DIVERGE!
Abweichendes vom rückschrittlichen «Fortschritt»

Hefte zur Förderung des Widerstands gegen den Technologischen Angriff

keep the future unwritten

BAND V: DIVERGE! – ABWEICHENDES VOM RÜCKSCHRITTLICHEN „FORTSCHRITT“

capulcu productions | Mai 2020 | capulcu.blackblogs.org
V.i.S.d.P. E. Schmidt | Am Zuckerberg 14 | 21984 Silikontal

bisher erschienen:

BAND IV: **DELETE! – DIGITALE FREMDBESTIMMUNG**

BAND III: **DISRUPT! – WIDERSTAND GEGEN DEN TECHNOLOGISCHEN ANGRIFF**

BAND II: **DISCONNECT! – KEEP THE FUTURE UNWRITTEN**

BAND I: **TAILS – THE AMNESIC INCOGNITO LIVE SYSTEM**

Inhalt

1 EINLEITUNG

2 DER NEUE GRIFF NACH DER WELTMACHT

4 LIBRA

9 EINE ART VON „KRIEG“ ODER DAS WÜTEN DES „DIGITALISIERENDEN VIRUS“

16 DIE „FREIWILLIGE“ CORONA-APP

24 BEHAVIORISMUS UND KYBERNETIK - GRUNDLAGEN DER VERHALTENSLENKUNG

27 HORIZONTE ÜBERSCHREITEN - EIN GASTBEITRAG VON SANDRA GÖBEL

33 KI ZUR PROGRAMMATISCHEN UNGLEICHBEHANDLUNG - ENTSOLIDARISIERUNG DURCH TECHNOKRATISCHEN SOLUTIONISMUS

40 WENIGER ÄRZTIN IM KÜNSTLICH INTELLIGENTEN GESUNDHEITSSYSTEM - DIGITALISIERUNG MIT NEBENWIRKUNGEN

46 ÖKOTECHNOKRATIE - „SMARTE“ ÖKOLOGIE VON OBEN

51 HONGKONG

60 WIDERSTAND GEGEN DIE INDIVIDUALISIERUNG DES SOZIALEN DURCH DEN TECHNOLOGISCHEN ANGRIFF

64 DOKUMENTIERTE WIDERSTÄNDE

77 GLOSSAR

Einleitung

Die derzeitige Coronakrise macht ein Abweichen (engl.: *diverge*) von technokratisch vorgegebenen Pfaden nicht gerade leichter, aber umso notwendiger. Erschienen Ansätze der Verhaltensökonomie den meisten (zumindest hier in Deutschland) noch vergleichsweise subtil „zukünftig", präsentieren sich derartige Methoden zum Bevölkerungsmanagement seit der Corona-Pandemie wie entfesselt. Wir erleben einen modernen Rückschritt in paternalistische Verhaltenslenkungsmuster, die bereits vor 70 Jahren nicht „fortschrittlich" waren. Ihren leider hochaktuellen Ausprägungen in der Gesundheits- und Klimakrise sowie ihren Wurzeln in der Kybernetik und dem eng verwandten Behaviorismus wollen wir in diesem Heft nachgehen.

Wie auch den globalen Machtverschiebungen und (sozial und wirtschafts)-kriegerischen Auseinandersetzungen im Kampf um die technologisch-politische Vorherrschaft. Im Zuge der Pandemie wird auch das Verhältnis zwischen politischen Eliten und den technologischen Avantgarden durch den Schub des „digitalisierenden Virus" neu ausgerichtet. Auch hier spielt die Initiative, eine digitale und global einsetzbare Währung auf den Weg zu bringen, eine Rolle.

Die umbrechenden technologischen Entwicklungen der letzten Jahre werden uns stetig und mit allergrößten Bemühungen als Fortschritt verkauft. Unsere Sicherheit, Gesundheit und gesellschaftliche Teilhabe werden immer wieder in die Waagschale geworfen, um zu zeigen, dass wir ohne die rasante technologische Entwicklung „nicht zu retten" sind. Die Technokratie und in ihrer Gefolgschaft der „Solutionismus" mit seinen vermeintlich unideologischen „Problemlösern" lösen mittlerweile nicht nur Probleme, die wir zuvor nicht hatten, sie verschärfen drängende Probleme und erschaffen dabei unsinnig viele neue. Insbesondere im Bereich der Klimakrise sorgt das für eine verheerende Rückschrittlichkeit des technokratischen „Fortschritts". Dass nach dem ökologischen Desaster der Abwrackprämie vor zehn Jahren überhaupt noch über eine Neuauflage als Kaufanreiz in der Coronakrise öffentlich nachgedacht werden kann, ist ein Ergebnis dieser kollektiv eingeübten Rückschrittlichkeit.

Der Einfluss der Tech-Giganten auf die Ökonomisierung der entlegensten Lebensbereiche nimmt stetig zu. Soziale Punktesysteme verlängern mit ihrem permanenten ›Rating‹ und ›Scoring‹ die Reichweite der lenkenden Disziplinierung weit über die direkte Ausbeutung im Arbeitsverhältnis hinaus. Es ist zu befürchten, dass wir noch sehr viel länger an den Folgen des pandemischen Ausnahmezustands knabbern werden, der sich dadurch auszeichnet, dass partielle Grundrechte zunächst temporär außer Kraft gesetzt oder in bedingte Zugeständnisse verwandelt werden. Dem pandemischen Ausnahmezustand droht wie schon dem „Ausnahmezustand" durch den *War on Terror* durch die (berechtigte) Befürchtung neuer Corona-Wellen bzw. neuer Virenstämme die Verstetigung. Ein etwaiger *War on Virus* verfügt dabei über eine ungleich größere Kapazität gesellschaftlicher Umgestaltung. Der Imperativ der „sozialen Distanzierung" ermöglicht den Eingriff in das Leben einer beliebig großen Gruppe von viralen Gefährder*innen bis hin zur Isolation im Sinne des Gemeinwohls – mit der Coronakrise sind alle zu Gefährder*innen geworden.

Bevormundende Verhaltenslenkung in hoch individualisierter Form lässt sich damit viel umfassender entwickeln. Kommende Beschränkungen im Zuge zukünftiger Epidemien brauchen dann nicht mehr per „Allgemeinverfügung" für alle geregelt werden. Stattdessen lässt ich feinkörnig vermessen, wer (per App) zur virologischen Gefahr erklärt wird und wer sich frei bewegen darf. Das ist zweifellos Gift für gesellschaftliche Solidarität. Letztere erfordert Mündigkeit und eigenverantwortliches Handeln statt autoritär verordnete (auch künstlich intelligente) Verhaltenslenkung. Es sind nicht irgend eine Ausgangssperre oder App, die uns schützen. Was uns schützt, ist unser Verhalten in solidarischer Selbstverantwortung.

Und daher müssen wir insbesondere eine raumgreifende Sozial-Technokratie angreifen, die sich in Ausnahmezuständen wie der Corona-Krise Akzeptanz verschafft. Ganz gleich, ob ihre Werkzeuge der Verhaltenslenkung dem chinesischen Shenzhen, dem US-amerikanischen Silicon Valley oder einem Problemlöser-Startup im hippen Berlin entspringen. In unseren Broschüren haben wir immer wieder dargelegt, worin der gesellschaftliche Rückschritt in diesen Technologien besteht und dass sie als Teil einer gesellschaftlichen Transformation funktionieren, die sich ohne weiteres einordnen lässt in historische Prozesse der letzten Jahrhunderte. Aber wir haben auch immer wieder Widerstände beleuchtet, die sich diesem Technologischen Angriff entgegenstellen. Widerstände, die den rückwärts gewandten Fortschrittsmarsch nicht mitgehen und Abweichendes bzw. Abzweige (ver-)suchen. Einige unserer Texte wagen daher den Sprung über die Leitplanke und beleuchten, welche gesellschaftlichen Prozesse jenseits der offensichtlichen Veränderungen angestoßen werden und was dies für unseren Widerstand bedeutet. Um unseren oftmals eurozentristischen Blick zu weiten, setzen wir uns in diesem Band auch kritisch mit den Protesten in Hongkong auseinander, wo eine Bewegung massiv auf Technologie setzt.

Digitale Versionen dieses Heftes sowie der Bände I –IV finden sich auf unserer Webseite:

https://capulcu.blackblogs.org

Der neue Griff nach der Weltmacht

„Griff nach der Weltmacht" ist eine Formulierung, die von Fritz Fischer Anfang der 60er Jahre des letzten Jahrhunderts für die Weltmachtansprüche des deutschen Kaiserreichs vor und im Ersten Weltkrieg gefunden wurde.[1] Eine genauere Analyse lokalisiert die Akteure dieses Griffs nicht in den politischen Eliten, sondern in den technologischen Avantgarden, die die Investitionsoffensive zu Beginn des 20. Jahrhunderts bestimmten. Und das nicht nur in Deutschland, sondern auch und sogar zuerst in den USA.[2] Die Offensive mit dem Ziel der Umwälzung der sozialen Verhältnisse und der technologischen Begründung einer neuen Macht in Produktion und Gesellschaft zielte auf die ganze Welt. Auf die Herstellung einer neuen Weltmacht mit den Mitteln, die die neuen Technologien den Avantgarden verliehen. Ihre Dynamik bezog sie aus der Gewalt zur Überwindung der sozialen Widerstände und der Konkurrenz. Jetzt allerdings nicht mehr nur zwischen den Unternehmen, sondern darüber hinaus zwischen den Ländern, die sie beherrschten. Das waren damals in erster Linie die USA und Deutschland, denen gegenüber Frankreich und England zurück fielen und zu denen später die Sowjetunion und Japan aufzuschließen suchten.

Heute sind es die USA und China und die europäische Union fällt zurück. Auch sie konkurrieren in einem neuen Griff nach der Weltmacht. Wir haben bisher die verschiedenen Vorstöße untersucht, in die sich der neue technologische Angriff auffächert. Wir wollen hier unsere Bemühungen aufgreifen, sie in einen größeren Zusammenhang zu stellen. Dabei sollen uns die Darstellungen zu den Entwicklungen vor hundert Jahren helfen Denn die aktuelle Konkurrenz wiederholt ihre Grundzüge auf neuem historischen Niveau. So wurde die heutige Innovationsoffensive bewusst im Rückbezug auf die damalige vorangetrieben.[3] Die Analogien sind denn auch Gegenstand wirtschafts- und politikgeschichtlicher Erörterungen in den USA, in aktuellen Debatten und auch beim IWF.

Woher kommen diese Analogien? Im Zuge ihrer Entfaltung geraten kapitalistische Innovations- und Investitionsoffensiven zunehmend in die Krise. Sie begegnen

1 F. Fischer, Griff nach der Weltmacht, Düsseldorf 1961.

2 D. Hartmann, Krisen, Kämpfe, Kriege, Innovative Barbarei gegen soziale Revolution. Kapitalismus und Massengewalt im 20. Jahrhundert, Kap. 2.

3 D. Hartmann, Krisen, Kämpfe, Kriege, Alan Greenspans endloser „Tsunami".- Eine Angriffswelle zur Erneuerung kapitalistischer Macht, Berlin 2015, S. 50 f.

sozialen Widerständen in Produktion und Gesellschaft, die mit den alten Methoden nicht mehr zu beheben sind. Das Wertaufkommen in anderen, vor allem peripheren Ländern reicht für eine absatzsichernde Nachfrage nicht mehr aus oder wird von Widerständen bedroht. Infolgedessen trachten vor allem neue kapitalistische Avantgarden danach, die überkommenen Verhältnisse bis in die internationalen Beziehungen hinein im Zuge einer neuen Innovationsoffensive zu zerstören, um neue an ihre Stelle zu setzen und sich selbst zu ihren Herren, Inhabern globaler Machtpositionen und Nutznießern des neu geschaffenen Reichtums zu machen.

Wie schon vor über hundert Jahren, so bildeten auch in der aktuellen Innovationsoffensive US-Unternehmer die Avantgarden des neuen Griffs nach der Weltmacht. Sie errichteten nicht nur – wie in Silicon Valley – die neuen Kathedralen globaler Macht. Sie schufen oder besetzten auch in anderen Ländern Brückenköpfe dieser Macht, brachen disruptiv die ökonomischen und sozialen Verhältnisse auf und griffen tief in die Arbeits- und Lebensverhältnisse. Mittelbar taten sie dies, indem sie Nachahmer anstachelten und vor sich hertrieben. Damit trieben sie die Durchdringung der Welt durch diese Offensive voran.

So wurden ebenso wie vor hundert Jahren sie und nicht die Regierungen zum zentralen Motor des neuen Griffs nach der Weltmacht. Nicht nur im Vortrieb der transnationalen Lieferketten und Start-up-Systeme, sondern auch (wie schon 1906 mit Bankhaus Morgans Erfindung des Trust-Systems) durch Facebooks beileibe noch nicht erledigten „Libra"-Vorstoß. Und sie werden es aufgrund ihrer technologischen Kompetenz und unternehmerischen Aggressivität auch bleiben. Da die Aufmerksamkeit meist der nationalen Politik gilt, bleibt unbemerkt, wie sehr die privaten Unternehmen, die sich nur wenig zur Treue gegenüber der US-Regierung verpflichtet sehen, noch immer die globale Durchsetzung der neuen Technologien bestimmen und kontrollieren. Allerdings sind sie zur Überwindung von Widerständen und Krisen zunehmend auf die Unterstützung der Staatsmacht und ihrer Fähigkeit, in soziale und internationale Konflikte einzugreifen, angewiesen. So wird der Griff nach der Weltmacht unternehmerischer Akteure auch jetzt wieder stärker zum jeweils nationalen Griff nach der Weltmacht werden. Obwohl die Rolle des Staats in China (die unternehmerischen und staatlichen Anteile sind manchmal schwer zu entwirren) - wie auch damals in Deutschland – weit gewichtiger ist als in den USA, so gewinnt sie auch hier zunehmend an Bedeutung. Der maßgebende Protagonist und Motor ist allerdings Donald Trump.

Trumps Bedeutung wird noch immer sträflich unterschätzt. Trump und seine republikanische Entourage orientieren sich ausdrücklich an dem Republikaner Theodore „Teddy" Roosevelt, der vor hundertzwanzig Jahren als Präsident und Führer der progressistischen Bewegung den staatlichen Antrieb der damaligen Innovationsoffensive organisierte[4]. Er leitete den neuen amerikanischen Griff nach der Weltmacht ein, er förderte die dehumanisierende Behandlung der Migrant*innen („schweinestallartige Lebensweise"), seine progressistischen „muckrakers" (Skandalmacher) betrieben die Auflösung der politisch korrekten zivilisierten Usancen der überkommenen Gesellschaft, so wie Trump heute wieder. Seine Orientierung an „Teddy" brachte Trump symbolisch zum Ausdruck, als er gleich zu seiner Inauguration „Teddys" Büste in die Bibliothek des Weißen Hauses stellen ließ, und sein Vize Mike Pence zog offiziell im Sommer 2017 den Vergleich zwischen Roosevelt und Trump.

Auf globalem Niveau betreibt Trump eine komplexe ökonomisch-politische Machtstrategie. Er zerstört das Netz multilateraler Handelsbeziehungen, indem er die Verträge kündigt und neue Vertragsstrukturen erzwingt und in den Dienst der amerikanischen Wirtschaft stellt. Er macht sich dabei die enorme Nachfragemacht der USA zunutze. Zu diesem Zweck schwächt er systematisch die Regelungsbefugnisse der internationalen Handelsorganisationen wie der WTO.

Wie schon vor über hundert Jahren, so ist auch heute die technologische Konkurrenz der zentrale Motor der Innovationsoffensive und des Griffs nach der Weltmacht. Diesmal zwischen chinesischen und US-Unternehmen. Eine wichtige Rolle spielt der militärische Bereich, den wir schon im Delete-Heft[5] dargestellt haben. Wie in der gesamten fordistischen Epoche, so ist dies der Sektor, auf dem der Innovationsdruck am unerbittlichsten auf andere Länder übertragen wird. Wer zurückfällt, wird militärisch anfällig und angreifbar. Hier spielt die staatliche Politik eine zunehmende Rolle, nicht nur in China, Russland und Israel, sondern auch in den USA. Da KI eine immer größere Bedeutung erlangt, wird die internationale Konkurrenz besonders auf diesem Sektor immer schärfer. Denn, wie wir Putin im Delete-Heft zitierten, „Wer immer sich zum Führer auf diesem Gebiet macht, wird die Welt beherrschen."

Die USA sehen sich gegenüber China auch im Hintertreffen bei der Konkurrenz um die Aufbringung der Datenmassen, die zur Durchsetzung der neuen Technologien aufgebracht werden müssen. Als totalitärer Staat ist China in der Lage, dies viel effizienter und ohne Rücksicht auf Persönlichkeitsschutz zu organisieren als die relativ liberalen USA.

---

4 Ist Trump der neue „Teddy"? Die Globalisierung des populistischen Momenmts, Hydra No. 1, www.the-hydra.world

5 https://capulcu.blackblogs.org/wp-content/uploads/sites/54/2018/12/DELETEA4_web.pdf

Eine große Rolle für die Durchsetzung der neuen Technologien spielt auch die Zurichtung der Bevölkerung und ihre Adaption an deren Anforderungen. So rücken etwa Scoring-Systeme zunehmend in den Fokus der Konkurrenz. Bei ihnen hat ein Regime wie das chinesische große Vorteile, wie die Entwicklung von *Sesame Credit* zeigt. Eine neue Massifizierung unter dem Regime der Informationstechnologien ist schon jetzt zu beobachten, ebenso wie die tayloristischen Technologien im fordistischen Zyklus für eine bis dahin ungekannte Massifizierung der Lebensbedingungen gesorgt hatten. Auch sie wird Gegenstand internationaler Konkurrenz bei der Effektivierung sozialer Kontrolle und damit Teil des neuen Griffs nach der Weltmacht.

Der von Trump entfesselte Handelskrieg wird zunehmend zum Medium der Konkurrenz im Griff nach der Weltmacht. Die USA haben zu diesem Zweck das überkommene WTO-System praktisch zertrümmert und nutzen, wie schon in der fordistischen Ära (wo Deutschlands merkantilistische Politik sich zum Vorreiter machte), ihre enorme wirtschaftliche Nachfragemacht dazu, den Handelspartnern ihre Bedingungen aufzuherrschen. So zum Beispiel darin, die Produkte der chinesischen Firma Huawei auf den von ihr kontrollierten Märkten zurückzudrängen. Sie wird nicht die einzige bleiben. Zudem hat die Regierung angekündigt, die Exporte von Produkten auf dem Gebiet der Informationstechnologie und hier besonders der KI zu regulieren und sogar einschränken zu wollen.

Es ist der Eintritt der Konkurrenz in ein Stadium des „technologischen kalten Kriegs", den Experten inzwischen diagnostizieren. Er kann jederzeit in einen heißen übergehen. Wie ihn ja auch die Treiber des technologischen Angriffs im Fordismus zur Durchsetzung der damals neuen Technologien im Griff nach der Weltmacht gesucht haben.

Libra

EINLEITUNG

Im Sommer 2019 macht Facebook öffentlich, woran es gerüchteweise schon länger arbeitet: Das Libra genannte Projekt soll eine neue Kryptowährung werden. Mit von der Partie sind Silicon-Valley-Größen wie Ebay und Uber, aber auch PayPal, MasterCard, Visa und Vodafone und einige mehr. Am 15.7.2019 erscheint das Whitepaper zum Projekt[6] – eine Art Werbetext, der zum einen weitere Mitstreiter*innen gewinnen will, aber im Wesentlichen Bedenken zerstreuen soll.
Das Whitepaper strotzt nur so vor Altruismus. „Finanzielle Inklusion" derjenigen, die bislang kein Bankkonto hatten, leichter Zugang zu billigen Krediten, Kontrolle über das eigene Geld und neue wirtschaftliche Möglichkeiten – der Aufbruch in eine bessere Welt (des Kapitalismus).

Was das Whitepaper verschweigt, ist das Business-Model dahinter. Nur vage ist von neuen FinTech-Produkten die Rede und einer größerer Zahl von Menschen, die enger an den Kapitalismus gebunden werden sollen. Warum starten Facebook und all die anderen dieses Projekt? Alle sind kapitalistische Unternehmen, die dem Shareholder Value verpflichtet sind. Altruismus mag zwar gut sein für den Ruf eines Unternehmens, wirkt sich aber auf den Börsenkurs kaum aus.

Anscheinend glaubt auch niemand diesen Altruismus – das Projekt bekommt viel Gegenwind und die Zahl der Mitstreiter*innen schwindet: Ebay steigt aus, später Visa, MasterCard und PayPal. Das Gründungspapier[7]

6 https://libra.org/en-US/white-paper/

7 https://libra.org/wp-content/uploads/2019/10/Libra-Association-Charter-Press-Release-.pdf

der Libra Association erscheint am 15.10.2019, die Anzahl der beteiligten Institutionen ist von 28 auf 21 geschrumpft.

„Regiert" werden soll Libra von der genannten Libra Association. Um ihr den Anstrich von Neutralität zu geben, soll der Sitz in der Schweiz sein. Anfangs ist die Schweizer Finanzaufsicht geneigt, Libra zu bewilligen, doch der internationale Druck führt im Januar 2020 zur Absage. Weitere Mitglieder der Libra Association streichen die Segel: Vodafone will sich lieber auf sein M-Pesa-Projekt[8] konzentrieren – einem Mix aus Zahlungsdienstleister und Bank, der z.Z. in Afrika ausgebaut wird.

Am Ende verspricht Mark Zuckerberg, Chef von Facebook, Libra erst dann zu starten, wenn alle Bedenken der US-Regulierungsbehörden ausgeräumt sind. Der harte Gegenwind war absehbar, trotzdem ist das Projekt in dieser Form gestartet.

STABLE COIN

Libra ist eine *Stable Coin*. Wie bei anderen Kryptowährungen auch, gibt es in dieser Währung keine Münzen oder Scheine, sondern Besitz an Libra manifestiert sind durch Kontostände im geteilten Buchhaltungssystem. Anders als bei Kryptowährungen wie *Bitcoin* oder *Ethereum* bestimmt sich der Wert von Libra nicht auf einem „Markt" - ein Bitcoin ist soviel Wert, wie jemand anderes bereit ist, dafür zu zahlen – sondern das Geld, was für den Erwerb einer bestimmten Menge Libra eingezahlt werden muss, wird „geparkt" und wieder ausgezahlt, werden die Libra zurückgetauscht. Eine Stable Coin ist also nicht den Wertschwankungen „normaler" Kryptowährungen ausgesetzt, sondern „nur" denen der hinterlegten Währungen. Dieser Mechanismus soll die Wertstabilität der Stable Coin realisieren.

Stable Coins (Libra ist weder die einzige noch die erste Stable Coin) sind ein vergleichsweise junges Phänomen in der Welt der Kryptowährungen. Sie dienen dazu, Geld zwischen den verschiedenen Handelsplätzen für Kryptowährungen (Exchanges) zu transferieren, Geld zu parken und die eigentliche Herkunft einer Transaktion zu verschleiern. Auch spielen sie eine zentrale Rolle beim on- und off-ramp – dem Transfer von „normalem" Geld in die Welt der Kryptowährungen und wieder zurück – und das möglichst anonym.

Das kollidiert nicht nur mit den diversen Gesetzgebungen gegen Geldwäsche, Steuerhinterziehung und verdeckter Finanzierung, sondern auch mit dem den Banken auferlegten Prinzip des „Know your customer".

Tether[9] ist die nach Marktkapitalisierung zur Zeit größte Stable Coin und blickt auf eine Geschichte von Betrugsverfahren, Geldwäsche, Beinaheinsolvenzen und Veruntreuung zurück[10]. Tethers zentrales Feature ist das on- und off-ramp, dieses Feature ist für die Welt der Kryptowährungen so zentral, dass selbst ein fundierter Veruntreuungsverdacht von hinterlegtem Geld nicht dazu führt, dass Leute die Finger davon lassen.

Für das on- und off-ramp ist eine Zusammenarbeit mit einer Bank notwendig. Den Betreibern von Tether ist Anti-Geldwäschegesetzgebung oder das „Know your customer"-Prinzip egal, für die Kunden von Tether ist es sogar ein Feature, dass Tether hier alle Augen zudrückt. Für die beteiligten Banken ist das allerdings heikel, so heikel, dass sich Tether in Banken einkaufen musste, um eine Zusammenarbeit zu gewährleisten – mindestens eine Bank[11] hat das dann auch in den Abgrund gezogen, sie hat ihre Lizenz verloren.

Dieser kurze Exkurs in die schattige Welt der Stable Coins mag eine Erklärung liefern, warum Institutionen wie PayPal, Visa und MasterCard aus der Stable Coin Libra ausgestiegen sind. PayPal riskiert seine Banklizenzen, Visa und MasterCard ihre guten Beziehungen in die Bankenwelt.

Eine zentrale Kritik der diversen Regierungen und Zentralbanken an Libra ist, dass dessen Betreiber*innen nicht zufriedenstellend erklären, wie sie Geldwäsche, verdeckte Finanzierung und Steuerhinterziehung verhindern und zumindest rückwirkend aufklären können.

ANONYM, PSEUDONYM, TOTAL ÜBERWACHT

„The Libra Blockchain is pseudonymous and allows users to hold one or more addresses that are not linked to their real-world identity."[12]

Dieser Satz aus dem Whitepaper ist bemerkenswert widersprüchlich – entweder ist Libra pseudonym, dann gibt es eine Verbindung zwischen Adressen (gemeint sind Konten) und „Real-World"-Identitäten – oder es gibt diese Verbindung nicht, dann wäre Libra anonym. Oder diese Verbindung existiert außerhalb der Libra-Blockchain, dann stellt sich die Frage, wer diese Daten erheben, verwalten und inwertsetzen kann.

8 https://www.vodafone.com/what-we-do/services/m-pesa

9 https://tether.to/

10 https://www.kalzumeus.com/2019/10/28/tether-and-bitfinex/

11 Noble Bank, Puerto Rico

12 Libra white paper

Dem Technical Paper zur Blockchain von Libra lässt sich entnehmen, dass Adressen nur von Validator*innen erzeugt - genauer: aktiviert werden können. Die Adresse muss jede*r Teilnehmer*in selbst erzeugen (es ist im Wesentlichen ein öffentlich/privates Schlüsselpaar), damit die Adresse aber nutzbar wird, muss sie dem System bekannt gemacht werden. Das geschieht durch eine initiale Transaktion auf diese Adresse – ausgeführt (oder verweigert) durch eine*n Validator*in.

Validator*innen gibt es in jeder Kryptowährung, ihre Rolle ist es, beantragte Transaktionen zu bestätigen und damit wirksam werden zu lassen. Dass Validator*innen auch das Aktivieren von Konten übernehmen, ist eine Eigenart von Libra – andere Kryptowährungen kennen das Konzept einer dezidierten Kontoaktivierung gar nicht. Wer wann Validator*in für wieviele Transaktionen werden kann, ist je nach Kryptowährung sehr unterschiedlich. Bitcoin etwa verlangt einen Proof of Work – wer/welche eine überprüfbare Menge an Rechenzeit investiert hat, darf den nächsten Block der Blockchain zusammenstellen und damit die in diesem Block enthaltenen Transaktionen validieren. Jeder/jede, der/die die entsprechende Rechenkapazität aufrufen kann, kann also Validator*in werden.

Libra arbeitet da anders – Validator*innen sind die Mitglieder der Libra Association. Sie sind durch ihre libra-spezifische Rolle als Türsteher*innen der Kontenaktivierung in einem Interessenkonflikt: Einerseits soll die Hürde für das Erstellen eines Libra-Kontos möglichst niedrig sein, damit schnell eine große Zahl an Nutzer*innen eingemeindet wird, andererseits muss das Prinzip des „Know your customer" befolgt werden, sonst droht Ärger von Seiten der diversen Regulator*innen.

Die Mitglieder der Libra Association haben jeweils 10 Millionen US-Dollar Eintrittsgeld bezahlt. Perspektivisch soll jedoch der Kreis der Validator*innen geöffnet werden – von einem Proof of Authority soll zu einem Proof of Stake gewechselt werden. Validator*in kann dann jede*r werden, wer/welche nachweislich Geld im System angelegt hat. Wann und wie genau dieser Übergang stattfinden soll, ist nicht formuliert. Mittlerweile scheint dieser Übergang obsolet geworden zu sein: In einem Statement vom 16.4.2020 verabschiedet sich die Libra Association von der Öffnung des Validator*innen-Pools. Die Association wird bis auf weiteres ein handverlesener Kreis bleiben.

Wie auch immer die Hürde zur Erlangung eines Libra-Kontos ausfallen wird, bei den Validator*innen laufen alle Daten zusammen – welche Transaktionen in welcher Höhe, Zeitpunkt der Transaktion, die beteiligten Konten und die Verknüpfung zu den *Real-World*-Identitäten hinter den beteiligten Konten.

Und: Wie auch immer die Hürde zur Erlangung eines Libra-Kontos ausfallen wird: Ist sie niedrig, dann ist die Chance auf eine schnelles Wachstum gegeben – mit einem hohen Rauschen in den Daten, oder sie ist hoch, dann wird das Wachstum nicht so stark ausfallen, die angesammelten Daten – die „Real-World"-Identitäten – sind dafür „echt"(er). Insofern ist eine Regulierung von Libra für Libra eventuell gar kein großes Problem.

Dass Libra ausgerechnet bei Facebook entwickelt wurde, lässt Schlimmes erahnen, was die Weiterverwertung der gesammelten Daten betrifft. Das scheint Facebook auch selbst bewusst zu sein – Facebook beteiligt sich nur über eine „unabhängige" Tochter (Calibra) an dem Projekt. Allerdings sind die Messaging Apps von Facebook – Facebook Messenger, WhatsApp und Instagram – die Apps, über die sich Libra als erstes nutzen lassen soll. Selbst wenn diese Apps die Transaktionen nicht selbst durchführen, sondern dafür Software der Libra Association (z.B. via Plugin) nutzen würden – aus dem Kontext allein fallen schon verwertbare Daten an.

Allein am Beispiel von WhatsApp lässt sich beurteilen, wie viel Wert das Versprechen von Facebook hat, sich aus der direkten Transaktionsabwicklung raus zu halten – nämlich keinen. Facebook hatte WhatsApp im Februar 2014 gekauft, mit dem Versprechen und der Auflage, die Nutzer*innen-Daten von WhatsApp nicht mit den Daten von Facebook zusammenzuführen. Spätestens 2016 war dieses Versprechen schon Makulatur und die EU-Kommission verhängte eine Strafe von 110 Millionen Euro als Warnung wegen Falschangaben bei der Unternehmensfusion. Gegen die Zusammenführung der Daten an sich gab es seitens der Brüsseler Behörde keine Einwände. Eine Einladung, das beim Libra-Projekt zu wiederholen.

LOGIN VIA FACEBOOK

Viele Webseiten erlauben schon jetzt den Zugriff auf personalisierte Dienstleistungen via eines Logins bei Facebook. Die Betreiber*in einer Webseite, die einen Login via Facebook erlaubt, bindet einen Codeschnippsel von Facebook statt des normalen Logins ein. Dieser Codeschnippsel implementiert einen tatsächlichen Login bei Facebook und liefert der Betreiber*in Name, Email und weitere Daten über die Person, die sich gerade eingeloggt hat. Facebook wird zum Garant für diese/n Nutzer*in – fast wie ein Melderegister. Die Facebook-ID bekommt den Charakter eines digitalen Personalausweises. Dass Facebook eine Klarnamenpflicht hat, passt zum Konzept.

Die Nutzer*in des Logins via Facebook „gehört" Facebook – das bestimmen die AGB des genannten Codeschnippsels. Facebook sichert sich damit Zugriff auf Nutzer*innenverhalten auf Seiten, die mit Facebook ansonsten gar nichts zu tun haben. Die „Like"-Buttons von Facebook fallen in die gleiche Kategorie.

Für Facebook liegt nichts näher, als auch das (oder die) Libra-Konten in das Nutzer*innenprofil zu integrieren. Die Facebook-ID erweitert sich vom Personalausweis zum Personalausweis mit Zahlungsfunktion.

Mit der Integration von Libra in die Messaging-Apps von Facebook verleiht Facebook dem erweiterten „Personalausweis" eine entsprechend große Nutzer*innenschaft. Funktionsmäßig würden diese Apps mit vergleichbaren chinesischen Apps gleichziehen oder sie evtl. sogar überholen. WeChat bietet neben Chat (also Messaging) diverse weitere Funktionen – u.a. eine Zahlungsfunktion: WeChat Pay. WeChat Pay implementiert allerdings keine eigene Währung, sondern ist eher mit PayPal vergleichbar.

Libra könnte für die Facebook Messaging-Apps zum Killerfeature werden. Und: Von Facebook vielleicht gar nicht intendiert, könnte das zum Killerfeature für Smartphones werden – ein Leben ohne die dann im Smartphone angesammelten Funktionalitäten wäre immer aufwendiger.

WÄHRUNGSPOLITIK

Libra werden erworben, indem sie gegen eine gleichwertige Menge einer klassischen Währung getauscht werden. Dabei passiert einer Verdopplung des Wertvolumens – das Wertvolumen existiert jetzt in Form von Libra und in Form der „hinterlegten" klassischen Währung. Erst beim Rücktausch löst sich diese Verdoppelung wieder auf. Libra verspricht, keine eigenständige Geldschöpfung zu betreiben, also kein Geld aus dem Nichts zu erschaffen. Technisch wäre das ohne Probleme möglich, es ist also an den Aufsichtsbehörden, entsprechende Machenschaften zu enttarnen.

Facebook sieht seine Messaging-Apps als Tools zur Benutzung von Libra vor. Libra ausgeben soll nicht schwieriger sein als das Versenden einer Message. Die Nutzer*innenzahl der drei Apps zusammen beträgt etwa 2,7 Milliarden – das entspricht grob einem Drittel der Menschheit. Sollte sich Libra etablieren, dann sammelt die Libra Association eine Menge Geld von einer Menge Nutzer*innen ein.

Selbst wenn die Libra Association das eingesammelte Geld nur in einen Tresor legen würde, wäre das schon ein Eingriff in den Devisenmarkt. Das eingelagerte Geld wäre der Zirkulationssphäre entzogen, würde also zu einer Verknappung führen und damit den Kurs der betroffenen Währungen steigern. Umgekehrt könnte die Libra Association durch eine gezielte Ausschüttung (z.B. durch Tausch einer Währung in eine andere) den Kurs einer Währung schwächen. Die Libra Association hat angekündigt, das hinterlegte Geld u.a. in Form eines „Währungskorbes" aus „stabilen" Währungen zusammenzusetzen – allein durch eine Verschiebung der Zusammensetzung dieses Währungskorbes kann die Association Politik über den Hebel des Devisenmarkts machen.

Schon im Whitepaper wird aber klargestellt, dass eine „Tresorlösung" nicht angestrebt wird – neben einem „Währungskorb" in Form von Bankeinlagen ist von kurzfristigen Staatsanleihen die Rede[13]. Das eingesammelte Geld wird also weiter verliehen – an Banken in Form von Einlagen oder an Staaten, die einzige „Bedingung" ist eine geringe Wertschwankung, was weitere Anlageformen explizit nicht ausschließt.

Libra strebt an, zu einer Art Schattenwährung zu werden, die parallel zu den jeweiligen Nationalwährungen existiert. Üblicherweise etablieren Staaten in ihrem Machtbereich ein „gesetzliches Zahlungsmittel" - die eigene Währung –, in dem Transaktionen akzeptiert werden müssen. Nationalbanken sichern sich so ihren währungspolitischen Hebel. Staaten mit inflationsgeplagten Währungen kennen das Problem, wenn Kapital aus der Nationalwährung in eine Schattenwährung flüchtet (historisch meist der US-Dollar, aber auch Euro oder Schweizer Franken). Geldpolitische Interventionen von Nationalbanken wirken sich dann auf eine geringer werdende Kapitalmasse aus. Was passiert, wenn eine Nationalbank komplett die Kontrolle über das „gesetzliche Zahlungsmittel" verliert, lässt sich am Beispiel von Griechenland studieren.

Sollte sich Libra etablieren, dann sammelt die Libra Association ein erhebliches ökonomisches Erpressungspotential ein.

Update: Am 16.4.2020 verkündete die Libra Association, Libra nicht mehr nur gegen einen Währungskorb, sondern auch gegen konkrete Währungen zu binden – es gäbe dann zusätzlich einen Euro-Libra, einen Dollar-Libra usw.

13 Libra whitepaper: … it (Libra) will be backed by a collection of low-volatility assets, such as bank deposits and short-term government securities in currencies from stable and reputable central banks.

PRIVATISIERUNG DES GELDES

Libra ist ein weiterer Schritt in der Entwicklung, alle möglichen Bereiche der Gesellschaft zu privatisieren. Libra ist die Privatisierung des Geldes. Dass Libra harten Gegenwind erfahren würde, war vorhersagbar, Libra ist schon fast der Maximalentwurf einer privatwirtschaftlichen Währung. Ein Testballon, um heraus zu bekommen, was an Privatisierung z.Z. durchsetzbar ist. Dass Libra dabei in der Umsetzung Abstriche vom Ursprungsentwurf machen muss, war vermutlich allen bewusst, die das Projekt gestartet haben.

Libra ist eine konsequente Umsetzung libertärer Ideologie, den Staat an möglichst vielen Stellen zurück zu drängen und in seiner Macht zu beschneiden. Damit reiht es sich in die anderen Kryptowährungen ein, die ebenfalls den Staat und seine Zentralbank als bekämpfenswertes Problem ausgemacht haben. Libra jedoch hat eine Zentralbank, nur dass diese verteilt auf die Mitglieder der Libra Association ist. Als Validator*innen kontrollieren die Mitglieder, welche Transaktionen wirksam werden und welche nicht, sie kontrollieren über die Kontenvergabe, wer mitspielen darf und können über den Währungskorb und die Verwendung des hinterlegten Geldes Geldpolitik betreiben.

Wer die Validator*innen kontrolliert, ist derzeit umkämpft – allerdings scheint es den Regulierungsbehörden mehr um Geldwäsche und Steuerhinterziehung zu gehen, als um die Auswirkungen einer Privatisierung. Es ist ein Nebenschauplatz und Mark Zuckerbergs Einknicken vor den US-Regulierungsbehörden weniger dramatisch für das Libra-Projekt, als es in den Medien erscheint.

Libra ist ein unverhohlener Griff nach der Macht. Ähnlich wie es neben Facebook fast unmöglich erscheint, ein zweites soziales Netzwerk (in dieser Größe und mit dieser Ausrichtung) zu etablieren, wird es schwierig, neben Libra eine zweite Kryptowährung mit vergleichbarem Charakter und entsprechender Größe aufzubauen – ein „Aus dem Stand"-Monopol.

Den Währungshüter*innen diverser Nationen ist das nicht entgangen. Schon vor Libra planten einige Zentralbanken an Blockchain gestützten Versionen der eigenen Währung. So hat die EZB bereits 2018 mit EUROchain einen Prototyp für einen Blockchain-Euro entwickelt.[14] Das Libraprojekt ist Wasser auf diese Mühlen und weitere Länder planen an digitalisierten Währungen – z.B. dem tunesischen E-Dinar. Auch China arbeitet an einer digitalen Version des Yuan, dem DPEC – unter anderem in bewusster Abgrenzung zu Libra, welches als „Äquivalent der Rückkehr zu einer primitiven Gesellschaft"[15] gezeichnet wird. Aber das gilt wohl für alle digitalen Währungen inklusive des DPEC.

Aus linksradikaler Perspektive ist am Staat, dessen Zentralbank und Nationalwährung kaum etwas Verteidigenswertes zu finden. Libra zeigt jedoch auf, dass es noch hässlicher werden kann.

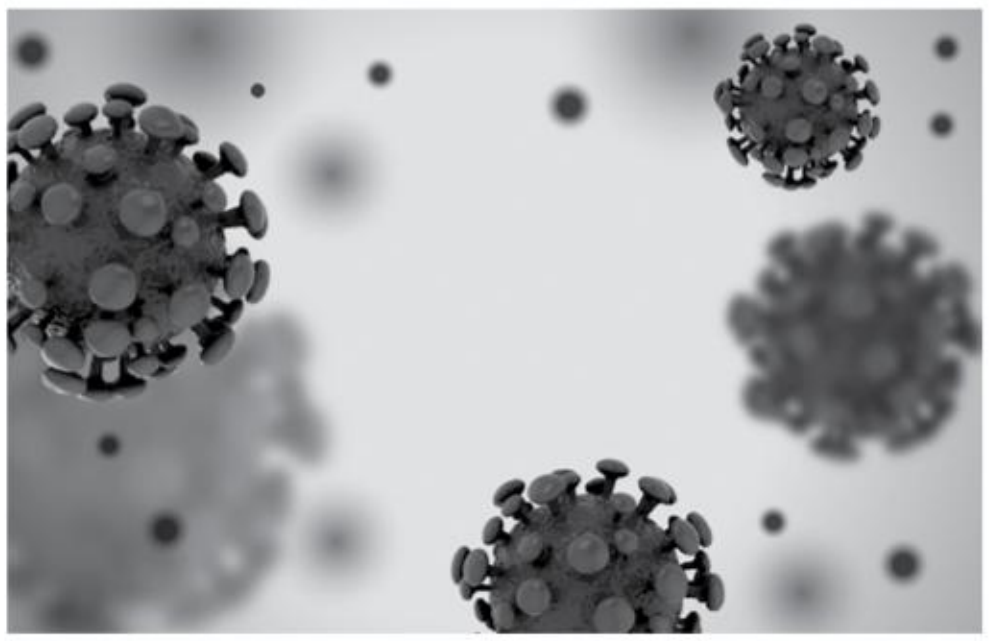
---

14 https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf

15 https://www.followcn.com/china-central-bank-will-be-the-first-to-issue-digital-money-says-prominent-political-figure/

Eine Art von „Krieg“ oder das Wüten des „digitalisierenden Virus“

Der Beitrag berichtet, wie der „Krieg“ gegen die Coronapandemie dazu genutzt wird, die „animal spirits“ (Keynes), die aggressiven unternehmerischen Kräfte der IT-Innovationsoffensive aus der Stagnation zu reißen und ihnen einen neuen Schub zu verleihen – ähnlich, wie es der Krieg 1914 mit den „animal spirts“ des Taylorismus getan hat. Wir haben wenig Zweifel an dieser Deutung. Denn wir haben hier immer wieder die Ähnlichkeiten und Analogien der großen historischen technologischen Angriffe herausgearbeitet. Allerdings greift unsere Deutung auf dem Hintergrund des Geschehenen mit Hilfe der historischen Erfahrungen prognostisch ins Unerforschte der zukünftigen Angriffsstrategien der Gegenseite. Darum versehen wir dieses Deutungsangebot mit zwei Ausrufezeichen und einem Fragezeichen.



Wir möchten mit drei Schlaglichtern zum aktuellen sozialpsychologischen Klima auf den autoritären Herrengestus, den unbedingten Willen zur Verwertung der Krise und die allgegenwärtige Kriegsmetaphorik einleiten. Sie wirken in unterschiedlichen Mischungen, Akzentuierungen und kulturell bedingten Einfärbungen in allen Ländern und beleuchten nicht nur treffend den komplexen Angriff des Corona-Moments, sondern formen auch die Zukunft und werden nicht mehr weggehen. Das erste ist ein Artikel von Wolfgang Michal im Freitag vom 16.4.2020 unter der Überschrift „Volksgemeinschaftsmoral bitte“. Darin analysiert er die Strategien der gegenwärtigen Coronakrisen-Inszenierung der Regierung unter dem Stichwort „Krisenkommunikationsstrategie“: lückenlose Geschlossenheit einer expertokratisch/politischen Dauershow im Sinne einer Hof- wie auch Frontberichterstattung. die infolge der föderalen Struktur auch Grüne einbindet. Sie lasse Risse nicht mehr erkennen und zelebriere die absolute Kommunikationshoheit, die die Bevölkerung zum volksgemeinschaftlichen Auditorium verkommen lasse. Empfohlen wird hierzu auch die Beleuchtung dieses Vorgangs als „Einübung in den Ausnahmezustand“ von Dirk Vogelskamp in *grundrechtekomitee.de*[16]. Aus der unten erörterten Parallelität zu 1914 könnte man hinzufügen: „Angesichts der Krise kenne ich keine Parteien mehr, ich kenne nur noch Deutsche“. Die Krise ist nach Meinung der Expert*innen katastrophisch. Sie übersteigt, ja, potenziert die von 2008, was soviel heißt, wie dass sie der Weltwirtschaftskrise von 1929 bis 1945 gleichkommt.

Das zweite Schlaglicht ist der offensichtliche unbedingte Wille, die Krise zu nutzen. Wir haben einen derartigen Willen Merkels schon gegenüber der Drohung des globalen Zusammenbruchs im Jahre 2010 kennengelernt[17]. Damals war es der Wille, die Krise zur Realisierung des alten deutschen Traums von einem deutschen Europa zu verwerten. In ähnlicher Weise spekuliert ihre Digital-Staatsministerin Dorothea Bär, so wie auch die führenden Akteure in anderen Ländern, nunmehr auf einen „massiven Schub“ durch die Coronakrise. In europäischer Verzweiflung allerdings im Kampf gegen die gähnende digitale Lücke gegenüber China und den USA (dazu unten mehr). Und schließlich rät der hierzulande als bloßer Spekulant sträflich unterschätzte George Soros, angesichts der Bedrohung Europas in dieser tiefen Krise und dem „once-in-a-lifetime war against a virus“, zur Anwendung von „perpetual bonds“, „ewigen Anleihen“, die von England schon in den napoleonischen Kriegen und dem Ersten Weltkrieg“ eingesetzt worden seien.[18] Zinstragende Anleihen ohne eine ausdrückliche Pflicht, aber mit dem Recht zur Rückzahlung, das von der englischen Regierung auch wahrgenommen wurde. Sie sind ein kriegsökonomisches Instrument und so ist auch die Kriegsmetaphorik allgegenwärtig, auch wenn die „Frontberichterstattung“ in Deutschland aus historischen Gründen das Wort „Krieg“ vermeidet. Wir kennen sie beispielsweise von Macron, oder dem ehemaligen Vorsitzenden der englischen Zentralbank Mark Carney. Auf den Punkt gebracht hat der zwar nach rechts abgeglittene, aber durchaus intelligente Varoufakis die Maßnahmen im Zusammenhang mit der schuldenfinanzierten Geldflutung als „Kriegsökonomie ohne Krieg“. „The analogue of war“, das war die Überschrift des Historikers William Leuchtenburg über Franklin D.

16 www.grundrechtekomitee.de/details/pandemie-versus-demokratie-oder-die-einuebung-in-den-ausnahmezustand

17 Vgl. dazu D. Hartmann, J. Malamatinas, Krisenlabor Griechenland, Berlin, Hamburg 2011, S. 53 ff.

18 The Guardian 21.4.20, wiederholt in einem Gastbeitrag im Spiegel vom 1.5.20.

Roosevelts 1933er Aufgalopp zum sogenannten „ersten New Deal“, der seine Verwirklichung im Übergang zur Kriegsökonomie der späten 30er Jahre finden würde[19]. Autoritärer Herrschaftsgestus, Krisennutzung, Kriegs- und Frontmetaphorik, Kriegsökonomie ohne Krieg, sie alle summieren sich, das sagt uns die Geschichte, zu einer äußerst brisanten Situation.

DIE KRISENLAGE

In einem Artikel vom 29.4.2020 für Project Syndicate thematisierte der renommierte amerikanische Ökonom von der New York University Nouriel Roubini, seit Jahrzehnten Mitarbeiter höchstrangiger Beratergremien, „Zehn Gründe, warum eine größere Depression in den 20er Jahren unvermeidlich ist“. Sie hätten allerdings für Trends gestanden, die schon vor Corona gewirkt hätten. Es sind im Kern diejenigen, die wir in der online-Zeitschrift „Hydra“[20] seit langem beobachten, vor allem das ungeheure Ausmaß ökonomisch nichttragbarer (unsustainable) Verschuldung auf allen Ebenen. Ebenso hat der „Hydra“-Krisenticker#3[21] den in den vorhergehenden Krisentickern dargestellten Krisenpegel in seiner ökonomischen Dimension durch eine dramatische Entwicklung der globalen Verschuldung charakterisiert. Waren sie vom Jahr des globalen Crashs 2008 bis Anfang 2017 von 97 Billionen (US-amerikanisch „trillions“) auf 169 (laut IWF Global-Data-Base sogar 184) Billionen angewachsen. So hat sich inzwischen die Verschuldung derart dramatisch weiterentwickelt, dass sich die amerikanische Federal Reserve (Fed) 2019 zur erneuten Anwendung einer Notmaßnahme aus dem Crash-Jahr 2008 gezwungen sah. Zur Sicherung des Vertrauens und der prophylaktischen Vermeidung einer totalen Austrocknung der Liquidität wurden wieder hohe „Übernachtkredite“ zur Verfügung gestellt. Das war noch unter den Bedingungen einer, wenn auch durch Schulden und Nachfrageverfall, Protektionismus, Abwertungswettbewerb stotternden globalen Mechanik. Der World Economic Outlook des IWF verzeichnet nunmehr aufgrund der durch Corona hinzugekommenen Bedingungen – Schuldensteigerung, Produktionseinschränkungen – den Absturz in die tiefste Krise seit der Großen Depression. Realistische Betrachter stellen sie dieser gleich.[22]

So mussten die USA Ende April dieses Jahres – bei einer Million Infizierter und 60 000 Toten – mehr als 30 Millionen krisenbedingte Arbeitslose hinnehmen, so viele wie nie in so kurzer Zeit, 18 % der Arbeitsbevölkerung mit einer Quote von fast 5 %, dazu einen dramatischen Wirtschaftseinbruch und im mittleren und unteren Bereich zahllose Firmenzusammenbrüche. Die deutschen Unternehmen haben für 10,1 Millionen Beschäftigte Kurzarbeit angemeldet bei gleichwohl zudem noch wachsender Arbeitslosigkeit und steigenden Firmenzusammenbrüchen, verfallenden Exporten und einem Rückgang der Wirtschaftsleistung um 6,3 %. In den übrigen großen Volkswirtschaften herrscht das gleiche Bild. Ebenso wie Roubini sieht der Finanzexperte aus Berkeley Barry Eichengreen Trumps ostentativen Optimismus als völlig verfehlt an. Er hält ihm die Gründe entgegen, warum die Auswirkungen des ökonomischen Schlags von Corona viele Jahre anhalten werden. Der ehemalige IWF-Chefökonom und Krisentheoretiker Kenneth Rogoff verweist darauf, dass kein Zusammenbruch der letzten 150 Jahre derart stark und schnell gewesen ist. Und China erlebt den schlimmsten Zusammenbruch seit der Kulturrevolution mit einem Mitte April registrierten Absturz des Wachstums von 6 % auf -6,8 % unter Einschluss des IT-Sektors und des Verbraucher*innenvertrauens. „Wir werden in China keinen V-förmigen Aufschwung sehen“, diagnostiziert der Chefökonom des auf China spezialisierten Berliner Mercator-Instituts.

Und vor allem: es ist kein „exogener“, dem Kapitalismus äußerlicher Schock. Vielmehr sind es die Bedingungen des Marktes und der Globalisierung, mit ihren bis ins Lokale reichenden Marktansammlungen, weltumspannenden Lieferketten und Verkehrsverbindungen, die die Coronaoffensive mit hervorgebracht haben. Sie ist ein genuines Produkt des gegenwärtigen Kapitalismus. Und das gilt auch für die Fluten eines weiteren „Geldtsunamis“, die, wie schon 2001 und 2008, zur Krisenlösung entfesselt werden.

STAGNATION DER DIGITALISIERUNG UND BLOCKIERUNG DER INNOVATIONSOFFENSIVE …

Wir wissen, dass Wachstum und Profitsteigerung nachhaltig nur durch Innovationsoffensiven erreicht werden können, weil allein sie die gesellschaftlichen Quellen von Produktivität angreifen, gestalten und erschließen und Produktivität erhöhen können. Dies ist auch die herrschende Meinung der Ökonom*innen. Innovationsoffensiven sind jedoch keine subjektfreien Geschehnisse. In ihnen verwirklicht sich das, was Keynes in seiner 1936 erschienen „General Theory“ die „animal spirits“ als subjektive, im weitesten Sinn unternehmerische Antriebskräfte bezeichnet hat, und was der ebenso bedeutende Ökonom Joseph Schumpeter als die in den innovativen Akteuren verkörperten Kräfte der

19 D. Hartmann, Krisen, Kämpfe, Kriege, Bd. 2, Innovative Barbarei gegen soziale Revolution. Kapitalismus und Massengewalt im 20. Jahrhundert, Berlin, Hamburg 2019, Kap. 8.4.

20 www.the-hydra.world/index.php/krisenticker/

21 Murmeltier ante portas, www.the-hydra.world Krisenticker#3

22 Auf den Hydra-Krisenticker#4 wird verwiesen.

„schöpferischen Zerstörung“ beschrieben hat.[23] All das begründet die Brisanz der Befunde aus dem Working Paper der OECD No. 1533 von Februar 1919. Danach stagnierten die Durchsetzung der IT-Technologien und Gewinne zugleich mit den in ihnen verkörperten „animal spirits“. In den großen Industriegiganten weitgehend verwirklicht, machte die Offensive an der Grenze zum Gefälle der überkommenen Betriebsformen halt. Die Ursachen können nur in Resistenzen – etwa das Beharren auf überkommenen Lebens- und Arbeitsformen – zu suchen sein, die die Fortsetzung der Digitalisierung blockieren. Es ist das, was Bär mit der gebotenen Zurückhaltung so charakterisiert: „Eine Studie, die ich seit längerem zitiere, sagt, dass wir Deutschen den Wandel nicht mögen, wenn wir aber dazu gezwungen werden, bewältigen wir ihn am besten.“[24] In der Tat sind die Wege aus der biedermeierähnlichen Gemütlichkeit der Stagnation des Kapitalismus in der deutschen Geschichte unter dem Diktat krisenhafter „Zwänge“ immer mit geballter Gewalt verbunden gewesen.

… UND DER DURCHBRUCH DURCH CORONA, DAS „DIGITALISIERENDE VIRUS“

Nachdem Bär ähnlich schon im November 1918 davon gesprochen hat, dass Deutschland eine Krisenmentalität brauche, um die Digitalisierungslücke zu schließen[25], sieht sie in der Coronaepidemie die Chance, „… dass die Digitalisierung auf diese Weise einen massiven Schub erfährt.“[26]Obwohl sie sich diese Weise nicht gewünscht habe. Selbstredend, geschenkt. Aber Bär ist nicht so zartfühlend, wie sie tut. So ist sie durch ihre Robustheit aufgefallen, als sie autonome Flugtaxis propagierte. Fürs erste sieht sie Einsatzfelder des Digitalisierungsschubs in Videokonferenzen, Homeoffice, Bildung und Erziehung („Vieles, was in der digitalen Bildung versäumt wurde, wird jetzt ausprobiert“), der staatlichen Verwaltung im E-Government oder dem „Digitalen Staat“ – und natürlich im Gesundheitssektor (auf Corona gemünzt: Vernetzung der Ärzte untereinander und mit Krankenhäusern, kontaktloses Fiebermessen, Pflegeroboter zur Medikamentenverteilung). Das gelte auch für die Corona-App. „… die man am Anfang jetzt mal freiwillig starten (muss), in der Hoffnung, dass es dann auch möglichst viele nutzen. Und dann muss man einfach dem Ganzen mal eine Chance geben.“.[27]

DIE TECHNOLOGISCHEN AUFMARSCHFELDER IN DER NUTZUNG DER CORONAKRISE

Als exemplarisch für die Unternehmerseite kann man das Startup-Management der Spherity GmbH anführen. Es vertreibt dezentrales Identitätsmanagement im Sinne sicherer Identitäten in der Kombination von Unternehmen, Maschinen, intelligenten Geräten und Algorithmen. Ihr Mitgründer und General Manager Carsten Stöcker hat in der FAZ vom 20.4.20 „Die positive Seite dieser Krise“ propagiert, bezeichnenderweise zusammen mit Hochschullehrer, Netzwerkberater und Vorstandmitglied des Blockchain Bundesverbandes Prof. Markus Büch und Kryptowährungsspezialisten Prof. Philipp Sandner. Danach fordert die Coronaepidemie zum Beispiel bei der Heimarbeit „einen hohen Grad von Digitalisierung“ heraus. „So ist Corona auch das ‚digitalisierende’ virus“, denn „grundsätzlich hat das Corona-Virus geschafft, was viele Manager und Digitalisierungsberater nicht geschafft haben.“ Als Einsatzfelder des viralen „Digitalisierungsschubs“ nennen die Autoren E-Justiz, E-Notariat und E-Government, E-Health mit Videosprechstunden, digitaler Versicherungskarte und Rezeptur, den digitalen Euro und digitale Bildung. Sie erwarten vom Corona-induzierten „Schub“ Wirkungen über die Zeit des Corona-Lockdown hinaus, wobei sie sich auf Ministerin Bärs Ferment der „Krisenmentalität“ berufen. Der Staat soll „als langsamer Tanker mit einer ganzen Flotte von Schnellbooten“ (gemeint sind wohl kleinere Unternehmen, Start-ups) im Sinne einer Public-Private-Partnership operieren. Er soll „die Komfortzone der Tagesgeschäfte verlassen … und den Turbo in der Digitalisierung zünden. Führt die Politik dann noch digitale Infrastrukturprogramme, digitale Identität und den digitalen Euro ein, so, wie es die Amerikaner mit ihrem Stimulusprogramm vorgemacht haben, entstehen neuartige digitale Ökosysteme. Nicht zu vergessen: Am Ende geht es darum, auch später mit digitalen Lösungen nachhaltig Geld zu verdienen. Denn nur so erreichen wir mehr, als das Heranzüchten digitaler Eintagsfliegen … Nun sollten proaktiv die entlegensten Winkel der Gesellschaft digital durchdrungen werden“.

Auch das Handelsblatt, als das grundsätzlich und in der Berichterstattung profilierteste Blatt, belegt in seiner Printausgabe – vornehmlich an Einzelbeispielen – diesen Schub: Zunächst grundsätzlich im Sinne eines Leitartikels: „Die Krise ist unsere Chance … schafft Bedingungen für radikale Veränderungen, … eine ‚Can-do’-Mentalität“ (16.4.20). „Corona spornt massive Investitionen in die Digitalisierung, d. h. die digital gestützte Automatisierung des Flughafenbetriebs an“ (23.4.20). „Das Coronavirus beschleunigt den Wandel … virale Beschleunigung im Hörsaal“ der privaten Hochschulen vornehmlich im Management- und Business-Bereich (24.4.20). Proptechs, also Immobi-

23 Dazu D. Hartmann, Krisen, Kämpfe, Kriege, Band 1, Alan Greenspans endloser „Tsunami“, Eine Angriffswelle zur Erneuerung kapitalistischer Macht, S. 66 ff., 199 ff, 202 ff.

24 Frankenpost vom 22.3.20

25 C. Stöcker, M. Büch, P. Sandner, Die positive Seite dieser Krise, FAZ 20.4.20

26 Frankenpost a.a.O.

27 www.teltarif.de/baer-digital--app-corona/news.80196.html

lien-Start-ups, macht Corona zu „Krisengewinnlern“. (24.4.20). Des Weiteren das Übliche zu Heimarbeit und Universitäten.

Der Digitalisierungsschub in der Justiz beschleunigt sich mit einer für diese konservative Schnecke rasenden Geschwindigkeit. Der Widerstand und das Beharrungsvermögen der an Papierakten gewöhnten Richter*innen bröckelt rapide, eine umfassende Digitalisierung wird eingeleitet. Auch des Schriftverkehrs und durch Videokonferenzen, etwa im Arbeits- und Sozialrecht. Ausgenommen dort, wo es auf den face-to-face-Eindruck und -einwirkung ankommt, bei Zeug*innenbefragungen und im Strafprozess.[28]

Shopping und Tourismus sollen laut DIHK durch den massiven Einsatz von Apps wiederbelebt werden. In einem Merkel und den Koalitionsspitzen zum Wochenende 25./26.4. zugeleiteten Konzeptpapier schlägt der DIHK vor, den Zugang zu Fußgängerzonen, Geschäften und Hotels über Tickets zu begrenzen, die über eine App ausgegeben werden könnten und mit deren Hilfe Kund*innen Einkaufszeiten und Dienstleistungen buchen könnten. An Stränden, Seen, in Nationalparks, Messen, – tendenziell wird praktisch der gesamte öffentliche Raum ins Visier genommen – könnten über Echtzeitpositionsdaten Personenströme reguliert werden. (Alle über das Redaktionsnetzwerk Deutschland (RND) versorgten Blätter, z. B. Spiegel 28.4.20, Weser-Kurier). Das ist ein kleiner Schritt in der Digitalisierungsoffensive, aber ein großer Schritt für die gesamte Innovationsoffensive. Denn es würde eine weitere epochale Etappe eines Strukturwandels der Öffentlichkeit eröffnen, der denjenigen tayloristischer Öffentlichkeitsrationalisierungen (vgl. Hydra#2) auf eine neue historische Stufe heben würde. Die App-vermittelten ersten Schritte hierzu haben wir bei Capulcu schon analysiert.

Dem notgedrungen knappen Schlaglicht auf die US-amerikanischen Entwicklungen kann man Microsoft-CEO Nadellas Quintessenz über die technologischen Wirkungen von Corona aus einem Bericht des Business Standard vom 30.4.20 voranstellen: „Zwei Jahre digitaler Transformation brauchen nur zwei Monate.“ Natürlich haben digitalisierte Videokonferenzen, Homeoffice und digitalisierter Unterricht einen enormen Schub erlebt. Aber in manchen Segmenten und Städten waren sie schon viel weiter entwickelt als in Deutschland und sogar als in Greater London, sodass niemand viel Aufhebens davon macht. Das gilt aber nicht für viele Städte und weite Landstriche zurückhängender Bundesstaaten, für die wenig anderes zu sagen ist, als für Deutschland. Kurz: das Binnengefälle ist krass. Daran mag es liegen, dass über Allgemeinheiten, wie die schlichte Konstatierung eines IT-Schubs hinaus, die Berichterstattung und Analysen von McKinsey nicht gerade spannend und hier kaum berichtenswert sind.[29] Beachtenswert ist hingegen der Bericht von Guido Mingels aus San Francisco[30], wonach der Schub in den coronabedingten IT-Anwendungen das angewachsene Misstrauen gegen Silicon Valley zum Schmelzen bringt: „Der Techlash ist vorerst abgesagt … Big Tech gewinnt“, zumal es seine Lieferketten erfolgreich habe reorganisieren können. Corona beschleunige Trends, mache manche Ideen und Firmen zu Gewinnern – hervorstechend Amazon als „unverzichtbarer Grundversorger“ – und andere zu Verlierern, wie die sogenannte „Sharing-Industrie“ oder besser „on-demand-Industrie“. Die Digital-Industrie werde nunmehr von der Option zum Standard, die verheerendste Folge für die Perspektiven der sozialen Revolution gegen den technologischen Angriff. Ist diese Wasserscheide in den USA wirklich überschritten, bei der nach Mingels die „Digitalisierung zur (technologisch definierten, Capulcu) Klassenfrage“ wird, zur Frage derjenigen, die aus unterbezahlten Positionen aus Supermärkten, Tankstellen, Kurierdiensten die Homeoffice-Elite mit dem Notwendigsten versorgen, zum Schaden urbaner Zentren?

Die Bewertung der Prozesse in den USA ist infolge der US-Führerschaft in der Innovationsoffensive und der – bisher noch prägenden – weit liberaleren sozial/ökonomischen Organisation eine andere. Der von privaten Unternehmen betriebene disruptive, zerstörerische Prozess wird bislang noch brutal fortgesetzt, der Moment einer staatlichen oder sonst gesamtgesellschaftlichen Hegemonisierung ist noch nicht erreicht (wie ja die USA in der Geschichte auch immer verspätet Anschluss an die von Deutschland vorangetriebene gesamtorganisatorische Entwicklung gesucht haben[31]). Andere, auch europäische Länder, in denen das Transformationsprofil blasser entwickelt ist, müssen hier unbehandelt bleiben.

CHAOS ODER LENKUNG?

Weder noch. All diese Vorstöße erscheinen chaotisch. Aber in der Geschichte der Innovationsoffensiven lag das „organisierende“ Moment immer, wie auch heute, begründet in vom Ehrgeiz befeuerten privaten Initiativen. Das sind Initiativen der großen Player wie Google, Amazon, Facebook, ja, sogar auch SAP unter ferner liefen. Aber auch der Start-ups und nicht zuletzt der innovativen Forschungsinstitute und darüber hinaus der

28 Spiegel vom 30.4.20

29 Vgl. www.mckinsey.com/industry/heathcare-systems-and-services/our-insights/beyond-coronavirus-the-path-to-the-next-normal

30 Abgedr. im Spiegel vom 16.4.20.

31 Vgl. D. Hartmann, Krisen, Kämpfe, Kriege, Bd. 2, … op. cit., Kap. 3.3, 8.4.

Problemlöser (vgl. der „Solutionismus“-beitrag), der Expert*innen, die – selten selbst Entscheider – Such- und Problemräume eröffnen und Lösungsmöglichkeiten anbieten. Alle suchen sie zugleich ihre Chancen. Und das „Organisierende“ daran ist die gleichgerichtete innovative Orientierung. Sie ist zugleich befeuert von Ehrgeiz, Profilierungseifer und Konkurrenz, geprägt vom gegenseitigen Lernen bis zum Klau und zur Hochstapelei. Mit (zeitweiligen) Vorreitern, Vorpreschern, Taktgebern. Sie sind es allesamt, in denen sich die „animal spirits“ des Schubs verkörpern, ausprägen und ausdifferenzieren. Und der Staat? Schiebt er nicht auch, wenn man Bär glauben darf und ernst nehmen möchte? Sicher doch. Aber ist nicht auf der anderen Seite das Analysepotential, Know-how und die Mischung von Gier und Ehrgeiz der „Privaten“ aller dieser Ebenen unvergleichlich größer? Ebenso sicher. Aber sie sind Konkurrenten und gönnen sich gegenseitig bei allen vorübergehenden Allianzen das Schwarze unterm Nagel nicht. So tritt denn, wie schon früher, der nicht nur ideelle (Engels), sondern eher reale Gesamtkapitalist als Garant nicht nur staatlicher und vor allem militärischer Macht, sondern als Angelpunkt auf, der eine kohärente Formierung der Initiativen zu einem komplexen historischen Schubs ermöglicht. Und gerade hier ist die Ähnlichkeit, die Analogie mit dem tayloristischen Schub im Ersten Weltkrieg (wiederholt im NS) besonders augenfällig. Es waren die Kapazitäten und die Akteur*innen aus den großen Playern (AEG, BASF), die den Krieg praktisch übernahmen und binnen Monaten das Kriegsministerium zu einem Wurmfortsatz der von ihnen geschaffenen gigantischen Strukturen machten. Komplettiert durch Horden ehrgeiziger wissenschaftlicher Problemlöser*innen aus den Universitäten, Instituten und dergleichen mehr, betrieben sie unter einer zusammenfassenden, richtunggebenden, aber sich zugleich verändernden Staatlichkeit ihre Konkurrenzen und zugleich die Formierung eines militärisch-industriell-wissenschaftlichen Komplexes und den Durchbruch des Fordismus/Taylorismus.[32]

Das von den „animal spirits“ des Schubs angestachelte Digitalisierungsrennen kann man in einer derart hektischen Phase nur mit Momentaufnahmen wiedergeben. Aufnahmen, die schon im nächsten Monat anders aussehen werden. Daher soll es mit dem hier fotografierten „Schnappschuss“ erst mal sein Bewenden haben. Wir verstehen diesen eher als Auftakt zu weiteren Schnappschüssen von Vorstößen, die wir in den kommenden Monaten und Jahren behandeln werden.

32 Ebd. Kap. 3, 8.3.

VORWARNUNGEN AUS DER GESCHICHTE UND AUSBLICK

Wir haben bei Capulcu wiederholt betont, dass die Schilderung von Facetten des technologischen Angriffs, über die wir berichten, immer wieder zeithistorisch in das komplexe Geschehens der Innovationsoffensive eingebettet und historisch zurückgebunden werden muss. Das müssen wir jetzt auch tun. Denn die über die großen Zyklen hinweg so ähnlichen Verlaufspfade bzw. das dynamische Profil solcher Offensiven sind jeweils unhintertreiblich ein historisches Gesamtgeschehen. In ihm verbinden sich unauflöslich Angriffsstränge, Finanzinstrumente/Ökonomie, Sozialstrategien, was immer die Analyse an Einzelsträngen da herauslösen mag. Das, was die oben referierten Autoren das „digitale Durchdringen auch der entlegensten Winkel der Gesellschaft“ nannten. Gegen die Bevölkerung in allen Dimensionen von Arbeiten und Leben gerichtet, hat die Offensive immer wieder – in den historischen Etappen von „Industrieller Revolution, tayloristischer bis zur heutigen IT-Offensive – den Durchbruch in einem epochal angelegten, technologisch/ökonomischen Vorstoß gesucht. Krisen sind sowohl den Resistenzen und Widerständen gegen die Offensive geschuldet, wie auch dem Ausbleiben der anvisierten Werte, die das jeweils modifizierte und gesteigerte Warenangebot tragen können. Die Krisenträchtigkeit der Verschuldungswellen haben wir hier und bei „Hydra“ nachgezeichnet. Das genannte OECD-paper hat der daraus resultierenden technologisch/ökonomischen Blockierung Rechnung getragen, für uns nicht überraschend. Corona hat nunmehr die Situation auf eine Weise so verschärft, dass die innovatorisch-kapitalistischen Eliten nunmehr die Gelegenheit ergreifen, die den Schock der Krise, die „shock and awe“-Wirkung des potenzierten technologischen Angriffs und vor allem die ökonomisch-existenzielle Angst der Menschen zu nutzen.

Die Analogien zu Krisensituationen wie 1913 f. und 1929 ff. liegen auf der Hand.[33] Im Zuge des Innovationsvortriebs, musste die Innovationsoffensive, damals ebenso wie heute, auf eine fundamentale ökonomisch/soziale Blockierung stoßen. Sie konnte, angesichts von Resistenzen und Widerständen und ausbleibenden ökonomischen Anpassungen, nie glatt durchgehen. Damals nutzten ihre Avantgarden den von ihnen nicht herbeigeführten, sondern allenfalls unterstützten Kriegseintritt, um den Durchbruch der Offensive in einem nie dagewesenen Blutbad zu suchen.[34] Und heute? In gleicher Weise, so sehr sich die Wirkungen von Corona vom

33 Vgl. dazu D. Hartmann, Krisen, Kämpfe, Kriege, Band 2, Innovative Barbarei gegen soziale Revolution. Kapitalismus und Massengewalt im 20. Jahrhundert, Berlin, Hamburg 2019, Kap. 3 und 5.

34 D. Hartmann, Krisen, Kämpfe, Kriege, Band 2, Innovative Barbarei gegen soziale Revolution. Kapitalismus und Massengewalt im 20. Jahrhundert, Kap 2 und 5.

damaligen Blutbad auch unterscheiden. Bedarf es zum Durchbruch der zerstörerischen Wirkungen und organisatorischen Prozesse eines Krieges, ist er anvisiert? Oder reicht vorerst eine Corona-induzierte Zerstörung mit einer „Kriegsökonomie ohne Krieg“ aus? Ebenso wie den Krieg von 1914 haben die Protagonisten der Offensive die Coronaepidemie nicht herbeigeführt (die Verschwörungstheorien lenken auf schändliche Weise vom wirklichen Geschehen ab). Aber sie nutzen sie in ähnlicher Weise. Und zwar durchaus unter bezeichnender Verwendung einer Kriegsrhetorik und mit aus der Kriegsökonomie bekannten Mitteln. Und zugleich vor dem Hintergrund und unter Nutzung politisch-strategischer und militärischer Spannungen, die wir im Beitrag zum „Griff nach der Weltmacht“ behandelt haben und die in der Lage sind, die „schöpferische Zerstörung“ durch Corona durch eine kriegerische zu steigern. Die amerikanische Futurologin und Beraterin hoher Militärs und Politiker*innen Amy Webb, beschwor in einem Handelsblatt-Interview und im Coronakontext am 22.4.20 die Gefahr eines „ökonomisch-technologischen Krieges“ und sagte: „China nutzt die Krise, um noch viel mehr Daten zu sammeln. Ortsdaten der Menschen, aber auch hochsensible biometrische Informationen. Dadurch werden die Datenanalysefähigkeiten und die KI-Technologien der dortigen Unternehmen noch besser. Diese Entwicklung trifft übrigens nicht nur die einzelnen Nutzer. Auch Unternehmen werden in China von automatischen Scoring-Systemen erfasst und kategorisiert. Gleichzeitig entsteht ein neuer militärisch-technologischer Komplex. Denn die Waffen der Zukunft sind Daten und Algorithmen. Und viele Unternehmen, die eng mit dem Militär kooperieren, sind auch diejenigen, die am weitesten mit der KI-Forschung sind. Ich mache mir Sorgen, dass die globale Pandemie einen ökonomisch-technologischen Krieg auslöst, wie wir ihn noch nicht gesehen haben.“ In Anbetracht unserer detaillierten Darstellungen in „Delete“ ist in diesem Statement für uns nur der Corona-Kontext neu, den sie zu Recht als Beschleuniger betrachtet. Webb redet mit Admiralen, Sterne-Generälen und Politiker*innen in strategischen Positionen. Ist die Tendenz zum Krieg in Kauf genommen, oder gar beabsichtigt? Die antichinesische Rhetorik – sie rechnet mit einer „De-Chinaisierung“ – ist von Trump bis zu den Demokraten unüberhörbar. Die hier und im Beitrag über den „Griff nach der Weltmacht“ angegebenen historischen Hinweise sagen uns, dass die USA innovationstreibende Kriege sowohl angezettelt, als auch aufgegriffen haben. Und das ist wichtig, denn die historische Orientierung spielt bei ihren Akteur*innen immer eine große Rolle. All das sagt mehr, als der nackte informative Inhalt ihres Statements und wird uns weiterhin beschäftigen.

Auch, wenn wir den rasenden Wirbel der Veränderung nur in Momentaufnahmen fassen können, einige Vorstöße übergreifender und grundsätzlicherer Natur wollen wir – ohne Anspruch auf Systematik und Vollständigkeit – benennen.

KONZENTRATIONS-, BEREINIGUNGSPROZESSE UND WEITERE AUSWIRKUNGEN.

Der 1. Weltkrieg wurde durch die Kriegsrohstoffabteilung wie auch durch analoge Organisationen in anderen kriegführenden Ländern über den Begriff der „Kriegswichtigkeit“ bzw. „Kriegsrelevanz“ unter dem Machtmonopol der damals innovativen Elektro- und Chemiegiganten zur gelenkten Konzentration und Unternehmensbereinigung genutzt. Etwas Ähnliches geschieht jetzt mit dem Instrumentarium der unter Bedingungen gestellten Kreditvergabe, die an der Leitlinie der „Systemrelevanz“ orientiert sind. Auf der neuen Innovationsstufe allerdings unter dem Machtmonopol der IT-Giganten.

Die Prozesse der *Konzentration, Auslese und Bereinigung* lassen auf allen industriellen Stufen Unternehmen verschwinden, wie es keine der früheren großen Krisen gründlicher bewerkstelligt hat. Am dramatischsten in der Luftfahrt und Flugzeugindustrie, wo ganze Airlines untergehen in Ländern, die sich eine auffangende Finanzierung nicht leisten können. Besonders dramatisch in Afrika, wo Ethiopian und Southafrican Airlines der Auflösung anheimgegeben scheinen. Außer es sammelt sie einer der großen metropolitanen Linien für einen Appel und ein Ei auf.

Ein ebenso dramatischer Prozess tobt im *Einzelhandel und Servicesektor*. Er ist von großer Bedeutung für tradierte Lebensformen und die in ihnen angelegten Resistenzpotentiale, insbesondere der mittlere und Kleinhandel auf Quartiers- und Stadtebene. Corona hat ihm in allen Ländern einen teilweise irreversiblen Schock versetzt. Nutznießer ist der Onlinehandel, auch Netflix, Ocado etc. Vor allem aber Amazon. Unter Corona hat das Unternehmen seinen Absatz auf US-$ 11 000 in der Sekunde hochgefahren, Bezos hat sein Vermögen auf 138 Milliarden erhöht und als reichster Mann der Welt den Abstand zu den ärmlichen, im unteren zweistelligen Milliardenbereich vegetierenden Hungerleidern noch ausgebaut. Seine gewachsene Arroganz gegenüber den Arbeiter*innen schlägt sich im amerikanischen System des „hire and fire“ in gewachsener Brutalität und Mitleidlosigkeit nieder. Der CEO von Ritholz Wealth Management, Josh Ritholz, gibt die übereinstimmende Meinung vieler wieder, wenn er sagt: „Amazon ist in dieser Krise ein öffentliches Versorgungsunternehmen geworden – aggressiv, verlässlich, unverzichtbar.“. Vizepräsident Mike Pence hat in einem U-turn gegenüber Trumps vorheriger Ablehnung seine Ergebenheitsad-

resse bei Bezos angebracht[35]. Das oben geschilderte Beispiel der Initiative des DIHT verleiht diesem Vorstoß der „schöpferischen Zerstörung“, d. h. der Zerstörung und Neuschöpfung der Lebenswelt, eine technologische Form, die für weitere Vorstöße prägend sein wird.

Eine Momentaufnahme an NRW-*Hochschulen* lieferte uns ein Genosse. Er berichtete davon, dass Hauptamtler*innen per Anordnung aus dem Ministerium verpflichtet wurden, den Unterricht mit den marktgängigen Hilfsmitteln selbst, aber mir finanzieller Unterstützung zu digitalisieren. Auch Nebenamtler*innen wurden aufgefordert, verbunden mit der Drohung des Gehaltsverlusts, wenn sie nicht spuren sollten.

In *finanztechnischer* Hinsicht verweisen wir auf die Beiträge zu „Libra“ und den Krisenticker#4 bei Hydra. Das Fluten des Schulden- und Liquiditätspegels in vielfacher Billionenhöhe, hat überall und auch in Deutschland Dämme brechen lassen und Fragen nach einer neuen Ökonomie aufgeworfen. Zum offensichtlichen coronabedingten Einbruch der Formen kontaktfreier Bezahlung, besonders durch Smartphones, liegen noch keine verlässlichen Berichte vor. Zum Gesundheitsbereich verweisen wir auf die entsprechenden Beiträge.

Die *Globalisierung* wird zurückgefahren, Lieferketten werden zurückgefahren und reorganisiert, Unternehmen richten Zwischenlager ein. Vorstellungen eines versorgungssicheren „Großraums“ werden nach 1914 ff. und 1933 ff. erneut erörtert.

Die *patriarchal-sexistische Gewalt-* und Ausbeutungskaskade, deren informationstechnologischen Ausdruck wir immer wieder beleuchtet haben, radikalisiert sich unter Corona einmal mehr. Frauen tragen eine unerträgliche Last in Heimarbeitsplätzen mit Kindern, aber auch in der Isolation häuslicher Versorgungsleistungen. Sie wird sich unter den Bedingungen der erwarteten ökonomischen Krise noch verschärfen.

In *Europa* spielen Merkel/Scholz va banque. Sie wollen ihr rigides an Griechenland entwickeltes Regime weiterverfolgen, das Europa inzwischen in drei Zonen einteilt: im Zentrum der alte wilhelminische und NS-Kern bestehend aus Deutschland, Österreich, Benelux und evtl. auch Frankreich, danach Italien und Spanien und schließlich die übrigen Länder.[36] Corona-Bonds wird's nicht geben, die Einigungslinie wird auf der „gemeinsamen“ Verschuldung über die Europäische Union gesucht, verbunden mit Machtgewinn für von der Leyens Europa als die BRD-dominierte Macht. Die EZB kauft weiter bonds, d. h. verbriefte Staats- und Unternehmensanleihen über die Ramschgrenze hinaus. Sie sieht sich als europäisches Organ durch die ablehnende Entscheidung des Bundesverfassungsgerichts nicht gehindert. Sie ventiliert gerade die Auslagerung in „bad banks“. Mit einer Bankenkrise wird gerechnet.

Die soziale Verwüstung in den *Ländern des globalen Südens* durch Corona wird als enorm eingeschätzt mit weiterer Verschärfung für die Migrant*innen. Schon die Gewaltausbrüche der letzten Wochen im Libanon werfen ein düsteres Licht darauf.

Das alles sind keine kurzatmigen *Projektionen*. Die Krise bleibt uns nach den letzten Meldungen und Einschätzungen auf unabsehbare Zeit erhalten. Die epidemieträchtigen Gebiete sind für weitere Ausbrüche gut. Der Innovationsdruck wird nicht nachlassen.
Der Schub ist beileibe *nicht konsolidiert*. Auch wenn es inzwischen auch in der Groko durchsickert, dass die Tage der Ära von tayloristischer Massenproduktion, -konsum und -kultur gezählt sind, ist das Beharrungsvermögen von Mittelstand und Mittelschicht nicht überwunden. Wir könnten – ähnlich wie in analogen historischen Situationen – einem Umbruchstheater mit wechselnden Inszenierungen entgegengehen. Aber: der Druck der ökonomischen und sozialen Krise nimmt unerbittlich zu. Auf der anderen Seite ist die Erwartung sozialer Unruhe weltweit ein schwer einzuschätzende Größe. Sie wird hier allerdings nicht behandelt, weil zu komplex. Denn der umbruchbedingte Zerfall der überkommenen Muster des Politischen ist unübersehbar, bedarf aber einer genauen Analyse.

„*A mental revolution*“ von oben, das war Taylors Formulierung für das auf eine Epoche angelegte tayloristische Programm. Zu seinen Produkten zählte daher die mentale Konsolidierung in Hitlers „Leistungsvolksgemeinschaft“, Volksgemeinschaftsmoral war kein schlechter Griff von Wolfgang Michal. Dazu ist im Beitrag zum „populistischen Moment“[37] genug gesagt, um hier auf eine Analyse seiner Fortentwicklung verzichten zu können. Zur Frage der staatlich/technologisch/ökonomischen Verfasstheit zeichnet sich schon jetzt eine Entwicklung in neokorporatistischer Richtung ab, ähnlich wie sie im ersten Weltkrieg als „militärisch-technologisch-ökonomischer Komplex“ unter deutscher Führung in allen kriegführenden Ländern eingeleitet wurde.[38] Amy Webb liegt nicht falsch, wenn sie dem Rechnung trägt.

35 R. Neate, Amazon reaps $11,000-a-second coronavirus lockdown bonanza, Guardian 15.4.20

36 Vgl. dazu D. Hartmann, Krisen, Kämpfe, Kriege, Bd. 2 …, op. cit., Kap. 3.1 und 8.3. John Malamatinas und Detlef Hartmann haben das schon im Buch über „Krisenlabor …, op. cit. beleuchtet

37 Bei www.the-hydra.world/fresh

38 D. Hartmann, Krisen, Kämpfe, Kriege, Bd.2 …op. cit., Kap. 3

Die „freiwillige“ Corona-App

Die Bundesregierung setzt für eine schrittweise Rücknahme der Corona-Kontaktbeschränkungen auf eine breite Akzeptanz für die voraussichtlich Mitte Juni geplante App zur nachträglichen Kontaktrekonstruktion Infizierter. Die (berechtigte) Angst vor dem Virus wird benutzt, um einem Großteil der Bevölkerung „freiwillig“ ein autoritär hochwirksames Werkzeug zu verabreichen.

*Obwohl sich die deutsche Bundesregierung nun für die dezentrale Variante entschieden hat, kritisieren wir in diesem Artikel sowohl die technische Konstruktion und Infrastruktur der Apps, als auch ihre sozial-technokratischen Konsequenzen. Selbst wenn das Protokollieren von Kontakten vollständig pseudonym erfolgen würde, müssen wir dringend vor dieser App warnen. In dem Moment, wo (sogar anonyme) Verhaltensdaten flächendeckend anfallen, sind die prädiktiven Modelle, die damit trainiert werden, dazu in der Lage, ganze Populationen in Risikogruppen einzuteilen und algorithmisch zu verwalten. Egal welche Variante der Corona-App sich langfristig durchsetzt: Es ist eine Überwachungsinfrastruktur, die da ausgerollt wird. Deshalb halten wir den Applaus einiger kritischer Datenschutzschützer*innen für unangemessen – ja sogar fahrlässig.*

DIE ZENTRALE VARIANTE: PEPP-PT

Im März wurde bekannt, dass ein internationales Team bestehend aus rund 130 Wissenschaftler*innen, IT-Entwickler*innen, Datenschutzerbeauftragten und Soldat*innen derzeit in einem Projekt mit dem Namen Pan European Privacy-Protecting Proximity Tracing (PEPP-PT) an einer Software arbeitete, welche die SARS-CoV-2-Virusverbreitung einschränken soll. Beteiligt sind aus Deutschland unter anderem das Robert-Koch-Institut (RKI), das Heinrich-Hertz-Institut (HHI) und das Bundesamt für Sicherheit in der Informationstechnik (BSI). Auch der Bundesdatenschutzbeauftragte begleitet die Entwicklung und Soldat*innen der Bundeswehr helfen bei den Tests. Bis auf das RKI sind sie auf der Website des Projekts nicht gelistet. Das HHI ist unter Fraunhofer subsumiert. Bislang sind Forscher*innen und Institute aus acht Ländern an der Entwicklung beteiligt: Belgien, Dänemark, Deutschland, Frankreich, Italien, Österreich, Spanien und die Schweiz.

Um die Ausbreitung einzudämmen, sollen Kontaktpersonen von Infizierten frühzeitig gewarnt werden. Wenn Menschen Symptome zeigen, dann haben sie das Virus höchstwahrscheinlich bereits weitergegeben. Deshalb sollen nach einer positiven Diagnose alle Smartphonebesitzer*innen benachrichtigt werden, deren Geräte in der Nähe des Erkrankten waren. Wenn es viele einzelne Ansätze und Software-Lösungen gibt, die jeweils nur ein kleiner Teil der Bevölkerung nutzt, kann das Konzept nicht aufgehen. Deshalb soll eine gemeinsame Grundlage entstehen, die möglichst schnell eine kritische Größe erreicht. Die Rede ist von einer gemeinsamen Plattform: einer Client/Server-Referenzimplementierung, aber auch von einem Softwaregerüst, auf dem Smartphone-Apps aufsetzen können. Diese Smartphone-Apps, die Nutzer*innen auf ihrem Telefon installieren, bilden einen wesentlichen Teil des Systems.

Um Infektionsketten wirksam zu unterbrechen, streben die Forscher*innen eine Nutzer*innenbasis von etwa 60 Prozent der Bevölkerung an. In Deutschland wären das 50 Millionen Menschen. Bislang gibt es in Deutschland keine App, die nicht auf Smartphones vorinstalliert ist und bewusst heruntergeladen werden muss, die so viele Nutzer*innen hat. Allerdings könnte auch ein geringerer Anteil helfen, die Ausbreitung zumindest zu verlangsamen. Laut Bitkom besitzen 81 Prozent aller Menschen in Deutschland über 14 Jahren ein Smartphone. Normale Handys und ältere Geräte unterstützen den nötigen Bluetooth-Standard noch nicht. Insbesondere Senior*innen, für die das Virus besonders gefährlich ist, können nur zum Teil gewarnt werden. Deshalb denken die Forscher*innen darüber nach, künftig auch

Bluetooth-Armbänder oder andere Wearables zu verteilen. Einer repräsentativen Umfrage (Stand 31.03.2020) zufolge, würden mehr als 70 Prozent der Befragten so eine App auf jeden Fall oder wahrscheinlich nutzen. Die Mehrheit gibt an, den Aufforderungen der App nachkommen zu wollen und sich in Quarantäne zu begeben, sollten sie mit einer infizierten Person in Kontakt gekommen sein. Umfragen zufolge wäre ein Großteil der Bevölkerung in Deutschland bereit, einen Teil ihrer Privatsphäre aufzugeben, um das Virus zu stoppen.

Vorbild ist TraceTogether, ein zunächst von Singapur entwickeltes Verfahren zur Kontaktverfolgung, das auf die Funktechnik Bluetooth Low Energy setzt. Das System soll als Gegenentwurf zu den repressiven und invasiven Ansätzen anderer Länder (wie China oder Südkorea) verstanden werden. Anstatt massenhaft sensible Standortdaten zu sammeln, Nutzer*innen zu überwachen oder Infizierte an einen digitalen Corona-Pranger zu stellen, soll PEPP-PT komplett freiwillig und datenschutzfreundlich sein. Die Betreiber versprechen, die Privatsphäre von Nutzer*innen der Software zu schützen. Die Identität der Nutzer*innen bleibt zu jedem Zeitpunkt geschützt heißt es: weder Ärzt*innen noch die Betreiber der Plattform können Einzelpersonen identifizieren. Für gute PR sorgen Zeitungen, die sogar von einer anonymen Nutzung schreiben, obwohl es sich um eine Pseudonymisierung handelt. Das PEPP-PT-Modell scheint auch nicht zu 100 Prozent Privacy-by-Design zu erfordern. Die Spezifikationen und den Quellcode gibt es laut der bisher sehr informationsarmen Webseite aktuell allerdings nur als Mitglied des Konsortiums.

Wir sagen: Code und alle Dokumente offenlegen, sonst glauben wir gar nichts. Und nicht nur irgendeine Client-Referenzimplementierung, sondern die ganze Spezifikation und den ganzen Server-Code.

Aber selbst wenn der Server-Code open-source ist, kann man nicht sicher sein, dass die Behörden diesen Code auch unverändert verwenden. Weiter kann man nicht sicher sein, dass die Daten nicht doch aus der Datenbank kopiert oder länger gespeichert werden.

Die PEPP-PT-App ist *nicht zu verwechseln mit der Corona-Datenspende-App* des RKI. Während der Debatte um die Corona-App und derartige Anwendungen, veröffentlichte das RKI am 7. April 2020 eine Corona-Datenspende-App für Android und iOS zur freiwilligen Weitergabe von Fitnesstracker-Daten an das RKI. Zweck dieser von der Bundesregierung beworbenen und vom Bundesgesundheitsministerium unterstützten App ist „eine bessere Vorhersage des bundesweiten Erkrankungsverlaufs mit Covid-19 und damit eine verbesserte Steuerung von Eindämmungsmaßnahmen gegen die Corona-Pandemie". Innerhalb einer Woche wurde diese im Auftrag des RKI von der mHealth Pioneers GmbH entwickelte und betriebene App von bereits mehr als 400.000 Freiwilligen heruntergeladen und mit einem Fitnesstracker verknüpft. Die Zahlen stagnierten bei 500.000 Nutzer*innen.

Wahrscheinlicher Grund war die einige Tage später veröffentlichte Analyse der Software des Chaos Computer Clubs (CCC). Neben unzureichendem Schutz der Zugangsdaten und organisatorischen Defiziten ist die Cloudanbindung und die mangelhafte Pseudonymisierung bemerkenswert. So holt sich das RKI die Daten der meisten Nutzer*innen wider Erwarten nicht vom Smartphone, sondern direkt von den Anbietern der Fitnesstracker. So hat das RKI über einen Zugangscode potenziell Zugriff sowohl auf Klarnamen der Spender*innen als auch deren Fitnessdaten. Bei einer einfachen Deinstallation der App bleibt dieser Zugriff auch weiterhin bestehen. Entgegen der Darstellungen werden die hochsensiblen Gesundheitsdaten der meisten Nutzer*innen nicht schon auf dem Smartphone pseudonymisiert, sondern vollständig und teils mitsamt Klarnamen der Datenspender*innen abgerufen. Eine Pseudonymisierung findet (wenn überhaupt) erst auf Seiten des RKI statt und kann durch die Nutzer*innen nicht kontrolliert oder verifiziert werden. Bemerkenswert ist auch, dass hier Datenschutz und IT-Sicherheit grob missachtet wurden, obwohl mit dem CCC und Datenschutzer*innen in dem anderen gemeinsamen Projekt (bei der PEPP-PT-App) zusammengearbeitet wurde.

TECHNISCHE DETAILS ZU PETT-PT

Folgende technische Details beruhen auf den wenigen Informationen der PEPP-PT-Website, auf Dokumenten der öffentlichen Git-Repositories[39] und Berichten von Netzpolitik.org. Vieles ist auch für die dezentrale Variante DP3T relevant.

Die Apps weisen jedem Gerät eine vorübergehend gültige, authentifizierte und zufällig generierte Identifikationsnummer (ID) zu. Diese ID funktioniert als Pseudonym, welches die Identität zuverlässig schützen soll. Sie wird in regelmäßigen Abständen geändert (die Rede ist von 30 Minuten) und soll nicht mit dem Telefon in Verbindung gebracht werden können. Des Weiteren soll niemand im Nachhinein herausfinden können, welche Person sich hinter einem solchen Pseudonym verbirgt.

Jedes PEPP-PT-Telefon (gemeint ist ein Smartphone, auf dem die App installiert ist) sendet über eine kurze Entfernung mit Bluetooth-Funktechnik (Bluetoo-

39 https://github.com/pepp-pt und https://github.com/DP-3T

th-Low-Energy) seine aktuelle ID und scannt gleichzeitig die Umgebung und erfasst, welche anderen Smartphones mit installierter PEPP-PT-Software sich in Reichweite befinden. Wenn sich zwei Geräte näher kommen, speichern die Apps die temporäre ID des jeweils anderen Smartphones. Die Annäherung von Telefonen anderer PEPP-PT-Benutzer wird durch die Messung von Funksignalen (Bluetooth usw.) realisiert.

Die Daten bleiben zunächst verschlüsselt auf dem Smartphone, niemand kann darauf zugreifen, heißt es. Aufgrund der geringen Informationen ist offen, wie das konkret kryptographisch umgesetzt wurde. Nicht jede Annäherung wird gespeichert. Nur wenn sich PEPP-PT-Telefon A über einen epidemiologisch ausreichenden Zeitraum in der Nähe von PEPP-PT-Telefon B befindet (die Rede ist von 15 Minuten in 1,5 Metern Entfernung), dann wird die aktuelle temporäre ID von Telefon B, in der verschlüsselten, lokal auf dem Telefon gespeicherten Annäherungsgeschichte (Proximity-Historie) von A gespeichert (und umgekehrt).

Offen bleibt, ob die Wahl von 15 Minuten eine sinnvolle Zeitdauer ist, denn Anhusten im Bus oder im Geschäft dauert nur wenige Sekunden, Kurzgespräche 1-2 Minuten. Das reicht auch schon für die Ansteckung. Offen bleibt auch was konkret gespeichert wird. Laut PEPP-PT-Website werden keine Geolokalisierung, keine persönlichen Informationen, einzigartige Gerätekennungen wie die IMEI-Nummer des Smartphones oder andere Daten protokolliert, die eine Identifizierung der Benutzer*in ermöglichen würden. Weiter heißt es: Die pseudonyme Annäherungsgeschichte kann von niemandem eingesehen werden, auch nicht vom Benutzer*in von Telefon A. Ältere Ereignisse in der Annäherungsgeschichte werden gelöscht, wenn sie epidemiologisch unbedeutend werden.

„Wir messen nur, wie lange und wie nahe sich zwei Personen begegnet sind", sagt Thomas Wiegand (Leiter des HHI). Wo das Treffen stattgefunden habe, sei dem Virus egal. „Das sind die einzigen Informationen, die epidemiologisch von Bedeutung sind." Nach 21 Tagen werden die Daten automatisch gelöscht. Statt auf Tracking setzt PEPP-PT auf Tracing – es sollen nicht die Bewegungen von Menschen verfolgt, sondern nur ihre Kontakte nachverfolgbar werden. Auf dem Smartphone entsteht eine Liste mit IDs mit Zeitstempeln, hinter denen sich Personen verbergen, die man selbst angesteckt haben könnte, oder von denen man Viren erhalten haben könnte.

Um Fehlalarme zu reduzieren, haben die Forscher*innen alle weit verbreiteten Smartphonemodelle untersucht und die Signalstärke der Funktechnik gemessen, da sie sich teils unterscheidet.

Soldat*innen der Bundeswehr haben geholfen, die Technik so zu kalibrieren, dass sie etwa erkennt, ob zwischen den beiden Kontaktpersonen eine Glasscheibe oder andere Hindernisse waren, die eine Übertragung des Virus verhindern. Eine zuverlässige Genauigkeit der Aussage, ob jemand innerhalb eines Radius von 1,5 Metern war oder nicht, mittels Bluetooth ist äußerst zweifelhaft.

In dem Fall, dass ein*e Benutzer*in nicht getestet wird oder negativ getestet wurde, bleibt die Annäherungsgeschichte auf dem Telefon der Benutzer*in verschlüsselt und kann von niemandem eingesehen oder übertragen werden. Wenn allerdings bestätigt wurde, dass die Benutzer*in von Telefon A SARS-CoV-2-positiv ist, (also in der Regel bereits an Covid-19 erkrankt ist), dann soll diese Person ihre aktuelle bis dato lokal gespeicherte ID-Liste in der Annäherungsgeschichte auf einen nationalen zentralen Server übermitteln. Das ist nicht ohne weiteres möglich. Ärzt*innen, Labore und Gesundheitsbehörden müssen die Meldung bestätigen. Es braucht also zwingend eine positive Diagnose. Dann setzen sich die Gesundheitsbehörden mit Benutzer*in A in Verbindung und stellen ihr eine TAN zur Verfügung, die sicherstellt, dass potenzielle Malware keine falschen Infektionsinformationen in das PEPP-PT-System einschleusen können. Die Schnittstelle soll verschlüsselt und geheim funktionieren, sodass die Identität der Erkrankten geschützt bleibt. Die Benutzer*in verwendet diese TAN, um freiwillig Informationen an den Server des nationalen Dienstleisters zu übermitteln, in Deutschland beispielsweise beim Robert-Koch-Institut, die die Benachrichtigung von PEPP-PT-Anwendungen ermöglichen, die in der Annäherungsgeschichte aufgezeichnet und somit potenziell infiziert sind.

Das Konsortium schreibt, da die Annäherungsgeschichte pseudonyme Identifikatoren enthält, kann der Server aus diesen IDs nicht auflösen, welche Menschen sich dahinter verbergen, er kann aber alle betroffenen Kontaktpersonen über die App benachrichtigen und auffordern, sich testen zu lassen.

Diese Benachrichtigung kann dabei ganz ohne Ansehen der Personen verschickt werden, die die Smartphones nutzen. Denn um eine Nachricht auf dem Smartphone anzeigen zu können sind keinerlei personenbezogene Daten erforderlich. Es genügt vielmehr ein sogenanntes Push-Token, eine einzigartige App-Geräte-Kennung, um über Apples oder Googles Push-Notification-Gateways eine Push-Nachricht auf das Gerät zu schicken. Dieses Push-Token wird bei der Installation der App auf dem Handy generiert. Zugleich hinterlegt die App sowohl das Push-Token als auch die temporären IDs, die sie im Laufe der Zeit aussendet, auf einem zentralen Server. Auf diese Weise können die Smartphones allein an-

hand von temporären IDs und Push-Tokens adressiert werden, ohne dass die Identität der Personen feststellbar wäre, die diese Smartphones bei sich tragen. Dazu ist es aber notwendig, dass zu jedem Account Push-Token und alle generierten aktuellen tempörären IDs inklusive Zeitstempel, wann sie generiert wurden, auf dem Server liegen. Es muss dem Server Vertrauen entgegengebracht werden, dass er nach 21 Tagen epidemiologisch irrelevante Daten löscht – und nicht für Big-Data-Zwecke weiterhin speichert. Sobald man die das Push-Token mit Daten des Providers verknüpfen würde (Push-Token-Zuordnung zu Gräte-ID, IMEI, oder Rufnummer), wäre eine Zuordnung möglich.

DIE DEZENTRALE VARIANTE: DP3T

Zwischen den Wissenschaftler*innen, die an der Entwicklung einer Technologie für die Covid-19-Kontaktrückverfolgung beteiligt sind, wird öffentlich ein Konflikt ausgetragen. Im Wesentlichen geht es um die Frage, ob die verschlüsselten IDs der einzelnen App-Nutzer*innen zentral auf einem Server gespeichert werden sollen oder auf dem jeweiligen Gerät verbleiben. Die Forscher*innen teilen unsere am 05. April 2020 veröffentlichte Kritik[40], dass das zentrale Verfahren, das Risiko einer (schleichenden) Ausweitung der Zweckbestimmung birgt. Dass sich nun (vermutlich) das dezentrale Modell durchgesetzt hat, hat unterschiedliche Gründe. Das PETT-Konsortium verfolgt durchaus zwei Ziele: Anfangs wurde die Nachvollziehbarkeit möglicher Infektionsketten und die Benachrichtigung potentiell infizierter als einziger Zweck öffentlich bekanntgegeben. Später offenbarte sich, dass durchaus großes Interesse an der-Data-Analyse der (epiminologischen) Daten besteht – angeblich nur um die Infektionsausbreitung zu erfassen.

Das was bei der App „Proximity-tracing“ genannt wird, ist ein Ausforschen des „Social-Graphs“, das soziale Geflecht also, in dem sich eine Person bewegt, wer*welche trifft sich mir wem, wann, wie lange und häufig. Zugestanden, Proximity-tracing erfasst auch die „Kontakte“ z. B. im Supermarkt, also mehr als die sozialen Kontakte. Die Social-Graphs sind aber als Untermenge ebenso vollständig enthalten und rekonstruierbar. Dass die Repressionsbehörden an solchen Social-Graphs brennend interessiert sind, ist vielfach belegt. Aber auch „nicht-kriminelle“ Verhaltensweisen (wie etwa Affären oder Nebenjobs) lassen sich damit erkennen. Im Grunde handelt es sich hierbei um das Metadaten-Problem, welches schon lange Thema der netzpolitischen Debatte ist. Jetzt werden die Daten aber nicht aus anderen Daten (Telefonate, E-Mail, etc.) extrahiert, sondern direkt erfasst – und das auch, wenn ansonsten keine digitale Kommunikation stattfindet. Diese Überwachungsinfrastruktur ist wesensgleich mit der Vorratsdatenspeicherung. Daten werden erhoben und gespeichert, mit der Argumentation einer zukünftigen „sinnvollen“ Verwendung. Es wird ersteinmal der Heuhaufen aufgehäuft, bevor die Nadel gesucht wird (frei nach K. Alexander, Ex-Chef der NSA[41]).

Welche Auswirkungen diese Überwachungstechnologie haben kann, zeigt ein Beispiel aus Südkorea.[42] Mittels aggressivem Tracking von Infektionssträngen mithilfe von Überwachungsdaten sowie einer radikalen Transparenz über Neuansteckungen, hatte Südkorea das Virus bisher eindämmen können. Jetzt machte es Schlagzeilen, dass ein Mann fünf Klubs und Bars der queeren Szene besuchte, potenziell mit 2.000 Menschen Kontakt gehabt hat und vermeintlich mehrere Menschen mit Corona infiziert habe. Da Südkorea nach wie vor eine homophobe Gesellschaft ohne Antidiskriminierungsgesetz ist, schreckt dies potenziell betroffene Menschen jener Nacht vor Tests zurück. Denn jede*r Neuinfizierte wird von den Behörden zwar anonymisiert, doch mit Alter, Nationalität, Wohnbezirk und Bewegungsabläufen während jener Nacht veröffentlicht. Wer sich jetzt meldet, riskiert also ein Zwangs-Outing.

Als Alternative zu einem zentralen Server, steht eine dezentrale Architektur für die Nachverfolgung von Kontakten zu verwenden. In einem solchen Modell verbleibt die Liste der IDs von Kontaktpersonen auf dem jeweiligen Endgerät. Infizierte schicken nach wie vor die Liste der IDs, die sie getroffen haben, an einen zentralen Server. Aber anstatt, dass der Server betroffene Personen benachrichtigt, erfragen die Apps in regelmäßigen Abständen, ob eine ID publiziert wurde, die sie in letzter Zeit getroffen haben. Die beiden Modelle zur digitalen Kontaktverfolgung unterscheiden sich also sehr grundsätzlich im Hinblick auf die Kontrolle über die anfallenden Daten, den Datenschutz und nicht zuletzt hinsichtlich der Missbrauchsmöglichkeiten. Aber auch der dezentrale Ansatz bietet keine absolute Sicherheit. Auch er funktioniert in den meisten Ausprägungen nicht „anonym“, selbst wenn das manche behaupten.

40 https://capulcu.blackblogs.org/wp-content/uploads/sites/54/2020/04/Corona-App-final.pdf

41 Der ehemalige NSA-Direktor General Keith Alexander rechtfertigte die Massenüberwachung: „Du brauchst den ganzen Heuhaufen, um die Nadel zu finden.“ vgl. Ellen Nakashima und Joby Warrick. For NSA chief, terrorist threat drives passion to ‘collect it all’. Washington Post. 14.07.2013 https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html

42 Fabian Kretschmer. Angst vor Zwangs-Outing per Tracking-App. 8.5.2020. Taz. https://taz.de/Angst-vor-Zwangs-Outing-per-Tracking-App/!5681439/

Auch hier gibt es kryptographische Probleme, die gelöst werden müssen: DP3T hat mittlerweile die Linkability zwischen einzelnen Pseudonymen als Problem erkannt und in ihrem aktualisierten Whitepaper einen Non-linkable-Ansatz eingebaut. Aber er kommt ohne die Voraussetzung aus, einer zentralen (staatlichen) Instanz vertrauen zu müssen, dass sie die Daten exakt so verwendet, wie versprochen und das morgen auch noch so tun wird. Zwar wissen die zentralen Stellen, welche Pseudonyme die Infizierten in der Vergangenheit verwendet haben und können beim Upload der IDs auch dem Pseudonym eine IP-Adresse zuordnen[43], sie können jedoch die individuellen Kontaktnetzwerke nicht rekonstruieren. Es entstehen also keine zentral gespeicherten Informationen über das soziale Umfeld der App-Nutzenden. Der Server der Gesundheitsbehörden kann keine Abbildung des sozialen Umfelds ableiten und lernt von Verdachtsfällen nur, wenn die Nutzenden sich nach einer Aufforderung der App beim Gesundheitsamt beziehungsweise einem Arzt melden. Verglichen mit dem zentralen Ansatz bewahren die Nutzenden der App ein erhebliches Maß an Privatsphäre und Autonomie gegenüber staatlichen Stellen und deren Infrastruktur.

Derzeit ist oft zu lesen, Datenschützer*innen sollten pragmatischer sein und sich endlich bewegen. Doch Vertrauen lässt sich nicht verordnen. Vertrauen erwirbt man durch Transparenz, zuverlässige Kommunikation und durch Institutionen, denen viele Menschen vertrauen. Hunderte Wissenschaftler*innen und diverse zivilgesellschaftliche Organisationen warnen inzwischen vor der zentralen Variante.

KRITIK AN ZIVILGESELLSCHAFTLICHEN AKTEUREN

Wenn es ideal umgesetzt werden würde und man die gesellschaftlichen Folgen ausblendet, dann wäre die dezentrale Variante eventuell für diesen Zweck ein hinnehmbares System. Aber es wird nicht ideal umgesetzt und es wird gesellschaftliche Folgen haben. Die App könnte wie ein Dammbruch fungieren. Deshalb ist es notwendig, Kritik am CCC und anderen zivilgesellschaftliche Akteur*innen zu üben. Zwar äußern sie sich kritisch[44], aber ihre Forderungen und Warnungen gehen nicht weit genug. Sie haben ein Klima der Akzeptanz für diese Apps geschaffen.

Es ist gesellschaftlich egal, ob das PEPP-PT-Framework, die dezentralisierte DP3T-Implementation, oder eine andere technische Umsetzung gewählt wird. Denn entscheidend ist doch die Schaffung der Akzeptanz, sich eine App für das vermeintliche gesellschaftliche Wohl zu installieren. Betont wird sowohl im zentralen und dezentralen Modell die Freiwilligkeit. Nur wer will, muss sich diese App installieren und nur auf initiative der Nutzer*innen, erfährt der zentrale Server, mit welchen anderen temporären IDs dieses Smartphone in Kontakt war. Der soziale Druck wird ausgeblendet.

Treffend formulieren Aktivist*innen eines Brandanschlags auf eine Datenleitung zum HHI am 14. April, dass die Debatte nicht um das Gesundheitssystem geht, sondern um das Individuum.

Die „Urängste der Menschen vor dem Tod werden mit dieser Pandemie instrumentalisiert. Mit diesen Ängsten wird „gespielt“. Nicht die Privatisierungspolitik in den Gesundheitssystemen wird in Frage gestellt, sondern ob DU genug Abstand zum Nächsten hältst. Ob DU die Regeln einhältst. Diese Regeln werden überwacht (und teilweise auch bestraft). Und sie fördern allerorten eine der deutschesten Tugenden: den Hang zur Denunziation. Ihm gesellt sich in intellektuellen Kreisen der Vorwurf hinzu, man sei unsolidarisch, wenn man nicht den Verordnungen folge. Wenn DU diese Regeln nicht einhältst, bist DU schuld daran, wenn Menschen sterben. Mit dem Verweis auf die „Risikogruppen“ werden andere Widersprüche abgewürgt. Die „Risikogruppen“ werden ungeachtet ihrer individuellen Haltung zu einem Faktor der moralischen Erpressung, um unter Freund_innen die staatlichen und politischen Regeln unhinterfragt durchzusetzen. Mit der medizinischen Hygiene geht eine soziale Hygiene einher, die kaum schmutziges, widerständiges Denken und Debattieren zulässt.“ [45]

---

43 Allerdings kann das durch Verwendung von Proxies, VPNs oder *Tor* verhindert werden.

44 Zu nennen sind hier beispielsweise eine gemeinsame Erklärung von 106 zivilgesellschaftlichen Organisationen, in der es heißt: „Staaten müssen beim Einsatz digitaler Überwachungstechnologien zur Bekämpfung von Pandemien die Menschenrechte achten“. Dort fordern sie „Regierungen nachdrücklich auf, bei der Bekämpfung der Pandemie sicherzustellen, dass der Einsatz digitaler Technologien zur Verfolgung und Überwachung von Einzelpersonen und Bevölkerungsgruppen streng im Einklang mit den Menschenrechten erfolgt.“ Weiter sind die 10 Prüfsteine für die Beurteilung von „Contact Tracing“-Apps des CCC zu nennen. Dort heißt es: „Sämtliche Konzepte [sind] strikt abzulehnen, die die Privatsphäre verletzen oder auch nur gefährden. Die auch bei konzeptionell und technisch sinnvollen Konzepten verbleibenden Restrisiken müssen fortlaufend beobachtet, offen debattiert und so weit wie möglich minimiert werden.“ Das Forum InformatikerInnen für Frieden und Gesellschaftliche Verantworung (FIfF) veröffentlichte eine Datenschutz-Folgenabschätzung (DSFA) für die Corona-App. In der es: „Wirksamkeit und Folgen entsprechender Apps sind noch nicht absehbar und es ist davon auszugehen, dass innerhalb der EU verschiedene Varianten erprobt und evaluiert werden. Die datenschutz- und somit grundrechtsrelevanten Folgen dieses Unterfangens betreffen potenziell nicht nur Einzelpersonen, sondern die Gesellschaft als Ganze.“

45 „Vulkangruppe shut down the power / Digitale Zurichtung sabotieren“, [B] Dokumentation: Shut down the power! Digitale Zurichtung sabotiert.“ veröffentlicht am: 2020-04-14 http://raxuatgmxdvnp4no.onion/?node=77193

Daten von denen versprochen wird, dass sie vertraulich behandelt werden, werden immer wieder anderweitig verwendet. Es wird nicht lange Dauern bis die Diskussion beginnt, diese Daten zur Strafverfolgung zu nutzen und die Debatte wird erst aufhören, wenn die Nutzung freigegeben wurde. Wo ein Trog ist, kommen die Schweine. Beispiele, wo es sich genauso zugetragen hat (wie etwa die Kennzeichenerfassung der elektronischen Maut) gibt es viele. Dazu kommt die behördliche Weigerung bei Löschung einst erhobener Daten.

Beim zentralen Modell müssen Personen aktiv die Daten ihrer Annäherungsgeschichte freigeben. Aber mit einem Software-Update ist es leicht zu beheben, derart dass immer alle Kontakte hochgeladen werden. So entsteht ein riesiger Heuhaufen, der für Big-Data-Zwecke nutzbar ist. Wenn immer alle Kontakt-IDs übermittelt werden (also nicht mehr nur freiwillig, wenn eine Person infiziert ist), dann kann der Server auch Traces bilden und Verbindungen herstellen, wer wie oft wen trifft. In Zusammenarbeit mit den Telekommunikationsanbietern zur Auflösung von IP-Adressen, könnten Strafverfolgungsbehörden dann auflösen, wer sich hinter den IDs verbirgt.

Selbst beim dezentralen Modell besteht die Gefahr, dass die IDs nicht mit anderen Merkmalen oder sogar dem Google- oder Apple-Konto verknüpft werden. Dennoch ist denkbar, dass wir in Zukunft Malware sehen, die genutzt wird, um diese Daten zusammenzutragen.

DIE ROLLE VON GOOGLE UND APPLE

Es ist wichtig, grundlegende Unterschiede zwischen den Tracing-Apps zu verstehen und ernst zu nehmen. Anstatt die technischen Details als Lappalie abzutun, sollten wir die Möglichkeit bedenken, dass Tracing-Apps womöglich keine temporäre Erscheinung sind, die wieder verschwindet, sobald die Pandemie unter Kontrolle gebracht ist. Tracing-Apps könnten sich als Instrument der Gesundheitspolitik oder in anderen Bereichen verstetigen. Wenn einmal ein großer Teil der Smartphone-Nutzenden eine solche App installiert hat und ihr Betrieb zum Normalfall geworden ist, ergeben sich womöglich weitere Anwendungsmöglichkeiten, die jetzt noch jenseits des Vorstellbaren liegen. Das Verfolgen der jährlichen Influenza-Welle wäre nur ein erster Schritt. Wenn diese Funktionalität zur Verfügung steht, dann gibt es in Zukunft wahrscheinlich noch mehr Apps, die so etwas nutzen. Des Weiteren haben Google und Apple auch Interesse an Social-Graphs.

Das Schreiben ist im Widerstandsteil dieser Broschüre dokumentiert.

Dass diese Entwicklung wahrscheinlich ist, ist daran festzumachen, dass Google und Apple gemeinsam an Contact-Tracing-Software arbeiten[46]. Zudem haben Google und Apple angekündigt, das dezentrale Modell der Kontaktverfolgung zu unterstützen, indem sie entsprechende Funktionen in ihre Smartphone-Betriebssysteme einbauen. Auf diese Weise kann die ständige Suche nach neuen Kontakten kontinuierlich im Hintergrund der Smartphones ablaufen, ohne den Akku zu sehr zu strapazieren. Die Kooperation könnte bald auf den meisten Smartphones auf der Welt Apps verfügbar machen, die ihre Nutzer*innen informieren, ob sie sich in der Nähe von möglichen Corona-Infizierten aufgehalten haben. Die außergewöhnliche Zusammenarbeit der zwei Technologiekonzerne schafft einen globalen Standard für Contact-Tracing. Denn anders als vielfach öffentlich kommuniziert, sind beide Ansätze auf eine Unterstützung durch die Betriebssysteme von Google und Apple angewiesen. Beide Unternehmen haben im Übrigen angekündigt, dass sie keine eigene Infrastruktur betreiben wollen, sondern diese Aufgabe den Gesundheitsbehörden überlassen werden, die an der digitalen Kontaktverfolgung mitwirken möchten. Die Schnittstelle im Betriebssystem der Smartphones soll dazu dienen, die notwendigen Daten lokal zu erheben und diese dann mit dem Server der Gesundheitsbehörden auszutauschen.

Offen bleibt die Frage, wie die geplanten Erweiterungen der Smartphone-Betriebssysteme genau umgesetzt werden; insbesondere, ob diese nicht vielleicht doch Informationen an die Konzerne zurücksenden könnten. Es ist daher essenziell, dass Google und Apple den Quellcode für ihre Erweiterungen offenlegen und damit unabhängigen Sicherheitsforscher*innen die Möglichkeit einräumen zu überprüfen, dass keine zusätzlichen Funktionen eingebaut wurden.

Nachdem Apple und Google 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[47]), investieren die IT-Konzerne Milliarden in eigene Gesundheitsdatenbanken und versuchen mit Hochdruck, erweiterte Gesundheitsdienste in ihre Softwareumgebungen zu integrieren. Deshalb sind sowohl Apple als auch Google eigenständige relevante Akteure auf dem Gesundheitssektor. Aus diesem Grund war die Unterstützung der dezentralen Varian-

46 Siehe dazu: Apple and Google partner on COVID-19 contact tracing technology https://blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology und https://netzpolitik.org/2020/apple-und-google-schaffen-globalen-standard/

47 http://fortune.com/2017/09/11/apple-tim-cook-education-health-care/

te eine wichtige strategische Entscheidung. Die öffentliche Entscheidung für das dezentrale Modell aus Privacy-Aspekten dient auch durchaus der Imagepflege. Es macht sie aber vor allem zur unausweichlichen Instanz. Sie sind die einzigen, die den Zugriff auf den gesamten Datensatz haben. Staatliche Akteure müssen mit ihnen verhandeln, wenn sie doch Zugriff auf den gesamten Datensatz erlangen wollen.

Wie weit die faktische Macht der beiden dominanten Smartphone-Betriebssystem-Anbieter geht, lässt sich am Rückzieher der australischen Regierung mit ihrer zentralen Corona-App ablesen[48]: Die bereits gut fünf Millionen Mal heruntergeladene Corona-App „Covidsafe" läuft auf iPhones nicht, da Bluetooth im Hintergrund nur eingeschränkt funktioniert. Daher musste die australische Regierung im Mai auf die Vorgabe von Apples und Googles geplanter Schnittstelle für Corona-Warn-Apps umsatteln.

SICHERHEITSLÜCKE BLUETOOTH

Heutzutage ist Bluetooth ein integraler Bestandteil von mobilen Geräten. Laptops und Smartphones lassen sich mit Smartwatches und drahtlosen Kopfhörern verbinden. Standardmäßig sind die meisten Geräte so konfiguriert, dass sie Bluetooth-Verbindungen von jedem nicht authentifiziertem Gerät in der Nähe zulassen. Bluetooth-Pakete werden durch den Bluetooth-Chip (auch Controller genannt) verarbeitet und dann an den Host (Android, Linux usw.) weitergeleitet. Sowohl die Firmware auf dem Chip, als auch das Bluetooth-Subsystem des Hosts, sind ein Ziel für Remote-Code-Execution-Angriffe (RCE).

Bluetooth hat eine 20 Jahre alte Geschichte der Unsicherheit. Alle paar Jahre gibt es einen neuen Angriff auf Bluetooths Pairing-Protokoll oder die verwendete Verschlüsselung. Auch aktuell gibt es eine Sicherheitslücke (CVE-2020-0022[49]) und Exploit der diese ausnutzt (Bluetooth zero-click short-distance RCE exploit against Android 8/9 [bei Android 10 keine RCE aber DoS]). Mit dieser Lücke und dem Exploit lässt sich ein Wurm schreiben, der sich ohne User-Interaktion über Bluetooth weiterverbreitet und auf den Geräten Schadcode in einem privilegierten Prozess ausführen kann[50].

Wer jemandem zu nahe kommt, kann sich nicht nur selbst mit Covid-19 infizieren, sondern mit einem CVE-2020-0022-Wurm – dank der Corona-App – auch sein Smartphone, welches den Wurm dann munter weitergibt.

Der Bug ist in dem Security-Patch von Android Open Source Project (AOSP) vom Februar 2020 gefixt. Aber welche Android-Smartphones werden den jemals erhalten?

AUCH ANONYM TRAINIEREN WIR KI

Die für Deutschland geplante Corona-App soll nicht auf personenbezogene Daten des einzelnen Individuums zugreifen. Doch die Gefahren entstehen nicht nur bei der digitalen Ausleuchtung einzelner, sondern dadurch, dass eine entstehende Datensammlung in Verknüpfung mit anderen Datenbanken algorithmische Verfahren zur Bevölkerungsverwaltung ermöglicht.

Im konkreten Fall der dezentralen Corona-App, welche die deutsche Bundesregierung nun favorisiert, gibt ein Zusatz zu denken: Es solle die Möglichkeit integriert werden, freiwillig in pseudonymisierter Form die Daten zur epidemiologischen Forschung und Qualitätssicherung an das RKI zu übermitteln.[51] Ein unbedeutend klingender „Zusatz", der die Dezentralität der Corona-App freiwillig aushebelt. Sollten Hunderttausende diese Option wählen (bzw. nicht abwählen), ließen sich aus den Zeitangaben der pseudonymen Tracing-Daten in der Verknüpfung z. B. mit einer Datenbank wann, wo, welche Großevents stattgefunden haben, erahnen, wo sich vermeintlich unverantwortlich verhalten wurde. So lassen sich über zeitlich korrelierte Häufungen Regionen ausmachen, die eine etwaige Sonderbehandlung „rechtfertigen". Spätestens, wenn sich die freiwilligen Meldungen vermeintlich Infizierter bei Gesundheitsämtern zeitlich in Verbindung bringen lassen, könnte (mit Einschränkungen) eine „Gefährder"karte erstellt werden.

Pseudonymisierte Massendaten dienen zum Training künstlicher Intelligenzen (KI) z. B. im Kontext vorhersagender Analysen. In dem Moment, wo Verhaltensdaten fast flächendeckend anfallen und (sei es auch anonymisiert) erhoben werden, sind die prädiktiven Modelle, die damit trainiert werden, dazu in der Lage, ganze Populationen in Risikogruppen einzuteilen und algorithmisch zu verwalten. Datenbasierte Algorithmen können die Gesellschaft dann in unsichtbare soziale Klassen einteilen, zum Beispiel in Bezug darauf, wer aufgrund seiner Bewegungsmuster vermeintlich ein besonderes

48 https://www.heise.de/mac-and-i/meldung/Australien-Corona-App-funktioniert-ohne-Apple-API-nicht-richtig-auf-iPhones-4716013.html

49 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0022

50 Für Angriffe auf BLE siehe beispielsweise https://www.andreafortuna.org/2020/02/18/sweyntooth-bluetooth-vulnerabilities-expose-many-ble-devices-to-attacks/ oder https://asset-group.github.io/disclosures/sweyntooth/

51 Taz 26.4.20: https://taz.de/Debatte-um-die-Corona-App/!5681031

Sicherheits- oder Gesundheitsrisiko darstellt, weil das Bewegungsprofil erkennen lässt, dass jemand das Virus in besonderem Maße verbreitet hat oder wer prioritären Zugang zu knappen medizinischen Ressourcen wie Beatmungsplätzen verdient. Dies ist möglich, ohne die Ortsdaten einzelner Individuen aufgezeichnet zu haben.

Algorithmische Scoring- und Entscheidungsverfahren beruhen auf einem anonymen Abgleich mit den Daten vieler anderer Individuen.

Daher kann mensch durch Weitergabe der eigenen (selbst anonymisierten oder pseudonymisierten) Daten potenziell anderen Individuen und Gruppen schaden und umgekehrt durch die Datenweitergabe anderer potenziell selbst betroffen sein. Diese Gefahr wird in der verkürzten Debatte um die Corona-App und auch schon bei der Weitergabe anonymisierter Telekom-Daten oder anonymisierter Google-Positionsdaten ausgeblendet. Sie ist auch nicht Gegenstand wirksamer datenschutzrechtlicher Bemühungen. So schützt auch die Datenschutzgrundverordnung DSGVO nicht vor der Verwendung anonymisierter Daten für prädiktive algorithmische Entscheidungen, Risikoklassifizierung (Scoring) und verhaltensbasierte Ungleichbehandlung von Individuen oder Gruppen. In diesem Sinne trägt jede*r, die*der die Corona-App nutzt, zu solch einer Ungleichbehandlung bei.

Hier ist die Unterscheidung von anonymen und personenbezogenen Daten überholt, weil irrelevant!

FREIWILLIGKEIT UND IMMUNITÄTSNACHWEIS

*„Bitte haben Sie Verständnis dafür, dass wir zu ihrer eigenen Sicherheit und zur Sicherheit unserer Mitarbeiter*innen nur nachweislich nicht-infizierte Personen befördern können."*

So könnte die Erklärung der Deutschen Bahn an allen Automaten und Ticket-Schaltern lauten, die ihre Dienstleistung „bis zum Ende der Corona-Krise" nur Fahrgästen mit einer ungefährlichen Kontakt-Tracing-Historie, wahlweise in Verbindung mit einem kürzlich durchgeführten Corona-Test (PCR oder Antikörper) oder einem „Immunitätsnachweis" anbietet.

Eine *freiwillige* Corona-App (egal ob zentral oder dezentral), die binnen der letzten zwei Wochen keinen Alarm geschlagen hat, ist eine Möglichkeit diesen „Nachweis" zu erbringen. Das entspräche dem Status „grün" der (zentralen) chinesischen App wahlweise bei der Fahrkartenkontrolle oder beim Betreten des Bahnhofs. Eine zweite Möglichkeit des Nachweises ist der geplante, ebenso *freiwillige* „digitale Immunitätsausweis". Die Notwendigkeit, einen der beiden *freiwilligen* Nachweise erbringen zu müssen, stellt die soziale Unfreiwilligkeit der Konstruktion dar.

Die technischen Pläne für einen digitalen Immunitätsausweis wurden veröffentlicht[52]: Die Bundesregierung plant als Imitation der Idee von Bill Gates (siehe dazu den Text „Weniger Arzt im künstlich intelligenten Gesundheitssystem" in dieser Broschüre) die Möglichkeit, Menschen bescheinigen zu lassen, dass sie eine Infektion mit dem Coronavirus überstanden haben – für den Fall, dass es gesicherte Erkenntnisse darüber gibt, dass eine überstandene Infektion für eine gewisse Zeit Immunität bedeutet. Derzeit gehen einige Wissenschaftler*innen (mit einer hohen Fehlerquote) von drei Monaten aus. Deutliche Kritik an diesem Vorhaben hat Gesundheitsminister Spahn Anfang Mai zum Rückzug eines Gesetzentwurfes gezwungen.

Es gibt einen historischen Vorläufer: Als das gefährliche Gelbfieber im 19. Jahrhundert in New Orleans grassierte, wurde ein „Immunitätsbonus" erprobt[53]. Die Folgen waren gravierend. Zusätzlich zur rassistischen Trennung zwischen Weißen und Schwarzen bildete sich nun auf beiden Seiten noch eine weitere unsichtbare Grenze aus: zwischen den bereits Immunen und den weiterhin vom Gelbfieber bedrohten. An der Immunität gegen Gelbfieber entschieden sich die berufliche Anstellung, der Wohnort und der Lohn, Kreditwürdigkeit und wen man heiraten konnte. Der „Immunitätsbonus" verstärkte Rassismus und Angestellte und Arbeiter*innen wurden dadurch unter Existenzdruck gehalten.

Nun soll ein solcher Ausweis in Nordrhein-Westfalen zunächst nur erprobt werden. An diesem Projekt arbeiten derzeit die Bundesdruckerei, die Lufthansa, die Unternehmen *Digital-Health Germany, m.Doc* und *GovDigital* sowie die Uniklinik und das Gesundheitsamt der Stadt Köln. Testpatienten*innen sollen mithilfe einer App ihr Corona-Testergebnis verschlüsselt in einer Datenbank abspeichern. Flughäfen, Infrastrukturunternehmen und Behörden sollen so auf das Coronavirus-Testergebnis zugreifen können! In Erweiterung der seit Mai geltenden Praxis an den Flughäfen Frankfurt und Wien, per selbst zu zahlendem Corona-Schnelltest vor Ort die zweiwöchige Einreise-Quarantäne umgehen zu können, würde dann die „fälschungssicher" nachgewiesene Immunität ebenfalls Bewegungsfreiheit garantieren. Eine Regelung mit der fatalen Nebenwirkung vieler sich bereitwillig Ansteckender, die zur Wahrung

52 https://ubirch.de/fileadmin/user_upload/2020-04-16_digital_corona_health_certificate.pdf

53 Johannes Saltzwedel. Corona-Vorgänger Gelbfieber: Immunität als Gottesgeschenk. 01.05.2020, https://www.spiegel.de/geschichte/corona-vorgaenger-gelbfieber-immunitaet-als-gottesgeschenk-a-2f639c0c-14d0-4aa3-9bf1-edfb868debff

ihrer Beweglichkeit das Gesundheitssystem an einem kritischen Punkt zusätzlich belasten könnten.

Die Konsequenz wäre eine gesellschaftlich spaltende Endsolidarisierung, die Corona-bedingte Einschränkung der Bewegungsfreiheit nur für diejenigen zu lockern, die sich zumindest einem der beiden Programme unterwerfen. Als am 10. April der CSU-Digitalpolitiker Hansjörg Durz vorschlug, nach dem Lockdown Druck auf potenzielle App-Verweigerer*innen auszuüben, haben die meisten diese Option als unrealistisch abgewunken. Tatsächlich schlug er vor, was Spahn zwei Wochen später mit seinem Immunitätsausweis probierte: „So könnten Grundrechte wie die Bewegungsfreiheit denen wieder gewährt werden, die die App installiert haben", sagte der Vize-Vorsitzende des Digitalausschusses im Bundestag dem Handelsblatt. „Wer sich gegen die Nutzung der Corona-App entscheidet, müsste im Gegenzug größere Einschränkungen anderer Grundrechte in Kauf nehmen." Es ist keineswegs zynisch, das Vorhaben mit einer elektronischen Fußfessel zu vergleichen – Freigänger müssen sie tragen, oder zurück in den geschlossenen Vollzug.

Die „freiwillige" Corona-App und der „freiwillige" Immunitätsnachweis sollen damit zu Unterscheidungs-Werkzeugen für individuelle soziale Teilhabe werden. Wer Bahn fahren oder fliegen will, bräuchte dann entweder die App- oder den Immunitätsnachweis. Der Staat „verordnet" diese App nicht, er stellt sie lediglich zur Verfügung. Wirtschaftliche Akteure – in unserem Beispiel die Deutsche Bahn – würden ihre Dienstleistung nur denen anbieten, die in diese algorithmischen Filter einwilligen. Regierung und Dienstleister würden dabei ganz im Sinne einer übergeordneten Verantwortung für das Gemeinwohl handeln. Wer will da noch meckern – wo doch nun alles so „datensparsam" dezentral gelöst ist. Der Applaus einiger verengt blickender Datenschützer*innen ist ihnen leider gewiss.

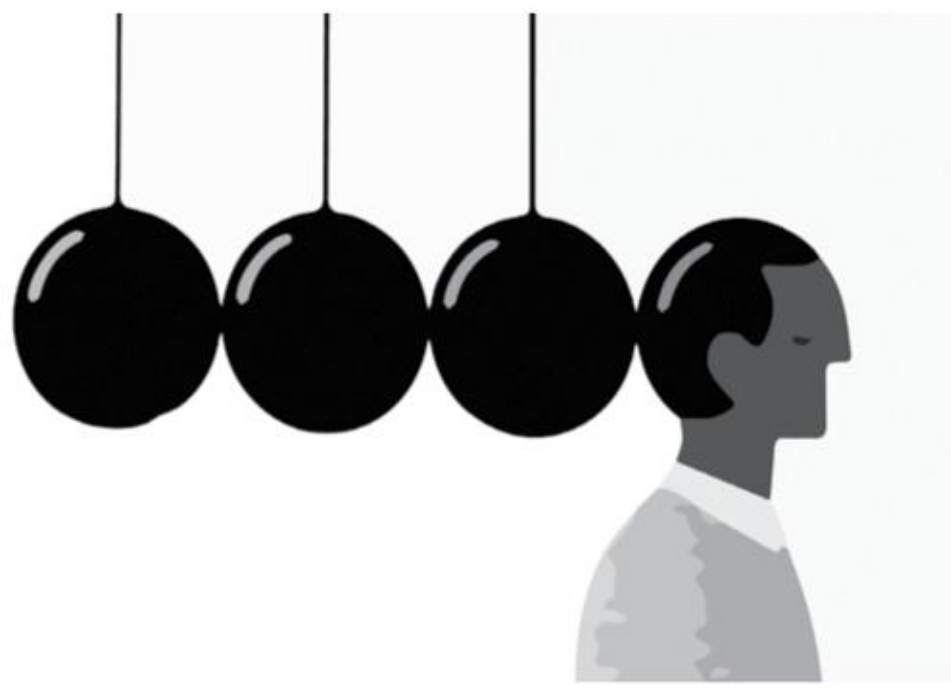
Auf dieser Form von „Freiwilligkeit" basieren viele der derzeit erprobten Social-Scoring-Modelle in China. Wer nicht mitmacht oder die erforderliche Eigenschaft nicht erfüllt, kann ohne Verbotsverfügung „freiwillig" vom öffentlichen Leben ausgeschlossen werden: Die Corona-App und der Immunitätspass als Einübung individueller Einschluss- / Ausschluss-Mechanismen zukünftiger Soziale-Punkte-Systeme auch in Deutschland – ganz ohne Zwang auszuüben.

Behaviorismus und Kybernetik

Grundlagen der Verhaltenslenkung

*Eine kleine patriarchale Elite von Technokrat*innen 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 worauf basiert die Idee dieser maximal invasiven Verhaltenslenkung? Tatsächlich finden wir im Behaviorismus die meisten Wurzeln der paternalistischen technototalitären Methoden.*

Und es gibt einen spannenden Vorläufer der aktuellen Auseinandersetzung um Autonomie in den USA der 1970er – eine erfolgreiche Widerstandsbewegung, die ein groß angelegtes Verhaltenslenkungsprogramm kippte.



John B. Watson beschrieb 1913 in seiner Antrittsvorlesung an der Columbia University die „Psychologie aus der Sicht des Behavioristen" als Disziplin mit dem „theoretischen Ziel, Verhalten vorherzusagen und zu steuern". Indem Watson die Tätigkeit des Gehirns oder „innere Zustände" als Blackbox außen vor ließ, konnte er allein mit dem beobachtbaren Verhalten lebendiger Wesen arbeiten und davon ausgehend eine Psychologie ohne jegliche Subjektivität entwerfen.

B. F. Skinner erforschte mit einer Methode, die er „operante Konditionierung" nannte, wie bestimmte äußere Reize das Lernen beeinflussen. Während die klassische (Pawlow'sche) Konditionierung einen Reiz schlicht mit einer Reaktion koppelt, ist bei der operanten Konditionierung das Verhalten anfangs spontan, doch die davon ausgelöste Rückkopplung bestärkt oder hemmt die Wiederkehr bestimmter Handlungen. Für Skinner ist der Mensch ein „Bündel von Verhaltensmustern" ohne Subjektivität – ein Automat mit erwartbaren und manipulierbaren Reaktionen auf die Umwelt.

Das Konzept der menschlichen Willensfreiheit habe seinen Sinn gehabt, solange Menschen gegen die Tyrannei von Despoten kämpfen mussten; nun aber habe es seine Schuldigkeit getan. Denn in der modernen Industriegesellschaft bringe gerade diese Freiheit, in Gestalt des ungehemmten Individualismus, Widersprüche und Missstände hervor: z. B. Überbevölkerung und Umweltzerstörung, so Skinner.

„Kontrolliert werden wir ohnehin – von Eltern, Lehrern, von der Werbung und der Regierung, aber wir werden auf dilettantische Weise kontrolliert."

Deswegen sei es in Wahrheit gar kein Risiko, wenn Menschen sich künftig einer Diktatur umfassender sozialer Steuerung und Kontrolle unterwerfen.

„Nur wenn wir die Vorstellung vom autonomen Menschen abschaffen – wenden wir uns den wahren Ursachen seines Verhaltens zu – vom nachträglich Vermuteten zum Beobachtbaren, vom Wundersamen zum Natürlichen, vom Ungreifbaren zum Manipulierbaren."

Skinner sieht auch viel grundsätzlichere Fragen von Gleichberechtigung der Geschlechter bis hin zum Abbau von Aggression, Neid und Eifersucht über seine Form der Konditionierung erreichbar, ganz ohne deren gesellschaftliche Hintergründe erforschen zu wollen. Für ihn ist die Verhaltenslenkung kein klassisch despotisch, repressives System, sondern eher belohnungszentrierter „sanfter Zwang". Er stellte sich vor, nicht nur einzelne Lernprozesse, sondern die gesamte Lebensführung von Gruppen nach verhaltenspsychologischen Maßregeln zu steuern.

Auf die Frage, wer solle denn die Normen für die Verhaltenslenkung setzen, (heute würden wir fragen: Wer schreibt den *Code*?) antwortet Skinner: „Wissenschaftler".

ANALOGIE ZUR KYBERNETIK

Die Kybernetik war die erste Wissenschaft, die Information und Leben identisch gesetzt hat. Es ist interessant zu beobachten, wie eng verbandelt der von Watson und Skinner geprägte Behaviorismus mit der Disziplin der Kybernetik ist, obwohl sie augenscheinlich aus unterschiedlichen Diszplinen herrühren. Es ist mehr als nur eine unheimliche Ähnlichkeit. Sowohl Norbert Wiener als auch B. F. Skinner arbeiteten während des zweiten Weltkriegs zeitgleich an Forschungsvorhaben des US-Militärs. Skinner dressierte Tauben zum Steuern von Raketen im Kamikaze-Stil innerhalb des Projekts „Pelikan".

Wiener entwickelte mit dem Ingenieur Julian Bigelow eine prognostizierende Flugabwehr, die maschinell den zukünftigen Kurs eines angreifenden Flugzeugs ermitteln sollte. Dabei ging Wiener davon aus, dass sich menschliches Verhalten statistisch modellieren lässt. Mithilfe eines speziellen Analyseverfahrens simulierte seien Forschungsgruppe vier Arten möglicher Flugbahnen, auf denen eine Maschine dem Artilleriefeuer entgehen konnte. Ein zugleich physikalisches, aber auch physiologisches Problem. Wiener bemerkte, dass sich das Verhalten des Piloten zwischen explodierenden Geschossen, Turbulenzen und dem Suchscheinwerferlicht auf wenige Reflexhandlungen reduzieren ließ. Er verglich die Ausweichstrategien des Piloten mit den Rückkopplungsprinzipien einfacher Mess- und Steuerkreise physikalischer Systeme.

So schloss Wiener, dass sich biologische Systeme funktional ähnlich und informationell gleich zu mechanischen Systemen beschreiben lassen. Diesen Grundgedanken baute Wiener zu einer umfassenden physiologischen Theorie. Obwohl Wieners Theorien aus seiner Ingenieurstätigkeit hervorgingen, basieren sie auf behavioristischem Denken: Er untersucht, um die zukünftigen Handlungen eines Organismus vorherzusagen, nicht dessen Struktur, sondern dessen Verhalten in der Vergangenheit. Wie die Kybernetik beruht auch der Behaviorismus auf einem rekursiven (Rückkopplungs-) Modell, das in der Biologie Verstärkung genannt wird. Rückkopplung ist nach Wieners Definition „die Fähigkeit, zukünftiges Verhalten an den Erfolgen des vergangenen auszurichten".[54]

54 Norbert Wiener, The Human Use of Human Being: Cybernetic and Society, Da Capo Press, Cambridge/MA 1988, S.33

Umgekehrt ähnelt Skinners Darstellung des aktiven Verhaltens als Repertoire möglicher Handlungen, unter denen einige durch Verstärkung begünstigt werden, Wiens Beschreibung von Informationsschleifen, bei denen eine negative Rückkopplung (Messen) ebenfalls den Input korrigiert (Steuern). Behaviorismus und Kybernetik beruhen auf Input-Output-Analysen, die sich nicht um die Struktur der „Black-Box" dazwischen kümmern. Beide kümmern sich um a) ausschließlich beobachtbares Verhalten und betrachten b) jedes Verhalten als in sich zielorientiert und / oder zweckdienlich.

In kybernetischen Begriffen sind ein Frosch, der es auf eine Fliege abgesehen hat, und eine zielsuchende Rakete dasselbe System: Beide sammeln Informationen, um ihr Handeln im weiteren Verlauf entsprechend anzupassen.

WIDERSTAND GEGEN GEDANKEN- UND VERHALTENSMODIFIKATION

„In jüngster Zeit hat die Technik mit der Entwicklung neuer Methoden der Verhaltenskontrolle begonnen, die in der Lage sind, nicht nur die Handlungsweise des Einzelnen zu verändern, sondern seine Persönlichkeit und seine Denkart an sich. (…) Die Verhaltenstechnologie wie man sie heute in den Vereinigten Staaten entwickelt, rührt an die grundlegenden Quellen der Individualität und an den Kern der persönlichen Freiheit. (…) Die größte Gefahr ist die Macht, die diese Technologie einem Einzelnen in die Hand gibt, seine Weltsicht und seine Werte einem anderen aufzuzwingen … Begriffe von Freiheit, Privatsphäre und Selbstbestimmung stehen ihrem Wesen nach im Konflikt mit Programmen, die darauf abzielen, nicht nur physische Freiheit zu kontrollieren, sondern die Quelle freien Denkens an sich."[55]

Das ist nicht etwa die besorgte Rede einer Abgeordneten bei der Anhörung von Mark Zuckerberg vor dem EU-Parlament 2018, sondern ein Auszug aus dem Bericht des US-Senatsausschusses von Senator Sam Ervin aus dem Jahr 1974(!). Es ist die beeindruckend klare Bewertung eines eher konservativen Demokraten und Verfassungsrechtlers, der sich als Senator von North Carolina Anfang der 1970er einer breiten Bürgerbewegung gegen staatliche Verhaltensmodifikation angeschlossen hatte. Aktivist*innen, Wissenschaftler*innen und Anwält*innen bescherten der Nixon-Regierung nach jahrelangem Protest 1974 eine bemerkenswerte Schlappe. Es war das bis dahin größte Aufbegehren einer Bewegung gegen den Einsatz von Verhaltensänderungsprogrammen in Erweiterung staatlicher Macht.

Erwin und andere untersuchten in mehrjähriger Arbeit „eine Reihe von Programmen, die darauf abzielten, menschliches Verhalten vorherzusagen, zu kontrollieren und zu modifizieren." Die antikommunistische Hetze während und nach dem Koreakrieg sowie die CIA-Berichte über „systematische Gehirnwäsche" amerikanischer Kriegsgefangener durch den Feind, hatten erfolgreich eine Stimmung erzeugt, in der es angemessen schien, eigene geheimdienstliche Forschungsprogramme auf diesem Gebiet zu intensivieren. Zur Entwicklung von Fähigkeiten zur Gedankenkontrolle, vom *depattering* und *rewriting* des Einzelnen bis hin zur Manipulation von Verhaltensweisen eines kompletten Staates. Die Mittel dazu klingen nicht nur martialisch. Im MKUltra-Projekt der CIA wurden chemische, biologische, radiologische und sogar mechanische Mittel der Psychochirurgie und Elektrophysiologie benutzt. PSYOPS (Psychological Operations) sollten „defekte Persönlichkeiten" „festgesetzter" Individuen in kontrollierten Umgebungen wie Gefängnis oder geschlossene Anstalt korrigieren: Persönlichkeit, Identität und die Fähigkeit zu selbstbestimmendem Verhalten ließe sich unterdrücken, eliminieren und durch eine externe Kontrolle ersetzen, so die Überzeugung.

Die im Kalten Krieg erzeugten Ängste, die Unruhen der späten 60er und frühen 70er machten es möglich, dass Law-and-Order Hardliner unter Berufung auf einen Ausnahmezustand(!) vorpreschten, um aktive Verhaltensmodifikation aus dem militärischen in den zivilen Bereich fortzusetzen. Auf einmal wurde auch wieder Skinners Forschung aufgegriffen. Für fortschrittliche Geister der Autonomie eine erdrückend autoritäre Stimmung, die unerwünschtes Verhalten auszumerzen suchte.

Aber es regte sich auch Widerstand. Noam Chomsky schrieb in einer detaillierten Kritik an Skinners „Forschungserfolgen":

„Es wäre nicht nur absurd, es wäre grotesk, aus der Tatsache, dass sich Umstände arrangieren lassen, unter denen Verhalten durchaus vorhersagbar ist – wie z. B. in einem Gefängnis oder … einem Konzentrationslager … – darauf zu schließen, man brauche sich deshalb keine Sorge um die Freiheit und Würde des ‚autonomen Menschen' zu machen."[56] (Noam Chomsky)

Angewidert von den Exzessen der Geheimdienste und den Machenschaften der Nixon-Regierung unterstützten mehr und mehr die Bürgerrechtsbewegung und so sah sich die Regierung gezwungen, den Einsatz verhaltensverändernder Techniken im zivilen Bereich zu stoppen. Nach der heftigen öffentlichen Ablehnung

55 Sam Ervin, Individual Rigts and the federal Role in Behavior Modification, http://www.healreport.tv/1974congressbehaviormod.pdf

56 Noam Chomsky, The Case Against B. F. Skinner, 1971

von „Jenseits von Freihit und Würde“ versuchte Skinner 1976 mit den „Missverständnissen“ um sein Werk aufzuräumen, aber sein Nachfolger „Was ist Behaviorismus?“ fand keine weitere Beachtung mehr.

Aber die nunmehr unpopulären Ideen zur Kommodifizierung des Verhaltens waren natürlich nicht ausgelöscht. Die Bundesgefängnisverwaltung in den USA empfahl, lediglich den Begriff „Verhaltensmodifikation“ zu vermeiden und stattdessen von „Belohnung und positiver Verstärkung“ zu sprechen, aber ansonsten die Programme weiterlaufen zu lassen. Ein offenes Ende eines hart umkämpften Sieges der Bürggerrechtsbewegung in den USA, das die heutigen rechten Technokraten mit ihren Verhaltenslenkungsplattformen, den *Scoring*-Modellen, dem *Nudging* und der *Gamification* dankend aufgegriffen haben …

Horizonte überschreiten

Von Sandra Göbel

Sandra, die Autorin des folgende Textes, war eine radikale Kämpferin seit ihrer Schulzeit in den 80er Jahren. Sie gab sich nie mit den Setzungen, Gewohnheiten und Limitierungen der vielen Ein-Punkt-Bewegungen innerhalb der linken Szene zufrieden. Sie recherchierte vermeintliche Gewissheiten neu und sprengte viel zu eng gefasste Szene-Kategorien auf. Als international agierende Sozial-Revolutionärin verknüpfte sie viele linke Kämpfe und ließ sich nicht auf ihr langjähriges Brennen für die (militante) Anti-Atom-Bewegung reduzieren. Ihre umfassende Technologie- und „Fortschritts“-kritik mündete in eine Auseinandersetzung mit der Kybernetik und in kritisch-philosophische Betrachtungen des grundsätzlichen Verhältnisses von Mensch und Natur. Sie starb leider viel zu früh im Juni 2019 infolge einer Krebserkrankung. Daher konnten einige Fragen hinsichtlich des nun folgenden Texts nicht abschließend geklärt werden. Dennoch freuen wir uns, ihre Gedanken ein letztes Mal mit ihr teilen und hiermit verbreiten zu können. Der Text wurde ebenfalls ins Französische und Englische[57] übersetzt.

57 https://thenewinquiry.com/trespassing-horizons/

Sein Blick ist vom Vorübergehn der Stäbe
so müd‘ geworden, dass er nichts mehr hält.
Ihm ist, als ob es tausend Stäbe gäbe
und hinter tausend Stäben keine Welt […]

Rainer Maria Rilke, Der Panther

Warum ist es immer so schwierig, über die neuesten technologischen Entwicklungen zu diskutieren, ohne die Anzeichen für den kommenden Weltuntergang aufzulisten oder den unvermeidlichen linearen Verlauf des Fortschrittes als gesetzt zu sehen? Es ist bedenklich, dass die Frage vergessen geht, was ein besseres Leben wäre, trotz des Lebens in einem offensichtlich zerstörerischen System, dessen einzige Zukunft keine Zukunft ist. Wie können wir unsere tiefsitzende Angst vor der Kante des Horizonts abschütteln, um wieder anzustreben, dass die Zukunft anders herauskommt, als sie scheint?

Wie Kinder werden wir hin und her geschüttelt zwischen Fakten und Fakes, zwischen dem Gedanken an uns selbst als Genie und dem nächsten als Narr. Wir sind hart in der Verteidigung des autonomen Individuums, das rational Werkzeuge einsetzt, um seine eigene kleine Welt zu bauen, und das doch zutiefst beunruhigt ist über die Aussicht, dass Maschinen klüger werden als ihre Erbauer. Wir sehen uns vor eine neue Normalität gestellt, die selbst den enthusiastischsten Klugscheißer überwältigt.

Die westliche Kultur begann irgendwann, Zeit mit Chronologie gleichzusetzen. Zeit wurde als Pfad konzipiert, der uns gradlinig von der Vergangenheit über die Gegenwart hin zur Zukunft führt. Während der industriellen Revolution im 19. Jahrhundert, einer Periode des Enthusiasmus für den Fortschritt und der Glorifizierung der Moderne, waren die Blicke positiv auf die Zukunft gerichtet. Zukunft wurde als Verbesserung des Gegenwärtigen interpretiert. Nachdem mit dem Ersten Weltkrieg der Glaube an den endgültigen Triumpf der Vernunft verloren ging, sowie mit den durchtechnologisierten Desastern des Zweiten Weltkrieges die Idee des Fortschrittes beendet wurde und sich die letzten alten Götter zurückgezogen hatten, waren die Technokraten diejenigen, die noch übrigblieben, um die Reihenfolge der Dinge zu benennen. Heute scheint es, als hätten wir uns im Großen und Ganzen an eine Reihe ihrer Grundannahmen gewöhnt, die uns lähmen. Dies macht uns alle – Kritiker und Protagonisten der intelligenten neuen Welt gleichermaßen – scheinbar unfähig, dem Denken an die Welt als einer quantifizierenden Logik auszuweichen und nicht selbst alles in Zahlen zu übersetzen.

In der Zeit des Kalten Krieges, als im Westen alle politischen Debatten im Entweder-oder des Antikommunismus ertränkt wurden, lautete das einzige Ergebnis, das allen Technokraten nützlich schien, dass jeder Vorschlag befreiend sei, der sich von allen politischen Positionen distanzierte und eine Ideologiefreiheit proklamierte. In dieser Periode, die sich dem Humanismus als Antihumanismus entgegenstellte, wurde der von Norbert Wiener für ein ballistisches Raketenprogramm entwickelte prospektive Kalkulationskreis, genannt Kybernetik, zum Modell für die Steuerung westlich-demokratischer Gesellschaften erweitert und in die Verwaltung der Wirtschaft eingebaut – was beides zunehmend zum Gleichen wurde.

Nach einer intensiven öffentlichen Debatte zwischen den 1950er- und 1970er-Jahren, die von der Feier der berechenbaren Zukunft bis hin zu nachdenklichen Kritiken reichte, die das kommende technokratische Regime vorwegnahmen, zog die Kybernetik in den folgenden Jahren ihre Zügel straffer, aber sie tat dies leise. In den Diskussionen um die Automatisierung während der 1980er-Jahre gerieten die grundlegenderen Implikationen dann zuerst aus dem Blickfeld. Das Bewusstsein hierfür kam erst wieder auf, als sich das Internet und seine erweiterte Virtu-/Realität spürbar machte. Plötzlich stellten die Menschen fest, dass in ihrem Leben etwas fehlt. Aber was? Wenn wir den künstlich erschaffenen Fetisch der Technik nicht selbst dafür verantwortlich machen wollen und nicht auf das Problem starren wollen, wie ein Kaninchen auf die Schlange, müssen wir auf dem eingeschlagenen Weg nach einer Antwort suchen. Wir müssen die gewählte Richtung und die konkreten Schritte untersuchen und das Gewordensein auf seine Idee und Entwicklung hin befragen. Da das Grundprinzip der Kybernetik die gerichtete Selbstorganisation ist, lautet der erste Schritt, eine Unterscheidung zwischen Richtung und Führung zu machen. Dieser Text ist ein Versuch, dies aufzuzeigen, indem ich mich einer Debatte widme, die vor dem Zweiten Weltkrieg stattfand, aber implizit schon sein Ende vorwegnahm.

Bereits sechs Jahre vor der ersten Macy-Konferenz, die den Begriff Kybernetik salonfähig machen sollte, fand in New York ein interdisziplinäres Symposium statt, genannt die „Conference on Science, Philosophy and Religion". Um eine hier geführte Debatte geht es mir. Organisiert wurde die Konferenz von neun Wissenschaftlern um den konservativen Denker Louis Finkelstein. Die Gruppe veranstaltete 1940 ihr erstes Symposium unter dem Motto, „die Krise unserer Kultur durch ein Experiment des unternehmerischen Denkens zu bewältigen". Eine Krise, deren Kern eine „intellektuelle Verwirrung" sei, die sie für genauso wichtig hielten, wenn nicht sogar für wichtiger als „die totalitäre Lebensweise, die sich schnell in der Welt ausbreitet bis hin zur drohenden Gefahr für die Zivilisation". Die Zielsetzung der Konferenz liest sich wie eine frühe Version des aktuellen Denkens über Extremismus, in der die Bedrohung der Demokratie ihren Kritikern untergeschoben wird. Und trotz der vagen Formulierung versteht man, dass nicht die Faschisten am meisten gefürchtet wurden:

Das Bestreben, konstruktive Ideen auszudrücken und zu formulieren, die zur Integration der verschiedenen Disziplinen mit traditionellen moralischen Werten und der demokratischen Lebensweise führen, wurde durch Einflüsse zunichte gemacht, die aus von unseren Bibliotheken und Labors weit entfernten Quellen stammen. Seit über zwei Jahrzehnten wird die öffentliche Meinung der starken Propaganda einiger weniger artikulierter Gegner unserer demokratischen Institutionen ausgesetzt. Ihr Einfluss wurde durch die Gemütsverfassung der breiten Leserschaft und durch die Zahl der Schriftsteller und Gelehrten verstärkt, deren selbstzerstörerische Skepsis den Totalitären direkt in die Hände gespielt hat. Alle Bemühungen, die enge Verbindung der modernen Wissenschaft und Geschichte mit der traditionellen Ethik und Religion aufzuzeigen, wurden als reaktionär angeprangert.[58]

Die Idee, „eine Einheit im Denken und Handeln [...] zu verwirklichen, um eine sicherere Grundlage für die Demokratie zu schaffen", kommt einer offenen Debatte in einem geschlossenen Zirkel gleich, weil der Begriff Demokratie dem American Way of Life gleichgesetzt wurde. Auch wenn man den Einfluss der Konferenz nicht

58 Louis Finkelstein, „The Aims of the Conference", Science, Philosophy and Religion, A Symposium. Conference on Science, Philosophy and Religion, New York: 1941, 12

überschätzen sollte und auch wenn direkte Hinweise auf wirtschaftliche Aspekte fehlen: Es versinnbildlicht, dass der Nährboden für die Ausprägung einer unsichtbaren Hand geschaffen wurde, die wiederum eine selbstregulierende Einheit steuert.

Es sollte Margaret Mead sein, die 1968 hierfür den Begriff der Kybernetik zweiter Ordnung schuf. Verwendet wurde der Begriff anschließend von ihrem Weggenossen Heinz von Foerster, der während seiner späten Schaffungsphase in den 1980er-Jahren – als der Neoliberalismus auf dem Nährboden technokratischer Selbstregulierungsprinzipien seine wilden Blüten trieb – bestrebt war, das Handeln von Managern mit seinem kybernetischen Jargon zu verklären.

Heinz von Foerster, ein Sinnbild des technokratischen Chamäleons: Im Zweiten Weltkrieg war er in die Radarentwicklung der Nazis eingebunden, um dann die politische Flagge zu wechseln und nach Amerika zu segeln. Bis Ende der 1960er-Jahre wickelte er Forschungsaufträge der amerikanischen Armee ab, um anschließend die Militärkritiker und Counterculturalisten in ihren Forderungen nach mehr Selbstregulierung zu unterstützen. Zu guter Letzt beriet er Managerschulen. Zeitgleich wie Heinz von Foerster mit den kybernetischen Prinzipien hausieren ging, speiste Margaret Mead auf leise Weise ihr anthropologisches Wissen, das sie sich auf zahlreichen Fernreisen angeeignet hatte, in die koloniale Logik des CIA ein.

MARGARET MEAD: DEMUT VOR DEN KULTURKRÄFTEN

Das oben genannte Symposium wurde 1941 erneut organisiert und Margaret Mead als Sprecherin eingeladen. In ihrem Beitrag ging sie der Frage nach, wie ihre anthropologische Position der Aufrechterhaltung jener Perspektive dienen könne, die die Konferenzteilnehmer zusammenbrachte, nämlich „diesen Glauben zu bekräftigen und zu versuchen, eine ganze Zivilisation in eine bestimmte Richtung zu führen". Mit dem zu bekräftigenden Glauben bezog sie sich auf den in Nordamerika einflussreichen Kulturrelativismus, in dem „jedes kulturelle Verhalten als relativ zu der Kultur zu betrachten ist, zu der es gehört". Ihre Betonung der „systematischen Wechselbeziehung verschiedener Kulturelemente" ist als Versuch zu verstehen, mit den in Gesellschaften vorhandenen Spannungen umzugehen, indem der Fokus von den inkompatiblen Zielen verschiedener Teile auf die problematische Beziehung verlagert wird, um schließlich die Kosten und Nutzen möglicher Entscheidungen abzuwägen. Das von Margaret Mead gewählte Beispiel – „die Frage der Zwangssterilisation der Untauglichen, um die Gemeinschaft vor den Kosten und der sozialen Verschwendung einer großen subnormalen Bevölkerung zu bewahren" – bewahrt uns davor anzunehmen, dass sie allzu aufgeschlossene und friedfertige Ansichten hatte. Dies zeigt sich insbesondere dann, wenn ihr Argument weiter unten dem Kommentar ihres Mannes Gregory Bateson gegenübergestellt wird.

Nach der Darstellung der Rolle der Anthropologin, "Kulturgegenstände in Relation zu setzen, unterschiedliche Gegenstände mit ganzen Systemen zu verknüpfen [...] sowie den Vergleich von einem System zum anderen zu nutzen, um Warnungen auszusprechen und auf die Auswirkungen verschiedener Veränderungen oder Trends innerhalb der chaotischen, heterogenen Kultur hinzuweisen, die die Konferenzteilnehmer versuchen, in Richtung von mehr Demokratie zu führen", zielte Mead auf den Hauptkonfliktpunkt:

Wenn wir aber die Frage einen Schritt weitertreiben und sagen: „Wir haben die Richtung festgelegt, in die wir uns bewegen wollen. Jetzt sagt uns, ihr Sozialwissenschaftler und Kulturspezialisten, wie wir dorthin kommen. Setzt unser spirituelles Programm für uns um!" Sind wir dann an einem Punkt angelangt, an dem die Willensfreiheit des Einzelnen und das wissenschaftliche Verfahren kollidieren? Erfordert die Umsetzung einer definierten Richtung nicht eine Kontrolle und wird diese Kontrolle – eine gemessene, berechnete und endgültige Kontrolle, also eine Kontrolle, die wirklich ihre Ziele erreicht – durch ihre bloße Existenz die Demokratie außer Kraft setzen, indem sie notwendigerweise einige Menschen auffordert, Kontrolle auszuüben, und alle anderen zu ihren Opfern degradiert?[59]

Mead wies anschließend darauf hin, dass die Umsetzung moralischer Verantwortung des Einzelnen komplizierter sei als die Durchsetzung von Gehorsam. Um dieses Ziel zu erreichen, hat der Wissenschaftler als Planer und Testamentsvollstrecker zuerst seine eigene Lage zu reflektieren. Sie seien Teil des Ganzen. Und weiter:

Kulturen haben keine wirkliche Existenz außerhalb der gewohnten Körper derjenigen, die sie leben. Hier liegt das Dilemma, das es zu lösen gilt [...]. Es bedeutet, dass die Umsetzung niemals in Form von fertigen Entwürfen der Zukunft erfolgen kann, sondern eine Richtung beinhalten muss, eine Ausrichtung der Kultur in eine Richtung, in der neue Individuen, die unter dem ersten Impuls dieser Richtung aufgewachsen sind, uns weiterbringen können und es auch werden.[60]

59 Margaret Mead, „The Comparative Study of Culture and the Purposive Cultivation of Democratic Values", in: Science, Philosophy and Religion, Second Symposium. Conference on Science, Philosophy and Religion, New York: 1942, 65f.
60 Mead, The Comparative Study, 66

Die Verlagerung des Fokus vom statischen Ergebnis hin auf dynamische Prozesse entsprach der von Mead angemerkten vermuteten Unmöglichkeit, „sich das Ende vor Augen zu führen, auf das hin der Wissenschaftler den Prozess in Gang setzt." Dies mindere aber seine Entschlossenheit nicht, „seine Hand auf einen Prozess der Kontrolle zu legen, die nicht minder sicher ist, aber an alles angepasst, was er über Kulturprozesse und die Eigenart seiner eigenen Kultur weiß." Nicht aus ethischen Gründen verwarf Mead den „fertigen Entwurf einer absolut wünschenswerten Lebensweise, der immer von der rücksichtslosen Manipulation des Menschen begleitet wurde, sich anzupassen". In Anbetracht der unausweichlichen Abhängigkeit der Kultur von ihrer Übertragung durch die Generationen erweise sich die direkte Manipulation als dysfunktional, da „die Opfer eines solchen Prozesses allmählich apathisch, passiv und ohne Spontaneität werden sowie die Anführer stetig paranoider."

Heute erkennen wir ihre Gedanken in unseren Realitäten wieder. Aber wie immer haben sich die Dinge doch etwas anders entwickelt. Was wir erleben, ist eine Herrschaftsform, die in ihrer Richtung und in ihrer Richtungsabhängigkeit fast unsichtbar ist, während die Regie noch immer mit den unverschämtesten Methoden der Manipulation durchgeführt wird, was genau die oben beschriebenen Effekte einer Verengung des Horizonts erzeugt. Vielleicht wird uns dies erst deutlich vor Augen geführt, seit die so genannten Soft Steering-Methoden tatsächlich ins Social Engineering integriert wurden.

Es scheint aber, als sei Mead damals nicht in ihrer vollen Konsequenz verstanden worden. Auch ihr Mann – derselbe Gregory Bateson, der später bekannt dafür werden sollte, die zyklischen Modelle der Kybernetik auf das Funktionieren von Verstand und Psyche umzumünzen, was wiederum Grundlage der selbstgesteuerten Therapie à la R.D. Laing bilden sollte – interpretierte den strategischen Schluss, den sie aus dem unvermeidlichen menschlichen Zustand zog, als Schwäche ihrer Überlegungen. Diese lassen sich in einem Dreischritt zusammenfassen: Erstens funktionieren Rückkopplungsschleifen über Generationen hinweg, was jegliche Planung erschwert. Daraus folgend kann zweitens der Einzelne, ganz unabhängig von seiner Entschlossenheit und seinem Einfluss, den Gesamtplan nie erfüllen. Dies setzt drittens in der Praxis nicht eine Manipulation des Einzelnen voraus, sondern die Manipulation der Bedingungen, die sein Potenzial zur Übereinstimmung mit dem Modell festlegen.

GREGORY BATESON: BEANTWORTUNG EINER NICHT GESTELLTEN FRAGE

In seinem Kommentar zu ihrem Konferenzpapier sprach Gregory Bateson, ebenfalls Anthropologe, den zu bearbeitenden Konflikt als einen zwischen demokratischen und instrumentellen Motiven an, als einen „Kampf um die Rolle, welche die Sozialwissenschaften bei der Ordnung der menschlichen Beziehungen spielen sollen". Nicht nur, dass dies die Einbindung der Wissenschaft in die Politik vorwegnahm, die das Zeitalter des Kalten Krieges tiefschürfend prägte. Es wirkt fast klischeehaft, dass er das Argument von Mead in einer Weise umdefiniert, die die von ihr entwickelten intergenerationellen Zeitaspekte komplett ignoriert. Daraus resultiert eine komplett andere Folgerung:

Sie sagt uns ganz klar, dass sie mit dieser Verschiebung der Betonung und Gestaltung unseres Denkens in unerforschte Gewässer eintreten wird. Wir können nicht wissen, welche Art von Menschen aus einem solchen Kurs resultiert, noch können wir sicher sein, dass wir uns selbst in der Welt von 1980 zu Hause fühlen werden. Dr. Mead kann uns nur sagen, dass wir mit Sicherheit auf einen Felsen treffen werden, wenn wir den Kurs fortsetzen, der uns am natürlichsten scheint, nämlich unsere sozialwissenschaftlichen Anwendungen als Mittel zur Erreichung eines definierten Ziels zu planen. Sie hat den Felsen für uns kartiert und rät uns, einen Kurs einzuschlagen, der nicht zum Felsen führt, sondern in eine neue, unbekannte Richtung. Ihr Beitrag wirft die Frage auf, wie wir diese neue Richtung einschlagen sollen.[61]

Während er den „verschiedene Arten der Erfassung von Verhaltensabläufen" folgt, stellt er diese wieder in den psychologischen Rahmen individuellen Lernens. Der Zeithorizont schrumpft auf eine Generation zusammen und auf die Frage, wie die jetzigen Kinder als Erwachsene auftreten sollen und was wir ihnen heute, Anfang der 1940er-Jahre, beibringen können. Es ist auffällig, dass seine Beispiele trotz erklärter Distanz zur Verhaltenstheorie des Behaviorismus immer noch stark an die Labors von Psychologen erinnern, die an Hunden und Tauben das Lernen studieren. Das Individuum wird zentriert, die Umgebung ignoriert. In seinem Setting wird die Idee von Mead reduziert, indem er sein Publikum implizit das Problem der kulturellen Einbindung vergessen lässt, das ihrem Vorschlag überhaupt erst zugrunde lag.

Er bezieht sich auf Mead, wenn er eine Diskrepanz zwischen Social Engineering als Manipulation des Menschen zur Erreichung einer geplanten Blaupausengesellschaft den Idealen der Demokratie als „höchsten Wert

61 Gregory Bateson, "Comments by" in: Science, Philosophy and Religion, Second Symposium. Conference on Science, Philosophy and Religion, New York: 1942, 86

und moralische Verantwortung des Einzelnen" gegenüberstellt. Nicht nur, dass diese scharfe Kontrastierung den Eindruck erweckt, dass Meads Beitrag überwiegend moralisch zu lesen sei: Bateson verändert die Funktion des Arguments. Während sie es im Sinne der Orientierung am Prozess statt am Ziel benutzt, bindet er das Social Engineering (ein Wort, dass sie übrigens nie benutzt hat) an die direkte Manipulation. Die ethischen Schwierigkeiten lösen sich dann irgendwie auf, wenn wir in die abstraktere Ebene der Wahrnehmung eintreten, oder so – denn das Recht auf Manipulation bleibt bei den „richtigen" Personen.

Sollen wir uns die Techniken und das Recht, Menschen zu manipulieren, als Privileg einiger weniger planungs-, zielorientierter und machthungriger Individuen vorbehalten, denen die Instrumentalität der Wissenschaft einen natürlichen Reiz verleiht? Werden wir jetzt, da wir die Techniken haben, die Menschen kaltblütig als Dinge behandeln? Oder was sollen wir mit diesen Techniken anfangen?[62]

Wenn er von Manipulation spricht, wählt er den Nationalsozialismus als Beispiel. Vor diesem Hintergrund steht die Idee Batesons, „die Gewohnheiten des Geistes" zu erfassen, um die Menschen vor Missbrauch zu bewahren. Es ist scheinbar besser, wenn Wissenschaftler die menschlichen Handlungen bewerten und steuern. Wer würde dann an der Notwendigkeit zweifeln, „etwas Besseres als eine zufällige Liste von Gewohnheiten zu bekommen?"

Dr. Mead sagt uns, wir sollen in noch unbekannte Gewässer segeln und eine neue Denkweise annehmen; aber wenn wir wüssten, wie diese Denkweise mit anderen zusammenhängt, könnten wir die Vorteile, Gefahren und möglichen Fallstricke eines solchen Kurses beurteilen. Ein solches Diagramm könnte uns die Antworten auf einige der Fragen geben, die Dr. Mead aufwirft – hinsichtlich der Frage, wie wir die Richtung und den Wert unserer geplanten Handlungen beurteilen sollen [...], könnten wir einige der grundlegenden Themen – die Himmelsrichtungen, wenn Sie so wollen – vorschlagen, auf denen die endgültige Klassifizierung aufgebaut werden muss.[63]

Ist der Vorschlag einer endgültigen Klassifizierung nicht genau das Gegenteil von dem, was Mead als möglich erachtete? Nach meiner Lesart zielte Bateson darauf ab, die eigentliche Grundlage ihres Arguments zu negieren, in dem er sagte, dass „die Erkenntnis, dass die Mitglieder dieser neuen Welt, von der wir träumen, sich so sehr von uns selbst unterscheiden, dass sie sie nicht mehr in dem Maße schätzen, wie wir sie jetzt wünschen." Zu Schluss schlug er vor, nicht mehr nur mehr über die Gewohnheiten herauszufinden, wie sie gelernt werden und in welchen Kulturen sie sich wie ausbilden. Vielmehr wählte er einen proaktiveren Ansatz:

Umgekehrt können wir vielleicht eine konkretere – operativere – Definition von Gewohnheiten wie der „Freiwilligkeit" bekommen, wenn wir uns fragen würden: „Welche Art von experimentellem Lernkontext würden wir entwickeln, um diese Gewohnheit zu vermitteln?" und „Wie könnten wir das Labyrinth oder die Problembox so manipulieren, damit die anthropomorphe Ratte einen wiederholten und verstärkten Eindruck von ihrem eigenen freien Willen erhält?"[64]

Was hier angekündigt wird, schlägt auf sich selbst zurück: Nachdem Mead die Frage aufgeworfen hatte, wie man mit dem schmalen Grat zwischen Wertepflege und Manipulation der Gesellschaft umgehen könne, wies Bateson ihre Analyse zurück und passte den Fokus auf den Prozess selbst an – um dann eine Karte des gewünschten Outputs zu erstellen mit dem Hinweis, wie dieser operativ anzusteuern sei.

EIN ERSTES RESÜMEE: DIE MASCHINE, DIE DER MASCHINE ALS IHR GEIST INNEWOHNT

Aus unserer gegenwärtigen Situation heraus neigen wir dazu, die technische Seite der Kybernetik zu überschätzen und die Roboterträume, die sich in Web-Realität verwandelten, als ihr Fundament zu deuten. Dabei gerät aus dem Blick, dass in der Phase, in der sie Gestalt annahm, Aspekte der Planbarkeit der zukünftigen Gesellschaft als ebenso wichtig eingestuft wurden. Anstatt hier also eine saubere akademische Analyse der Genealogie der Kybernetik anzubieten oder die Geschichte in ein Vor- und Post- zu teilen, und nur das Dazwischen als wesentlich zu erachten, wurden zwei Texte gewählt, um Methoden der Kybernetik zu verdeutlichen.

Eines ihrer Mittel ist der Versuch, gegenwärtige Bemühungen am Ziel auszurichten. Dieses hat sich inzwischen vollständig in die Strukturen eingefressen, nicht nur als Unternehmensberatung. Bekanntheit erlangte diese Methode durch die sogenannte Futurologie oder Zukunftsforschung. Sie wurde gegründet in Zeiten der Bedrohung durch den Atomkrieg als Strategie zur Rüstungskontrolle. Anschließend entwickelte sie sich schnell zum Forschungsinstrumentarium des Social Engineering weiter, um damit kapitalistische Krisen zu vermeiden. Zu diesem Zweck wurden einige Lehren aus der Hysterie des Kalten Krieges gezogen: So erklärten Louis Armand und Michel Drancourt bereits 1961, dass nach der zweiten Phase der industriellen Revolution, die

62 Bateson, Comments by, 84
63 Bateson, Comments by, 87
64 Bateson, Comments by, 92

eine Ära des Überflusses verspreche, Ideologien so obsolet werden würden, wie die wirtschaftlichen und politischen Strukturen ihrer Zeit.

Laut Herman Kahn, der wohl prägendsten und widerlichsten Figur der Futurologie, war Ziel der Zukunftsforschung die Erzeugung einer „widerspruchsfreien Projektion". Dies war für Jacques de Bourbon-Busset noch nicht ausreichend, er wollte „keine wahrscheinliche Zukunft vorhersagen, sondern eine wünschenswerte Zukunft vorbereiten und vielleicht sogar noch weiter gehen: sich bemühen, die wünschenswerte Zukunft wahrscheinlich zu machen". An dieser Stelle wird der von Bateson vorgeschlagene Fokus auf die praktische Anwendung im gemeinsamen Verständnis der Zukunftsforscher zur Realität. Es ist weder ihre Aufgabe, soziale Widersprüche zu erklären noch Lösungen vorzuschlagen, sondern zu zeigen, wie diese Probleme von den Ereignissen übernommen werden können. Es geht darum, wie Fakten überhaupt produziert und als solche ausgegeben werden können.

Die Vision, für die der Planungswissenschaftler Hasan Ozbekhan stellvertretend steht, war die Nutzung von Datenbanken, um zukünftige Situationen zu berechnen, d. h. eine „Antizipation zu konstruieren und rückwärts zu manipulieren, um zu sehen, ob die von der Antizipation angezeigte und gewählte Situation darauf hinweist, welche Veränderungen vorgenommen werden müssen, um die Antizipation zu erreichen." Dies mache die Zukunftsforschung zu einer „Planungsmethode, die die Zukunft als operatives Instrument nutzt, um Veränderungen in der Gegenwart zu bewirken – und durch solche Veränderungen die konzeptualisierte Zukunft in Bewegung zu setzen."

Zukunftsforscher waren oft Menschen mit guten Absichten, die Kriege weniger wahrscheinlich – oder zumindest weniger brutal – machen wollten. Sie glaubten, dass der Kapitalismus seinen Kurs ändert, sobald die Dynamik seiner Plünderung verstanden wird. Während die Absichten bald vergessen gingen, blieben die Logik und die Technologien übrig. Prognosen werden gemacht, um die Gegenwart zu gestalten.
Vielleicht konnten die Futurologen nicht vorhersehen, wie umfassend ihr Wertewandel werden würde. Als echte Zukunftsforscher lebten sie schon im toten Winkel, an dessen Entstehung sie mitgewirkt hatten: nicht zu erkennen, dass das „Ende der Ideologien" eine Unmöglichkeit für den Menschen ist. Das Ziel kann nicht abgeschafft, sondern nur vergessen werden, denn die Absenz von Werten ist auch ein Wert. Wenn die Maschine nicht von Menschen gesteuert wird, wird die Maschine selbst zur Richtung – und dies hat zur Folge, dass der Wunsch zu überleben einen kontraproduktiven Weg einschlägt. Meiner Meinung nach sollten wir uns, um einen interessanteren Weg zu finden, eine mehr als individuelle Perspektive einräumen – um nicht nur vereinzelt auf den schwarzen Spiegel zu starren, sondern ihn gemeinsam zu durchschreiten.

Die Kybernetik reduziert nicht nur die Welt auf ihr Modell, sie verschiebt bereits unsere Wahrnehmung, so dass der Unterschied zwischen Welt und Weltmodell sich zu erübrigen scheint. Wie Panther schieben wir uns vor Stäben hin und her, wissend, dass dahinter die Welt liegt. Wenn wir für mehr Autonomie kämpfen, ist jedoch die Unterscheidung von Welt und Modell grundsätzlich, denn ohne den Durst nach dem darüber Hinausgehenden, nach der Schönheit des Universums – ein Durst, der aus der plötzlichen Überraschung entspringt, zu erkennen, dass man inmitten einer ganzen Menge anderer Lebewesen am Leben ist – werden wir nicht in der Lage sein, den kleinen Schritt zur Seite zu machen, der notwendig ist, um herauszukommen und unsere Füße auf festen Boden zu stellen. Deshalb betrachte ich die Kybernetik als eine Ideologie der Verwirrung, oder noch schlimmer – als Ideologie des organisierten Vergessens. Nicht die Steuerung ist das Grundproblem, sondern unsere Furcht davor, den Horizont zu überschreiten und in unbekannte Zukünfte zu treten.

Verwendete Literatur:

- Van Wyck Brooks, "Conference on Science, Philosophy and Religion in Their Relation to the Democratic way of Life", in: Science, Philosophy and Religion, A Symposium. Conference on Science, Philosophy and Religion, New York: 1941
- Louis Finkelstein, "The Aims of the Conference", in: Science, Philosophy and Religion, A Symposium. Conference on Science, Philosophy and Religion, New York: 1941
- Margaret Mead, "The Comparative Study of Culture and the Purposive Cultivation of Democratic Values", in: Science, Philosophy and Religion, Second Symposium. Conference on Science, Philosophy and Religion, New York: 1942
- Gregory Bateson, Comments by. in: Science, Philosophy and Religion, Second Symposium. Conference on Science, Philosophy and Religion, New York: 1942
- Louis Armand et Michel Drancourt, Plaidoyer pour l'avenir, Paris: 1961
- Herman Kahn and Anthony J. Wiener. The Year 2000: a framework for peculation on the next thirty-three years, New York/London: 1967
- Jacques de Bourbon-Busset, „Réflexions sur l'attitude prospective", in: Prospective # 10, December 1962
- Hasan Ozbekhan, The Idea of a ‚Look-Out'-Institution, SDC-Paper SP 2017

KI zur Programmatischen Ungleichbehandlung

Entsolidarisierung durch Technokratischen Solutionismus

„Die Zukunft ist schon da – nur noch ungleich verteilt"
(William Gibson)

Die Corona-Pandemie verleiht den dunkelsten techno-totalitären Ideen der sogenannten *Solutionisten* (technologie-fixierte Problemlöser*innen) Flügel. „Solutionismus" sucht nach Lösungen über neue Technologien, die oftmals an den Problemen vorbeigehen. Das eigentliche Problem wird zum Teil nicht einmal ansatzweise gelöst[65]. Der Solutionismus steht vielmehr für die Vertauschung von Problem und Lösung: Statt ein Problem mit einer technischen Erfindung zu lösen, preist der Solutionist technische Erfindungen als Lösung für Probleme an, von denen man nicht weiß, nicht wissen will, oder verschleiern will, welcher Art und Komplexität sie sind.

Die Solutionist*in löst zu ihrer eigenen Legitimation als „Problemlöser*in" in der Regel technologisch fassbare, leichter zu lösende Ersatzprobleme, die sich die Technokrat*in gerne zunutze macht: Warum sollte eine Regierung zum Beispiel in den Wiederaufbau bröckelnder öffentlicher Verkehrssysteme investieren, wenn sie einfach große Daten nutzen kann, um personalisierte Anreize für Fahrgäste zu schaffen, die sie von Fahrten zu Spitzenzeiten abhalten? Lösungen auf der Angebotsseite, wie der Bau weiterer Verkehrslinien sind ziemlich teuer. Stattdessen wird nach Möglichkeiten gesucht, die Nachfrageseite (per KI und BigData) zu steuern indem sie den Einwohner*innen „helfen, das Konzept der besseren Reisezeit zu verstehen".

Wer nun immer noch George Orwells 1984 als Blaupause für den neueren Überwachungsstaat bemüht, unterschätzt den Solutionismus. Letzterer gibt vor, mit seinen „pragmatischen" Problemlösungsstrategien „post-ideologsch" zu sein. Tatsächlich ist die Radikalität, mit der Technokrat*innen den Solutionismus zum einzig „denkbaren" Ansatz für gesellschaftliche Probleme erheben, alles andere als unideologisch. Man muss die konsequente Art, lediglich digitale Pflaster auf die eklatantesten Wunden des krisenhaften Kapitalismus zu kleben, sehr wohl als Ideologie, – nämlich als Ideologie der Politik-Vermeidung – begreifen. Mit der machtvollen Neusetzung gesellschaftlicher Strukturen macht er seinerseits (eine andere) Politik. Technokrat*in und Solutionist*in versuchen alles, außer den Markt zu zerstören und zu revolutionieren. Die derzeitigen digitalen Plattformen sind Orte der Isolation und Individualisierung, nicht der gegenseitigen Hilfe und Solidarität.

Die Coronakrise scheint noch viel mehr (als die Klimakrise) dazu geeignet zu sein, das technokratische Instrumentarium als Standardoption für die „Lösung" sämtlicher existenzieller Probleme festzuschreiben. Darüber schrumpft (selbstverstärkend) die Vorstellungskraft, eine Welt jenseits der Technokratie auch nur zu erdenken. Insbesondere in Situationen existenzieller Angst verfangen unsere abstrakten Versprechen der politischen Emanzipation weit weniger, als das konkrete Versprechen einer App, die Leuten sagt, ob sie sich sicher fühlen dürfen und wie sie ihren Alltag noch sicherer machen können. Eine post-solutionistische Politik ist nach der Permanentisierung des *War on Terror* und dem nun voraussichtlich verstetigten *War on Virus* nicht in Sicht. Unterschiedliche Formen des Techno-Autoritarismus machen derzeit das Rennen.

Unser Beitrag soll zeigen, dass insbesondere die auf künstlicher Intelligenz basierenden Lösungsansätze des Solutionismus auf Ungleichbehandlung setzen. Die Entsolidarisierung ist dabei nicht nur ein Nebeneffekt, sondern Programm.

65 Siehe dazu den Text „Öko-Technokratie" hier in dieser Broschüre.

KURZE VORBEMERKUNG ZU ALGORITHMEN

Der klassische Algorithmus

Den klassischen Algorithmus können wir vereinfacht als Abfolge von *Wenn-Dann*-Beziehungen verstehen. Schon in dieser mathematisch formalisierten Beschreibung ist kein Platz mehr für Ambivalenz, übergeordnete Kontextabhängigkeit oder Skeptizismus – ganz unabhängig von der Übersetzung des Algorithmus in ein ausführbares Computerprogramm.

Ein Beispiel: Ein befreundeter Krankenpfleger hat uns davon berichtet, wie sich sein Arbeitsalltag durch die Einführung einer digitalen Zeiterfassung verändert hat. Per App auf seinem Dienst-Tablet wird seit letztem Jahr seine Ankunfts- und Abfahrtszeit bei jeder Patient*in erfasst – einfach durch Anklicken auf deren Namen im Tages-Dienstplan. Daraus wird die Pünktlichkeit, seine Arbeitsleistung im statistischen Vergleich mit anderen Kolleg*innen vermessen und das für bestimmte Pflegetätigkeiten zugestandene, mittlere Zeitkontingent neudefiniert. Ein banales Programm, ganz ohne künstliche Intelligenz. Die Auswirkungen gegenüber der alten, analogen Zeiterfassung sind jedoch gravierend. Ein nachträgliches Ausgleichen unterschiedlich zeitaufwändiger Patient*innen auf dem Zettel ist nicht mehr möglich. Wenn das Waschen und Anziehen von Patient*in A schneller ging als vorgesehen, kann dieser Zeitgewinn nicht mehr für ein aufbauendes Gespräch mit der darauf folgenden Patient*in B genutzt werden. „Schieben" geht nicht mehr – ein Abschließen des Pflegeauftrags für Patientin A muss vor Abreise in Richtung Patientin B erfolgen.

Allein die Feinvermessung der Arbeitsabläufe mündet so in eine Enteignung der Arbeitstätigkeit zugunsten einer Effizienzsteigerung – nichts Neues, sondern lediglich die digitalisierte Version der Fließbandidee. Amazon treibt das Monitoring und den Echtzeit-Performance-Vergleich seiner Mitarbeiter*innen in einem nicht-einsehbaren Ranking besonders weit. Die Intransparenz der Rangliste sorgt dafür, dass die Mitarbeiter*innen die Optimierung ihrer Selbst verinnerlichen, aus Angst, unter dem (ihren Arbeitsplatz gefährdenden) Leistungsdurchschnitt zu liegen.[66]

Statistik auf grossen Datenmengen

Unter bestimmten Bedingungen lässt sich die *Wenn-Dann*-Beziehung des klassischen Algorithmus umkehren: Dies ermöglicht dann die Berechnung der zu einer erwünschten *Dann*-Folge notwendigen *Wenn*-Basis. Bei komplexeren Problemen menschlichen Verhaltens reißt dieser Umkehrfaden jedoch schnell ab – zu viele mögliche Parameter machen die *Dann-Wenn*-Umkehrung (für den Einzelfall) uneindeutig.

Sammelt man hingegen sehr viele Verhaltens-Daten und lassen sich mehrere unterschiedliche Datenbanken verknüpfen, werden unerwünschte *Dann*-Folgen mit hoher Genauigkeit vorhersehbar und ermöglichen ein lenkendes Eingreifen in die *Wenn*-Basis. So lässt sich zumindest im statistischen Mittel bestimmtes Verhalten unterdrücken und anderes fördern.

Künstliche Intelligenz (KI)

Eine derzeit für das Lösen von Optimierungsaufgaben besonders vielversprechende Klasse *künstlich intelligenter Algorithmen* sind sogenannte „selbst-lernende neuronale Netze". Diese Algorithmen „lernen" auf der Basis von Trainingsdaten und passen „selbständig" ihre Muster (die Lösungsstrategie) dem zu lösenden Problem an. Mit jedem neuen Datensatz, auf den das zugehörige Programm angewendet wird, verändert es sich. Auch hier ein Beispiel: Amazons selbstlernende Rekrutierungssoftware versuchte auf der Basis von 5000 bereits bewerteten Bewerbungsmappen zu „lernen", welche Muster in den Bewerber*innen-Daten zu einer positiven Bewertung geführt haben können. Die Gewichtung z. B. der Abschlussnoten im Vergleich zur bereits gemachten Arbeitserfahrung und anderer Parameter für das Endergebnis der Bewertung verändert sich mit jeder weiteren Anwendung des Programms auf neue Bewerbungsunterlagen.

Die Veränderung des „selbst-lernenden" Programms hat den schwerwiegenden Effekt, dass das Bewertungsergebnis des Programms in Anwendung auf eine einzelne Bewerbungsmappe nicht vorhersagbar ist. Die (veränderliche) Gewichtungen der Bewertungskriterien, sind für den Betrachter intransparent – sie sind sogar für die Programmierer*in nicht mehr nachvollziehbar und damit auch nicht korrigierbar! Wir werden auf die Nichtnachvollziehbarkeit dieser Wenn-Dann-Beziehung als kritische Eigenschaft zurückkommen.

Im konkreten Fall von Amazons Rekrutierungs-Software, stellte sich heraus, dass das Programm nach der Trainingsphase das Muster „männlich" für besonders erfolgversprechend hielt und fortan weibliche Bewerberinnen im Bewerbungsprozess ausnahmslos benachteiligte. Amazon musste die Software ausmustern. Ein nachträgliches Justieren der Programmparameter war nicht möglich.

66 https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations

DISKRIMINIERENDE ALGORITHMEN

Künstliche Intelligenz, automatisierte oder datengesteuerte Entscheidungssysteme, algorithmische Entscheidungsfindung, aber auch die Zusammenführung großer Datensätze mit persönlichen und biometrischen Informationen werden zunehmend in Bereichen (des öffentlichen Lebens) eingesetzt, die sich inhärent stärker auf marginalisierte Gruppen und People of Colour auswirken. Wir erleben dieses Kategorisieren und Experimentieren an marginalisierten Gemeinschaften bei der Polizeiarbeit, unter dem Vorwand der Terrorismusbekämpfung und der Migrationskontrolle.[67] So trifft es vor allem rassifizierte Menschen und Migrant*innen (ohne Papiere) aber auch queere Communities und Menschen mit Behinderungen.

Gesichtserkennung

Rassistische Gesichtserkennung ist vielerorts üblich. Ein Beispiel rassistischer Gesichtserkennung ist das Überwachungssystem in der Region Xinjiang in China.[68] Es ist das erste bekannte Beispiel, in dem eine Regierung mit Absicht künstliche Intelligenz für Racial Profiling nutzt und dafür medial Aufmerksamkeit erhält.

Gesichtserkennungssysteme in zahlreichen Städten Chinas sind darauf ausgerichtet, Mitglieder der Minderheit der Uiguren automatisch zu erkennen und zu tracken. Seit 2017 ist bekannt, dass die Chinesche Regierung die biometrischen Daten[69] aller Uiguren zwischen 12 und 65 Jahren erfassen ließ. Die New York Times berichtete unter Berufung auf Dokumente, Datenbanken und Interviews, dass in nur einem Monat 500.000 Uigur*innen mittels Gesichtserkennung erfasst und getrackt worden seien.

Hikvision, der weltgrößte Hersteller von Überwachungskameras, hat auf seiner chinesischen Webseite eine Überwachungskamera vermarktet, die automatisch Angehörige der ethnischen Minderheit der Uigur*innen erkennen soll. In der Produktbeschreibung[70] hieß es, dass die Kamera Geschlecht (männlich, weiblich), ethnische Zugehörigkeit (z. B. Uiguren, Han) und Hautfarbe (z. B. weiß, gelb oder schwarz) analysieren könne.

Ein anderes Beispiel ist die Gesichtserkennungstechnologie des in Moskau ansässige Unternehmens NtechLab.[71] Das Unternehmen bewarb die von ihm verkaufte Gesichtserkennungstechnologie mit einem Algorithmus zur „Ethnizitätserkennung" zur Klassifizierung von Menschen in die Kategorien „europäisch", „afrikanisch" und „arabisch".

Auch Amazon hat ein leistungsfähiges und gefährliches neues Bilderkennungssystem entwickelt. Es wird von US-Behörden eingesetzt.[72] Amazon nennt den Dienst „Rekognition". Mit der KI können Objekte, Personen, Text, Szenen und Aktivitäten in Bildern und Videos identifiziert werden. Es bietet aber auch Gesichtsanalyse- und Gesichtssuchfunktionen, mit denen Gesichter für eine Vielzahl von Benutzerverifikationen, Personenzählungen und Anwendungsfällen der Behörden erkannt, analysiert und verglichen werden können. Rekognition kann Personen in Echtzeit identifizieren, verfolgen und analysieren sowie bis zu 100 Personen auf einem einzigen Bild erkennen. Die gesammelten Informationen werden mit Datenbanken abgeglichen, die mehrere Millionen von Gesichtern enthalten.

Hier zeigt sich ein rassistischer Bias. In einem Experiment der American Civil Liberties Union (ALCU)[73] identifizierte Amamzons Software fälschlicherweise 28 Kongressmitglieder als andere Personen, die wegen eines Verbrechens verhaftet worden waren. Die falschen Übereinstimmungen betrafen unverhältnismäßig viele Farbige.

Aber nicht nur Amazons KI hat einen rassistischen Bias. Im Jahr 2015 brachte ein schwarzer Softwareentwickler Google schlechte PR, indem er twitterte, dass der Dienst ‚Google Photos' Fotos von ihm mit einem schwarzen Freund als „Gorillas" bezeichnet hatte.[74] Google erklär-

67 Patrick Williams und Eric Kind. Data-driven Policing: The hardwiring of discriminatory policing practices across europe. 2019 https://www.enar-eu.org/IMG/pdf/data-driven-profiling-web-final.pdf

68 Markus Reuter. Gesichtserkennung: Automatisierter Rassismus gegen uigurische Minderheit in China. 15.04.2019 https://netzpolitik.org/2019/gesichtserkennung-automatisierter-rassismus-gegen-uigurische-minderheit-in-china/

69 Dazu gehörten die Blutgruppe, Fotos des Gesichtes, ein Iris-Scan, Fingerabdrücke und die DNA.

70 Produktbeschreibung der Hikvision-Kamera: https://web.archive.org/web/20191107042500/http://www1.hikvision.com/cn/prgs.aspx?c_kind=2&c_kind2=2&c_kind3=445&c_kind4=446&id=42808

71 Dave Gershgorn. This startup's racial-profiling algorithm shows AI can be dangerous way before any robot apocalypse. 23.05.2018 https://qz.com/1286533/a-startup-selling-racial-profiling-software-shows-how-ai-can-be-dangerous-way-before-any-robot-apocalypse/

72 Matt Cagle und Nicole Ozer. Amazon Teams Up With Government to Deploy Dangerous New Facial Recognition Technology, aclu.org, 22.05.2018 https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazon-teams-government-deploy-dangerous-new

73 Jacob Snow: Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots, aclu.org, 26.07.2018, Thoughts On Machine Learning Accuracy, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28

74 Tom Simonite: When It Comes to Gorillas, Google Photos Remains Blind, wired.com, 01.11.2018 https://www.wired.com/story/

te sich selbst „entsetzt und aufrichtig traurig“ und versprach eine Lösung. Eine dieser Korrekturen war das Löschen von Gorillas und einigen anderen Primaten aus dem Lexikon des Dienstes.

Auch Microsoft räumte in der Vergangenheit einen Bias bei einigen Gesichtserkennungstechnologien ein. Dort sind höhere Fehlerquoten bei der Bestimmung des Geschlechts von Frauen und farbigen Personen aufgetreten.[75]

Sexismus und Rassismus in Sprache

Statistische Methoden und KI haben sich in den Bereichen Spracherkennung und -verarbeitung durchgesetzt. Der Ansatz, der bereits in der Websuche und der maschinellen Übersetzung verwendet wird, funktioniert durch den Aufbau einer mathematischen Repräsentation der Sprache, bei der die Bedeutung eines Wortes in eine Reihe von Zahlen (bekannt als Wortvektor) destilliert wird, auf deren Grundlage andere Wörter am häufigsten neben dem Wort erscheinen. Es mag überraschen, dass dieser rein statistische Ansatz den reichen kulturellen und sozialen Kontext der Bedeutung eines Wortes in einer Weise zu erfassen scheint, wie es eine Wörterbuchdefinition nicht vermag.

Allerdings zeigt sich oft ein sexistischer und rassistischer Bias.[76] Die Wörter „weiblich“ und „Frau“ wurden enger mit Kunst, geisteswissenschaftlichen Berufen und mit dem Haushalt in Verbindung gebracht, während „männlich“ und „Mann“ eher den Berufen in Mathematik und Ingenieurwesen entsprachen. Des Weiteren verband das KI-System europäisch-amerikanische Namen eher mit angenehmen Wörtern wie „Geschenk“ oder „glücklich“, während afroamerikanische Namen eher mit unangenehmen Wörtern assoziiert wurden.

Das in der Studie verwendete maschinelle Lernwerkzeug wurde auf einem Datensatz trainiert, der als „Common Crawl“-Korpus bekannt ist – eine Liste von 840 Milliarden Wörtern, die so entnommen wurden, wie sie aus online veröffentlichtem Material erscheinen. Ähnliche Ergebnisse wurden gefunden, als die gleichen Tools auf Daten von Google News trainiert wurden.

Predictive Policing

Predictive Policing beschreibt im Wesentlichen die Verwendung von Daten zur Vorhersage, wo Verbrechen geschehen werden, und die Zuweisung von Strafverfolgungsressourcen in diese Bereiche. Weltweit werden in vielen Polizeibehörden personenbezogene, vorhersagende Polizeisysteme (Predictive-Policing-Software) erprobt und implementiert. Diese versuchen auf Basis vorhandener Daten Aussagen darüber zu treffen, welche Personen statistisch gesehen am wahrscheinlichsten ein Verbrechen begehen werden.

Predictive Policing richtet sich gegen die „Kriminalität“ der Unterschichten. Steuerflucht, millionenschwerer Betrug und Geldwäsche im großen Stil zählen nicht zu den Anwendungsgebieten. Es ist bekannt, dass diese Systeme selbstverstärkend sind und die rassistische und klassistische Polizeipraxis widerspiegeln.

Besonders diskriminierende Beispiele hierfür sind die Gangs Matrix[77] in Großbritannien oder die Top 600 und Top 400 Listen[78] in den Niederlanden. Im Fall der Niederlande wird versucht vorherzusagen, mit welcher Wahrscheinlichkeit bestimmte Kinder unter 12 Jahren zukünftige Kriminelle werden. Diskriminiert werden überwiegend dunkelhäutige Männer und Jungen.

Andere Systeme sind nicht personen-, sondern ortsbasiert. Sie versprechen auf Grundlage verschiedener Datensätze einschließlich sozioökonomischer Daten und Kriminalitätstatistiken zukünftige Kriminalitätsraten in bestimmten Gebieten zu bestimmen. Solche Vorhersagen sind nicht nur in Hinblick auf die rechtlich geltende Unschuldsvermutung problematisch. Sie treffen auch, ebenso wie viele Vorverurteilungen und Verdächtigungen, primär dunkelhäutiger Menschen in ökonomisch marginalisierten Vierteln. Deshalb handelt es sich eigentlich um eine Kodierung.

Risikobewertungen im Rechtssystem

Risikobewertungen anhand von Scoring, also der Vorhersage der Wahrscheinlichkeit, dass die Person ein zukünftiges Verbrechen begeht, sind in Gerichtssälen in den USA immer häufiger anzutreffen. Sie werden unterschiedlich verwendet. Beispielsweise bei der Zuweisung von Kautionsbeträgen. In einigen Staaten „helfen“ diese Algorithmen bei Entscheidungen wie Freilassung, Verurteilung und Bewährung.

---

when-it-comes-to-gorillas-google-photos-remains-blind/

75 Brad Smith: Facial recognition: It's time for action, blogs.microsoft.com, 06.12.2018 https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/

76 Hannah Devlin 13.4.2017, AI Problems exhibit racial and gender biases, research shows. https://www.theguardian.com/technology/2017/apr/13/ai-programs-exhibit-racist-and-sexist-biases-research-reveals

77 https://www.libertyhumanrights.org.uk/tags/gang-matrix

78 https://datajusticeproject.net/wp-content/uploads/sites/30/2019/05/Report-Data-Driven-Policing-EU.pdf

Auch diese Systeme zeigten einen rassistischen Bias.[79] Das Programm, Correctional Offender Management Profiling for Alternative Sanctions (Compas), neigte dazu, schwarze Angeklagte fälschlicherweise als rückfallgefährdet einzustufen. Laut der investigativen Journalistenorganisation ProPublica wurden sie fast doppelt so häufig wie Weiße (45 % bis 24 %) markiert.

Finanzierung und Kreditvergabe

Ein weiterer Bereich ist die maschinelle Verzerrung bei der Finanzierung und Kreditvergabe. Die Algorithmen, die die Versicherungsprämien bestimmen, sind sexistisch und rassistisch voreingenommen, ebenso wie die Systeme, die für Kreditvergabedienste werben. Wohnungsanbieter und Banken wenden algorithmische Tools an, um herauszufinden, wer einen Job oder ein Haus oder eine Hypothek oder ein Darlehen zu welchem Zinssatz erhält.

DATENRASSISMUS

Die oben genannten Beispiele haben viele Gemeinsamkeiten. Es sind vielfältige Systeme und Technologien, die in den verschiedensten Bereichen eingesetzt werden, die entweder primär auf Migrant*innen und People of Colour abzielen oder diese unverhältnismäßig stark beeinträchtigen. Diese Unverhältnismäßigkeit muss im breiteren Kontext von strukturellem Rassismus gesehen werden. Es repräsentiert die Realität bestehender historischer Ungerechtigkeiten, anhaltender Ungleichheiten in den Bereichen Wohnen, Gesundheit, Beschäftigung und Bildung, die entlang der Achsen von race und Ethnizität verlaufen sowie, zuletzt, wiederholte Erfahrungen mit staatlicher Gewalt und Straflosigkeit.[80]

Es ist nicht neu, dass Systeme verwendet werden, um Individuen zu kategorisieren und zu überwachen und der Diskriminierung so eine Logik zu geben. Neu ist jedoch der Diskurs der Neutralität, die „Kombination aus kodierter Voreingenommenheit und imaginärer Objektivität", das der Diskriminierung durch Technologie entgegengebracht wird[81]. Die Verwendung „objektiver" wissenschaftlicher Methoden zur Kategorisierung und „Risikobewertung" von Einzelpersonen und Gemeinschaften zum Zwecke der Ausgrenzung hat bislang wenig Aufmerksamkeit erhalten. Das liegt auch an der simplen, aber oft erfolgreichen Argumentation, dass Technologien „nicht im klassischen Sinne rassistisch" sein können, da „der Computer keine Seele hat und somit nicht den menschlichen Fehler haben kann, Personen nach ihrer Hautfarbe zu klassifizieren"[82].

Nicht nur der Bias der Daten ist ein Problem, sondern auch der Blick der Technokrat*innen und Solutionist*innen. Der Techsektor und die Informatiker*innen bauen ihre Weltsicht (einschließlich ihrer Vorurteile) zwangsläufig und (un)bewusst in die Modelle ein, die sie konstruieren. 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.

Im Folgenden soll es darum gehen, wie eine KI-basierte Diskriminierung nicht mehr nur entlang vermeintlicher Gruppenmerkmale, sondern bis zur Ebene einzeln unterscheidbarer Individuen erfolgt.

KATEGORISIERUNG OHNE KATEGORIEN

KI-Programme werden mittlerweile standardmäßig zur Verhaltenslenkung eingesetzt. Überall verstecken sich mehr oder weniger aufwändig programmierte künstlich intelligente Assistenten – in jeder Spracherkennungssoftware beispielsweise oder bei der individuellen Profilerstellung bei Datensammeldiensten wie Google, facebook, Palantir oder Amplitude. Wer erhält welche Bonusmöglichkeiten beim (Online-)Einkauf? Hoch individualisiert und nicht nachvollziehbar! Doch dabei bleibt es nicht: Social-Scoring-Systeme werden auch außerhalb von China immer populärer. Verschiedene Wohn-, Job-, Kredit- oder Mobilitätsangebote gelten nur für Teilnehmer*innen mit genügend hohem „Score" (= erworbene Punkte durch belohnenswertes Verhalten). Das bedeutet, dass nicht nur preisliche Vergünstigungen hoch individualisiert vergeben werden, sondern soziale Teilhabemöglichkeiten.

Die künstlich intelligente Lenkung von Lebensprozessen erfordert ihre möglichst detaillierte *Erfassung* und anschließende *Bewertung*. Die KI in Kombination mit Big Data-Methoden ermöglicht dabei eine dynamische! Verhaltenslenkung: Erfassung und Bewertung erfolgen nicht mehr nach statischen Kategorien – das Ablagesystem ist in Ausprägung und Anzahl der „Schubladen" variabel. Eine Schufa, die eine Einstufung der Kreditwürdigkeit mit feststehender Gewichtung einmal benannter

79 Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner. Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks. 23.05.2016 https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

80 Sarah Chander. Datenrassismus - Eine neue Ära. 29.02.2020 https://netzpolitik.org/2020/eine-neue-aera/

81 Benjamin, R. (2019). Race After Technology: Abolitionist tools for the New Jim Code. Polity.

82 Ebd.

Kriterien erlaubt, wäre ein hoffnungslos veraltetes finanzpolitisches Instrument.

Wer hat Zugang zu welchem Gebäude oder gar Stadtteil? Dies *generell* per KI zu regulieren erscheint uns heute (noch!) als eine dystopische Übertreibung[83]. Die Idee einer App-gesteuerten Lockerung der Kontaktbeschränkungen nach dem Lockdown in der Cornakrise macht jedoch genau das: die Vermessung der individuellen Ansteckungsgefährdung für andere per Tracing (Corona-App) oder per „Immunitätsnachweis" soll in unterschiedliche Bewegungsfreiheit münden.

Ist es in ordnungspolitischer Denkweise nicht konsequent, generell die Kategorie „Gefährder" entlang unterschiedlicher Risiken weiter zu differenzieren und gemäß „Gefährdergrad" unterschiedliche Einschränkungen zu verordnen? Bei sehr vielen Gefährdungsstufen landen wir ebenfalls beim Scoring. Denn es ist unerheblich, ob mensch hoch differenzierte Einschränkungen per Malus verhängt oder in der Umkehrung soziale Teilhabechancen per Bonus diversifiziert.
Es entsteht kein grobes Schubladensystem einzelner Klassen, sondern eine feinstkörnige Individualisierung. Feinstkörnig in dem Sinn, dass die Differenzierung entlang so vieler Parameter durchgeführt wird, dass sie vollständig ist. Eine weitere Unterscheidung über noch mehr Parameter verändert die „Körnigkeit" nicht weiter, sondern macht es lediglich noch unwahrscheinlicher, dass zwei Menschen in derselben „Kategorie" landen, also exakt gleiche Teilhabemöglichkeiten (= gleiche Punktezahl) zugewiesen bekommen.

Der Begriff der Kategorie ergibt dann keinen Sinn mehr. Auch der Begriff der *Klasse* verliert seine Aussagekraft. Armut (im Sinne beschränkter gesellschaftlicher Partizipationsmöglichkeiten) kann in einer per Score und Ranking verfassten Gesellschaft nicht mehr durch eine eindimensionale Bewertung von (lohn-abhängiger) Arbeit definiert werden. Stattdessen führt die Erfassung von tausenden Mustern von Verhalten, Kontakten, Einstellungen und Wünschen auch jenseits der Lohnarbeit zu einem niedrigen Score – das ist neue „klassenlose" Armut, so wie in vielen Metropolen Chinas bereits lebensbestimmende Realität.

PROGRAMMATISCHE UNGLEICHBEHANDLUNG

Die „Individuierung" per Score wird von Solutionist*innen vorangetrieben und so findet sie entlang kapitalistisch motivierter (und motivierender) Bewertungskriterien statt. Sie ordnet aber nicht nur den Markt neu, sondern auch die politische Administration. Wir werden daran gewöhnt, dass regelnde Verordnungen nicht mehr *gleich* für alle lauten. Das bisherige Steuersystem z. B. ist so verfasst, dass sich Steuerklassen und der letztendliche Steuerbetrag einer Person über einen simplen klassischen Algorithmus berechnen lassen – also eine einfache Abfolge von Wenn-Dann-Beziehungen. In einer feinstkörnigen Scoring-Gesellschaft hingegen gelten für jede*n andere Regeln. Es gibt keine Steuerklassen. Stattdessen erhält jede*r individuelle Verhaltensempfehlungen von einem KI-basierten digitalen Assistenten. Diese Handlungsempfehlungen umzusetzen oder zu ignorieren wird mit Bonus- oder Malus-Punkten belohnt oder sanktioniert. Das ergibt maximale Individuierung in dem Sinne, dass niemandes Situation mit der eines anderen vergleichbar ist. Die Bedingungen Punkte zu sammeln sind nicht vergleichbar. Das befördert maximale Entsolidarisierung. Ein kollektives Aufbegehren wird erschwert. Gruppen von (vergleichbar) Betroffenen lassen sich nur aufwändig bilden, obwohl durchaus eine Vergleichbarkeit der Lebensrealitäten existiert.

Gesellschaftliche Gerechtigkeitsvorstellungen basieren auf Vergleichbarkeit und suchen Ungleichheiten perspektivisch abzuschaffen. Wer will Ungleichbehandlung beklagen oder gar skandalisieren, wenn sie programmatisch, ja sogar konstitutiv für das System ist?

INTRANSPARENZ ALS BASIS FÜR SELBSTOPTIMIERUNG

Ein zweites, wesentliches Merkmal KI-basierter Scoring-Systeme zur Verhaltenslenkung ist die *Undurchsichtigkeit der Erfassungs- und Bewertungskriterien.*

Die Kategorien, gemäß derer Verhalten erfasst werden und deren Einfluss auf die Gesamtbewertung, bleiben bewusst (z. B. Schufa-)Geheimnis. Mehr noch, die Muster nach denen sich besonders effizient Verhalten unterscheiden lässt, verändern sich im Rahmen einer selbstlernenden KI. Je mehr Daten ins System eingespeist werden, desto besser findet die KI eine Unterscheidung gemäß ihrer Lernvorgaben „wesentlicher" Verhaltensmerkmale. Die zu bewertenden Individuen können diese *dynamische Kategorisierung* gar nicht kennen. Sie können lediglich erahnen und spielerisch (Gamification) erforschen, welches Verhalten ihre Punktezahl (aktuell!) wie stark beeinflusst. Eine optimale Voraussetzung dafür, sich in Unkenntnis der Bewertungsmodalitäten in der Hoffnung auf einen besseren Score umfassend selbst zu optimieren. Denn das Scoring-System ist über ein (nicht einsehbares) Ranking konkurrenzbasiert.

83 Für einige Orte ist dies schon Realität und das nicht nur in China. Wenn lokale US-Polizeibehörden ihre Datenbanken vernetzen und Personengruppen aus Gebieten fernhalten, wenn ganze sogenannte *gated communities* sich abschotten und Zutritt nur per *Amazon Ring* gestatten.

Die Situation ist noch komplexer: Selbst die Informatiker*innen, die das Bewertungsprogramm entwickelt haben, können nur zu Beginn eine Aussage darüber treffen, welches Verhalten zu welchem Score in der KI-Bewertung führt. Nach (selbstlernender) Weiterentwicklung des Programms, verändern sich die relevanten Muster und ihrer Gewichtung für den Score. Die Informatiker*in kennt dann die „Gewichte" ihrer eigenen Individuierungs-Software nicht mehr. Diese Unkenntnis ist nicht Ausdruck ihrer Unfähigkeit, sondern systemisch bedingt und ist eher als ein Maß für die Effektivität einer KI-basierten Optimierung, ohne starke Vorgaben zu verstehen.

Diese Freiheit der KI ist Vorzug und Makel zugleich. Selbstlernende neuronale Netze arbeiten besonders gut, wenn diese ihre Optimierungsmuster so „frei" wie möglich selbst entwickeln können. Sprachübersetzungsprogramme z. B. haben sich wie oben bereits erwähnt als besonders gut herausgestellt, wenn sie ohne Kenntnis der Grammatik der beteiligten Sprachen eigenständig Muster für eine passende Übersetzung suchen. Der Nachteil: Wir verstehen nicht, wie das Programm zu seiner Entscheidung (ein Wort so, oder anders zu übersetzen) kommt; mit dem Nebeneffekt: wir lernen auch nichts aus der Vielzahl eingespeister Texte und ihrer Übersetzung. Hier wird kein gesellschaftlich extrahierbares, sondern hoch proprietäres Wissen erzeugt, das nur innerhalb dieser spezifischen KI genutzt werden kann.

Die Details des künstlich intelligenten Scorings[84] entziehen sich menschlicher Nachvollziehbarkeit.

KÜNSTLICH INTELLIGENTE „ENTSCHEIDUNGSHILFE"

Nicht zu wissen, wie die KI zu ihrer Bewertung kommt, ist ein ernstzunehmendes generelles Problem – nicht nur hinsichtlich der Akzeptanz der Bevölkerung für die Einführung KI-basierter Assistenz in immer mehr Lebensbereichen. Wenn z. B. eine solche selbstlernende KI die Gerichte entlasten und eigenständig (nach einem Training mit tausenden ähnlich gelagerten Fällen) Entscheidungen treffen soll, dann genügen die so gefällten Urteile in den meisten Justizsystemen einer zentralen juristischen Forderung nicht: Das Urteil schuldig oder nicht, muss für die Prozessbeteiligten nachvollziehbar sein. Das Gericht muss deutlich machen, wie es zu seiner Entscheidung gekommen ist. Auch in anderen Bereichen, wie z. B. in der Medizin, gibt es ein breites Unbehagen, einer Technologie zu vertrauen, die sich nicht einmal ansatzweise vermitteln kann.

Die Technokratie behilft sich derzeit mit dem Konstrukt *KI-basierter „Entscheidungshilfe"*. Die letztendliche Entscheidung „relevanter" Fragestellungen solle beim Mensch (Richter*in / Ärzt*in) verbleiben.

Mit diesem Griff versucht man, dem massiven Akzeptanzproblem beizukommen, welches die KI in der Bevölkerung derzeit noch hat. Der gesetzliche Rahmen des neuen Digitale-Versorgung-Gesetzes in Deutschland schreibt ein Hinzuziehen der KI in der Diagnostik vor. Real ist es bereits jetzt ein Problem für eine Ärzt*in, sich gegen eine KI-Diagnose durchzusetzen. In Frankreich, wo die KI in der Krebs-Erkennung bereits etablierter ist, kam es bereits zu Todesfällen, da Ärzt*innen die Unbedenklichkeits-Analyse der KI nicht zu korrigieren wagten. Es bedarf eines größeren Selbstbewusstseins und zusätzlicher Zeit, den automatisierten Befund zu korrigieren und diese menschliche Korrektur mit ihren Folgekosten gegenüber den Krankenkassen zu vertreten. Angesichts einer massiven KI-Fähigkeits-Propaganda der Technokrat*innen ist es unklar, wie sich menschliches Erfahrungswissen gegenüber der KI behaupten soll: Welche Krankenkasse verschenkt freiwillig die Einsparpotenziale (auch nur im Einzelfall), die eine um den Faktor zehn schnellere KI-Diagnose „verspricht"?

Vielfach wird mittlerweile die Verantwortung von Institutionen, die KI einsetzen, an den intransparenten Algorithmus „wegdelegiert" und dessen Nichtnachvollziehbarkeit schlicht weitergereicht. Die Polizist*in, die im Rahmen des Predictive Policing in einem durch die KI ausgewiesenen „Gefahrengebiet" Personenkontrollen durchführt, macht sich nicht einmal mehr die Mühe, ihre Kontrolle zu legitimieren und verweist auf die KI. Diese entscheide, welche Straßenzüge an welchem Tag zu welcher Tageszeit zum Gefahrengebiet erklärt werden und damit das Recht zur anlasslosen Personalienfeststellung gibt. Die Bankmitarbeiter*in verweist auf das künstlich intelligente Computerprogramm *infoscore*; das habe den Kredit verweigert – sie könne nicht sehen warum. Sie würde ja gerne anders entscheiden, aber ihr seien die Hände gebunden. Hier wird sich nicht einmal mehr die Mühe gemacht, die von der KI getroffene Entscheidung nachträglich zu humanisieren, also minimal nachvollziehbar zu machen. Ehrlicherweise ist es ja auch nicht möglich.

*Was bedeutet es für eine Gesellschaft, die sich demokratisch verfasst nennt, wenn sie es Technokrat*innen überlässt, Regeln zu entwerfen, die auf Ungleichbehandlung setzen und weder beständig noch vermittelbar, ja, nicht einmal bekannt sind? Wie weit hat der techno-totalitär agierende Solutionismus bereits unseren dringend notwendigen Zweifel verdrängt?*

84 Auf der Basis besonders effektiver sogenannter selbstlernender neuronaler Netze.

Weniger Ärztin im künstlich intelligenten Gesundheitssystem

DIGITALISIERUNG MIT NEBENWIRKUNGEN

Online-Sprechstunden bei der Ärztin[85] *per Telemedizin und Gesundheits-Apps auf Rezept – die Digitalisierung des Gesundheitssystems verspricht „zeitgemäßen Service" für die Patientin. Doch es geht um mehr: Gesundheitsindustrie und Krankenkassen wollen das persönliche Gesundheitsbemühen jeder „Kundin" erfassen und durch die Einführung von dynamischen Tarifen individuell bepreisen. Der ehemalige Solidargedanke hat ausgedient. Die freie Ärztinwahl ebenfalls: künstlich intelligente Gesundheits-Apps sollen zukünftig vorfiltern, wer mit welchem Anliegen (nicht-virtuellen) Zugang zur Ärztin bekommt. Insbesondere der Schock der Corona-Krise wirkt wie ein Brandbeschleuniger für die Etablierung weitreichender telemedizinischer und künstlich intelligenter Anwendungen.*

Es geht um wesentlich mehr als um „Datensicherheit" oder die Wahrung unserer „Privatsphäre". Auf diese zu verteidigende, aber vordergründige Ebene wird der öffentliche Diskurs aktuell reduziert. Um die Tiefe des Problems adäquat zu beschreiben, müssen wir von DER fundamentalen Transformation des Gesundheitswesens des 21. Jahrhunderts sprechen. Es geht um einen gigantischen Markt neuer Gesundheitsdienstleistungen in einem biopolitisch neu gerahmten Gesundheits- und Menschen-Bild und es geht um ein dem entsprechend massives Entsolidarisierungs-Programm. Dieses Programm wäre völlig unzureichend mit einer „Neoliberalisierung" des Gesundheitswesens beschrieben.

85 Zur besseren Lesbarkeit schreiben wir diesen Text vornehmlich in der weiblichen Form. Gemeint sind immer alle Geschlechter.

DIE CORONAKRISE ALS BOOST FÜR DIE TELEMEDIZIN

Das Versprechen der Telemedizin ist bestechend. Und tatsächlich kann das Anbinden von kleinen regionalen Krankenhäusern an Spezialkliniken per Telemedizin als sinnvoll erachtet werden. So stehen z. B. die Universitätsklinken in Aachen und Münster per Videokonferenzen mit kleineren Krankenhäusern und Arztpraxen in Kontakt, um Fälle in der Intensivmedizin und Infektionspatientinnen zu besprechen. In Anwesenheit einer Ärztin (vor Ort!) wird bei der Untersuchung eine weitere aus der Spezialklinik dazugeschaltet. Der Start für das Projekt „virtuelles Krankenhaus" wurde wegen des Bedarfs in der Corona-Krise auf den 29.3.20 vorverlegt und auf 200 angeschlossene Kliniken in NRW erweitert. So kann eine Expertise in verantwortungsvoller Weise hinzugezogen werden, die aus verständlichen Gründen nicht in allen Regionalkrankenhäusern zur Verfügung steht. Wir würden dieses Einsatzgebiet der Telemedizin als unstrittig bezeichnen. Zentral ist die Betreuung der Patientin durch eine lokale Ärztin.

Anders sieht das bei Online-Arztbesuchen aus. Medizinische Videosprechstunden sind technisch nicht aufwändiger als ein Videochat mit *jitsi* oder *zoom*. Egal, ob die Ärzt*in gerade in der Praxis, zu Hause oder auf Reisen ist, je ein Laptop mit Kamera und Mikrofon auf Seiten der Ärztin und bei der Patientin genügen. Die Patientin braucht nur ihre Krankenkassenkarte in die Kamera zu halten und schon kann es losgehen. Die Tele-Ärztin wird durch eine entsprechende Software automatisch dazu angehalten, den Befund während der Sitzung in die elektronische Patientenakte einzutippen. Um die Sicherheit der sensiblen Patientendaten steht es dabei leider schlecht, wie verschiedene Untersuchungen der Telematik-Infrastruktur ergeben haben. Aber das scheint kein Hindernis für deren Nutzung zu sein.

Normalerweise kostet die Nutzung der Software die Ärztin monatlich 30 – 150 Euro. Einige der derzeit 23 von der Kassenärztlichen Bundesvereinigung zugelassenen Software-Anbieter verlangen als Lockangebot während der Coronakrise kein Geld für diesen Softwaredienst. Das, was im letzten Jahr nur wenig Zuspruch erfahren hat, entpuppt sich in der Epidemie als

attraktives Angebot. Die Anmeldezahlen schnellen nach oben. Niemand setzt sich in Coronazeiten gern in ein Wartezimmer. Ärztinnen werden mit einer Technikpauschale geködert. Sie können überdies für die ersten 50 Videosprechstunden im Quartal je zehn Euro mehr abrechnen als für ein persönliches Gespräch in der Praxis. Die bisher festgelegte Begrenzung der Onlinekonsultationen auf maximal 20 Prozent aller Patientenkontakte, wurde wegen der Corona-Krise bis mindestens zum 30. Juni ausgesetzt.

Das Bewertungs- und Datensammel-Portal *Jameda* vermittelt nicht nur Videosprechstunden zur eigenen Haus- oder Fachärztin, sondern zu beliebigen Ärztinnen irgendwo in Deutschland. Weil die Wartezimmer vieler Arztpraxen in Coronazeiten weitgehend leer bleiben, bieten einige Ärztinnen schon für den gleichen oder den Folgetag Videosprechstunden-Termine auch überregional an. Auch Rezepte können nach einer Videosprechstunde ausgestellt werden. Für Privatpatientinnen geht das manchmal online, allen anderen muss das Rezept bis Ende 2020 noch per Post zugeschickt werden. Mit einer Ausnahmeregelung für die Zeit der Coronakrise ist es möglich, dass eine Ärztin den Patienten, den sie noch nie persönlich getroffen hat, bis zu zwei Wochen krankschreibt.

Der Ersatz von realen Arztbesuchen durch telemedizinische Sprechstunden stellt eine gefährliche Tendenz eines zukünftigen „Vielklassensystems" dar, dessen Klassen bzw. Tarife eng verknüpft sind mit der Bereitschaft der Patientin, a) intime Gesundheitsdaten zur Verfügung zu stellen und darüber b) das eigene Gesundheitsbemühen bewerten zu lassen. Wir werden sehen, dass die Online-Sprechstunde kein Nebeneffekt einer virologischen Ausnahmesituation, sondern kalkuliertes Ziel eines auf (weiter gesteigerte) Kosteneffizienz reduzierten Gesundheitssystems ist. Auch der Video-Chat mit der Therapeutin, deren offline-Sitzungen während der Kontaktbeschränkung in der Coronakrise nicht stattfinden konnten, muss als Türöffner für eine bedenklich eingeschränkte (Basis-)Gesundheitsleistung auch jenseits der Epidemie verstanden werden.

Gerade für die ärztliche Versorgung in ländlichen Gebieten wird der Verweis auf den Tele-Doktor zu einer noch schlechteren Abdeckung durch ortsansässige Ärztinnen führen. Es ist zynisch, den für viele Ärztinnen unattraktiven ländlichen Raum als Argument für die telemedizinische Sprechstunde heranzuziehen. Eine (dort) höhere Vergütung, statt einer Abwertung der Versorgung, sollte das Mittel der Wahl sein. Die bisher geltende freie, nicht-virtuelle Arztwahl ist angezählt.

„SELBSTERMÄCHTIGUNG" DURCH DEN QUANTIFIED-SELF-TREND

Begonnen hat alles ganz harmlos mit den Bonus-Tarifen einiger Krankenversicherungen, die ihren Versicherten einen Jahresbonus gewährten, wenn diese ausreichend tägliche Bewegung über einen Schrittzähler (Fitnessarmband, Smartwatch, …) nachweisen. Dahinter steckt die gleiche Idee wie bei der „Blackbox" der Autoversicherer, die das individuelle Fahrverhalten aufzeichnet und der Fahrerin bei ausreichend defensiver Fahrweise (wenige abrupte Brems- oder Beschleunigungsmanöver) gegebenenfalls einen Bonus auf den zu zahlenden Fahrzeugversicherungstarif anrechnet. Das, was als Bonus begann, soll in individualisierte Tarife, also programmatische Ungleichbehandlung münden. Aus der Ausnahme des Bonustarifs für explizite Sparfüchse wird über wenige Jahre der Regelfall: In neuen Automodellen sind Blackboxes ab Mai 2022 europaweit verpflichtend. Ab 2024 müssen alle Neuwagen damit ausgestattet werden.

Das Anliegen der Versicherungen ist simpel: das Filetieren eines immer genauer abschätzbaren Versicherungsrisikos durch immer genauere Verhaltensdaten. Der entsolidarisierende Effekt dieser ausdifferenzierten Tariflandschaft geht aber weit über die Banalität der Versicherungsmathematik hinaus. Die inaktive Couch-Potato wird, wie die unbeliebte Auto-Raserin, durch eine teurere Versicherung abgestraft. „Gesellschaftlich unerwünschtes" Verhalten wird detektierbar, mit einem Malus belegt und damit steuerbar. Wichtig anzumerken ist hierbei, dass die Definition, welches Verhalten im Sinne des Allgemeinwohls als zu belohnen oder zu bestrafen gilt, nicht gesamt-gesellschaftlich ausgehandelt, sondern von Versicherungsunternehmen in einer intransparenten (künstlich intelligenten) Bewertungssoftware (variabel) festgelegt wird. Damit lässt sich sehr effektiv Bevölkerungsmanagement betreiben. Und es eröffnet sich ein neuer Markt an „medizinischer" Hard- und Software zur Selbstvermessung und Selbstoptimierung.

„Wir befähigen das Individuum, seine Gesundheit selbst in die Hand zu nehmen."

So der Apple-Chef Tim Cook, 2019 bei der Vorstellung des bislang größten „kardiologischen" Feldversuchs in den USA unter Mitwirkung der Stanford Universität. 400.000 Applewatch-Nutzerinnen geben Nonstop ihre Kreislaufdaten über den in der Uhr verbauten EKG-Sensor weiter. Dieser Puls-Sensor kann angeblich sogar das Infarkt-relavante Vorhofflimmern diagnostizieren. Stiftung Warentest attestiert den Fitness-Smart-Watches ein schwaches Abschneiden, sowohl in Bezug auf deren medizinische Genauigkeit, als auch auf den

Datenschutz. Ärztinnen berichten immer wieder von vermeintlich akut herzkranken Smart-Watch-Trägern in der Notaufnahme, deren „Leiden" sich über medizinisch zugelassene Diagnose-Verfahren nicht bestätigen lässt (Spiegel, 21.11.19).

Unbeirrt von der mangelnden medizinischen Aussagekraft der so ermittelten Daten, findet eine wachsende Gewöhnung an die (Selbst-)Quantifizierung des Alltags und an die individuelle Verantwortung um die eigene Gesundheit als zentrale Größe im künstlich-intelligenten Krankenversicherungswesen statt. Diese Form der fremdbestimmten Verhaltenslenkung als „Selbstermächtigung" zu verkaufen, kann durchaus als „Nudging" verstanden werden. Überhaupt setzt die eingeleitete Transformation des Gesundheitswesens viel weniger auf repressives Verordnen, als auf (ökonomisch) verführendes Anstupsen im Sinne eines neuen Lifestyles, der sich durch ein gefördertes Bemühen um die eigene Gesundheit auszeichnet.

LIFESTYLE-MEDIZIN ALS TÜRÖFFNER

Nachdem viele kleine Start-ups mit individuellen Online-Ernährungsberatungen und auf den spezifischen Stoffwechsel-Typ ausgerichteten Nahrungsergänzungsmitteln auf dem erweiterten Gesundheitsmarkt vorgeprescht sind, zieht nun auch der Lebensmittelriese Nestlé nach. Mit dem *Wellness Ambassador* Programm, kann mensch sich für gut 600 Dollar im Jahr nach einem integrierten DNA-Test und der ständigen Übermittlung von Lebens- und Ernährungsgewohnheiten von einer KI individuell optimierte Lebensmittel zusammenstellen lassen. Das Angebot richtet sich insbesondere an eine Klientel mit Diabetes und hohen Cholesterinwerten. Konkret bekommt die Kundin eine individuelle Mischung von Smoothies, Tees, Vitamin-Snacks empfohlen. Das Programm startete nicht zufällig in Japan und erfreut sich insbesondere in Deutschland einer großen Nachfrage. Beide Gesellschaften haben einen hohen Altersdurchschnitt.

Auch andere Anbieter wie *mymuesli* versprechen über diverse „personalised nutrition"-Programme, mögliche Nährstoffdefizite zu identifizieren – ebenfalls auf Grundlage von DNA- und Ernährungstests. Bei vielen Anbietern gibt es halb-wissenschaftliche Testergebnisse, deren Bedeutung sich für den Kunden nicht unmittelbar erschließt. Wer sich damit überfordert fühlt, kann sich bei der Interpretation mit einem zusätzlich zu bezahlenden Online-Coaching helfen lassen.

Über eine Zweitverwertung der so gesammelten Ernährungsgewohnheiten ist bisher nichts bekannt. Es werden lediglich die Persönlichkeitsrechte im Rahmen der Datenschutzgrundverordnung garantiert.

ADA – DIE GESUNDHEITSAPP

Am Beispiel des medizin-informatischen Startups Ada lassen sich Umfang und Perspektive der aktuellen gesundheitspolitischen Transformation nachzeichnen. Ada ist zunächst eine App, eine Art Chatbot, der eine Online Symptom-Analyse auf der Basis einer selbstlernenden KI anbietet. Die App soll „allen Menschen Zugang zur personalisierten Medizin der Zukunft verschaffen", so Martin Hirsch, Chef des gleichnamigen Kreuzberger Unternehmens Ada. „Ada stellt dir einfache Fragen und vergleicht deine Antworten mit Tausenden von ähnlichen Fällen, um die wahrscheinlichsten Ursachen für deine Symptome zu ermitteln." Mehr als acht Millionen Menschen haben die App bereits heruntergeladen.

Bekannt geworden ist Ada über einen Datenskandal: *„Alle Daten sind verschlüsselt bei Ada gespeichert und werden niemals ohne Einverständnis mit Dritten geteilt"*, versprach die Ada Health GmbH auf der Webseite zur App. Dem ist nicht so. Ein Mitarbeiter der Heise-Redaktion gibt im Dezember 2019 zu Testzwecken „Inkontinenz" in die Maske der Diagnose-App ein. Die Information wird jedoch nicht nur an Ada übermittelt, sondern auch an den Analysedienst Amplitude mit Hauptsitz in San Francisco. Der übertragene Datensatz umfasst insgesamt über 2.000 Zeichen, darin enthalten sind neben der Inkontinenz auch eine User-ID, der Zeitpunkt, das verwendete Betriebssystem, die Android Werbe-ID und vieles mehr. Auch die anschließend abgefragten Symptome werden übermittelt. Parallel dazu läuft eine Verbindung zu Facebook und zur Analysefirma Adjust. Auch hier werden persönliche Daten übermittelt[86].

„Es ist generell schwierig, die Privatsphäre im digitalen Bereich aufrecht zu erhalten", so Stefan Vilsmeier von der Firma Brainlab, die digitalisierte Chirurgie-Lösungen anbietet und eine Art App-Store für medizinische KI-Anwendungen entwickeln will. Der bayrische Ministerpräsident Söder geht noch einen Schritt weiter: *„Gesundheitsdaten müssen aus den Fängen des Datenschutzes befreit werden."* Ein Blick in die USA zeigt wie selbstbewusst Google diese „Befreiung" vorantreibt.

GOOGLES PROJEKT NIGHTINGALE

Google arbeitet in den USA seit 2018 mit der Gesundheitsorganisation *Ascension* zusammen, die 150 Kran-

86 Detaillierte Analyse unter https://www.heise.de/select/ct/2019/23/1573230323059682

kenhäuser und Tausende Arztpraxen betreibt. Gesundheitsdaten von mehr als 50 Millionen Menschen sollen bereits auf Googles Servern gelandet sein. Das umfasst Laborergebnisse, ärztliche Diagnosen, Behandlungsverläufe und Krankenhausaufenthalte – nicht etwa anonymisiert, sondern verknüpft mit Namen und Adressen der Patientinnen. Google-Mitarbeiterinnen haben vollen Zugriff auf diese Daten.

Google entwickelt eine Software, die mit Hilfe von künstlicher Intelligenz (KI) und maschinellem Lernen vorschlägt, wie sich die Versorgung einzelner Patientinnen verbessern lässt. Es soll eine gewaltige Patientinnendatenbank entstehen, die optisch an Googles Suchmaschine erinnert. Die Software vervollständigt automatisch Eingaben zu den Patientennamen, die mit sämtlichen gespeicherten Gesundheitsdaten verknüpft sind. Ärztinnen sollen nicht nur individuelle Informationen einsehen, sondern grafische Zeitverläufe erstellen und Datensätze miteinander vergleichen können. Google hofft, diese Infrastruktur künftig an andere Gesundheitsdienstleister verkaufen zu können. All das geschieht, ohne dass die betroffenen Patientinnen zugestimmt haben.

Im November 2019 hatte sich ein Google-Mitarbeiter dazu entschieden, als Whistleblower geheime Dokumente über das Projekt Nightingale zu veröffentlichen. Aus diesen geht hervor, dass Google sogar die aus der Kooperation abgeschöpften Gesundheitsdaten selbst „zukünftig teilen oder verkaufen und für das Bewerben entwickelter Gesundheitsprodukte nutzen“ will.

Die öffentliche Debatte verbleibt jedoch an der Oberfläche, wenn sie mit Ada und Nightingale (und vielen weiteren „Einzelfällen“) den exzeptionellen „Datenunfall“ skandalisiert und das dahinter liegende (gewöhnliche) Geschäftsmodell als unproblematisch anerkennt. Das Problem residiert im Regelfall, nicht im Störfall! Der Markt für KI-basierte Gesundheitsanwendungen und -produkte expandiert massiv und benötigt für das Trainieren der KI detaillierte Datensätze. Deren Wert steigt.

WACHSENDER GESUNDHEITSMARKT

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)[87], investieren sie Milliarden in die Biotech-Forschung und versuchen mit Hochdruck, erweiterte Gesundheitsdienste in ihre Softwareumgebungen zu integrieren. Das Smartphone soll dabei zur neuen persönlichen Gesundheitszentrale avancieren, in seiner Funktionalität erweitert durch Zusatzgeräte wie Fitness-Armbänder oder Smart-Watches. Amazon nähert sich dem vielversprechenden Gesundheitsmarkt gleich auf drei Weisen. Der Konzern 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 des Versicherten ist, desto exakter lässt sich dieses Risiko berechnen. Ein Wettbewerbsvorteil gegenüber der Konkurrenz. Daher liegt es nahe, dass Google und Amazon sich in diesem Geschäft behaupten könnten – die fehlende Expertise im Versicherungswesen lässt sich einkaufen.

Der Wert personalisierter Patientinnendaten variiert stark, aber er steigt. Im Schnitt sind medizinische Daten zehnmal mehr wert als Kreditkartendaten[88]. Gesundheitsdaten sind unwiderruflich, unabänderbar und damit viel länger nutzbar. Spätestens als die amerikanische Roche-Tochter *Genentech* für 3000 Datensätze 60 Mio. US-Dollar ans Startup-Unternehmen *23andMe* bezahlte, wurde offensichtlich, wie wertvoll Patientinnendaten sind. Die Angaben stammten von 600.000 Personen, die für 99 US-Dollar einen Gentest kauften, ihre Einwilligung gaben, dass die Daten für Forschungszwecke verwendbar sind, und bei denen ein häufig bei Parkinson-Erkrankungen auftretendes Genom entdeckt wurde.

Nach dem im November 2019 in Deutschland verabschiedeten „Digitale-Versorgung-Gesetz“[89], sollen nun seit 1.1.2020 sensible Daten der elektronischen Patientenakte zentral zusammengefasst werden, um sie dann „pseudonomisiert“ Behörden, Forschungseinrichtungen und Universitätskliniken zur Verfügung zu stellen. Die Zusammenführung der Daten trotz der nachgewiesenen Sicherheitsmängel in der veralteten Telematik-Infrastruktur sowie das Fehlen einer Opt-Out Möglichkeit für die 73 Mio. gesetzlich Krankenversicherten sind heftig und breit kritisiert worden. Dennoch lautet der gesetzliche Beschluss: Es besteht kein Recht, sich einer Verwertung der sensibelsten aller Daten zu verweigern. Somit besteht die ernst zu nehmende Gefahr, dass Krankenkassen oder Dritte Gesundheitsprofile anlegen.

ZENTRALER PLAYER: BERTELSMANN

Die hundertprozentige Bertelsmann-Tochter Arvato ist für viele deutsche Behörden zentraler IT-Dienstleister. Das Gesundheitsministerium hat Arvato damit beauf-

87 http://fortune.com/2017/09/11/apple-tim-cook-education-health-care/

88 https://www.althammer-kill.de/news-detail/gesundheitsdaten-sind-wertvoller-als-finanzdaten/

89 DVG, 19/13438

tragt, die für die elektronische Gesundheitsakte notwendige Telematikinfrastruktur[90] bereitzustellen und zu verwalten. Zudem ist Arvato nach der Übernahme von welldoo[91] unter dem neuen Namen *Vilua* selbst Gesundheitsdienstleister geworden. Darüber hinaus betreibt Arvato den Finanzdienst *Infoscore*, der seit 2005 (neben der Schufa) von vielen Banken zur Ermittlung der Kreditwürdigkeit herangezogen wird. Infoscore schlägt Finanzakteuren nicht nur vor, ob eine Kundin einen Kredit erhalten soll – Infoscore berechnet aus den vielen persönlichen Daten der Kundin einen dem Kreditrisiko angemessenen Zinssatz. Diese unternehmerische Verflechtung von Gesundheits- und Finanzdienstleistungen ist ein abenteuerliches Risiko hinsichtlich der zweckgebundenen Trennung beider Datenbanken. Arvato beteuert, dass beide Unternehmensbereiche durch eine „chinesische Mauer" voneinander getrennt seien. Wenig glaubwürdig, denn Arvato hatte zuvor ebenfalls garantiert, dass ihre für die DB Fahrpreisnacherhebung gepflegte Datei von „Schwarzfahrerinnen" nicht in die infoscore-Datenbank einfließen würde. Fehlanzeige – das Unternehmen gab kleinlaut zu, die Erkenntnisse für die Ermittlung der Kreditwürdigkeit mitgenutzt zu haben. Solche (unglaubwürdigen) Separierungs-Versprechen kennen wir ebenfalls von der *whatsapp*-Übernahme durch facebook: Trotz gegenteiliger Zusicherung führte facebook seine Datenbank nach nur zwei Jahren mit der von whatsapp zusammen.

Bertelsmann nimmt darüber hinaus über seine gleichnamige Stiftung Einfluss auf die Entwicklung der Gesundheitsversorgung in Deutschland. Im Sommer 2019 veröffentlichte Brigitte Mohn als Vorsitzende der Bertelsmannstiftung eine Studie[92] zur Reduzierung der Krankenhäuser in Deutschland. 1960 gab es allein in Westdeutschland 3600 Krankenhäuser. Die Zahl hat sich auf derzeit 1400 bundesweit reduziert. Die Autorinnen fordern, die Zahl der Krankenhäuser noch einmal drastisch zu senken, auf bundesweit 600. Wie fragwürdig ein weiteres Reduzieren von Krankenhauskapazitäten zugunsten einer profitablen Gesundheitsversorgung erscheint, bedarf in Zeiten des Coronavirus keiner weiteren Ausführung. Dass Brigitte Mohn zusätzlich im Aufsichtsrat der Rhön-Klinik Kette sitzt, sei nur am Rande erwähnt.

SMARTES VORFILTERN

Die Uniklinik in Essen bezeichnet sich selbst als „Smart Hospital". Sie nutzt Ada für die „Triagierung" von Patienten in der Notaufnahme. Das bedeutet, der Chatbot von Ada soll die dringenden Fälle von denen, die länger warten können, trennen. Ein ähnlicher Test läuft an der Uni Gießen-Marburg. Genau das ist die Perspektive vieler Krankenkassen, die schon jetzt offenbaren: „Der Goldstandard der freien Arztwahl ist nicht mehr zu halten". Die Kostensteigerung sei zu groß. Ebenso wie die vermeintlichen Einsparpotenziale des digitalisierten Gesundheitswesens. So soll ein künstlich intelligentes System basierend auf den individuellen Patientinnendaten zukünftig fallspezifisch entscheiden:

- *Wer kann mit einem Rezept oder einer Kaufempfehlung für frei erhältliche Medizinprodukte per KI-Ferndiagnose à la Ada abgefertigt werden?*
- *Wer soll einen Termin für eine Online-Sprechstunde bei einer Telemedizinerin erhalten ?*
- *Wer erhält (als letzte Option) den nicht-virtuellen Arzt-Besuch?*

Der althergebrachte, „zu teure", analoge Arztbesuch soll auf ein Minimum reduziert werden. Der damit einhergehende Qualitätsverlust in der Gesundheitsversorgung wird billigend in Kauf genommen und hinter der Werbung für ein „zeitgemäß digitales" Gesundheitsmanagement versteckt. Die durch das „Digitale-Versorgung-Gesetz" geförderte Verschreibung von „Gesundheits-Apps" leistet einer solchen Virtualisierung von Gesundheits(dienst)leistungen Vorschub. Die Verabreichung von Apps als medizinische Produkte auf Rezept ist eine nicht zu unterschätzende Finanzierungshilfe für medizinische Start-Ups und soll eine bedenkliche Appifizierung der Diagnose- und Behandlungs-Methoden forcieren. Es ist bezeichnend, dass die Qualitätskontrolle des bereits mehrere Hunderttausend Apps umfassenden Zoos an „medizinischen" Beratungsapps erst im nächsten Jahr „nachgereicht" werden soll.

In den USA sind offenbar Millionen Afroamerikanerinnen bei der medizinischen Versorgung benachteiligt worden. Laut einem Bericht des Wissenschaftsmagazins „Science"[93] hat eine weit verbreitete Software weißen Patientinnen eher eine teure medizinische Behandlung zugesprochen als schwarzen. In dem Bericht heißt es, dass der Algorithmus jedes Jahr für rund 200 Millionen (ver-

90 Im Dezember 2019 gelang dem Chaos Computer Club ein spektakulär einfacher Hack des Systems, welches bereits jetzt sensible Patientendaten übermittelt. Sicherheitsforschern ist es gelungen, sich gültige Heilberufsausweise, Praxisausweise, Konnektorkarten und Gesundheitskarten auf die Identitäten Dritter zu verschaffen. Mit diesen Identitäten konnten sie anschließend auf Anwendungen der Telematik-Infrastruktur und Gesundheitsdaten von Versicherten zugreifen. (siehe https://www.ccc.de/de/updates/2019/neue-schwachstellen-gesundheitsnetzwerk)

91 Welldoo ist ein Gesundheitsapp-Entwickler vor dessen Daten(un)sicherheit der damalige Gesundheitsminister Hermann Gröhe 2015 explizit gewarnt hatte.

92 https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/VV_Bericht_KH-Landschaft_final.pdf

93 https://science.sciencemag.org/content/366/6464/447

sicherte) Patientinnen in den USA ausrechnet, ob eine Sonderbehandlung für sie infrage kommt. Die Software wird unter anderem von Krankenhäusern und Versicherungen eingesetzt, um automatisiert Patientinnen zu identifizieren, die am ehesten von aufwendigen und damit auch teuren Behandlungen profitieren würden. Das Problem liege an den Daten, mit denen der Algorithmus arbeitet. Als Grundlage für die Berechnung eines Risikofaktors habe der nämlich die Behandlungskosten einer Patientin genommen: Wer im Laufe des Jahres mehr Geld für medizinische Betreuung ausgibt, hat eine höhere Risikobewertung. Das System geht davon aus, dass höhere Behandlungskosten dafür sprechen, dass eine Person mehr medizinische Hilfe benötigt.

Laut der Studie nehmen Afroamerikanerinnen in den USA weniger medizinische Behandlungen in Anspruch. Im Schnitt liegen die Behandlungskosten um 1801 Dollar im Jahr niedriger als für eine vergleichbar kranke Weiße. Ursachen für die geringeren Behandlungskosten von Afroamerikanerinnen sind laut dem Bericht unter anderem Armut und Rassismus. Die Folge: Afroamerikanerinnen müssen kranker sein, damit die Software einen höheren Risikofaktor erkennt, der zusätzliche Unterstützung rechtfertigt. Demnach habe der Algorithmus nur 17,7 Prozent der dunkelhäutigen Patientinnen eine zusätzliche Behandlung zugestanden. Laut Forscherinnen würde der Anteil bei 46,5 Prozent liegen, wenn die Software ohne Benachteiligung rechnen würde.

VOLLSTÄNDIG PERSONALISIERTE MEDIZIN UND PERMANENTE VORSORGE

Bei Bluthochdruck Mittel A, bei Herzschwäche Mittel B: Dass Patientinnen mit gleicher Krankheit meist die gleiche Medikation erhalten, soll bald der Vergangenheit angehören. Dazu braucht die Pharmabranche massenhaft Patientinnendaten. Sie sollen aus Studien, Apps und Arztpraxen kommen. Ärztinnen sollen nun mehr und mehr auf die elektronische Patientenakte umstellen, damit diese Daten en passant anfallen. „Wir können in den nächsten Jahren mit einer Explosion an Daten rechnen", sagt Anne-Marie Martin, Leiterin der Präzisionsmedizin bei Novartis. Die Analyse massenhafter Daten soll Zusammenhänge aufzeigen, die bis dahin unbekannt waren. Bestimmte Gen- oder Zelleigenschaften, Alter, Gewicht, eine Vorerkrankung, andere Medikamente, Wohnort, Ethnie oder die Uhrzeit der Einnahme könnten Einfluss haben, ob ein Mittel wirkt oder nicht. Big Data soll die Unkenntnis der Wirkungsweise durch die schiere Masse an Daten erschlagen – so die Hoffnung der Technokratinnen, die eine vollständig personalisierte Medizin herbeisehnen.[94]

Eines Tages werde jede Bürgerin ihr Genom entschlüsseln lassen, so Ada-Chef Martin Hirsch. *„Dann wird Ada in der Lage sein, aufgrund des Gentests und der jeweils neuesten medizinischen Erkenntnisse genaue Ratschläge zu erteilen, was man tun oder unterlassen kann, um gesund zu bleiben."*

Diese Vorstellung deckt sich mit der Zukunftsvision von Google: Im Mai 2018 sickerte ein internes Firmenvideo[95] der Forschungsabteilung Google X in die Öffentlichkeit. Unter dem Namen „*The selfish ledger*", was sich ungelenk mit dem „Buch des Lebens" übersetzen lässt, beschreibt Google seine Zukunftsvision einer bevormundenden Gesundheitsvorsorge. Ein persönliches Journal „sämtlicher Handlungen, Entscheidungen, Vorlieben, Aufenthaltsorte und Beziehungen" ist die Grundlage für ein System digitaler Assistenz, das KI-basiert auf jeden einzelnen zugeschnittene „Handlungsempfehlungen" ausspricht. Google verspricht perspektivisch Armut und Krankheiten überwinden zu können unter der freimütig vorgetragenen Bedingung: die Aufgabe der freien Entscheidung. Nur dann ließen sich effektiv „potentielle Fehler im Verhalten der Nutzer detektieren und korrigieren".

Microsoft Chef Bill Gates treibt seit Jahren maßgeblich die Initiative ID2020 voran. Hierbei geht es um eine digitale ID auf Basis der Blockchain-Technologie[96] – eine Art Personalausweis, in dem sämtliche bekannten Daten über das Leben eines Menschen (vergleichbar mit Googles *ledger*) gespeichert werden. Die Corona-Pandemie kann nach Vorstellung der Gates-Foundation der Einführung eines solchen globalen Registers Auftrieb verleihen: Sobald ein Impfstoff vorhanden ist, ließe sich ein Impfgebot umsetzen[97]. Die Funktion eines Impfregisters, wäre dann der einführende Basisbaustein für die ID2020. Eine Anwendung dieses Registers: Individualisierte Zugangsbeschränkungen in Abhängigkeit eines

94 Auch hier „hilft" das Digitale-Versorgung-Gesetz, nachdem eine Ärztin nur noch geringere Kosten abrechnen kann, wenn sie sich der digitalen Datenerfassung entzieht, also weiter „analog" mit den Krankenkassen kommuniziert und sich nicht über die (nachweislich unsichere) Telematik-Infrastruktur vernetzt. Gesundheitsminister Spahn: „Ich werde die Telematik und die elektronische Patientenakte vorantreiben, Hacker hin oder her."

95 Geleaktes Firmenvideo von Google: https://vimeo.com/270713969

96 Die Blockchain soll hier eine selbstkonsistente, verteilte Speicherung der persönlichen Daten ohne zentrale Behörde ermöglichen. Es handelt sich (grob) um das dezentrale Speichern der Daten an viele Orten, um ein hohes Maß an Fälschungssicherheit zu garantieren.

97 Diese Idee macht B. Gates derzeit zu einem gefundenen Fressen für Verschwörungstheoretikerinnen, von deren teils absurder Kritik wir uns hier deutlich abgrenzen wollen.

Immunitätsnachweises. Die Nutzung der ID als global lesbare Patientenakte – ein nächster angedachter Schritt über den geregelt werden kann, wer Anspruch auf welche Gesundheitsleistungen hat.

Der Anwendungsbereich der ID geht jedoch weit über den Gesundheitssektor hinaus. Im Sinne eines „human capital investment" soll die ID Aufschluss über „persönliche Potenziale und Schwächen" geben. Zum Beispiel könne die Förderungswürdigkeit eines Menschen hinsichtlich seiner (Aus-)Bildung – gemäß der Initiatorinnen dieser „allumfassenden" Akte – über die erkennbare Leistungsbereitschaft ermittelt werden. Dazu werde dann nicht mehr nur die detailliert festgehaltene Ausbildungshistorie herangezogen; eine KI solle vielmehr aus sämtlichen Handlungen, Überzeugungen und Wünschen statistische Muster für ein ungleich „genaueres Abbild" des persönlichen Bemühens erkennen lassen.

Selbstbewusst stellt Google in Aussicht: *„Noch passen sich die Systeme ihren Nutzern an. Dieses Verhältnis wird sich bald umkehren."* Die diesen Ansichten zugrundeliegende, erschreckend totalitär anmutende Sicht auf eine vermeintlich bessere Welt in Bevormundung durch künstlich-intelligente Expertensysteme, knüpft nahtlos an die Vorstellungen von Skinners Behaviorismus an. Dieser geht angesichts zu komplexer Lebensverhältnisse von einer notwendigen Verhaltenssteuerung andernfalls nicht-rational handelnder Individuen aus – ein längst überwunden geglaubtes, zutiefst paternalistisches und im Einklang mit Chinas Social-Scoring-Systemen erschreckend „aktuelles" Menschenbild.

Ökotechnokratie

„Smarte" Ökologie von oben

Die Klimafrage beherrscht derzeit die öffentliche Debatte. Selbst das Weltwirtschaftsforum in Davos (Februar 2020) gibt vor, die Brisanz des Umweltschutzes verstanden zu haben. Hunderttausende von Toten und ein monatelanges Wachkoma der Weltwirtschaft während der Corona-Pandemie, haben deutlich werden lassen, wie heftig sich die Vernichtung von Lebensräumen für Tiere zugunsten von Landwirtschaft, Berg- und Städtebau als virologische Bedrohung für den Menschen auswirken kann. Wildtiere, oftmals die letzten ihrer Art, kommen in direkten Kontakt mit anderen Spezies und letztlich dem Menschen.

Die Bewegung Fridays for Future hat den durch die viel zu hohen CO2-Emissionen verursachten Klimawandel endlich zum weltweiten Gesprächsthema gemacht. Als Hauptursache für die steigenden CO2-Emissionen gelten der weltweit steigende Energiehunger in Wirtschaft und Gesellschaft und seine Sättigung mit fossiler Energieerzeugung. Wenn sich nichts Grundlegendes ändert, so warnt der Weltklimarat, werde sich die Erde in den nächsten 20 Jahren um mindestens 1,5 Grad erwärmen (im Vergleich zum vorindustriellen Klima). Hungersnöte, Waldbrände, Unwetter und Artensterben würden sich bereits bis zum Jahr 2040 drastisch verschlimmern. Jenseits der 1,5 Grad droht sogar eine Hitzespirale: Biomasse in auftauenden Permafrostböden in Nordkanada, Alaska, Grönland und Ostsibirien würden Milliarden Tonnen zusätzliches CO2 freisetzen, genau wie Waldbrände in der Tundra oder den Tropen. Schmelzendes Eis in der Arktis könnte mittelbar den Golfstrom versiegen lassen. Wie Dominosteine könnten sogenannte „Kippelemente des Klimas" eine Krise nach der anderen auslösen. Auf der Erde würde es immer heißer werden. Was dann genau passieren wird, kann die Wissenschaft nicht vorhersagen.[98]

Dagegen versprechen Technologiegläubige mit einer Digitalisierung sämtlicher Lebensprozesse über Big-Da-

98 https://www.de-ipcc.de/256.php und https://www.zeit.de/wissen/umwelt/2018-08/klimawandel-erderwaermung-duerre-risiko-klima-forschung-kippelemente

ta-Techniken und Künstlicher Intelligenz (KI) Lösungen für das Klimaproblem zu liefern – u. a. durch KI-gestützte Prozessoptimierung. Dummerweise hat die Informationstechnik für ihre zahllosen Rechner und Geräte, ihre ungeheuren Datenmengen in Rechenzentren und weltumspannenden Netze einen immensen Energiebedarf, für dessen Bereitstellung schon jetzt mehr CO2 freigesetzt wird, als durch den gesamten Flugverkehr weltweit. Der rasante Anstieg dieses Ressourcenverbrauchs wird vor allem von Cloud- und Streamingdiensten sowie Online-Gaming und neuesten KI-Anwendungen getrieben.

Das Grundmuster der herrschafts- und profitorientierten „Technokratie-Falle" ist in allen der im Folgenden diskutierten technologischen Innovationen gleich: Technologie-zentrierte Antworten befeuern das Technologie-induzierte Problem des wachsenden Energiehungers. Sie sind damit vielmehr Teil des Problems als dessen Lösung. Statt die Ursachen der Zerstörung des Planeten ergebnisoffen zu beforschen und dann radikal zu bekämpfen, wird „fortschrittsblind" nach Technologien gesucht, die (vergeblich) versuchen, die Konsequenzen eines weiter-wie-bisher einzuhegen.

Der Klimawandel trifft dabei nicht alle gleichermaßen – die Bedrohung „der Menschheit" als Ganzes ist eine wenig hilfreiche Unterschlagung der unterschiedlichen sozialen Konsequenzen. Reiche trifft die Klimakrise weniger als Arme, den globalen Norden weniger als den Süden. Wenn mensch in die Chefetagen der IT-Konzerne schaut, dann sitzt da die wohl am wenigsten gefährdete Bevölkerungsgruppe an den Hebeln. Das hat durchaus Einfluss darauf, was für „Lösungsvorschläge" von dort kommen.

Besonders eindrücklich versinnbildlichen riesige CO2-Staubsauger des Startups *Climeworks* der ETH Zürich das Dilemma der Technokratie: Die Anlage, die aussieht wie ein Raketentriebwerk, soll das CO2-Problem lösen, indem sie das klimaschädliche Gas mit riesigen Turbinen aus der Luft filtert und bindet. Tatsächlich erzeugt sie aber ein massives Energieproblem, denn: Um auch nur ein Prozent des jährlichen, weltweiten CO2-Ausstoßes aus der Luft zu filtern, bräuchte es 250.000 dieser Anlagen. Deren Betrieb fräße so viel Strom wie alle bundesdeutschen Haushalte zusammen – und emittiert darüber zusätzliches CO2.

DIGITALER ENERGIEHUNGER LÄSST SICH NICHT WEG-VIRTUALISIEREN

Die Virtualisierung von Anwendungen in der *cloud* verschleiert zwar ihren ökologischen Fußabdruck, aber sie vergrößert ihn in der Regel: Das einstündige Videostreaming über *youtube* verbraucht über die involvierte Server- und Netzinfrastruktur so viel Strom, wie die halbstündige Nutzung der Heizplatte eines E-Herds. Die Herstellung und der Vertrieb von DVDs waren deutlich ressourcenschonender! Wir sehen keinerlei Anzeichen für eine tatsächliche Ressourceneinsparung durch Digitalisierung. Im Gegenteil: die Digitalisierung wirke als „Brandbeschleuniger von Wachstumsmustern, die planetarische Leitplanken durchbrechen"[99].

Die Digitalisierung hat eine klare materielle Basis, die unausweichlich mit unserem Ökosystem zu tun hat. Deshalb können wir nicht nur über Zukunftstechnologie und Mensch reden, sondern müssen Umwelt dazunehmen. Alles andere gibt keine Zukunft.

Laut der französischen Umweltorganisation *The Shift Project*[100] steigt der Energieverbrauch digitaler Technologien am schnellsten an. Weltweit waren digitale Dienste noch 2015 für rund zwei Prozent aller CO2-Emissionen verantwortlich, ähnlich viel wie der CO2-Ausstoß aller weltweiten Urlaubsflieger. Bereits 2018 galt das Verhältnis nicht mehr. Derzeit liege ihr Anteil bei vier Prozent der weltweiten CO2-Emissionen, heißt es: Das sei mehr, als der gesamte weltweite Flugverkehr ausmache. Zwar ist der Schaden durch Flugzeuge immer noch deutlich höher – sie pusten ihre Schadstoffe direkt in die Atmosphäre – doch der Strombedarf der Informations- und Kommunikationstechnologie wird weiter steigen: Bis zum Jahr 2025 könnte sich der Anteil auf insgesamt acht Prozent verdoppeln, so die Umweltorganisation.

„Wenn wir uns überlegen, dass der weltweite Datenverkehr jedes Jahr um 25 Prozent ansteigt, dann müssen wir ganz offensichtlich dringend darüber nachdenken, welche Inhalte wir über die Netzwerke schicken", sagt Zeynep Kahraman-Clause (Projekt-Managerin des „Shift Project").

Der sogenannte *Rebound-Effekt* ist das eigentliche Problem: Die steigende Energieeffizienz neuer digitaler Technologien führt eben nicht dazu, dass weniger Strom verbraucht werde. Ganz im Gegenteil: Die Möglichkeiten werden immer komplett ausgereizt; der Gesamtstromverbrauch steigt weiter an. Der Rebound-Effekt ist seit 150 Jahre bekannt: Dem britischen Ökonomen William Stanley Jevons war 1865 aufgefallen, dass die Dampfmaschine von James Watt zwar effizienter Kohle verbrannte als zuvor, aber damit nahm die Industrialisierung erst richtig Fahrt auf. Insgesamt wurde viel mehr Kohle verbraucht als vor der Erfindung der sparsameren Dampfmaschine. In dieses Muster reihen sich viele der alltagstauglichen technischen Innovationen ein: On-

99 Wissenschaftlicher Beirat „Globale Umweltveränderung", April 2019

100 https://theshiftproject.org/wp-content/uploads/2019/11/2019-11-07_Synthesis-Report_Exploring-Futures-to-Plan-Energy-Transition_The-Shift-Project.pdf

linezeitung statt Printausgabe, Emails statt Briefe, Musikstreaming statt CD, ...

Bei einem Großteil der Strom-Verbraucher sorgt vor allem die Produktionsphase für eine schlechte Umweltbilanz. Knapp die Hälfte der Emissionen entstehen bei der Herstellung. Bei einem Smartphone sei die Energiebilanz besonders verheerend: Ausgehend von einer zweijährigen Nutzung sind bereits 90 Prozent der Energie im Lebenszyklus eines solchen Telefons verbraucht, bevor ein Kunde das Gerät überhaupt gekauft habe.

STROMHUNGRIGE KI SOLL DAS KLIMAPROBLEM LÖSEN

Zum Energiebedarf der KI errechnet eine Studie des MIT, dass der CO2-Fußabdruck für das Training eines einzigen modernen „neuronalen Netzes" (einer derzeit besonders erfolgversprechenden Art „künstlich-intelligenter" Algorithmen) dem fünffachen CO2-Fußabdruck des Lebenszyklus' eines Kraftfahrzeugs inklusive seines Verbrauchs entspricht. Oder anders verglichen: Anstelle eines KI-Trainings kann man über 300 Mal von San Francisco nach New York und zurück fliegen.

Die Wissenschaftler*innen betrachten dabei Modelle aus der Verarbeitung natürlicher Sprache. Für eine einzelne Berechnung eines sogenannten *Deep-Learning-Modells* (einer populären Variante künstlicher neuronaler Netze) sind die Stromkosten vergleichsweise gering. Was aber viel Energie verbraucht, ist das Einstellen optimaler Parameter. Da es sich um ein hochdimensionales Optimierungsproblem mit vielen verschiedenen Parametern handelt, und da aus der Wahl nicht direkt auf eine Verbesserung oder Verschlechterung geschlossen werden kann, sondern erst das „neuronale Netz" neu trainiert werden muss, ist es üblich, die Parameter zu erraten und verschiedene Konfigurationen durchzuprobieren, um die besten Ergebnisse zu erzielen. Der Parameterraum ist allerdings zu groß um sämtliche Möglichkeiten durchzuprobieren.

Bislang sind Prognosen des Hasso-Plattner-Instituts, „Clean IT" könnte zu Energieeinsparungen im Bereich der KI-Anwendungen um den Faktor 20 führen, einen Beweis schuldig geblieben. Neben dem reinen Stromverbrauch ist für die ökologischen Folgen natürlich auch relevant, wo die Betreiber der Infrastruktur ihren Strom beziehen. Die MIT-Wissenschaftler*innen zitieren dabei einen Vergleich von Greenpeace. Während in Googles Rechenzentren angeblich „immerhin die Hälfte" des Stroms aus „erneuerbaren"[101] Energien stammt, entspricht Amazons Strommix trotz ökologischer Versprechen immer noch dem US-amerikanischen Durchschnitt – größtenteils fossile Energieträger mit sogar einem Drittel aus Kohlekraftwerken.

ELEKTROMOBILITÄT

Das E-Auto ist ein Alptraum. Der angesagte *Plugin-Hybrid* (Elektro+Verbrennungsmotor) ist besonders unsinnig: er dient nur den Auto-Herstellern beim Weiterverkauf einer Fahrzeugflotte mit übergewichtigen und hoch-motorisierten SUV. Zum einen lassen sich Milliarden an EU-Fördergeldern kassieren, zum anderen bewahren Hybrid-Autos die großen Hersteller vor Strafzahlungen wegen Nichterreichens der europäischen Klimavorgaben, da sie mit angeblichen Zero-Emissionsmodellen den Ausstoß im Flottenmix nach unten drücken. Es geht selbstredend auch um ein „grünes" Markenimage und um Technologiekontrolle. Man baut Hybrid-Autos im Wissen, dass sie alles andere als die automobile Zukunft sein werden.

Aber auch reine Elektro-Fahrzeuge lösen keine Klimaprobleme: Der Bau eines Akkus für einen Tesla ist so umweltschädlich wie acht Jahre Betrieb eines Verbrennungsmotors. Und dieser Akku hat wegen der begrenzten Ladezyklen nach acht Jahren nur noch Schrottwert. Aus diesem Grund fällt die Öko-Bilanz für *E-Scooter* (Elektro-Tretroller) mit deren noch geringerer Akku-Haltbarkeit von nur wenigen Monaten besonders katastrophal aus. Die Fertigung von Elektro-Autos stößt zudem an Ressourcengrenzen, wenn es um die benötigten Rohstoffe für den Bau von Akkus geht. Deren Abbau in Chile (Lithium) und Zentralafrika (Kobalt) ist nicht nur extrem umweltunverträglich, sondern geht in weiten Teilen mit unvertretbarer Kinderarbeit einher. Der Bedarf an Lithium allein in der E-Mobilität steigt bis 2030 auf das 20-40fache. Daran ändert auch die zukünftig anvisierte Feststoff-Batterie nichts – auch sie benötigt Lithium. Für Kobalt sieht die derzeitige Prognose sogar noch dramatischer aus: »Würde Audi den A4 in großer Serie rein elektrisch bauen, müssten sie den halben Weltmarkt an Kobalt leer kaufen.« (Professor Jörg Wellnitz von TH Ingolstadt). Bei VW – so Wellnitz – habe man so eine Rechnung schon mal aufgemacht und sei zu dem Ergebnis gekommen, dass der Konzern für seine Produktion von E-Autos rund 130 000 Tonnen Kobalt benötigen würde. Die Weltproduktion liegt derzeit bei 123 000 Tonnen.

Wenn uns nun auch noch das E-Flugtaxi als Mobilitätskonzept der Zukunft verkauft wird (um dem Problem der zu hohen Verkehrsdichte am Boden zu begegnen), dann klingt das wie ein Rückfall in die 50er Jahre des letzten Jahrhunderts. Damals wie heute war und ist klar, dass jegliche Art des Fliegens einen deutlich höheren

101 https://www.versobooks.com/blogs/3797-end-the-green-delusions-industrial-scale-renewable-energy-is-fossil-fuel

Energieaufwand bedeutet, als die gleiche Strecke am Boden zurückzulegen. Dennoch bekommen wir nun 70 Jahre später erneut Drohnen-ähnliche Flugtaxis als moderne und vermeintlich ökologische Form der Fortbewegung angepriesen. Selbst optisch haben sie sich nur wenig von den futuristischen Männerfantasien der technokratischen Blütezeit entfernt (siehe Abbildungen) – Retro-Futurismus der primitiven und rückschrittlichen Sorte. Die damalige, blinde Fortschrittsgläubigkeit halluzinierte übrigens atomgetriebene Fahrzeuge herbei, die sich im Jahr 2000(!) innerstädtisch mit bis zu 300 km/h und außerhalb geschlossener Ortschaften mit bis zu 1000 km/h schnell bewegen würden. Eine nicht ganz treffende Prognose für einen Individualverkehr, der in den Ballungsgebieten täglich mehrere hundert Kilometer Stau produziert.

Die Technokratie gibt sich hier äußerst konservativ. Sie versucht den Automobilismus einfach fortzusetzen, indem sie vom Verbrenner- auf den E-Antrieb umsteigt und ansonsten die Verkehrskonzepte aus dem letzten Jahrhundert unverändert beibehält. Ein zweieinhalb Tonnen schwerer 600-PS-Elektro-Porsche muss als trotzig-zynische Antwort der deutschen Automobil-Branche auf die Klima- und Mobilitätskrise verstanden werden.

Ohne eine grundlegende Abkehr von den derzeitigen, völlig überkommenen Mobilitätsvorstellungen des automobilen Individualverkehrs wird es nicht möglich sein, den Klimawandel auf ein langfristig überlebbares Maß zu reduzieren. Wer an einer Expansion des Welthandels und des Tourismus festhält und dabei glaubt, unser Lebensstandard ließe sich (technologisch innovativ) auf den restlichen Teil der Weltbevölkerung verallgemeinern, beraubt sich jeglicher Chance, diesen Planeten vor dem Kollaps zu bewahren. In nahezu allen Bereichen werden vermeintlich innovative Energie-Effizienz-Steigerungen durch den „Rebound-Effekt" aufgefressen.

RENAISSANCE DER ATOMKRAFT?

Als Anfang der 1950er Jahre der Wohlstand spürbar zunahm, begann eine Phase eines geradezu euphorischen Fortschritts- und Technikglaubens. Konzeptfahrzeuge von atomkraftbetriebenen Autos wurden vorgestellt. Die Genfer Atomkonferenz (1955), das Bundesministerium für Atomfragen (ab Oktober 1955; erster Minister: Franz Josef Strauß) und die Deutsche Atomkommission (1956) brachten den politischen Durchbruch der Kernenergie in Westdeutschland.

Rund 50 Jahre ist es her, dass sich erstmals überregional Widerstand gegen die atomare Stromerzeugung regte. Riskant, gesundheitsschädlich, zerstörerisch und zentral herrschaftssichernd – diese Aspekte sind mit der Atomenergie verbunden. In den vergangenen Jahrzehnten stieg mit den großen atomaren Unfällen in Tschernobyl 1986 sowie Fukushima 2011 die Skepsis gegenüber dieser Form der Energieerzeugung. In Deutschland wurde nach dem Super-GAU in Japan der „endgültige Ausstieg" aus der Atomkraft besiegelt. 2022 sollen die letzten Meiler abgeschaltet werden. Jetzt im Zuge des (halbherzigen) „Kohleausstiegs" scheinen einige in der CDU den Rückwärtsgang einlegen zu wollen. Ein Positionspapier erwägt die Rückkehr zur Kernkraft. Erstellt hat das Dokument der Bundesfachausschuss Wirtschaft, Arbeitsplätze und Steuern. Wasser auf die Mühlen des konservativen Flügels: Man wolle „Technologie-offen" bleiben. Auf der Liste der Unterstützer*innen dieser Idee steht unter anderem die internationale Energieagentur IEA, die Subventionen für die nukleare Energieerzeugung fordern. In ihren Analysen wird Atomenergie in einem Zug mit Erneuerbaren Energien als klimafreundliche Energiequelle genannt.

Das ist nachweisbar grober Unfug. Nur wer den Blick auf den Reaktorbetrieb einschränkt, kann ein AKW klimagasfrei nennen – wenn die gesamte Kette Bergbau, Aufbereitung, Anreicherung, Transport, Kernspaltung berücksichtigt wird, entspricht der Klimagasausstoß eines AKW dem eines Gaskraftwerks – das ungelöste Entsorgungsproblem noch nicht mal eingerechnet. Um Kohle, Öl und Gas zu ersetzen, müssten hunderte AKW gebaut werden. Beim derzeitigen Verbrauch von Uran beträgt dessen Reichweite nur ein paar Jahrzehnte. Kommen hunderte neuer Anlagen dazu entsprechend weniger. AKW werden für Laufzeiten von etwa 40 Jahren kalkuliert – wenn viele neue Anlagen hinzukommen, geht diese Rechnung nicht mehr auf.

Der sogenannte „*energy cliff*" beschreibt den Moment, bei dem zur Herstellung eines Brennstoffes gleich viel Energie reingesteckt wird, wie dieser dann freisetzen kann. Bei Uran ist die kritische Stelle der Abbau. Ab einer Konzentration von 0.04 % Uran im Erz ist der „cliff" erreicht: Bei niedrigerer Konzentration ist es wirtschaftlicher die Energie, die in den Abbau gesteckt wird, direkt zu nutzen und das Uran in der Erde zu lassen. Aktuelle (neue) Minen bauen bereits Erz mit weniger als 1 % Urangehalt ab – der cliff ist nicht mehr weit. Ergo: Atomenergie als Lösung des Klimawandels zu propagieren ist Augenwischerei.

Die EU-Kommission hat im Dezember 2019 einen Plan vorgestellt, Europa bis 2050 zum ersten klimaneutralen Kontinent der Welt zu machen. Darin spielt die Kernenergie keine Rolle, allerdings steht das Vorhaben noch unter dem Vorbehalt der Zustimmung der Mitgliedstaaten. Diese streiten noch über die Frage der Atomkraft. Auf Druck osteuropäischer Länder und Frankreichs

nannte der EU-Gipfel der Staats- und Regierungschefs Atomkraft als mögliche Energiequelle auf dem Weg zur Klimaneutralität. Eine politisch geförderte Rückkehr der Dinosaurier wäre ein GAU für die Umweltbewegung. Diese muss nun unmissverständlich deutlich machen, dass jede nukleare Option an ihrem heftigen und breiten Widerstand scheitern würde.

ÖKOLOGISCHE VERHALTENSLENKUNG – SMARTER BEHAVIORISMUS

Die Glaubwürdigkeit der Technokrat*innen, das Klimaproblem rein technologisch in den Griff zu kriegen, schwindet zusehends. Selbst in einer Ingenieurs-geprägten Gesellschaft wie der französischen, die zudem nicht auf ein besonders ausgeprägtes Umweltbewusstsein zurückgreifen kann, schwindet seit den beiden unerträglich heißen bzw. extrem trockenen Sommern 2018 und 2019 der Fortschrittsglaube der Bevölkerung an die Fähigkeiten der Technokratie. Im Gegenteil, die „Kollapsologen" sind in der öffentlichen Debatte immer stärker vertreten. Die „Kollapsologie" als interdisziplinärer Wissenschaftsansatz – weit über die engen Grenzen der Umweltwissenschaften hinaus – gibt es seit dem 2015 von Pablo Servigne und Raphaël Stevens erschienenen Essay „Wie alles zusammenbrechen kann – kleines Kollapsologie-Handbuch für gegenwärtige Generationen". Darin gehen die Autoren von einer höchst wahrscheinlichen Unfähigkeit des Kapitalismus aus, den ökologischen Zusammenbruch verhindern zu können.

Mit einem weiter schwindenden Vertrauen in den technologischen „Fortschritt" versucht der Kapitalismus seine „Nachhaltigkeits"-Glaubwürdigkeit anders herzustellen und gleichzeitig die Ressource Mensch besser inwertsetzen zu können. Smarte (algorithmische) Verhaltenslenkung, basierend auf einer eher rückschrittlichen Auslegung des „Behaviorismus", steht (nicht nur in China!) hoch im Kurs. Die Zukunftsvision vieler Tech-Giganten einer paternalistisch geführten Welt fußt auf der Idee dieses Behaviorismus. Ein persönliches Journal „sämtlicher Handlungen, Entscheidungen, Vorlieben, Aufenthaltsorte und Beziehungen" soll die Grundlage sein für ein System digitaler Assistenz, das KI-basiert auf jeden Einzelnen zugeschnittene „Handlungsempfehlungen" ausspricht. Angesichts „zu komplexer Lebensverhältnisse" gehen z. B. die Visionär*innen von Google von einer notwendigen Verhaltenssteuerung andernfalls nicht-rational handelnder Individuen aus – ein paternalistisches und rückschrittliches Menschenbild. Mehr Retrotopie, als technologie-affine Utopie.

SMART-CITY ALS DURCHSETZUNGSRAHMEN

Realisiert sehen wir die teilweise geradezu „totalitär" anmutende Rückbesinnung auf den Behaviorismus derzeit in vielen Smart-City Ansätzen – vorgeblich zugunsten einer vermeintlich besseren und ökologischeren Lebensweise:

In einem Pilotprojekt in der als ökologische Vorzeigestadt in der Wüste Abu Dhabis konzipierte Retorten-Stadt *Masdar* City unter der Leitung von Professor Scott Kennedy (Masdar Institute) wurde bereits vor mehr als zehn Jahren der individuelle Energie- und Wasserverbrauch überwacht und verschiedene Anreizmechanismen zum Einsparen getestet. Grundvoraussetzung für das System war, dass in jeder Wohnung der Verbrauch von Strom sowie kaltem und warmem Wasser minutengenau gemessen wurde. Heute sind wir mit der Einführung der Smart Meter und zeitvariabler Stromtarife diesem Prototyp der ökologischen Verhaltenslenkung sehr nah.

Die „grüne" Stadt" *Songdo* in Südkorea findet in ihrem „technologisch deterministischen Ansatz" als geschlossen gedachtes System keine Antworten auf die „komplexen Herausforderungen" urbanen Lebens. Mit ihren rigide formalisierten Steuerungsparametern wird der grüne Smart City-Ansatz den unterschiedlichen Möglichkeiten verschiedener Bevölkerungsschichten beim Zugang zu städtischen Dienstleistungen nicht gerecht. „Die Stadt wurde derart vorrangig als technologisches System gedacht, dass soziale Dimensionen in Songdo's Smart-City-Vokabular gar nicht erst vorkamen." (Paul D. Mullins)[102]

In mehreren Großstädten Chinas wurde 2017 auf öffentlichen Toiletten eine Gesichtserkennung eingeführt, um den übermäßigen Verbrauch an Toilettenpapier einzudämmen. Ein Automat händigt eine fest kontingentierte maximale Tagesmenge Toilettenpapier aus. Das klingt fast unglaubwürdig absurd: Ökologie-Erziehung mit schwerem Geschütz oder aber die gewöhnende Einübung einer permanenten Präsenz digitaler „Assistenz"? Beides sind gleichermaßen ernst zu nehmende Motive. Jetzt mag mensch einwenden, dass China in Alleinstellung ja doch eh sämtliche Lebensäußerungen nutzt, um die KI-Algorithmen seiner „Sozialen-Punkte-Systeme" mit möglichst vielen Alltags-Datensätzen zu füttern. Das stimmt – bis auf die Alleinstellung. Manche europäische Smart-City-Projekte zur „Ökologisierung" erscheinen da nur unwesentlich sinnvoller: Ein Pilotprojekt zur personalisierten Abfallentsorgung in

102 Paul D. Mullins, 2017, „The Ubiquitous-Eco-City of Songdo: An Urban Systems Perspective on South Korea's Green City Approach", Urban Planning (ISSN: 2183–7635)2017, Volume 2, Issue 2

den Niederlanden sollte RFID-gesteuert erkennen, wer berechtigt ist welche Mülltonne zu befüllen – angeblich um Missbrauch zu verhindern bzw. zu detektieren. Der Überwachungseifer zugunsten der Quantifizierbarkeit vermeintlich relevanter Parameter scheint auch außerhalb Chinas extrem zu sein. Das Projekt wurde jedoch durch Verweigerung und Sabotage der Probanden (zunächst) wieder zu Fall gebracht.

Auch in Deutschland schätzen Technokrat*innen die Möglichkeit einer versteckten top-down-Bevormundung zu umweltbewussterem Verhalten. So schreibt das Bundesinstitut für Bau-, Stadt- und Raumforschung in einer Bestandsaufnahme unterschiedlicher Smart-City-Ansätze: „Um den Nutzer der städtischen Infrastrukturen zu bestimmten, zum Beispiel ökologisch wertvollen Verhaltensweisen zu motivieren, (...) testen die Städte verschiedene Anreiz- und Aktivierungsmodelle. Hier werden mithin neue Formen des städtischen Regierens in Form einer gewollten Steuerung von Verhaltensformen erprobt."[103]

Es ist skurril: Wir erleben aktuell einen „postfaktischen" Zerfall der Realität in konkurrierende „Wahrheiten" und gleichzeitig wird DIE Wahrheit – als faktisch verbindliche Lebensrealität der einen Welt, in der wir nun mal leben – algorithmisch durchgesetzt, ohne wahrnehmbaren Expert*innenstreit und ohne gesellschaftlich ausgehandelte, transparente Regeln. Der nicht einsehbare Code einer *Smartifizierung* urbanen Lebens bestimmt schleichend und schwer angreifbar unser Verhalten. Hierzu benötigt die Technokratie nicht einmal mehr einen Vertrauensvorschuss.

Angesichts der Dringlichkeit eines irreversiblen Klimawandels erscheint es überlebensnotwendig, sich von der Technokratie aktiv abzuwenden und anzuerkennen, dass eine grundsätzliche und einschneidende Änderung unserer Wirtschafts- und Lebensweise notwendig ist.

103 Smart Cities International, Bundesinstitut für Bau-, Stadt- und Raumforschung (BBSR)

Hongkong

*Seit dem 9. Juni 2019 gibt es erneut Proteste in Hongkong. Die Demonstrationen erreichen eine Größe von bis zu zwei Millionen Menschen. Die Bewegung organisiert sich dezentral und anführer*innenlos. Dadurch unterscheidet sie sich stark von früheren Protestzyklen. Bemerkenswert ist auch, dass die Organisierung stark auf digitalen Technologien basiert. Im Folgenden wird versucht, die Geschehnisse einzuordnen und die Kommunikationsformen der Massenproteste zu analysieren, um daraus zu lernen.*

Dies beinhaltet sowohl die gesellschaftliche Dynamik zu verstehen, als auch methodisch zu lernen und technische sowie subversive Aspekte abzuschauen.

Für eine detaillierte Auseinandersetzung mit den gesellschaftlichen Hintergründen und eine Einordnung des Protests, verweisen wir auf zwei Artikel von CrimethInc[104].

KONTEXT

Im Jahr 1997, nach etwa 140 Jahren Kolonialherrschaft durch Großbritannien, wurde durch eine chinesisch-britische Erklärung, Hongkong der Volksrepublik China übergeben. Die Volksrepublik sicherte in dieser zu, dass Hongkong entsprechend dem Grundsatz „ein

104 CrimethInc. Hong Kong: Anarchists in the Resistance to the Extradition Bill – An Interview. 22.06.2019. https://crimethinc.com/2019/06/22/hong-kong-anarchists-in-the-resistance-to-the-extradition-bill-an-interview und CrimethInc. Three Months of Insurrection – An Anarchist Collective in Hong Kong Appraises the Achievements and Limits of the Revolt. 20.09.2019. https://crimethinc.com/2019/09/20/three-months-of-insurrection-an-anarchist-collective-in-hong-kong-appraises-the-achievements-and-limits-of-the-revolt

Land, zwei Systeme“ weitere 50 Jahre nach der Übergabe ein liberal-kapitalistisches Wirtschaftssystem behalten und in dieser Zeit eine Sonderverwaltungszone bilden werde, sodass Hongkong bis 2047 über ein eigenes politisches und rechtliches System verfügen soll. Seit der Übergabe gab es einige Gesetzesvorhaben, die eine Annäherung bewirken sollten und zu Protesten führten.

Beispielsweise 2003 Proteste mit bis zu 700.000 Menschen (bei einer Bewohner*innenzahl von ca. 7 Millionen) gegen einen Versuch, eine Anti-Subversionsgesetzgebung einzuführen (National Security Legislative Provisions Bill 2003, gemeinhin als Artikel 23 bezeichnet). Als Vorwand dienten Hochverrat, Aufruhr und Subversion gegen die chinesische Regierung und der Diebstahl von Staatsgeheimnissen. Doch viele Menschen befürchteten die Einschränkung vieler bürgerlicher Freiheiten, insbesondere freie Meinungsäußerung. Die große Zahl der Demonstrant*innen zwang eine große Regierungspartei, ihre Unterstützung für den Gesetzentwurf rückgängig zu machen.

Im Jahr 2012 versuchten die Behörden, den Lehrplan des Hongkonger Schulsystems zu ändern und Themen zur Geschichte und Kultur Chinas sowie zur nationalen Identität aufzunehmen. Viele Schüler*innen, Eltern und Lehrer*innen lehnten diese Idee ab. Bis zu 400.000 Menschen nahmen am 29. Juli 2012 an einem Protest gegen die Curriculum-Reform teil. Im September wurde den Schulen bei der Umsetzung des Lehrplans ein Ermessensspielraum eingeräumt. Dadurch war die Reform praktisch vom Tisch.

2014 entstand die Regenschirm-Bewegung aus einem Gesetzesvorhaben aus Beijing für eine Wahl-Reform. Vorschläge, den Wähler*innen nur eine Auswahl aus einer von Beijing überprüften Liste von Kandidat*innen zu gestatten, wurden von einem Großteil der Bevölkerung abgelehnt. Die Proteste gewannen an Dynamik, nachdem es zu Zusammenstößen zwischen Bullen und meist jungen Demonstrant*innen gekommen war, die versuchten, einen öffentlichen Platz zurückzufordern, der nach den Protesten von 2012 gesperrt worden war. Ereignisse, die die Regenschirm-Bewegung geprägt haben, sind eine für viele erschreckende Machtdemonstration der Bullen, wonach sich die öffentliche Empörung in riesigen Demos und anschließenden Besetzungen manifestierte. Organisiert und verstanden als friedliche Demonstrationen der Staatsbürgertugend. Menschen besetzten etwa zehn Wochen die Straßen um Regierungsgebäude und Bürotürme im Finanzzentrum, erstickten den Verkehr und machten wichtige Durchgangsstraßen unpassierbar. Besetzungen tauchten auch in Causeway Bay auf – einem bei Tourist*innen und Einkäufer*innen beliebten Gebiet – und in Mong Kok, einem Arbeiter*innenviertel auf der Halbinsel Kowloon. Da sich die Bewegung aber vor allem dadurch ausgezeichnet hat, das Verhalten aller mit einem vorgeschriebenen Skript (dos and don‘ts) in Einklang zu bringen, brach die Bewegung zusammen. Es gab aber auch viele neue und emanzipatorische Praktiken und Begegnungen, die nicht in der offiziellen Erzählung aufgingen. Die Besetzung endete ohne Zugeständnisse von Beijing und die öffentliche Meinung wandte sich gegen die Besetzung. Nach 79 Tagen entfernten die Bullen gewaltsam die verbliebenen Demonstrant*innen, die Transparente an Brücken und Schilder mit dem Versprechen „Wir kommen wieder“ auf ihren Campingplätzen verstreut hinterließen.

Am 8. Februar 2016 kam es zu Ausschreitungen – den sogenannten ‚Fishball-Riots‘ – gegen ein hartes Vorgehen gegen Straßenverkäufer*innen (nicht lizenzierte Lebensmittelverkäufer*innen) im Stadtteil Mong Kok. Sie waren eine sich steigernde Explosion der Wut gegen die Bullen und ein völlig unerwartetes Nachbeben nach dem Zusammenbruch der Regenschirm-Bewegung. Die Lebensmittelhändler*innen waren wütend, als Beamte versuchten, ihre Stände aus Gesundheits- und Hygienegründen zu schließen. Aber dies war nicht nur ein Kampf um Lebensmittelvorschriften. Aktivist*innen begannen, sich um die Fischverkäufer*innen zu scharen.
Im selben Jahr entstanden aber auch vermehrt Unabhängigkeitsgruppen (darunter auch die inzwischen verbotene Hong Kong National Party), welche die vollständige Unabhängigkeit Hongkongs vom Festland forderten.

In diese Reihe lassen sich auch die aktuellen Proteste einreihen, denn sie entstanden aus einem Gesetzesvorhaben im Februar 2019, das es ermöglichen sollte, Menschen in Länder auszuliefern, mit denen die Regierung Hongkongs keine bestehenden Auslieferungsabkommen hat – einschließlich Festlandchina. Am 9. Juni gingen über eine Million Menschen auf die Straße, am 12. Juni nahmen Demonstrant*innen an Konfrontationen mit den Bullen teil; am 16. Juni beteiligten sich zwei Millionen Menschen an der bisher größten Demo in der Geschichte der Stadt.

Der Protest geht durch alle Milieus. Die Gründe sind vielfältig: Teils sind sie progressiv, teils ist es schlicht Angst vor dem autoritären System der Volksrepublik. Aber wie fast überall, ist die primäre Form der Identifikation, der sich viele anschließen, und der Antrieb für soziale Kämpfe in dieser Stadt, die Idee der Staatsbürgerschaft in einem nationalen Rahmen. Daraus folgt, dass diese imaginäre Zugehörigkeit auf Negation, Ausgrenzung und Abgrenzung vom Festland beruht. Darüber hinaus ist es keine Übertreibung zu sagen, dass der Gründungsmythos dieser Stadt darin besteht, dass Dissident*innen vor der kommunistischen Verfolgung

geflohen sind, um eine Oase des Reichtums und der Freiheit zu erbauen, eine Festung der bürgerlichen Freiheiten, geschützt durch die Herrschaft des Rechtsstaats. Geflüchtete aus Festlandchina wurden als Verbündete im gemeinsamen Kampf gesehen. Mit der Übergabe Hongkongs an Festlandchina nahm die Anzahl der Geflüchteten ab und die Zahl der durchaus wohlhabenden Tourist*innen und Geschäftsleute zu. Die Folge war ein Prozess der Gentrifizierung, von dem sich die Einheimischen an den Rand gedrängt fühlen. Das Verhältnis zu Menschen aus Festlandchina kippt in nationalistische Ablehnung.

So, wie viele Menschen leidenschaftlich für eine Regierung sind, die „wirklich für sie" ist, wünschen sie sich auch einen Kapitalismus, der „wirklich für sie" arbeitet: einen Kapitalismus frei von Korruption, politischer Gängelung und dergleichen. Die „freie Marktwirtschaft" wird von vielen als zentrales Merkmal der kulturellen Identität Hongkongs angesehen, die sie von dem von der Kommunistischen Partei verwalteten „roten" Kapitalismus unterscheidet. Wann immer diese Werte gefährdet werden, werden sie verteidigt und in der Öffentlichkeit inszeniert.

Dynamik und Moral dieses Kampfes im gesamten sozialen Spektrum ist eine ständige Anrufung des „Hongkonger Volkes", das dazu angespornt wird, sein Zuhause um jeden Preis zu schützen. Das verleiht den Ereignissen einen ausgesprochen konservativen und reaktionären Beigeschmack – egal wie radikal und dezentral die neuen Aktionsformen sind. Nationalismus bietet einen identitären Kitt, der in der Lage ist, widerstrebende Positionen zusammenzuhalten, indem sie unsichtbar gemacht werden. Eine zutiefst beunruhigende Einstimmigkeit, die viele soziale Probleme überdeckt.

„Die Linke" ist in Hongkong institutionalisiert und ineffektiv. Im Allgemeinen haben die Liberalen der sogenannten „scholaristischen" Fraktion der Student*innen und "bürgerliche" Rechte bei Protesten, insbesondere wenn Festlandchina beteiligt ist, die Narrative fest im Griff. Das Wort „links" hat in Hongkong zwei Konnotationen. Für die ältere Generation bedeutet „links" kommunistisch. Deshalb kann sich „links" auf einen Geschäftsmann beziehen, der Parteimitglied ist, oder auf einen etablierten, notorisch pro-chinesischen Politiker. Für jüngere Menschen ist das Wort „Links" ein Stigma, das mit einer Generation von Aktivist*innen verbunden wird, die in einen früheren Zyklus sozialer Kämpfe involviert waren, darunter Kämpfe gegen den Abriss des Queen's Ferry Pier im Zentrum, gegen den Bau des Hochgeschwindigkeitszuges durch den Nordosten von Hongkong nach China und gegen die Zerstörung großer Teile des Ackerlandes in den Territorien des Nordostens, die alle mit demoralisierenden Niederlagen endeten. Diese Bewegungen wurden oft von Sprecher*innen (meist Künstler*innen oder NGO-Vertreter*innen) angeführt, die taktische Allianzen mit Progressiven in der pan-demokratischen Bewegung schlossen. Die Niederlagen dieser Bewegungen, die auf ihre Vorbehalte gegen direkte Aktionen und ihre Zurückhaltung und Geduld bei Verhandlungen mit den Behörden zurückzuführen sind, wird dieser Aktivist*innengeneration nun angelastet. All die Wut und der Frust der in dieser Zeit aufgewachsenen jungen Menschen, die auf die Beschwichtigungen jener Galionsfiguren gehört und jede Niederlage passiv hingenommen haben, haben mit der Zeit eine Orientierung nach rechts eingeleitet. Ein entscheidender Grundsatz dieser Generation, der auf die massiven Enttäuschungen und Misserfolge zurückgeht, ist ein Fokus auf direkte Aktionen und die konsequente Ablehnung von „Kleingruppendiskussionen", „Konsens" und dergleichen. Ein Thema, das erstmals in der Regenschirm-Bewegung auftauchte, vor allem im Camp in Mong Kok, wo die Möglichkeiten am größten waren, aber wo sich leider auch die Rechte fest etablieren konnte. Das Misstrauen gegenüber der vorherigen Generation ist nach wie vor groß. Darüber hinaus sind die sichtbaren, anerkannten Protagonist*innen früherer Protestzyklen besiegt, diskreditiert oder inhaftiert. Dazu zählen sowohl politische Parteien und Student*innenenbewegungen, aber auch rechte und populistische Gruppen.

Nichtsdestotrotz muss man differenzieren. Nationalismus in der BRD ist ein anderer als ein Nationalismus in Hongkong, Katalonien oder beispielsweise in einem ehemaligen Satellitenstaat der UdSSR, da er jeweils in einem historischen Kontext entsteht. Selbst innerhalb von Europa ist es nicht leicht, nationalistische Tendenzen treffend zu bewerten. Hongkongs Geschichte der Kolonialherrschaft ist ganz wesentlich für die Konstruktion eines gemeinsamen „Wir" gegen „Die" (erst Großbritannien, jetzt China) – also der Schaffung eines Kollektivs zur gemeinsamen Abwehr der Fremdbestimmung. Trotzdem bleibt es ein Nationalismus, der zu benennen und zu bekämpfen ist!

Wichtig ist, in dieser Bewegung progressive Kräfte zu suchen und zu identifizieren, wie sie auf die Bewegung wirken. Anarchist*innen, Hacker*innen und Hacktivist*innen sind in der Bewegung aktiv. Ihre Taten und Einflüsse gehen leider nicht in der aktuellen öffentlich wahrnehmbaren Erzählung auf.

DER AKTUELLE PROTEST

Im Gegensatz zur Regenschirm-Bewegung 2014 sind die aktuellen Protestformen sehr divers. Die Bewegung ist nicht so friedlich wie jene 2014, sondern es kommt

immer wieder zu vielen Auseinandersetzungen mit den Bullen. Allerdings – und das ist anders zu vorherigen Protesten – lässt sich der Protest daran nicht spalten.

Eine Lehre aus der Regenschirm-Bewegung war, keine Anführer*innen zu haben, weil diese während und nach den Protesten 2014 massive Repression erfahren haben und ihre Inhaftierung Lücken in die Organisierung gerissen hat, die erst wieder mühsam gefüllt werden mussten. Anstatt auf Personen zu setzen, organisiert sich dieser Protest rund um Debatten und Diskurse. Das führt entsprechend zu neuen Anforderungen an die Art der Organisierung, der Kommunikation und der Entscheidungsfindung.

Durch einen partizipativen Prozess können Aktivist*innen zusammenarbeiten, indem sie unterschiedliche Taktiken ausprobieren und die nächsten Schritte in einer egalitären Weise planen, bei der alle gleichberechtigt mitreden können. Telegram-Chat-Gruppen und Online-Foren mit Abstimmungsmechanismen für kollektive Entscheidungen haben diese Art der flexiblen Koordination erleichtert. Die Annahme einer Vielfalt von Taktiken hat es den Teilnehmer*innen ermöglicht, sich auf verschiedenen Handlungsebenen zu engagieren und gleichzeitig die Rollen zu respektieren, die andere spielen.

Es gibt keinen Konsens, der bestimmte Handlungen zulässt und andere verbietet. Dies steht in direktem Gegensatz zu den Protesten von 2014, bei denen mehrere Protestgruppen sich gegenseitig kritisierten. Die Minimierung interner Konflikte wird als Schlüssel zur Erreichung gemeinsamer Ziele gesehen. Das Motto lautet: Wir kämpfen unterschiedlich, aber mit einem gemeinsamen Ziel. Insbesondere gibt es fünf Forderungen, die nach und nach kollektiv erarbeitet wurden und von fast allen getragen werden:

1. Komplette Rücknahme des Gesetzesentwurfs,
2. Freilassung aller gefangengenommenen Aktivist*innen,
3. Rücknahme der Charakterisierung jedes Protests als Aufstand,
4. unabhängige Untersuchung von Polizeibrutalität,
5. Rücktritt der Regierungschefin Carrie Lam und Implementierung eines vollständigen und universellen Wahlrechts.

Die Forderungen 2 bis 4 ergaben sich durch massive Repression mit bisher über 6000 Festnahmen mit Anklagen bis zu zehn Jahren Haft (wegen Rioting).

Neu in der aktuellen Situation ist, dass viele Menschen realisieren, dass Solidarität mit dem Kampf, auch wenn sie nur geringfügig ist, zur Verhaftung führen kann. Diese Haltung und mentale Vorbereitung auf Inhaftierung war früher auf „professionelle Aktivist*innen" an der Spitze sozialer Bewegungen beschränkt. Gleichzeitig gibt es keine Diskussion darüber, was Staat und Recht eigentlich sind, wie sie funktionieren oder welche Legitimität Bullen und Gefängnisse als Institutionen haben. Die Menschen haben einfach das Gefühl, dass sie über das Gesetz hinausgehen müssen, um die Heiligkeit des Gesetzes zu bewahren, das von korrupten Kommunist*innen verletzt und entehrt wurde. Das beeinflusst auch den Umgang mit Technologie: Vielen ist bewusst, dass sie (digitale) Spuren hinterlassen. Aber das wird in Kauf genommen und, anders als etwa bei Videokameras, werden die Langzeitfolgen eher ignoriert. Kurzfristige Repression (inklusive Haft) wird bedrohlich wahrgenommen. Dies scheint unter anderem deshalb, weil eine Verhaftung bedeuten würde, nicht mehr am Protest teilnehmen zu können. Aber es ist auch Angst vor Auslieferung an China, Gewalt und ökonomischer Ausgrenzung, die Menschen antreibt. Es herrscht Endzeitstimmung und es scheint ein verbreitetes *Mindset* zu sein, dass eine Niederlage keine Option ist.

Während der Straßenproteste haben sich die Methoden des Schwarzen Blocks zur Wahrung der Anonymität durchgesetzt. Die Teilnehmer*innen an Demonstrationen sind zunehmend schwarz gekleidet und tragen Schutzhelme und Handschuhe. Um der polizeilichen Überwachung zu widerstehen und sich vor chemischen Waffen, wie Tränengas und Pfefferspray, zu schützen, sind Gesichtsmasken und Schutzbrillen ebenfalls beliebte Kleidungsstücke. Das Leitmotiv lautet, „Wasser zu sein", was bedeutet, zu fließen und zu brechen, um als Gruppe effektiver zu funktionieren. Die Metapher wurde erweitert, um „stark wie Eis" zu sein, wenn sie den Bullen gegenüberstehen, „sich wie Tau zu sammeln", wenn die Protestierenden Flashmob-Proteste organisieren, und „sich wie Nebel zu zerstreuen", um sicherzustellen, dass die Protestierenden vor der polizeilichen Räumung fliehen können, um einer Verhaftung zu entgehen. Auseinandersetzungen mit den Bullen finden in aller Regel nach der hit-and-run-Taktik statt: Bullen werden angegriffen, dann verstreuen sich die Gruppen, um Festnahmen zu verhindern, bevor weitere Bullen eintreffen oder die Bullen zugreifen können.

Eine weitere Taktik ist die geografische Streuung. Während sich die Proteste in Hongkong 2014 auf drei Orte konzentrierten, verteilten sich die Demonstrationen und Zusammenstöße mit den Bullen im Jahr 2019 auf über 20 verschiedene Stadtviertel, die über Hongkong Island, Kowloon und die New Territories verteilt waren.

Die Bullenpräsenz ist stark, aber die Repression in Hongkong ist bisher noch ganz anders, als beispielsweise in der muslimischen Provinz Xinjiang. Dort geht die

chinesische Zentralregierung mit großer Härte gegen die muslimische Minderheit der 11 Millionen Uigur*innen vor. Bis zu einer Million Menschen sollen zumindest vorübergehend in Umerziehungslagern gefangen worden sein. Die chinesische Regierung will die dortige Unabhängigkeitsbewegung brechen und begründet die Maßnahmen mit dem „Kampf gegen den Terrorismus". Dabei setzt sie, neben der schon implementierten Gesichtserkennung, den intelligenten Brillen für Bullen und dem Sozialkredit-System, auf zusätzliche repressive Mittel. Mittels Videoüberwachung und künstlicher Intelligenz betreibt sie Racial-Profiling, um Mitglieder der uigurischen Minderheit im öffentlichen Raum zu erfassen und zu verfolgen. Im Zentrum des Überwachungsapparates steht eine Plattform mit zugehörigem Algorithmus. Sie bilden zusammen das zentrale Datenerfassungs- und Verarbeitungssystem der chinesischen Regierung, in dem alle als wichtig erachteten Informationen zusammenlaufen und ausgewertet werden. Des Weiteren baut sie eine Biometrie-Datenbank aller Bürger*innen zwischen 12 und 65 Jahren in der Provinz auf. In dieser Datenbank werden Blutgruppe, Fotos des Gesichtes, ein Iris-Scan, Fingerabdrücke und DNA gespeichert. Darüber hinaus setzt sie auch vogelähnliche Drohnen („Dove-Drohnen") zur Beobachtung ein und versieht Muslime und Muslima auf dem Weg nach Mekka und Medina mit GPS-Trackern. Diese massive Repression in Xinjiang hat selbstverständlich auch Einfluss auf die Proteste in Hongkong.

Dass die Repression in Hongkong so verschieden zu der in Xinjiang ist, liegt wahrscheinlich daran, dass Hongkong sich unter der britischen Kolonialherrschaft zu einem (auch für Festlandchina) wichtigen Finanzzentrum entwickelt hat. Private Geldflüsse der Reichen in China (sowohl der Parteieliten, als auch der kapitalistischen Führungsschicht) gehen durch Hongkong. Hier massiv aufzutreten, würde das Finanzkapital verschrecken und vertreiben. Gleichzeitig ist die Drohkulisse real: Festlandchina hat Polizeieinheiten an der Grenze zu Hongkong in Stellung gebracht, die nur noch auf den Einsatzbefehl warten. Andere Maßnahmen, wie etwa das (temporäre) Deaktivieren des Internets, verbieten sich aus dem gleichen Grund.

SOZIO-TECHNISCHE ASPEKTE DES AKTUELLEN PROTESTS

Bemerkenswert ist, wie gesagt, dass die Organisierung stark auf digitalen Technologien basiert. Dies betrifft vor allem Informationsverbreitung, Kommunikationsstrukturen und dezentrale Entscheidungsfindung. Einhergehend sind Fragen der (IT-)Sicherheit und Anonymität sowie Zentralität und Zensur von Diensten.

LIHKG

Das Multi-Kategorie-Online-Forum LIHKG hat als zentrale Anlaufstelle für junge Menschen fungiert, um sich zu organisieren, politische Scharmützel auszutragen und Informationen über den Kampf zu verbreiten. Die Website hat seit ihrer Einführung im Jahr 2016 an Popularität gewonnen und wird oft als die Hongkong-Version von Reddit bezeichnet. Die Website ist bekannt dafür, dass sie eine der Hauptplattformen für die Diskussion der Strategien für die Proteste gegen das Auslieferungsgesetz ist. Zum ersten Mal widmeten sich eine ganze Reihe von Threads auf dieser Website dem Versuch, die Kluft zwischen bürgerlichen und militanten Aktivist*innen zu überbrücken. Alle möglichen Gruppen versuchen, nach ihren Möglichkeiten zum Kampf beizutragen.

Die Registrierung der Mitgliedschaft ist (allerdings) auf Personen mit einer Hongkonger ISP- oder Hochschul-E-Mail-Adresse mit Sitz in Hongkong beschränkt. Folglich ist keine anonyme Nutzung des Forums möglich und die Aktivität ist höchsten pseudonym. Von außen lässt sich nicht direkt die wahre Identität einer Person erschließen. Da das Pseudonym aber an die E-Mail-Adresse gebunden ist, lässt sich die wahre Identität ermitteln.

Registrierte Mitglieder können Themen auf der Website erstellen und Inhalte wie Textbeiträge, Hyperlinks oder Bilder hochladen. Die Beiträge erhalten dann Antworten und können von anderen Mitgliedern nach oben oder unten abgestimmt werden. Die Beiträge werden in verschiedene Kategorien unterteilt. Themen mit mehr Stimmen und Antworten erscheinen am Anfang der Themenabschnitte und, wenn sie genügend Stimmen und Antworten erhalten, erscheinen sie im Abschnitt „beliebt" der Website. So bildet sich dynamisch der Mainstream, wobei selbstverständlich diese Dynamik etwas selbstverstärkendes hat. Das, was „beliebt" ist, findet mehr Beachtung.

Es gab viele Vorschläge für „non-kooperative" Aktionen, wie die Störung einer ganzen U-Bahn durch koordinierte Gruppen, die die Wagen mit Personen und Gepäck verstopfen, oder die Auflösung von Bankkonten und massenhafte Abhebungen, um Inflation zu erzeugen. Einige haben Vorschläge verbreitet, wie Menschen sich der Steuerzahlung für den Rest ihres Lebens entziehen können. Das mag nicht nach viel klingen, aber interessant ist die unermüdliche Verbreitung von Vorschlägen, in allen möglichen Stadtvierteln, von Menschen mit unterschiedlichen Fachkenntnissen, darüber, wie Menschen dort, wo sie leben oder arbeiten, in ihrem Alltag eigeninitiativ handeln können, statt sich „den Kampf"

nur als etwas vorzustellen, das von maskierten, körperlich fitten jungen Menschen auf der Straße geführt wird.

Diese gewaltige Übung in kollektiver Intelligenz ist unglaublich beeindruckend. Eine Aktion kann in einer Messenger-Gruppe oder einem anonymen Board-Thread vorgeschlagen werden, ein paar Leute organisieren sich, und es wird ohne großes Hin und Her gemacht. Aktionsformen werden ausprobiert, modifiziert, dann verbreiten sie sich einfach weiter. Es geht nicht mehr nur um eine winzige Szene von Aktivist*innen, die Taktiken und Programme zusammenstellen und versuchen, sie an die Öffentlichkeit zu tragen. „Die Öffentlichkeit" handelt überall, tauscht Techniken aus, entwickelt Wege, um der Überwachung zu entgehen, um nicht verhaftet zu werden. Es ist aktuell möglich, an einem Nachmittag mehr über die Bekämpfung von Bullen zu lernen, als viele es in einigen Jahren zuvor getan haben.

Telegram

Ein weiterer Aspekt der Kommunikationsinfrastruktur sind Messenger, insbesondere Telegram. Seit 2015 gibt es bei Telegram Channels (Kanäle). Channels sind eine Form der Einweg-Nachrichtenübermittlung, bei der die Administrator*innen (Admins) des Channels Nachrichten an eine unbegrenzte Anzahl von Abonnent*innen posten können, andere Benutzer*innen jedoch nicht. Jede*r Benutzer*in kann Channels erstellen und abonnieren. Sie können öffentlich sein, sodass jede*r beitreten kann. Benutzer*innen, die einem Kanal beitreten, können den gesamten Nachrichtenverlauf einsehen. Je nach den Einstellungen eines Channels können Nachrichten mit dem Namen des Channels oder mit dem Benutzernamen der Administrator*in signiert werden. Jede Nachricht hat einen eigenen Ansichtszähler, der anzeigt, wie viele Benutzer*innen diese Nachricht gesehen haben, dies schließt Ansichten von weitergeleiteten Nachrichten ein. Ab Mai 2019 können Admins eines Channels eine Diskussionsgruppe hinzufügen, eine separate Gruppe, in der Nachrichten im Channel automatisch für die Abonnent*innen zur Kommunikation gepostet werden. Des Weiteren können Admins die Erlaubnis erteilen, mithilfe von Bots Kommentare auf dem Telegram-Channel zu veröffentlichen. Bots sind Accounts, die von Programmen betrieben werden. Sie können auf Nachrichten oder Erwähnungen antworten, können in Gruppen eingeladen werden und können in andere Programme integriert werden. Diese Channels und Bots werden vielfältig genutzt. Auf zwei Beispiele soll im Folgenden eingegangen werden.

1. Scouting-Channels
Strategisch wichtig ist es zu wissen, wo gerade Bullen präsent sind. Zum einen um den Kontakt zu vermeiden, zum anderen auch, um sie anzugreifen. Deshalb wurden Scouting-Channels (Kundschafter*innen-Kanäle) eingerichtet, in denen die aktuelle Bullenbewegung kollektiv zusammengetragen wird. Menschen, die Bullenbewegung sehen, übermitteln an einen Bot ihre Beobachtung, idealerweise mit Informationen, um was für eine Einheit es sich handelt (die meisten Menschen können aber wahrscheinlich die unterschiedlichen Einheiten nicht auseinanderhalten), die Anzahl der Bullen und GPS-Koordinaten. Der Bot postet die Nachricht dann in einem Telegram-Channel mit einem entsprechenden Hashtag für den Standort.

Diese Berichte werden von anderen Programmen automatisiert ausgelesen, (mit openlayers) in eine Openstreetmap-Karte übersetzt und für alle abrufbar auf der Website *hkmap.live* veröffentlicht. Anhand von Symbolen auf der Karte wird die kollektiv zusammengetragene Lage visualisiert[105]. Die Karte ist nicht selbsterklärend: Hundewelpen und Raubsaurier repräsentieren Bullen. Wassertropfen repräsentieren Wasserwerfer. Kameras bedeuten, dass es einen Live-Stream vom Geschehen gibt. Es gibt noch eine ganze Reihe weiterer Symbole. Dadurch, dass es für alle Mitglieder des Channels möglich ist Informationen beizutragen, ist es nicht davor gewahrt, dass Fehlinformationen eingespielt werden. Die Informationen sind allerdings Telefonnummern zuordenbar. Es wird auch angezeigt, wann der Bericht eingespielt wurde und es ist möglich diesen zu verifizieren.

Einige Journalist*innen streamen die Proteste. Es gibt auch eine Website, die bis zu neun Live-Streams parallel anzeigt, sodass Menschen sich parallel aus unterschiedlichen Perspektiven ein Bild von den Lage machen können.

2. Undercover-Cops
Wenn die U-Bahn ausfällt, wird kollektiv mit Privatautos der Transport von Personen organisiert. Da Menschen Angst haben, bei Undercover-Bullen ins Auto zu steigen, gibt es eine inoffizielle Datenbank mit Nummernschildern, die Undercover-Bullen zugeordnet wurden. Es gibt einen Telegram-Bot, der diese Datenbank abfragt und für alle zugänglich macht. Menschen können also einfach ein Nummernschild dem Bot mitteilen und der Bot antwortet, ob das Schild bekannt ist oder nicht.

Sollte das Nummernschild unbekannt sein, so kann dieses aber auch aufgrund der Unvollständigkeit der Datenbank der Fall sein und die Anfragende in einer falschen Sicherheit wiegen. Ein vollständiges Vertrauen in die Technik wäre fahrlässig.

105 Eine etwas andere, aber dennoch vergleichbare Umsetzung ist das Projekt *Cop Map* des Peng!-Kollektivs. Siehe https://pen.gg/campaign/cop-map/ und https://www.cop-map.com/

Dezentrale Entscheidungsfindung

Schwierig ist die Entscheidungsfindung mit tausenden bis hunderttausenden von Menschen. Dieses beinhaltet sowohl ad hoc als auch strategische Entscheidungen.

Es gibt viele Diskussionen in denen Menschen sich mitteilen, was ihrer Meinung nach passieren sollte, welche Ziele verfolgt werden sollten und was die richtige Strategie ist. Für die Entscheidungsfindung werden unterschiedliche Plattformen verwendet. Zum einen läuft viel über Telegram-Channels, Whatsapp oder Facebook-Gruppen. Zum anderen finden viele Diskussionen auf LIHKG statt. Die Diskussionen verlaufen nach folgendem Prinzip: Wenn Menschen ein Argument haben, das sie für wichtig halten, teilen sie es mit anderen. Diskussionen und Entscheidungsfindung verlaufen dadurch wie ein Schneeballeffekt. Argumente, mit denen die Leute einverstanden sind, tauchen (ggf. paraphrasiert) in verschiedenen Gruppen immer wieder auf.

Entscheidungen werden aber auch über Umfragen in Telegram-Channels gefällt. In Gruppen mit mehreren zehntausend Personen, fragen Admins Optionen A-B-C-D ab. So wurden vor allem anfangs die fünf Forderungen formuliert. Diese Technik ermöglicht aber auch kurzfristige und unmittelbare Entscheidungen vor Ort (vorausgesetzt, Personen haben ihr Smartphone dabei).

Ein interessantes Beispiel für solch eine Entscheidung war die Besetzung und Stilllegung des Hongkonger Flughafens am 12. August 2019 für mehrere Stunden. Die Bullen griffen Besetzer*innen mit Tränengas an. In einem Kanal mit ca. 60.000 Abonnent*innen wurde stetig abgefragt, bleiben oder gehen wir? So war es eine kollektive Entscheidung, eine bestimmte Dauer zu bleiben und irgendwann zu gehen.

Sicherheit und Anonymität

Sicherheit und Anonymität sind unglaublich wichtig geworden. Die Sache mit dem Gefühl, dass ihr politisches System ausgehöhlt wird und alle Sicherheiten, Gewissheiten und Rechte verschwinden, ist die Ungewissheit. Viele Menschen haben das Gefühl, nicht mehr politisch sprechen zu können, weil sie nicht wissen, welche Folgen das haben wird. Menschen legen sich Pseudonyme zu, ändern ihre Namen auf ihren Facebook-Konten, schließen ihre Social-Media-Accounts und sprechen in Codes, weil sie sich nicht mehr trauen, etwas, was sie vor einem Jahr noch offen gesagt hätten, unter ihrem eigenen Namen zu sagen. In jeder Gruppe (insbesondere jeder größeren) wird angenommen, dass die geteilten/veröffentlichen Informationen von jemanden aus der Gruppe an Bullen weitergegeben werden.

Auch die Ereignisse der letzten Jahre – beispielsweise Buchhändler*innen aus Hongkong, die wegen des Verkaufs von auf dem Festland verbotenen Publikationen verschwunden sind, oder Aktivist*innen, die beim Grenzübertritt festgenommen und jeglichen Kontakts beraubt wurden – bieten wenig Anlass, einer Partei zu vertrauen, die Anklagen erhebt und das Gesetz missachtet, wann immer sie möchte.

Die dezentrale Organisierung der Bewegung basiert so stark auf digitaler Technologie, dass die damit einhergehende Überwachung in Kauf genommen wird. Burnerphones (Wegwerf-Handy mit Prepaid-SIM) werden zwar vereinzelt eingesetzt, aber der offensichtliche Nachteil dieser Methode ist, dass niemand diese neue Telefonnummer kennt und deren Reputation bei Null liegt – das erschwert ganz wesentlich die Teilnahme an der dezentralen Organisierung. Wenn also schon das private Phone mit muss, dann möglichst sicher – Aktivist*innen deaktivieren die Entsperrung des Geräts durch biometrische Verfahren (Gesichtserkennung, Fingerabdruck), da die Biometrie auch gegen den Willen der Betroffenen „genommen“ werden kann. Es gibt Berichte darüber, dass Bullen festgenommenen Aktivist*innen einfach ihr Phone vor das Gesicht gehalten haben, um es zu entsperren.

Es gibt einige Threads und Telegram-Channel die sich mit IT-Sicherheit befassen. Dort wird unter anderem auch versucht, die Themen herunterzubrechen und vielen Menschen zugänglich zu machen. Dies geschieht beispielsweise durch Verschicken/Weiterleiten einfacher visualisierter Anleitungen (JPEG). Ganz konkret beispielsweise, wie bestimmte Einstellungen in Telegram vorzunehmen sind.

Die Standardnachrichten und -medien werden bei Telegram serverseitig verschlüsselt. D. h. Telegram kann diese Daten entschlüsseln. Optional bietet Telegram Ende-zu-Ende-Verschlüsselung für „geheime“ Chats zwischen zwei Kommunikationsteilnehmenden, jedoch nicht für Gruppen oder Kanäle. Darüber hinaus haben Kanäle das Problem, dass Abonnent*innen andere Abonnent*innen sehen können. Trotzdem wird aufgrund der Features an der Plattform festgehalten.

Der Messenger Signal wird anscheinend nicht oder nur von wenigen verwendet. Das liegt vermutlich daran, dass es zwar verschlüsselte Gruppenchats gibt, aber keine Channels und Bots.

Videoüberwachung

Das Bedürfnis nach Anonymität mag zu der massiven Ablehnung der Videoüberwachung beigetragen haben. Videokameras zu zerstören, ist zum Protestsport geworden. Gesprühte Farbe auf Überwachungskameras

und entfaltete Regenschirme werden benutzt, um die Identität der Gruppe in Aktion zu schützen. Es kommt auch vor, dass Aktivist*innen ausgestattet mit einer Flex Straßenlampen, an denen Kameras mit Gesichtserkennungsalgorithmen installiert sind, umsägen, die Platinen ausbauen und erschließen, wo die Komponenten produziert werden.

Kameramänner*frauen werden gebeten, nur die Vermummten zu filmen. Des Weiteren organisieren Menschen Kleiderspenden, damit Aktivist*innen in Seitenstraßen ihre (schwarzen) Klamotten wechseln können. Allerdings hilft das nur gegen die visuelle Erfassung und Einsortierung durch die Bullen und nur bedingt gegen eine Künstliche Intelligenz. Im September 2019 wurde bekannt, dass China eine 500-Megapixel-Gesichtserkennungskamera entwickelt hat, die in der Lage ist, tausende von Gesichtern in perfekter Detailgenauigkeit zu erfassen und ihre Gesichtsdaten zu generieren, während sie ein bestimmtes Ziel in einem Augenblick lokalisiert. Wichtig beim Thema Gesichtserkennung ist auch, dass einige Überwachungssysteme heutzutage schon Sensorintegration betreiben, um ein multi-modales Dataset zu erzeugen. Größe, Gang (Skelett-Geometrie), Kleidung (Marken, Modelljahre), aber auch Funksignale von mobilen Geräten werden erfasst. Noch werden diese hochauflösenden Kameras und sensorintegrierten Systeme nicht weitverbreitet eingesetzt. Vermutlich ist es leider aber nur eine Frage der Kosten.

Doxxing

Anonymität scheint ein Reizthema zu sein: Als Bullen anfingen, ihre Namensschilder/ID-Nummern nicht mehr an ihrer Uniform zu tragen, startete eine *Doxxing*-Welle, bei der Bullen mit Namen, Wohnort, Familienangehörigen, etc. veröffentlicht wurden. 4.359 Fälle (Stand Dezember 2019) von Doxxing stehen im Zusammenhang mit den Protesten. Die Fälle, bei denen Bullen oder ihre Familienangehörigen betroffen waren, machten 36 Prozent aller gemeldeten oder entdeckten Fälle von Doxxing aus. Das Doxxing passierte in sechzehn Online-Plattformen und Foren. Doxxing gab es aber auch in die andere Richtung; regierungsfreundliche Persönlichkeiten des öffentlichen Lebens, Protestierende, regierungsfeindliche Bürger*innen und Aktivist*innen wurden gleichermaßen geoutet.

Octopus-Tickets

Es wird versucht, digitale Spuren zu vermeiden – die Nutzung von Verschlüsselung ist da nur die eine Seite. (Papier)Tickets für den ÖPNV sind massiv im Trend. In Hongkong ist ein System installiert, welches ein Ticket auf RFID-Basis realisiert, die Octopus-Karte. Tickets aus dem Automaten sind eigentlich nur für Tourist*innen gedacht. Da über die Octopus-Karte aber die Bewegungsdaten rekonstruierbar sind, weichen die Aktivist*innen auf Papier aus.

Dezentrale Infrastruktur

Die Themen Kontrolle und Zentralität/Dezentralität sind Gegenstand von Diskussionen. Insbesondere, wenn es Angriffe auf die Infrastruktur gibt, dann finden die Diskussionen statt. Telegram wurde in letzter Zeit mehrmals Ziel von DDoS-Angriffen (dabei handelt es sich um einen Angriff auf die Verfügbarkeit des Dienstes durch die Erzeugung einer Überlast). Telegram behauptet, es wäre China gewesen. Aber auch die LIHKG-Website war im Dezember 2019 Gegenstand eines DDoS-Angriffs (wahrscheinlich der sogenannten „Großen Kanone“ von China – einem Angriffswerkzeug, das verwendet wird, um DDoS-Angriffe auf Webseiten zu starten, indem es eine möglichst große Anzahl an IP-Paketen abfängt und sie gezielt auf die anzugreifenden Webseiten umleitet). Trotz der Angriffe ist es eine organisatorische Hürde, viele Menschen zu einer anderen Plattform zu bewegen. Nichtsdestotrotz wurde rasch mit Technologien experimentiert, die nicht zentral überwachbar oder abschaltbar sind, um sowohl die Kommunikation innerhalb der Protestbewegung aufrechtzuerhalten, als auch die Zensurbestrebungen des chinesischen Festlandes zu umgehen, die verzerrte und begrenzte Informationen über Proteste gegen Auslieferungsgesetze haben. Die Demonstrant*innen hatten bereits auf traditionelle SMS, E-Mail und WeChat verzichtet, die vom Staat überwacht werden oder leicht zu überwachen sind. Angesichts der sich abzeichnenden Möglichkeit, dass die Regierung Notstandsgesetze erlassen könnte, einschließlich Maßnahmen zur Abschaltung der Internet-Konnektivität, wurde auf peer-to-peer-basierte Bluetooth- oder WiFi-übertragende Messenger und Mesh-Netzwerkanwendung gesetzt. Sie funktionieren zwar nur über kurze Distanzen, wie beispielsweise auf einer Demonstration oder im U-Bahn-Abteil. Dadurch, dass sie keine Server benötigen, sind sie aber schlechter angreifbar und abschaltbar.

Bei den Protesten in Hongkong im Jahr 2014 wurde vor allem die proprietäre Software FireChat für die Ad-hoc-Vernetzung von Smartphones über Bluetooth verwendet. Heute sind die verwendeten Anwendungen diverser. Neben den proprietären Messengern FireChat und AirDrop wird auch die Open-Source-Software Briar eingesetzt, die verschlüsselte Nachrichtenübertragung und Foren zur Verfügung stellt. Als Peer-to-Peer-Bluetooth-Mesh-Netzwerkanwendung wird ein Ad-hoc-Netzwerksoftwarepaket für Smartphones namens Bridgefy eingesetzt. Obwohl das Bluetooth-Protokoll nicht sicher ist und die Metadaten auch von denjenigen, die über die technischen Mittel verfügen, lokalisiert werden können, ermöglicht die Anwendung

die Übertragung von Nachrichten ohne Internetverbindung. Die Anwendung funktioniert durch die Vernetzung der Standard-Bluetooth-Verbindungen der Benutzer*innen durch die Schaffung eines Mesh-Netzwerks über eine ganze Stadt hinweg. Die Nachrichten werden über die Telefone anderer Bridgefy-Benutzer*innen weitergeleitet, bis sie das beabsichtigte Ziel erreichen. Direkte Nachrichten werden verschlüsselt, während öffentlich gesendete Nachrichten nicht verschlüsselt werden. Der Broadcast-Modus ermöglicht es, Nachrichten an alle Benutzer*innen in unmittelbarer Reichweite zu senden. Der App-Herausgeber gab bekannt, dass die Downloads im Laufe des Augusts um das Vierzig-fache gestiegen seien, mit 60.000 App-Installationen allein in der letzten Augustwoche 2019, die meisten davon aus Hongkong.

CORONA

Corona weckt Erinnerungen an die SARS-Epidemie im Jahr 2003. Damals war Hongkong ein Hotspot und es gab große Frustration in der Bevölkerung wegen des inkompetenten Umgangs der Regierung mit der Krise. Dementsprechend sind aktuell die Erwartungen der Bevölkerung an die Regierung. Die Bewegung ist eingefroren. Angesichts der aktuellen Pandemie und der Erfahrung aus 2003 fährt die Öffentlichkeit – unabhängig von Regierungsverordnungen – ihren Protest runter, wie eine Wiederholung der Maßnahmen von 2003. Dieses Runterfahren ist aber bewusst vorübergehend – die nächsten Protestmärsche sind für Anfang Juni (dem Jahrestag der vergangenen Proteste aus 2019) geplant.

Nationalismus ist ein Problem, welches mit dem Coronavirus zugenommen hat. In der öffentlichen Wahrnehmung wurde SARS 2003 von Festlandchina aus „eingeschleppt". Dementsprechend gibt es Forderungen, die Grenzen zu schließen. Carrie Lam (Regierungchefin) kommt dem nur zögerlich nach, vor allem wegen der gestiegenen ökonomischen Verflechtungen. Eine komplette Schließung sieht sie als epidemiologisch nicht sinnvoll an, was in der Bevölkerung, gelinde gesagt, auf Unverständnis trifft. Der „Nationalismus" breitet sich in Folge aus – Festlandchines*innen sind ungern gesehen und werden in Läden nicht mehr bedient. Es gab „Bomben"anschläge auf U-Bahnstationen, die von Einreisenden benutzt werden.

Die Regierung von Hongkong hat ein „Vermummungsverbot" für politische Demonstrationen verhängt. Das kollidiert mit der Aufforderung der Gesundheitsbehörden, Gesichtsmasken zu tragen. Strukturen, die sich während der Proteste 2019 gebildet haben (insbesondere Gewerkschaften) fordern Maßnahmen, wie beispielsweise die Ausgabe von Gesichtsmasken. Die neuen Strukturen erweisen sich als mächtig genug, die Regierung in Zugzwang zu bringen. Der gewerkschaftliche Organisierungsgrad ist (oder vielleicht: war) in Hongkong gering.

ANSTELLE EINES FAZITS

Soziale Bewegungen brauchen eine Selbstverortung, welche die Bewegung zusammenhält. Die Unterpräsenz eines linken Selbstverständnisses macht die Bewegung anfällig für Surrogate wie einen äußeren Feind (Festlandchina) und Nationalismus. Gleichzeitig beteiligen sich sehr viele Menschen an den Protesten und erleben Selbstermächtigung. Diese antiautoritäre Tendenz steht einer klassisch rechten Ideologie entgegen und es entstehen auch Chancen für emanzipatorische Politik. Die fünf Forderungen beziehen sich – neben der Forderung das Auslieferungsgesetz zu kippen – hauptsächlich auf Antirepressionsaspekte, also die Folgen der Proteste. Einzig die Forderung nach gleichem Wahlrecht geht über den Anlass der Proteste hinaus. Soziale Forderungen fehlen.

Der Artikel zeigt, wie sozio-technische Systeme in einer Bewegung offensiv und defensiv genutzt werden. Vieles davon lässt sich adaptieren und in anderen Situationen anwenden. Nichtsdestotrotz stellt sich die Frage, ob wir wirklich daraus lernen können – oder ob *hier* nicht ganz andere Verhältnisse vorherrschen.

Widerstand gegen die Individualisierung des Sozialen durch den Technologischen Angriff

Seit dem letzten Heft haben wir viel diskutiert und versucht, die Ansätze aus der Einleitung des Widerstandskapitels unserer letzten Broschüre weiter zu entwickeln.Ein Fokus dabei war der mögliche Widerstand gegen die Individualisierung des Sozialen durch den Technologischen Angriff und das damit verbundene „Schaffen einer neuen Sozialität".

Den Ist-Zustand und auch die zu erwartenden Entwicklungen des Technologischen Angriffs haben wir ausführlich in unseren Broschüren beleuchtet. Immer wieder haben wir dabei mehr oder weniger auch den Bereich des sozialen Miteinanders berührt. Im letzten Heft haben wir zudem Kollektives Lernen, Hacking und Sabotage, Alternativen, Verweigerung und Solidarität als fünf Stränge aufgezeigt, die wir zu einer gemeinsamen Strategie verknüpfen müssen. Diese Stränge lassen sich auf verschiedene Bereiche anwenden und anhand ihrer Widerstandsszenarien entwickeln. Was dabei aber immer wieder auftaucht, ist das soziale Miteinander in unseren Leben und damit auch in unseren Kämpfen. Wir haben uns diesmal bemüht, dieses soziale Miteinander mit den fünf Strängen zu verknüpfen und daraus Ideen für eine neue Sozialität zu entwickeln, die uns hilft, der Individualisierung des Sozialen entgegen zu treten.

IST-ZUSTAND DES VERHÄLTNISSES ZWISCHEN TECHNOLOGIE UND GESELLSCHAFT

Vorweg noch zwei Anmerkungen:
1) Unterschiedliche Technologien werden in unterschiedlichen Kontexten gepusht, das bringt natürlich regionale Unterschiede mit sich, die besonders im Vergleich zwischen ländlichem Raum und Metropole sichtbar werden. Das bringt aber auch unterschiedliche Interventionsmöglichkeiten mit sich.

2) Wir sprechen aus einer weißen, westlichen und ungemein privilegierten Position. Was in diesem Text nicht auftaucht, sind Perspektiven des Globalen Südens. Der Text beschäftigt sich nicht mit den globalen Auswirkungen und beleuchtet keine Widerstände vor Ort. Dieser Text ist außerdem sprachlich adressiert an eine radikale Linke und soll Diskussionen ankurbeln, die wir gerne mit euch, aber auch anderen gemeinsam führen möchten.

Der Technologische Angriff rückt uns immer dichter auf die Pelle. Immer mehr informationserfassende und verarbeitende Maschinerie befindet sich in unserer unmittelbaren Nähe, seien es Smartphones oder „Fitness"-Sensoren, alle arbeiten mit unseren teils sehr persönlichen Daten. Die Umstellung des Individuums erreicht Ausmaße, die Zweifel an einem erfolgreichen Widerstand dagegen schüren. Diese scheinbare Unausweichlichkeit der technologischen Entwicklung ist aber Ideologie, die die Verinnerlichung des Kommandos befördern und schon den bloßen Gedanken an Widerstand ersticken soll. Diese Technologie braucht Kooperation, eben weil sie so nah an uns heran rückt. Die Angriffsfläche wird also größer, aber auch komplizierter, weil einfache Verweigerung und Sabotage schon mitgedacht und in den Algorithmen „behandelt" werden. Wir werden umdenken müssen, weil unser Gegenüber unsere Schritte versucht zu antizipieren und vorgefertigte Antworten implementieren kann.

Ein ernsthaftes Stören erscheint immer weniger möglich. Aber merken nur „wir" das? Was ist mit den ganzen Nutzer*innen der „Neuen" Technologien? Bemerken sie überhaupt einen Technologischen Angriff? Bemerken „wir" ihn? Fakt ist, wir müssen aus einer massiven Defensive raus. Das Allumfassende des Technologischen Angriffs und die damit verbundene technologische Zerstörung von Gesellschaflichkeit heißt, dass eine radikale Technologiekritik nur als radikale Gesellschaftskritik möglich ist. Der Technologische Angriff ist auch eine Kampfansage gegen die Zeit. Zeiträume für gesellschaftliche Prozesse und Interventionsmöglichkeiten haben

sich durch die technologische Entwicklung der letzten Jahrzehnte und die damit verbundene rasante Veränderung des gesellschaftlichen Lebens massiv verkürzt. Der IT-kapitalisierte Alltag nagt an uns und laugt uns aus.

Der Technologische Angriff hat unsere Gesellschaft und unser Leben fest im Griff, daher ist es fast schon verständlich, dass die Menschen eine versöhnliche Technologiekritik wollen. Eine radikale Kritik greift massiv in ihren bzw. unseren Alltag ein. Wir befinden uns in einem Dilemma, aus dem wir scheinbar nicht mehr heraus kommen. Einfache Beispiele hierfür sind zum Einen Fitnesstracker, die einerseits Zwang ausüben und andererseits viele Menschen aber auch motivieren. Zum Anderen auch Lieferdienste wie Lieferando; sie schaffen ein Dienstbot*innenverhältnis, welches aus einem radikalen linken Selbstverständnis heraus undenkbar ist, und trotzdem sind sie mittlerweile tief eingedrungen in viele unserer Hausprojekte und WGs. Die dadurch entstehende Wirkmächtigkeit des Technologischen Angriffs führt zu einer Erosion des eigenen sozialen Standpunktes. Was aber auch heißt: Technologiekritisch Mit einer rein auf die Technologie orientierten Kritik haben wir keine Chance. Wenn wir aus unserer kämpferischen Defensive raus wollen, dann geht dies nur durch eine radikale Gesellschaftskritik und eine damit verbundene neue Sozialität.

Und warum steht das „Wir" hier so oft in Anführungszeichen? Die Virtualisierung des Soziallebens macht natürlich auch nicht vor der Linken halt. Ein paar Beispiele:

- *Indymedia statt Infoladen:* Waren noch vor 20 Jahren die Infoläden in den Städten Dreh- und Angelpunkte des regionalen und überregionalen politischen Austauschs, sind dies nun oft Internetseiten wie Indymedia oder lokale Blogs. Es ist so schön einfach, von zu Hause aus die neuesten Nachrichten und Diskussionen zu verfolgen. Die Infoläden, so es sie noch gibt, sind nur noch selten das verlängerte Wohnzimmer der lokalen linken Szene. Die informelle Vernetzung, die im persönlichen Kontakt entsteht, ist über Indymedia und Blogs nicht möglich.

- *Streamen statt Spielen:* Netflix und die Mediatheken bringen uns die Berieselung ins Wohnzimmer. Alleine, mit unserer Beziehung und ab und zu auch mit unserer WG verbringen wir die Abende vorm Bildschirm. Spieleabende sind selten geworden und finden manchmal sogar virtuell statt. Kneipenabende oder nächtelange Küchentisch-Diskussionen werden entweder ganz ersetzt oder thematisch bestimmt durch die neuesten Serien und Filme.

- *Apropos Kneipenabende:* Das Smartphone steht allzu oft zwischen uns. Wann haben wir uns das letzte Mal beim Warten in der Kneipe mit uns unbekannten Menschen unterhalten? Das Smartphone ermöglicht jederzeit Beschäftigung mit uns selbst und der virtuellen Welt und verhindert den Kontakt im Realen. Und zusammen mit Freund*innen? „Hast du das schon gesehen?" „Kennst du schon dieses Video?" „Ich guck das schnell mal nach!" ...

- *Signal statt Straße:* Die lokale Messengergruppe meldet sich minütlich mit den neuesten „relevanten" Nachrichten. Eine unglaubliche Aktivität findet in den Signalgruppen unserer regionalen Bezugsräume statt. Aber schaffen wir es auch, die Aktivität nach Außen auf die Straße zu tragen? Oder sorgt diese Aktivität nicht vielmehr dafür, dass wir uns zurücklehnen, weil ja schon so viel passiert?

Wohlgemerkt wollen wir hier nicht mit dem Finger auf jemanden zeigen, sondern diese Beispiele kennen wir auch aus unserem eigenen Verhalten und Umfeld.
Das Bedürfnis nach sozialer Nähe oder Gesellschaftlichkeit bricht sich aber immer wieder seinen Weg. Nicht umsonst bietet der Technologische Angriff eine unüberschaubare Form an Substituten in Form von Sozialen Netzwerken und Anderem. Und wenn das nicht reicht, dann gibt es ja noch unsere Liebesbeziehungen. Mit unseren Demos und Veranstaltungen gaukeln wir uns Masse und Aktivität vor. Sie sind Ausflüge in das Territorium der Bemühungen, uns und unsere Beziehungen und Verbindungen aus den Kämpfen heraus zu verändern. Nur selten reichen diese Ausflüge und Bemühungen soweit, dass wir dahin kommen, uns mit Hilfe anderer mit unseren Mängeln, Ängsten und Nöten auseinanderzusetzen.

SOZIALITÄT UND KAMPF - ODER: ÜBER DIE AUS WIDERSTÄNDISCHER PRAXIS ENTSTANDENE NÄHE UND VERBINDUNG

Viele von uns kennen sie, die Vertrautheit und Nähe zu Menschen, mit denen wir gemeinsame kämpferische Momente erlebt haben. Sei es die aktive Erste Reihe auf der Demo oder die gemeinsamen Aktionen in vielen schlaflosen Nächten. Aber auch die gemeinsame Trauer oder der gemeinsame Schock nach aufreibenden Situationen schaffen diese Nähe. Hier entsteht ein Gefühl, was auch einige kontaktlose Jahre später noch schimmert und sich anhand von kleinen Gemeinsamkeiten schnell wieder entzünden kann. An diesem besonderen Gefühl zeigen sich einige wichtige Schlussfolgerungen:

Soziale Bewegungen brauchen einen Ort, um diese Form von Sozialität zu entwickeln. Nicht das Digitale,

sondern unser soziales Umfeld ist dieser Meta-Ort. Soziale Beziehungen, die in Kämpfen entstehen, sind aus unserer Erfahrung heraus oft sehr tragfähig.

Eine weitere Schlussfolgerung: Wir müssen unseren Kampfbegriff breiter aufstellen und ausfüllen. Unser Kampf für einer andere Welt bewegt sich meistens entweder auf der Seite „sozial-zwischenmenschlich" oder auf der Seite „reiner Blick auf die Inhalte". Der Kampfbegriff wird oft als klare Entscheidung für eine Seite gesehen und der anderen wird er abgesprochen. Wir müssen lernen, ihn in voller Breite auszufüllen und damit auch den Kampf in voller Breite zu führen. Wo das passiert, entwickelt sich eine starke Bewegung.
Dazu gehört auch, dass wir akzeptieren, dass es oft anstrengend ist, soziale stabile Beziehungen zu halten. Auch das ist also Teil von unserem Kampf.

Was also ist nötig, diesen Kampfbegriff zu erweitern und die Brücke zwischen dem Sozialen / Zwischenmenschlichen und unseren Inhalten zu schlagen?

Wir müssen lernen, uns in unserer Unterschiedlichkeit auszuhalten. Auch wenn es anstrengend ist. Dazu gehört auch, dass wir lernen, uns kritisch, aber solidarisch miteinander auseinanderzusetzen, aufeinander zu zu gehen und die unterschiedlichen Positionen sehen zu können. Gerade Letzteres braucht eine Bereitschaft und Offenheit für andere Lebensrealitäten. Und das Ganze nicht nur szeneintern, sondern unbedingt auch darüber hinaus, um Anknüpfungspunkte zu bieten. Natürlich heißt das nicht, dass wir Dinge widerspruchslos hinnehmen sollen, vielmehr brauchen wir die Bereitschaft zu erkennen, welchen Einfluss unsere Lebensrealität auf unsere Postionen hat. Das Gleiche gilt für unser Gegenüber. Vor diesem Hintergrund sollten wir versuchen, eine gemeinsame Sprache, die dies berücksichtigt, für unsere Auseinandersetzungen zu finden.

Wir müssen uns fragen: Woher kommt unser Drive? Woher kommt unsere Power, und was vertreibt den vielen Frust und die Niedergeschlagenheit? Wir müssen in kleinen Schritten lernen, uns Sachen zu trauen, die wir uns vorher nicht getraut haben. So entsteht Ermächtigung. Diese Schritte könnten für uns nicht unterschiedlicher sein. Bei dem Einen ist es das Verteilen von Flugblättern, bei der Anderen ist es das Sabotieren von Funkmasten. Wieder beim Anderen bedeutet es, sich endlich zu trauen, mit der Freund*in über die eigenen Ängste zu reden. Auch hier müssen wir lernen, die Vielschichtigkeit des Kampfes zu betrachten.

Wir müssen Territorien befreien. Sowohl psychisch, um Denkräume zu eröffnen, als auch physisch, um Handlungsräume zu eröffnen. Die Größe dieser Territorien ist wieder unterschiedlich. Vom Sprühengehen bis hin zur gemeinsamen Ökonomie mit Gefährt*innen eröffnet Vieles unterschiedlich große Räume. Kurz gesagt, wir brauchen eine Verräumlichung des Widerstandes.

Der Technologische Angriff ist global und vielfältig. Genauso müssen unsere Kämpfe sein, das heißt, wir brauchen eine Verbindung zu anderen Kämpfen, sei es geographisch oder thematisch.

Oft wird als Alternative dem Technologischem Angriff nur ein Zurück entgegen gestellt. Somit würde nur ein Vor oder Zurück bleiben. Ein Ausbrechen aus dieser Linearität eröffnet uns neue Räume der Auseinandersetzung. Wieso nicht mal zur Seite? Klingt im ersten Moment passiv, aber das Herstellen von etwas Neuem, in der Geschichte noch nicht Dagewesenen, könnte aktiver nicht sein. Wir müssen dem Neuem, was dem Technologischem Angriff innewohnt, auch etwas völlig Neues entgegensetzen. Dazu müssen wir lernen, unsere Positionen gemeinsam stetig zu erweitern und zu verändern, denn wir haben nicht DIE richtige Lösung. Ein reines Reagieren reicht da nicht aus, sondern wir müssen uns auch aktiv mit unseren Perspektiven beschäftigen, uns diese entwickeln.

Am jetzigem Punkt der Analyse bleiben für uns ein paar Fragen, die eher etwas für die lokalen Gruppen und Diskussionen sind und uns dort vielleicht weiterbringen können:

Lasst uns kritisch hinterfragen, wie unser Alltag aussieht. Oder ist unsere Progressivität nicht alltäglich und beschränkt auf Aktionen, Demos oder Ähnliches? Wie lässt sich das ändern, ohne uns zu überfordern? Aus den 68ern gibt es dazu den passenden Spruch „Das Private ist politisch".

Warum schaffen wir keine starke Gegenbewegung gegen den Technologischen Angriff und die von ihm angebotenen Lösungen? Und wenn es sie gibt, warum lässt sie sich oft so schnell vereinnahmen durch die Techindustrie?

Wie können wir eine Geschichte erzählen, die ganz klar sagt: Technokrat*innen verpisst euch, wir brauchen eure Lösungen nicht?

Warum ist es immer wieder so schwierig, unsere Zusammenhänge und Gruppen zusammenzuhalten? Was gibt der Gruppe, dem Zusammenhang, dem sozialem Umfeld überhaupt einen Zusammenhalt? Wie funktioniert unsere Bindung durch Beziehung und wie lässt sich diese in unseren Widerstand transferieren?

FÜNF STRÄNGE RELOADED

Ausgehend von diesen Betrachtungen und Analysen zum Komplex der Neuen Sozialität haben wir uns die oben genannten „fünf Stränge" aus unserer letzten Broschüre nochmal angeschaut und ein paar Ideen dazu gesammelt, was das im Hinblick auf diese Neue Sozialität in den unterschiedlichen Widerstandssträngen heißt und braucht.

Kollektives Lernen heißt, sich gemeinsam auseinanderzusetzen. Ob mit konkreten Inhalten oder auch mit Erfahrungen und Gefühlen. Um dabei wirklich in einen gemeinsamen Prozess zu kommen, braucht es Verbindlichkeit und Kontinuität, aber auch Spaß. Das heißt auch, dass wir lernen müssen, uns dafür schöne Räume zu schaffen, in denen wir uns wohl fühlen, sowohl psychisch als auch physisch. Um dabei dann anknüpfbar zu sein, brauchen wir einfache Formate sowie Offenheit und Neugier für die anderen Positionen, immer aber auch verbunden mit einer eigenen Haltung dazu.

Zwei von unseren fünf Ansätzen sind *Sabotage/Hacking* und *Verweigerung*. In unseren Diskussionen wurden sie immer wieder zusammengefasst unter dem Begriff der praktischen Intervention, obwohl wir bei Verweigerung erstmal eher an passives Verhalten denken. Für uns gibt es aber auch die aktive Verweigerung, welche sich in eine direkte Konfrontation mit dem Bestehendem begibt.

Die gemeinsame praktische Intervention schafft Vertrauen und stärkt unsere sozialen Beziehungen. Wir müssen uns die Frage stellen, wie wir diese Praxis in den Alltag bringen. Wie intervenierst du alltäglich? Die Sabotage der atomisierten Gesellschaft findet im Alltag statt. Die bei den meisten von uns stattfindende stetige Trennung von Alltag und Kampf macht uns kaputt, da wir immer wieder umschalten im Kopf.

Wir brauchen in unseren Kämpfen eine Authentizität, und die kommt nur, wenn wir ehrlich zu uns selbst und zu anderen sind. Das heißt aber auch, dass wir uns gegenseitig widersprechen können und unsere Konflikte austragen müssen. Im Großen heißt es, dass wir alltäglich unseren Konflikt mit dem Bestehenden ausleben sollten. Ganz wichtig: Das kann auf unterschiedlichen Ebenen stattfinden und wir(in unseren sozialen Zusammenhängen) müssen immer wieder gemeinsam schauen, welche Ebene gerade funktioniert. Ist es das aktive Krankfeiern und mehr Zeit für Politarbeit zu haben, oder ist es der Ausstieg aus dem Job und rein in die nächste Waldbesetzung? Wichtig ist, wir müssen das mit unseren sozialen Zusammenhängen gemeinsam entwickeln, denn es gibt kein richtiges Leben im Falschen, ohne Einzelne zu überfordern und abzuhängen. Hier müssen wir aufpassen und dürfen nicht Wir dürfen nicht zulassen, dass sich die Vereinzelung durchsetzt und wir Gefährt*innen verlieren.

Wir brauchen nicht nur Kritik, sondern auch *Alternativen*. Eigentlich ist „Alternative" ein unpassender Begriff, denn unsere Ideen und Konzepte sollen nicht neben dem Herrschenden stehen, sondern sie langfristig verdrängen. Wir wollen sie nicht nur ersetzen durch etwas gleicher Funktionalität, sondern wir wollen etwas eigenes, passenderes. Unsere Utopie sollte aus unserer eigenen Perspektive kommen und nicht nur reaktiv sein. Vieles von dem, was wir heute als Alternative bezeichnen, wie z. B. gemeinsame Ökonomie, eigene Projekte etc., sind „nur" Werkzeuge auf dem Weg zu unserer Utopie von einem tragfähigen und lebhaften Sozialen.

Und auch der Begriff *„Solidarität"* ist eigentlich nicht wirklich passend. Er verfestigt und zeigt Er macht eine Trennung von MIR zu DIR auf. ICH bin solidarisch mit DIR. Er lässt mich hier auf meiner Position und den anderen dort drüben auf seiner. Aber das Gefühl, das hinter diesem Begriff steht, ist das, was für uns wichtig ist. Wir verbinden Solidarität ja eigentlich alle mit etwas Verbindendem. Und das ist wichtig, wenn das Trennende zwischen uns Individuen aufgehoben ist, dann entsteht ein gemeinsamer Kampf. Oft lohnt sich eine genauer Blick, warum wir uns bemüßigt fühlen, solidarisch zu sein, um die gemeinsamen Kämpfe zu begreifen und sichtbar zu machen.

Alles in Allem heißt das für uns primär: Wir müssen Resonanzräume für unser Handeln aufstoßen und eine eigene Erzählung, unsere Blickweisen und Utopien entwickeln. Dafür brauchen wir keinen Katastrophismus oder den Tunnelblick der Technikbegeisterten, sondern wir brauchen den Mut, Perspektiven rauszuhauen, die themenübergreifend sind und gegen die Fragmentierung von Themengebieten wirken. Hierbei dürfen wir uns nicht nur auf das Offensichtliche konzentrieren. Nicht nur Klima und Technologie gehören zusammen, sondern auch Antifaschismus, Antirassismus und vieles mehr sind mit Technologiekritik direkt zu verknüpfen. Wir müssen uns Räume wieder aneignen, und da die Parameter für unsere Utopien nicht von der Gegenseite bestimmt werden sollten, müssen wir uns diese Räume auch *neu* aneignen. Wir brauchen sowohl eine physische als auch eine soziale Verortung, um der Entfremdung von unseren Lebensgrundlagen entgegenzuwirken. Es geht um die Schaffung anderer Sozialitäten, auf die wir unseren Kampf stützen und aufbauen können.

Dokumentierte Widerstände

Im Folgenden dokumentieren wir beispielhaft einige Widerstandsbemühungen gegen den technologischen Angriff. Teilweise reproduzieren wir hierfür Zeitungsartikel sowie Selbstbezichtigungsschreiben, die von Hacks und Sabotagen berichten. Teilweise haben wir Ereignisse und Entwicklungen selbst zusammengefasst und kontextualisiert. Die gekennzeichneten Selbstbezichtigungsschreiben der dokumentierten Aktionen geben dabei nicht unbedingt die Meinung der Redaktion wider. Im Gegensatz zu vorherigen Widerstandsdokumentationen finden sich in dieser vor allem einzelne Aktionen und keine Berichte von größeren sozialen Bewegungen oder Kämpfen. Was nicht bedeutet, dass diese nicht stattfinden.

HACKS

Wir beginnen mit digitalen Banküberfällen, dann berichten wir von Datenklau bei Rüstungskonzernen und Gerichten sowie über die Nutzung von Jammern. Diese Beispiele können bei Weitem nicht die ganze Palette an Widerstand und Delinquenz abbilden, die sich als Anwort auf den technologischen Angriff entfalten. Vielmehr dienen diese Beispiele als Schlaglichter.

Digitaler Bankraub

Ableger von Cayman National Bank and Trust gehackt

Hundertausende interne Dokumente wurden in der Folge des bereits 2016 stattgefundenen Hacks im Internet veröffentlicht und ein entsprechendes Manifest von Phineas Fisher veröffentlicht. Zudem soll ein sechsstelliger Geldbetrag entwendet worden sein. Es dürfte kein Zufall sein, dass es eine Bank auf den Cayman Islands trifft, da viele internationale Firmen und Banken anonym ihr Geld dorthin verschieben, weil sich die Insel zu einem Zentrum der internationalen Geldwäsche und Steuerflucht entwickelt hat (40 % der weltweiten Hedgefonds sind hier angesiedelt). Bei dem erfolgreichen Hack wurden mehr als zwei Terrabyte an Daten von einem Teil der dort angesiedelten Firmen veröffentlicht1. Betroffen sind die Kundendaten von 1400 Konten und detaillierte Finanzinformationen von über 3800 Firmen (insgesamt handelt es sich um 600.000 interne Dokumente aus der britischen Steueroase Cayman Islands).

Als Begründung für das Veröffentlichen der Dokumente und den digitalen Bankraub schreibt die Hacker*in Phineas Fisher: „Privatsphäre für die Mächtigen ist nicht dasselbe, wenn sie es ihnen erlaubt, die Grenzen eines Systems zu umgehen, um davon zu profitieren.“ In dem Manifest, das einen Leitfaden zum Hacken von Banken enthält, heißt es weiter: „Ich habe eine Bank ausgeraubt und das Geld verschenkt […] Im digitalen Zeitalter ist ein Banküberfall ein gewaltloser Akt, weniger riskant, und die Belohnung ist höher als je zuvor. Keiner der Finanz-Hacks, die ich durchgeführt habe oder von denen ich wusste, wurde gemeldet. Dies wird der erste sein, und zwar nicht, weil die Bank es wollte, sondern weil ich beschlossen habe, es zu veröffentlichen.“

In einem Interview erwähnt sie oder er noch: „Die globale Finanzelite ist Unterdrücker, nicht Opfer [...] Diese Elite zu hacken und den kleinsten Teil des gestohlenen Reichtums zurückzugeben, macht sie nicht zu Opfern […] Es ist Cyberkriminalität. Aber es ist auch Aktivismus. Es ist motiviert durch den Wunsch nach sozialer Veränderung, ich persönlich profitiere nicht davon.“ Zudem bezieht sich Phineas Fisher in dem Manifest auf Tupac Katari, der sein Leben dem Kampf gegen die Ausbeutung der indigenen Bevölkerung durch den spanischen Kolonialismus gewidmet hat: „Ich bin nichts weiter als das Produkt eines Systems, das nicht funktioniert. Solange es Ungerechtigkeit, Ausbeutung, Entfremdung, Gewalt und Umweltzerstörung gibt, werden noch viele andere kommen wie ich: eine endlose Reihe von Menschen, die das System, das für dieses Leiden verantwortlich ist, als illegitim ablehnen werden. Das System wird nicht dadurch repariert werden, dass man mich verhaftet. Ich bin nur einer von Millionen von Samen, die Tupac vor 238 Jahren in La Paz gepflanzt hat, und ich hoffe, dass meine Handlungen und Schriften den Samen der Rebellion in ihren Herzen tränken.“

Die damalige Aufstandsbewegung im heutigen Bolivien hatte eine breite Unterstützung und lange Dauer. Die letzten Worte von Tupac Katari bei seiner Hinrichtung durch die spanische Kolonialmacht waren: „Sie töten nur mich. Ich werde millionenfach zurückkehren …“

100.000 Dollar Belohnung für antikapitalistische Firmen-Hacks.
Was ist das Hacken einer Bank gegen die Gründung einer Bank? In dem veröffentlichten Manifest zu dem Cayman Bank Hack bietet Phineas Fisher 100.000 Dollar Belohnung für weitere geleakte Dokumente, die im „öffentlichen Interesse" stehen. Dazu zählen u. a. Firmen, die an der Entwicklung von Spionage-Software beteiligt sind oder amerikanische Ölfirmen wie Halliburton. Die Belohnung für weitere imageschädigende oder antikapitalistische Hacks kann laut Phineas Fisher in der Cryptowährung Bitcoin oder Monero ausgezahlt werden. Zudem veröffentlichte Phineas Fisher den Guide „Hack Back! Ein DIY-Leitfaden für Banküberfälle"[106]

Größter (digitaler) Bankraub des Jahrhunderts
Einer Gruppe, die sich Carbanak nennt, gelang es laut dem Softwareunternehmen Kaspersky Anfang 2015 dutzende Banken um eine Milliarde Dollar zu erleichtern. Über Phishing-Angriffe, bei denen Bankangestellte dazu animiert wurden, Anhänge ihrer Mails zu öffnen, konnte Software zur Überwachung auf diversen Bank-Computern installiert werden. Dadurch war es möglich, die Rechner als Eingangspunkte für den Angriff zu nutzen. Die infizierten Rechner durchsuchten anschließend das Intranet der Banken und brachten über manipulierte Software weitere Rechner unter ihre Kontrolle. Nach einiger Zeit und entsprechender Beobachtung konnten die kritischen Finanzsysteme in den jeweiligen Banken identifiziert und für den digitalen Bankraub genutzt werden. Neben Geldüberweisungen gelang der Gruppe auch ein entfernter Zugriff auf Bankautomaten. Im Durchschnitt dauerte es zwischen zwei und vier Monaten, um eine Bank zu bestehlen. In den jeweiligen Banken wurden auf diesem Weg zwischen 2,5 - 10 Millionen Dollar geklaut. Insgesamt beläuft sich Summe auf etwa eine Milliarde Dollar. Diverse Sicherheitsbehörden machen sich daher Sorgen um den Zustand der globalen Finanzwelt und deren mögliche Angreifbarkeit. Eine ungeklärte Frage bleibt: Was wäre passiert, wenn die Angreifer*innen statt zur eigenen Bereicherung Sabotage als ein Hauptziel im Fokus gehabt hätten? Wäre ein systemischer globaler Absturz der vernetzten Finanzsysteme möglich gewesen? Laut dem Sicherheitsunternehmen Kaspersky lassen „das Ausmaß und die Tragweite des Angriffs jedoch Zweifel daran aufkommen, dass sich das Finanzsystem vollständig vor dieser neuen Art von Cyber-Bedrohungen schützen kann".[107]

Weiterer digitaler Milliarden-Bankraub scheitert wegen eines Tippfehlers
Durch die Ausnutzung einer Sicherheitslücke wäre die Zentralbank im südasiatischen Bangladesch im Jahr 2016 fast um eine Milliarde Dollar bestohlen worden. Während einige der Überweisungen bereits abgewickelt waren, fiel einem Mitarbeiter der Deutschen Bank (einer der Übermittler der Transaktionen) ein Schreibfehler bei den Überweisungen auf und er ließ deshalb die laufende Aktion scheitern. Daraufhin wurden die Aufträge und noch ausstehende Überweisungen von etwa 850 Millionen Dollar storniert. Die Summe von 81 Millionen Dollar aus den ersten vier Überweisungen ist allerdings nicht mehr auffindbar und von den Täter*innen fehlt jede Spur. Das Geld aus den Überweisungen soll anschließend über Spielcasinos „gewaschen" worden sein.[108]

Weitere Hacks

Nicht verwunderlich finden immer wieder Hacks gegen staatliche Institutionen und auch Unternehmen statt. Wir dokumentieren hier vier solcher Hacks. Auch, wenn beim zweiten und dritten die Motive unklar sind und auch beim zweiten nicht eindeutig, zeigen sie eindrücklich, wie sich Hacks und Schadsoftware auswirken können.

Gefängnisausbruch 2.0
Durch eine geschickte Täuschung per E-Mail gelang einem britischen Gefangenen im Frühjahr 2015 die Flucht aus einem Londoner Gefängnis. Mittels eines eingeschmuggelten Smartphones fälschte der in U-Haft einsitzende eine Webseite, die dem zuständigen Gericht stark ähnelte. Über E-Mail Verkehr, in dem er sich als leitender Beamter ausgab, schickte er Anweisungen zu seiner Entlassung an die Gefängnisleitung. Da die E-Mail dieselbe Domain-Endung wie die gefälschte Webseite hatte, fiel seine Flucht erst drei Tage später auf. Die Domain hatte er auf den Namen des gegen ihn ermittelnden Bullen registriert.[109]

Trojaner-Attacke auf Berliner Kammergericht folgenreicher als vermutet
Seit Monaten plagen das Berliner Kammergericht die Konsequenzen eines Angriffs mit der Schadsoftware Emotet. Das Netzwerk war offenbar haarsträubend schlecht für so einen Fall gerüstet:
27.1.20 Das Computerproblem des Berliner Kammergerichts ist offenbar schwerwiegender als bislang bekannt. Das berichtet der „Tagesspiegel" unter Berufung auf ein

106 https://data.ddosecrets.com/file/Sherwood/HackBack_EN.txt
107 https://www.kaspersky.de/blog/der-groste-bankraub-des-jahrhunderts-hacker-stehlen-1-milliarde-dollar/4843/
108 Quelle: https://www.vice.com/de/article/d7ynyx/bangladesch-fed-reserve-bank-hacker-klauen-87-mio-usd-ohne-einen-rechtschreibfehler-waere-es-1-mrd-gewesen
109 Quelle: https://www.heise.de/newsticker/meldung/Gefaengnisausbruch-mittels-E-Mail-Betrug-2587303.html

Gutachten von T-Systems. Ein Einblick in diese Untersuchung des IT-Dienstleisters war dem Vorsitzenden des Rechtsausschusses des Berliner Abgeordnetenhauses Anfang des Monats noch verweigert worden.

Das Kammergericht war Ende September von einem Computerproblem lahmgelegt worden – und viele Richter und Beschäftigte sind im Alltag nach wie vor mit den Folgen konfrontiert. „Wegen einer festgestellten Schadsoftware ist das Computersystem des Kammergerichts vorübergehend vom Netz genommen worden", heißt es noch immer auf der Website des Kammergerichts. „Das Kammergericht ist bis auf Weiteres nur telefonisch, per Fax und postalisch zu erreichen." Seine „Arbeitsfähigkeit" sei aber gewährleistet.

Bei der erwähnten Schadsoftware handelt es sich um *Emotet*, einen Trojaner, vor dem das Bundesamt für Sicherheit in der Informationstechnik (BSI) schon seit Langem warnt, der aber immer wieder Unternehmen und Organisationen in Bedrängnis bringt. Emotet wird unter anderem über Spam-E-Mails verbreitet, die wie Nachrichten von Kontakten daherkommen, mit denen jemand tatsächlich in Kontakt stand. Dem BSI zufolge enthalten die Mails „entweder ein schädliches Office-Dokument direkt als Dateianhang oder einen Link, welcher zum Download eines solchen Dokuments führt": Über in den Dokumenten enthaltene Makros würden die Opfersysteme mit dem Schadprogramm infiziert. Anschließend spähe Emotet Zugangsdaten zu E-Mail-Konten aus und verbreite sich mithilfe darin auffindbarer Adressen weiter.

Die eigentliche Infektion eines Netzwerks ist aber oft nur der erste Schritt: Emotet bietet den Angreifern auch die Möglichkeit, weitere Schadsoftware wie Banking- und Verschlüsselungstrojaner nachzuladen, mit denen sich dann Unternehmen erpressen lassen.

Das Gutachten von T-Systems liefert nach „Tagesspiegel"-Informationen keine klare Antwort auf die Frage, wie Emotet ins IT-System des Kammergerichts gelangt ist. Neben E-Mails mit Office-Dokumenten im Anhang könnten aber offenbar auch private Speichermedien wie USB-Sticks, die Mitarbeiter*innen des Gerichts für den Datentransport zwischen Büro- und Heimarbeitsplatz nutzten, ein Einfallstor gewesen sein.

Darauf, dass es um die IT-Sicherheit des Gerichts schlecht stand, deutet dem Bericht zufolge einiges hin. Ein lokales Bekämpfen der Schadsoftware sei nicht möglich gewesen, heißt es, dafür habe es an Netzwerksegmentierung gemangelt. Die Protokollierung von sicherheitskritischen Vorfällen sei kaum hilfreich gewesen, weil der dafür zur Verfügung stehende Speicherplatz so klein gewählt war, dass er alle paar Tage überschrieben wurde. Software von *McAfee* habe die Schadprogramme nicht erkannt. Der „Tagesspiegel" schreibt, dass zudem sämtliche Back-up-Server des Kammergerichts zum Zeitpunkt des Bekanntwerdens der Infektion defekt gewesen seien.

Anders als bisher bekannt, soll es auch einen Datenabfluss gegeben haben. Zu welchem Zeitpunkt und in welchem Umfang dieser stattfand, wird laut „Tagesspiegel" im Gutachten aber nicht beschrieben. Im Herbst hatte unter anderem der Berliner Justizsenator Dirk Behrendt gesagt, dass nach „bisherigem Kenntnisstand" keine Daten abhandengekommen seien.

Die beauftragten IT-Expert*innen stellt der zeitliche Ablauf augenscheinlich nicht nur in Sachen Datenabfluss vor Rätsel. So soll es im Gutachten heißen, dass sich nicht rekonstruieren lasse, wann genau Emotet das Netzwerk infiziert habe.

Update, 13.50 Uhr: Mittlerweile ist eine öffentliche Version des Gutachtens auf der Website der Senatsverwaltung zu finden. Die IT-Expert*innen von T-Systems raten dem Gericht darin zu einem „kompletten Neuaufbau der IT-Infrastruktur". Die Untersuchung eines infizierten Computers hat dem Dokument zufolge ergeben, dass Emotet auf dem Rechner die eigentliche Schadsoftware Trickbot nachgeladen hat. „TrickBot ist in der Lage beliebige Schadmodule auszuführen", heißt es weiter: „Auf dem untersuchten Computer ließen sich drei Module identifizieren: Auf dem System gespeicherte Passwörter (insbesondere Browserpasswörter) werden extrahiert und an die Angreifer weitergeleitet. Dem Nutzer werden im Webbrowser Passwörter aktiv entlockt, insbesondere von Online-Banking Webseiten. Informationen über die Systeme werden dem Angreifer zugespielt."

Zum möglichen Startpunkt des Befalls heißt es: „Durch Untersuchung eines Clients ist eine Infektion ab spätestens 20.09.2019 um 17:52 nachgewiesen." Außerdem schreibt T-Systems: *„Die Module von Trickbot sind klar auf Datenabfluss ausgerichtet. Eine Verschlüsselung oder Manipulation von Dateien auf den Geräten konnte nicht nachgewiesen werden."*[110]

Daten von Rheinmetall gehackt

28.04.20 Interne Unterlagen im Netz: Der Rüstungskonzern Rheinmetall ist nach NDR-Recherchen von einem Datenleck betroffen. Mehr als 1000 interne Unterlagen kursieren im Netz, auch zu Panzerfahrzeugen. Neben dem Image-Schaden droht dem Konzern ein Bußgeld.

110 Quelle: https://www.spiegel.de/netzwelt/netzpolitik/emotet-trojaner-attacke-auf-berliner-kammergericht-folgenreicher-als-bisher-bekannt-a-5bf07265-0956-4a73-8c5d-5fe36c06771c

Interne Unterlagen des größten deutschen Rüstungskonzern Rheinmetall sind im Internet aufgetaucht, nachdem Hacker die Daten kopiert und zum Kauf angeboten hatten. Ein Aktivist kaufte die insgesamt 1400 Dateien nach eigener Aussage und stellte den Datensatz dann für jedermann zugänglich zum Download bereit. Das ist das Ergebnis einer Recherche des NDR.

Die Dokumente sind zum Teil mehrere Seiten lang und betreffen einen Zeitraum von etwa einem Jahr, die jüngsten Unterlagen sind auf Ende Januar dieses Jahres datiert. Der Datensatz liegt dem NDR vor. Es handelt sich überwiegend um Lieferscheine von Zulieferern und Dokumente aus der Qualitätssicherung von Rheinmetall.

Darunter sind auch Konstruktionspläne von Bauteilen gepanzerter Fahrzeuge, wie die Modelle Fuchs, Boxer, Yak und Scout. Die Bundeswehr und ausländische Armeen nutzen diese Fahrzeuge aktuell, auch in Auslandseinsätzen. Einige der Dokumente beinhalten Vertraulichkeitsvereinbarungen der Zulieferer, zum Teil tragen die Unterlagen Prüfstempel des Bundesamts für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr.

Woher die Daten genau stammen, ist unklar. Rheinmetall erklärt auf Anfrage, dass die konzerneigene IT nicht gehackt worden sei. Vielmehr sei ein externer Dienstleister, der für zwei Rheinmetall-Tochtergesellschaften tätig war, von dem „unzulässigen Datenabgriff durch Dritte" betroffen gewesen. Es handle sich demnach um „Lieferscheine sowie etwaige Begleitdokumente aus lokaler Warenanlieferung an einem deutschen Standort der beiden Rheinmetall-Tochtergesellschaften", so ein Sprecher. „Verschlusssachen und sonstige geheime Informationen" seien davon nicht betroffen. Man habe die Zusammenarbeit mit dem Dienstleister eingestellt und „alle notwendigen Maßnahmen ergriffen, um die Schwachstelle zu identifizieren, den Fehler abzustellen und vergleichbare Vorfälle für die Zukunft auszuschließen", teilte der Konzern-Sprecher weiter mit. Man habe außerdem die Behörden informiert und Anzeige gegen Unbekannt erstattet. Um welche Behörden es sich handelt, wollte der Sprecher auf Nachfrage nicht mitteilen. Das Bundesverteidigungsministerium erklärte auf Anfrage, man schätze das Datenleck als unkritisch für die Bundeswehr ein. Ob auch andere Nationen, deren Armeen Rheinmetall-Fahrzeuge einsetzen, informiert wurden und die Papiere sichten konnten, dazu äußerte sich Rheinmetall nicht.

Auch wenn das Datenleck die Sicherheit der Bundeswehr nicht gefährdet, könnte der Vorgang für Rheinmetall in Deutschland unangenehme Folgen haben. Die Datenschutzbehörde Nordrhein-Westfalen, wo Rheinmetall seinen Hauptsitz hat, sagte auf Anfrage, dass sie über den Vorfall zumindest nicht informiert worden sei. Auch auf wiederholte Nachfrage wollte sich Rheinmetall nicht dazu äußern, ob überhaupt eine Datenschutzbehörde über den Vorfall in Kenntnis gesetzt wurde.

NDR-Reporter konnten die Person recherchieren, die die Daten mutmaßlich veröffentlicht hat. Der Mann veröffentlicht regelmäßig im sogenannten Darknet – einem Bereich des Internets, der nur mit besonderer Software zugänglich ist und als besonders anonym gilt – gehackte Informationen. Er sagt von sich selbst, dass er aus aktivistischen Beweggründen gehandelt habe: *„Ich habe die Daten veröffentlicht, weil ich gegen den Handel mit Waffen bin"*, schrieb er dem NDR.

Das Veröffentlichen der Daten sei für ihn *„ein Weg des Protests"*. Nach eigenen Angaben kaufte er die Rheinmetall-Daten für 600 US-Dollar von einem ihm bekannten Hacker. Dieser habe bewusst einen deutschen Dienstleister aus der Rüstungsindustrie ins Visier genommen und dabei die Rheinmetall-Daten kopiert. Überprüfen lassen sich diese Aussagen nicht, der Hacker selbst war nach Aussage des Aktivisten nicht zu einem Gespräch bereit.

Bei einem anderen Vorfall war Rheinmetall im September 2019 von Hackern angegriffen worden. Dabei konnten die Angreifer nach Angaben des Konzerns eine Schadsoftware einschleusen, die die Produktion des Konzerns in Nord- und Südamerika stark beeinträchtigt hatte. In Brasilien, Mexiko und den USA sei die Produktion daraufhin eingestellt oder stark behindert worden. Rheinmetall stellt in den damals betroffenen Fabriken Bauteile für die Autoindustrie her.[111]

Türen öffnen per Webbrowser

Laut einer Meldung von *heise.de* (03.02.2020) beobachten Sicherheitsforscher weltweite Angriffe gegen Türöffnungssysteme, welche anschließend oft für *„Distributed Denial of Service (DDoS)"*-Angriffe genutzt werden (ähnlich wie die Ausnutzung von Schwachstellen in Überwachungskameras, die über das Internet erreichbar sind). Außerdem ist denkbar, dass die Angriffe für einen ersten Eingang in Firmennetzwerke ausgenutzt werden könnten. Hierfür wird eine kritische Sicherheitslücke (CVE-2019-7256) ausgenutzt, für die bis heute keine Sicherheitspatches existieren. Für einen erfolgreichen Angriff reicht eine präparierte HTTP-Anfrage aus, da die Türöffnungssysteme mittels eines Web-Servers gesteuert werden, der über einen normalen Browser ansprechbar ist.

111 Quelle: https://www.tagesschau.de/investigativ/ndr/rheinmetall-datenleck-101.html

Einsatz von Störsendern

Störsender zum Öffnen von Autos
Laut einer Meldung der Düsseldorfer Polizei wurden in der Vergangenheit wiederholt Störsender („Jammer") benutzt, um ein Verriegeln von teuren Autos zu verhindern. Anschließend wurden diverse hochwertige Dinge aus den Luxus-Autos entwendet. Als Störsender wurde laut der Pressemeldung ein Walkie-Talkie verwendet, das zu einem starken Störsender umgebaut worden ist. Anscheinend wird die Methode wiederholt zur Aneignung von wertvollen Gegenständen genutzt. In einer weiteren Pressemeldung wird von einer Personenkontrolle und dem Auffinden von weiteren Störsendern berichtet, die für das zuvor beschriebene Öffnen von Autos verwendet werden können. Da die Ermittlungsbehörden den beiden Kontrollierten keine Straftat nachweisen konnten und der Besitz von Störsender nicht illegal ist, mussten sie wieder auf freien Fuß gesetzt werden.

Risikofaktor GPS
Nach dem Wikipedia Beitrag „GPS-Jammer" ist die Signalstärke von GPS mit ca. −155 dBW außerordentlich schwach. Ein Störsender von nur wenigen Watt kann daher den Empfangsbereich von praktisch jedem Signal unterdrücken. Neben dem aktiven Stören von GPS-Signalen besteht laut dem Beitrag auch noch die Möglichkeit, die Koordinaten durch sogenanntes GPS-Spoofing zu fälschen. Zahlreichee Endgeräte nutzten GPS und verlieren ohne entsprechende Signale ihre Orientierung. Neben Smartphones wird GPS von Drohnen, Luxusjachten oder auch bei den noch in der Testphase befindlichen autonomen Fahrzeugen genutzt. Viele Geräte und Menschen verlassen sich auf die Technik, obwohl sie schwerwiegende, nicht zu behebende Schwachstellen aufweist. Neben *heise.de* kommt eine vom „Royal Institute of Navigation" organisierte Konferenz zu folgender Erkenntnis: *„GPS-Signale lassen sich noch immer problemlos unterdrücken und – was noch schwerwiegender ist – sogar manipulieren, um Nutzer in die Irre zu führen. […] Die leichte Unterdrückbarkeit ergibt sich schon aus der bescheidenen Sendeleistung. Die Signalstärke, die an einer herkömmlichen GPS-Antenne auf der Erde ankommt, entspricht in etwa der Stärke einer 25-Watt-Birne, wenn sie bei Tageslicht von einem Satelliten auf die Erde gerichtet und von unserem Heimatplaneten aus betrachtet würde."*

David Last vom Royal Institute of Navigation befürchtet, dass GPS-Jammer bald eine ähnliche Verbreitung finden könnten, wie sogenannte Handy-Blocker (Cafés und Kinos setzen die preisgünstigen Geräte in manchen Ländern bereits flächendeckend ein). Die Kosten für die GPS-Jammer sind ähnlich gering: Im Internet werden die Geräte bereits für unter 100 Dollar verhökert und längst von Kriminellen eingesetzt, um die Fluchtrouten geklauter Fahrzeuge zu verschleiern. Neben dem kommen Sicherheitsforscher*innen des „Argonne National Laboratory" zu dem Schluss, dass sich GPS „einfach fälschen" lässt. Die Hoffnung von Sicherheitsforscher*innen verschiedenster Couleur, dass die Schwachstellen durch den GPS-Nachfolger Galileo behoben werden, scheinen sich nicht zu erfüllen: Auf Druck der USA wird es auch hier möglich sein, das Signal per Jammer zu unterdrücken. Für David Last ist GPS in seinem aktuellen Zustand daher „wie ein Betriebssystem, bevor es die ersten Datenschädlinge gab". [112]

Student*innen kapern Drohne
In der Rubrik „Netzwelt" von Spiegel Online lässt sich ein Bericht über das Kapern von Drohnen finden, in dem erläutert wird, wie US-Student*innen durch einen Hack das GPS-System einer Drohne manipuliert haben und somit in der Lage waren, die Drohne, die sich in einem Kilometer Entfernung befand, fernzusteuern (in einer Vorführung ein Jahr später wurde gezeigt, dass dies auch bei einer Entfernung von zehn Kilometern funktioniert). Das Fernsteuern gelang über das Manipulieren der Signale der Navigationsatelliten (GPS-Spoofing). Das Expriment der Universität von Texas sollte grundsätzlich zeigen wie leicht es ist, zivile Drohnen fernzusteuern. Laut Todd Humphreys, dem Leiter des Forschungsprojekts, werden in fünf Jahren 30.000 Drohnen im Luftraum verkehren. In einem Interview mit Fox News gab er Folgendes im Bezug auf das Experiment der Student*innen zu bedenken: „Wenn man es mit den kleinen machen kann, dann kann man es auch mit den großen.". Zudem weist er darauf hin, dass militärisch genutzte Drohnen ein verschlüsseltes GPS-System nutzen (was es wesentlich schwerer machen dürfte, dort einzubrechen). Bei zivilen Drohnen hingegen gebe es „keine Absicherung" gegen derartige Angriffe. Laut der britischen BBC hat die Ausrüstung für den Versuch ca. 1000 Dollar gekostet.

Ein Mitbegründer des Internationalen Komitees für Roboter-Rüstungskontrolle fügt in einem BBC-Interview noch folgendes hinzu „Es ist sehr gefährlich – wenn eine Drohne mit ihrem GPS irgendwohin gelenkt wird, kann [ein Spoofer] ihr ‚einreden' sie sei woanders, um sie dann abstürzen zu lassen.". In einem Beitrag auf golem.de erklärt der Leiter des zuvor beschriebenen Test-Szenarios, dass ein stärkeres GPS-Signal immer gewinnt. Zudem hätte kein ziviler GPS-Empfänger ihrer Angriffstechnik im Labor widerstanden.

Kinder legen Drohnen lahm
In einem Cyper-Security-Wettbewerb in den USA gelang es zwei Schulkindern im Alter von elf und 14 Jahren, mit einfachen Mitteln, Drohnen zum Landen

112 Quellen: https://de.wikipedia.org/wiki/GPS-Jammer; https://www.heise.de/tr/artikel/Risikofaktor-GPS-943614.html

zu zwingen. Laut einer Meldung auf der Webseite von heise.de schafften sie dies mittels eines permanenten Störens („Jammen") der WLAN-Funksignale. Bei dem Wettbewerb wurden Parrot-Drohnen zum Landen gezwungen und konnten nicht wieder aufsteigen. Da die Drohnen auch von Sicherheitsbehörden genutzt werden, stellt heise.de die Frage in den Raum, inwieweit die Steuersignale nicht besser geschützt werden müssten.

Luxusjacht auf falschem Kurs
Forscher*innen aus der Uni Texas schafften es, eine 65 Meter lange Luxusjacht durch manipulierte Signale (GPS-Spoofing) auf den falschen Kurs zu bringen. Durch ein selbstgebautes Gerät war es möglich, die Satellitensignale zu „übertönen". Hierfür musste das an Bord gebrachte Gerät, das die Größe von einem Aktenordner besaß, aktiviert werden. Da das Gerät etwas stärkere Signale als der GPS-Satellit sendete, konnte das ursprüngliche Signal gefälscht werden. Die Crew der Jacht stellte während des Angriffs keine Unregelmäßigkeiten fest, sondern glaubte, dass sie auf dem richtigen Kurs ist. Ein an dem Experiment beteiligter Wissenschaftler (Todd Humphreys) betonte, dass das Experiment auch auf halbautonome Fahrzeuge, die ein ziviles GPS nutzen, angewendet werden kann und macht sich um die Sicherheit der weltweiten Container-Schiffe sorgen: „90 Prozent der weltweiten Fracht wird über die Meere transportiert. Stellen Sie sich vor, Sie schließen einen Hafen. Stellen Sie sich vor, Sie lassen ein Schiff auf den Grund sinken. Das sind die Auswirkungen, über die wir uns Sorgen machen."

Störsender gegen Smart Speaker
Ein Armband gegen Alexa: Die Mikrofone in einem Amazon Echo, Google Home oder anderen smarten Lautsprecher sind immer an. Anders könnten die Geräte schließlich nicht per Sprachbefehl aktiviert werden. In der Regel beginnen die Gesprächsaufzeichnung und die Verbindung zum Server des Herstellers erst nach dem Aktivierungswort, also etwa „OK Google" oder „Alexa". Aber keine Regel ohne Ausnahme.

Interpretiert das Gerät ein anderes Geräusch als Aktivierungswort, kann die Aufzeichnung auch unbemerkt starten. Um solche Situationen zu vermeiden, haben Forscher an der Universität von Chicago ein Armband entwickelt, das wie ein Störsender funktioniert. Wer es aktiviert, überlagert die Mikrofonaufzeichnungen von Smarthome-Geräten, aber auch Laptops und allem anderen, was ein Mikrofon hat.

Dafür sorgen kleine 24 Lautsprecher, die Ultraschallsignale aussenden. Für die meisten ist das unhörbar – außer für einige junge Menschen –, aber in Mikrofonen stören die Signale jede Sprachaufzeichnung. Übrig bleibt nur Rauschen.

Das Armband soll aus zwei Gründen besonders gut geeignet sein, um auch versteckte oder sonst wie nicht sichtbare Mikrofone zu erreichen: Erstens können die 24 Lautsprecher, ringförmig angeordnet, in viele Richtungen gleichzeitig abstrahlen. Zweitens ist die Hand beim Sprechen häufig in Bewegung, wodurch die Störsignale noch besser verteilt werden. „Blinde Flecken" der Abdeckung sollen so vermieden werden.[113]

SABOTAGE

Wie die angeführten Hacks, sind auch die hier beschriebenen Sabotageaktionen nur als Splitter oder Schlaglichter zu verstehen und nicht als eine erschöpfende Chronologie des weltweiten Dissens gegenüber dem technologschen Angriff. Sie zeigen unterschiedliche Wege auf, die Menschen im Widerstand gegen den technologschen Angriff einschlagen, wie auch immer wir diese bewerten mögen.

Brandstiftungsserie gegen Mobilfunkmasten April/Mai 2020

In den letzten Jahren war zu beobachten, dass vermehrt Funkmasten Ziel von Sabotageaktionen wurden. Bisher fanden diese Sabotagen jedoch eher vereinzelt statt und wurden häufig von einem Selbstbezichtigungsschreiben begleitet. In diesen Schreiben wurde zumeist die Motivation der Saboteur*innen dargelegt. Meist haben sich die Saboteur*innen dabei gegen die zunehmende Digitalisierung, Überwachung, etc. ausgesprochen. Anfang April 2020 fand nun eine europaweite Sabotagewelle statt, die medial wenig Beachtung fand. Die Föderation belgischer Technologieunternehmen Agoria zählte für April 88 solcher Sabotagen – großteils Brandstiftungen. Diese sollen im April in ganz Europa stattgefunden haben. Davon allein 61 in Großbritannien und 20 in den Niederlanden. Dabei dürfte die tatsächliche Zahl der sabotierten Funkmasten noch höher liegen. So konnten wir bei einer simplen Internet-Recherche weitere Beispiele von Funkmastbrandstiftungen in Italien, Belgien, Frankreich, Zypern, Deutschland und Irland finden. Und auch im Mai ebbte diese Sabotagewelle nicht ab. Sie weitete sich sogar weltweit aus. So gab es im Mai zusätzlich Funkmastbrandstiftungen in den USA und Kanada. Weiter stieg die Zahl der angezündeten Funkmasten vor allem in Frankreich an. Fast jede zweite Nacht brannten dort teils mehrere Funkmasten.

Die Motivation der einzelnen Saboteur*innen ist nicht bekannt, da bei dieser Welle an Funkmastsabotage bisher kaum Selbstbezichtigungsschreiben vorliegen. Der englische Guardian verbreitete die Theorie, dass es sich bei den Saboteur*innen um Verschwörungstheoreti-

113 Quelle: https://www.spiegel.de/netzwelt/gadgets/ein-armband-gegen-alexa-a-d6522934-fb01-480d-b911-efc94120c9c4

ker*innen handelt. Diese Behauptung wurde von anderen Medien aufgegriffen und auch im deutschsprachigen Raum z. B. in Faktenchecks zu Verschwörungstheorien reproduziert. Nachdem jedoch bisher kaum Leute für diese Sabotagen gefasst wurden und so gut wie keine Selbstbezichtigungen vorliegen, muss diese Behauptung mit Vorsicht genossen werden.

Viel eher kann diese Einordnung als Versuch gedeutet werden, diese anonyme Sabotagewelle inhaltlich komplett zu delegitimieren, indem die vermeintlichen Saboteur*innen – ohne große Evidenz – ins Verschwörer*inneneck gerückt werden. In Frankreich wurde medial ein ähnliches Manöver vollzogen. Dort wurden die vermeintlichen Saboteur*innen einer konstruierten „mouvance d'ultra-gauche" [„ultralinke Bewegung"] zugerechnet. Wir wissen nicht, wer hinter diesen Sabotagen steckt. Wir wollen auch gar nicht darüber spekulieren. Viel spannender finden wir es darauf hinzuweisen, dass die Dauer, Intensität und Ausbreitung dieser Sabotagewelle aufzeigt, dass unter der Oberfläche der Dissens gegen den fortlaufenden technologischen Angriff zu gären scheint. Vielleicht sogar mehr, als wir erklärte Kritiker*innen dieses Angriffs manchmal selbst für möglich halten. Und dass es offensichtlich zunehmend Menschen gibt – wie auch immer deren Motivation konkret aussehen mag – die zu dem Schluss kommen, dass der technologische Angriff schwerlich mit demokratischen Mitteln abgewandt werden kann.

Sabotage gegen Klimakiller

Schon seit mehreren Jahren sind Sabotagen im und um den Hambacherforst zu beobachten. Diese richtet sich direkt gegen die Infrastruktur von RWE, die RWE benötigt, um die Zerstörung des Hambacher Forsts ungestört fortzusetzen, wie Pumpen, Stromkästen, Kameramasten, etc. Auch um die Jahreswechsel 2018/19 und 2019/20 kam es wieder zu solchen Sabotagen. Doch diese Sabotagen gegen die Kohleindustrie beschränken sich nicht nur auf den Hambi, wie eine Sabotage zeigt, die am 07.08.2019 im Tagebau Vereinigtes Schleenhain in Pödelwitz bei Leipzig stattgefunden hat. Dort soll ein Kohleförderband durch eine nicht näher beschriebene Sabotageaktion lahmgelegt worden sein.[114]

Außerdem wurde 2019 durch zwei Sabotageaktionen der Bogen zwischen dem Ausbau und der Allgegenwart von digitaler Infrastruktur und Umweltzerstörung gespannt. Die erste fand in Berlin statt, wo am 23. September im Rahmen des Generalstreiks von Fridays for Future die Kabelstränge an mehreren Zugverbindungen angezündet wurden, unter anderem zum Flughafen Schönefeld. In dem längeren Schreiben[115] gehen die Saboteur*innen auf Flugverkehr und Umweltzerstörung und die Klimafrage ein.

Eine weitere Sabotage ereignete sich im Dezember 2019 in München, wir zitieren die Selbstbezichtigung:

„In der Nacht zum 19.12.2019 haben wir zwei Hauptkabel von Vodafone und den Stadtwerken München an zwei Isarbrücken in München mit Feuer lahmgelegt. Die Kabel versorgen neben Großbetrieben wie BMW das Heizkraftwerk Nord der Münchner Stadtwerke. Ziel war, einen möglichst hohen Sachschaden anzurichten, um die herrschende Klimapolitik praktisch anzugreifen.
Im Heizkraftwerk Nord wird noch viele Jahre Kohle verfeuert um Strom und Fernwärme zu gewinnen. Die Stadt München ignoriert konsequent den Bürgerentscheid gegen einen Weiterbetrieb, weil es angeblich als Hauptlastreserve am Netz bleiben muss – es bleibt nur die Möglichkeit, die Kosten für die Stadtwerke in die Höhe zu treiben um eine vorzeitige Stilllegung durchzusetzen.
Wir können nicht genau abschätzen, wie umfangreich die Störungen durch unsere kleinen Brände gewesen sind. In den spärlichen Zeitungsmeldungen wurde von tagelangen Reparaturarbeiten und einen Sachschaden von wenigstens 100.000 Euro gesprochen. [...]" [116]

Sabotage digitaler Überwachungs-Infrastruktur

Im April 2020 wurde in Berlin Charlottenburg ein offenliegendes Telekommunikationskabel bei einer Baustelle angezündet. Ziel der Saboteur*innen war das Stören des Heinrich-Hertz Instituts (HHI), welches zu dieser Zeit an der Corona-App gearbeitet hat. Wir dokumentieren hier das Schreiben der Saboteur*innen:

„Shut down the power! Digitale Zurichtung sabotiert. Wir erteilen der sogenannten Corona-App eine Absage und sind in Vorleistung gegangen. Wir haben heute, um jeder weiteren Aufweichung der Grundrechte und dem Ausbau der Überwachungsmaßnahmen entgegenzuwirken, einen Schacht mit Kommunikationskabeln, die u. a. das „Heinrich-Herz-Institut" versorgen, in Brand gesetzt. Die Netzkabel von Colt, Telekom und anderen Anbietern sollten durch unseren Anschlag zerstört werden. „Das Heinrich-Hertz-Institut" (HHI) war Ziel unseren Angriffs. Den offenen Schacht, in dem neue Kabel verlegt werden, haben wir als Zuleitung zum „HHI" identifiziert. Der kurzfristige Shutdown betraf auch weitere ansässige Konzerne, etwa Autohäuser von den Klimakillern VW, Alfa Romeo, Jeep, Mercedes, Audi, Porsche etc. Eine Gefährdung für Menschenleben haben wir ausgeschlossen.

114 Quelle: http://4sy6ebszykvcv2n6.onion/node/35621
115 Quelle: http://4sy6ebszykvcv2n6.onion/node/37756
116 Quelle: http://4sy6ebszykvcv2n6.onion/node/56930

Warum wir die Nutzung der App politisch sobotieren:
Die Verordnungen gegen die Pandemie bringen Ausgangssperren, Kontaktverbote und weitere Eingriffe mit sich, die in der Geschwindigkeit ihrer Umsetzung und ihrer Grundsätzlichkeit in der Geschichte der Bundesrepublik beispiellos sind. Begleitet werden diese Eingriffe immer wieder mit Kriegssprache. Das Vorbild für diese „Regeln" bildetet Chinas Umgang mit dem Virus. China: eine patriarchale Diktatur, die jede Bewegung der Menschen überwacht, kontrolliert und Verstöße gegen die von der kommunistisch-kapitalistischen Elite gesetzten „Regeln" bestraft. Die Abriegelungen von Millionenstädten kann nur in einem so effizienten totalitären System durchgeführt werden, als Maßgabe dafür, was möglich ist. China ist kurzfristig mit seiner 60 Tage dauernden totalen Ausgangssperre (bspw. in Wuhan) und der totalen Kontrolle der Menschen zum Modellfall der (behaupteten) Eindämmung der Pandemie für die Regierungen fast der ganz Welt geworden. Anfang Januar wurden diese Maßnahmen noch als totalitär und menschenrechtsverletzend kritisiert. Jetzt werden diese in abgewandelter Form ebenfalls in die anderen Erdteile transferiert.

Ganz in diesem Sinne schlug Jens Spahn mehrmals die Handyortung, das Daten-Tracking eines jeden Menschen vor, um die Infizierten und potenziell Neuinfizierte ausfindig zu machen und zu isolieren. Die Kritik von Verfassungsrechtler_innen und Datenschützer_innen hielt er sich mindestens zwei Meter vom Leib. Die totale Ortung des Bewegungsprofils eines jeden Menschen hat er sich von China und Südkorea abgeschaut. Der Parlamentspräsident in Österreich plädierte für die verpflichtende Einführung einer vergleichbaren App. Auch hierzulande wurden entsprechende Forderungen laut. Schon die Diskussionen sind kalkulierte Tabubrüche mit dem Ergebnis dem wachsendem Überwachunsgpotential neuer Technologien zur Akzeptanz zu verhelfen und gegebenenfalls auch autoritär zu steuern, wenn es nicht „freiwillig" geht.

In China wird die App von „Ant Financial" bei öffentlichen Kontrollen durch die Polizei eingesetzt. Der persönliche QR-Code entscheidet über den Einkauf im Supermarkt und den Spaziergang. Bei einem roten oder gelben QR-Code erfolgen Anweisungen der Behörden. Diese Bezahl-App entscheidet in intransparenter Weise über die „soziale Corona-Virus-Last". In Südkorea ist noch keine Ausgangssperre verhängt worden. Alle Menschen „dürfen" so lange weiterarbeiten, bis das Smartphone sie als „infiziert" oder als „Verdachtsfall" identifiziert und der staatliche Zugriff angeordnet wird. Aktuell zwingt die Regierung die Menschen in Südkorea, „freiwillig" ihre Handydaten und Zugänge offen zu legen. Das Tracking von Daten ist in Südkorea u. a. mit dem Programm „Total Information Awareness" erprobt worden, das von der NSA heimlich als „Prism" weiterbetrieben wurde, wie der Whistleblower Ed Snowden offenlegte. In den USA wollen Google und Apple eine Corona-App gleich automatisch als Betriebssystembestandteil mit einem kommenden Update verteilen.

Ein Daten-Tracing soll bald in Form einer installierten App auch in Deutschland etabliert werden. Die Propaganda für diese App arbeitet bereits auf Hochtouren. Die Politik wird massive Werbung dafür zumachen, denn nur die breite Akzeptanz verspricht ihrer Ansicht nach die gewünschten Effekte. Oberflächlich betrachtet hört sich die Nutzung der App sinnvoll an. Bei der Einführung setzt man (zunächst) auf Freiwilligkeit, um den frontalen Verfassungsbruch zu umgehen. Denn Kontakte, also infizierte und nicht infizierte Personen und ihr Umfeld, können ausgespäht werden. Aber wie auch bei der Weiterleitung (angeblich) anonymisierter Bewegungsprofile durch Mobilfunkanbieter, bei der die Betroffenen schon keine Einwilligungs- oder Verzichtmöglichkeit hatten, ist davon auszugehen, dass die in der App enthaltenen Überwachungsmöglichkeiten schnell zu einem zwingenden Standard werden, sind sie einmal bei einer kritischen Menge „freiwillig" etabliert: Wer in die Bibliothek will muss die App haben - der Besuch der Bibliothek ist ja freiwillig... Da der Quellcode der Software nicht offen liegt, ist keine Überprüfung möglich, ob die Propaganda zur Nutzung der App mit der Realität übereinstimmt, bzw. wer sich noch alles der Daten bedienen kann. Und ob nicht doch Möglichkeiten zum Daten-Tracking eingebaut sind. Ein einfaches Update der Software wäre jederzeit möglich. An dieser App arbeitet aktuell das „Robert-Koch-Institut" u.a. zusammen mit dem „Heinrich-Herz-Institut" und dem Bundesamt für Sicherheit in der Informationstechnik und der Bundeswehr.

Es wird reguliert:
Die Geschwindigkeit der täglichen Veränderungen ist kaum zu verarbeiten. Die Bekämpfung der Pandemie wird nicht umsonst immer wieder mit bewusst gewählter Kriegsrhetorik untermauert. Denn ein Krieg ist immer auch ein sozialer Angriff nach innen, um die „Volksgemeinschaft" oder - und das ist im Fall Corona neu - die Weltgemeinschaft auf die Interessen der Herrschaft neu zuzurichten. Dahinter steckt kein Plan der Verschwörung. Es ist die fortlaufende Dynamik herrschaftlicher Entwicklung, die seit Jahrtausenden nicht durch eine umfassende Revolution der Befreiung von allen Herrschaftsformen gebrochen werden konnte. Das Muster ist nicht neu: Krisen werden immer als Katalysatoren für repressive Regulationen der Bevölkerung genutzt, wenn eine revolutionäre Kraft nicht andere Akzente setzt. Im Angesicht der Pandemie wird eine Maschinerie der inneren Sicherheit in Gang gebracht, die davon lebt, dass alle mitmachen. Bei vielen Menschen

regeln die konzerneigenen Algorithmen hinter den Apps bereits die Tagesabläufe, sind ständiger Begleiter. Nun in Zeiten von Corona also sich einschränken, sich sozial distanzieren, bei Kontakt sich (und die anderen) beobachten - und sich dieses mit der App dann irgendwann einfach machen. Gutes und verantwortungsbewußtes Gefühl inklusive, man hat etwas zur Sicherheit aller beigetragen.

Neue Unwörter tauchen auf.
Mit dem „Krieg gegen den Virus" verändert sich auch die Sprache und das Denken. Plötzlich gibt es „systemrelevante" Menschen. „Risikogruppen", die sich selber isolieren sollen. „Soziale Distanz" als Heilsbringer zum Schutz der „Risikogruppen" und der „systemrelevanten" Menschen, den „Helden des Alltags". Letztere, das Pflegepersonal, die Supermarktangestellten, LKW-Fahrer_innen etc. werden zu Kämpfer_innen an der „Front" gemacht, anstatt sie anständig zu bezahlen - während die Manager sich weiterhin ihre Boni genehmigen und Hilfsmilliarden für ihre Konzerne kassieren. Das militärmedizinische Konzept der „Triage" stößt ins Zivile vor: die systematische Sortierung von Menschen: Wer zu retten ist und für wen es sich nicht mehr „lohnt", wer auf dem „Schlachtfeld des Virus" zurückgelassen werden muss. Dabei führt nicht der Virus als solcher zur Krise, sondern ein privatisiertes und profitorientiertes Gesundheitssystem führt zu dem gefürchteten Notstand in den Krankenhäusern und Pflegeheimen. In Spanien, in Italien und womöglich auch hier.

Dass jeder Mensch dem Tod schutzlos gegenüber tritt, zumal wenn er als unsichtbarer Virus auftritt und als neue Pandemie überhaupt nicht einschätzbar erscheint, schafft Ängste. Diese Ängste gilt es nicht kleinzureden. Es gilt, diese Ängste auch nicht zu überhöhen, zu etwas ganz außergewöhnlichem werden zu lassen, da wir alle eines Tages sterben werden. Doch die Urängste der Menschen vor dem Tod werden mit dieser Pandemie instrumentalisiert. Mit diesen Ängsten wird „gespielt". Nicht die Privatisierungspolitik in den Gesundheitssystemen wird in Frage gestellt, sondern ob DU genug Abstand zum Nächsten hältst. Ob DU die Regeln einhältst. Diese Regeln werden überwacht (und teilweise auch bestraft). Und sie fördern allerorten eine der deutschesten Tugenden: den Hang zur Denunziation. Ihm gesellt sich in intellektuellen Kreisen der Vorwurf hinzu, man sei unsolidarisch, wenn man nicht den Verordnungen folge. Wenn DU diese Regeln nicht einhältst, bist DU schuld daran, wenn Menschen sterben. Mit dem Verweis auf die „Risikogruppen" werden andere Widersprüche abgewürgt. Die „Risikogruppen" werden ungeachtet ihrer individuellen Haltung zu einem Faktor der moralischen Erpressung, um unter Freund_innen die staatlichen und politischen Regeln unhinterfragt durchzusetzen. Mit der medizinischen Hygiene geht eine soziale Hygiene einher, die kaum schmutziges, widerständiges Denken und Debattieren zulässt.

Von daher ist wahrscheinlich:
Unsere Aktion wird als unsolidarisch bezeichnet werden von jenen, die sich auch bei anderer Gelegenheit zum Handlanger staatlicher neuer Herrschaftstechniken und des sozialen technologischen Angriffes machen – auch ohne dass sie das vielleicht wollen. Unsere Erklärung wird entweder unterschlagen und einer unsichtbaren Nachrichtensperre unterliegen oder als wirr deklariert werden.

Wir stehen dabei solidarisch im Abseits:
Wir machen diese risikoreiche Aktion nicht, um breite Zustimmung zu erringen, dazu sind die Auseinandersetzungen im konterrevolutionären Sinne zu sehr zu unseren Ungunsten polarisiert. Wir wissen um die Zustimmung eines Teils der Gesellschaft. Wir stehen an der Seite derer, die nicht bereit sind, der Zerstörung historisch und schmerzvoll erkämpfter Menschenrechte zuzusehen. Wir stehen an der Seite der Geflüchteten an den Grenzen und in den Lagern. Wir stehen an der Seite derer, die die Instrumentalisierung der Pandemie und der Ängste erkennen und gegensteuern. Wir stehen an der Seite derer, die der wachsenden Überwachung beunruhigt gegenüber stehen.

Wie digitale Zurichtung geschieht:
Die Digitalisierung des Alltags, die unter dem Kontaktverbot und der Ausgangssperre zwangsläufig um sich greift und die plötzlich keine analogen Alternativen mehr zu kennen scheint, sehen wir als eine digitale Zurichtung der Gesellschaft. Auf den ersten Blick ist es für die isolierten Menschen die einzige Möglichkeit um miteinander in Kontakt zu bleiben. Aber der Raum, in dem das stattfindet, ist kein neutraler Raum. Er ist gesteuert und überwacht. Die sozialen Subjekte, die Menschen, werden zu virtuellen Figuren, die der Algorithmus in Datensätze zerlegt und anhand geheimer Kriterien beurteilt, Werbung steuert, Fehlverhalten markiert und meldet, Untertanentum belohnt. „Soziale Distanz" oder „Abstand ist Anstand" sind Begriffe, als wären sie aus Huxleys „Schöne Neue Welt" oder Orwells „1984" entlehnt. Es sind nackt besehen Kampfbegriffe, die uns ein Eintauchen in der virtuellen Welt als umfassende soziale Handlung zuweist. Ein „Wir" wird vorgegaukelt und dem „Wir" wird das Netz als neuer Ort der sozialen Begegnung und der Arbeitswelt angeboten - dabei wird die bereits durch den technologischen Angriff laufende soziale Vereinzelung weiter zementiert. Hier formiert sich die aktuelle und zukünftige Beherrschbarkeit ganzer Gesellschaften über das Netz.

Onlinehandel, digitaler Schulunterricht, Online-Seminare der Unis, Videokonferenzen, Homeoffice, elektro-

nische Patientenakten, Amazon, Zalando, Netflix, Lieferando, Kartenzahlungen, Datingportale, Videostreams und Spiele usw. sind Voraussetzungen dafür. Hier formiert sich Gesellschaft neu. Hier findet Gewöhnung statt, hier verändert sich Gesellschaft in einem Tempo, dessen Preis – die totale Manipulierbarkeit und damit Beherrschbarkeit - uns in allen Einzelheiten erst in den nächsten Jahren klar werden wird. Derzeit wird ein neues, nämlich hygienisches (nationales) „Wir" konstruiert, um alle möglichen Maßnahmen durchzusetzen, gegen die in der Vergangenheit Vorbehalte und Widerstände existierten, wie zum Beispiel bei der Digitalisierung in den Schulen, der gläsernen Krankenkassenkarten und Patientenakten oder der Online-Bezahlungen und dem Verschwinden des Bargeldes.

Die Telekom stellt, ganz uneigennützig, cloudbasierte „Web Conferencing Services" für Schüler_innen, Studierende und Lehrende umsonst zu Verfügung. Ähnliche Angebote gibt es passgenau auch für Unternehmen und deren Bedarf nach Homeoffice. Und für die Freizeit gibt es für die Kleinen den neuen Streamingdienst von Disney. Und zusätzlich 10 Gigabyte für das mobile Surfen obendrauf. Vorerst umsonst. Während die Telekom „Wir verbinden Deutschland" propagiert, lautet der Schlachtruf von Vodafone „Deutschland bleibt vernetzt". Die Angebotspalette unterscheidet sich nicht wesentlich. Aber Deutschland und das digitale Netz – das schafft Zusammenhalt. Der Coronavirus, ein Glücksfall für die Netzbetreiber: Neuer Bedarf nach schneller, breiter, mehr. Mit den aktuellen Angeboten bindet man zukünftige Kunden und generiert noch mehr Daten, auf die Firmen und Geheimdienste gleichermaßen zugreifen. So arbeitet Vodafone eng mit dem britischen Geheimdienst zusammen, der wiederum der engste Partner des amerikanischen NSA ist. Da die Menschen mehr Zeit im Netz mit sozialen Kontakten, Arbeiten und Vergnügungen zubringen, ist dies ein Fest für die Geheimdienste und Konzerne. Mehr Zugriff auf soziales Leben geht nicht. Wie viel mehr an Profit, wie viel mehr an Überwachung und Steuerung des Kaufverhaltens, der gewünschten Lebensweisen, der Früherkennung von Revolten lassen sich aus diesen Daten ableiten!

Spätestens seit Edward Snowdens Veröffentlichungen zu den weltweiten Überwachungen der NSA von Staaten und Gruppen bis hin zu einzelnen digitalen Äußerungen einzelner Menschen ist bekannt: Jede technische Möglichkeit der digitalen Überwachung und Verhaltenssteuerung wird auch genutzt. In China, in den USA, in Russland und auch in Deutschland. Die Corona-App ist ein Türöffner. Das Szenario, dass mindestens 60 Prozent der Bevölkerung in Deutschland auf eine App „freiwillig" konditioniert werden sollen, auf einen Standard, auf eine Intention, auf eine „freiwillige" Durchleuchtung aller privaten und öffentlichen Kontakte - das fordert unsere Sabotage geradezu heraus.

Was noch gesagt werden muss:
Wir erleben gerade eine weltweite Bürgerkriegsübung für zukünftige Krisen- und Kriegsfälle. Die Folgen dieser „Übung" werden die Welt verändern. Die Heftigkeit der Pandemie, deren Ausbreitung und die Masse der sterbenden Menschen sind die Matrix, auf der wir in ein neues Zeitalter der Krisen als Dauerzustand eingeführt werden. Im Zweifel zählen weder Grundrechte des jeweiligen Landes (die noch nie für alle galten) noch Menschenrechte. Während Kontaktverbote und Ausgangssperren erlassen werden, wird der Zwang zur Lohnarbeit aufrechterhalten und es ins Ermessen der Unternehmer gestellt, ob sie weiter wie gehabt arbeiten lassen, sich Kurzarbeit subventionieren lassen oder die Produktion auf Profitableres umstellen. Anderswo brachen da wenigstens die Streiks los. Hierzulande endet die Pandemiebekämpfung an den Werkstoren. Am Band und sonst, wo kein Homeoffice möglich ist, sollten die Menschen solange arbeiten wie es der Profitmaximierung dient und dann schnell in ihre Familien-Waben zurückkehren, da lassen auch die Gewerkschaften nichts anderes hören. Während die Waren weiterhin frei zirkulieren und die osteuropäischen Wanderarbeiter*innen pünktlich antreten sollen, damit die Wirtschaft nicht zusammen bricht, werden Geflüchtete in Lagern gehalten - Lager, die die rasante Ausbreitung des Virus garantieren und angemessene Gesundheitsversorgung garantiert nicht gewährleisten.

Die eine Krise löst nicht nur die Nächste ab, sondern bringt Themen zum Verschwinden. Die Klimakrise verschwindet hinter Corona. Verschwunden auch die Kriege und deren Folgen. Und die Gründe für die Kriege sowieso. Ungeklärt ist, wo die 10.000 Menschen hingekommen sind, die an der Grenze zwischen Türkei und Griechenland festsaßen. Unbestraft bleibt die EU, die diese Grenzen immer mehr in Todesstreifen verwandelt. Unbeobachtet bleiben auch die Vorbereitung von Pogromen in Ungarn gegen Roma und Sinti durch Orban und die Rechten. Ohne Reaktion bleibt die Nutzung des Virus für die Etablierung autoritärer Regierungen gegen die Verfassung wie in Polen. Oder den Machterhalt des korrupten israelischen Präsidenten. Oder für die Festigung der Macht von Putin.

Spätestens jetzt sollte erkennbar sein, wann die Regierung und die Wirtschaft auf Expert_innen und die Wissenschaft vertraut und wann nicht. Warum kann eine Pandemie ein Notprogramm und weltweite einschneidende Maßnahmen auslösen, der bereits stattfindende Kollaps des Klimas aber nicht? Diese Fragestellung ist übertragbar auf alle weltweiten Missstände.

Im Falle der Zerstörung des Klimas, welches die gesamte Menschheit mindestens ebenso betrifft wie die Pandemie, wurden und werden die Mahnungen und Vorschläge der Experten im Großen und Ganzen in den Wind geschlagen. Denn gegen die Folgen der Störung des Klimas ist es mit einem Impfstoff nicht getan. Ganz anders Corona: Gesundheitsexperten finden nicht nur offene Ohren, sondern ihr medizinischer Zugang zur Pandemiebekämpfung eröffnet der Politik neue Spielräume. Eine mörderische Wirtschaftsweise, ein kriegerisches Weltsystem und eine auf die Zerstörung der Erde und der Grundlage allen Lebens hinauslaufende Fortschritts- und Wachstumsorientierung werden mit Billionen Dollars und Euros gerettet, Proteste dagegen gesundheitsamtlich verboten. Es ist das koloniale Prinzip, nach dem Menschenleben unterschiedlicher Wert beigemessen wird. Jährlich sterben 100.000 Menschen an der Malaria. Der Klimawandel tötet schon heute: Hunderte Millionen Menschen hungern oder verhungern. Milliarden Menschen haben kein Zugang zu sauberem Trinkwasser.

In diesem neuen Zeitalter müssen sich die Kräfte, die eine grundsätzliche Veränderung wollen, neu orientieren und international neu aufstellen. Eine umfassende Umwälzung und Überwindung patriarchaler, kolonialer und kapitalistischer Verhältnisse ist keine Luxusfrage, sondern existenziell.

Wir werden uns nie gewöhnen, woran wir uns gewöhnen sollen. *Vulkangruppe shut down the power / Digitale Zurichtung sabotieren* P.S.: Für einen revolutionären 1. Mai gegen Kolonialismus, Patriarchat und Nationalismus“[117]

Sabotage gegen einzelne Akteur*innen

Die Akteur*innen und Profiteur*innen, die den technologischen Angriff vorantreiben, sind nicht nur von digitaler Infrastruktur abhängig. Genauso wenig wie ihre Projekt und Vorstöße, die nach und nach unser aller Leben umgestalten, nicht nur auf das Virtuelle beschränkt sind. Im Nachfolgenden besprechen wir Widerstandsmeldungen, die dies verdeutlichen.

Google: Im Widerstandsteil der letzten Ausagbe (Delete) berichteten wir über die Verhinderung des Google-Campus in Berlin Kreuzberg. Im Juni 2019 musste die „Google Cloud Experience Tour“ vorzeitig abgebrochen werden, nachdem der 15 Meter lange Tourbus in Frankfurt am Main abgebrannt ist. Ob es sich dabei um Brandstiftung gehandelt hat oder Google einfach nur schlechte Technik verwendet, blieb dabei offen. Wäre ersteres der Fall, wäre dies ein Zeichen, dass Google nicht nur in Berlin unerwünscht ist, sondern auch andernorts nicht willkommen.

Amazon: Nach Google versucht jetzt Amazon sein Glück in Berlin. In den im Bau befindlichen Edge-Tower sollen 3000 Mitarbeiter*innen von Amazon einziehen. Widerstand ist angekündigt und angelaufen. Wie sich diese Mobilisierung entwickeln wird, werden wir wohl in der nächsten Augabe besprechen. Darüber hinaus sind Büros, Locker und Lieferautos von Amazon mehrmalig Ziel von Sabotagen geworden.

So z. B. 2019, wo Anfang Februar in Berlin mehrere Autos von Amazon angezündet wurden, das Amazon Development Center Germany in Berlin-Mitte mit Pflastersteinen beworfen wurde sowie das Haus dessen Chef mit Farbe eingesaut wurde.[118]

Dass der Widerstand gegen Amazon nicht immer spektakulär ausfallen muss, zeigte z. B. auch ein Sabotageakt in München, wo im April 2020 acht ihrer Lieferautos die Reifen aufgestochen wurden. Dass diese Animosität gegen Amazon nicht nur ein deutschsprachiges Phänomen ist, zeigt z. B. ein Selbstbezichtigungsschreiben aus den USA, wo in LA County um den 1. Mai 2020 herum ein Amazon Van angezündet wurde. Die Saboteur*innen begründeten ihre Tat damit, dass Amazon unter anderem den Cloud-Service für die US Abschiebe-Behörde ICE stellt.

Tesla: Nach der Ankündigung von Tesla, eine Autofabrik für E-Autos in Grünheide (Brandenburg) zu bauen, gab es verschiedene Versuche, diesen Plan zu durchkreuzen. So wurde der Wald, der für diese Wohltat weichen muss, kurzzeitig besetzt – jedoch auch wieder geräumt. Des Weiteren wurden in Hamburg im Februar 2020 in Solidarität mit der Besetzung zwölf Tesla Autos mit Bitumen eingefärbt. Dazu schreiben die Saboteur*innen: „[…] Tesla ist ein Unternehmen, das von der Ideologie profitiert man könne alle Probleme dieser Welt letztendlich durch die Weiterentwicklung von Technologien lösen. Ein wichtiger Teil ihres Image ist es, dass die Technologien, an denen sie arbeiten (so sind sie z.B. Vorreiter in Sachen Künstlicher Intelligenz und Autonomes Fahren), einen Wert für die Allgemeinheit in sozialen, umweltbedingten und sicherheitstechnischen Bereichen haben. Wir lehnen die ständige Perfektion des Menschen durch die Technologie ab, da sie mit der Ausweitung von Kontrolle und der weiteren Einschränkung der Freiheit. Auch stellen wir uns gegen die Zerstörung der Natur, die entgegen gängiger Behauptungen, mit der Erweiterung von Technologien zwangsläufig einhergeht.

117 Quelle: http://4sy6ebszykvcv2n6.onion/node/77193

118 Quelle: http://4sy6ebszykvcv2n6.onion/node/28737

Wie heuchlerisch der Tesla Konzern ist zeigt sich gerade in Brandenburg. Innerhalb von wenigen Tagen hat Tesla in Grünheide (Brandenburg) 90 Hektar Wald abgeholzt um dort im Namen von Fortschritt und Profit eine riesige Fabrik zu bauen. 65 Hektar sollen noch folgen. Symbolisch wurden für die Presse ein paar Tiere „gerettet", die umgesiedelt werden sollen, während 30 „Harvester" Maschinen in Rekordtempo unzählige Tiere und ihren Lebensraum niedermetzeln. […]" [119]

Uber: Mit 2019 ist ein neues Gadget in die meisten Städt eingezogen, die dafür groß genug sind – Share E-Tret-Roller (E-Scooter). Diese ergänzen seither die (E-)Leihbikes, um die auch niemand gebeten hat. Weltweit wurde diesem Verstoß, der nicht nur die Daten der Nutzer*innen absaugt, sondern auch zutiefst umweltschädlich ist, sowohl mit Zustimmung als auch entschiedener Ablehnung begegnet. In den USA gab es einen eigenen Instagram-Account „Bird Graveyard", der nur der Dokumentation von Vandalismus gegen diese Tretroller gewidmet war. In Deutschland wurde zu einer Kampagne „Uber plätten" aufgerufen (https://uberplaetten.blackblogs.org/) mit dem Anliegen, sich speziell auf die Roller und Bikes von Uber zu konzentrieren – als Wiederstand gegen den ausbeuterischen Plattformkapitalismus.

Wer regelmäßig Zeitung liest, wird mitbekommen haben, dass der Vandalismus fast überall, wo diese Tret-Roller eingeführt wurden, zu einem Phänomen geworden ist. Ob dabei aus Spaß an der Sache oder bewusste Zurückweisung dieser intrusiven Gadgets, ist wohl eine Frage, die schwer zu beantworten ist. Jedenfalls zeugen mehrere Selbstbezichtigungsschreiben davon, dass es sich hierbei nicht nur um „blinden Vandalismus" handelt. So berichten etwa Saboteur*innen aus Köln in einem Schreiben, dass sie es geschafft hätten, durch konzentrierte Sabotage, die Roller aus einem Viertel zu verdrängen.[120]

Weiter dokumentieren wir hier noch ein Selbstbezichtigungsschreiben aus dem Jannuar 2020 aus der Schweiz, in dem darauf eingegangen wird, wie das Prinzip Uber funktioniert:

„Scherben bei WEF-Partner Uber
Während sich in diesen Tagen die Reichen und Mächtigen am World Economic Forum in Davos treffen, haben wir gestern Abend (23.Januar 2020) einen strategischen Partner des WEF besucht: Bei der Uber-Niederlassung an der Badenerstrasse in Zürich sind nun alle Scheiben kaputt. Uber bietet prinzipiell als strategischer Partner am Gipfeltreffen genügend Gründe für einen Angriff. Wir wollen zudem vertiefter auf die Machenschaften von Uber abseits des WEF eingehen.

Was 2009 in der USA begann, entwickelte sich zu einer Plattform mit jährlichen Umsätzen von weit über 10 Milliarden US-Dollar. Das Unternehmen agiert weltweit und ist heute viel mehr als ein günstiger Taxi-Ersatz und Essenslieferdienst. Zu den grossen Investoren gehören Goldman Sachs und Google (bzw. der Alphabet Konzern), die kaum aus gemeinnützigem Interesse Millionen investieren. Bei Uber geht es darum, neue Bereiche im Feld der Mobilität und allgemein des sozialen Lebens der kapitalistischen Verwertungslogik zu unterwerfen. Die Digitalisierung weiterer Lebensbereiche schreitet voran. In dieser neuen „smarten" Welt schiessen Apps und Plattformen wie Pilze aus dem Boden. Technologischer Fortschritt, welcher immer weitere Teil des Lebens für das Kapital nutzbar macht und immer weitere Teile des Lebens intensiviert nach seiner Logik strukturiert.

Firmen wie Uber präsentieren sich als neutrale Arbeitsvermittlungsplattformen und versuchen so zu vertuschen, wie sie ausbeuten. Sie sagen, dass sie nicht Chefs sind, die Mehrwert abzwacken, sondern lediglich Vermittler zwischen Selbständigen. Ihre verlogene Devise: FahrerInnen arbeiten nicht für, sondern mit Uber! Diese seien keine ArbeiterInnen, sondern VertragspartnerInnen. Was Uber als neue Form der Selbstständigkeit tarnt – vertraglich ist es den FahrerInnen offiziell selber überlassen, wieviel sie arbeiten wollen (Selbstausbeutung ahoi) - hat Kalkül. Mit dieser Anstellungsform stellt Uber seinen Arbeitskräften keine eigenen Produktionsmittel zur Verfügung. Die FahrerInnen tragen die Kosten für Auto, Versicherung, Benzin und Reparaturen selbst. Noch dazu stehen FahrerInnen als "Selbstständige" ohne soziale Absicherungen wie Unfallversicherung oder Rente da. Ein Zustand, der sogar die bürgerliche Justiz beschäftigt: Vor Bundesgericht wird darüber gestritten, ob Uber für Sozialabgaben an die FahrerInnen verantwortlich ist. Das Grossunternehmen droht für die Möglichkeit eines Urteils zu ihren Ungunsten (d.h. zu Gunsten der ArbeiterInnen) mit dem Wegzug aus der Schweiz. Für Uber bleibts in der Zwischenzeit auf alle Fälle ein lohnendes Geschäft, da sie pro Fahrt jeweils eine Provision von rund 20 Prozent des Fahrpreises für sich abzweigen. Die Pseudoselbstständigkeit der FahrerInnen verdeckt also den Zwang zur Lohnarbeit und zur Selbstoptimierung, denn Uber misst und bewertet das Arbeitsverhalten fortlaufend. Die zeitliche Verfügbarkeit oder die Anzahl abgelehnter und ausgeführter Fahrten werden bewertet und in einem Score erfasst. Mit diesem Score kann wiederum ein Algorithmus automatisiert beeinflussen, wer bevorzugt mit Fahraufträgen versorgt wird. Die immer weitergehende Prekarisierung von Arbeitsverhältnissen ist damit Teil des Uber-Geschäfts.

119 Quelle: http://4sy6ebszykvcv2n6.onion/node/68295
120 Quelle: http://4sy6ebszykvcv2n6.onion/node/57673

Von ihrer ungeheuren Datensammelwut und Datenauswertung, die natürlich auch die Uber-PassagiererInnen betreffen, ganz zu schweigen. Google und Facebook haben es bereits vorgemacht: Die Verwertung von Daten wird zum profitablen Geschäftsmodell und umfasst nicht nur die Erfassung, sondern auch Lenkungsmöglichkeit sozialer Konnektivität. Digitale Unternehmen arbeiten weiter daran, uns die Digitalisierung als technlogischem Allerheilmittel zu verkaufen.

Wir möchten auf alle Fälle dazu einladen, sich nicht von Uber und Konsorten blenden zu lassen, sich nicht auf ihre Selbstdarstellung als unangreifbare Akteure in einer fernen nicht-materiellen Cloud einzulassen. Sondern sich mit ihnen und der Arbeits- und Lebenslogik, die sie entwickeln und potenzieren, auseinanderzusetzen und genau hinzuschauen, wo sie angreifbar sind. Auch die digitalen Giganten haben Büros und Schnittstellen mit der nicht-digitalen Welt, an denen sie angreifbar sind. Uber hat etwa Zweigstellen wie die angegriffene, bei der es kurze Arbeitseinführungen gibt oder Uber-Eats-Tragtaschen verteilt werden, Google besetzt weite Teile der Europaallee mit ihren Büros und Firmen wie Amazon sind auf eine vernetzte und komplexe Logistik angewiesen, die an jeder Schnittstelle wiederum angreifbar sein kann. Setzen wir ihrem digitalen Angriff unseren analogen Widerstand entgegen.
Uber heisst Ausbeutung - Smash WEF!“[121]

121 Quelle: https://barrikade.info/article/3119

Autonomes Fahren und die smarte Überwachungen der Straßen: Eine interessante Sabotage gegen den Vorstoß des Autonomen Fahrens ereignete sich im Dezember 2019 in Osnabrück. Dort wurden die Wegmarker, an denen sich der autonome Bus (Hubi) orientiert, entfernt bzw. farblich verändert. Die Saboteur*innen begründeten ihre Aktion wie folgt: „Das Fahrzeug soll die Strecke einlesen und später dann willige Mithelfer*innen, die sich, natürlich per App, als Testnutzer*innen verdingen können, aufnehmen. Im Klartext: Der Bus filmt alles und jede*n ab, sammelt also Daten ohne Ende. Die werden analysiert, verarbeitet und dank vieler vernetzter Sensoren Bewegungsmuster erstellt. […] Gegen die Smartifizierung von Städten, Kontrolle und Macht. Smarte Infrastruktur angreifen; […]“[122]

Eine weitere Sabotage ereignete sich im Juli 2019 in NRW, dort wurde an der B514 eine Mautsäule angezündet. Die Saboteur*innen schrieben dazu folgendes: „[…] Das Aufstellen dieser Kamerasäulen an den Bundestraßen nehmen wir als direkten Angriff auf unser freies, also unüberwachtes, unregistriertes Bewegen wahr. Dies reiht sich ein in das von den Herrschenden stark vorangestriebene Projekt jeden Aspekt unseres Lebens kontrollieren und steuern zu wollen. Gerade in dieser sich immer autoritärer entwickelnden, durchdigitalisierten Gesellschaft ist es erforderlich die Überwachungstechnik anzugreifen – überall! Mit jeder Kamera, die nicht mehr filmt, mit jeder Mautsäule, die nicht mehr registriert, mit jedem „smarten“ Gerät, das nicht mehr mithört, erkämpfen wir uns ein (kleines) Stück Freiheit. […]“[123]

122 Quelle: http://4sy6ebszykvcv2n6.onion/node/53333
123 Quelle: http://4sy6ebszykvcv2n6.onion/node/34391

Glossar

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 kriegen. Oft ein wohl gehütetes Geheimnis.

Altruismus - Selbstlose Denk- und Handlungsweise; Uneigennützigkeit.

Bias - Durch falsche Methoden/Vorannahmen verursachte Verzerrung des Ergebnisses.

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.

Blockchain - Kontinuierlich erweiterbare Liste von Datensätzen, „Blöcke" genannt, die mittels kryptographischer Verfahren miteinander verkettet sind.

disruptiv - Als disruptiv wird etwas bezeichnet, was etwas Bestehendes (System/Technologie) aus dem Gleichgewicht bringt oder zerstört.

DDoS - Blockade eines Onlinedienstes durch zahlreiche Anfragen ausgehend von verteilten Quellen (z. B. Botnetze).

Doxxing - Internetbasiertes Zusammentragen und anschließendes Veröffentlichen von persönlichen Daten mit bösartigen Absichten gegenüber der betroffenen Person.

Egalitär - Heißt, etwas ist auf Gleichheit gerichtet oder strebt soziale Gleichheit an.

Fin-Tech - Meint Finanztechnologie, ein Sammelbegriff für technologische „Innovationen" im Finanzsektor.

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.

Hegemonisierung - Ausweiten einer Vorherrschaft.

Malus - Das Gegenteil eines Bonus, wenn beispielsweise Krankenkassen ein für sie aus wirtschaftlicher Sicht negatives Verhalten (wie beispielsweise Zigaretten rauchen) mit höheren Gebühren bestrafen.

Metadaten - Daten, die Informationen über andere Daten enthalten. Z. B. bei einem Telefongespräch nicht die Gesprächsinhalte, sondern wer mit wem telefoniert.

Nudging - Das Beeinflussen von Personen zu bestimmten Handlungen mittels Anreizen.

Partizipation - Gleichbedeutend mit Beteiligung und Teilhabe, z. B. an gesellschaftlichen Prozessen.

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

peripher - Gleichbedeutend für am Rande liegend. Zum Beispiel die Außenbezirke der Städte.

Postfaktisch - Handeln und Denken, bei dem Fakten nicht im Mittelpunkt stehen.

Pseudonym - Bedeutet hier, dass bei einer Verarbeitung von personenbezogenen Daten der Bezug zu einer natürlichen Person nur unter Zuhilfenahme zusätzlicher Daten möglich ist.

Retropie - Eine rückwärtsgewandte Utopie.

Smartifizierung - Erweiterung eines normalen Industrieprodukts um „intelligente" Eigenschaften, mit Hilfe von Informationstechnologien.

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.

Telematik - Bereich in der IT, welcher die Bereiche Telekommunikation und Information vernetzt.

A DIY guide to robbing banks

«**I hacked a bank.** I did it to give an injection of liquidity, but this time from below, for the simple and humble people that resist and rebel against injustice all over the world. In other words, I robbed a bank and gave away the money. But I didn´t do it myself. The free software movement, the offensive powershell community, the metasploit project, and the general hacker community made the hack possible. The community at exploit.in made it possible to turn the compromise of a bank´s computers into cash and bitcoin. And the Tor, Qubes, and Whonix projects, along with cryptographers, and anonymity and privacy activists, are my nahuales (protectors). They accompany me every night and make it possible for me to remain free.

I didn´t do anything complicated. I just saw the injustice in this world, felt love for everyone, and expressed that love the best way I knew how, through the tools I knew how to use. I´m not motivated by hate for banks or the rich, but by a love for life, and a desire for a world where everyone can realise their potential and live fully. I hope to explain a little how I see the world, so you can understand how I came to feel and act this way. And I hope this guide is a recipe you can follow, to combine the same ingredients and bake the same cake.
Who knows, maybe these same powerful tools can help you to express your love.

Make no mistake, expropriation is not theft. It is not the confiscation of «hard-earned» money. It is not the stealing of private property. It is, rather, the recuperation of massive amounts of land and wealth that have been built on the back of stolen natural resources, human enslavement, and coerced labor, and amassed over a number of centuries by a small minority. This wealth ... is illegitimate, both in moral principle and in the exploitative mechanisms in which it has used to create itself.

Through our collective belief that the financial system is unchallengeable, we control ourselves, and maintain the class system without those at the top really needing to do anything. Seeing how vulnerable and fragile the financial system really is helps to break that collective delusion. So banks have a strong incentive to not report hacks, and to overstate the sophistication of the attackers. Every financial hack that I´ve done or known of has not been made public. This will be the first, and only because I decided to publish, not the bank.

As you´ll learn in this DIY guide, hacking a bank and wiring out money through the SWIFT network does not require the backing of a government, or a large, professional and specialised group. It is entirely possible as an amateur, unsophisticated hacker, with public tools and basic scripting knowledge.»

(...)

DIY-Anleitung zum Bankraub

100.000 Dollar für antikapitalistische Firmen-Hacks

Was ist das Hacken einer Bank gegen die Gründung einer Bank? Dieses abgewandelte Brecht-Zitat scheint das Motto von Phineas Fisher zu sein. Mit dem erbeuteten Geld stiftet sie oder er zu antikapitalistische Hacks an.

In einem «hacktivistischen Bug-Bounty-Programm» verspricht Phineas bis zu 100.000 US-Dollar für jeden erfolgreichen Angriff in Abhängigkeit vom öffentlichen Interesse und der Wirkung des Hacks sowie dem damit verbundenen Aufwand. Phineas wolle mit dem Geld niemanden reich machen, sondern lediglich ausreichende Mittel bereitstellen, damit Hacker ihren Lebensunterhalt in würdiger Weise mit guter Arbeit verdienen könnten, erklärt Fisher. Die Hacker*in war bekannt geworden, weil sie in den vergangenen Jahren die Trojaner-Hersteller Gamma International und Hacking Team gehackt hatte.

Die Ankündigung findet sich in einer spanischsprachigen Anleitung, in der Phineas Fisher den Hack der Offshore-Bank Cayman Bank and Trust Company vor fast vier Jahren beschreibt. Das kapitalismuskritische Manifest wurde ebenso wie zwei Terabyte an Daten auf der Domain Ddossecrets.com veröffentlicht.

Der Anleitung zufolge überwachte die Hacker*in die drei für Swift-Überweisungen zuständigen Bankmitarbeiter mit Hilfe von Keyloggern und Screengrabbern. Da sie die Passwörter der Mitarbeiter erbeutet hatte, konnte anschließend selbst Überweisungen veranlassen. Allerdings fielen die illegalen Überweisungen bereits nach einem Tag auf, weil sie bei einer geplanten Transaktion in Höhe von 200.000 Britischen Pfund nach Mexiko eine falsche Angabe gemacht hatte.

Mit dem erbeuteten Geld zielt Phineas Fisher nun auf Hacks von Firmen, die im Bergbau sowie in der Holz- und Viehwirtschaft aktiv sind «und unser schönes Lateinamerika ausbeuten». Auch interessiert sie Material zu Militärdienstleistern wie Blackwater (jetzt Academi) oder Halliburton sowie zu privaten Gefängnisbetreibern oder Lobbyisten wie ALEC.

Phineas Fisher will aber mit dem Geld aus seinem digitalen Bankraub nicht nur Hacker finanzieren, sondern auch Mitarbeiter zum Ausspionieren ihrer Firma oder Chefs anstiften. Als Beispiel nennt sie die Installation von Keyloggern oder das Verstecken von Mikrofonen in Konferenzräumen.

Die englische Übersetzung der Erklärung:
https://data.ddosecrets.com/file/Sherwood/HackBack_EN.txt

Das spanische Original:
https://web.archive.org/web/20191117042838/http://data.ddosecrets.com/file/Sherwood/HackBack.txt