht zu Dienstag über Stunden nicht oder nur verlangsamt auf Twitter, Facebook, Whatsapp, Youtube oder Spotify zugreifen. Serien bei Netflix streamten zögerlich oder überhaupt nicht. Live-TV-Übertragungen von RTL, Pro Sieben und VOX hingen sich auf, die Deutsche Bahn konnte auf ihrer Homepage keine Auskünfte erteilen. Das Internet war lahmgelegt.

Grund für die Drosselung oder den kompletten Stillstand auf zahlreichen Webseiten war ein Stromausfall in einem Rechenzentrum in Frankfurt-Fechenheim. Hier – nicht etwa im US-amerikanischen Silicon Valley - liegt der gemessen am Datenverkehr größte Internetknoten der Welt namens DE-CIX. Pro Sekunde werden über seine Rechner 6,4 Terabit Daten ausgetauscht, das sind ins Analoge umgerechnet DIN-A-4-Seiten, beschrieben und gestapelt, in 140 Kilometer Höhe. Betrieben wird der Knotenpunkt von dem Unternehmen Deutsche Commercial Internet Exchange (DE-CIX), einer Tochter des größten europäischen Internetwirtschaftsverbands eco.

Knotenpunkte wie DE-CIX ermöglichen Internet-Providern und Unternehmen, die Inhalte im Web liefern, kostenneutralen und schnellen Datenaustausch. So sparen Firmen sich den teuren internationalen Datenversand, außerdem können die Daten über kürzere Strecken schneller fließen – Nutzer profitieren also von einer sehr viel besseren Performanz. Je mehr Knotenpunkte, desto schneller das Netz – für die Branche, in der jede Millisekunde zählt, sind sie einer der wichtigsten Innovationstreiber.

Mehr als 850 Internetprovider und -unternehmen aus 21 Ländern sind Kunden bei DE-CIX, darunter Vodafone, Kabel Deutschland, die Deutsche Telekom, Facebook und Twitter. Hinter ihnen stehen Millionen von Nutzern – nicht nur in Deutschland, sondern in ganz Europa. Die bekamen Montagnacht zu spüren, was ein Fehler im System bewirken kann: In einem von 21 Rechenzentren, die DE-CIX in Frankfurt nutzt, fiel gegen 21 Uhr für rund zwei Stunden der Strom aus. Gegen 5 Uhr am Dienstagmorgen sei es zu weiteren Ausfällen gekommen, teilt DE-CIX mit. 220 Kunden waren nach Aussage des Unternehmens von der Störung betroffen. Wie viele Endnutzer, bleibt unklar. Mittlerweile sollen alle Systeme wieder stabil laufen.

Das betroffene Rechenzentrum FRA 5 wird vom Dienstleister Interxion betrieben, den Strom liefert das Frankfurter Energieunternehmen Mainova. Seitens der Mainova habe es keine Störung gegeben, sagte Unternehmenssprecher Sven Birgmeier. „Das Problem liegt kundenseitig." Interxion spricht bisher lediglich von einer „technischen Störung", man arbeite an Ursachenforschung und Problemhebung, teilte Sprecherin Mareike Jacobshagen mit.

Lässt sich das Internet in Deutschland also so leicht abschalten? Nein, sagt Thomas King, Chief Innovation Officer bei DE-CIX. Eigentlich seien die Rechenzentren des Internetknotens durch ein sogenanntes redundantes System gleich mehrfach gegen Stromausfälle gesichert. „Alle Geräte haben zwei unabhängige Stromleitungen und – Stecker. Falls ein Stromversorger ausfällt, greift der andere. Fällt auch der aus, können wir Strom über Batterien und Dieselgeneratoren liefern."

Dasselbe Sicherheitssystem sollte allerdings auch Dienstleister Interxion haben. Es ist Voraussetzung, damit DE-CIX sich in Rechenzentren einmietet. Nachdem die primäre Stromversorgung ausgefallen sei, sollte eigentlich nach zwei Sekunden ein Dieselgenerator als sekundäre Stromversorgung anspringen. Doch die technische Störung habe sich auch auf diesen Generator übertragen, und auf den nächsten, „wie bei Dominosteinen", sagte Interxion-Sprecherin Jacobshagen. „Unsere Techniker arbeiten derzeit mit Hochdruck daran, die Ursache des Problems herauszufinden", sagte sie

Frankfurter Rundschau 10.4.2018

Sabotage von Funkmasten in Europa

Wir drucken diese Erklärung ab, obwohl die im Autonomen Blättchen#30 (September 2017) gefundene Übersetzung aus dem Französischen schwer lesbar ist.

„Wenn Stille beängstigend ist, dann vielleicht weil wir durch die Abwesenheit von gewohnten Geräuschen dazu neigen uns selbst abzulehnen. Wenn wir in die stille Dunkelheit vordringen ist es nicht unüblich zu uns selbst zu sprechen, eine Melodie zu pfeifen oder laut nachzudenken um nicht von der Angst aufgefressen zu werden. Dies ist nicht einfach und vielleicht bedarf es sogar ein wenig Übung da unsere Gehirne konditioniert wurden Stille als Gefahr und Dunkelheit als Risiko zu identifizieren. Es ist die Qual die die Leere provoziert, es ist das Gefühl am Rande eines Abgrunds zu stehen und nicht in der Lage zu sein unsere Augen von dem Abgrund, der sich vor uns auftut, abzuwenden. Dennoch sind es auch diese Momente in denen mensch dazu neigt näher zu sich selbst zu seien, ohne eine Vermittler*in, mit Geistesgegenwart und wesentlich bestimmteren Emotionen.

Es is schwierig in der modernen Welt Stille oder Dunkelheit zu finden. Industrielle Geräusche begleiten uns, permanent senden die Apparate ihre elektronischen Geräusche aus, und selbst wenn nicht, dann gibt es fast immer jemanden der*die das Nichts mit Geschwätz füllen wird, welches genauso undurchdringbar wie oberflächlich ist. Heutzutage ist die Angst vor dem Nichts, die Qual der Stille, erhöht durch die permanente Konnektivität. Niemals allein, niemals von Stille umgeben, niemals vorm Abgrund und somit niemals von Angesicht zu Angesicht mit uns selbst. Rufe und Stimmen aus dem „Inneren", das ganze Universum von Vorstellungskraft, Bewusstsein, Sensibilität und Reflektion werden zum Verstummen gebracht, ignoriert und platt gedrückt, um ersetzt zu werden von einem Bombardement aus Informationen, E-Mails, Terminen, Verbraucherwarnungen und Erinnerungen. Somit vervollständigt die moderne Welt das innere Universum des Individuums.

Mit einem ausgelöschtem Inneren wird sich das menschliche Wesen in dem idealen Zustand wieder finden um die Sklaverei zu akzeptieren und mehr noch, es wird die Sklaverei umarmen, ohne die Fähigkeit zu haben zu erkennen wo es sich befindet.

Gefangen im Netz

All dies ist allerdings nicht neu. Die Geschichte der Unterdrückung hat nicht mit dem Smartphone begonnen. Noch vor gar nicht allzu langer Zeit wurde der menschliche Geist hauptsächlich mittels einer Galaxis von Camps konditioniert. Das Fabrik-Camp, des Erziehungscamp(was die Schule ist), das Kontrollcamp (was die Autorität der Familie ist) und die Kultstätten. Dennoch, gab es trotz der Verwobenheit all dieser Herrschaftsstrukturen immer noch, relativ gesehen, viel Leere. Es war dieses Nichts das die Revolte in den Camps befeuerte und umgekehrt. Die Augen der meuternden Gefangenen sind dennoch vom Horizont jenseits der Mauern gefesselt, wobei es nicht darauf ankommt ob uns ihre Vorstellung des Horizonts zufriedenstellt oder nicht.

Obwohl die verschiedenen Arten von Camps gewiss nicht verschwunden sind, zielt die permanente kapitalistische und staatliche Restrukturierung, besonders durch die weit verbreitete zunehmende Einführung von Technologie, in ihrer Totalität. jenseits von der erhöhten Ausbeutung und Kontrolle, auf die Beseitigung jeder Art von Leere. Der Spruch der permanenten Konnektivität ist der Kern dieser tödlichen Symphonie. Online sind wir immer ein bisschen auf der Arbeit, ein bisschen bei der Familie, ein bisschen im Supermarkt, ein bisschen beim Konzert. Connected ist mensch ständig den Anordnungen der Macht, den Vorladungen zu konsumieren und den Augen der Kontrolle, ausgeliefert. Wir stehen dem Kapital gänzlich zur Verfügung, wir sind die Sklaven welche unsichtbare Ketten tragen.

Jemand hat mal gesagt dass wenn die Gesellschaft ein Freiluftgefängnis ist, dann sind es diese Antennen und diese Kommunikationsrelais, die überall gegen den blauen Himmel kontrastieren, die die modernen Gefängniszellen darstellen und die Glasfaserleitungen und die Elektrokabel der Stacheldraht. In der Tat scheint es für jene, die die davon träumen die Reproduktion der Herrschaft zu stoppen, unerlässlich zu sein dass sie auf eine andere Weise und woanders hinschauen können. Es ist zwar nicht so dass die örtliche Polizeistation nicht länger die Aufmerksamkeit der Feinde jeglicher Autorität auf sich ziehen sollte oder dass die Fenster der Bank es nicht länger verdient haben eingeschmissen zu werden oder dass das Gericht nicht bekommen sollte was es verdient; aber es stimmt halt auch dass Herrschaft eine Unmenge von relativ kleinen und ungeschützten Konstruktionen auf der Erde ausgebreitet hat; von welchen mehr und mehr, wenn nicht sogar alles abhängt. Es ist in diesen kleinen Dingen in denen sich das unsichtbare Netz materialisiert, welches uns umschließt, und welches es dem Staat und dem Kapital ermöglicht sich zu restrukturieren. Es sind diese Adern der Herrschaft, welche die Ausbeutung und Unterdrückung bewässern, die angegriffen werden können und womit die technologischen Prothesen und ihr versklavtes Geschwätz zum Schweigen gebracht werden können.

Dies ist was geschah als durch ein Feuer die technischen Gerätschaften und Kabel des Fernsehsenders France 3 am 21. April 2017 in Vanves (Hauts-Seines), Frankreich, zerstört wurden und die Übertragung unterbrochen war. Dies ist was geschah als anonyme Hände in Morbihan, Frankreich, am 4. Mai, fünfzehn Minuten vor dem Präsidenten Fernsehduell, das Orange-Telefonkabel durchtrennten was tausende von Zuschauer*innen und hunderte von Unternehmen ihrer Konnektivität beraubte. Dies ist was geschah als am 7. Juni, einen Tag nach der Verurteilung einer anarchistischen Gefährtin wegen Bankraubs durch das Gericht von Aachen, auf dem Monte Finonchio in Trentino, Italien, mehrere Sender und Verteilerkästen für Radio, Fernsehen, Mobilfunk und Militärfunk durch Feuer zerstört wurden. Dies ist was geschah als am 12. Juni in Hamburg eine U-Bahnstation in Brand gesetzt wurde. (A.d.Ü.: Wahrscheinlich ist eine Mobilfunkantenne nahe einer U-Bahnstation gemeint). Dies ist was ein paar Tage später in Piégros-la-Clastre, Frankreich, geschah als Nachteulen eine Fernsehsendeanlage und eine Mobilfunkantenne in Brand setzten und später verkündeten dass „die Masten die überall wachsen sind sensible und verwundbare Punkte da hier der Fluß konzentriert wird und es ein paar Liter Benzin genügen um sie ernsthaft zu beschädigen". Am 23. Juni wurde in Vilvoorde in Belgien eine Sendeantenne durch ein freiwilliges Feuer zerstört.

Diese wenigen Beispiele, wahrscheinlich weit davon entfernt vollständig zu sein und lediglich aus einigen Wochen rausgesucht, zeigen das die Unterbrechung überall möglich ist. Es muss auch gesagt werden dass wir, anders als die Autoritären welche sich die Umwälzung der Welt nur mithilfe der Erstürmung der Tempel der Macht und durch das Organisieren von großen Massen vorstellen können, was eine unmögliche Symmetrie mit einem viel besser ausgestatten Feind wäre; als Anarchist*innen die Beweglichkeit kleiner Gruppen wichtig finden, die Fähigkeiten des Individuums, das Ausbreiten von [unseren] Feindseligkeiten mehr als ihre Zentralisierung und die Beziehung zwischen Individuen durch Gegenseitigkeit, Vertrauen und Wissen. Diese Art des Organisierens erscheint uns wesentlich interessanter um den, aufgrund der Verwobenheit aller seiner Strukturen immer mächtigeren Feind, anzugreifen. Konfrontiert mit der Ausbreitung von einer Unmenge kleiner Sendeeinheiten, ist nichts angebrachter als mit einer Unzahl, autonom agierender, kleiner Gruppen, welche die Möglichkeit besitzen sich zu koordinieren, wenn es sinnvoll ist, die alte Kunst der Sabotage gegen die Adern der Macht zu praktizieren. In der Stille die sie Maschinen aufzwingen, in der Störung die sie der „wirklichen Zeit" von Unterdrückung hinzufügen, werden wir uns selbst in Angesicht zu Angesicht mit uns selbst wieder finden. Dies ist eine unumgängliche Voraussetzung für eine

Praxis der Freiheit."

anonym

übersetzte Erklärung von *cettesemaine.info/breves*

Vom Kurzschluss zum sozialen Blackout

„Der folgende Text wurde anlässlich eines anarchistischen Treffens im Jahr 2012 verfasst, hat aber seitdem eher an Bedeutung gewonnen.

Die Strukturen der Herrschaft und der Ausbeutung bleiben nicht immer gleich. Sie ändern sich und verwandeln sich im Laufe der Geschichte, aus Gründen, die mit ihrem Hang zur Selbsterhaltung zusammenhängen und folglich einem direkten und unbestreitbaren Verhältnis zur sozialen Konfliktualität stehen. Wenn man bis in die 70er Jahre starke Spannungen und bedeutende Turbulenzen im produktiven Bereich wahrnehmen konnte, die sich logi-

scherweise auf dem Gebiet der grossen Fabriken konzentrierten, oder zumindest mit allen Blicken dahin gerichtet, so scheint sich die Konfliktualität heute, im alten Europa, in andere Bereiche „verschoben" zu haben.

Was nicht daran hindert, dass die Ausbeutung fortdauert, bei der Arbeit sowie anderswo, sicherlich aber auf andere Weise als zuvor, sicherlich auf „dezentralisiertere" Weise, sicherlich besser gegen die eventuellen Infragestellungen aus dem „Innern" geschützt.

Heute geht es im Grunde darum, die Analyse der Strukturen der Macht und der Ausbeutung weiterzuführen, sie zu aktualisieren und zu vertiefen. Die alten Modelle wurden bereits verlassen, auch wenn es noch immer Leute gibt, die weiterhin an die Konstituierung des „Proletariats" als Kraft und an seine Bekräftigung innerhalb der produktiven Sphäre glauben. Eine solche „neue" Analyse wurde bereits vor einigen Jahrzehnten begonnen, heute aber scheint es, dass sich ein zusätzlicher Schritt aufdrängt.

Die Grundlage der Ausbeutung, oder besser, ihrer Selbsterhaltung, liegt in der sozialen Reproduktion. Es gibt nicht nur die offensichtliche Suche nach Macht und Akkumulation, sonder auch die Konflikte, die im Innern ihrer Logik untergebracht sind, reproduzieren die Ordnung der Dinge. Festzustellen ist, dass der Arbeiter die Ausbeutung produziert und dass die Ausbeutung den Arbeiter reproduziert. Ebenso wie der Bürger die Macht produziert und die Macht den Bürger reproduziert. Die Möglichkeiten, um diesen Teufelskreis zu durchbrechen, befinden sich nicht mehr da, wo die alten Bücher der revolutionären Bewegung sie verorteten, und auch nicht in einer neuen Version eines langsamen und endlosen Prozesses der Bewusstwerdung, sondern anderswo. Und es ist dieses aufständische Anderswo, das wir analysieren und ausprobieren müssen.

Die Ausbeutung und folglich die soziale Reproduktion folgen nicht mehr konzentrationshaften Linien, wie sie es in der Vergangenheit tun konnten. Die grossen Industriekomplexe mit ihrer Kreierung von Arbeitern, die fähig sind, sich untereinander wiederzuerkennen, sind vorbei; die grossen Kampfverbände, die fähig sind, tausende Leute zu begeistern und zu mobilisieren, sind vorbei. Die Ausbeutung hat sich heute so sehr diversifiziert und dezentralisiert, dass sie das Aufkommen eines kollektiven Subjektes, eines „Proletariats" verunmöglicht, selbstverständlich ohne dass dies bedeutet, dass es keine „Proletarier" mehr gäbe. Die Ausbeutung strebt es nicht mehr an, sich in einer grossen Struktur zu konzentrieren, sondern, auf dem ganzen Gebiet kleine Strukturen zu verstreuen, die alle durch Energie- und Kommunikationsnetze verbunden sind, welche die Produktion unter ständigem Fluss und eine dichte Reproduktion der Herrschaft ermöglichen. Wenn die heutige Gesellschaft einem grossen Gefängnis unter offenem Himmel gleicht, dann wären seine Stacheldrähte aus Glasfaser und seine Wachtürme wären vielmehr Kommunikationsantennen.

Wenn wir diese Entwicklung unterstreichen, dann nicht aus blosser Neugierde und Lust daran, zu verstehen, wieso die soziale Konfliktualität heute nicht mehr dem alten, gut geordneten Schema des Klassenkampfes zwischen Proletariat und Bourgeoisie folgt, den beiden gut indentifizierbaren Blöcken, die sich um eine Festung streiten, sondern, um Interventionswege zu entdecken, Punkte, an denen es möglich ist, die Ausbeutung, und somit die soziale Reproduktion, anzugreifen. Diese Wege finden sich unserer Meinung nach unter anderem in den Infrastrukturen, von denen die Wirtschaft und die Macht abhängen. Diese dezentralisierte und höchst komplex gewordene Infrastruktur hat die neuen Formen der Ausbeutung ermöglicht (es genügt, an die heutige Notwendigkeit zu denken, in jedem Moment per Mobiltelefon erreichbar zu sein, in der Logik der Flexibilisierung der Arbeit), und in ihr ist es folglich, wo die Ausbeutung von heute angegriffen werden kann. Die Glasfaserkabel, die Transportnetze, die Energieversorgung, die Kommunikationsinfrastrukturen wie die Mobilfunkantennen: dies ist ein ganzer Interventionsbereich, der aufgrund seiner Natur unkontrollierbar ist, in dem es kein Zentrum mehr gibt, dass es zu erobern gilt, und keine Position mehr gibt, die es zu halten gilt, in dem die Dezentralisierung, durch die Logik der Dinge, eine dezentralisierte, informelle, aus kleinen Gruppen bestehende, auf den Angriff abzielende Organisation impliziert.

Viele Personen haben die Verletzlichkeit dieser Infrastrukturen aufgezeigt, aber es gibt noch viel Klärungs- und Aufzeigearbeit zu machen. Man könnte nur schon damit beginnen, die praktischen Ratschläge zu empfangen und zu vertiefen, die aus der zeitgenössischen Konfliktualität hervorkommen. Anstatt sich auf die Konfrontationen mit der Polizei zu fokussieren, würde man besser daran tun, zu betrachten, wie in gewissen Aufruhren in den Metropolen und ihren Peripherien die Infrastruktur angegriffen wird: Sabotage der öffentlichen Beleuchtung, Brandstiftungen von Generatoren und Elektrotransformatoren, Sabotagen der Transportachsen der Eisenbahn oder des öffentlichen Verkehrsnetzes. Eine aktuelle Analyse der Metropole könnte beispielsweise die Wichtigkeit der Transporte (von Menschen, von Waren, von Informationen) nicht unbeachtet lassen. Aber die Aufklärungsarbeit kann sich nicht darauf beschränken. Wir brauchen präzise Angaben, präzise Analysen und präzise technische Kenntnisse.

Selbstverständlich hat die Möglichkeit und die Notwendigkeit des verstreuten Angriffs gegen die Infrastrukturen der Macht wenig Sinn, wenn sie nicht in eine breitere Projektualität eingeschrieben ist. Auch wenn es bestimmt

immer gut und angebracht ist, zu sabotieren, darf man nicht vergessen, dass es bei allem ein Vorher, ein Während und ein Nachher gibt. Wenn Brüche in der Normalität, in der sozialen Reproduktion, Möglichkeiten bieten, dann müssen diese bereits im Voraus erdacht werden. Was tun im Falle einer Kappung der Elektrizität? Was tun, wenn die öffentlichen Transportmittel nicht mehr funktionieren und inmitten einer Stadt ein unglaubliches Chaos erzeugen? Abgesehen davon, dürfte diese ganze Frage der Infrastruktur nicht als etwas betrachtet werden, das von den anderen Konfrontationsbereichen getrennt ist. Sie kann freilich in jedes beliebige Kampfprojekt integriert werden. Wenn die Konfliktualität heute ungleich und verstreut ist, ohne ein „zentrales" Terrain, dann geht es nicht darum, wieder eine Zentralität zu finden oder zu konstruieren, die die verstreuten Feindlichkeiten in einem einzigen revolutionären Projekt vereinigen würde, sondern darum, zwischen den verschiedenen Konfliktualitäten Brücken aufzubauen und zu schlagen. Ein präziser Angriff gegen die Infrastrukturen hat beispielsweise immer Konsequenzen, die breiter sind als ein Aspekt der Macht. In einem Aufruhr die Beleuchtung eines Viertels zu kappen, ist nicht nur eine Frage davon, die Vorstosse der Ordnungskräfte zu erschweren, sondern wird Echos haben, die weit über jede technische Erwägung des Moments hinausgehen. Man lebt nicht gleich, wenn es dunkel ist. Dieser Aspekt ist noch viel eklatanter im Bezug auf das Energienetz; wo die Konsequenzen oft weit über das erste, vorgestellte Ziel hinausgehen werden.

Zweitens geht es nicht darum, diese Überlegungen und Vorschläge als Vorwände für eine grosse Technikerverschwörung zu nehmen, die die Städte ins Dunkel, oder vielmehr, wie es heute der Fall wäre, in ein Informations- und Kommunikations-Blackout tauchen würde. Was es auszuarbeiten gilt, das sind Projektualitäten, und seien es auch bescheidene, die all jenen diese Angriffsmöglichkeit aufzeigen, die auf einer radikalen Grundlage kämpfen wollen, und somit nicht nur den Revolutionären. Die Frage auf eine militaristische Weise anzugehen, erneut die Zentralisierung gegenüber der Verstreuung zu preisen, über alles in Sachen „Effizienz" nachzudenken, zeugt davon, von dem, was gesagt wurde, rein gar nichts verstanden zu haben. Was heute „neu" ist, das ist beispielsweise nicht die Möglichkeit, eine Elektrozentrale in Angriff zu nehmen, um die Stadt ins Dunkel zu tauchen, sondern die Möglichkeit, überall das integrierte und verstreute Stromnetzwerk in Angriff zu nehmen. Diese Möglichkeit erfordert keine grossen Organisationen, und auch keine Formalisierungen der subversiven Spannung, sie ermöglicht direkte, einfache und leicht zu reproduzierende Angriffe.

Wenn es stimmt, dass die Stabilität der etablierten Ordnung seit einigen Jahren am Bröckeln ist, wenn es stimmt, dass das Verschwinden der alten Kampfmodelle und der Vermittlungsorganisationen von neuen Formen der sozialen Konfliktualität gefolgt wird, die viel weniger kontrollierbar und viel wilder sind, dann müssten wir unsere theoretische und praktische Aufmerksamkeit auf das richten, was dazu beitragen könnte, diesen unkontrollierbaren Sumpf auszuweiten. In diesem Sumpf kann uns nichts garantieren, dass es die anarchistischen Ideen und die Freiheit sein werden, die den Sieg davon tragen, was aber sicher ist, das ist, dass er für diese Wünsche bereits einen viel fruchtbareren Boden bietet."

Einige Untergräber des sozialen Gebäudes

Quelle: Autonomes Blättchen #30 (September 2017)

Ein Funkmast brennt

Dokumentation: Berlin, Juni 2018

„Die Restrukturierung der Macht durch die Digitalisierung befindet sich in vollem Gange. Kaum etwas, das in diesem Prozess an seinem Platz bleibt, dass sich nicht durch ein „smart" im Namen ergänzen lässt und so einen neuen Ort in der Welt bekommt. Alles wird vernetzt. Kameras, Sensoren und Chips senden unentwegt und lassen die Dinge kommunizieren. „Big Data" ist die Währung von morgen. Selbst unsere Beziehungen, unser Handeln und Denken ist permanent dem digitalen Zugriff ausgesetzt. Auf Informationen reduziert füttern wir so die Algorithmen der Maschinen, die auch das Zukünftige beherrsch- und steuerbar machen sollen.

Dabei fällt es nicht immer leicht, bei dem rasenden Tempo in dem sich der technologische Angriff ausweitet und ein Netz der Herrschaft um uns spannt, an der Möglichkeit der Zerstörung dieses Systems festzuhalten. Um so wichtiger sind dafür die Momente des Gegenangriffs, um die Ohnmacht, die sich angesichts der aktuellen Entwicklungen breit macht, zurück zu weisen. So freut es uns umso mehr, dass auch in Berlin immer wieder unversöhnliche Antworten auf das Elend, das die Kolonialisierung der Welt durch die techno-industrielle Vorherr-

schaft produziert, gefunden werden. Im Zusammenhang mit dem geplanten Google-Campus in Kreuzberg hat sich ein Kampf entwickelt, der nicht nur auf den Tech-Giganten und sein Universum, sondern auch auf das Soziale abzielt. Selbstorganisierung, direkte Kommunikation und die Wirkungskraft des Angriffs sind dabei die Mittel der Wahl. Verschiedenste Sabotageaktionen wie zuletzt Ende März durch die „Vulkangruppe NetzHerrschaft zerreißen" haben gezeigt, das die Infrastruktur der Warenströme, Kommunikations- und Datennetze verletzbar ist und durch Brandlegungen an Kabeln und Funkantennen empfindlich gestört werden kann. Aber auch andere Akteure der Smartifizierung der Stadt und des Lebens sind zum Ziel der Wut geworden, wie die abgefackelten Amazon-Fahrzeuge, die Mollis auf die Start-Up-Factory, die Angriffe auf Zalando oder den Technologiepark Humboldthain etc. zeigen. Wir wollen diese Konflikte mit unserem Beitrag weiter befeuern und haben uns dafür einige altbekannte Player rausgesucht, die aktiv daran arbeiten, das Netz der Herrschaft und Kontrolle auszubauen und zu optimieren.

Deshalb haben wir in der Nacht zum vierzehnten Juni im Tiergarten, kurz vor Beginn der dortigen Fanmeile, Kabel und Schaltkästen einer Funkantenne von Vodafone in Brand gesetzt. Diese Antenne wird neben dem Mobilfunk auch für den BOS-Funk der Bullen und Behörden genutzt. Wir sind optimistisch mit unserem Eingriff zumindest dieser Antenne eine Sendepause gegönnt, und so für einen Moment der Funkstille gesorgt zu haben. Der Bullenticker schweigt dazu, womöglich ist diese Info auf dem Weg zur Zentrale in den verkohlten Kabel, die nun die Anlage schmücken, hängen geblieben.

In der Nacht zum fünfzehnten Juni haben wir den Fuhrpark der Deutsche Bahn in der Kaskelstraße abgefackelt und in der Nacht zum neunzehnten Juni haben wir Brandsätze unter den Autos der Telekom in der Sewanstraße platziert, und so weitere sechs Fahrzeuge auf den Schrottplatz befördert. Mit diesen Angriffen zielen wir auf einige der großen Netzbetreiber Deutschlands, die mit Funkantennen, Glasfaserkabeln und dem Schienennetz wichtige Grundpfeiler der Waren- und Datenströme bilden. Diese sind für das Funktionieren des Kapitalismus unverzichtbar. Alle drei Konzerne haben sich aber weit mehr auf die Fahne geschrieben als nur die Infrastruktur zu stellen. Sie sind mit ihren technologischen Entwicklungen in den Bereichen Überwachung, Kontrolle, Internet der Dinge (IoT), Industrie 4.0, Smart City, Smart Home etc. eine treibende Kraft in der Neuorganisierung der Herrschaft im kybernetischen Zeitalter.

Mit diesen Taten senden wir Rauchzeichen an alle Gefangenen des sozialen Krieges und an diejenigen, die sich vor dem Zugriff der Schergen auf der Flucht befinden. Spezielle Grüße gehen an Lisa, Thomas, Nero, Isa, UP3 und die G20-Gefangenen.

MOBILFUNK UND ÖFFENTLICHER VERKEHR IM DIENSTE DER MACHT

Medien, Politiker*Innen und Lobbyist*Innen schüren seit Jahren eine Stimmung der Angst. Vor dem Fremden, den Geflüchteten, dem Terrorismus. Damit einher geht der Ruf nach Autorität. Ein neues Polizeigesetz jagt das Andere. Die Entwickler von Sicherheitstechnologien freut das, denn mit der Angst lässt sich nicht nur Politik machen, sondern auch einen Haufen Geld verdienen. So verwundert es nicht, dass die etablierten Großkonzerne hier ganz vorne mitmischen und im Sinne der Herrschaft unerbittlich an der Aufrechterhaltung der bestehenden Ordnung mitwirken.

Die Telekom ist das größte Telekommunikationsunternehmen Europas und betreibt technische Netze für Telefon, Mobilfunk, Datentransfer und Onlinedienste. Neben Deutschland hat das Unternehmen in vierzehn weiteren europäischen Staaten Tochtergesellschaften oder ist beteiligt an Mobilfunk- und Festnetzanbietern. Mit dem international operierenden Tochterunternehmen T-Systems ist der Konzern einer der weltweit führenden Dienstleister für Informations- und Kommunikationstechnologie und richtet sich an Kunden*Innen der Großindustrie, dem Finanzsektor, der Energiebranche und der öffentlichen Verwaltung und Sicherheit.

Für Polizei, Militär und sonstige Sicherheitsbehörden bietet T-Systems allumfassende Lösungen und Informationstechnologie. Unter dem Titel „PLX" entwickelt die Telekom unter anderem ein Informations- und Fahndungssystem für die Bullen, in dem alle relevanten Meldeprozesse, wie z.B. erkennungsdienstliche Behandlungen, Haftdaten, Kriminalakten-Nachweise etc. integriert sind. So sollen alle Abläufe in der Vorgangsbearbeitung, von der Ersterfassung bis zur Abgabe der Vorgänge an die Justiz, unterstützt werden.

Ergänzend dazu bietet T-Systems Technik für einen „Interaktiven Funkstreifenwagen (IfuStw)". Ein mobiler polizeilicher Arbeitsplatz durch Multifunktions-PC's im Fahrzeug, welcher die volle Integration in die jeweils bestehende polizeiliche Infra- und Kommunikationsstruktur erlaubt. Diese Verknüpfungen sollen die Reaktions- und Interventionszeiten verkürzen und gleichzeitig eine beweissichere Dokumentation durch Videoaufzeichnung erleichtern.

Auch Vodafone, die deutsche Tochtergesellschaft der britischen Vodafone Group und zweitgrößter Mobilfunkan-

bieter Deutschlands, wirbt für mehr Sicherheit. So liefert Vodafone nicht nur einen Messenger-Dienst für die bayrischen Bullen oder Bodycams für die Bundespolizei, sondern entwickelt auch smarte Drohnen. Diese, mit Bordkamera und SIM-Karte für den LTE-Funk ausgerüsteten Drohnen, liefert und analysiert Videomaterial in Echtzeit. Damit sollen bei Großveranstaltungen z.B. Personen gezählt oder Menschenströme beobachtet und gelenkt werden. Aber auch Verkehrsüberwachung und Kennzeichenerkennung sind Teil der Aufgaben solcher Anwendungen. Das diese Technik beliebig durch weitere Überwachungssoftware, wie z.B. Gesichtserkennung ergänzt werden kann, liegt dabei auf der Hand.

Mit solchen und ähnlichen Produkten sind Telekom und Vodafone, neben vielen anderen Unternehmen aus der Sicherheitsindustrie, seit vielen Jahren als Aussteller auf Messen wie dem europäischen Polizeikongress vertreten, wo sie um das Interesse ihrer Kunden*Innen aus den Bereichen Militär, Polizei, Geheimdiensten und Grenzschutz konkurrieren.

Die Deutsche Bahn hingegen, als Betreiber von Bahnhöfen und dem deutschen Streckennetz, kommt hier eher die Rolle des Abnehmers solcher Technologien zu. Gleichzeitig bietet die Infrastruktur des Konzerns aber auch ein riesiges Experimentierfeld, um unter realen Bedingungen den Einsatz neuester Überwachungstechnologien zu testen. Der wohl populärste Feldversuch der Deutschen Bahn, in Kooperation mit der Bundespolizei, dem BKA und dem Bundesinnenministerium, läuft zur Zeit am Bahnhof Südkreuz in Berlin. Dort sollen intelligente Videokameras mit eingebauter Gesichtserkennungs-Software automatisiert Personen erkennen, verfolgen und auffälliges Verhalten melden. Mit solchen Projekten legen sie den Grundstein für eine totalitäre Kontrollgesellschaft. Selbstverständlich werden bei positiven Ergebnis für die Betreiber*Innen, solche Technologien auch an anderen Orten zum Einsatz kommen. Bereits jetzt werden 900 Bahnhöfe der Deutschen Bahn mit 6000 Videokameras überwacht, welche aufgerüstet durch intelligente Überwachungssoftware, ganz im Sinne des Innenministers, ein fast lückenloses Netz der personalisierten Verfolgung und Kontrolle im öffentlichen Verkehr ermöglichen würden. So spielt dieser Konzern eine Schlüsselrolle bei der Umsetzung neuer Überwachungs- und Verfolgungsparagraphen, wie sie im neuen bayrischen Polizeiaufgabengesetz (PAG) vorkommen.

VOM INTERNET DER DINGE ZUR SMART CITY UND ZURÜCK

Das Internet der Dinge gilt als größtes Wachstumssegment im Mobilfunk. Experten*Innen rechnen mit bis zu 50 Milliarden miteinander vernetzten Geräten weltweit. Dies setzt leistungsstarke Netze, die schnell große Datenmengen austauschen können, voraus. Deshalb investieren die Mobilfunkanbieter Unmengen an Geld in die Infrastruktur von Glasfaserkabeln, Narrowband und 5G, um den aktuellen und zukünftigen Anforderung gerecht zu werden. Gleichzeitig arbeiten diese aktiv an verschiedensten europäischen Smart City Projekten mit und entwickeln allerlei Dinge, welche die total vernetzte Welt zur Realität werden lassen soll.

Die Telekom betreibt dazu einen sogenannten „Hub:raum" als Inkubator für Start-ups und führt Programme unter dem Titel „Smart City Lab/T-Labs", mit denen die digitale Effizienz der Städte vorangetrieben werden soll. Smarte Transportlösungen, Smart Parking, Smart Electric Vehicle Charging, Verkehrs- und Passagiermanagementsysteme, Smart Waste Management, Smart Lighting, Smart Metering und Smart Public Safety sind nur einige Stichworte, die zeigen, wie umfassend die Pläne der Konzerne sind, um Dinge zu schaffen, welche Informationen produzieren und sich so in die Wertschöpfungskette integrieren lassen. Ziel der Telekom ist es führender Anbieter in Europa für Smart City Lösungen zu sein. Dabei gibt man sich umweltbewusst, und verspricht so Probleme wie Klimawandel, Ressourcenknappheit, demographischen Wandel etc. anzugehen, um den Menschen ein langfristiges Überleben auf der Erde zu ermöglichen. Die Tatsache, dass die Zerstörung des Planeten ein Resultat der kapitalistischen Logik ist und den Unternehmen dabei horrende Profite winken, bleibt unerwähnt.

Auch bei Vodafone stehen die Argumente der Ökologie, neben der Sicherheit und wirtschaftlichen Effizienz im Vordergrund ihrer Smart City Projekte. Gemeinsam mit dem RWE „Öko"- Tochterunternehmen „Innogy" entwickelt der Konzern Konzepte für die intelligente Stadt. Vernetzte Verkehrsanlagen und -teilnehmer*Innen, ein intelligentes Abfall-Management und smarte Beleuchtungssysteme sind dabei für die Unternehmenskooperation die drei wesentlichen Eckpfeiler auf dem Weg dorthin. Intelligente Multifunktionsmasten unter dem Titel „Innogized Poles" sollen mit Sensoren und Geräten bestückt eine Allround-Lösung für die urbane Vernetzung bieten. Diese könnten einerseits als Ladestationen für alle möglichen E-Fahrzeuge dienen, die Luftbelastung und Temperatur messen und digitale Werbung auf LED-Screens produzieren. Andererseits aber sollen sie auch die Überwachung durch intelligente Videokameras im öffentlichen Raum vereinfachen. Ein weiteres Produkt von Vodafone ist die smarte Mauer. Sensoren sollen dabei nicht nur Bewegungen erkennen, sondern auch chemische Stoffe und einzelne Sprayfarbpartikel. Wird eine Wand besprüht, alarmiert der Sensor automatisch die Ordnungsmacht. Aber auch Technologien, die direkt als Überwachungs-Instrumente in unseren Alltag integriert werden können, kommen aus dem Hause Vodafone. Mit

„Smart Level Glasses", die in Zusammenarbeit mit dem US-Hersteller VSP entwickelt wurden, bietet der Konzern eine Brille, die voller smarter Technik ist. Diese soll vor allem als Fitness-Tracker dienen, hält aber auch Ortungsfunktionen und weiteres bereit. Ein Schrittzahl-Ranking, mit dem ab einem gewissen Punktestand soziale Projekte und bedürftige Menschen unterstützt werden, soll für die Nutzer*Innen einen Anreiz sein, die Brille auch dauerhaft einzusetzen. So wird die emotionale Erpressung zum Datenfresser gleich mitgeliefert.

Mit solchen und ähnlichen Anwendungen machen die Konzerne deutlich in welche Richtung sich die Prozesse der Smartifizierung tatsächlich entwickeln. Das was uns als Erleichterungen für den Alltag im Namen der Ökologie verkauft wird, entpuppt sich als grüner Kapitalismus in Reinform. Es geht um Macht und Geld. Und so wird sich die Verwüstung unaufhaltsam ausbreiten und unsere Lebensräume Stück für Stück zu Orten absoluter Kontrolle werden. Was uns bleibt, ist an der Idee eines anderen Lebens und der Möglichkeit der Zerstörung dieser Welt der Herrschaft und Kontrolle festzuhalten und dies in Taten umzusetzen."

*Die Netzbeschmutzer*Innen*

http://4sy6ebszykvcv2n6.onion/node/22034 (nur über *Tor*)

Angriff auf Smart City – Feuer gegen Amazon Lieferwagen

Dokumentation, Berlin 06.06.2018

„ DIE GEDANKEN SIND FREI …

Über den technologischen Angriff auf das Individuum wurde seit der immensen Entwicklung verschiedener Akteure und der zerstörerischen Ausweitung auf dem bisher einzig besiedelten Planeten viel berichtet.

Eine Form der glücklichen Versklavung hat unser Zeitalter erreicht, welcher sich die Menschheit hemmungslos hingeben will.

So denken wir an Facebook. Die Vernetzung aller Menschen. Jede kann zu jedem Kontakt aufnehmen. Facebook findet von ganz allein alte Schulfreund*innen und noch besser, Facebook findet mich auch selbstständig auf Fotos, von denen ich nie was wusste. Es bilden sich online-Gruppen zu allen möglichen Themen und jede*r kann Teil davon sein. Wir teilen Nachrichten über den ganzen Planeten und bewerten diese mit gut oder schlecht.

Dann ist da Google. 1, 2, 3, 4 mal genutzt und Google weiß schon beim zweiten Buchstaben, nach was für einem Thema ich suche. Zauberei.

Dann ist da Amazon. Ein Unternehmen zur Erleichterung des ungesättigten Konsums.

Jede Preisklasse, jede Kategorie, jedes Land. Wirklich für alle was dabei… könnte schön so weiterlaufen, wären da nicht einige Stimmen, die auf einmal erzählen wie Scheiße und unmenschlich dort gearbeitet werden muss. Arbeiter*innen erzählen von einem regelrechten Drill und Überwachungsmaßnahmen vom feinsten. Von Arbeitsteams die gemeinsam bestraft oder belohnt werden. Anscheißertum ist eine Tugend bei Amazon.

Und in den USA stellt Amazon bevorzugt ehemalige Angehörige der Mittelschicht, die inzwischen in ihren Autos leben, ein, um sich einer Klasse entrechteter Arbeitsnomaden zu bedienen.

Allerdings ist dieser Konzern in jener Hinsicht natürlich nur ein Paradebeispiel von vielen. Der Zwang zur Arbeit um essentielle Lebensgrundlagen zu haben ist paradox. Die unmenschlichen Bedingungen, denen so viele tagtäglich ausgesetzt sind, sind eigentlich bekannt.

Wenn auch im gegenwärtigen anarchistischen Diskurs der Klassenwiderspruch nach Marx vollkommen überholt scheint und vom Klassenkampf im klassischen Sinne keine Rede sein kann, lässt sich das Herrschaftsgefüge sehr wohl durch Machtverhältnisse, ökonomische Zwänge und soziale Stellungen definieren.

Es formt sich Protest gegen Google. Die Umstrukturierung der Stadt in Form von Start-up Wohn- und Arbeitscommunities, Factories oder einem Google Campus in Kreuzberg.

Und auch Amazon ist nicht mehr das nette Verkaufsportal im Internet. Viele solidarische Menschen haben im letzten Jahr Aktionen gemacht und Analysen verbreitet um auf den Kampf der Arbeiter*innen hinzuweisen und Amazon als einen Player digitaler Herrschaft heraus zu kristallisieren.

Welchen Umfang die Sabotage annimmt, lässt sich kaum sagen; mit brennenden Amazon Trucks wie Anfang Mai in Philadelphia wird versucht, die politische Bedeutung abzuerkennen.

Sicher nicht zufällig ging in der Nähe von Birmingham/ UK Anfang November 2017 ein Amazon Lager in Flammen auf und das selbe Warenhaus in Rugeley, Staffordshire, wurde bereits im November 2016 Ziel einer Brandstiftung , beide Feuer störten das Weihnachtsgeschäft erheblich.

Ob sich dieser Widerstand als Klassenkampf bezeichnen lässt, spielt dabei weniger eine Rolle als die konkrete Unterdrückung derer die für Amazon arbeiten müssen oder die faktische Überwachung derer die Amazon nutzen. Genauere Analysen bedürfen weiterer Betrachtungen und müssten auch ausserhalb der engen Szenekreise erforscht werden, auch wenn dafür aus manchen Gebieten, wie Atlanta leider nur Twitter als Quelle vorliegt.

Übrigens wurde bereits im November 2017 in Berlin gegen Amazon gezündelt und in München Paketstationen beschädigt ,leider hat die https://makeamazonpay.org/ Kampagne den militanten Widerstand ignoriert.

...WER KANN SIE ERRATEN ...

Die schleichende gesellschaftliche Veränderung, hat vor allem für die Jugend mittlerweile an Normalität gewonnen. Der Zugang zu den intimsten Bedürfnissen vieler Menschen hat Konzernen wie Google und Amazon Möglichkeiten geschaffen diese zu kontrollieren und zu steuern. Vereinzelung und die Unfähigkeit sozialer Interaktion mit lebenden Menschen sind die Folgen. Der zwischenmenschliche Austausch hat an Einfluss verloren, dass Internet weiss meist schon viel mehr über dich als deine Freund*innen.

Eine Offenheit in der Gesellschaft über Tabuthemen, wie psychische Probleme, Zwänge oder Armut reden zu können, wäre wünschenswert. Niemand sollte sich selbst krank reden, weil man nicht in die gesellschaftliche Norm passt.

Ein kapitalistisches System kann nicht funktionieren, wenn nicht alle mitspielen. Deshalb benötigt es Kontrolle und Sanktionen, die Menschen gefügig zu machen. Der Staat kann Freidenker*innen nur durch Härte zwingen, sich zu unterwerfen.

Die digitale Herrschaft hat sich das Ziel gesteckt, die Menschen gleichzustellen. Überall im Leben präsent zu sein und durch cleveres Vorgehen von Nutzen und dann unabdingbar zu werden. Jede noch so kleine Information ist wichtig unsere Gedanken zu verstehen um sie zu verändern.

Einige Konzerne und Länder haben sich die smarte Technologie in Form von z.B. sozialen Rankings mittlerweile zu nutzen gemacht um repressiv gegen die Bevölkerung vorzugehen.

Andere Konzerne wie Amazon haben es geschafft das Kaufverhalten ihrer Kund*innen zu analysieren, zu beeinflussen und die Ware auch noch zum Verkauf anzubieten.

Von uns gab es am 4. Mai auch zwei Päckchen an Amazon beim Kissingenplatz in Berlin-Pankow. Leider konnte nur eines zugestellt werden. Das andere ist in der BigData verschwunden.

Wir haben uns einer im Internet verbreiteten Anleitung bedient https://www.liveleak.com/view?i=f2f_1423574431 die uns sicher erscheint, die selbstverständlich nicht genau genug ist, um jede Zufälligkeit mit obrigkeitshörigen Passantinnen zu vermeiden."

anonym

Kampfschrift gegen ein zweites Headquarter von Amazon

Wenn Du es endlich geschafft hast, Dich durch den Verkehr zu kämpfen und in Deiner Wohnung gelandet bist, ist Deine Mitbewohnerin bereits seit einigen Stunden im Netflixrausch. Du willst Ihr erzählen, wie Dein Tag so war, aber sie ist offenbar schon mit sich selbst beschäftigt. Trotzdem hast Du das Bedürfnis nach irgendeiner Art von Kommunikation.

„Alexa, spiel mir etwas Entspannungsmusik."

Du lässt Dich in Deine Schaumstoffmatratze mit Gedächtnis sinken und denkst an alles, was Du gerne hättest, all die kleinen Projekte, die Du angehen willst, zu denen Du aber nie kommst, weil Dir die Energie und die Zeit dazu fehlen. Wenn Deine Aquarellfarben nicht so mies wären, hättest Du vielleicht mehr Lust zu malen.

„Alexa, bestell mir einen neuen Aquarellmalkasten."

"Okay. Wie wär es mit diesen hier…?"

Amazon erfüllt Dir alle Deine Wünsche.

Zum Glück macht Amazon das Leben leicht: klicken, bestätigen, Problem gelöst. Amazon erinnert Dich nicht nur an die Dinge, die Du vergessen hast zu besorgen, sondern stellt Dir auch Produkte vor, von denen Du nicht wusstest, dass Du sie willst. Es gibt sogar einen Laden in Seattle, der Dir nerviges Anstehen und krampfige Gespräche mit Kassieren erspart.

Allerdings liegt in der Vereinfachung von allem auch etwas Beunruhigendes; das Geschäftsmodell einer Firma, die alles schluckt, ist irgendwie auch suspekt. Du hast mitangesehen, wie Dein Lieblingsbioladen vor Ort von Whole Foods aufgekauft wurde, nur um dann verwirrt zuzugucken, wie Whole Foods von Amazon übernommen wurde. Dann war da noch diese Amazon Werbung, wo wir um unsere Hausschlüssel gebeten wurden, damit Pakete direkt ins Haus geliefert werden konnten. Als diese Idee dann doch etwas zu unheimlich erschien, versuchten sie uns mit der Installation von Überwachungskameras zu beruhigen, die mit einem Live-Stream über eine App direkt mit unseren Smartphones verbunden sein würden.

Amazon zieht es vor die konkreten Abläufe zu verstecken – die Realität in Form öder Reihen von Mega-Lagerhallen und Zulieferer-Farmen in der wirklichen Welt – um als eine wohltätige, unsichtbare Kuscheldecke zu erscheinen. Aber dieses Jahr brauchen sie einen Ort um eine neue Hauptgeschäftsstelle – HQ2 – zu errichten. Die Veröffentlichung der finalen zwanzig konkurrierenden Städte hat die Gestalt eines Todesspiels aus der „Die Tribute von Panem" Romantrilogie angenommen, wo Stadtverwaltungen und Makler sich abstrampeln, ganze Stadtbezirke freiwillig auf dem Altar zu opfern. Überall im Land streiten sich Städte, wer sich für die größten Steuererleichterungen bereitstellt oder die interessantesten Stadterneuerungspläne vorlegen kann, um die Unterbringung zu und den Transport der 50.000 technischen Arbeitskräfte zu sichern, die HQ2 mitbringen würde.

Als Einwohner Atlantas sehen wir, was wirklich gespielt wird: ein wilder Mietpreisanstieg, noch mehr Straßenverstopfung und demnächst auch noch Lieferdrohnen, die über unseren Köpfen brummen. Das Einströmen tausender sozial isolierter Techniker wird die kulturelle Lebendigkeit beschädigen, und people of colour und die arme Arbeiterschicht werden aus dem Umkreis verdrängt werden. Für die, die es schaffen, in der Stadt zu bleiben, wird es wird ein paar mehr befristete und zuschlagsfreie „Jobs" in Lagern geben, wo die Arbetier wie die Roboter, durch die sie bald ersetzt werden, behandelt werden.

Der Bürgermeister wird dem Unternehmenschef Lord Jeff Bezos krönen, und das Amazon Imperium wird nicht nur expandieren, um das ganze Internet zu annektieren, sondern auch die Viertel und Gemeinden, in denen wir aufgewachsen sind.

Die Visionäre der Cloud träumen von einer Welt, in der ungelernte Arbeit durch Roboter ersetzt wird, ein universelles Grundeinkommen die Armen in Schach hält, und Smart Cities der Lebensarbeitsspielplatz der Neureichen wird. Von unserem geerdeten Standpunkt aus betrachtet sehen wir nur einen Alptraum, in dem alle Daten transparent sind, alle Bewegungen überwacht werden, und unser Zugang zur Wirtschaft direkt proportional ist zum Anteil persönlicher Freiheit, die wir aufzugeben bereit sind.

Folglich würden wir gerne eine einfaches Statement machen, von dem wir hoffen, dass Ihr ihm zustimmt: Nein, wir wollen Amazon nicht hier. Tatsächlich wollen wir Amazon nirgendwo. Wir glauben, dass Leute in Atlanta und Leute mit Gewissen im ganzen Land sich gegen HQ2 stellen sollten bevor die Entscheidung fällt.

„Alexa? Hörst Du mir zu..."

Wenn die Entscheidung bekannt gegeben wird, wird es bereits zu spät sein.

Heute ist der erste Tag des Widerstandes gegen HQ2

http://atlantaagainstamazon.org/

Ergänzung der Redaktion: *Im November 2018 gab Jeff Bezos das Ergebnis der Ausschreibung bekannt: das neue Headquater des Konzerns soll auf die beiden Städte New York City und Arlington (Virginia) aufgeteilt werden. Hierhin will Amazon zusammen 50.000 Arbeitsplätze verlegen bzw. neu schaffen. Zusätzlich soll ein neues Verteilzentrum in Nashville entstehen. Alle drei Orte haben Amazon Geldgeschenke von 3.5 Mrd Dollar versprochen. Insgesamt 200 Bewerberstädte hatten sich gegenseitig mit „finanziellen Hilfen" für Amazon überboten. Pennsylvania hatte zwei Städte im Rennen und zusammen 4.6 Mrd Dollar geboten. New Jersey bot 7 Mrd und Maryland war bereit sogar 8,5 Mrd zu verschenken, damit Amazon zu ihnen kommt. Ein unwürdiges Spektakel für einen Konzern, der sich weigert Steuern zu zahlen, und dafür auch noch hofiert wird.*

Evict Google

Absage der „Google Campus"-Pläne in Berlin-Kreuzberg

Kein Kreuzberg für Google: In den letzten zwei Jahren haben mehrere Initiativen gemeinsam mit Anwohner*innen gegen die Pläne des Unternehmens gekämpft, mit seinem „Google Campus" in das alte Umspannwerk am Kreuzberger Landwehrkanal einzuziehen – mit Erfolg. Über ein Jahr lang wurden Demonstrationen und Kiezspaziergänge organisiert, es wurde diskutiert, gelärmt, besetzt und in Broschüren, auf Plakaten und Flyern zum Ausdruck gebracht, dass Google nicht der gute Nachbar gewesen wäre, als der sich das Unternehmen mit seinem Motto „Do the right thing" gern selbst präsentiert. Stattdessen haben Aufklärungsarbeit, Protest und ziviler Ungehorsam sichtbar gemacht, dass Google ein Akteur der Verdrängung ist, der mit seinen Campus-Projekten alles Mögliche, aber sicher keinen „Mehrwert für den Kiez" schafft, wie Pressesprecher Ralf Bremer uns gern Glauben gemacht hätte. Google, als womöglich größter Player im digitalen Kapitalismus, will nicht nur Daten sammeln und Technologien entwickeln, die sowohl Profit- als auch Überwachungs- und militärischen Interessen dienen können (Stichwort „Project Maven", zeit.de/digital/internet/2018-06/maven-militaerprojekt-google-ausstieg-ruestungsexperte-paul-scharre). Google will uns seine optimierte, transhumanistische Zukunft auch als Zukunft der Städte verkaufen. Das hat ein breites Spektrum an Protestierenden dazu motiviert, mit Analyse und Kritik, Spraydose und Farbei gegen die ideologische Reinhaltung des Konzernimages vorzugehen, das für die Durchsetzung von Googles Interessen von so zentraler Bedeutung ist.

SPÄTE EINSICHT, SCHMUTZIGE WÄSCHE

Dass Google nicht richtig, sondern gänzlich daneben lag, als es einst entschied, die Stadt mit einem weiteren sogenannten Start-Up-„Incubator" zu beglücken, hat das Unternehmen an einem Mittwoch Ende Oktober selbst eingestehen müssen. In einer sorgfältig inszenierten Pressekonferenz mit Schlüsselübergabe verkündeten Bremer und Googles Start-Up-Stratege Rowan Barnett, dass der Campus in Kreuzberg (vorerst) nicht eröffnen wird. Stattdessen werden die Fundraising-Plattform betterplace.org und der Jugendhilfeverein KARUNA, der u.a. mit Blockchain-Technologie eine App für das bargeldolose Überweisen von „Spendenbeträge für zweckgebundene Hilfsangebote" bereitstellt [arup.com/de-de/projects/mokli-karuna], die Räume des Umspannwerkes beziehen: für fünf volle Jahre in eigener Verwaltung, unter der schützenden Hand Googles, das den Mietvertrag gern bezahlt, weil es ihn dadurch schließlich behalten darf. Man habe aber eingesehen, dass Kreuzberg nicht der richtige Ort für einen Google Campus sei, wird Bremer zitiert [taz.de/!5545724/].

Dieser Teilrückzug war ein allzu offensichtlicher Versuch, das vom Protest beschmutzte fortschrittliche Erscheinungsbild Googles einem erneuten Imagewashing zu unterziehen. Und dennoch ist die einstweilige Absage des Campus ein Etappensieg für alle, die sich in Berlin und über seine Grenzen hinaus zusammengetan haben – um mit ihren Vorstellungen einer solidarischen Stadt den Zumutungen der kapitalistischen Stadt zu begegnen. Letztere werden von den Tech-Konzernen und der ihnen wohlgesonnenen Politik, die die Ideologie der optimierten „Smart Cities" teilen, nicht verbessert, sondern verschärft. Trotz seines Einlenken will ein Konzern wie Google mit seinen Ideen natürlich nicht daneben gelegen haben: Immer noch ist man in der Berliner Filiale der Ansicht, das Richtige zu tun, wenn man sich jetzt mit der Geste des großzügigen Mäzens einen sozialen Anstrich gibt, um sich zugleich die Hintertür zum Umspannwerk im achso-dynamischen-und-bunten Kreuzberg offen zu lassen. Synergie, Diversität und Innovation sind die Schlagwörter von Googles wirklicher Mehrwertsteigerung, für die es Kreuzberg in Dienst wollte und will, weil sich der Rohstoff Kreativität so gut in der Mine des ‚rebellischen' Kiezes schürfen lässt. Dass diese Wirtschaftsweise keine Arbeitsplätze, sondern vor allem weitere prekäre Arbeitsverhältnisse und Selbstausbeutungs-Ideolog*innen nach Kreuzberg oder Berlin bringt, ist inzwischen selbstverständlich. Aber auch mit sozialer Münze lässt sich erst einmal Mehrwert für den Konzern generieren: Dafür spannt der friendly capitalist mit den beiden sogenannten Sozial-Businesses nun erst einmal andere vor den Karren. Und die nehmen die Räume, die kein Geld, sondern allein ein kleines bisschen Würde kosten, gern in Anspruch.

SHUT DOWN GOOGLE, START UP REVOLT

Im Selbstverständnis von Google hat der Teilrückzug selbstverständlich nichts mit den Protesten zu tun, von denen man sich ja, so Bremer, nicht die Firmenpolitik diktieren lasse. Aber nicht nur die Berliner Spatzen pfeifen es von den Dächern, auch internationale Medien von Guardian über Libération bis New York Times sind sich einig: Google hat eine Niederlage einstecken müssen, und mit ihr der Start-Up-freundliche Berliner Senat, der um

den Preis, ein kleines bisschen Silicon Valley-Feeling an die Spree zu holen, stets das Wohl derer zu opfern bereit ist, die sich das Leben vor Ort wegen solcher „Innovationen“ nicht mehr leisten können. Auch die Berliner Wirtschaftssenatorin, Ramona Pop, freut sich über die Lösung, hatte sie in einem Interview doch kürzlich erst ein „nachhaltiges Start-Up Ökosystem“ gefordert, und sieht genau das jetzt in das Umspannwerk einziehen. Gegen den Google Campus hatte sie allerdings ebenfalls kaum Einwände, ebenso wenig wie gegen den sich ankündigenden „Innovations-Campus“ Siemensstadt. Indes bleibt der Kurs von Rot-rot-grün gewohnt engspurig. Geprägt von Opportunismus und Sachzwangausflüchten unterscheidet sich die Regierung kaum von ihren früheren Versionen: Um Berlin in der Standortkonkurrenz fit zu bekommen, eifert sie um jeden Preis dem kalifornischen Vorbild nach – ohne dabei die sozialen Verwüstungen mitzubenennen, die der (Tech-)Kapitalismus dort täglich vorantreibt. Im kalifornischen San José, wo ebenfalls ein Campus geplant ist, gab es übrigens erst kürzlich erneute Proteste gegen die berüchtigten Busse, die exklusiv die Google-Pendler zu ihrem Arbeitsplatz und wieder zurück verfrachten: „Evict Google“ („Räumt Google“) hieß es dort, mit solidarischen Grüßen nach Berlin. Zeitgleich regt sich in *Tor*onto der Widerstand, Google als Experimentierfeld für seine „Sidewalk Labs“ zu dienen, mit denen ganze Stadtviertel digital erschlossen und reorganisiert werden sollen [theintercept.com/2018/11/13/google-quayside-toronto-smart-city/].

SCHLECHTE VERLIERER

Der Internationalität der Proteste zum Trotz tun sich ganz besonders schlechte Verlierer des Rückzugs damit hervor, die Protestierenden als „Kiez- und Milieuschutzfanatiker“ zu bezeichnen – so Sebastian Czaja, Vorsitzender der Berliner FDP-Fraktion. „Kommt bloß nicht nach Berlin, erst recht nicht nach Kreuzberg“ sei die Botschaft, die vom Paul-Lincke-Ufer in die Welt gehe. Dem können wir uns durchaus anschließen. Dass er aber von „kiezbezogenem Nationalismus“ schwadroniert, um die Proteste zu diskreditieren, andere von „No-Go-Areas“ für Tech-Unternehmen sprechen, zeigt nur eines: den plumpen Abwehrreflex derjenigen, die ihre neoliberale Ideologie als Interesse am Gemeinwohl vermarkten. Während sie nur die alte Sprechblase vom Wirtschaftsstandort und den angeblich verlorenen Steuereinnahmen und Arbeitsplätzen in immer neuen Varianten predigen, sind es vielmehr die Protestierenden, die eine globale Dimension aufgezeigt haben: Arbeitskämpfe im digitalen Kapitalismus, Kämpfe um das Leben in den Städten und gegen das Zusammengehen von Staat und Technologie-Unternehmen bei der Militarisierung von Armee, Polizei und Überwachungsapparaten sind Kämpfe, die in von Google-Projekten betroffenen Städten wie Saò Paulo, Rennes, San Francisco, *Tor*onto und Kreuzberg in solidarischer, internationaler Perspektive geführt werden können. Menschen mit unterschiedlichen Hintergründen kommen hier zusammen, weil Lokal- und Stadtpolitik Klassenpolitik sind.

PROTEST WIRKT

Kiez- und Klassenpolitik von oben hingegen sieht so aus, dass die CDU in der Folge den Campus nach Lichtenberg in die ehemalige Stasi-Zentrale holen wollte, und der Konzern auch im SPD-regierten Spandau umworben wurde. Google hat ihnen allen inzwischen eine Absage erteilt, und dennoch zeigen diese demütigen Werbeversuche, dass der Glaube an die Start-Up-Ideologie in der Berliner Politik fest verankert ist, die Preisgabe von Wohnraum und sozialen Orten zugunsten des Wirtschaftsstandorts also weitergehen wird. Doch die Vernetzung und Zusammenarbeit für eine Stadtpolitik von unten durch Nachbarschaften, stadtpolitische Intiativen und radikale Linke zeigt: Protest wirkt, es ist möglich, sich zusammenzufinden, sich Gedanken über eine solidarische Stadt zu machen und den Akteuren der Verdrängung auf die Füße zu treten. Wenn jetzt auch einige Linke und Grüne vorsichtig applaudieren, darf dies getrost als verlogen bezeichnet werden: Unter ihrer Regierung wird die Berliner Linie durchgesetzt und Besetzungen in der Regel innerhalb von Stunden brutal geräumt. Das betretene Schweigen der SPD braucht derweil in seiner Kläglichkeit kaum noch eigens kommentiert zu werden.

EIN ETAPPENSIEG

Alles in allem: Trotz Google wird der Verdrängungsprozess in Kreuzberg und anderswo weitergehen. Weitere Leuchtturmprojekte des digitalen Kapitalismus in der Stadt, wie Pandions „The Shelf“ oder die neue Zalando-Zentrale kündigen sich an, andere Co-Working-Spaces oder Wohnraumverwertungsagenturen wie rent24 schießen weiterhin aus dem Boden. Gleichzeitig droht die Räumung der Liebig 34 und anderer selbstverwalteter Räume, und die Luft für Mieter*innen wird weiterhin enger. Die Smart City, die vom Senat gewollt ist, ist die Stadt der Verdrängung und Kontrolle. Deshalb gilt es, weiter Kristallisationspunkte sichtbar zu machen, an denen soziale, stadtpolitische und technologiekritische Kämpfe zusammengeführt werden können, und dabei Player wie Google und seine Social-Business-Platzwärmer, aber auch andere Tech-Konzerne und Start-Ups auf dem Schirm zu behalten.

Das Fernziel bleibt, eine Stadt von unten aufzubauen und dafür zu streiten, dass Unternehmen, die mit den Daten aller die Interessen von Kapital und Staat bedienen, enteignet gehören. Die Initiativen und Anwohner*innen in Kreuzberg feiern einen ersten Etappensieg, der Mut macht, und auf dem soziale und stadtpolitische Kämpfe aufbauen können. Während dieser Erfolg von den Chefideolog*innen des Neoliberalismus notdürftig kaschiert wird, weisen die Proteste in Richtung einer solidarischen Stadt, die eine bessere Zukunft für alle nicht nur verspricht, sondern realisiert.

Counter_Campus und GoogleCampus Co & verhindern

https://de.indymedia.org/node/25987

Glossar

Affirmativ – Ein anderes Wort für bejahend, zustimmend und bestätigend.

Affirmative Action – Bezeichnet gesellschaftspolitische Maßnahmen, die der negativen Diskriminierung sozialer Gruppen in Form gesellschaftlicher Benachteiligung durch gezielte Vorteilsgewährung entgegenwirken sollen. „Affirmativ" in diesem Sinne bedeutet die besondere Bestätigung und Unterstützung solcher Gruppen.

Aggregieren – Das Zusammensammeln, Verdichten und Anhäufen von z. B. Nachrichten.

Algorithmus – Eine exakt beschriebene Vorgehensweise zum Lösen eines Problems in endlich vielen und eindeutig beschriebenen Schritten. In der Informatik ist damit oft der Kern der Software bezeichnet, in dem z. B. das Lernverhalten von KI festgelegt wird, oder der festlegt, welche Ergebnisse wir bei einer Google-Suche angezeigt bekommen. Oft ein wohlgehütetes Geheimnis.

Antagonismus – Bedeutet das einander Entgegenwirken/Entgegenstehen von Strukturen, Systemen oder Menschen.

Asymmetrische Kriegsführung – Ein asymmetrischer Krieg ist eine militärische Auseinandersetzung zwischen Parteien, die waffentechnisch, organisatorisch und strategisch stark unterschiedlich ausgerichtet sind. Typischerweise ist eine der beteiligten Kriegsparteien waffentechnisch und zahlenmäßig so überlegen, dass die andere Kriegspartei militärisch in offen geführten Gefechten nicht gewinnen kann. Langfristig können jedoch nadelstichartige Verluste und Zermürbung durch wiederholte kleinere Angriffe zum Rückzug der überlegenen Partei führen. In den meisten Fällen agiert dabei die militärisch überlegene Partei, meist reguläres Militär eines Staates, auf dem Territorium eines anderen Landes und kämpft gegen eine militante Widerstands- bzw. Untergrundbewegung, die sich aus der lokalen Bevölkerung gebildet hat.

Big Data – „Big Data" wird häufig als Sammelbegriff für digitale Technologien und Produkte verwendet, die auf großen Datenmengen beruhen, welche nur automatisch auswertbar sind, und die in technischer Hinsicht für eine neue Ära digitaler Kommunikation und Verarbeitung und in sozialer Hinsicht für einen gesellschaftlichen Umbruch verantwortlich gemacht werden.

Cybersyn Projekt – Das Projekt Cybersyn („cybernetic synergy") war während der Regierung Salvador Allendes (1970–1973) ein chilenischer Versuch, die Zentralverwaltungswirtschaft in Echtzeit durch Computer zu kontrollieren. Im Wesentlichen war es ein Fernschreiber-Netzwerk, das Fabriken mit einem zentralen Computer in Santiago verband.

Denial-of-Service-Angriffe (kurz:**DDoS**) – sind etwa so, als ob sich ein riesiger Flashmob in einen Supermarkt begibt. Weil es so viele sind, kann sich keiner mehr bewegen und der Betrieb kommt zum Erliegen. Die Lagerräume, die Kasse, die Zuliefererkette, die Verkäufer werden nicht angegriffen. Es wird nichts gestohlen. Es wird blockiert für ein paar Stunden. Der Schaden ist, dass für ein paar Stunden keiner einkaufen kann.

Dystopie – Eine Geschichte, die in einer fiktiven Gesellschaft spielt, die sich zum Negativen entwickelt hat. Das Gegenteil von Utopie.

Echokammern – Mit Echokammern wird ein Umfeld bezeichnet, in dem man nur noch Informationen angeboten bekommt/aufnimmt, die den eigenen Vorlieben entsprechen. Dies wird heute oft auf Alte und Neue Medien angewendet.

Egalitär – Bedeutet, etwas ist auf Gleichheit gerichtet oder strebt soziale Gleichheit an.

Erratisch – Meint zufällig, unvorhersehbar.

Filterblasen – Ein Umfeld, in dem durch filternde Algorithmen eine Isolation einer Internet-Benutzer*in gegenüber Informationen, die nicht ihrem Standpunkt entsprechen, bewirkt wird. Wenn man beispielsweise jemandem auf Twitter folgt, bekommt man automatisiert Vorschläge zu weiteren Personen, denen man folgen könnte oder Themen, die die Algorithmen als möglicherweise interessant für jemanden errechnet haben. Bleibt man innerhalb dieses vorgegebenen Rahmens, so bildet sich eine Filterblase, in der man sich bewegt, und diese zu verlassen bedarf eines aktiven Durchbrechens.

Framing – Komplexe Themen werden soweit runter gebrochen, dass konkrete Deutungsmuster oder Handlungsempfehlungen durch die Zielgruppe "erkannt" werden, womit sich z. B. die Aufmerksamkeit zu oder von einem Thema ablenken lässt. Durch Exklusion und Inklusion von Sichtweisen auf Inhalte bzw. von Inhalten selbst sowie durch Kategorisierung, kann Einfluss auf die Realität in einer Gesellschaft genommen werden.

Fordismus – Als Fordismus bezeichnet man eine nach dem Ersten Weltkrieg etablierte Form industrieller Warenproduktion. Sie ist benannt nach dem US-amerikanischen Industriellen Henry Ford, dessen Organisation von Arbeit und Kapital als typisch für die gesamte Epoche angesehen wird. Der Fordismus basiert auf stark standardisierter Massenproduktion und -konsumtion von Konsumgütern mit Hilfe hoch spezialisierter, monofunktionaler Maschinen, Fließbandfertigung und dem Taylorismus.

HAL9000 – Ist der Computer an Bord des Raumschiff Discovery aus dem Film „2001 Odysee im Weltraum". HAL zeigt während der Reise zum Planeten Jupiter mehr und mehr eine Art neurotisches Verhalten. Er scheint sich in einer Fehleranalyse zu irren (oder vielleicht täuscht er auch nur einen Fehler vor; dies wird im Film nicht deutlich). Nachdem er herausfindet, dass die Besatzung ihn abschalten will, falls sich die Irrtümlichkeit seiner Fehleranalyse bestätigen sollte, versucht er, die Besatzung auszuschalten, um seine Mission zum Jupiter fortführen zu können – „unbeirrbar und allein".

Inhärent – Etwas ist anhaftend, innewohnend.

Kohärent – Etwas ist zusammenhängend, verbunden mit, einheitlich.

Kybernetik – Kybernetik ist die Wissenschaft der Steuerung und Regelung von Maschinen, lebenden Organismen und sozialen Organisationen und wurde auch mit der Formel „Die Kunst des Steuerns" beschrieben. Ein typisches Beispiel für das Prinzip eines kybernetischen Systems ist ein Thermostat. Er vergleicht den Istwert eines Thermometers mit einem Sollwert, der als gewünschte Temperatur eingestellt wurde. Ein Unterschied zwischen diesen beiden Werten veranlasst den Regler im Thermostat dazu, die Heizung so zu regulieren, dass sich der Istwert dem Sollwert angleicht

Nudging – Das Treiben von Personen zu bestimmten Handlungen mittels Anreizen.

Segregation – In der Soziologie: Die Trennung von Bevölkerungsgruppen aus religiösen, ethnischen oder sozialen Gründen.

Paternalistisch/Paternalismus – Meint eine Herrschaftsordnung, die ihre Autorität und Herrschaftslegitimierung auf eine vormundschaftliche Beziehung zwischen herrschenden und beherrschten Personen begründet. Paternalistisch meint oft bevormundend.

Taylorismus – Als Taylorismus bezeichnet man das von dem US-Amerikaner Frederick Winslow Taylor (1856–1915) begründete Prinzip einer Prozesssteuerung von Arbeitsabläufen, die von einem auf Arbeitsstudien gestützten und arbeitsvorbereitenden Management detailliert vorgeschrieben werden. Der Begriff Taylorismus wird synonym, jedoch in vorwiegend kritischem Kontext verwendet. Ziel des Taylorismus ist ein möglichst wirtschaftlicher Betriebsablauf.

Solutionist*innen – Beschreibt Problemlöser*innen, Anpacker*innen etc.

Universalismus – Denkart, die den Vorrang des Allgemeinen beziehungsweise des Ganzen gegenüber dem Besonderen und Einzelnen betont.

Das çapulcu redaktionskollektiv untersucht in DELETE! die aktuelle Transformation des Kapitalismus – und damit auch der Machtverhältnisse – durch den ›technologischen Angriff‹.

Der Einfluss der Tech-Giganten auf die Ökonomisierung der entlegensten Lebensbereiche nimmt stetig zu, während klassische politische Institutionen an Bedeutung verlieren. Soziale Punktesysteme verlängern mit ihrem permanenten ›Rating‹ und ›Scoring‹ die Reichweite der lenkenden Disziplinierung weit über die direkte Ausbeutung im Arbeitsverhältnis hinaus.

Doch mit welchen Methoden und Zukunftsvisionen überformen Unternehmen wie Facebook, Google, Amazon & Co. unsere Kommunikation und unser Denken? Wie verändern sich angesichts einer zunehmend digitalisierten Fremdbestimmung die Bedingungen für Autonomie und soziale Revolte? Und wie lässt sich die beabsichtigte Vereinzelung und Entsolidarisierung bekämpfen?

Im Zentrum des Heftes steht erneut die Selbstbehauptung, also der vielfältige Widerstand gegen den umfassenden technologischen Angriff. „Wir fällen nicht das lächerliche Urteil, dass die Technologie schlecht ist. Aus welcher - ohnehin historisch bedingten - Ethik heraus denn auch? Wir sagen, sie ist Gewalt und sozialer Krieg. Unsere Kritik richtet sich gegen die technologische Aneignung von Lebensprozessen.“

keep the future unwritten