Regierungsforschung.de
Das wissenschaftliche Online-Magazin
der NRW School of Governance

Essay

Daniel Moßbrucker

Überwachbare Welt: Wird das Darknet zum Mainstream digitaler Kommunikation?

30. Mai 2018

UNIVERSITÄT DUISBURG ESSEN

NRW School of Governance
www.nrwschool.de

Redaktion/ Wissenschaftliche Koordination

Julia Rakers
Tel. +49 (0) 203 / 379 – 3742

Sekretariat

Anita Weber
Tel. +49 (0) 203 / 379 - 2045
Fax +49 (0) 203 / 379 - 3179
anita.weber@uni-due.de

Herausgeber (V.i.S.d.P.)

Univ. Prof. Dr. Karl-Rudolf Korte

Redaktionsanschrift

Redaktion Regierungsforschung.de
NRW School of Governance
Institut für Politikwissenschaft
Lotharstraße 53
47057 Duisburg

redaktion@regierungsforschung.de

Zitationshinweis

Moßbrucker, Daniel (2018): Überwachbare Welt: Wird das Darknet
zum Mainstream digitaler Kommunikation?, Essay, Erschienen auf: regierungsforschung.de

Überwachbare Welt: Wird das Darknet zum Mainstream digitaler Kommunikation?

Von Daniel Moßbrucker[1]

Abstract

Der Beitrag diskutiert die Frage, inwiefern das Darknet Zukunftspotentiale für digitale Kommunikation besitzt. Aufgrund staatlicher Machtstrukturen ist davon auszugehen, dass Überwachungs- und Kontrollmöglichkeiten zukünftig auf die digitale Sphäre übertragen werden. Davon könnte auch das Darknet betroffen sein, das als Sinnbild eines „freien Netzes" gilt. Dem staatlichen Trend wirken gerade diejenigen entgegen, die als Risikogruppen von Überwachung gelten, zum Beispiel JournalistInnen. Sie benötigen weiterhin Freiheitsräume im Internet, um ihrer gesellschaftlichen Aufgabe nachkommen zu können. Das Darknet kann dabei eine Rolle spielen, wenn es so weiterentwickelt wird, dass es die Sicherheitsbedürfnisse dieser Risikogruppen befriedigt. Diese liegen insbesondere darin, verschlüsselte Kommunikation zusätzlich zu anonymisieren. Praktisch müssten dafür bestehende Kommunikationsangebote wie Chat-Apps eine Zusatzfunktion zur Anonymisierung integrieren. Das Darknet würde damit „sein Gesicht" verändern, weg von einer internetähnlichen Website-Sammlung, hin zu einer im Hintergrund arbeitenden Technologie moderner Kommunikationsmittel. Diese Entwicklung wird nicht von allein einsetzen, weil globale Technologie-Konzerne digitale Innovation bestimmen und kein ökonomisches Interesse an einer Anonymisierung haben. Stattdessen müssten die Risikogruppen als Treiber einer „Darknet-Reform" fungieren, indem sie politisch und wirtschaftlich hierfür eintreten.

1. Bleibt Anonymität im Digitalen möglich?

Das Internet ist für die Ausübung gesellschaftlicher Freiheiten zu einem mächtigen Instrument avanciert, was neue Kommunikationsmöglichkeiten wie soziale Netzwerke täglich vor Augen führen. Ebenso evident ist, dass die Digitalisierung gerade Redefreiheit und Privatheit vor eine Herausforderung stellt: Wenn alles mit allem vernetzt ist, dann erhalten diejenigen tiefste Einblicke in die Privatsphäre, die Zugriff auf solche Netzwerke haben. Das sind zuvorderst kommerziell agierende Unternehmen, doch auch Staaten verschaffen sich Zugriff auf globale Informationsflüsse oder verpflichten Unternehmen zur Kooperation.

[1]Daniel Moßbrucker arbeitet als Security-Trainer für JournalistInnen in Berlin und publiziert regelmäßig zu den Themen Überwachung, Datenschutz und Internetregulierung. Er studierte Journalistik an der TU Dortmund sowie Digital Journalism an der Hamburg Media School. Bei der Menschenrechtsorganisation Reporter ohne Grenzen ist er als Referent für Internetfreiheit tätig. Außerdem arbeitet er an einer Promotion zur Frage, wie sich Überwachung langfristig auf den Journalismus auswirkt.

Ein digitales Zeitalter ist qua Definition ein überwachbares Zeitalter. Spätestens der durch Edward Snowden aufgedeckte Geheimdienst-Skandal offenbarte, dass Regierungen sukzessive ihre Überwachungsprogramme auf digitale Räume ausweiten. Das Ziel ist nicht unbedingt, alles zu wissen, sondern alles wissen zu können. Wohin führt diese Entwicklung? Beschreibt sie das Ende von Redefreiheit und Privatheit, den Beginn eines „neuen Typs" dieser Freiheiten oder ist das Internet an sich so beschaffen, dass es immer Räume bieten wird, die sich dem staatlichen Zugriff entziehen?

Die Analyse dieser Fragen führt am Ende unweigerlich zum Darknet, denn es steht heute als Relikt eines freien, zensurfreien Internets. Es gilt als Netz der Extreme, in denen Kriminelle mit Drogen und Waffen handeln können. ErmittlerInnen hingegen können trotz Massenüberwachung und Hacking-Fähigkeiten nur schwierig die Täter überführen. Die EntwicklerInnen der Technologie rechtfertigen ihren Einsatz mit den positiven Zwecken des Darknets, wenn es etwa AktivistInnen in repressiven Ländern hilft. Das Darknet ist damit das digitale Dilemma par excellence, mit dem öffentlich der Konflikt von „Sicherheit versus Freiheit" diskutiert wird. Seine Zukunft steht insofern sinnbildlich für die Zukunft der Online-Freiheiten überhaupt. Entweder fällt es der staatlichen Überwachung zum Opfer oder, im anderen Extrem, das Darknet und die damit verknüpften Ideale wie Anonymität werden zum Mainstream digitaler Kommunikation, sodass die digitale Überwachung insgesamt zurückgeht.

Dieser Beitrag diskutiert die Zukunftspotentiale des Darknets im Kontext staatlicher Überwachung. Zunächst wird Überwachung konzeptionell begründet als inhärenter Teil staatlicher Machtausübung. Es zeigt sich, dass es im aktuellen Staatensystem kein „natürliches Ende" im Ausbau der Überwachung geben wird. Umso relevanter wird es, die „Gegenseite" in den Blick zu nehmen: Wer hat ein Interesse daran, das Darknet weiterzuentwickeln, um gesellschaftliche Freiheiten zu bewahren? Es sind vor allem einige Gesellschaftsgruppen wie JournalistInnen und ihre Quellen, die auf Schutz vor Überwachung angewiesen sind. Sie kommen als Treiber einer „Darknet-Reform" in Betracht. In der Analyse ihrer Bedürfnisse zeigt sich, was das „Darknet der Zukunft" leisten müsste, um fortbestehen und massentauglich zu werden. Zuletzt wird kritisch hinterfragt, ob diese Entwicklung des Darknets realistisch sein kann, wenn globale Technologie-Konzerne wie Google, Facebook oder Apple weiterhin digitale Innovation bestimmen, weil sie an einem anonymen, schwer überwachbaren Internet kaum ein Interesse haben dürften.

2. Der „natürliche" Ausbau staatlicher Überwachung

Diskussionen um eine zeitgemäße Sicherheitspolitik sind heute gekennzeichnet durch zwei Lager. Auf der einen Seite stehen diejenigen, die im Lichte „neuartiger Gefahren" stärkere Überwachungsbefugnisse staatlicher Behörden fordern. Als Rechtfertigung werden meist zwei Argumente angeführt: Erstens habe der Staat die Aufgabe, für die Sicherheit seiner BürgerInnen zu sorgen und damit die natürliche Pflicht, in individuelle Rechte wie etwa das Kommunikationsgeheimnis einzugreifen. Es gibt demnach ein Grundrecht auf Sicherheit (Isensee 2012). Zweitens richteten sich die Maßnahmen nur gegen Kriminelle, sodass gesetzestreue BürgerInnen nichts zu befürchten haben. Greifbar wird diese Haltung in Phrasen wie „Datenschutz

darf kein Täterschutz sein“ (Lohmann 2017). Sicherheit wird dadurch zu einem Wert an sich, der andere Werte überragt oder zumindest mit anderen in Balance gebracht werden muss (siehe 2.1). Auf der anderen Seite stehen diejenigen, die ihre Argumentation nicht von einer abzuwehrenden Gefahr ausgehend denken, sondern von individueller Freiheit, die es zu verteidigen gilt. Im Kern steht dahinter die These, dass der Staat die Freiheit seiner BürgerInnen nicht schützen kann, indem er diese Freiheit zunehmend einschränkt (Baumann et. al 2014: 134-144; Weller 2012). Gesellschaftliche Gruppen wie JournalistInnen, die auf die Wahrung ihrer Freiheiten angewiesen sind, gehören daher zu Vertretern dieser Position (siehe 2.2).

2.1. Panoptismus als Organisation staatlicher Macht

Prinzipiell können sicherheitspolitische Prozesse auf zwei Weisen enden: Entweder mit einer Zunahme an Überwachung, wenn sich das „Sicherheitslager“ durchsetzt, oder mit einer Zunahme an Freiheit, wenn sich das „Freiheitslager“ durchsetzt. In der Praxis zeigt sich jedoch, dass seit Jahrhunderten, spätestens seit Beginn der Industrialisierung, die Überwachungsgesetze eher verschärft statt abgebaut werden. Dies hat vor allem damit zu tun, wie die beiden „Lager“ verteilt sind: Der Staat, genauer: die Regierung, steht tendenziell für stärkere Kontrollmöglichkeiten gegenüber den eigenen BürgerInnen ein, anstatt sie zu begrenzen. Das gilt auch für freiheitlich-demokratische Gesellschaften, denn auch hier fordern die BürgerInnen Sicherheit für ihr eigenes Leben, für die staatliche Institutionen zu sorgen haben. Die BürgerInnen legitimieren das staatliche Gewaltmonopol immer auch dann, wenn sie dafür ein Mehr an Sicherheit erhalten, notfalls auch zu Lasten individueller Freiheiten. Überwachung ist im diesen Verständnis eine moderne Form staatlicher Macht, das Mittel zum Zweck „Sicherheit“, welche der Staat einsetzen muss, um die gesellschaftlichen Interessen zu wahren.

Historisch hat diese Entwicklung der französische Philosoph und Soziologe Michel Foucault in seinem Werk „Überwachen und Strafen“ aufgearbeitet (Foucault 1977). Sein darin begründeter Panoptismus gilt als eine der grundlegenden Theorien, um Funktion und Wirkung von Überwachung untersuchen zu können. Foucault analysierte hierfür einen Wandel in den europäischen Justiz- und Bestrafungssystemen seit dem 18. Jahrhundert. Bestrafung durch die Staatsgewalt wurde „milder“, weg von grausamer Folter und Todesstrafen, hin zu Freiheitsentzug, um TäterInnen zu resozialisieren. (Foucault 1977: 102-104).

Die Entwicklung ist zeitlich gekoppelt an die Industrialisierung. So wurden etwa auch die Großfabriken architektonisch und organisatorisch verstärkt so konzipiert, dass jeder Mensch feste Arbeitsorte, -zeiten und -aufgaben erhielt. Normabweichendes Verhalten oder schlichtweg zu geringe Produktivität waren einfacher identifizier- und sanktionierbar. Es entstand ein hierarchisches System, welches derjenige steuerte, der es bestmöglich kontrollierte. Hieraus entwickelte sich eine neue Form der Macht, weg von einer direkten, repressiven Durchsetzung von Interessen, hin zu einer granularen Machtverteilung. In diesem Verständnis besitzt ein System selbst Macht und wirkt auf freie Subjekte disziplinierend. Hierarchische Überwachung ist Grundlage dieses Machttyps, der zum Zwecke der Produktivitätssteigerung nicht als Terror auftreten darf, sondern als „Zuchtgewalt“, die „anstatt zu entziehen und zu entnehmen, vor allem

aufrichtet, herrichtet, zurichtet – um dann allerdings um so mehr entziehen und entnehmen zu können“ (1977: 220). Es ist eine „Disziplinarmacht“, die systeminhärent wirkt, ohne sichtbar sein zu müssen – und dennoch kontrollierbar ist, nämlich durch den Überwacher an der Spitze der Hierarchie.

Symbolisiert wird diese Machtform der „Disziplinargesellschaft“ im Panoptikum, einem Gefängnis, das auf Jeremy Bentham zurückgeht (Bentham 1791). Es ist ein rundes Gefängnis, in dem die Gefangenenzellen auf der Kreislinie liegen. In der Mitte steht ein Wachturm. Für die Häftlinge ist nicht zu erkennen, wo oder ob überhaupt ein Wächter im Turm steht. Sie gehen davon aus, zu jeder Zeit überwacht werden zu können. Überwachung wirkt, selbst wenn sie gar nicht stattfindet.

Das Modell des Panoptikums ist laut Foucault nicht auf ein Gefängnis beschränkt, sondern auf die Gesellschaft selbst übertragbar. Die Disziplinargesellschaft ist insofern immer auch eine panoptische Gesellschaft, in der ständiger Druck „bereits vor der Begehung von Fehlern, Irrtümern, Verbrechern wirkt“. Sie ist dann am produktivsten, wenn „die Macht ohne Unterbrechung bis in die elementarsten und feinsten Bestandteile der Gesellschaft eindringen kann (...)“. Zu diesem Zweck ist lückenlose Überwachbarkeit das Mittel (Foucault 1977: 264-267).

Der Panoptismus ist bis heute ein wichtiges Theoriekonzept für die sogenannten „Surveillance Studies“, in denen Überwachung sozialwissenschaftlich erforscht wird. Foucaults Thesen wurden hier weiterentwickelt, aber auch kritisiert. Gerade im Kontext der Digitalisierung wird diskutiert, inwiefern Foucaults skizzierte Machtasymmetrie zwischen Staat (Überwacher) und BürgerInnen (Überwachte) noch zutrifft. Unter Begriffen wie „sousveillance“ oder „counter-surveillance“ (Mann et al. 2003, Schaefer/Steinmetz 2014, Rothmann 2017) wird argumentiert, dass heute auch BürgerInnen vielfältige Überwachungsmöglichkeiten (gegenüber dem Staat oder anderen BürgerInnen) besitzen und selbst zu Überwachenden werden, zum Beispiel, weil die Kosten für Überwachungskameras sinken (Koskela 2011) oder weil in sozialen Netzwerken eine Partizipationskultur entstanden ist, die mit freiwilliger Überwachbarkeit einhergeht (Fuchs 2014). Dies ist durchaus zutreffend, da das simple Bild „Staat versus BürgerInnen“ die komplexe, ausdifferenzierte moderne Gesellschaft natürlich nicht adäquat beschreibt. Es gibt nicht „den Staat“ und selbst innerhalb einer Regierung gibt es verschiedene Lager, die in der Sicherheitspolitik diametrale Auffassungen haben können. Diese Kritiken sind daher wichtige Differenzierungen und Weiterentwicklungen des foucaultschen Panoptismus. Sie entkräften aber nicht dessen Grundannahme, wonach Überwachung Teil moderner Macht ist und mit ihr eine abschreckende Wirkung erzielt werden soll. Der Panoptismus ist als Modell zu begreifen, welches Argumentationslinien erklären kann, aber in dieser Form nicht vollständig realisiert ist in unserer Gesellschaft.

Gleichwohl lässt sich die Entwicklung zu einer überwachbaren Gesellschaft auch empirisch belegen. Als eines der ältesten Beispiele staatlicher Überwachung gilt das englische „Domesday Book“ aus dem Jahr 1086, in welchem Informationen über mehr als 13.000 Bürger gesammelt wurden. Allerdings waren solche Methoden der Datensammelei unstrukturiert, was sich mit der Industrialisierung änderte. Es entstand ein „modern bureaucratic surveillance system“ (Weller

2012: 58). Ein Treiber hierfür waren gesellschaftliche Krisen wie Migrationsströme oder Revolutionen in Kommunikation und Transportwesen. Eng damit verbunden war der fast automatische Reflex, dass neue Technologien ebenfalls zur Überwachung durch den Staat genutzt werden sollten. Bis zur Entstehung der Sicherheitsdienste zum Ende des 19. Jahrhunderts ging es um die Sammlung offen verfügbarer oder persönlich abzufragender Informationen. Weitergehenden Überwachungsbefugnissen wie etwa heimlicher Überwachung stimmten die BürgerInnen eher in Bedrohungslagen zu. Allerdings erstarkte hierfür die Forderung, dass mit mehr Überwachung eine Steigerung der Kriegsführbarkeit sowie eine Haftung für die Überwachung durch den Staat einhergehen müssten (Weller 2012).

Im Grundsatz gilt dies für autoritäre Staaten ebenso wie für demokratische. Die Frage in der staatlichen Logik ist weniger, ob es mehr Überwachung bedarf, sondern wie dieses Mehr an Überwachung ausbalanciert werden kann im Lichte zu wahrender Freiheiten. Hier ergeben sich dann Unterschiede zwischen Demokratie und Autokratie, da in einer Demokratie die Opposition zur Regierung stärker ist und zivilgesellschaftliche AkteurInnen Einfluss auf die Gesetzgebung ausüben.

Im Ergebnis ist ein Anstieg an Überwachung in einem Nationalstaat jedoch „folgerichtig", was sich auch in Deutschland beobachten lässt. So setzte etwa die damalige Große Koalition aus Union und SPD („Sicherheitslager") bis Juni 2017 in weniger als zwei Jahren elf Gesetze im Zeichen des Anti-Terror-Kampfes durch, in denen die Überwachungs- und Datenauswertungsbefugnisse der Sicherheitsbehörden ausgebaut wurden. Ein Schutz von JournalistInnen, die als Träger der Pressefreiheit ein elementares Grundbedürfnis der Demokratie sicherstellen („Freiheitslager"), ist jedoch nur teilweise berücksichtigt worden und erreicht nicht mehr das Schutzniveau aus vordigitalen Zeiten (Moßbrucker 2017a).

Nüchtern betrachtet steht hinter dem Begriff der „Totalüberwachung" kein überzogener Vorwurf von Datenschützern, sondern ein politisches Ziel, welches aus dem Bedürfnis der BürgerInnen nach Sicherheit entsteht und einer foucaultschen Machtlogik folgt. Im Vorfeld der Bundestagswahl 2017 etwa gaben in einer repräsentativen Umfrage des Forschungsinstituts Emnid im Auftrag des Fernsehsenders N24 rund 70 Prozent der Befragten an, „Innere Sicherheit" sei eines der wichtigsten Themen im Wahlkampf. Nur „soziale Gerechtigkeit" erreichte einen höheren Wert (N24/Emnid 2017). In der politischen Logik kann der Staat diesen Auftrag bestmöglich umsetzen, wenn er das System, in dem die BürgerInnen leben, lückenlos kontrollieren kann.

Dass die Digitalisierung an sich staatliche Überwachung verändert oder zu einem Anstieg führt, ist demnach zwar eine populäre, aber sehr unscharfe Analyse. Der Eindruck von einer Gesellschaft, in der Überwachung „immer mehr" wird, entsteht dadurch, dass unsere Gesellschaft vernetzter und damit überwachbarer wird. (Potentielle) Überwachung wird präsenter im Alltag. Dass aber Regierungen das Internet total überwachbar gestalten wollen, ist in ihrer Logik normal. Die Problematik ergibt sich eher daraus, dass Überwachung durch die digitale Vernetzung sämtlicher Gesellschafts- und Lebensbereiche so umfassend werden kann, dass gewisse Freiheiten komplett

ausgehöhlt werden können. Wenn das Leben also komplett an vernetzten Geräten hängt und diese überwachbar sind, ist Privatheit im herkömmlichen Verständnis abgeschafft.

Betrachtet man allein die panoptische Machtlogik, ist jedoch genau davon auszugehen. Es kann demnach kein „natürliches Ende“ der Überwachbarkeit geben. Umso relevanter wird die Frage, was gesellschaftliche Gruppen entgegensetzen können, die diesen Trend stoppen oder zumindest abschwächen möchten. Diese Gruppen sind keinesfalls homogen (siehe 2.2), finden sich in allen Teilen der Gesellschaft und haben bisweilen unterschiedlichste Motive – sie eint „nur“, dass sie bestimmte Überwachungsvorhaben der Regierung nicht für richtig halten. Im Ergebnis hängt an ihrem Erfolg aber die Frage, ob Redefreiheit und Privatheit geschützt werden können, auch wenn sie an überwachbare Infrastrukturen gekoppelt werden müssen oder wenn bis heute „freie“ Teile des Internets wie das Darknet überwachbar gemacht werden sollen.

2.2. Risikogruppen von Überwachung als Treiber von Privatheit

„Treiber“ von Sicherheitspolitik ist Kriminalität, denn sie gilt es für einen Staat zu bekämpfen. (Mögliche) Überwachung ist Ausdruck staatlicher Präsenz und soll abschrecken. Dies gilt auch bei Ermittlungen gegen Online-Kriminalität, etwa im Darknet. Der Annahme, diese digitale Parallelwelt sei ein „rechtsfreier Raum“, will der Staat entgegenwirken. Auch deutsche Sicherheitsbehörden begründen eine Ausweitung von Überwachungsmöglichkeiten mit Darknet-Kriminalität oder kommunizieren Ermittlungserfolge intensiv nach außen. Die Botschaft soll lauten: „Wir kriegen Euch alle!“ (Mey 2017a: 154-156)

Technologien wie das Darknet werden Kriminelle auch in Zukunft für ihre Zwecke missbrauchen. Als Treiber für mehr Privatheit (und weniger Überwachung) fallen sie allerdings aus: Sie werden naturgemäß nicht politisch für mehr Kriminalitätsmöglichkeiten werben und sind in der Vergangenheit auch nicht damit aufgefallen, Kommunikationstechnologie im Digitalen selbst zu entwickeln. Das Darknet, wie es hier verstanden wird (siehe 3.1), wird stattdessen von der Tor-Stiftung weiterentwickelt – im Namen der Freiheit im Netz. Es soll nach Tor-Angaben der Anonymisierung im Internet für Militär, Strafverfolger, Journalisten und Aktivisten dienen (Tor Project 2018).

Während Militär und Strafverfolger als staatliche Akteure wegen des Missbrauchspotentials ein ambivalentes Verhältnis zur Anonymität im Internet haben, sind andere Gruppen in besonderer Weise darauf angewiesen. JournalistInnen etwa, indem sie frei von staatlicher Kontrolle kommunizieren und ihre Wächterfunktion ausüben, aber auch um „ansprechbar“ für Quellen zu sein. Diese könnten sich mit einem „Leak“ strafbar machen und damit in den Fokus der ErmittlerInnen geraten. Als Vertreter des „Freiheitslagers“ sind JournalistInnen und ihre InformantInnen ein mögliches Opfer der abschreckenden Wirkung durch Überwachung, selbst wenn sich die Ausweitung von Befugnissen gar nicht gegen sie richtet.

Wie in Abschnitt 2.1 ausgeführt, kann allein die Möglichkeit der Überwachung menschliches Verhalten verändern. Nehmen Menschen (beispielsweise aus Angst vor Sanktionen) deswegen keine Freiheitsrechte mehr wahr, spricht man von Chilling Effects. Sie treten auf, „where one is

deterred from undertaking a certain action X as a result of some possible consequence Y. Additionally, a chilling effect is an indirect effect: it occurs when the deterrence does not stem from the direct restriction, but as an indirect consequence of the restriction's application" (Youn 2013: 1481).

Die Theorie der Chilling Effects kann auch im Rückgriff auf Foucault entwickelt werden, entstammt ursprünglich jedoch der angloamerikanischen Rechtstradition. Sie wird zunehmend von deutschen und europäischen Gerichten anerkannt (Assion 2014: 52). Im Urteil zur Vorratsdatenspeicherung etwa hielt das Bundesverfassungsgericht die Maßnahme für geeignet, „ein diffus bedrohliches Gefühl des Beobachtet-Seins hervorzurufen" (Bundesverfassungsgericht 2010: Rn 212). Solche Chilling Effects werden gemeinhin negativ bewertet und wirken langfristig sowie unbewusst. In der Rechtsprechung wird einzelnen Gruppen ein erhöhtes Risiko zugeschrieben: Einerseits Verfechtern von „Minderheitenmeinungen", die in einer Mehrheitsgesellschaft besonderen Schutz benötigen und sich gegen den „Mainstream" stellen. Ein Beispiel ist das Veröffentlichen eines kritischen Artikels in einem Massenmedium. Andererseits sind „MeinungsführerInnen" besonders betroffen, wozu JournalistInnen zählen, aber auch GewerkschaftsführerInnen, PfarrerInnen, Unternehmenslenker und AmtsträgerInnen. Am stärksten betroffen von Chilling Effects sind damit „MeinungsführerInnen von Minderheitenmeinungen", zum Beispiel JournalistInnen mit einer kritischen Meinung gegenüber dem gesellschaftlichen Tenor (Assion 2014: 62-70). Solche AkteurInnen sind für eine freie Gesellschaft essenziell, weil ihre Akzente dafür sorgen, dass der gesellschaftliche Diskurs nicht erschlafft.

Ähnlich bedeutsam, aber tendenziell weniger organisiert sind all jene Menschen, die „etwas zu verbergen haben", allerdings nichts Kriminelles. Genannt seien beispielhaft psychisch Kranke, vom Mainstream Abweichende wie etwa Transgender oder schlichtweg Menschen, die sich durch die Beobachtung ihres Lebens durch Dritte in ihrer Persönlichkeitsentfaltung behindert fühlen. Auch sie benötigen Freiheitsrechte. Sie können sich entweder dafür öffentlich einsetzen, zum Beispiel durch Unterstützung von Lobbyorganisationen, oder sie müssen ihre Rechte vertreten lassen, indem die genannten, professionellen Gruppen ihre Interessen in den öffentlichen Diskurs einbringen – zum Beispiel, indem JournalistInnen über ihre Argumente berichten oder AnwältInnen sie gerichtlich vertreten können.

Es gibt empirische Hinweise, dass digitale Überwachung durch den Staat zu Chilling Effects führt, wenngleich solche unbewussten Wirkungen schwierig zu messen sind. Die Schriftsteller-Organisation PEN America etwa führte im Zuge des NSA-Skandals im Jahr 2013 eine Umfrage unter U.S.-amerikanischen Mitgliedern durch, wonach 24 Prozent der Befragten über bestimmte Themen per Telefon und E-Mail nicht kommunizieren wollten. 16 Prozent unterließen Online-Recherchen zu bestimmten Themen (PEN America 2014). 2015 bestätigte die Organisation die Ergebnisse in einer weltweiten Umfrage und fand heraus, dass die Furcht vor Überwachung in autokratischen Ländern höher ist als in demokratischen, wobei die Bedenken in demokratischen Ländern steigen (PEN America 2015).

Wichtig ist dabei, dass Chilling Effects sowohl durch gezielte („individuelle“) als auch durch massenhafte Überwachung erzeugt werden können. Bei gezielter Überwachung führen Einzelfälle zu einer Abschreckung bei anderen Mitgliedern der Personengruppe und den Betroffenen selbst (Assion 2014: 44). Bei der Massenüberwachung besteht geradezu der Zweck der Maßnahme darin, aufgrund von potentieller Betroffenheit des/der Einzelnen eine Abschreckung zu erzielen (siehe 2.1).

Solche Gesellschaftsgruppen wie etwa JournalistInnen kommen damit am ehesten als Treiber in Frage, die in ihrem eigenen Interesse für eine Stärkung der Freiheit im Netz eintreten könnten. Dies gilt sowohl politisch bei der Wahrung ihrer Rechte, insbesondere jedoch auch technologisch bei der Entwicklung neuer Kommunikations- und Recherchemöglichkeiten. In der Analyse ihrer Bedürfnisse wird sichtbar, was ein „Darknet der Zukunft“ leisten müsste, um von diesen Gruppen gefördert zu werden.

3. Das Darknet als Technologie der Anonymität

Das Darknet gilt heute als Inbegriff digitaler Anonymität und genießt in der Öffentlichkeit einen eher zweifelhaften Ruf. Bekannt ist vor allem, dass in dieser Online-Parallelwelt Kriminelle den Schutz der Anonymität missbrauchen und ungeniert mit Drogen, Waffen oder Aufnahmen von Kindesmissbrauch handeln. ErmittlerInnen müssen dem regelmäßig tatenlos zusehen, weil sie nicht in der Lage sind, das Darknet „zu knacken“. In Medienberichten über die digitale Unterwelt wird regelmäßig auch von einer „hellen Seite“ des Darknets gesprochen, auf der JournalistInnen, AktivistInnen und WhistleblowerInnen am Staat vorbei kommunizieren und Missstände aufdecken. Das Darknet ist in der medialen Darstellung für „Gut und Böse“ da, wenngleich sich die „helle Seite“ eher der Sichtbarkeit entzieht. Allen, die ins Darknet abtauchen wollen, dürfte (zunächst) vor allem die „dunkle Seite“ begegnen (Moßbrucker 2017b, Mey 2017a: 65-82, Bartlett 2014).

3.1. Grundfunktionen des Darknets

So populär der Darknet-Begriff ist, so unscharf ist er auch. Was genau ein Darknet ausmacht, hängt von der Definition ab, weshalb eine Einordnung für die folgende Analyse notwendig ist. Zurückgegriffen wird auf die Dreiteilung zwischen Darknet, Deep Web und Clearnet (Bergman 2001). Letzteres, das auch als Surface Web oder Visible Web bezeichnet wird, meint das World Wide Web, das mittels Browsern wie Firefox oder Safari erreichbar ist, von Suchmaschinen indexiert wird und einer regulierten Adressvergabe unterliegt, etwa indem in Deutschland die Top-Level-Domain „.de“ von der Genossenschaft DENIC verwaltet wird. Technisch gesehen gibt es zum Deep Web (auch: Hidden Web oder Invisible Web) kaum Unterschiede, außer dass dieser Teil des World Wide Web nicht durch Suchmaschinen erfasst wird und meist gegen den allgemeinen Zugriff gesichert wird, etwa durch Passwörter. Ein Anwendungsfall sind interne Firmennetzwerke, die sich nur an MitarbeiterInnen richten.

Das Deep Web hat jedoch nichts mit einem Darknet zu tun. Hierbei handelt es sich um ein eigenes Netzwerk, das auf dem World Wide Web aufsetzt, aber eine anonyme Schicht auf dieses legt. Mittels eigener Software schirmen sich die Nutzer vom Clearnet ab und stellen Anonymität her. Ein

Darknet ist mit herkömmlichen Browsern nicht zu erreichen. Die bekanntesten Darknets sind das GNUnet, das Freenet und insbesondere das Tor-Netzwerk (Mey 2017b).

Wird von „dem Darknet" gesprochen, ist fast immer das Tor-Netzwerk gemeint. Es wird von der Tor-Stiftung finanziert und durch EntwicklerInnen auf der ganzen Welt gepflegt (Mey 2017a: 103-140). Das Prinzip ist simpel: Verbindet sich ein Internetnutzer im herkömmlichen Surface Web über seinen Provider direkt mit der Ziel-Website, schaltet sich im Tor-Netzwerk zusätzlich eine Kette aus drei Servern dazwischen. NutzerInnen sagen ihren Providern demnach nur, dass sie ins Tor-Netzwerk einsteigen möchten, nicht aber wo die Reise eigentlich hingehen soll. Dass sie also zum Beispiel „Google.de" aufrufen wollen, können Telekom, Vodafone & Co. nicht sehen, weil diese Information verschlüsselt wird. Die Provider erfahren nur, dass die NutzerInnen zum Tor-Netzwerk möchten. Hier angekommen, wird eine Verbindung schrittweise weitergeleitet. Die einzelnen Tor-Server erfahren immer nur, wohin sie die Verbindung als nächstes herstellen müssen. Die Information, wer der/die eigentliche AbsenderIn war, geht so verloren – und wohin schlussendlich verbunden werden soll, erfährt erst der letzte Server. So bleibt die Verknüpfung zwischen der Identität der Tor-NutzerInnen und ihren Ziel-Websites auf der Strecke.

Diese Technologie ist noch nicht das Darknet, sondern anonymisiert NutzerInnen bei der Nutzung im Surface Web. Es ist aber auch möglich, im Tor-Netzwerk selbst Websites zu betreiben, die sogenannten Hidden Services. Dies ist das Darknet, auf das nur mit dem Tor-Browser zugegriffen werden kann. Diese Hidden Services können anonym betrieben werden. Im Ergebnis bleibt unklar, wer der/die BetreiberIn eines Hidden Services ist und wo der Server physisch steht. Versuche Dritter, die Seite zu löschen, laufen zwangsläufig ins Leere: Das Darknet ist zensurresistent (Mey 2017b).

Diese Anonymität stellt Tor durch eine Kombination von Verschlüsselungs- und Verschleierungsmethoden her. Zwischen beiden muss jedoch unterschieden werden: Verschlüsselung macht „nur" Inhalte von Kommunikation für Dritte unverständlich, zum Beispiel indem die Botschaft durch einen Geheimtext ersetzt wird. Den kann nur entziffern, wer die Buchstaben des Geheimtextes so anordnen kann, dass er wieder Sinn ergibt. Allerdings ist für Überwachende trotz Verschlüsselung klar, dass kommuniziert wird – und ohne Schutzmaßnahmen durch den/die NutzerIn auch, wer kommuniziert. Hier schaffen Anonymisierungsnetzwerke Abhilfe, weil den Kommunizierenden andere Identitäten verliehen werden. Im Fall von Tor ist es die IP-Adresse des letzten Tor-Servers in der Dreier-Kette. Erst die Kombination von Verschlüsselung und Anonymisierung verhindert, dass für Dritte bekannt wird, wer mit wem worüber kommuniziert (Singh 2014).

3.2. Bedürfnisse der Risikogruppen von Überwachung

Sollen Online-Freiheiten mittels Technologie gestärkt werden, müssen diejenigen Gruppen dafür eintreten, die ein besonderes Interesse daran haben (siehe 2.2). Dies erfolgt im Folgenden am Beispiel von JournalistInnen und ihren InformantInnen, könnte aber auch diskutiert werden mit AnwältInnen (und ihren MandantInnen), Geistlichen (und ihren Gläubigen), ÄrztInnen (und ihren PatientInnen), Oppositionellen (und ihren MitstreiterInnen) oder Menschen, die aus

unterschiedlichsten Gründen etwas Privates schützen möchten, etwa ihre sexuelle Orientierung oder eine Krankheit.

JournalistInnen werden dann für eine Stärkung des Darknets eintreten, wenn es ihre aktuellen Bedürfnisse befriedigt, sie sich also staatlicher Überwachung entziehen können. Wie kann der Staat sie angreifen? [2] Zu unterscheiden sind zwei Szenarien: (1) JournalistInnen werden gezielt überwacht, sodass ihre Recherchen und Quellen unmittelbar offen liegen. (2) JournalistInnen geraten bei einer willkürlichen Massenüberwachung in einen „Datenberg" und werden allein durch die Existenz der Daten eingeschüchtert, weil sie oder ihre Quellen auffliegen könnten. In beiden Fällen kann es entweder darum gehen, „nur" die Verbindungsdaten abzugreifen, um zu sehen, mit wem JournalistInnen Kontakt haben. Oder es ist von Interesse, die Inhalte einer bereits als „interessant" identifizierten Kommunikation zu erfahren (siehe 3.1).

3.2.1. Schutz durch Verschlüsselung

Ein Angriff auf Inhalte von Kommunikation ist durch Verschlüsselung heute verhältnismäßig einfach abzuwehren. Für gängige Kanäle – Telefonie, Kurznachrichten, Videokonferenzen, Emails, Filesharing – existieren kostenlose Möglichkeiten, mit einer Ende-zu-Ende-Verschlüsselung die Inhalte nur für sich selbst und den/die KommunikationspartnerIn sichtbar zu machen. Die wichtigsten Verschlüsselungsprotokolle gelten heute als „unknackbar". Zwar werden immer wieder Möglichkeiten bekannt, um verschlüsselte Kommunikation zu dechiffrieren, aber dabei werden Schwachstellen meist in der Implementierung der Verschlüsselung angegriffen. So war es etwa auch, als im Mai 2018 Schwachstellen der populären Email-Verschlüsselung Pretty Good Privacy (PGP) bekannt wurden. Nicht PGP selbst, sondern sein Gebrauch in Programmen wie Outlook, Thunderbird oder Apple Mail bot Lücken, die AngreiferInnen ausnutzen konnten (Poddebniak et al. 2018). Tendenziell dürfte sichere Verschlüsselung in Zukunft ständig weiterentwickelt und zum Standard für jede Digital-Aktivität werden. Ein wesentlicher Treiber hierfür werden finanzkräftige Unternehmen sein, die ihre Geschäftskommunikation absichern müssen und hierfür rechtlich verpflichtet werden (Bundesministerium des Innern 2016: 20-25).

Der Staat gerät hier in ein Dilemma, weil Verschlüsselung ein Wirtschaftsfaktor ist und ihr Schutz im In- und Ausland eine völkerrechtliche Verpflichtung, für die sich die UN-Mitgliedstaaten zum Wohl des Menschenrechts auf Meinungsfreiheit einsetzen müssen (Human Rights Council 2015). Gleichzeitig erschwert Verschlüsselung die Überwachbarkeit von Kommunikation. Es wird von einem „Going Dark"-Phänomen gesprochen (Schulze 2017). Staaten sehen sich daher zunehmend genötigt, zur „Ultima Ratio" zu greifen und die IT-Systeme ihrer Bürger direkt anzugreifen. Die Logik: Wenn die Kommunikation zwischen zwei Geräten verschlüsselt und nicht mehr abzugreifen ist, muss der Staat auf die Geräte selbst zugreifen, um die Inhalte abzufangen, bevor sie verschlüsselt oder nachdem sie entschlüsselt worden sind. Dafür hackt der/die AngreiferIn das Gerät, spielt unbemerkt ein Späh-Programm auf und schneidet Kommunikation dann mit, wenn sie unverschlüsselt ist, zum Beispiel beim Eintippen auf dem Smartphone vor dem Versand. In

[2] In der IT-Sicherheit ist es üblich, von „Angriffen" oder „Opfern" zu sprechen. Diese Terminologien werden für diesen Aufsatz allein in diesem Verständnis gebraucht.

Deutschland ist dies unter dem Begriff der Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) bekannt. Die rechtliche Grundlage für den Einsatz im Strafverfahren ist in Deutschland im Sommer 2017 gelegt worden (Bundesgesetzblatt 2017; Freiling/Safferling/Rückert 2018).

Weil der Staat nicht mehr „nur" mitliest oder -hört, sondern seine eigenen BürgerInnen direkt angreift, ist diese Maßnahme umstritten – auch, weil für das Aufspielen der Späh-Software Sicherheitslücken zurückgehalten werden müssen, mit denen auch Kriminelle die Geräte der BürgerInnen angreifen können (Herpig 2018). Es ist überdies zweifelhaft, ob die Quellen-TKÜ für Strafverfolger eine ähnliche Relevanz entwickeln kann wie die klassische Telekommunikationsüberwachung, von der 2016 noch über 35.000 in Strafverfahren angeordnet wurden (Bundesamt für Justiz 2017). Sicherheitslücken sind teuer auf einem Schwarzmarkt einzukaufen und jeder Einsatz eines Überwachungsprogramms kann dazu führen, dass das Späh-Programm sichtbar wird, etwa beim Aufspielen. Die Lücke kann dann vom Software-Hersteller geschlossen werden (Safferling/Rückert 2018: 6-7).

Die Funktion dieses sogenannten „Staatstrojaners" ist wohl am ehesten in der Analogie des Panoptikums zu verstehen: Er ist gewissermaßen der Wachturm in der Mitte des Gefängnisses, der den Häftlingen das Gefühl geben soll, überwacht werden zu können (siehe 2.1). Der mögliche Einsatz des „Staatstrojaners" sendet das Signal an Kriminelle, dass zum Beispiel selbst das Darknet seinen Schutz verlieren kann, wenn der Staat „ernst" macht und sich direkt auf die Geräte schleicht. Bei den Ermittlungen gegen den Darknet-Marktplatz „Hansa" setzte die niederländische Polizei ebenfalls Hacking-Technologie ein, um Dealer zu identifizieren und sagte im Anschluss tatsächlich öffentlich, dass mit dem Vorgehen gerade auch Vertrauen der Kriminellen in die Technologie an sich zerstört werden sollte (Greenberg 2018). Trotzdem wissen Kriminelle, dass der Wächter im Panoptikum seine Augen nicht überall haben kann, also im Darknet nicht jeder Kriminelle gehackt werden kann. In der Praxis wird der „Staatstrojaner" kein Masseninstrument für ErmittlerInnen werden können, weshalb auch die Kriminalität im Darknet nicht „ausgerottet" wird.

Auch JournalistInnen wissen, dass ein Angriff auf sie mittels Trojaner zwar möglich, aber nur die Ausnahme sein wird. Um sich bestmöglich dagegen zu schützen, dürften sie vor allem für eine starke IT-Sicherheit einstehen, um keine „Einfallstore" für den Späh-Trojaner zu bieten. Dies könnte sowohl für die Sicherheit der eigenen IT-Systeme gelten, zum Beispiel die Infrastruktur von Verlagshäusern und Rundfunksendern, als auch für die finanzielle Förderung von Forschung zu starker Verschlüsselung insgesamt. Außerdem wird das Wissen um IT-Sicherheit für JournalistInnen in der digitalen Berufspraxis zu einer Pflicht, um das Aufspielen von Trojanern falls möglich erkennen zu können. Eine Weiterbildung in digitaler Sicherheit für JournalistInnen müsste folglich an Bedeutung gewinnen.

3.2.2. Schutz durch Anonymisierung

Der beste Schutz gegen gezielte Hacking-Angriffe auf JournalistInnen ist es, gar nicht „auf den Radar" der Überwacher zu geraten. Hier liegt aktuell der weitaus größere Bedarf, weil Kommunikationskanäle heute alle stark verschlüsselt werden können (siehe 3.2.1), ihre NutzerInnen jedoch standardmäßig nicht anonymisiert sind. Dies ist im Journalismus aber ein

zentrales Sicherheitsbedürfnis: Für manche Storys kommen gegebenenfalls nur zwei, drei Personen als InformantInnen in Frage. Wenn Überwacher hier mitbekommen, dass ein/e JournalistIn mit einer dieser Personen kommuniziert hat, liegt die Quelle faktisch offen, selbst wenn der Inhalt stark verschlüsselt ist.

Daher wiegen aus journalistischer Perspektive die Bestrebungen so schwer, wenn Kommunikationsmetadaten verdachtsunabhängig auf Vorrat durch den Staat gespeichert werden. In Deutschland ist empirisch belegt, dass eine investigative Recherche mit all ihren InformantInnen gläsern wird, wenn der Staat „nur" erfahren kann, wer mit wem über Telefon und Email kommuniziert (Moßbrucker 2017c). Genau diese Metadaten-Analysen sind aus staatlicher Perspektive wiederum attraktiv, weil sie hoch aussagekräftig sind, systematisiert ablaufen können und noch dazu weniger Speicherplatz benötigen als Inhalte. Im NSA-Skandal wurde deutlich, wie wertvoll der US- Geheimdienst diese Daten einstufte. Das Ziel sei eine Totalerfassung, um globale Kommunikationsbeziehungen lückenlos offenzulegen und dann gegebenenfalls eine gezielte Überwachung einzuleiten (Rosenbach/Stark 2015: 120-137). Weil sich durch die Fortentwicklung von Verschlüsselung das „Going Dark"-Phänomen tendenziell verstärken wird, dürfte die Metadaten-Analyse an Bedeutung gewinnen – sie ist technisch nämlich heute einfach umzusetzen, hier gibt es (noch) kein flächendeckendes „Going Dark".

An dieser Stelle entwickelt das Darknet sein Potential für die Zukunft, denn genau die Verschleierung von Metadaten ist seine Kernfunktion. Theoretisch möglich ist es bereits heute, sich mittels Virtual Private Networks (VPN) oder eben Anonymisierungsnetzwerken wie Tor andere Identitäten zu geben. Doch es muss zusätzlich integriert werden, also selbstständig vom Nutzer vor die Kommunikationstools geschaltet werden. Dies ist für manche NutzerInnen nicht trivial und fehleranfällig, viele dürften ferner auch gar nicht wissen, dass Verschlüsselung nicht zwangsläufig Anonymität garantiert. Die eigene Anonymisierung ist daher nicht massenhafte Praxis, auch nicht im Journalismus. In der standardmäßigen Integration solcher Darknet-Funktionen in bestehende Kommunikationskanäle wie Chat-Apps oder Email-Dienste besteht daher ein echtes Zukunftspotential des Darknets.

3.3. Zukunftspotenziale des Darknets

„Das Darknet" ist heute bekannt als digitale Parallelwelt, das wie das Surface Web der 1990er Jahre anmutet und vor allem durch kriminelle Inhalte auffällt. Verschiedene Studien haben bereits versucht, die Verteilung von „Gut und Böse" zu quantifizieren. Dabei kam heraus, dass 57 Prozent der abrufbaren Seiten (Moore/Rid 2016: 18-27) oder 55 Prozent (Owen/Savage 2016) der sichtbaren Inhalte auf Hidden Services im Tor-Netzwerk illegal waren. Der Rest war nicht eindeutig illegal, was nicht heißt, dass sie eindeutig „positiv" sein müssen.

Mey (2017a: 67-80) unterscheidet auf der nicht-illegalen Seite drei Nutzungsformen: (1) Das Darknet als alternativen Zugang zu Inhalten, die es auch im Surface Web gibt. So werden zum Beispiel Websites als Hidden Service gespiegelt. Facebook etwa bietet eine Möglichkeit, das soziale Netzwerk über das Darknet anonym zu nutzen. (2) Das Darknet als Baustein für andere Technologien, zum Beispiel beim anonymen Hochladen und Teilen von Dokumenten. Dies machen

sich JournalistInnen zum Beispiel mit „anonymen Briefkästen“ für WhistleblowerInnen zunutze. (3) Exklusive Darknet-Inhalte, die nur hier zu finden sind, wobei hiervon wenige existieren.

Aus der obigen Analyse der Bedürfnisse von JournalistInnen als potenzielle Treiber für eine „Darknet-Reform“ (siehe 3.2) folgt, dass sich die Nutzungsformen als alternativer Wissenszugang (1) oder exklusiver Inhalt (3) kaum weiterentwickeln, sondern in der aktuellen Form stagnieren dürften. Die Vorstellung, dass im Darknet regierungskritische Blogs bestehen und WhistleblowerInnen offen sensible Daten teilen, mag einer romantischen Utopie entspringen, geht aber an der Realität weit vorbei. Es wäre bei gleichzeitiger Existenz und Erreichbarkeit des Surface Web schlichtweg unlogisch, als JournalistIn im Darknet selbst zu publizieren. Dort gibt es faktisch kein Publikum und Inhalte sind in der Anonymität schwierig zu finden. Ferner kann das langsame Tor-Netzwerk „moderne“ Medienformen wie Videoinhalte kaum darstellen (Moßbrucker 2017b). Entwicklungspotential besteht hingegen darin, das Darknet als Technologie zu begreifen, die zu bestehender Kommunikation hinzugefügt wird, um diese zu anonymisieren. Hidden Services könnten als Zusatzkomponente weiterentwickelt werden, mit denen JournalistInnen und andere Gruppen bei Bedarf die Produktion von identifizieren Metadaten verhindern können.

Wie könnte dies konkret aussehen? Derzeit am wahrscheinlichsten ist die Option, bei textbasierter Kommunikation – beispielsweise Emails oder Instant Messaging-Apps – solche Funktionen zu integrieren, sie also über einen eigenen Hidden Service auf dem Computer oder Smartphone abzuwickeln. Hier fallen geringe Datenmengen an, sodass auch „langsame“ Anonymisierungsnetzwerke genutzt werden könnten. Die Apps WhatsApp, Threema und Signal sind heute bereits standardmäßig Ende-zu-Ende-verschlüsselt, bei Telegram oder dem Facebook-Messenger kann dies als „sicherer Chat“ auf Wunsch für bestimmte Konversationen hinzu geschaltet werden. Notwendig wäre es, dass solche Apps „auf Knopfdruck“ einen eigenen Darknet-Knotenpunkt auf dem Gerät installieren und die Kommunikation über diesen Kanal abliefe. Identifizierende Informationen wie die IP-Adresse, die Telefonnummer oder die gerätespezifische MAC-Adresse müssten dabei gar nicht erst übermittelt, mindestens aber verschleiert werden. Das Projekt Ricochet verfolgt einen solchen Ansatz, hat bis heute jedoch noch keine App in den populären App-Stores von Google und Apple veröffentlicht. Einen ähnlichen Weg geht der bereits nutzbare Messenger Bleep, doch beide Angebote kommen aus der „Nische“ nicht heraus (Kühl 2014).

Eine Herausforderung für solche Features stellt das „Wesen“ der Anonymität dar, dass nämlich NutzerInnen nicht identifizierbar und schwierig auffindbar sind. Dieser Zielkonflikt wird nie ganz auflösbar sein. Dennoch sind für den Alltag praktikable Wege denkbar. Um beim Journalismus zu bleiben: JournalistInnen selbst könnten ihre Kontaktmöglichkeiten veröffentlichen, etwa in messengereigenen Adressdatenbanken inklusive ihres Namens oder auf ihren Websites und Social Media-Profilen. Sie wären damit ansprechbar für potentielle Quellen oder ihre KollegInnen. Die Anonymisierung würde dennoch bezwecken, dass Überwachende nur sehen, dass über den Dienst kommuniziert wird, aber nicht mit wem. Auch die Option, seine eigenen Kontakte aus dem Telefonbuch mit möglichen „Darknet-Chatadressen“ abzugleichen, ist nicht per se

kompromittierend für die Anonymität, gerade für den Fall, wenn JournalistInnen untereinander kommunizieren.

Im Grundprinzip ist diese „Zusatzoption Anonymität“, die im Tor-Netzwerk durch einen individuellen Hidden Service realisiert werden könnte, auf alle Kommunikationsformen anwendbar. Realistisch ist es hingegen zunächst vor allem für textbasierten Informationsaustausch, weil Sprach- oder gar Videotelefonie so datenintensiv ist, dass es derzeit kaum massentauglich über das Tor-Netzwerk abgewickelt werden könnte. Eine zwingende Voraussetzung zur Realisierung besteht daher eindeutig darin, die Leistungsfähigkeit der Anonymisierungsnetzwerke zu stärken, etwa durch das Betreiben eigener Verschleierungsserver. Auch hier wären die „Treiber der Darknet-Reform“ wie Medienunternehmen aufgefordert, zu investieren und ihren Beitrag zu leisten.

Proprietäre Einzellösungen oder neue Player am Markt, die solche Features anbieten, sind nicht wünschenswert. Ihnen fehlen Bekanntheit und Nutzerbasis, um für NutzerInnen attraktiv zu sein. Sinnvoller wäre es, wenn die marktdominierenden Unternehmen den „anonymen Darknet-Button“ als Zusatzfeature in ihr bestehendes Angebot integrieren. Zu denken wäre aktuell beispielsweise an den Facebook-Messenger, WhatsApp, Telegram, Signal, Threema, Skype, Gmail und andere große Email-Dienste. Hier wird jedoch eine weitere Schwierigkeit des Ansatzes deutlich: Gerade Facebook (und WhatsApp, das zu Facebook gehört) sowie Google und große Email-Anbieter betreiben ihre Dienste nicht zum Selbstzweck. Vielmehr besteht ein Sinn des Angebots gerade darin, NutzerInnen-Daten zu generieren, um sie mit der Ausspielung von personalisierter Werbung zu monetisieren. Eher in Betracht kommen daher Anbieter, die (1) von unabhängiger Hand finanziert und ohne kommerzielles Interesse entwickelt werden (z.B. Signal), (2) deren Markenkern ohnehin Sicherheit ist (z.B. Threema und Telegram) oder die (3) ein funktionierendes Business-Modell durch zahlende NutzerInnen haben und mit dem Zusatzfeature für neue Kundengruppen attraktiver würden (z.B. Skype).

Durch ihre gezielte Unterstützung könnten diejenigen, die ein veritables Interesse an anonymer Kommunikation haben, wie zum Beispiel JournalistInnen, die Weiterentwicklung der Darknet-Technologie fördern. Denkbar sind zum Beispiel strategische Kooperationen oder Zusagen, bei einer erfolgreichen Entwicklung als dauerhafte Kunden zu fungieren – oder direkt als Investoren einzusteigen. Ferner bleiben diese „Risikogruppen“ von Überwachung gehalten, ihren politischen Einfluss geltend zu machen. Sie sollten ihre Rechte einfordern und einer unverhältnismäßigen Beschränkung der Technologien entgegentreten. Stünde beispielsweise im Raum, Anonymisierungsmöglichkeiten „gesetzlich verbieten“ zu wollen, würde dies nicht die Rechtssicherheit schaffen, die bei einer ohnehin risikoreichen Investition aus unternehmerischer Perspektive notwendig ist.

4. Fazit

Das Darknet besitzt enormes Zukunftspotential, weil seine Kernfunktion genau die ist, die heute beim Schutz von privater Kommunikation im Internet am wichtigsten geworden ist: die Verschleierung von identifizierenden Daten. Es ist nicht zu erwarten, dass sich das Darknet, wie wir

es als anonymes Abbild des Internets in Form von Websites kennen, konzeptionell weiterentwickeln und vergrößern wird. Es dürfte in der Nische verbleiben. Massentauglich kann das Darknet aber werden, wenn es als Technologie-Komponente begriffen und zu bestehenden Kommunikationsmitteln hinzugefügt wird. Also etwa, indem es Chat-Apps hilft, neben der Verschlüsselung auch noch eine Anonymisierung zu garantieren. Es wäre das „neue Gesicht des Darknets", das unbemerkt im Hintergrund arbeitet.

Selbst mit diesen Zusatzfeatures ist nicht automatisch davon auszugehen, dass Anonymisierung zum Mainstream würde, schlichtweg weil durchschnittliche NutzerInnen das Gefahrenpotential von Metadaten für eher geringhalten dürften. Sie dürften weiterhin kommerzielle Angebote nutzen, weil diese nicht das „sicherste", sondern das anwendungsfreundlichste Produkt anbieten. Doch gerade, wenn die „Kosten" wegfallen, es also keine Einschränkungen im Vergleich zu identifizierender Kommunikation mehr gibt, dürfte der Gebrauch steigen. „Kosten" haben dann automatisch diejenigen, die ihre Daten freiwillig preisgeben und gläsern werden. Voraussetzung für eine solche Entwicklung ist allerdings, dass nicht neue, sondern bestehende Anbieter mit entsprechender NutzerInnenbasis solche „Anonymitätsoptionen" in ihre Produkte integrieren.

Hierfür kommen vor allem die Produkte in betrachtet, deren Betrieb nicht die Analyse von Daten bezweckt. Diese werden sich gegen diese Entwicklung wehren, weil es ihr Geschäftsmodell bedroht. Denkbar sind ähnliche Szenarien wie heute beim Gebrauch von Werbeblockern im Internet: Wenn NutzerInnen sich online nicht mehr überwachen und tracken lassen möchten, werden sie vom Angebot ausgespart. Damit dies nicht auch auf dem Messenger-Markt geschieht, müssen die Anonymitätsoption gerade die Angebote anbieten, die dies auch „verkraften" können.

Dieser Trend wird nicht von allein einsetzen, dafür ist der ökonomische Druck seitens der NutzerInnen zu gering. Außerdem wird der Trend von Staaten anhalten, mehr überwachen zu können (und damit gegen Anonymität vorzugehen). In der Verantwortung stehen eher „Risikogruppen" von Überwachung jenseits der Kriminalität, also JournalistInnen, AktivistInnen, AnwältInnen, beratend tätige MedizinerInnen oder Oppositionelle und diejenigen, die diese Gruppen im Hintergrund (finanziell) unterstützen, wie zum Beispiel Stiftungen und Nichtregierungsorganisationen. Alle Gruppen haben die politischen und wirtschaftlichen Ressourcen, solche technologischen Innovationen anzuschieben – im Sinne eines stärkeren Schutzes der Privatsphäre für alle BürgerInnen, letztlich aber auch im ureigenen Interesse.

Literatur:

Assion, Simon (2014): Überwachung und Chilling Effects. In: *Telemedicus: Überwachung und Recht. Tagungsband zur Telemedicus-Sommerkonferenz*. Jg. 1, S. 31-82, URL: https://www.telemedicus.info/uploads/Dokumente/Ueberwachung-und-Recht-Tagungsband-Soko14.pdf (letzter Zugriff: 28. Mai 2017).

Bartlett, Jamie (2014): *The Darknet. Unterwegs in den dunklen Kanälen der digitalen Unterwelt*. Kulmbach: Börsenmedien AG.

Bauman, Zygmunt/**Bigo**, Didier/**Esteves**, Paulo/**Guild**, Elspeth/**Jabri**, Vivienne/**Lyon**, David & **Walker**, R. B. J. (2014): After Snowden: Rethinking the Impact of Surveillance. In: *International Political Sociology*. 8, S. 121-144.

Bentham, Jeremy (1791): *Panopticon. Or the Inspection House*. Whitefish: Kessinger Publishing.

Bergman, Michael (2001): White Paper: The Deep Web: Surfacing Hidden Value. In: *the journal of electronic publishing*. Jg. 7, Nr. 1.

Bundesamt für Justiz (2017): *Übersicht Telekommunikationsüberwachung (Maßnahmen nach § 100a StPO) für 2016.* URL: https://www.bundesjustizamt.de/DE/SharedDocs/Publikationen/Justizstatistik/Uebersicht_TKUE_2016.pdf?__blob=publicationFile&v=2 (letzter Zugriff: 28. Mai 2018).

Bundesministerium des Innern (2016): *Cyber-Sicherheitsstrategie für Deutschland. 2016.* URL: https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (letzter Zugriff: 28. Mai 2018).

Bundesverfassungsgericht (2010): *Urteil vom 02. März 2010 - 1 BvR 256/08.* URL: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2010/03/rs20100302_1bvr025608.html (letzter Zugriff: 28. Mai 2018).

Bundesgesetzblatt (2017): Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens. In: *Bundesgesetzblatt*. Jg. 2017, Nr. 58, S. 3202-3213.

Foucault, Michel (1977): *Überwachen und Strafen. Die Geburt des Gefängnisses.* Frankfurt am Main: Suhrkamp.

Freiling, Felix/**Safferling**, Christoph/**Rückert**, Christian (2018): Quellen-TKÜ und Online-Durchsuchung als neue Maßnahmen für die Strafverfolgung: Rechtliche und technische Herausforderungen. In: *Juristische Wochenschau*. Jg. 2018, Nr. 1, S. 9-22.

Fuchs, Christian (2014): *Social Media. A critical introduction*. London: Sage Publications Ltd.

Greenberg, Andy (2018): *Operation Bayonett: Inside the sting that hijacked an entire dark web drug market*, URL: https://www.wired.com/story/hansa-dutch-police-sting-operation/ (letzter Zugriff: 28.05.2018).

Herpig, Sven (2018): *Government Hacking. Global Challenges.* URL: https://www.stiftung-nv.de/sites/default/files/government_hacking_akt.feb_.pdf (letzter Zugriff: 28. Mai 2018).

Human Rights Council (2015): *Report of the Special Rapporteur on the promotion and protection oft he right to freedom of opinion and expression, David Kaye (A/HRC/29/32)*, URL: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc (letzter Zugriff: 28. Mai 2018).

Isensee, Josef (2012): *Das Grundrecht auf Sicherheit. Zu den Schutzpflichten des freiheitlichen Verfassungsstaates. Vortrag gehalten vor der Berliner Juristischen Gesellschaft am 24. November 1982 - erweiterte Fassung*. Berlin: de Gruyer.

Koskela, Hille (2011): Hijackers and Humble Servants: Individuals as Camwitnesses in Contemporary Controlwork. In: *Theoretical Criminology*. Jg. 15, Nr. 3, S. 269-282.

Kühl, Eike (2014): *Chatten ohne Metadaten. Bleep und Ricochet.* URL: https://www.zeit.de/digital/datenschutz/2014-09/messenger-chat-sicher-bleep-ricochet/komplettansicht (letzter Zugriff: 28. Mai 2018).

Lohmann, Michael (2017): *Datenschutz = Täterschutz*, URL: https://www.heise.de/tp/features/Datenschutz-Taeterschutz-3851993.html?seite=all (letzter Zugriff: 28. Mai 2018).

Mann, Steve/**Nolan**, Jason/**Wellman**, Barry (2003): Sousveillance: Inventing and Using Wearable Devices for Data Collection in Surveillance Environments. In: *Surveillance & Society*. Jg. 1, Nr. 3, S. 331-355.

Mey, Stefan (2017a): *Darknet. Waffen, Drogen Whistleblower. Wie die digitale Unterwelt funktioniert*. München: C.H. Beck.

Mey, Stefan (2017b): „Tor" in eine andere Welt? Begriffe, Technologien und Widersprüche des Darknets. In: *Aus Politik und Zeitgeschichte*. Jg. 67, Nr. 46, S. 4-9.

Moßbrucker, Daniel (2017a): Erfasst. In*: journalist. Das Medienmagazin*. Jg. 67, Nr. 9, S. 18-24.

Moßbrucker, Daniel (2017b): Netz der Dissidenten. Die helle Seite im Darknet. In: *Aus Politik und Zeitgeschichte*. Jg. 67, Nr. 46, S. 16-22.

Moßbrucker, Daniel (2017c): Digitaler Informantenschutz, in: Schröder, Michael/Schwanebeck, Axel (Hrsg.): *Big Data – In den Fängen der Datenkraken. Die (un-)heimliche Macht der Algorithmen*. Baden-Baden: Nomos, S. 85-104.

Moore, Daniel/**Rid**, Thomas (2016): Cryptopolitik and the Darknet. In: *Survival*. Jg. 58, Nr. 1, S. 7-38.

N24/Emnid (2017): *N24-Emnid-Umfrage zum Bundestagswahlkampf: Soziale Gerechtigkeit und Innere Sicherheit wichtigste Wahlkampfthemen. Mehrheit für Familienförderung und Equal Pay*, URL: https://www.presseportal.de/pm/13399/3605994 (letzter Zugriff: 28. Mai 2018).

Owen, Gareth/**Savage**, Nick (2016): Empirical analysis of Tor Hidden Services. In: *IET Information Security*. Jg. 10, Nr. 3, S. 113-118.

PEN America (2014): *Chilling Effects: NSA Surveillance Drives U.S. Writes to Self Censor*. URL: https://pen.org/sites/default/files/2014-08-01_Full%20Report_Chilling%20Effects%20w%20Color%20cover-UPDATED.pdf (letzter Zugriff: 28. Mai 2018).

PEN America (2015): *Global Chilling.* URL: https://pen.org/sites/default/files/globalchilling_2015.pdf (letzter Zugriff: 28. Mai 2018).

Poddebniak, Damian/**Dresen**, Christian/**Müller**, Jens/**Ising**, Fabian/**Schinzel**, Sebastian/**Friedberger**, Simon/**Somorovsky**, Juraj/**Schwenk**, Jörg (2018): *Efail: Breaking S/MIME and OpenPGP Email Encryption using Exfiltration Channels (draft 0.9.1).* URL: https://www.efail.de/efail-attack-paper.pdf (letzter Zugriff: 28. Mai 2018).

Rosenbach, Marcel/**Stark**, Holger (2015): *Der NSA-Komplex. Edward Snowden und der Weg in die totale Überwachung*. München: Wilhelm Goldmann Verlag.

Rothmann, Robert (2017): Video Surveillance and the Right of Access: The Empirical Proof of Panoptical Asymmetries. In: *Surveillance & Society*. Jg. 15, Nr. 2, S. 222-238.

Safferling, Christoph/**Rückert**, Christian (2018): Das Strafrecht und die Underground Economy. In: Konrad Adenauer-Stiftung: *Analysen & Argumente*, Februrar 2018, Nr. 291, URL: http://www.kas.de/wf/doc/kas_51506-544-1-30.pdf?180209124944 (letzter Zugriff: 28. Mai 2018).

Schaefer, Brian/**Steinmetz**, Kevin (2014): Watching the Watchers and McLuhan's tetrad: The Limits of Cop-Watching in the Internet Age. In: *Surveillance & Society*. Jg. 12, Nr. 4, S. 502-515.

Schulze, Matthias (2017): Going Dark? Dilemma zwischen sicherer, privater Kommunikation und den Sicherheitsinteressen von Staaten. In: *Aus Politik und Zeitgeschichte*. Jg. 67, Nr. 46, S. 23-28.

Singh, Simon (2014): *Codes. Die Kunst der Verschlüsslungen. Geschichte Geheimnisse Tricks*. München: Deutscher Taschenbuch Verlag (6. Auflage).

Tor Project (2018): *Inception*. URL: https://www.torproject.org/about/torusers.html.en (letzter Zugriff: 28. Mai 2018).

Weller, Toni (2012): The information state. An historical perspective on surveillance, in: Ball, Kirstie/Haggerty, Kevin & Lyon, David (Hrsg.): *Routledge Handbook of Surveillance Studies*. Abindon: Routledge, S. 277-284.

Youn, Monica (2013): The Chilling Effect and the Problem of Private Action. In: *Vanderbilt Law Review*. Jg. 66 Nr. 5, S. 1473-1539.