FIELD OF FOCUS 4
SELF-REGULATION AND REGULATION
INDIVIDUALS AND ORGANISATIONS

UNIVERSITÄT HEIDELBERG
ZUKUNFT SEIT 1386

Volume 1/2015

Journal of Self-Regulation and Regulation

Special Issue
Wer regiert das Internet? Regulierungsstrukturen und -prozesse im virtuellen Raum

Guest Editors
Wolf J. Schünemann, Sebastian Harnisch

Contributors
Markus Beckedahl, Jeanette Hofmann, Marianne Kneuer, Kai Cornelius, A. Michael Froomkin, Milton L. Mueller, Ekkehart Reimer, William Binney, Myriam Dunn Cavelty

Inhaltsverzeichnis

Editorial

Sabina Pauen

Welcome to the first edition of our *Journal of Self-Regulation and Regulation*.
This new journal serves as an outlet for researchers investigating how individuals and organizations regulate their (inter-)actions, thus allowing us to address a broad range of social phenomena of high public relevance.

We are dedicated to support high-quality work crossing disciplinary boundaries. Due to the fact that each discipline has its own „style of publishing", we allow for different formats of contributions, ranging from comments and essays over data-based research papers to literature reviews. The journal welcomes contributions in both English and German.

We plan to publish two volumes each year. One will provide the reader with a collection of papers that all center around one general theme. This will be an invited issue with guest editors. The other volume(s) will be collections of individual peer-reviewed papers, edited by the research council of Field of Focus 4 from Heidelberg University – an interdisciplinary group of nine senior scientists (see www.uni-heidelberg.de/fof4 for more information).

We decided to start with a thematic collection that nicely demonstrates the variety of perspectives which can be taken on a truly „hot topic" of our modern times: One year ago, two colleagues from the Department of Political Science from Heidelberg University raised the important question: „Who governs the internet?" It seems self-evident that this issue can only be investigated successfully if social, economic, political, and legal experts work together. Hence, an interdisciplinary group was formed that organized a series of weekly public lectures to be held by well-known experts in the field, each addressing the same question from a rather different theoretical viewpoint. This lecture series attracted a large audience of about 100 listeners each week, including researchers and students, local authorities, members of the press and ordinary citizens. Given the great success of this lecture series, we asked the organizers to collect all individual contributions and to publish them in the first volume of our journal.

We hope that the readers will find this issue interesting and feel inspired to consider the *Journal of Self-Regulation and Regulation* as a potential outlet for their own work. For the moment, we are still in a phase of experimenting to find the best way to organize our journal. Comments and suggestions are thus highly welcomed. Support us in broadening our perspective to meet some of the great social challenges that we are faced with today by providing high-quality interdisciplinary research!

Heidelberg, September 2015 Sabina Pauen

Vorwort der Herausgeber

Wolf J. Schünemann und Sebastian Harnisch

Es ist noch nicht lange her, da wollten alle einfach ins Netz. Die Frage eines in Deutschland berühmten Werbespots des amerikanischen Anbieters AOL aus den 1990er Jahren: „Bin ich schon drin oder was?“ oder auch die Redewendung „ich geh‘ ins Netz“ zeugen von dem Bedürfnis nach einem reibungslosen Übergang in den virtuellen Raum. Dank der technologischen Entwicklung wird uns dieser Übertritt heute kaum noch so bewusst wie in Zeiten pfeifender Modems: Viele unserer technischen Geräte sind jetzt schon ständig online und nehmen die dafür nötige Verbindungsprozedur automatisch vor.

Unsere Bedürfnisse und Ungeduld können wir entdecken, wenn wir nicht online sind. Es reicht schon sich selbst zu beobachten, wenn man sich am Flughafen, im Café oder auf dem Marktplatz mit dem Notebook oder Smartphone rasch in ein verfügbares WLAN einwählt und dazu in gewohnter Manier Nutzungsbedingungen ungelesen als akzeptiert wegklickt, um schnell ‚drin‘ zu sein. Von diesem unvorsichtigen Nutzungsverhalten mag es löbliche Ausnahmen geben; das Gegenteil ist die Regel.

Gleichwohl ist das öffentliche Bewusstsein für die Herausforderungen und Gefahren im Umgang mit dem Internet und digitaler Kommunikation zumindest auf der abstrakten Ebene in den vergangenen Jahren erheblich gestiegen. Wer ins Netz geht, der ist – und dieser Nachsatz wird immer deutlicher – ins Netz gegangen – nämlich in das Netz der Geheimdienste. Denn spätestens seit den Enthüllungen von Edward Snowden wissen wir, dass die Dienste mehrerer Staaten anlasslos und transnational Meta- und Inhaltsdaten digitaler Kommunikation mitschneiden, Leitungen anzapfen, Daten untereinander austauschen und so den Grundrechtsschutz von Bürgern weltweit umgehen. Auch wenn diese Enthüllungen viele Bürger zu öffentlicher Empörung veranlasst haben, die alltäglichen Nutzungsgewohnheiten im Umgang mit privatwirtschaftlichen Angeboten scheinen sie kaum zu berühren. Nach wie vor gehen viele Menschen auch den nicht weniger datenhungrigen Internetunternehmen ins Netz. Diese bieten ihre Dienste meist gratis an, weil sie ihr Geschäft mit unseren Informationen und Daten machen. Nicht wenige dieser Unternehmen kooperieren zudem aktiv mit Regierungen und deren Geheimdiensten, so dass sich die ausgeworfenen Fangnetze immer enger um die Nutzer schließen.

Aus beiden Beobachtungen und der öffentlichen Aufmerksamkeit, die aus ihnen erwächst, lassen sich viele Fragen und Forderungen an die Regulierung des Internets ableiten: an staatliche Akteure und internationale Organisationen, aber auch an jeden Nutzer selbst im Sinne einer Selbstregulierung im Umgang mit digitalen Medien. Für

beide Aspekte ist eine zweite meist missverstandene Eigenschaft des Internets von Bedeutung. Denn an der Wendung „Ich geh' ins Netz" ist irreführend, dass es das eine Netz so gar nicht gibt. Das Internet ist ein Netzwerk der Netzwerke. Es ist in seiner grundlegenden Architektur fragmentiert, so dass Kommunikation über die Grenzen dieser Fragmente hinweg erst über allgemeinverbindliche Protokolle und Standards hergestellt werden muss. Diese Eigenschaft setzt internationale Verständigung, zumindest aber gegenseitige Akzeptanz, voraus. Dabei decken sich die Muster der Fragmentierung des Netzes der Netze keineswegs mit der territorialstaatlichen Strukturierung politischer und rechtlicher Ordnung. Vielmehr liegen beide Ordnungen, der On- und der Offlinewelt, wie Patchworkdecken mit unterschiedlich großen Flicken übereinander. Es ist diese Strukturdifferenz, die die Bildung politischer Interessen und Koalitionen, die Prozesse der Beschränkung und Ermöglichung von Netzaufbau und Nutzung so schwierig und komplex werden lässt.

Aus diesen Gründen schien es uns naheliegend und geradezu zwingend, die Regulierung und Selbstregulierung im virtuellen Raum zum interdisziplinären Forschungsthema im Rahmen des an der Universität Heidelberg etablierten *Field of Focus 4*: *Selbstregulation und Regulation: Individuen und Organisationen* zu platzieren. Die großzügige ideelle und finanzielle Förderung durch das FoF4, welches Teil der Exzellenzinitiative der Universität Heidelberg ist, hat den Ausbau einer bereits geplanten Vortragsreihe zu einer Ringvorlesung mit renommierten Wissenschaftlerinnen und Wissenschaftlern sowie Expertinnen und Experten aus der Praxis ermöglicht. Diese erste FoF4-Ringvorlesung unter dem Titel *Wer regiert das Internet?* fand von Mitte Oktober 2014 bis Ende Januar 2015 statt. Aus der erfolgreichen Veranstaltungsreihe mit ihren elf Einzelvorträgen ist dieser Band entstanden.[1] Die Beiträge sind alle grundlegend überbearbeitet worden, einige sind mehr auf ein Fachpublikum ausgerichtet als andere. Unser Ziel als Herausgeber war es, den Autoren so viel Freiheit wie möglich in der Fokussierung der Beiträge zu lassen und gleichzeitig so viel Kohärenz und Information wie möglich für ein breites Publikum bereitzustellen, welche interessierte Bürger und Fachkolleginnen gleichermaßen einschließt.

Der vorliegende Band ist gleichzeitig auch die erste Ausgabe (und ein Special Issue) des neuen *Journal of Self-Regulation and Regulation*, das fortan zweimal im Jahr vom FoF4 als Open Journal herausgegeben wird. Es ist aus unserer Sicht daher besonders trefflich, dass wir mit dem Thema den Anfang des Journals besetzen dürfen. Mit Hilfe der Universitätsbibliothek in Heidelberg ist es uns so gelungen, der breiteren Öffentlichkeit und der wissenschaftlichen Gemeinschaft eine leicht zugängliche Online-Zeitschrift bereitstellen zu können, die ohne die mittlerweile teils horrenden Lizenzgebühren auskommt. An der Praxis der großen Wissenschaftsverlage lässt sich gut beobachten, wie sich etablierte Unternehmen ihre einträglichen Geschäftsmodelle si-

1 Alle Originalvorträge finden sich dokumentiert, im Video- und Audioformat sowie mit prägnanten schriftlichen Zusammenfassungen, auf der Internetseite www.uni-heidelberg.de/netzpolitik.

chern, dabei allerdings zunehmend vom digitalen Strukturwandel unter Druck gesetzt werden. Die Netzpolitik kennt vergleichbare Konfliktkonstellationen schon seit langem. Die weltweiten Auseinandersetzungen um das File-Sharing und das dadurch bedrohte Urheberrecht bilden quasi den Urkonflikt der internationalen Netzpolitik. Als Herausgeber begrüßen wir das Angebot eines Open-Journal-Formats durch die Universitätsbibliothek Heidelberg und freuen uns darüber, uns mit dem Special Issue an diesem innovativen Veröffentlichungsmodus zu beteiligen.

Was bietet das Sonderheft zur Ringvorlesung *Wer regiert das Internet?* – Keine einfache Antwort, sondern viele differenzierte Antworten. Sie seien im Folgenden kurz skizziert, so dass der geneigte Leser sich leichter orientieren kann. Zunächst leuchtet der netzpolitische Aktivist, Journalist und Gründer der Plattform netzpolitik.org Markus Beckedahl in seinem Text *Die digitale Gesellschaft – Netzpolitik, Bürgerrechte und die Machtfrage* anhand von vier wichtigen Teilbereichen das emergente Politikfeld Netzpolitik aus. Beckedahl betrachtet die Praktiken der Massenüberwachung im Lichte des NSA-Skandals, das Prinzip der Netzneutralität und seine Herausforderung, die Strukturen des Urheberrechts und ihren Reformbedarf sowie die Privatisierung von Öffentlichkeit im Rahmen von sozialen Netzwerken. Am Ende des engagierten und pointierten Beitrags steht der Appell des Aktivisten für ein demokratisches Internet.

Um die Gestaltung des Internets auf internationaler Ebene geht es auch im politikwissenschaftlichen Beitrag von Jeanette Hofmann unter dem Titel *Internet Governance: Theoretische und empirische Annäherungen an einen schwer fassbaren Gegenstand*. Sie geht von einem Vergleich mit der staatlichen und multilateralen Regulierung klassischer Kommunikationssysteme wie dem Postwesen oder der Telefonie aus, um die Besonderheiten und neuen Ansprüche der Gestaltung des Internets, zumindest aber der Verwaltung seiner kritischen Ressourcen, klar zu identifizieren. Begriffe von Planung, Steuerung, selbst Regulierung helfen in Bezug auf das Internet nach Ansicht der Autorin nicht weiter: Das Internet entzieht sich aus ihrer Sicht einer hierarchischen Ordnung zugunsten staatlicher Einheiten ebenso wie der Vorstellung eines intendierten Gestaltungshandelns. An deren Stelle setzt Hofmann ein Governance-Konzept, das Koordination zwischen staatlichen und nicht-staatlichen Akteuren in kritischen Momenten meint, Leitplanken für die weitere Entwicklung einzieht, wenn Koordination selbst zum Problem geworden.

Im Hinblick auf den demokratischen oder demokratisierenden Gehalt der Internetentwicklung vertritt Marianne Kneuer in ihrer Beantwortung der Frage *Mehr demokratische Qualität durch das Internet?* eine netzrealistische Position. Eine solche Mittelposition verortet sich zwischen den netzpolitischen Optimisten eines neuen demokratischen Zeitalters aus der Pionierzeit des Internets (oder etwa in Ausdeutung des Arabischen Frühlings 2011) und den kulturkritischen Pessimisten, die einen Werte- und Gesellschaftszerfall in Folge digitaler Kommunikation konstatieren. Auf Grundlage empirischer Untersuchungen zu Partizipationsformen und -qualität in Deutschland sowie im internationalen Vergleich rechnet die Autorin nicht mit nachhaltigen Verbesserungen

der Demokratiequalität durch das Internet. Ihr ernüchterndes Fazit lautet vielmehr, dass es zwar auch innovative Partizipationsformen durch das Internet gibt, diese aber weniger genutzt werden als gedacht.

Der Beitrag Milton Muellers zur Frage *Gibt es Souveränität im Cyberspace?* widmet sich explizit der Herausforderung klassischer politischer Regulierungsinstanzen durch die Internetentwicklung. Mueller unterscheidet zwischen Souveränität im Cyberspace, verstanden als virtuelles Äquivalent zum physischen Gewaltmonopol im materiellen Raum, und einer Souveränität über den Cyberspace, im Sinne einer staatlichen Kontrolle über die kritischen Ressourcen und Normen in der virtuellen Welt. Für beide Formen staatlicher Souveränität betrachtet er den Erhalt oder die Wiederherstellung mit großer Skepsis. Insbesondere die Souveränität über den Cyberspace sei zwar technisch möglich, doch keineswegs wünschenswert. Gesellschaftliche Innovationen würden dadurch gehemmt und das Internet, wie wir es kennen, durch Fragmentierung faktisch zerstört.

Direkt anschlussfähig an die Problematisierung staatlicher Souveränität im Internetzeitalter legt sich Ekkehart Reimer für seine rechtswissenschaftliche Untersuchung eine finanzpolitische Frage vor: *Wer besteuert das Internet? Die Steuersparmodelle von Amazon, Google & Co. als juristische Reformimpulse*. Das Internet – so die Ausgangslage – verschärfe das Problem der potentiellen Minderbesteuerung transnational tätiger Unternehmen, weil gerade die Geschäftsmodelle und -praktiken von Internetunternehmen vornehmlich auf geistigem Eigentum basierten. Reimer setzt sich sodann das Ziel, die Grundstrukturen und Determinanten des Steuerrechts in der virtuellen Welt zu bestimmen. Er identifiziert und beschreibt ausführlich die vorherrschenden Steuersparmodelle und erörtert konzis auch potentielle Lösungsansätze. Im Ergebnis münden seine Überlegungen in einen Ausblick, der an Milton Mueller erinnert: Das Internet könnte die Lösung jener Probleme bereitstellen, die es selbst geschaffen hat.

Mit dem nächsten Beitrag *Das Internet: ein umfassendes Überwachungssystem* wendet sich das Heft dem bestimmenden Thema der netzpolitischen Debatten in den vergangenen Jahren zu, der transnationalen Praktiken der Massenüberwachung durch die US-amerikanische National Security Agency (NSA) sowie der Geheimdienste verbündeter Staaten. Den Einstieg in diesen Themenkomplex leistet ein Praktiker mit einschlägigen Erfahrungen: William Binney war bis 2001 Technischer Direktor der NSA. Er quittierte den Dienst aus Protest gegen den Ausbau der Überwachungstätigkeit nach den Terroranschlägen vom 11. September 2001. Fortan betätigte er sich als früher Whistleblower. In seinem politisch engagierten Beitrag für die Ringvorlesung und diesen Band erklärt Binney zentrale Funktionsweisen der Internetüberwachung auf nationaler wie internationaler Ebene. Er zeigt auf, dass und wie die Praktiken der NSA gegen US-amerikanisches Recht verstoßen. Mit Blick auf die überbordenden Datenmengen, die durch die Geheimdienste abgefangen und mitgeschnitten werden, aber kaum mehr analysiert werden könnten, kommt Binney zu dem paradoxen Urteil, dass die Effizienz der Programme und damit die Sicherheit der zu schützenden Gesellschaften eher ein-

geschränkt als befördert würden. Die NSA könne ihre eigentliche Aufgabe also kaum noch erfüllen. Vor diesem Hintergrund präsentiert der Beitrag auch alternative Analysetechniken einer nach Meinung des Autors zielgerichteten und beschränkten, und daher auch rechtmäßigen Überwachung.

Einen ebenso kritischen Essay, allerdings aus der Perspektive des Rechtswissenschaftlers, legt Michael Froomkin vor. In *From Anonymity to Identification* befasst er sich mit der Anonymität in der Online-Kommunikation und ihrer Gefährdung durch die Massenüberwachung, technologische und andere netzpolitische Entwicklungen. Anonymität versteht Froomkin als fundamentalen und stärksten Schutz der freien Meinungsäußerung. Er beschreibt, wie früher Techniken der Kryptographie funktionierten und wie die US-Regierung versuchte deren Verbreitung zu verhindern. Nach Ansicht des Autors ist Anonymität in der Online-Kommunikation heute nur noch sehr schwer, wenn überhaupt erreichbar und im Umgang mit Mobiltelefonen sogar unmöglich. Selbst Verschlüsselungstechniken seien unsicher geworden. Hinzu komme die Selbstüberwachung der Nutzer durch Facebook und andere soziale Netzwerke. Von einem internationalen Menschenrechtsschutz, so das ernüchternde Urteil, sei nicht viel zu erwarten, da dieser außerhalb Europas kaum mehr durchsetzbar sei.

In einem weiteren rechtswissenschaftlichen Beitrag mit dem Titel *Im Netz der Geheimdienste – strafrechtliche Aspekte der Massenüberwachung im Internet* unternimmt Kai Cornelius eine strafrechtliche Bewertung von Überwachungspraktiken in verschiedenen Szenarien für den Fall Deutschland. Die Anwendungsbeispiele orientieren sich an den aufgedeckten Spionageaktivitäten Treasuremap, Regin und Eikonal. Während Ersteres noch keine strafbaren Handlungen umfasst, ist Strafbarkeit in den Fällen von Regin und Eikonal nach Analyse des Autors durchaus gegeben, allerdings gestaltet sich die Strafverfolgung in beiden Fällen schwierig. Cornelius argumentiert gleichwohl, dass eine strafrechtliche Bewertung vorzunehmen sei, um daran die Legitimität und Angemessenheit staatlicher Überwachung zu bemessen.

In ihrer politikwissenschaftlichen Analyse: *Die materiellen Ursachen des Cyberkriegs – Cybersicherheitspolitik jenseits diskursiver Erklärungen* knüpft Myriam Dunn Cavelty an die Frage nach dem Verhältnis von Staaten und dem Cyberspace an, verfolgt dann allerdings eine andere Fragestellung. Sie unternimmt den Versuch, das verstärkte staatliche Handeln und den gestiegenen staatlichen Einfluss auf das Internet zu erklären. Die Autorin verwendet einen um die Foucaultsche Gouvernementalitätstheorie erweiterten Sekuritisierungsansatz und analysiert, in deutlicher Abgrenzung zu früheren Studien dieser Art, nicht nur Sprechakte, sondern auch nicht-diskursives staatliches Handeln in Form technisch-materieller Fakten und Praktiken. Dunn Cavelty argumentiert so, dass nationalstaatliche Regierungen unter Hinweis auf die Gefährdung kritischer Infrastrukturen durch Cyberangriffe immer größere Teile des virtuellen Raums ihrer Kontrolle unterworfen hätten.

Im abschließenden Aufsatz zur Leitfrage des Bandes *Wer regiert das Internet? – sechs Thesen und einige Tendenzen* versuchen wir selbst eine Zusammenfassung der

verschiedenen Beiträge und eine Synthese wesentlicher Aspekte und Überlegungen darin. Anhand von sechs Thesen diskutieren wir aus einer politikwissenschaftlichen Perspektive die Chancen und Grenzen der Internetregulierung, das demokratische Versprechen der Internetentwicklung, Anspruch und Wirklichkeit des Datenschutzes im Online-Zeitalter, die ausufernden Praktiken der Massenüberwachung, die Aussichten für eine Restitution staatlicher Souveränität sowie die Risiken und Bedrohungen durch Cyberangriffe und Cyberterror.

Als Herausgeber dieses Special Issue dürfen und wollen wir einer längeren Reihe von Einrichtungen und vor allem Personen ganz ausdrücklich danken, denn ohne das Engagement und nahtlose Ineinandergreifen Vieler wäre das pünktliche Erscheinen des vorliegenden Bandes nicht möglich gewesen. Unser erster Dank gilt den Autoren und Autorinnen des Bandes, die durch ihre Vorträge und schriftlichen Beiträge die intellektuelle Substanz für diesen Band geliefert und darüber hinaus die netzpolitische Forschung in Heidelberg befruchtet haben. Die Einladungen nach Heidelberg auszusprechen, eine Ringvorlesung dieser Qualität durchzuführen, ein Special Issue herauszugeben und auch in der Forschung innovative Studien durchführen zu können, verdanken wir der großzügigen Förderung durch das Field of Focus 4 im Rahmen der Exzellenzinitiative. Für die ideelle und materielle Förderung des FoF4 möchten wir uns ganz besonders bei der Sprecherin des Research Council Frau Professor Dr. Sabina Pauen, bei dem politikwissenschaftlichen Gremiumsmitglied Frau Professor Dr. Jale Tosun sowie insbesondere bei der Fachreferentin Sabine Falke bedanken. Ohne den großen Einsatz und die Verlässlichkeit von Sabine Falke in der Organisation und der inhaltlichen Planung und Vorbereitung wären weder Ringvorlesung noch diese Ausgabe zustande gekommen.

Ebenso sind wir den Mitgliedern der Netzpolitik AG, also Stefan Artmann, Stefan Steiger, Sebastian Stier und Milan Tahraoui, zu großem Dank verpflichtet. Sie haben viel und wertvolle inhaltliche Arbeit geleistet und dann auch die organisatorische Durchführung der Ringvorlesung teils ehrenamtlich, teils als Hilfskräfte maßgeblich begleitet. Darüber hinaus haben sie, insbesondere Stefan Artmann, den Editionsprozess für diese Ausgabe unterstützt.

Für die Unterstützung bei der Vorbereitung des Bandes gilt unser abschließender und besonders großer Dank aber der wissenschaftlichen Hilfskraft Melanie Bräunche, die den zum Teil hektischen Editionsprozess bis hin zur Publikation mit professioneller Ruhe begleitet und dabei alle Arbeitsschritte kompetent und sehr verlässlich durchgeführt hat. Ohne ihre unermüdlichen und gewissenhaften Überarbeitungen hätte dieses Heft nicht in dieser Form und gewiss nicht am heutigen Tag publiziert werden können.

Heidelberg, im September 2015

Wolf J. Schünemann
Sebastian Harnisch

Die digitale Gesellschaft – Netzpolitik, Bürgerrechte und die Machtfrage

Markus Beckedahl[1]

1 Einleitung

Um das ganze Spektrum an Netzpolitik beschreiben zu können, habe ich für diesen Beitrag vier Themenfelder ausgewählt, die natürlich nur einen kleinen Auszug aus ganz vielen Themen repräsentieren, die mir aber aktuell in besonderem Maße relevant erscheinen. Als wir im Oktober 2014 das zehnjährige Jubiläum von *netzpolitik.org* gefeiert haben, hatten wir knapp 35 unterschiedliche Sprecherinnen und Sprecher: Damit, so dachten wir, könnten wir das Spektrum netzpolitischer Themen gut abbilden. Schon als wir das Programm planten, stellten wir aber fest, dass damit eigentlich nur ein ganz kleiner Teil von dem beleuchtet würde, was Netzpolitik mittlerweile ausmacht.

Ein weiteres Beispiel dafür, wie sich das Thema Netzpolitik entwickelt hat, ist die Häufigkeit mit der darüber diskutiert und berichtet wird. Als ich vor zehn Jahren anfing, über Netzpolitik zu schreiben, gab es im Bundestag vielleicht einmal im Monat etwas zu diesem Thema. Mittlerweile, also im Jahr 2014, ist es so, dass wir in der Sitzungswoche gar nicht mehr nachkommen, all die unterschiedlichen Ausschüsse, die netzpolitisch relevante Themen behandeln, auch entsprechend zu dokumentieren.

In den vergangenen Jahren ist also sehr viel passiert und es wird wahrscheinlich auch in der Zukunft noch viel mehr geschehen. Nach dieser knappen Entwicklungsskizze werde ich die ausgewählten Themenfelder im Folgenden einzeln behandeln, um abschließend zu einem Fazit zu gelangen.

2 NSA und BND: Praktiken und Gefahren der Massenüberwachung

Als ich vor 15 Jahren anfing, mich mit Netzpolitik zu beschäftigen, gab es bereits einen NSA-Skandal, den später allerdings die meisten vergessen haben, wenn sie es überhaupt mitbekommen hatten. Schon damals gab es Enthüllungen, dass weitgehend unkontrollierte Geheimdienste, NSA und Co., technisch alles machen, was möglich ist, um das Netz flächendeckend zu überwachen (vgl. Tagesschau 2015a). Dies hat dann ein EU-Untersuchungsausschuss, der Nichtständige Ausschuss über das Abhörsystem Echelon, im Sommer 2001 im Parlament aufgegriffen und einen Abschlussbericht vorgelegt, der im Herbst desselben Jahres diskutiert werden sollte (vgl. Europäisches Par-

1 Der Text beruht auf einem Vortrag. Er wurde von Wolf J. Schünemann und Melanie Bräunche erstellt.

lament 2001). Doch infolge der Terroranschläge vom 11. September 2011 entwickelte sich geradezu eine ‚Überwachungsspirale auf Steroiden', was bedeutet, dass die Überwachung noch weiter ausgebaut wurde. Allerdings interessierte dies zu diesem Zeitpunkt niemanden mehr, da man für vermeintlich mehr Sicherheit gerne bereit war, Freiheit aufzugeben.

An dieser Einstellung änderte sich wenig, bis dann im Juni 2013 durch Edward Snowden die Spähaktionen der NSA bekannt wurden (vgl. Spiegel Online 2013b). Für uns netzpolitisch Aktive war es davor schwierig gewesen, über den NSA-Überwachungsskandal zu reden oder auch nur darüber, was technisch möglich wäre, wenn ein Geheimdienst wie die NSA weitgehend unkontrolliert agieren kann, wenn er 50 Milliarden Dollar jährlich zur Verfügung hat. Mit solchen Warnungen wurde man sehr schnell in eine verschwörungstheoretische Ecke gerückt, weshalb man viele Konjunktive verwenden musste. Es gab nur wenige Orte, wie den *Chaos Communication Congress* vom Chaos Computer Club, wo man tatsächlich darüber sprechen konnte. Aus diesem Grund sind wir Edward Snowden sehr dankbar, dass er mit unglaublich viel Zivilcourage und Mut geholfen hat, offen zu legen, was da passiert. Dadurch können wir endlich darüber sprechen, können endlich eine gesellschaftliche Debatte darüber führen, ob wir akzeptieren wollen, dass Geheimdienste jeden Klick von uns, jeden Schritt im Netz, wenn man es so nennen kann, überwachen können und die einzigen Fragen, die noch bleiben, sind: Wird das gespeichert? Wenn ja, wo? Wird das für immer gespeichert? Und wird das mal gegen uns verwendet oder nicht?

Die deutsche Bundesregierung zeigte sich damals sehr verwundert, als die Enthüllungen bekannt wurden und erklärte über die damals Verantwortlichen, Hans-Peter Friedrich als ehemaliger Bundesinnenminister und Ronald Pofalla als ehemaliger Kanzleramtschef, die NSA-Affäre für beendet:

> „Ja. Alle Verdächtigungen, die erhoben wurden, sind ausgeräumt. Fest steht: Es gab keine ‚massenhaften Grundrechtsverletzungen' amerikanischer Geheimdienste auf deutschem Boden, wie behauptet wurde. […] Auf jeden Fall viel Lärm um falsche Behauptungen und Verdächtigungen, die sich in Luft aufgelöst haben" (Friedrich 2013).

> „Unsere zentrale Forderung, dass auf deutschem Boden deutsches Recht eingehalten werden muss, wird demnach durch die NSA erfüllt. Das haben wir jetzt nicht nur mündlich, sondern auch noch einmal schriftlich bestätigt bekommen" (Pofalla 2013).

Beide verwiesen in diesem Zusammenhang auch auf das geplante No-Spy-Abkommen mit den USA um ihre Aussagen zu untermauern, obwohl zu diesem Zeitpunkt schon klar war, dass es dieses Abkommen nicht geben wird (vgl. Süddeutsche Zeitung 2015). Die damalige Bundesregierung verbreitete demnach die Botschaft, dass das Ausspähen beendet sei, bis im Oktober 2013 öffentlich bekannt wurde, dass auch Angela Merkels Handy seit 2002 überwacht wurde (vgl. Spiegel Online 2013a). Auf diese Enthüllung folgte ein kurzer öffentlicher Aufschrei der Empörung. In diesem Zeitfenster hätte die Bundesregierung etwas unternehmen können, tat es aber nicht. Über diese Zurückhaltung wunderten sich viele bis wenig später bekannt wurde, dass der deutsche Bundes-

nachrichtendienst (BND), der Auslandsgeheimdienst seine Finger im Spiel hatte. Zwar hatten wir schon vorher den Verdacht, dass mehr überwacht wurde, als wir ahnten, da es einmal im Jahr kolportierte Meldungen gab, wie viele Filterungen durch den BND am DE-CIX, also am zentralen Internetknoten in Frankfurt, vorgenommen wurden. Dabei wurde berichtet, dass es Filter gebe um deutsche Staatsbürger zu schützen, indem insbesondere der E-Mail-Verkehr mit DE-Domains automatisch herausgefiltert würde. Zugespitzt gesagt: Die Inhaber solcher E-Mail-Adressen besitzen das Grundrecht des Fernmeldegeheimnisses (Art. 10 GG), alle anderen leider nicht.

Es war aber nie so ganz klar, was genau der BND eigentlich macht. Mittlerweile, über ein Jahr später, wissen wir, dass der BND in viele kooperative Aktivitäten mit NSA, GCHQ usw. eingebunden ist.[2] Das politische Interesse hält sich jedoch in Grenzen, was sich insbesondere am Verhalten der Bundesregierung zeigt. Der derzeitige Bundesinnenminister Thomas de Maizière äußerte zwar etwas mehr Kritik an den USA, indem er sinngemäß sagte, dass, wenn nur ein Teil der Vorwürfe zuträfe, das Maß voll wäre (vgl. Zeit Online 2014). Der amtierende Außenminister Frank Walter Steinmeier hingegen geriet selbst in die Kritik, als herauskam, dass die Bundesregierung 2004, in seiner Zeit als Kanzleramtsminister, eine Kooperation mit der NSA vereinbart hatte, womit die Echtzeitüberwachung am DE-CIX in Frankfurt dem Internetknoten der NSA vereinbart worden war. Auch wurde deutlich, dass die Filter nicht funktionierten – welch Wunder?! –, weshalb die NSA viel mehr Daten bekommen hat, als sie eigentlich bekommen sollte. Aber auch das hat nicht zu großer Empörung und Aufmerksamkeit geführt. Verantwortlich für diesen Zeitraum waren also Frank-Walter Steinmeier und Thomas de Maizière, weiterhin Mitglieder unserer Bundesregierung. Die Nachfolge von Ronald Pofalla wurde zweigeteilt: auf der einen Seite gibt es jetzt einen Geheimdienstkoordinator, Klaus-Dieter Fritsche, der ‚Mann fürs Grobe', vorher Verfassungsschutzvizepräsident, auf der anderen Peter Altmaier, bekanntester deutscher ‚Politiktwitterer', bevor er Kanzleramtsminister wurde.

Im Oktober 2014, passend zu unserem zehnten Geburtstag, hat Kanzleramtsminister Peter Altmaier ein Schreiben an die Mitarbeiter/-innen und Abgeordneten des NSA-Untersuchungsausschusses geschickt. Sie wurden davor gewarnt, weiterhin Dokumente – etwa auch an uns – zu leaken. Sie wurden gebeten, dies aus Gründen des Staatswohls zu unterlassen. Damit wurde Menschen quasi mit Strafen gedroht, wenn sie sich weiter als Whistleblower betätigen, und das im Kontext eines Untersuchungsausschusses, der erst eingerichtet wurde, weil ein Whistleblower den Mut gehabt hatte, Dokumente an Journalisten zu leaken.

2 Durch das 2002 unterzeichnete "Memorandum of Agreement" ist ein Datenaustausch von BND und NSA durchaus gewollt, um gemeinsam gegen Terrorismus vorzugehen. Aktuelle Erkenntnisse zeigen aber, dass der BND zusammen mit der NSA auch Frankreichs Außenministerium und Präsidentenamt sowie diverse EU-Politiker abgehört hat, wobei der BND die Daten auch selbst ausgewertet haben soll (vgl. Tagesschau 2015b).

Es gibt also einen NSA-Untersuchungsausschuss zur Aufarbeitung des NSA-Skandals, was aber bald zwei Jahre nach den Snowden-Enthüllungen leider kaum noch jemanden interessiert. Inzwischen haben wir schon wieder die nächste Spirale mit dem Islamischen Staat im Irak und in Syrien (ISIS) usw., und wir sehen eigentlich dieselben Entwicklungen, wie wir sie 2001 gesehen haben. Jetzt könnte nur noch über weitere Grundrechtseinschränkungen und Überwachungsausbau diskutiert werden.

Die Enthüllungen von Edward Snowden haben dabei im Wesentlichen das bestätigt, was wir vorher schon wussten. Es gab in Deutschland eine große Diskussion über die sogenannte Vorratsdatenspeicherung, die eigentlich das ist, was BND und NSA im Großen Maße weltweit machen. Dabei wird überwacht, wer mit wem kommuniziert und wo wessen Handy oder Computer sich gerade befindet. Das Bundesverfassungsgericht hat die Vorratsdatenspeicherung für unrechtmäßig erklärt, leider nur das Gesetz dazu. Der Europäische Gerichtshof hat ein Urteil gegen die Praxis der Speicherung gefällt, trotzdem wird genau das weiterhin gemacht, nämlich die Daten im großen Stil zu speichern. Sie fragen sich vielleicht, warum die Vorratsdatenspeicherung so gefährlich ist – weil so genau herausgefunden werden kann, wer sich wann wo aufhält, da ihre Handys alle in derselben Funkzelle eingeloggt sind. Stellen Sie sich mal vor, hier[3] säße jemand, der Terrorverdächtiger sein könnte. Dann werden Algorithmen sofort feststellen, dass Sie mit einem Terrorverdächtigen in derselben Funkzelle zum selben Zeitpunkt waren und dann sind Sie vielleicht auch terrorverdächtig. Glauben Sie nicht? Das gab es aber schon.

In Berlin wurde z.B. mal jemand gesucht, der Autos angezündet hatte. Da ein politisches Motiv vermutet wurde, ließ die Polizei ganz viele Funkzellenabfragen durchführen – das lief völlig unkontrolliert ab, da die Provider einfach alle Telefonnummern schicken sollten, die zur fraglichen Zeit dort eingeloggt waren –, bis dann irgendwann festgestellt wurde, dass ein geistig Verwirrter der Täter war und dieser noch nicht einmal ein Handy besessen hatte. Das wurde später über andere Wege festgestellt, aber bis dahin waren ganz viele Leute, die zufällig in der Nähe waren und deren Handy eingeschaltet war, automatisch verdächtig. Und wenn zwei-, dreimal ein Auto in ihrer Nähe brannte, wurden Sie vermutlich noch stärker verdächtigt. Das also ist die schöne neue Welt. Und die Frage ist doch: Würden wir jemals akzeptieren – in der analogen Welt –, dass irgendwo gespeichert würde, wer gerade mit wem zum Kaffeekränzchen zusammen sitzt? Also bei meinen Eltern, die für das Digitale kein großes Interesse haben, die sich mehr mit ihrem Videotext beschäftigen, habe ich eher das Gefühl, dass sie auf die Barrikaden gehen würden, wenn der Staat anfinge aufzuschreiben, mit welchen Nachbarn sie sich wann treffen. Das würden sie als inakzeptabel empfinden. Also warum sollten wir akzeptieren oder warum akzeptieren wir, dass das alles mit digitalen Daten über uns irgendwo gespeichert wird? Ist es Unwissenheit? Ist diese Art der

3 Der Beitrag bezieht sich auf den Vortrag von Markus Beckedahl vom 30.10.2014 in Heidelberg.

Überwachung einfach wenig greifbar? Man sieht sie nicht, man fühlt sie nicht, deswegen kümmert man sich auch nicht darum? Das sind die großen Fragen.

Wenn wir jetzt den NSA-Skandal anschauen, gibt es eine Vielzahl an Maßnahmen, die man durchführen könnte. Man könnte lange weiter diskutieren, was eigentlich politisch gemacht werden sollte, und genau darin besteht das Problem in dieser Debatte. Im Gegensatz zu den meisten anderen Debatten, kann man bei der Vorratsdatenspeicherung nicht einfach beschließen eine Kampagne gegen dieses oder jenes durchzuführen, oder für Tag X zu kämpfen, an dem eine Entscheidung getroffen werden wird. Die Lösungswege aus diesem NSA-Skandal sind so vielschichtig, dass man auf politischer und technischer Ebene, auf den unterschiedlichen Ebenen wiederum national und international verschiedene Entscheidungen treffen müsste. Dafür fehlt im Moment aber der politische Wille. Deswegen glauben wir, dass es hinsichtlich der technologischen Möglichkeiten eher mittel- als kurzfristig Hoffnung gibt. Schon heute könnte der Staat Verschlüsselungs- und Anonymisierungstechnologien fördern. Allerdings stehen dem natürlich die Sicherheitsbehörden im Weg, die genau das gegensätzliche Interesse haben. Wir können in dieser Frage eine Art Abwägungsprozess beobachten, der, je nachdem wie gerade die Stimmung in den Medien ist, mal zur einen, mal zur anderen Seite ausschlägt. Aber wir selbst als Bürger und Bürgerinnen haben durchaus die Möglichkeit diese Projekte zu unterstützen, sei es, dass wir Entwickler sind, sei es, dass wir sie selbst einfach nur nutzen, um Totalüberwachung, anlasslose Totalüberwachung teurer zu machen, zu erschweren oder indem wir Anleitungen schreiben, oder anderen einfach zeigen, wie sie Verschlüsselungs- und Anonymisierungstechnologien nutzen können.

Auf industrieller Seite haben wir auch die Chance, freie Software und freie Hardware mit zu entwickeln – dies gilt vielleicht in geringerem Maße für Politikwissenschaftler/-innen – Computerwissenschaftler/-innen, Ingenieure und sog. ‚Nerds' haben aber die Chance irgendwann vertrauenswürdige Infrastrukturen zu erschaffen, durch die wir dann das Gefühl haben, dass dort vielleicht weniger Hintertüren eingebaut worden sind. Das ist ja das eigentlich skurrile in der ganzen Debatte: Jahrelang wurde uns immer erzählt: „Kauft keine Produkte von Chinesen, weil es da Hintertüren gibt". Also haben sich alle Produkte von amerikanischen Herstellern gekauft. Dank Edward Snowden wissen wir heute, dass dort ebenfalls überall Hintertüren eingebaut sind (ANT Product Data 2008: S3221–S32242). Was wir bisher offensichtlich vergessen haben, ist, dass wir tatsächlich vertrauenswürdige Infrastrukturen brauchen, die vielleicht nicht in China oder in Russland oder in USA hergestellt werden. Insofern sollte es vielleicht auch irgendwann einmal die Entwicklung hin zu einer europäischen Industrie in diesem Sektor geben. Auf europäischer Eben hat man aber unter Umständen wieder ein Problem mit Großbritannien. Das Vereinigte Königreich ist zwar auch Mitglied der EU, ist aber eigentlich der größte „Komplize" der USA in Sachen Massenüberwachung im globalen Netz (vgl. The Guardian 2013).

Eine weitere mögliche Maßnahme besteht darin, das Netz wieder zurück zu entwickeln, dahin, wie es früher war, nämlich dezentral. Freie Funknetzwerke sind beispielsweise eine Möglichkeit für die kommunale Ebene. Wir haben in den letzten Jahren nicht aufgepasst und nicht verhindert, oder vielmehr sogar zugelassen, dass das Netz immer zentraler wurde, immer monopolistischer. Und je zentraler es ist, je monopolistischer es ist, umso einfacher ist es, alles abzuhören. Das wäre viel schwieriger und aufwändiger, wenn es dezentral wäre und verschlüsselt kommuniziert würde.

Allerdings stehen die nächsten technologischen Entwicklungen schon vor der Tür. Es wird also eher noch komplizierter werden. Mittlerweile gibt es Produkte wie *Google Glasses* in der ersten Version. Wenn sich diese Technologie durchsetzt, werden wir demnächst vielleicht das Vergnügen oder eher das Pech haben, dass ganz viele Menschen mit versteckten Kameras herumlaufen werden. Das kann man natürlich positiv und negativ bewerten. Ich persönlich fände es vielleicht gar nicht schlecht, wenn ich das eingebaut hätte, denn dann könnte ich mir genau anschauen, wer in meiner näheren Umgebung ist, wen ich vielleicht schon über Facebook oder sonst woher kenne und mit wem ich sprechen möchte. Andererseits möchte ich umgekehrt nicht, dass, wenn ich irgendwo sitze, mich jemand anderes auf diese Weise identifizieren kann. Wie aber kommen wir zu solchen Mechanismen, dass man solche Identifikationsmöglichkeiten auch als passiv Betroffener ein- und ausschalten kann, dass man also selbstbestimmt darüber entscheiden kann, ob man diesen Service haben oder besser ermöglichen möchte oder nicht? Das ist eine schwierige Frage, denn es ist kompliziert, sich gegen derartige Privatüberwachung zu wehren, möchte man sich nicht optisch verändern und mit professionellen Schminktipps beschäftigen.

Ein nächstes Problem ist die Überwachung von oben. Schon heute gibt es Technologien, also Drohnen, die in der Lage sind, einfach über Heidelberg zu fliegen und in Echtzeit alles von oben zu überwachen, was hier passiert. Dies kann auch genutzt werden, um einzelne Personen zu verfolgen. Zum Glück ist das alles noch recht teuer, d.h. die Polizei Heidelberg kann sich noch keine Drohnen leisten, aber wer weiß, wie schnell diese Entwicklung noch weitergeht, wie lange es dauert, bis das zu einem gängigen Instrument geworden ist.

Von staatlichen Ermittlungsstellen eingesetzte Drohnen sind das eine, die immer häufiger eingesetzten Hobbydrohnen das andere. Die gibt es mittlerweile auch für 300 Euro oder günstiger zu kaufen. Stellen Sie sich mal vor, Sie haben ein Einfamilienhaus und lassen seit zwanzig Jahren die Hecke hoch wachsen, damit die Nachbarn nicht darüber schauen, und auf einmal fliegt die Drohne vom Nachbarssohn über ihren Garten, wo Sie sich gerade nackt sonnen. Die Frage ist, was macht man dann? Also erst einmal stellt sich natürlich die Frage, ob es legal ist, eine Drohne fliegen zu lassen. Wir haben einmal versucht das in Berlin herauszufinden und stießen auf die berüchtigten drei Experten mit fünf verschiedenen Meinungen. Die Bandbreite reichte bis zu der Empfehlung, wir müssten jeden Drohnenflug anmelden. Das aber macht natürlich niemand. Die andere Frage ist auch hier, wie man sich dagegen wehren kann. Innerhalb von Ha-

ckerkreisen wird das verbreitet diskutiert, weil alle Drohnen cool finden, aber keiner selbst von einer Drohne beobachtet werden möchte. Da gehen die Diskussionen auseinander. Die Vorschläge reichen vom Einsatz von Bodenluftraketen, wenn es über dem eigenen Garten ist, bis hin zum Erlass neuer Gesetze.

Damit ist das neue Spannungsfeld zu den Themen Überwachung und Datenschutz einmal in verschiedenen Facetten skizziert. Es ist zu erwarten, dass noch viel mehr dieser Art auf uns zukommen wird, wenn erstmal alles mit Sensoren ausgestattet ist. Wenn wir dann auch nicht genau aufpassen, wie wir die rechtlichen Rahmenbedingungen dafür schaffen, könnte unsere Privatsphäre ausgehöhlt werden, was wir vermutlich nicht akzeptieren wollen. Das eigentliche Problem besteht zudem darin, dass, wenn wir akzeptieren, dass wir komplett überwacht werden, wir damit auch zulassen, dass unsere freiheitliche Demokratie nicht mehr funktioniert. Denn dann können wir das Recht auf freie Meinungsäußerung nicht mehr richtig ausnutzen, weil wir ständig Angst haben müssen, richtig zu kommunizieren. Unser Recht auf informationelle Selbstbestimmung werden wir dann ohnehin nicht mehr aufrechthalten können, weil wir die ganze Zeit beobachtet werden können.

3 Netzneutralität und Breitbandausbau

Damit komme ich zum zweiten Punkt, mit dem ich vielleicht besser hätte beginnen sollen, weil es mit „Internet für Einsteiger“ überschrieben werden könnte, aber Edward Snowden und die Massenüberwachung passen seit 2013 besser. Das Internet ist ein Netzwerk aus Netzwerken, die sich über Kabel oder über Antennen zusammengeschlossen haben. Vor über dreißig Jahren haben sich Computerwissenschaftler und Nerds wie David P. Reed[4] hingesetzt und sehr kluge Designentscheidungen getroffen, die natürlich auch technisch bedingt waren. Die Begründer des Internets waren damals der Meinung, dass sie etwas ganz Neues konzipieren wollten, bei dem im Gegensatz zu anderen Medienformen nicht jemand in der Mitte bestimmen sollte, welche Daten durchgeleitet werden. Man hatte damals schon im Kopf, dass sich so auch verschiedene Netzwerke zusammenschließen können, dabei wollte man diese Zusammenschlüsse der Netzwerke so dumm wie möglich halten. Deshalb entschied man sich für eine sehr schlaue Grundregel, nämlich das „Ende zu Ende Prinzip“, das besagt, dass wir an den Enden des Internets das Recht haben sollten, jede Hardware zu nutzen, jede Software zu nutzen, jedes Protokoll zu nutzen, jeden Dienst zu nutzen, um mit anderen Menschen, Geräten, an den anderen Enden des Internets kommunizieren zu können. Dies alles sollte möglich sein, ohne dass jemand in der Mitte sagt: Das geht, das geht nicht und das geht schneller, das geht langsamer, oder hier nehmen wir Mautgebühren.

Dieses Prinzip hat das Internet so groß gemacht, das war die revolutionäre Designentscheidung. Man muss nicht irgendjemanden um Erlaubnis fragen, man braucht keine knappe UKW-Frequenz oder sonst irgendetwas, um auf Sendung zu gehen oder

4 Für weitere Informationen siehe: Reed o.J.

um die Wikipedia zu gründen oder einfach nur um in einem Blog sein Recht auf freie Meinungsäußerung nutzen zu können. Auf dieser technischen Infrastruktur baute dann Tim Berners-Lee[5] das World Wide Web auf: Alles wurde bunt, mit Browsern. Das Internet veränderte sich rasant, aber auch Berners-Lee profitierte von dieser ursprünglichen Designentscheidung, er schaffte dann eigentlich nur noch den weiteren Baustein für das, was wir jetzt Internet nennen. Das Ende-zu-Ende-Prinzip war eigentlich immer eingebaut und jeder hat es akzeptiert, weil es gut funktionierte.

Seit einigen Jahren haben wir allerdings eine politische Debatte, die sich Netzneutralitätsdebatte nennt. Netzneutralität beschreibt dabei dieses neutrale Netz, dieses Ende-zu-Ende-Prinzip, und der erste, der es auf den Begriff brachte, war der amerikanische Jurist Tim Wu[6], der irgendwann, bevor er in die Wissenschaft ging, bei einem Unternehmen arbeitete, welches die so genannte Deep Packet Inspection anbietet. Deep Packet Inspections von Cisco werden heute sowohl von der deutschen Telekom zur Durchleuchtung von Datenpaketen als auch von der chinesischen Regierung zur Netzzensur eingesetzt. Dies ist also eine Technologie, die auch bei Diensteanbietern hierzulande Begehrlichkeiten weckt, weil man mit ihr in der Lage ist, gleichsam in der Mitte von Netzen zu bestimmen, was schneller durchgeht, was langsamer durchgeht, was zusätzliches Geld kostet und was nicht. Aus Sicht von Telekommunikationsunternehmen ist es freilich eine gute Sache, wenn sie so etwas haben und dafür mag es auch gewisse technische Gründe geben. Wenn man mit Nerds, die das Thema unpolitisch betrachten, oder mit Marketing-Menschen, etwa aus der Telekommunikationsbranche, darüber spricht, dann werden durchaus Argumente gebracht und all die Möglichkeiten gesehen, was man damit machen könnte. Wenn man sich politisch damit beschäftigt, sieht man allerdings, dass es ein grundlegendes Problem gibt. Ein Internet ohne Netzneutralität ist wie eine Bank, auf die man sich nicht wirklich setzen kann oder ein Auto mit drei Rädern.

Jetzt werden Sie vielleicht sagen: Angriffe auf die Netzneutralität sind etwas, das es vielleicht später mal geben wird. Aber haben Sie sich schon mal die Allgemeinen Geschäftsbedingungen von ihren Mobilfunktarifen angeschaut? Da gibt es dann so Formulierungen wie bei Vodafone: „Die Nutzung von Peer-to-Peer-Kommunikation ist nicht gestattet“ (Vodafone 2013: Red M Tarif/Screenshot auf netzpolitik.org).[7] Doch was wird als Peer-to-Peer-Verbindung definiert? Ein Blick auf die Webseiten, konkret, deren Hilfeforen, schafft nicht wirklich Abhilfe. Denn dort wird im Allgemeinen nur von Computer-zu-Computer-Verbindungen gesprochen.[8]

5 Für weitere Informationen siehe: Berners-Lee o.J.

6 Für weitere Informationen siehe: Wu o.J.

7 Inzwischen reagierte Vodafone und erlaubt nun Peer-to-Peer-Kommunikation (vgl. Vodafone 2015a).

8 Inzwischen hat Vodafone sein Hilfeforum aktualisiert und dort steht jetzt: „Peer-to-Peer (P2P) Netzwerke sind Netzwerk-Systeme ohne zentrale Zugriffskontrolle, in denen alle Rechner gleichberechtigt agieren. Der englische Begriff „peer“ steht im deutschen für „Gleichgestellte“ oder „Ebenbürtiger“ (Vodafone 2015b).

Zugespitzt formuliert, wird Ihnen hier also Internet verkauft, aber im Kleingedruckten die Nutzung des Internets verboten. Dabei möchten die Unternehmen eigentlich nur einzelne Dienste verbieten. Sie verletzten aber ebenso die Netzneutralität, wenn sie sagten: Sie können alles nutzen, aber die und die und die Dienste nicht mehr. Natürlich dient es den Telekommunikationsunternehmen in erster Linie dazu, ihre Geschäftsmodelle abzusichern. In diesem Sinne blockieren sie vornehmlich z.B. *Skype Voice over IP*, weil sie selbst ihr Geld mit Telefonaten verdienen. Instant Messaging wird in der Regel auch immer mit verboten. Da fragt man sich natürlich als Nutzer, ob damit *WhatsApp* gemeint ist oder der *Facebook Chat*. Was ist, wenn ich *Facebook* nutze und mich chattet jemand an, verletzte ich damit dann schon gegen die Allgemeinen Geschäftsbedingungen? Kann mir dann der Vertrag gekündigt werden? Das scheinen noch weitgehend ungeklärte Fragen zu sein.

Lange Zeit haben auch diese Entwicklungen kaum jemanden interessiert, bis im letzten Jahr ein heimischer Singvogel, die Drossel, im Internet bekannt wurde – mit der Kampagne gegen die „Drosselkom“ (vgl. N24 2013). Die Deutsche Telekom präsentierte plötzlich ein neues Vertragsmodell. Die Vorstellung war, dass es demnächst nur noch 75 GB Datenvolumen inklusive im DSL-Anschluss geben sollte. Wenn der Kunde diese Grenze überschreitet, sollte er nur noch Dienste der Deutschen Telekom und ihrer Partner mit gewohnter Schnelligkeit erhalten sollen, für die restliche Datenübertragung sollte die Geschwindigkeit ge*drosselt* werden und faktisch so langsam erfolgen wie das Internet in den 1990er Jahren. 75 GB pro Monat mag zunächst nach viel klingen. Wir können das Problem dahinter aber schon im Mobilfunkbereich beobachten. Die Deutsche Telekom ist z.B. am Unternehmen Spotify und dessen Musikstreaming beteiligt. Die Deutsche Telekom hat auch 30-40 Prozent Marktanteil im Mobilfunkmarkt. Wenn sie aus den Ballungsgebieten herausfahren, ist die Deutsche Telekom mit T-Mobil manchmal regelrecht Monopolist, weil es keinen anderen Anbieter gibt. Spotify, der Musikstreaming-Dienst, wird gegenüber allen anderen Streaming-Diensten bevorzugt, weil er vom kontingentierten Datenvolumen ausgenommen ist. Wenn sie nur 300MB haben, dann hören sie keine andere Musik über ihr Monatsvolumen, weil es sonst ganz schnell weg wäre und sie Geld nachwerfen müssten. Spotify aber kriegen sie die ganze Zeit in gewohnter Geschwindigkeit. Das ist eine Bevorzugung eines Partnerunterunternehmens und eine Benachteiligung oder eine Diskriminierung von allen anderen Anbietern. Das bedeutet zum einen, dass alle anderen viel schlechtere Marktchancen haben, aber das bedeutet gleichzeitig auch, dass mein eigener Podcast bei *netzpolitik.org* gegenüber Spotify benachteiligt wird.

Im vergangenen Jahr gab es einige Proteste gegen die Telekom, an denen wir uns von der netzpolitik.org-Redaktion beteiligt haben. Wir haben u.a. eine Onlinedemo auf der Seite der Telekom organisiert, bis sie das JavaScript abgeändert haben. Wir sind auch zu einer Hauptversammlung nach Köln gefahren und haben dort ein riesiges Plakat aufgehängt und damit gewissermaßen die Medienberichterstattung ein bisschen

‚gehackt', aber wir warten die ganze Zeit darauf, dass die Politik sich in dieser Frage substanziell äußert. Es kursierte lediglich ein Zitat von Angela Merkel:

> „Und, das Stichwort Netzneutralität ist für uns sehr wichtig. Jeder Nutzer, egal was er verdient, welchen Bildungsgrad er hat, soll die Möglichkeit haben, den gleichen Zugang zum Internet zu bekommen. Es darf kein Internet erster und zweiter Klasse geben" (Merkel 2011).

Diese Aussage gefiel uns zunächst gut. Dass es „kein Internet erster und zweiter Klasse geben" dürfe, fanden wir richtig. Das ist auch unsere Meinung. Sie formulierte diese Forderung allerdings in ihrem Podcast vor über zwei Jahren. Mittlerweile haben Telekommunikationsunternehmen massiv Lobbying betrieben. Im Oktober 2014 erklärte Angela Merkel die Debatte um Netzneutralität für beendet, und zwar mit der aufschiebenden Aussage, dass man sich mit Netzneutralität erst beschäftigen muss, wenn es gar kein Problem mehr geben wird, weil Netzneutralität vor allen Dingen, oder die Verletzung von Netzneutralität vor allen Dingen ein Verknappungsproblem sein wird (vgl. Merkel 2014).

In Ländern, in denen es einen richtigen Breitbandausbau gibt, wo also mehrere hundert Megabyte pro Sekunde durch Glasfaserkabel übertragen werden, wie in Schweden usw., gibt es kaum oder keine Probleme mit Netzneutralität. Das Problem existiert nur in Ländern wie Deutschland, wo der Breitbandausbau einfach versäumt worden ist, weil die ganze Zeit die Politik den Markt das regeln lassen wollte. Da der Breitbandausbau aber sehr viel kostet, wurde nur dort ausgebaut, wo es sich geschäftlich lohnt. Das hat dazu geführt, dass Deutschland auf Platz 15 im europäischen Vergleich ist, was die Versorgung mit Breitband betrifft.[9] Vor Deutschland in dieser Rangfolge befinden sich eine ganze Reihe wirtschaftsschwächerer und ärmerer Länder mit weniger Ansprüchen, die einfach mehr in den Breitbandausbau investiert haben, die das als gesellschaftliche Aufgabe gesehen haben, während in Deutschland alles dem Markt überlassen wurde, der die Aufgabe aber nicht übernommen hat.

Mittlerweile scheint gewiss, dass die politische Debatte über Netzneutralität in Brüssel entschieden wird. Das Europaparlament hat vor einem halben Jahr gesagt, dass es ganz klare Regeln für Netzneutralität geben muss (vgl. Europäisches Parlament 2014). Das Ganze ist jetzt im Ministerrat gelandet, in dem Deutschland sich als einer der stärksten Player positioniert hat. Auf einmal gibt die Politik Signale, die genauso klingen wie von den Lobbyisten der Deutschen Telekom. Wir können uns das nur so erklären, dass ein Hütchen- oder Taschenspielertrick angewendet wird. Die Politik sagt weiterhin, dass der Breitbandausbau vorangetrieben werden soll, weil immerhin die digitale Agenda mit einer Zielvereinbarung von 50 Megabyte bis 2018, im Koalitionsvertrag steht. Im Übrigen man kann es, diplomatisch ausgedrückt, als sehr unterambitioniert bezeichnen, 50 Megabyte erst 2018 überall im Land haben zu wollen. Selbst

9 Eurostat: Versorgung mit festen Breitbandanschlüssen (isoc_tc_fbcov), abrufbar unter: http://ec.europa.eu/eurostat/web/products-datasets/-/isoc_tc_fbcov.

das dünn besiedelte Australien erreicht schon jetzt ein Vielfaches (vgl. Beckert et al. 2012).

Der Taschenspielertrick scheint aber nun darin zu bestehen, dass die Politik, kein Geld investiert und dafür gewissermaßen ‚Regulierungsferien' gibt. Die Telekommunikationsbranche darf bzw. muss dann Netzneutralitätsregeln vorübergehend nicht beachten, darf in dieser Hinsicht also machen, was sie will. Wir befürchten, dass dieser Trick nach hinten losgeht, weil es weiterhin keine Anreize geben wird, das Netz auszubauen, sondern eher Anreize, aus dem bestehenden Netz durch neuartige Geschäftsmodelle noch viel mehr rauszuholen und damit das Zweiklassennetz zu legalisieren. Deswegen sollte man aus unserer Sicht jetzt unbedingt fordern, dass Netzneutralität im Gesetz verankert werden muss. Auf EU Ebene hätten wir die Möglichkeit dazu. Die neuesten Aussagen der Bundesregierung klingen danach, dass wir zumindest auf der bundesdeutschen Ebene verloren haben. Es sei denn, die anderen 27 EU-Staaten haben eine andere Meinung, aber das ist nicht immer gewährleistet.

4 Urheberrecht: Nutzung, Probleme und Auswirkungen

Damit komme ich zum dritten Thema, das früher einmal das größte Thema war und besonders kontrovers diskutiert wurde: das Urheberrecht. Ich habe mich immer gefragt, nachdem ich Jahre lang an Urheberrechtsdiskussionen teilgenommen hatte: Wann war eigentlich meine erste Urheberrechtsverletzung? Ich vermute, es war in der ersten oder zweiten Schulklasse. Denn in dieser Zeit haben wir in der Schule Collagen gebastelt. Wir haben aus Zeitungen Bilder ausgeschnitten und sie aufeinander geklebt. Das war alles vollkommen legal und vom Recht auf Privatkopie gedeckt. Allerdings haben wir sie danach in der Schule ausgestellt. Das ist verboten, weil es sich um eine öffentliche Aufführung handelt. Natürlich hatten wir Glück, dass damals nicht irgendwelche Abmahnanwälte durch die Schulen liefen, um einmal nachzuschauen, was dort alles hängt und ob die Rechte für diese öffentlichen Aufführungen alle vorab geklärt worden sind.

Mittlerweile haben wir das Netz und die Nutzer produzieren permanent Collagen und stellen sie ins Netz, was dazu führt, dass automatisierte Abmahnroboter automatisierte Abmahnungen über 1000 Euro verschicken. Das ist ein ziemliches Problem. Auf der einen Seite besteht auch meine Arbeit aus oder basiert auf Urheberrechten. Ich bin Journalist, ich schreibe ganz viel und habe auch kein Interesse daran, dass der Axel Springer Verlag meine ganzen Texte nimmt und damit Geld verdient. Mit dem Blick auf die private Nutzung des Internets haben wir aber ein Problem, weil das Urheberrecht nach strenger Lesart sagt: Alles ist verboten, was Spaß macht. Zumindest ist Vieles verboten, wenn man nicht eine Einwilligung dafür hat. Außerdem ist das Urheberrecht sehr unterschiedlich. Es gibt ein europäisches Urheberrecht mit einer deutschen und einer französischen Tradition, dazu ein europäisches Urheberrecht mit einer britischen Variante, die sehr nah an dem amerikanischen ist – und in den USA kann man ohnehin

viel mehr im Netz machen, auch Collagen usw., als in Deutschland. In Deutschland, so könnte man überspitzt formulieren, ist erst einmal alles verboten. Es heißt in den meisten Fällen nur: Man müsste eigentlich jeden einzeln erst einmal um Erlaubnis fragen, bevor man etwas nutzen kann.

Das wäre erst einmal kein Problem, wenn Computer nicht Kopiermaschinen wären und nicht die ganze Zeit Einsen und Nullen hin- und her kopiert würden, so dass eigentlich nur die Frage ist, wie hoch die Schöpfungshöhe von jedem einzelnen Kopiervorgang ist, der vonstattengeht, wenn wir gerade eine Taste drücken.

Allerdings war dieser technische Wesenszug solange kein Problem oder wurde so lange nicht als Problem wahrgenommen, bis eine gewisse Software auftauchte: Napster. Ich erinnere mich noch daran, denn das war einer der schönsten Internetmomente meines Lebens – Napster. Wir hatten damals 1998/99 nur ISDN und ich habe sofort eine Flatrate gebucht. Ich hatte zum ersten Mal Zugriff auf die Musik der Welt, wovon ich mein Leben lang geträumt hatte. Bisher musste ich immer in Plattenläden anstehen und ein paar Sachen heraussuchen, mit *Napster* dagegen konnte man alles herunterladen, was es gab – d.h. damals max. 25 Megabyte pro Stunde, mehr ging nicht über ISDN. Ich hätte dafür auch Geld ausgegeben, es gab diesen Service aber nicht. Diese Bereitschaft war nicht nur bei mir, sondern bei Vielen zu beobachten.

Probleme entstanden dann natürlich dadurch, dass kein Interesse vorhanden war, das ganze legal werden zu lassen oder zuzulassen, dass weiterhin Menschen Musikstücke kopieren. Es gab Klagewellen gegen Napster und Co. In anderen Ländern wurden sogar Netzsperren eingeführt, was das Problem aber nicht gelöst hat. Menschen haben weiterhin kopiert, auch wenn laut Verbraucherzentrale Bundesverband (Stand 2012) in Deutschland vier Millionen Abmahnungen verschickt worden sein sollen. Auch heute gibt es noch viele Menschen, die Musik, Filme und Bücher kopieren. Das Skurrile war, dass es so lange gedauert hat, bis sich legale Alternativen etabliert hatten. Viele Nutzer fragten sich: Warum muss ich eigentlich zu *kino.to* gehen, wo es total kompliziert gemacht wird, um mir einen Film anzuschauen? Die Menüführung war sehr kompliziert und die Nutzer mussten darauf achten, sich keine Viren einzufangen. Es war jedoch die einzige Möglichkeit überhaupt, Zugriff auf bestimmte Filme zu bekommen. Angesichts dieser Tatsachen fragt man sich: Wieso hat diesen Markt denn keiner gesehen? Warum stellte lange Zeit niemand legale Angebote bereit. Im Musikbereich war es viel auffälliger. Jahrelang wurde die Entwicklung einfach nicht beachtet, oder es wurden Angebote ins Netz gestellt, die es einem extrem schwierig machten zu bezahlen, etwas rauszusuchen und dann auch noch möglicherweise auf mehreren eigenen Rechnern und Geräten anzuhören.

Diese falsch geführte Tauschbörsendebatte ist ein Teil einer breiteren Urheberrechtsdebatte, die so komplex ist, dass man den ganzen Tag darstellen könnte, was die netzpolitischen Implikationen von Urheberrecht sind. Ich möchte aber noch auf etwas anderes eingehen, und zwar auf die Remixe: den Remix-Aspekt, also das Collagen-Erstellen im audiovisuellen Format. DJ Danger Mouse ist später erst berühmt gewor-

den, aber bereits vor über zehn Jahren hat er etwas vollbracht, womit er bei Musikkritikern als Entdeckung des Jahres bezeichnet wurde. Er hat das *Weiße Album* von den Beatles genommen und es komplett mit dem *Black Album* von Jay Z gemixt. Das hatte noch nie jemand vor ihm versucht, und viele waren begeistert, wie kreativ und gut gelungen das war. Er bekam von verschiedenen Seiten höchstes Lob, das Problem war aber, dass die Rechte nicht geklärt waren. Sony verweigerte die Rechte, er hat es trotzdem online gestellt. Das wiederum versuchten die Anwälte von Sony mit Abmahnungen rückgängig zu machen.[10] Es gab Solidarisierungswellen, als das Album etwa im Jahr 2003 auf Tausenden Servern geteilt wurde, um es dieser Art von ‚Zensur' zu entziehen, damit dieses künstlerische Werk weiterhin allen zugänglich bleibt. Das Absurde an der Geschichte ist ja, dass damit eine Reihe von Beteiligten und vor allem Sony und Co. eine ganze Menge Geld hätten verdienen können, sie wollten es nur nicht.

Im Bereich des Urheberrechts gibt es aber wenigstens positive Tendenzen. Man hat gewissermaßen etwas daraus gelernt, und mittlerweile wird es durchaus auch als vertriebsunterstützende Maßnahme oder Marketingmaßnahme angesehen. Sie kennen vielleicht das Video „Gangnam Style". Das heißt, vielleicht kennen sie es auch nicht oder nur vom Hören, weil man es in Deutschland nicht sehen kann. Das liegt am problematischen Zusammenspiel von GEMA und YouTube. Ich denke, beide Seiten sind an dem jetzigen Zustand schuld. Zwar versucht YouTube immer, die Verantwortung der GEMA in die Schuhe zu schieben, aber das scheint nur die halbe Wahrheit. Im Fall des Musikvideos des Rappers Psy[11] führte es auf jeden Fall dazu, dass wir Deutschen es nicht sehen konnten, während zur gleichen Zeit weltweit fast eine Million Remixe von diesem Video erschienen sind. Dabei haben viele Menschen durch einen Remix eigentlich erstmal eine gemeinsame Popkultur erlebt, waren kreativ, haben Medienkompetenz gezeigt und sich dabei auch noch bewegt, saßen also nicht nur vorm Rechner. Man konnte es sogar für politische Zwecke nutzen, wie ein Video des Künstlers Ai Weiwei zeigt.[12] Dieses Video wiederum war in China gesperrt. Man kann also festhalten, dass dieses Gangnam Style sehr viele verschiedene Aspekte an Remixkultur und freier Meinungsäußerung hervorgebracht hat. Wären diese Remixe alle verklagt und aus dem Netz genommen worden, wären kostenloses Marketing und Tantiemen in geschätzter Höhe von einer Milliarde Dollar nicht eingenommen worden.

Das Beispiel zeigt auch, dass die nationalen Regeln sehr unterschiedlich sind, so dass es dem Nutzer, der ein Angebot im globalen Netz betrachten will, willkürlich erscheinen muss. In den USA etwa ist das Remixen in dieser Weise erlaubt. Die USA haben so genannte Fair-use-Regeln. Zu künstlerischen, wissenschaftlichen, und zu Bildungszwecken oder zu Zwecken der freien Meinungsäußerung dürfen dort Remixe produziert werden, und zwar nicht nur im stillen Kämmerlein, wie in Deutschland, sie

10 Für nähere Informationen siehe: http://museum.rechtaufremix.org/.

11 Psy: Gangnam Style: https://www.youtube.com/watch?v=CH1XGdu-hzQ und die Remixe: https://www.youtube.com/results?search_query=gangnam+style+remix.

12 Ai Weiwei does Gangnam Style: https://www.youtube.com/watch?v=n281GWfT1E8.

dürfen sie auch legal mit anderen teilen. Das ist dort durch die Rechtslage gedeckt, in Deutschland aber leider nicht. Das liegt an der europäischen Urheberrechtsrichtlinie. Um diese zu ändern, müsste es neue Schrankenregelungen[13] geben. Prinzipiell wäre das möglich, es müsste nur angegangen werden. Die netzpolitische Kompetenz in den zuständigen europäischen Gremien lässt bisher zu wünschen übrig. Die Besetzung des Digitalkommissars Oettinger wurde in diesem Sinne von der digitalen Zivilgesellschaft kritisiert.

Wir haben dazu auch eine Initiative gestartet, genannt „Recht auf Remix“, mit der wir auch die kulturellen Elemente von Remixen, die sich früher schon ähnlich zeigten, ansprechen. Medienwissenschaftlich gesehen, ist die ganze Mediengeschichte voll von Remixkunst. Allerdings beobachten wir nun eben eine Demokratisierung in diesem Bereich, jeder kann remixen. Früher konnten wir auch Collagen erstellen, aber jetzt können wir richtig cool remixen, wenn wir wollen.

Die Kampagne soll auch dazu beitragen, die Zusammenhänge von Internet und Urheberrecht zu erklären und das Remixen so auch aus der ‚Schmuddelecke‘ herauszuholen. In Deutschland wird es sehr streng als eine Urheberrechtsverletzung bewertet. Wenn man hierzulande eine Urheberrechtsverletzung begeht, begibt man sich sofort in den Verdacht, am Untergang des Abendlandes beteiligt zu sein und Urheber entrechten zu wollen, wobei die meisten doch lediglich zur Kultur beitragen möchten. Es gibt auch einen Menüpunkt „Remix vor Gericht“ auf museum.rechtaufremix.org. Dort haben wir nochmal versucht feuilletonkompatibel zu erklären was ein Remix überhaupt ist, eben für diejenigen, die befürchten, dass ein Remix den Untergang des Abendlandes bedeuten könnte. Das ist der eine Aspekt, der mir in der Urheberrechtsdebatte wichtig scheint, vielleicht verbunden mit der Klarstellung, dass Fallschirm-Abmahnungen unsinnig sind und im Grunde nur Anwälten etwas bringen, aber sonst niemandem.

Nun zum anderen Aspekt: Wahrscheinlich kennen Sie alle E-Book Reader. Ich habe selbst auch so ein Teil. Tatsächlich zähle ich auch exakt zur Zielgruppe, nutze ihn allerdings kaum, obwohl ich die ganze Zeit Bücher lese. Wenn ich in den Urlaub fahre, nehme ich mir lieber ‘normale’ Bücher mit. Ich hab auch mal einen E-Book-Reader mit in den Urlaub genommen, doch leider hat sich jemand draufgesetzt, und ich hatte dann gar keine Bücher mehr dabei. Das eigentliche Problem aber ist, dass ich keine E-Books kaufen möchte. Haben Sie schon einmal die Allgemeinen Geschäftsbedingungen für die Bücher durchgelesen? Wahrscheinlich nicht, oder?

Was alles möglich ist, lässt sich vielleicht am besten an einem Beispiel illustrieren: Es gibt den Fall des Buches 1984. Bei Amazon gab es 1984 zu kaufen und irgendwann stellte sich heraus, dass die Rechtefrage nicht ganz geklärt ist, also ob Amazon das

13 Die Schranken des Urheberrechts sollen einen Ausgleich zwischen den Interessen des Urhebers, dem das deutsche Urheberrecht ausschließliche Nutzungsrechte einräumt, und gegenläufigen Interessen schaffen (justlaw o.J.).

Buch über seinen Online-Store verkaufen durfte. Was daraufhin passierte war, dass Amazon, das Buch zurückgezogen hat. Diesen Vorgang können sie sich in der analogen Welt so vorstellen: Sie kaufen ein Buch im Buchladen und nachts steigt der Buchhändler bei Ihnen ein, nimmt das Buch wieder mit, legt einen Zehner hin, und sie können nichts dagegen unternehmen. Genau das aber kann passieren. Sie haben sich wahrscheinlich noch nicht die Allgemeinen Geschäftsbedingungen von einem E-Book durchgelesen, wahrscheinlich auch nicht von einem normalen Buch – ich kann mir sogar vorstellen, dass es die mittlerweile auch gibt. Auf jeden Fall erwerben wir im Fall von E-Books gar nicht mehr ein Buch, wir erwerben auch keine Datei, wir erwerben ein Nutzungsrecht, und dieses Nutzungsrecht kann uns wieder entzogen werden. Das kann manchmal zu Problemen führen, wie z.B. wenn sie 1984 gekauft hatten oder aber wenn sie die ersten Konkurrenz-mp3s von Microsoft gekauft hatten. I-tunes ging online, Apple rollte damit den ganzen Musikmarkt auf, Microsoft wollte dabei sein und verkaufte über seinen Musikstore mit dem Logo „Plays for sure“ kopiergeschützte Musikdateien, die man nirgendwo sonst abspielen konnte. Dabei wurde die ganze Zeit über suggeriert, die Dateien könnten überall abgespielt werden. Gemeint war natürlich: überall, wo Windows installiert ist, aber sonst leider nicht. Da stand ja auch: „Plays for sure“. Zwei Jahre später wurde der Kopierschutz dann verändert, weil der alte nicht gut funktionierte. Daraufhin dachte Microsoft tatsächlich, dass sie damit durchkommen, dass sich die Leute die ganze Musik neu kaufen, da die alten Dateien nicht mehr gelesen werden konnten (vgl. Spiegel Online 2008).

Das zeigt die Problematik auf, dass es Kopierschutzsysteme gibt, die nicht mehr nachhaltig sind. Wenn wir Pech haben, können wir in 50 Jahren nicht mehr auf unsere Dateien von heute zugreifen oder Archäologen in 100 Jahren nicht mehr auf ihr gespeichertes Material zugreifen, weil das alles kopiergeschützt ist. Aber hier zeigt sich auch eine Form der Gängelung für Nutzer durch solche Systeme und Regeln. Warum soll ich denn so etwas kaufen, was in der Tauschbörse kostenlos und offen und vor allem nachhaltig verfügbar ist. Außerdem werfen diese Erfahrungen ganz viele Fragen auf, wie: Wem vererben sie eigentlich mal ihre Musiksammlung? Und können sie überhaupt ihre Musiksammlung vererben? Auch diese Fragen sind vollkommen ungeklärt. Fragt man zwei Juristen, bekommt man drei Antworten. Auch die Politik versucht sich an verschiedenen Lösungen. Es ließe sich auch hinbekommen, genau wie bei einem Zweitmarkt. Interessante Unterschiede lassen sich auch beim E-Book zeigen: Wenn sie ein normales Buch kaufen, können sie es zerreißen, weiter verschenken, verleihen, es weiter verkaufen. Wenn sie allerdings ein E-Book kaufen, können sie all das nicht tun. Wenn sie Pech haben, ist es auch nächstes Jahr gar nicht mehr abspielbar, aber sie haben dasselbe bezahlt.

Auch in Zukunft kommen gerade im Bereich Urheberrecht noch sehr spannende Debatten auf uns zu. Im Vergleich dazu waren die bisherigen Probleme noch relativ einfach. Kennen Sie 3D-Drucker? Es gibt Leute, die behaupten, dass in zehn Jahren so ein Teil überall steht. Vielleicht kennen Sie Star Trek. Die Figuren in der Serie stehen

immer wieder vor einer Art Mikrowelle, drücken einen Knopf und dann kommt z.B. ein Hühnchen heraus. Es ist nun nicht so, dass es bei einem 3D-Drucker um etwas Essbares geht, aber diese Geräte können Ihnen irgendwelche Gegenstände ausdrucken und das funktioniert schon ganz ordentlich. Ich bezweifle zwar, dass wir in zehn Jahren alle so etwas im Keller stehen haben, aber ich habe in der Tat schon viele Freunde und Bekannte, die tatsächlich ein solches Gerät besitzen und damit herum experimentieren. Das ist ja auch sinnvoll und schön. Man kann dann z.B. Baumaterialien oder Baupläne teilen und ausdrucken sowie Autos und Motoren nachbauen. Man kann mittlerweile Gebisse usw. nachbauen und sogar Waffenteile. Letzteres wirft natürlich ganz andere Fragen auf, es gibt nämlich libertäre Zirkel in den USA, die unbedingt Waffen drucken wollen. Die halten das für ein großes Grundrecht, das machen zu können. Aber wie gehen wir eigentlich damit um, dass auf einmal Baupläne geteilt werden können? Natürlich versucht man jetzt auch Kopierschutzsysteme usw. einzubauen, aber eigentlich warten Eltern doch nur darauf, dass man endlich mal Lego ausdrucken kann, oder?

Die eigentliche Frage dahinter ist: Wie lösen wir diesen grundlegenden Urheberrechtskonflikt? Ich habe im Vorangegangenen ja einige Zusammenhänge angedeutet, in denen wir auf der einen Seite Urheber haben, auf der anderen Verwerter, und wir Nutzer sind auch noch dabei. Teilweise sind wir sogar alles zugleich. Also ich bin sowohl Verwerter von meinem Blog, als auch Urheber, als auch Nutzer. Ich habe sozusagen drei verschiedene Interessen. Aber bisher haben wir eigentlich das Urheberrecht immer nur aus einer Perspektive verhandelt, nämlich der des Urhebers. Es soll härter durchgegriffen werden, das alte Urheberrecht soll aus der analogen Welt übertragen werden. Wir haben die ganze Zeit darüber diskutiert, Vorratsdaten zu speichern, Netzsperren zu errichten, Leuten das Internet wegzunehmen. Vielleicht sollten wir besser darüber diskutieren, das Urheberrecht so zu reformieren, das weiterhin Künstler vergütet werden, aber wir auch Rechte als Nutzer haben und nicht zu Kriminellen gemacht werden, und zwar aufgrund solcher Aktivitäten, die in Amerika alle legal sind.

Deswegen gab es vor zwei Jahren große Demonstrationen. Das war zum ersten Mal ein Punkt, an dem die Jugend auf die Straße ging, um gegenüber überbordenden Maßnahmen einfach mal „Stopp“ zu sagen: Bis hierhin und nicht weiter. Das hat in der Politik, zumindest auf EU-Ebene, dazu geführt, dass man sich zwei Jahre lang nicht mehr an die Urheberrechtsreformen getraut hat, sondern erst einmal die Wahlen abwarten wollte. Das hat wiederum dazu geführt, dass wir zwar zum ersten Mal so einen Stopp-Moment hatten, dann aber doch immer weiter das Urheberrecht durchgesetzt wurde, ohne über eine Reform wirklich nachzudenken. Jetzt soll der Digitalkommissar Günther Oettinger das Ganze reformieren. Trotz aller Bedenken besteht seitens der digitalen Zivilgesellschaft immer noch die Hoffnung, dass er uns positiv überraschen wird und wir alle nur Vorurteile haben.

5 Datenschutz: Zentralisierung und Netzwerkeffekte

Damit kommen wir zum letzten Thema: Datenschutz. Wir haben, wenn wir uns auf einem Marktplatz versammeln, Rechte: das Versammlungsrecht, die Meinungsfreiheit, also Grundrechte, die unsere Vorfahren erkämpft haben und wir profitieren davon. Wir können auf die Straße gehen, können demonstrieren. Wir können unser Recht auf freie Meinungsäußerung praktizieren. Aber versuchen sie das einmal in einem Einkaufszentrum. Haben Sie schon einmal die Allgemeinen Geschäftsbedingungen von einem Einkaufszentrum gelesen? Die gibt es auch. Da steht nämlich, dass alles verboten ist, was Spaß macht, oder sagen wir mal, Ihre Grundrechte gelten da nur bedingt. Weswegen beschreibe ich das? – Wir machen uns immer abhängiger von privatisierten Öffentlichkeiten im Netz, vielen privat betriebenen Online-Plattformen, die ihre Server in anderen Jurisdiktionen stehen haben. Es gibt zentrale Plattformen, die in den USA stehen, wo also US-amerikanische Datenschutzgesetze gelten, die eigentlich das Wort nicht wert sind. Bei der Bewegung auf solchen Plattformen wie z.B. Facebook, weiß keiner genau, was die Betreiber überhaupt mit unseren Daten machen, wo die Allgemeinen Geschäftsbedingungen gelten, die Sie sich wahrscheinlich nie durchgelesen haben, denn diese sind noch länger als alle anderen, also über 50 Seiten. Dazu gibt es noch die Datenschutzbestimmungen. Darin besteht ein echtes Problem, wenn 50 bis 60 Prozent aller deutschen Internetnutzer jetzt schon bei Facebook sind. Es gibt eine Sogwirkung. Natürlich kann man sagen: Ich bin nicht bei Facebook, ich verweigere mich dem. Dann hat man aber mit anderen sozialen Folgen zu kämpfen, dass man etwa nicht mehr zu Partys eingeladen wird oder Ähnliches.

Heute fangen ja sogar immer mehr Politiker an, über Facebook mit ihren Wählern zu kommunizieren, weil es einfach ist und sie ja eh in Facebook sind. Also haben wir hier eine große Sogwirkung. Und genau darin besteht das grundlegende Problem: Wir dachten früher, das Netz führe zu Dezentralität. Dezentralität ist prinzipiell gut. Stattdessen sind wir komplett überrascht worden in unserem utopischen Denken. Das Netz führt nämlich zu massiven Netzwerkeffekten und tendiert aufgrund dessen zu Monopolen. Das ist genau der Grund, warum es zwar ganz viele soziale Netzwerke gibt, aber trotzdem alle bei Facebook sind, weil eben alle anderen dort sind. Gerade gibt es noch für eine Woche einen neuen Trend *ello*, also ein neues Netzwerk. Da ist aber jetzt auch schon wieder keiner mehr. Für eine Woche dachten alle, es würde neu dazu kommen, aber dem war nicht so. Es gibt dezentrale Netzwerke wie *Diaspora*. Das finde ich sehr gut, aber mein Problem ist, dass ich dort niemanden zum Kommunizieren habe, weil alle bei Facebook sind.

Die Netzwerkeffekte sind eine zentrale Herausforderung, denn gerade auf diesen Plattformen begeben wir uns in privatisierte Öffentlichkeiten, machen uns von privatisierten Infrastrukturen abhängig. Dort gelten jedoch eher die Regeln eines Einkaufszentrums als eines Marktplatzes. Dort gibt es dann z.B. auch privates Sicherheitspersonal, welches einfach Leute aussperren kann. Das können in der virtuellen Welt auch

Algorithmen sein. Es gab mal eine Zeit lang das große Problem von stillenden Müttern, die zur Solidarisierung die ganze Zeit Fotos von sich und ihrem Kind an der Brust auf Facebook luden, aber Algorithmen das wegen „nudity“, also wegen Nacktheit herunter genommen haben. Problematisch sind wohlgemerkt nur nackte Oberkörper von Frauen, nackte Oberkörper von Männern stellen kein Problem dar. Da haben wir also amerikanische Werte, die dort über Algorithmen und über Allgemeine Geschäftsbedingungen zur Geltung gebracht werden. Man kann natürlich glücklich sein, dass wir hier in einer liberalen Gesellschaft leben, und nicht in den USA, aber wie wir sehen, können wir in einem Netzwerk wie dem von Facebook trotzdem davon betroffen sein.

Das führt dann zu anderen Problemen: Was ist, wenn sie auf einmal persönlich betroffen sind? Der skurrilste Fall, von dem ich mal gehört habe, ist dieser: Es gibt ein großes Medium, dessen Namen ich einmal nicht nenne. Dort arbeiten verschiedene Leute, die ich kenne, als Administratoren von dessen Facebookseite, einfach weil sie in der Onlineabteilung arbeiten. Aus irgendeinem Grund haben sie dort das Bild von einer Playboy-Ausgabe auf die Facebookseite gestellt. Warum auch immer, sie arbeiten nicht für den Playboy. Das führte dazu, dass das Bild als anstößig gemeldet wurde, obwohl es in jedem Kiosk auslag. Das Ganze verursachte den erheblichen Kollateralschaden, dass auch alle Administratoren gesperrt wurden, die für diese Seite zuständig waren. Sie wurden nicht nur als Administratoren der Seite gesperrt, sondern auch ihr privater Facebookaccount wurde gesperrt. So sind die Regeln bei Facebook. Da hat jemand die zusätzliche Rolle bekommen, auch noch Administrator für die dienstliche Seite zu sein und wird aufgrund dieser Tätigkeit auf einmal auch vom privaten Gebrauch ausgeschlossen. Stellen Sie sich für diesen Fall einmal vor, es handelte sich nicht um ein großes Unternehmen, ein großes Medium, in dem Sie ganz schnell die Pressestelle anrufen können, über die eine komplizierte Klärung und Lösung des Problems vorgenommen werden kann, so dass Ihr Benutzerkonto bald reaktiviert wird und Sie wieder an ihrem sozialen Leben teilhaben können. Stellen Sie sich nun noch vor, Sie kennen noch nicht mal die Pressestelle. Dann sind Sie ein Nichts für Facebook und haben Probleme, weil irgendein Algorithmus gedacht hat, dass Sie gegen die Allgemeinen Geschäftsbedingungen verstoßen. Offensichtlich haben wir also das Problem, dass wir uns als Gesellschaft immer abhängiger von diesen Infrastrukturen machen und keine Sanktionsmöglichkeiten oder Rechtsmöglichkeiten haben, um gegen, sagen wir einmal: Missbrauch durch die andere Seite, vorzugehen. Die einen sagen, das müssen wir uns erkämpfen, die anderen sagen, wir müssen dezentrale offene Infrastrukturen fördern und aufbauen, damit wir morgen möglichst eine Alternative haben, auch wenn sie heute noch nicht da ist.

6 Fazit

Zusammenfassend möchte ich als Bilanz und Aufforderung zugleich formulieren: Es ist unser Netz! Und wenn die Frage gestellt wird: Wer kontrolliert oder regiert das Inter-

net? Dann kann man schon sagen: Natürlich haben wir das Problem, dass die ganzen Infrastrukturen dieses Netzes in privater Hand sind, ebenso die großen Plattformen und das Kabelnetz. Die Politik kann aber Regeln setzen und wir können Politik mitbestimmen. Wenn wir aber die ganze Zeit nur als Konsumenten da sitzen und nichts tun und hoffen, dass irgendetwas passiert, dann wird über unsere Interessen hinweg entschieden. Deswegen noch einmal zum Schluss: Wir sind das Internet und wir können auch für ein demokratisches Internet kämpfen.

Literatur

ANT Product Data (2008): NSA/CSSM 1–52, S32221–S32242, https://search.edwardsnowden.com/docs/ANTProductData20131230 (23.08.2015).

Beckert, Bernd / Riem, Ulrich (2012): Gesetzliche Regelungen für den Zugang zur Informationsgesellschaft. Endbericht zum Monitoring des Büros für Technikfolgenabschätzung (TAB), https://www.tab-beim-bundestag.de/de/pdf/publikationen/berichte/TAB-Arbeitsbericht-ab149.pdf (23.08.2015).

Berners-Lee, Tim (o.J.): Tim Berners-Lee, https://www.w3.org/People/Berners-Lee/ (24.08.2015).

Europäisches Parlament (2014): EU-Abgeordnete setzen sich für Netzneutralität ein, erlauben aber spezialisierte Dienste, 20.03.2014, http://www.europarl.europa.eu/news/de/news-room/content/20140319STO39309/html/MEPs-setzen-sich-f%C3%BCr-Netzneutralit%C3%A4t-ein-erlauben-aber-spezialisierte-Dienste (23.08.2015).

Europäisches Parlament (2001): Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)), 11.07.2001, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//DE (22.08.2015).

Friedrich, Hans-Peter (2013): Interview, in: Rheinische Post Online: Friedrich: "Stolz auf unsere Geheimdienste", 16.08.2013, http://www.rp-online.de/politik/deutschland/friedrich-stolz-auf-unsere-geheimdienste-aid-1.3607811 (22.08.2015).

Just Law (o.J.): Einschränkungen des Urheberrechts, §§ 44a - 63a UrhG, http://www.urheberrecht.justlaw.de/schranken.htm (23.08.2015).

Merkel, Angela (2014): Rede von Bundeskanzlerin Merkel anlässlich des 8. Nationalen IT-Gipfels am 21.Oktober 2014, http://www.bundesregierung.de/Content/DE/Rede/2014/10/2014-10-20-merkel-it-gipfel.html (23.08.2015).

Merkel, Angela (2011): Internet ist eine positive Revolution, 22.10.2011, http://www.bundeskanzlerin.de/nn_707282/Content/DE/Podcast/2011/2011-10-22-Video-Podcast/2011-10-22-Video-Podcast.html (23.08.2015).

N24 (2013): Gericht stoppt „Drosselkom“, 30.10.2013, http://www.n24.de/n24/Nachrichten/Wirtschaft/d/3755852/gericht-stoppt--drosselkom-.html (23.08.2013).

Pofalla, Ronald (2013): Statement zur NSA-Affäre, in: PhoenixTV - Kontrollgremium NSA-Affäre (05) Ronald Pofalla #CDU (1/2), 12.08.2013, https://www.youtube.com/watch?v=bkBdHYvDYPE (22.08.2015).

Reed, David (o.J.): Biography, http://www.reed.com/dpr/locus/dprbiog/ (24.08.2015).

Remix Museum (o.J.): Danker Mouse – the grey album, http://museum.rechtaufremix.org/exponate/danger-mouse-the-grey-album/ (23.08.2015)

Spiegel Online (2013a): NSA-Überwachung: Merkels Handy steht seit 2002 auf US-Abhörliste, 26.10.2013, http://www.spiegel.de/politik/deutschland/nsa-ueberwachung-merkel-steht-seit-2002-auf-us-abhoerliste-a-930193.html (22.08.2015).

Spiegel Online (2013b): NSA-Enthüllungen: Chronologie der Snowden-Affäre, 12.07.2013, http://www.spiegel.de/politik/ausland/nsa-spaehaktion-eine-chronologie-der-enthuellungen-a-910838.html (22.08.2015).
Spiegel Online (2008): DRM-Debakel: Bürgerrechtler wüten gegen Microsoft-Musik mit Verfallsdatum, 30.04.2008, http://www.spiegel.de/netzwelt/web/drm-debakel-buergerrechtler-wueten-gegen-microsoft-musik-mit-verfallsdatum-a-550686.html (24.08.2015).
Süddeutsche Zeitung (2015): Geschichte eines Täuschungsmanövers, 27.05.2015, http://www.sueddeutsche.de/politik/no-spy-abkommen-geschichte-eines-taeuschungsmanoevers-1.2494417 (22.08.2015).
Tagesschau (2015a): Kanzleramt schon seit Kohl-Ära im NSA-Visier, 09.07.2015, https://www.tagesschau.de/inland/nsa-wikileaks-103.html (22.08.2015).
Tagesschau (2015b): Was bekannt ist und was vermutet wird, 07.05.2015, https://www.tagesschau.de/inland/bnd-203~_origin-a2b1e25e-7b65-42a9-ba40-44e6a468226e.html (22.08.2015).
The Guardian (2013): GCHQ taps fibre-optic cables for secret access to world's communications, 21.06.2013, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (23.08.2015).
Verbraucherzentrale Bundesverband (2012): Umfrage: Millionen Verbraucher von Abmahnungen wegen Urheberrechtsverstößen betroffen, 20.06.2012, http://www.vzbv.de/meldung/umfrage-millionen-verbraucher-von-abmahnungen-wegen-urheberrechtsverstoessen-betroffen (23.08.2015).
Vodafone (2015a): Vodafone Red Business Data-Tarife, https://www.vodafone.de/business/firmenkunden/telefonie-internet/internet-und-daten-tarife-fuer-tablets-netbooks-surfsticks-vodafone-red-business-data.html (23.08.2015).
Vodafone (2015b): Begriffsklärung, http://www.vodafone.de/privat/hilfe-support/glossar.html (23.08.2015).
Vodafone (2013): Red M Tarif, Screenshot in: netzpolitik.org 2013: Netzneutralität: Der Trick mit dem Kleingedruckten, 26.04.2013, http://www.netzwelt.de/news/95709-netzneutralitaet-trick-kleingedruckten.html (23.08.2015).
Wu, Tim (o.J.): Tim Wu, http://www.timwu.org/ (24.08.2015).
Zeit Online (2014): De Maizière nennt US-Überwachung maßlos, 06.04.2014, http://www.zeit.de/politik/2014-04/maiziere-nsa-usa (22.08.2015).

Autor

Markus Beckedahl
Gründer und Chefredakteur von netzpolitik.org
Schönhauser Allee 6/7
DE-10119 Berlin
markus@netzpolitik.org

DOI: 10.11588/josar.2015.0.23478

Internet Governance: Theoretische und empirische Annäherungen an einen schwer fassbaren Gegenstand

Jeanette Hofmann

1 Einleitung

Dieser Beitrag befasst sich mit drei Aspekten der Internet Governance. Zum Ersten geht es um den Gegenstandsbereich: Welchen Ausschnitt der Realität erfasst der Begriff, der reguliert wird? Zum Zweiten wird der Governance-Begriff selbst in konzeptioneller Absicht behandelt.[1] Dabei wird der Governance-Begriff, wie er im Rahmen der Internet-Governance-Literatur überwiegend verwendet wird, problematisiert und seine Neukonzeptualisierung vorgeschlagen. Diese Neukonzeptualisierung werde ich kurz vorstellen, um dann im dritten Teil die beiden zuvor thematisierten Aspekte in eine vorläufige Synthese zu bringen. Ziel des Aufsatzes ist es mithin, einen Beitrag zur wissenschaftlichen Debatte über die Art und Weise der Internet Governance zu leisten.

2 Zum Gegenstandsbereich: Was ist Internet Governance?

2.1 Ursprünge und Anlage

Was ist eigentlich Internet Governance? Wenn man den internationalen fachlichen und politischen Diskussionen über dieses Thema folgt, so könnte man – etwas flapsig formuliert – den Eindruck gewinnen, dass hier nahezu jede Woche eine neue Sau durch das Dorf getrieben wird. Wie grenzt man also einen Gegenstandsbereich ein, der so uferlos und auf den ersten Blick relativ unstrukturiert wirkt? Eine alt bewährte Art und Weise, sich dem Kern einer Sache anzunähern, ist der Vergleich. Ein Vergleich zwischen dem Internet und anderen Kommunikationsstrukturen wird möglich, wenn man den Gegenstandsbereich um eine Abstraktionsebene anhebt und sich anschaut, wie denn eigentlich andere internationale oder globale Kommunikationsstrukturen verwaltet werden (Hofmann 2005b).

In einem ersten Zugriff lassen sich Post und Telefon als vergleichbare Kommunikationsinfrastrukturen identifizieren. Wie das Internet zielen Post und Telefon auf eine globale Verfügbarkeit; sie beruhen mithin auf transnationalen Infrastrukturen und können aus diesem Grund kaum national verwaltet werden. Charakteristisch für Post und Telefon ist daher ihre frühe völkerrechtliche Einbettung. Für beide Kommunikationsinfrastrukturen wurden UN-Sonderorganisationen gegründet, so dass man von

1 Die zugehörigen Ausführungen beruhen auf einem Paper, das ich im Sommer 2014 mit zwei KollegInnen verfasst habe (Hofmann et al. 2014).

multilateralen Regimen in diesen Kommunikationssektoren sprechen kann. Vor allem nach dem Zweiten Weltkrieg galten internationale Organisationen als angemessene Form, um solches transnationales Handeln zu strukturieren und durch Transparenz berechenbar zu machen. Entsprechend konstituiert der Weltpostvertrag ein globales Postgebiet und in vergleichbarer Weise strukturieren internationale Verträge und allgemein anerkannte technische Standards das globale Telefonsystem (Alleyne 1995).

Im Unterschied dazu zeichnet sich das Internet bislang durch das Fehlen einer solchen Einbettung in die UN-Organisationsstruktur aus. Das Internet entstand vielmehr in Konkurrenz zu multilateralen Bemühungen um ein gemeinsames internationales Datennetz. Materiell ist das Internet aus der Vernetzung von Computern hervorgegangen. Die daran beteiligten Informatiker grenzten sich technisch, kulturell, aber auch politisch von der Tradition der Telefonie ab. Zeitweilig bestand geradezu eine Antipathie zwischen den jeweiligen Professionskulturen und ihren institutionellen Handlungskontexten (technische Standardsetzung, Marktstrukturen und Geschäftsmodelle, (vgl. zu dieser Frühphase auch Mueller 2002: 73–104).

Bis zu ihrer Privatisierung waren Post und Telefon auch auf nationalstaatlicher Ebene als staatliche Universal- bzw. Monopoldienste organisiert. Das heißt, staatliche Behörden entschieden über die Nutzungsbedingungen und -formen der Netzinfrastruktur. Die Nutzung von Modems beispielsweise erforderte noch in den 1980er Jahren eine Zulassung der Post. Im Unterschied zu den zentral gesteuerten Telefonnetzen bot das Internet bis vor wenigen Jahren gar nicht die Möglichkeit, die Nutzung von Anwendungen zu kontrollieren. Das Internet wurde vielmehr als Netz von Netzen konzipiert, dessen Kontrolle allein an den Endpunkten liegen sollte. Hinzukommt, dass das Internet durch offene, nicht-proprietäre Standards konstituiert wird. Die offenen Standards stellten sicher, dass Eigentumsrechte nicht als Vetoinstanz für neue Dienste und andere Angebote eingesetzt werden können. Ein gutes Beispiel ist Skype. Erst im mobilen Internet ist es Internet Service Providern gelungen, diese Konkurrenz zur bezahlten Telefonie zu blockieren. Lange Zeit galt, dass die dezentrale Architektur und die offenen Standards die Innovationsfreiheit des Internets sicherstellen.

Aufgrund der unterschiedlichen regulatorischen Traditionen war es den Vätern des Internets – Mütter sind nicht bekannt – zudem wichtig, dass das Internet nicht von einer UN-Organisation koordiniert wird. Unklar war und ist dagegen, wie und von wem das Internet stattdessen verwaltet werden soll. Uneinigkeit besteht ferner darüber, in welchem Umfang gemeinsame Regeln für die Entwicklung des Internets erforderlich sind. Diese beiden offenen Fragen stehen seit rund 20 Jahren im Zentrum der Diskussion über Internet Governance. Es geht also gleichermaßen um Prinzipien (zentral versus dezentral, privatwirtschaftlich versus demokratisch bzw. partizipationsorientiert) als auch um konkrete Regelungsbereiche, ihre Akteure und Regelungsinhalte (Hofmann 2007a; Mueller 2010). Traditionell bezieht sich der Begriff Internet Governance auf die Regulierung der globalen Netzinfrastruktur, praktisch findet er inzwischen aber auch auf nationale Aspekte Anwendung.

Die Privatisierung von Post und Telefon haben die Governance-Frage von Kommunikationsinfrastrukturen auf nationaler Ebene auf den Plan gerufen. Auf internationaler Ebene ist bis heute die Internationale Fernmeldeunion (ITU) die zentrale Koordinationsinstanz. Das Internet wurde dagegen Anfang der 1990er Jahre für die private Nutzung freigegeben, ohne dass Regulierungsbedarfe oder nationale und internationale Regulierungskompetenzen definiert worden wären. Die Internet-Governance-Frage stellte sich das erste Mal Mitte der 1990er Jahre. Der Anlass dafür bestand in einem Konflikt, der aus dem tiefgreifenden Funktionswandel des Domainnamensystems (DNS) entstand. Heute kann man sich kaum mehr vorstellen, dass das Domainnamensystem mal eine viel simplere Rolle gespielt hat als heute. Das DNS wurde ursprünglich geschaffen, um das Einprägen der vergleichsweise langen numerischen Internetadressen zu umgehen. Domainnamen waren einfach als Platzhalter für das internetspezifische Äquivalent zur Telefonnummer gedacht (Hofmann 2003).

Bis Anfang der 1990er-Jahre war das Internet ein Wissenschaftsnetz, dessen Nutzung überwiegend Forschungseinrichtungen vorbehalten war. Die Entwickler des DNS gingen davon aus, dass wissenschaftliche Organisationen ihren jeweiligen Namen als Domainnamen wählen würden. Sie gingen nicht davon aus, dass Domainnamen nicht nur Organisationen, sondern irgendwann auch beliebige Objekte bezeichnen könnten und somit der Bedarf nach Domainnamen erheblich zunehmen würde. Das lag unter anderem daran, dass das DNS vor dem WorldWideWeb etabliert wurde. Erst mit dem WWW entstand der Dienst, der die Vernetzung von Informationsressourcen im Internet realisierte und damit erhebliche Anreize zur Registrierung von Domainnamen zwecks besserer Auffindbarkeit solcher Ressourcen schuf – bevor Suchmaschinen ihre heutige Qualität erreichten, waren Domainnamen wichtig, um Informationen und Organisationen im Internet zu orten. Ebenso wenig gingen die Entwickler des DNS davon aus, dass Unternehmen das Internet als Handelsplatz und einprägsame Domainnamen als Asset, vergleichbar mit der guten Adresse in der Innenstadt, entdecken und für sich reklamieren würden. Aufgrund des spezifisch akademischen Entstehungskontextes des DNS wurden rechtliche Konflikte nicht vorhergesehen und tatsächlich keine verbindlichen Nutzungsregeln festgelegt.

Mitte der 1990er Jahre kam es zu ersten gerichtlichen Auseinandersetzungen um die Nutzungsrechte an Domainnamen. Zur Debatte stand, ob das Markenrecht auf das Domainnamensystem anzuwenden ist und ob Unternehmen wie McDonalds Ansprüche auf entsprechende Domainnamen haben oder nicht (vgl. Mueller 2002: Kap. 6). Solche Fragen konnten nicht auf Dauer Gerichten überantwortet werden; sie warfen vielmehr den Bedarf nach allgemeinen Regeln mit einer internetweiten Geltung auf. Die Diskussion über die Vergabe von Domainnamen bildete empirisch den Beginn von Internet Governance im Sinne einer transnationalen Regulierung der Internetinfrastruktur (Bendrath et al. 2008).

Die Elemente der Netzinfrastruktur, die einer netzweiten Regelung bedürfen, werden als Critical Internet Resources bezeichnet. Dazu zählen neben dem DNS vor allem

das Adressierungssystem (IP-Adressen, derzeit IPv4 und IPv6) und einige weitere technische Parameter. Für Domainnamen und IP-Adressen gilt, dass beide, Namen und Nummern, jeweils nur einmal vergeben werden dürfen. Entsprechend werden globale Vergaberegeln benötigt, die eine Doppelnutzung ausschließen. Die kritischen Internetressourcen entstanden im Rahmen eines experimentellen Entwicklungszusammenhangs, in dem technische Funktionalität wie etwa Skalierbarkeit eine große, legitime Entscheidungsverfahren dagegen eine eher kleine Rolle spielten. Der praktische Betrieb des Internets schuf Konflikte, deren Lösung dann nach und nach Regulierungsmaßnahmen erforderlich machten. Den Prozess zum heutigen institutionellen Rahmen von Internet Governance habe ich an anderer Stelle als einen kollektiven Suchprozess beschrieben (Hofmann 2007a). Es ging und geht darum, legitime Lösungen jenseits des UN-Modells zu finden, die auch im internationalen Maßstab akzeptabel und als legitim anerkannt sind. Für die Entwicklung von Internet Governance gibt es sehr wenige Vorbilder, auf die sich die beteiligten Akteure stützen können. Insofern kommt einem der Wandel dieses Feldes manchmal wie eine Art Blindflug vor.

2.2 Etappen und Akteure der Internet Governance-Entwicklung

Dieser Abschnitt nimmt die Organisationsentwicklung von Internet Governance in den Blick. Eigentlich könnte man zu jeder einzelnen Etappe in diesem Prozess eine eigene Geschichte erzählen. Zu den ersten und bis heute wichtigsten Organisationen gehört die Internet Assigned Numbers Authority (IANA). Ursprünglich handelte es sich bei dieser Autorität um eine Person: Jon Postel gehörte zur ersten Generation der Internetentwickler. Er gilt als der maßgebliche Entwickler des DNS. Zugleich hat er eine Registrarrolle für die kritischen Internet-Ressourcen übernommen. Dazu gehörten die Vergabe von Internetadressen und die Allokation von Top Level Domains, der obersten Ebene des DNS (.com, .de etc.). Jon Postel hat die Funktion der Numbers Authority übernommen, ohne dafür gewählt oder nominiert worden zu sein. Erst mit den Konflikten um einzelne Domainnamen und die Frage, wer über die Einrichtung zusätzlicher Top Level Domains entscheiden soll, wurde IANA als Kompetenz und Prozess allmählich politisiert. In der Folge – das kann Politologen kaum verwundern – setzte ein Verregelungs- und Institutionalisierungsprozess ein, der bis heute nicht abgeschlossen ist (Hofmann 2005b). Heute unterliegen die sogenannten IANA-Funktionen der politischen Aufsicht der US-Regierung und bilden eine Abteilung der Internet Corporation for Assigned Names and Numbers (ICANN), auf die ich gleich noch zu sprechen komme. Aktuell wird in Internet-Governance-Kreisen über eine vollständige Beendigung der US Aufsicht verhandelt (vgl. den Beitrag von Milton Mueller in diesem Band).

Parallel zu IANA entwickelte sich die Internet Engineering Task Force (IETF), die wichtigste Standardisierungsorganisation für das Internet. In den 1990er Jahren erschien mir die IETF wie eine verfassungsgebende Versammlung für das Internet, weil die technischen Standards in hohem Maße unsere Kommunikationsbedingungen prä-

gen. Faszinierend daran ist, dass die IETF im Unterschied zu manch anderen Standardisierungsorganisationen nicht formal inkorporiert ist. Die IETF ist eine offene Organisation, an der sich jede/r beteiligen kann. Die IETF sieht sich selbst als Meritokratie. Tonangebende Stimmen in der IETF sind die, die technische Expertise und Arbeitszeit einbringen und sich engagieren. Zunächst waren es überwiegend Akademiker, die an Hochschulen arbeiten. Heute sind es mehrheitlich Unternehmen, die die technische Entwicklung des Internets finanzieren und bestimmen. Gleichwohl hält die IETF an dem Prinzip fest, dass die individuelle Stimme und nicht der Geldgeber den Ausschlag in der Entwicklung technischer Lösungen gibt. Die als Protokolle bezeichneten Standards der IETF haben den Charakter von Empfehlungen. Letztlich ist es der Markt, der entscheidet, ob sich ein Standard durchsetzt oder nicht. Charakteristisch für die technische Entwicklung des Internets ist, dass es keine Autorität gibt, die technische Lösungen verbindlich vorschreiben kann. Das hat allerdings auch seine Schattenseiten. Ein Beispiel dafür ist der missglückte Übergang auf ein neues Addressierungssystem mit einem größeren Adressenpool (vgl. Hofmann 2010). Auch die Durchsetzung eines Authentifizierungsstandards für E-Mails ist vorläufig konkurrierenden Ansätzen zum Opfer gefallen (vgl. Ermert et al. 2004).

Später als IANA und IETF wurde 1998 die Internet Corporation for Assigned Names and Numbers (ICANN) gegründet und von der US-Regierung beauftragt, die Konflikte über das Domainnamensystem unter Beteiligung aller betroffenen Gruppen im Rahmen eines Bottom-up-Verfahrens zu lösen. Für eine Interimsperiode von einigen Jahren setzte sich die US-Regierung selbst als Aufsichtsinstanz über das privatwirtschaftlich konzipierte Regime ein. ICANN hat ein vertragsbasiertes Regime etabliert, das sich über alle Betreiber der sogenannten generischen Top Level Domains und der Registrare erstreckt. Je länger ICANN existiert, desto komplexer werden die Fragen, mit denen sich die Organisation unter Einbeziehung unterschiedlicher politischer Kulturen und wirtschaftlicher Interessen befassen muss. Vor allem die Schaffung neuer Top Level Domains ruft viele Kontroversen hervor, über die sich nur schwer Einvernehmen erzielen lässt. Parallel dazu ist ICANN bis heute damit beschäftigt, die Legitimität, Repräsentativität und Zurechenbarkeit seiner Strukturen sicherzustellen. Wie eingangs schon erwähnt, gibt es für privatwirtschaftliche Formen der transnationalen Regulierung keine Vorbilder, auf die Internet-Governance-Organisationen zurückgreifen können.

Als vorerst letzte Etappe in der institutionellen Entwicklung von Internet Governance wird hier die Gründung des Internet Governance Forum (IGF) analysiert. Dieses Forum ging aus dem UN World Summit on Information Society (WSIS) hervor. Die UN veranstaltete diesen Gipfel zwischen 2002 und 2005. Sein ursprüngliches Ziel war es, das Problem der digital divide, also des abgehängten globalen Südens in der Internetentwicklung zu thematisieren und, wenn möglich, Investitionen aus dem globalen Norden in den Süden zu initiieren. Praktisch hat sich der Vorbereitungsprozess des Gipfels dann zu einem internationalen Forum über die Zukunft von Internet Governance entwickelt. Der WSIS war die erste multilaterale Konferenz, bei der sich Regierungen de-

tailliert mit der Frage befasst haben, wie das Internet in Zukunft reguliert werden soll. Wie zu erwarten, gingen die politischen Vorstellungen weit auseinander. Viele G77-Länder argumentierten dafür, das Internet einer UN-Organisation zu unterstellen. Die USA und einige andere Länder verteidigten dagegen das bestehende privatwirtschaftliche Regime. Da auch nach drei Jahren Gipfelprozess keine Einigung in Sicht war, wurde das Problem kurzerhand prozeduralisiert. Das Abschlussdokument von WSIS, die Tunis Agenda, skizziert die Einrichtung des IGF, einer neuen Institution, die den Dialog über Internet Governance auf Dauer stellt (Hofmann et al. 2014).

2.3 Der Multistakeholder-Ansatz

Als Ergebnis von WSIS und der Gründung des IGF verändert sich die Zusammensetzung der Akteure im Feld von Internet Governance – ein Umstand, der sich auch sprachlich niederschlägt. So migriert der Begriff „Multistakeholderprozess“ im Zuge von WSIS in die Regulierung des Internets. Das Konzept existierte zwar schon seit einigen Jahren, aber mit dem Internet verknüpft wurde es erst durch den World Summit on Information Society. Während man bis 2005 noch von „private sector-led“ Bottom-up-Prozessen sprach, hat sich der Multistakeholder-Begriff seither zu einer Art neuem Branding entwickelt, das als legitimationssteigernd gilt. Selbst die ITU hat den Begriff inzwischen adaptiert (ITU 2013).

Der Stakeholder-Begriff selbst kommt aus der Managementliteratur. Die Literatur zu Corporate Social Responsibility wiederum, die das Handeln von Unternehmen unter normativen und politischen Gesichtspunkten thematisiert, hat das Stakeholder-Konzept erweitert. Aus dem „Stakeholder“ wird in dem Moment ein „Multistakeholder“, in dem Unternehmen als ein Akteur unter mehreren betrachtet werden. Es steht nicht mehr das einzelne Unternehmen im Zentrum der Betrachtung, sondern das jeweilige Problem oder *issue*. Aus dem Stakeholderbegriff gehen so Multistakeholder-Prozesse hervor. Unternehmen sind darin zwar wesentliche Akteure, aber im Mittelpunkt steht das politisch-normative Problem. Alle Akteure, die einen „Stake haben“, sollen ihre Anliegen artikulieren können. Auf der internationalen Ebene finden Multistakeholder-Prozesse vor allem im Umweltbereich, aber auch bei der Aushandlung von Arbeitsverhältnissen statt. Zumeist sind sie projektbezogen und outputorientiert. Das IGF dürfte der erste Fall sein, der einen eigenen längerfristig angelegten Organisationsstatus besitzt, auf der anderen Seite jedoch rein dialogisch angelegt ist und nicht auf einen konkreten Output hin arbeitet (Malcom 2008; Kleinwächter 2010).

Hinter „Multistakeholder“ schart sich heute die Mehrheit der Internet-Governance-Community. Denn es ist geradezu die Grundbedingung, um dort mitzumachen und ernstgenommen zu werden, sich dem Multistakeholder-Begriff und seinen Annahmen zu verschreiben. Wer das nicht akzeptiert und sagt, er möchte einen multilateralen Prozess, marginalisiert sich selbst. Das ist eine der Grenzziehungen dieser Community:

Man darf der Praxis des Multistakeholder-Prozesses kritisch gegenüberstehen, aber grundlegend ablehnen darf man ihn nicht (Doria 2013).

Die Leitidee von Multistakeholder-Prozessen lautet: Verhandeln auf Augenhöhe. Regierungen, Wirtschaft, Zivilgesellschaft und die technische Community begegnen sich und versuchen Konsens zu strittigen Fragen herzustellen. Das geschieht unter Bedingungen, die so transparent sind, dass auch Leute, die nicht vor Ort sind, dem Dialog folgen und sich beteiligen können. Es wird also sehr viel Wert auf Partizipation gelegt. Bei Netmundial etwa ist die globale Partizipation geradezu zelebriert worden (Kleinwächter 2014). Es wurden lokale Communities von nahezu allen Kontinenten eingeblendet. Im großen Konferenzsaal konnte man sehen, wie sie die ganze Nacht aufblieben wegen der Zeitverschiebung, der Diskussion in Sao Paulo folgten, sich beteiligten und ihre Statements vorlasen. Diese Möglichkeiten zur remote participation sowie das Archivieren der Transkripte zum Nachlesen der Diskussionen zeigen, dass Verfahrensfragen in Multistakeholder-Prozessen sehr, sehr wichtig sind.

Das wichtigste Beispiel hierfür ist das Internet Governance Forum. Es ist sozusagen die Krönung des Multistakeholder-Prozesses. In der Tunis Agenda, dem Abschlussdokument des UN World Summit on Information Society steht, was das IGF tun soll und was es nicht tun soll. Das wichtigste Merkmal ist seine dialogbezogene Rolle. Es besitzt keinerlei Entscheidungsautorität und die kann es freilich unter den Bedingungen eines offenen Prozesses auch nicht haben. Noch wichtiger scheint mir die Feststellung – wenngleich sie durchaus kontrovers sein dürfte –, dass das Internet Governance Forum faktisch keinen Output produziert. Der einzige formale Output, den es gibt, ist der Chairman's Report, der versucht, so neutral wie möglich am Ende zusammenzufassen, worüber bei den jährlichen Treffen gesprochen wurde. Vielen Teilnehmern reicht das nicht aus (zu dieser wiederkehrenden Debatte: vgl. schon Mueller 2010: 120). Allerdings weiß ich aus Hintergrundgesprächen und eigener Erfahrungen, dass die bestehende Regelung ihre Vorzüge hat, schon weil multilaterale Prozesse häufig alle Aufmerksamkeit auf die Verhandlung von Formulierungen legen. Nach Meinung vieler Beobachter kann der Stein der Weisen nicht darin liegen, über Monate und Jahre Texte zu verhandeln.

Das IGF selbst begann 2006 in Athen mit einigen hundert Teilnehmern. In diesem Jahr (2014) waren es schon 2400. Das IGF wächst stetig, nicht nur während seiner Jahreskonferenzen, sondern auch im Rahmen seiner regionalen Abkömmlinge. Jetzt steht gerade das ostafrikanische IGF bevor, es gibt ein europäisches IGF, aber auch nationale IGFs. Sie alle drehen sich – und darin lässt sich eine gewisse Beschränkung erblicken – allein um Fragen der globalen Internet Governance (Epstein 2013). Ich denke allerdings, eine größere Wirkung wird das Multistakeholder-Modell erst dann erzielen, wenn es einen größeren Schwerpunkt auf die nationalen oder regionalen Themen legt, die von politischer Relevanz für das Internet sind und die relevanten Regierungsvertreter lokalen Öffentlichkeiten Rede und Antwort stehen müssen.

Was leistet das IGF nun tatsächlich? Seine unmittelbare Wirkung besteht in der Konstitution einer globalen Öffentlichkeit für einen begrenzten Zeitraum. Jeder, der sich für Fragen um Internet Governance interessiert, wird feststellen, dass in den Wochen, bevor das IGF stattfindet, und auch währenddessen viele Tausende Leute das Geschehen verfolgen und dort miteinander disputieren. Solche Entwicklungen sieht man in anderen Politikbereichen natürlich auch. Das muss allen denen, die sagen, Demokratie kann nur national funktionieren, weil man zum Beispiel unterschiedliche Sprachen spricht, schon zu denken geben. Das IGF zeigt, dass es tatsächlich möglich ist, über viele Jahre eine Institutionsentwicklung zu betreiben, deren womöglich wichtigstes Ergebnis darin besteht, eine gemeinsame Sprache sowie gemeinsame Problemsichten auf gewisse Sachverhalte und Gegenstandsbereiche zu entwickeln. Das ist sicher ein mühsamer Prozess, aber trotzdem kann man, denke ich, wenn man sich das über mehrere Jahre anschaut, sehen, dass hier etwas Neues, etwas qualitativ Neues im Bereich transnationaler Regulierung entsteht (Balleste 2015: 91–128).

3 Zur Konzeptualisierung von Internet Governance

Im Folgenden soll der Fokus von der Beschreibung der Prozesse und Organisationsformen von Internet Governance zu konzeptionellen Fragen übergehen. Im Mittelpunkt steht hier die Frage, wie Internet Governance untersucht werden kann und soll.

Der Governance-Begriff – das wird auch in der Literatur zu Internet Governance deutlich – wird sehr unterschiedlich gebraucht (Hofmann et al. 2014). Man kann sehen, dass in der amerikanischen Literatur andere Interpretationen oder Nutzungsweisen des Begriffs vorherrschen als in der europäischen und vor allem in der deutschen Literatur. So lässt sich etwa auch in Europa erkennen, dass der britische Sprachgebrauch vom deutschen ganz klar abweicht. In der anglo-amerikanischen Literatur ist über lange Zeit Governance mit Government gleichgesetzt worden. Erst in den späten 1980er und frühen 1990er Jahren problematisieren erste Autoren diese Gleichsetzung und weisen darauf hin, dass es Regulierungsformen und Ordnungsweisen gibt, in denen die Regierung nicht der einzige Player ist. Dieses Phänomen ist natürlich vorher auch schon beobachtet worden, aber Autoren wie Rosenau und Czempiel (1992) greifen es nun politikwissenschaftlich im Kontext des Governance-Begriffs auf und generalisieren ihre Beobachtungen. Dennoch wird vor allem im US-amerikanischen Kontext bis heute Governance ganz häufig mit Regierungen mehr oder weniger gleichgesetzt. Interessanterweise ist das in der deutschen Entwicklung vollkommen anders. Wir haben uns in der deutschsprachigen Literatur diesem Begriff in einer viel – man könnte fast sagen – schmerzhafteren Weise angenähert; ein Schmerz, der eigentlich bis heute anhält, weil nach wie vor viel publiziert wird zu der Frage, was Governance genau bezeichnet und das Konzept von Begriffen wie Steuerung und Regulierung unterscheidet (Hofmann 2007a). Die Entwicklung in der deutschen Literatur zum Governance-Begriff hat Renate Mayntz (2009) treffend auf den Punkt gebracht. Sie erklärt es in einem Dreischritt. Po-

litische Prozesse wurden in den 1950er und 60er Jahren überwiegend als Planungsprozess verstanden. Der Staat plant, dann verkündet er was zu tun ist, und alle folgen der Planung. Die Vergangenheitsform soll nicht zum Ausdruck bringen, dass Planung nicht mehr stattfindet. Natürlich plant der Staat immer noch. Er tut das in der Stadtplanung, in der Raumplanung und anderswo. Aber der Planungsbegriff als dominantes Bild dafür, wie Politik praktisch funktioniert, kam in den 1970er Jahren weitgehend aus der Mode. Das geschah bis zu einem Grad, dass von Planung, zumindest in der politikwissenschaftlichen Literatur, heute kaum noch die Rede ist. Danach ersetzte die Idee der Steuerung den Planungsbegriff. Der Staat agiert hier immer noch als die zentrale Instanz. Politik geht vom Staat aus. Es handelt sich hierbei immer noch um eine sehr hierarchische Praxis, die aber Interaktionen, mit den Regelungssubjekten, berücksichtigt.

Erst in den 1990er Jahren verliert auch der Steuerungsbegriff allmählich seinen Reiz. Wir finden ihn trotzdem immer noch vor; Politik wird von vielen Forschern immer noch als Steuerungsprozess verstanden – ungeachtet des Umstands, dass davon in der Realität gar nicht so viel zu sehen ist. Demgegenüber öffnet sich der Governance-Begriff konzeptionell in einem solchen Umfang, dass Aktivitäten, Prozesse und Akteure, die vorher gar nicht als politisch wahrgenommen wurden, plötzlich ins Scheinwerferlicht des politischen Prozesses treten. Diese im Vergleich zum Steuerungsbegriff große Öffnung, auch für nicht demokratisch legitimierte Akteure und ihre Interaktionsformen, hat jedoch ihren Preis: Der Governance-Begriff schließt nun als politische Interventionen viele Akteure und Praktiken mit ein, wird aber darüber selbst so vage, dass der Begriff grenzen- und uferlos wirkt. Wenn Governance alle Akteure und alle Formen der Absprache, der Kooperation und Regelbildung einschließt, was ist dann eigentlich nicht Governance? Deshalb drehte sich die deutsche Diskussion – und tut es noch bis heute – um die Frage: Was ist Governance und was ist nicht Governance? Wie soll man den Governance-Begriff eigentlich fassen (Hofmann et al. 2014)?

Die pragmatische Lösung, die sehr viele deutsche Politikwissenschaftler für sich gewählt haben, ist Governance einfach mit Regulierung gleichzusetzen. Das scheint mir derzeit die dominante Interpretation in der deutschen Literatur zu sein. Governance entspricht hier Regulierung; womit man – durch die Hintertür – den Steuerungsbegriff doch irgendwie rettet. Das, was den Regulierungsbegriff im Kern definiert, ist intentionales Handeln eines autoritativen Akteurs. Selbst wenn man private Regulierung miteinbezieht, bleibt doch häufig die Annahme, dass es der Staat ist, der reguliert. Wir – und damit meine ich die Forscherinnen und Forscher am Humboldt Institut für Internet und Gesellschaft (HIIG) – sind mit dieser Lösung unglücklich gewesen. Wir sind der Auffassung, dass der Regulierungsbegriff sehr viele Prozesse, die enorm wichtig für die Entwicklung von Internet Governance sind, nicht erfasst. Das wesentliche Argument, das wir in diesem Zusammenhang vorbringen, lautet, dass alle komplexen Strukturen, die man nicht auf intentionales Handeln zurückführen kann, mit einem solch engen Governance-Begriff nicht verstanden werden. Wenn man Governance als Regulierung interpretiert, kann man die Entstehung des IGF, ja eigentlich die Entwicklung des ge-

samten Internet-Governance-Institutionengefüges nicht nachvollziehen, weil es hier eben kein intendiertes Regulieren gibt. Natürlich handeln auch Internet-Governance-Akteure intentional, aber ihre Absichten sind in vielen Fällen nicht darauf gerichtet gewesen, eine Institutionenarchitektur aufzubauen, um das Internet zu verwalten. Es kommen, im Gegenteil, sehr viele Intentionen zum Einsatz, die womöglich auf etwas ganz anderes zielen und stattdessen im Nebeneffekt ordnungsbildend gewirkt haben. Das, was ich an der Internet-Governance-Institutionenstruktur aufgezeigt habe, ist von niemandem in dieser Form intendiert gewesen. Das Schema dieser Entwicklung ist eher der Effekt eines kollektiven Handelns, der jede Art der Intention deutlich überschreitet. Für Internet Governance, wie vermutlich für sehr viele Politikbereiche, entfaltet der nichtintendierte Nebeneffekt eine stark ordnungsbildende Entwicklung und Kraft. Es braucht auch deshalb, aus unserer Sicht, einen Governance-Begriff der nichtintendierte Effekte miteinschließt.

Die Frage ist, wie man das konzeptionell realisiert. Wie ist es möglich einen Governancebegriff zu konstruieren, der nicht so eng ausfällt, dass er auf Steuerung und Regulierung reduziert wird, aber umgekehrt nicht so umfassend ist, dass alles zu Governance wird? Wie viele Forscher vor uns auch schon, haben wir uns über viele Monate über diese Frage die Haare gerauft und sind dann zu dem Vorschlag gekommen, Governance als eine spezifische Form von Koordination zu verstehen. Ein wichtiges Element dabei ist, dass wir unseren Governance-Begriff in alltäglichen Koordinationsweisen einbetten (siehe Beispiel im nächsten Abschnitt). Governance beginnt aus unserer Sicht dann, wenn etablierte Koordinationsformen an ihre Grenzen kommen und problematisch werden.

Ein Beispiel mag diesen Zusammenhang verdeutlichen: Ein Jeder kennt diese Situation: Schmale Straße; ein Auto fährt in die eine Richtung und ein Auto kommt aus der anderen Richtung. Was macht man? In dem Moment beginnt für uns Reflexion und Koordination. Etablierte Koordinationsformen funktionieren nicht mehr, die Akteure müssen sich darüber verständigen, wie sie sich koordinieren können. Das ist die zentrale Idee. Und die Momente, wo das passiert, bezeichnen wir, im Anschluss an Luc Boltanski und Laurent Thevenot (2006) als *critical moments*. In dem Moment, wo sich zwei Autos in einer schmalen Straße begegnen, fängt jeder an zu mobilisieren. Gerechtigkeitsvorstellungen mögen dabei eine Rolle spielen, im Sinne von: „Ich bin als erste/r in die Straße gefahren." Ebenso können Machtvorstellungen in Anschlag gebracht werden wie: „Mein Auto ist das größere." Alle möglichen Vorstellungen können hier angeführt werden. Wir denken, dass es aus politikwissenschaftlicher Sicht diese *critical moments* sind, in denen Koordination nicht mehr funktioniert und selbst koordinationsbedürftig wird, die man als Governance bezeichnen sollte. Es sind diese Momente, die wirklich untersuchenswert sind, weil hier so viel politikwissenschaftlich Relevantes zutage tritt, gewissermaßen neu verhandelt, daher sichtbar und relevant wird. Relevant also in dem Sinne, dass critical moments uns etwas sagen über das zugrundeliegende Governance-Arrangement: Welche moralischen Vorstellungen in der Situation

anzuwenden sind, was als Normalfall zu gelten hat, wie sich der Normallfall zu der ungewöhnlichen neuen Situation verhält; welche Ressourcen zum Einsatz gebracht werden – in critical moments werden diese Fragen im Rahmen von Governance-Strukturen neu ausgehandelt. Daran zeigt sich auch, dass unser Governance-Begriff ein temporärer ist. Governance findet also möglicherweise nicht die ganze Zeit statt. Wenn ein Vorfahrtsschild das Problem auf dieser Straße löst, dann haben wir es wieder mit einer alltäglichen unproblematischen Koordinationsform zu tun.

Das heißt, aus unserer Sicht findet Governance dann statt, wenn Koordination zum Problem wird. Dann haben wir eine Governance-Situation. Koordination verstehen wir als reziproke soziale Prozesse. Das Erfolgskriterium dabei ist, dass man sich wechselseitig versteht. Eine einfache Form der Koordination ist Sprache. Wir verstehen uns, weil wir die gleiche Sprache sprechen. Aber schon in dem Moment, in dem wir aus unterschiedlichen wissenschaftlichen Disziplinen kommen, stellen wir fest, dass wir gleiche Begriffe mit unterschiedlichen Bedeutungen belegen. Schon dann wird Verständigung koordinationsbedürftig. Wir müssen bereits hier Regelungen finden, um die Bedeutung von Begriffen miteinander abzustimmen.

Governance und Regulierung sind aus unserer Sicht also Teilmengen oder Formen von Koordinationshandlungen. Bei Governance liegt der Fokus ganz klar auf Prozessen – es gibt häufig keine ex-ante-Ziele. Regulierung dagegen verstehen wir als einen intentionalen Prozess, bei dem es ein Ziel und ein klares Erfolgskriterium gibt: Erreicht etwa Förderungsprogramm xy sein Ziel? Ein wesentliches Element von Governance-Prozessen ist, dass diese Art von Erfolgskriterien, häufig nicht vorliegen, weil Zielsetzungen wiederum Zwischenschritte oder Bestandteil eines Prozesses sind. Das lässt sich in Internet-Governance-Prozessen beobachten. Die Prozesse mäandern vor sich hin: Ziele werden reinterpretiert, angepasst und neu formuliert. Ein Ziel, auf das alle hinsteuern, zu formulieren, ist in diesem Sinne Teil und Erfolgsindikator des Prozesses. So beschreiben und verstehen wir Governance als Prozess.

4 Synthese: Die critical moments von Internet Governance

Wozu aber dienen die vorangegangenen Ausführungen zur Governance-Exegese? Wir denken, dass unser Governance-Begriff es besser erlaubt, Internet-Governance-Prozesse, wie ich sie im ersten Teil dieses Beitrages beschrieben habe, zu beleuchten und ihre besonderen Charakteristika auf transnationaler Ebene herauszuarbeiten.

Ein wichtiges Merkmal für dieses Politikfeld ist, dass sich nur bei wenigen Internet Governance-Organisationen klare Zielsetzungen finden. Das Internet Governance Forum hatte ursprünglich das Ziel, den Konflikt um die Zuständigkeiten bei der Verwaltung der *critical internet resources* zu lösen. Dieses ursprüngliche Ziel ist mehr oder weniger komplett verloren gegangen. Das Programm und die Themen, die das IGF verhandelt, sind heute sehr viel breiter und vielfältiger. Es haben sich inzwischen viele andere Themen um die einst zentrale Frage der Verwaltung der kritischen Internet

Ressourcen gruppiert. Wenn es zurzeit überhaupt so etwas wie ein gemeinsames Ziel gibt, dann besteht es darin, das Internet Governance Forum selbst zu erhalten. Denn es hat jeweils nur ein fünfjähriges Mandat, das von der UN immer wieder bestätigt werden muss. Ende 2015 steht wieder eine Mandatsverlängerung bevor. Sofern ein solch breiter Prozess, der so viele verschiedene Akteure einbindet, überhaupt eine klare Zielsetzung formulieren kann, strebt das IGF also vornehmlich nach institutioneller Fortexistenz, aber darüber hinaus sind keine über das Mandat des IGF hinausreichenden Ziele zu erkennen. Diese starke Prozessorientierung ist ein Phänomen, das der Regulierungsbegriff nicht angemessen beschreiben kann.

Sehr wichtig erscheinen mir in diesem Zusammenhang *critical moments,* in denen routineförmige institutionalisierte Koordinationsprozesse, plötzlich problematisch werden. Im Bereich Internet Governance passiert dies häufig. Zudem werden die wenigen klar formulierten Ziele, die sich vor allem in der Verwaltung des Domainnamensystems durch ICANN finden, häufig nicht oder nur mit großer zeitlicher Verzögerung erreicht. Auch hier kann ein Beispiel der Illustration dienen: ICANN hat nahezu 15 Jahre gebraucht, um einen Prozess für die Neueinrichtung von Top Level Domains zu etablieren. Begonnen aber hatte ICANN seine Arbeit als neue Organisation, mit vielen Vorschusslorbeeren versehen, unter dem Vorzeichen „private authority“. ICANN, so die Erwartung, würde so viel schneller, wendiger und fachlich kundiger sein im Umgang mit den kritischen Internetressourcen als eine staatliche oder intergouvernementale Behörde jemals sein könnte. „Private sector“, „industry led“ und „bottom-up“ waren die wichtigen Vokabeln, die die Gründung von ICANN rahmten. Heute zeigt sich, dass ICANN genauso langsam und schwerfällig in der Entwicklung von Policies ist wie jede andere Organisation auch. Zugleich sind aber Integration, Partizipation und Multistakeholder, das heißt die Prozesse eine sehr wichtige Legitimationsquelle geworden. In diesem Sinne bemisst sich der Erfolg von Organisationen wie ICANN oder dem IGF auch an der Zahl der Partizipierenden. Zugespitzt formuliert: Die aktive Partizipation von Akteuren und weniger die konkreten Ergebnisse ihrer Teilnehmer entscheiden über den Erfolg der Organisation. Ich halte es für wichtig, für solche Phänomene wie die starke Prozessorientierung in Internet Governance eine wissenschaftliche Sprache zu finden, die weder beschönigend ist, noch vernichtend. Das soll ein Governance-Begriff, wie wir ihn vorschlagen, leisten.

Weitere critical moments für Internet Governance entstanden im Nachgang der Enthüllungen durch Edward Snowden. Im September 2013 hielt die brasilianische Präsidentin eine eindrückliche Rede vor der UN-Vollversammlung. Frau Rousseff war, wie Frau Merkel auch, von der NSA abgehört worden. Aber anders als die deutsche Bundeskanzlerin war sie darüber so erbost, dass sie sich öffentlich dazu geäußert und über Abhilfe nachgedacht hat. Wörtlich sagte sie:

> „Information and telecommunication technologies cannot be the new battlefield between States. Time is ripe to create the conditions to prevent cyberspace from being used as a weapon of war, through espionage, sabotage, and attacks against systems and infrastructure of other countries. (...)

> For this reason, Brazil will present proposals for the establishment of a civilian multilateral framework for the governance and use of the Internet and to ensure the effective protection of data that travels through the web. We need to create multilateral mechanisms for the worldwide network that are capable ensuring principles such as: 1 - Freedom of expression, privacy of the individual and respect for human rights. 2 - Open, multilateral and democratic governance, carried out with transparency by stimulating collective creativity and the participation of society, Governments and the private sector" (Rousseff 2013).

In Reaktion auf diese Rede hat eine Reihe wichtiger Organisationen, die mit dem Betrieb der Internetinfrastruktur befasst sind, sich kollektiv von der US-Regierung und ihrer Aufsichtsrolle über Teile der Netzinfrastruktur distanziert. Einige Monate später hat die US-Regierung im März 2014 ihre Absicht bekannt gegeben, sich unter bestimmten Bedingungen dauerhaft aus der Aufsicht über die Netzinfastruktur zurückzuziehen (NTIA 2014).

Seither stellt sich erstmals ernsthaft die große Frage der globalen Rechenschaftspflicht von privaten Organisationen wie ICANN im Feld von Internet Governance. Auch wenn die Rolle der US-Regierung häufig als bloß symbolisch beschrieben worden ist, so wird man doch nicht bestreiten können, dass die Präsenz staatlicher Regulierungsautorität einen Einfluss auf die Praxis privater Selbstregulierung hat. Die Reaktion auf die Enthüllungen von Snowden ist insofern auch ein Governance-Prozess, der sich mit der Koordination der Koordination befasst: Wie muss sich das Institutionsgefüge weiterentwickeln, um den Rückzug der US-Regierung in angemessener Weise kompensieren zu können? Das ist seit Ende 2013 das wichtigste Thema in der Internet Governance.

5 Fazit

Von außen betrachtet, wirkt die Entwicklung von Internet Governance wie ein mäandernder Prozess ohne viele Fortschritte. Dies gilt vor allem dann, wenn man Governance-Prozesse mit Regulierungsmaßnahmen gleichsetzt. Wir plädieren nicht zuletzt aus diesem Grund dafür, analytisch zwischen Regulierung und Governance als kategorial verschiedenen Koordinationsformen zu unterscheiden. Regulierungsmaßnahmen, verstanden als intentionale politische Programme mit klar definierten Zielsetzungen sind häufig in abstraktere Governance-Prozesse eingebettet, welche die Frage nach der Koordinierung von Koordination aufwerfen. Diese Metafrage stellt sich im nichtkonstitutionalisierten transnationalen Bereich, in dem verschiedene Akteurskonstellationen kooperieren, vermutlich häufiger und grundlegender als auf der Ebene des Nationalstaates. Noch liegen keine systematischen Vergleiche zwischen Internet Governance und anderen transnationalen Regelungsbereichen vor, die diese Annahme empirisch untermauern könnten. Verallgemeinerbar scheint jedoch über das Beispiel Internet Governance hinaus, dass die institutionellen Architekturen, die sich vor allem seit den 1980er Jahren auf der transnationalen Ebene herausgebildet haben, nicht im Rahmen eines Steuerungsparadigmas erklärt werden können. Im Bereich des Internets wie auch anderer Politikfelder wird darum gerungen, grenzüberschreitend wirksame wie auch legitime Formen der Koordination zu entwickeln. Für die Analyse dieser Pro-

zesse ist ein Begriff von Governance notwendig, der Ordnungsbildung auch jenseits intentionalen Handelns erfassen kann.

Literatur

Alleyne, Mark D. (1995): International Power and International Communication, Macmillan: London.

Balleste, Roy 2015: Internet Governance: Origins, Current Issues, and Future Possibilities, Rowman& Littlefield: Lanham.

Bendrath, Ralf / Hofmann, Jeanette / Leib, Volker / Mayer, Peter / Zürn, Michael (2008): Namensräume, Datenschutz und elektronischer Handel: Die Suche nach Regeln für das Internet, in: Hurrelmann, Achim / Leibfried, Stephan / Martens, Kerstin / Mayer, Peter (Hrsg.): Zerfasert der Nationalstaat? Die Internationalisierung politischer Verantwortung, Campus: Frankfurt, 209–239.

Boltanski, Luc / Thévenot, Laurent (2006): On Justification: Economies of Worth. Princeton University Press: Princeton.

Doria, Avri (2013): Use [and abuse] of multistakeholderism in the internet, in: Radu, Roxana / Chenou, Jean-Marie / Weber, Rolf (Hrsg.): The evolution of global internet governance: Principles and policies in the making, Springer: New York, 115–140.

Ermert, Monika (2011): IPv6-Einführung bleibt hinter den Erwartungen zurück Nachgefragt, in: Magazin für professionelle Informationstechnik 11:2011, 118–119.

Ermert, Monika / Bleich, Holger (2004): Anti-Spam-Standard Sender ID: Zurück auf Start, heise online, 10.09.2004, http://www.heise.de/newsticker/meldung/Anti-Spam-Standard-Sender-ID-Zurueck-auf-Start-104602.html (10.8.2015).

Epstein, Dmitry (2013): Multistakeholderism in praxis: The case of the regional and national IGF initiatives, http://www.internetsociety.org/sites/default/files/RegionalNationalIGFs-ISOC%20-%20Dmitry%20Epstein.pdf (24.07.2015).

Hofmann, Jeanette (2010): Before the Sky Falls Down: A Constitutional Dialogue over the Depletion of Internet Adresses, in Bridget Hutter (Hrsg.): Anticipating Risks and Organizing Risk Regulation, Cambridge University Press: New York, 46–67.

Hofmann, Jeanette (2007a): Internet Governance: A Regulative Idea in Flux, in: Bandamutha, Ravi Kumar Jain (Hrsg.): Internet Governance: An Introduction, The Icfai University Press: Hyderabad, 74–108.

Hofmann, Jeanette (2007b): Wandel von Staatlichkeit in digitalen Namensräumen – Zwischen Hierarchie und Selbstregulierung, Discussion Paper SP III 2007–107, Wissenschaftszentrum Berlin für Sozialforschung, 67.

Hofmann, Jeanette (2005a): Internet Governance. Zwischen staatlicher Autorität und privater Koordination, in: Internationale Politik und Gesellschaft 3, 10–29.

Hofmann, Jeanette (2005b): Internet Governance: Eine regulative Idee auf der Suche nach ihrem Gegenstand, in: Schuppert, Gunnar Folke (Hrsg.): Governance-Forschung: Vergewisserung über Stand und Entwicklungslinien, Bd. 1 der Reihe „Schriften zur Governance-Forschung“, Nomos-Verlag: Baden-Baden, 277–301.

Hofmann, Jeanette (2003): Die Regulierung des Domainnamensystems - Entscheidungsprozess und gesellschaftliche Auswirkungen der Einrichtung neuer Top Level Domains im Internet, Discussion Paper SP III 2003–104, Wissenschaftszentrum Berlin für Sozialforschung.

Hofmann, Jeanette / Katzenbach, Christian / Gollatz, Kirsten (2014): Between Coordination and Regulation: Conceptualizing Governance, in: Internet Governance August 21, 2014, HIIG Discussion Paper Series No. 2014–4, http://ssrn.com/abstract=2484463, http://dx.doi.org/10.2139/ssrn.2484463 (24.07.2015).

International Telecommunication Union (2013): Supporting Multi-stakeholderism in Internet Governance, WTPF Backgrounder Series, http://www.itu.int/en/wtpf-13/Documents/backgrounder-wtpf-13-internet-governance-en.pdf (24.07.2015).

Kleinwächter, Wolfgang (2014): NETMundial: Watershed in Internet Policy-Making? In: Drake, William / Price, Monroe (Hrsg.): Beyond NETmundal: The Roadmap for Institutional Improvements to the Global Internet Governance Ecosystem, 112–121,

http://www.global.asc.upenn.edu/app/uploads/2014/08/BeyondNETmundial_FINAL.pdf (24.07.2015).

Kleinwächter, Wolfgang (2010): Multistakeholderism and the IGF: Lab oratory, clearinghouse, watchdog, in Drake, William (Hrsg.): Internet governance: Creating opportunities for all, United Nations: New York, 76–91.

Malcolm, Jeremy (2008): Multi-stakeholder governance and the Internet Governance Forum, Terminus Press: Perth, Australia.

Mayntz, Renate (2004): Governance Theory als fortentwickelte Steuerungstheorie?, in: Mayntz, Renate: Über Governance. Institutionen und Prozesse politischer Regelung, Schriften aus dem Max-Planck-Institut für Gesellschaftsforschung, Bd. 62, Campus Verlag: Frankfurt am Main, 41–53.

Mueller, Milton L. (2010): Networks and States: The Global Politics of Internet Governance, The MIT Press: Cambridge, Mass.

Mueller, Milton L. (2002): Ruling the Root: Internet Governance and the Taming of Cyberspace, The MIT Press: Cambridge, Mass.

National Telecommunications & Information Administration (2014): NTIA Announces Intent to Transition Key Internet Domain Name Functions, 14.03.2014, http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions (10.08.2015).

Rosenau, James / Czempiel, Enrst-Otto (Hrsg.) (1992): Governance Without Government: Order and Change in World Politics, Cambridge University Press: New York.

Rousseff, Dilma (2013): Statement at the Opening of the General Debate of the 68th Session of the United Nations General Assembly, 24 September 2013, New York, http://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf (10.08.2015).

Autorin

Prof. Dr. Jeanette Hofmann
Direktorin des Alexander von Humboldt Instituts für Internet und Gesellschaft (HIIG)
Oberwallstraße 9
DE-10117 Berlin
jeanette.hofmann@hiig.de

DOI: 10.11588/josar.2015.0.23479

Mehr demokratische Qualität durch das Internet?

Marianne Kneuer

1 Einleitung: Das Internet als Bereicherung oder Stressfaktor für die demokratische Qualität?

Inmitten der Ermüdung, in die das repräsentative Demokratiemodell in den letzten Jahren und Jahrzehnten nach Meinung vieler gekommen ist, erscheint das Internet wie ein Erfrischungselixier, gar als neues Heilmittel, das mindestens zur Revitalisierung, vielleicht sogar zur Erneuerung taugen mag. Insbesondere in Bezug auf die wachsende Forderung nach Mitsprache und Beteiligung wird den digitalen Medien und deren vielfältigen Möglichkeiten der Kommunikation das Potenzial zugeschrieben, die repräsentative Demokratie wiederzubeleben und zu modernisieren.[1]

Das politische, politikwissenschaftliche und mediale Interesse an dem Thema Internet hat insbesondere seit 2011 stark zugenommen, seit sich nämlich auf nationaler wie internationaler Ebene herauskristallisiert hat, wie Bewegungen mit ganz unterschiedlichen Zielsetzungen das Internet sehr effektiv nutzen konnten. Beispiele dafür sind: die Entstehung der Piratenpartei, die mit netzpolitischen Forderungen relativ schnell und erfolgreich in Länderparlamente einziehen konnte; Aufstände in etlichen Ländern der arabischen Welt, die als Facebook- oder Twitter-Revolutionen etikettiert wurden; die Heilsbotschaft einer neuen Transparenz, die durch WikiLeaks verkündet wurde oder die Gesetzgebung zu dem Handelsabkommen ACTA, einem in jahrelanger Abstimmungsarbeit verhandelten internationalen Regelwerk, das innerhalb kürzester Zeit durch eine Welle des transnationalen Protests hinweggefegt wurde.

Es verwundert daher nicht, dass das Internet nicht nur in seiner wirtschaftlichen und zwischenmenschlichen, sondern auch in seiner politischen Dimension als Versprechen empfunden wird. Bereits die Web 1.0-Technologie hatte eine Netzeuphorie ausgelöst, die auf der Hoffnung nach Revitalisierung der Demokratie basierte. Dem Internet wurde demokratisierendes Potenzial zugeschrieben (Hindman 2009: 2–19). Vor allem die Anfang der 1990er Jahre in den USA entwickelten netzoptimistischen Vorstellungen von Nicholas Negroponte, Howard Rheingold oder Alvin Toffler stellten auf Verbesserungen in der politischen Partizipation ab (vgl. Wilhelm 2000; Grunwald et al. 2006), also auf die Ergänzung repräsentativer Verfahren durch direktdemokratische

1 Die netzoptimistische Literatur ist seit den 1990er Jahren zu zahlreich, um hier auch nur annähernd einen Überblick geben zu können. Referenzen für diese Position sind u.a. insbesondere Negroponte 1996, Rheingold 1993, Shirky 2009. Überblicksdarstellungen und Auseinandersetzungen finden sich etwa bei Coleman et al. 2009, Grundwald et al. 2006, Hindman 2009, Kneuer 2013, Wilhelm 2000.

oder gar durch das überwiegende Ersetzen repräsentativer Verfahren durch bürgerliche Selbstregierung. Insgesamt, aber ganz besonders in der letzten Variante, kommt der aktiven und aktivierenden Zivilgesellschaft eine gewichtige Rolle zu. Das Internet solle, so die Mobilisierungsthese etwa von Rheingold vertreten, zu basisdemokratischem politischem Aktivismus führen und den Austausch der Ideen anregen (Rheingold 1993). Das Internet könne ebenfalls die Befähigung des Bürgers fördern, sich auch in großem Umfang an politischen Prozessen zu beteiligen (net empowerment). Der entscheidende Beitrag des Internets aber wurde in der Verwirklichung direkter Entscheidungen auf elektronischem Wege gesehen, also e-voting, e-petitions und e-referenda. Es wurde gar die Vision eines neuen Modells generiert: die *cyberdemocracy*, eine virtuelle *agora* bzw. *ekklesia*, mit der das athenische Ideal der Selbstregierung der Bürger verwirklicht werden könnte.

Der Euphorie über das demokratiestärkende Potenzial des Internets folgten dann nicht nur pessimistische Sichtweisen, sondern auch eine allgemeine Ernüchterung angesichts erster empirischer Befunde. Ein „zweiter Blick" auf die Rolle des Internets (Grunwald et al. 2006: 13) brachte differenziertere Zugänge hervor. Mittlerweile ist aber ein dritter Blick notwendig geworden, denn mit der raschen Verbreitung der Web 2.0-Technologie bekommt die Debatte um die Vitalisierung, Modernisierung oder Reform der repräsentativen Demokratie neue Nahrung: Die Dynamik der technischen Entwicklung (drahtlose Netzwerke, internetfähige Mobiltelefone u.ä., Entwicklung von social software) und die rasche Penetration durch neue Formen der Vernetzung (social media) bringen neue Aspekte hinsichtlich der sich eröffnenden, neuen und umfassenden Möglichkeiten der Bürgerteilhabe ins Spiel. Web 2.0 beinhaltet neue technische Möglichkeiten wie die interaktive many-to-many-Kommunikation, die (transnationale) Vernetzung in sozialen Gemeinschaften, synchrone Echtzeitkommunikation – auch Bild- und Tonwiedergabe. Zudem ist eine neue Rolle des Nutzers entstanden, nämlich der „content provider", d.h. der Nutzer, der selbst Inhalte generiert und verbreitet.

Die Aufstände in der arabischen Region, auch Beispiele wie die Acampada- und Occupy-Bewegungen oder andere Formen sozialen Protestes haben verdeutlicht, dass die Wirkmächtigkeit weit über die schlichte Kommunikation hinausgeht. Soziale Medien können eine wichtige Rolle bei der Organisation und Mobilisierung von Kampagnen und Protesten spielen (Kneuer et al. 2015). Die sozialen Medien verändern nicht nur die Informationsgewinnung, Informationsweitergabe und die Kommunikation im politischen Raum, sondern üben auch in vielfältiger Weise Einfluss auf politische Entscheidungsprozesse und auf das Verhältnis zwischen Repräsentierten und Repräsentanten aus. Die Parlamentarier und Regierungsmitglieder sind Kommunikationspartner geworden, mit denen sich der Bürger direkt austauschen kann; beziehungsweise umgekehrt: Parlamentarier und Regierungsmitglieder empfinden den Vorteil (oder die Verpflichtung), Twitter, Blogs, Facebook etc. zu nutzen, um so direkt und permanent mit dem Bürger in Kontakt zu kommen. Noch weiter gedacht nehmen die Implikationen der neuen Informations- und Kommunikationstechnologien (IKT) Einfluss auf das Ver-

hältnis zwischen Staat und Gesellschaft. Die Gesellschaft trägt Erwartungen an den Staat heran, insofern er ebenso von den Vorzügen des Internets profitieren (z.B. im Sinne des Netzzugangs) als auch vor seinen Nachteilen geschützt werden möchte (so etwa durch effektiven Datenschutz). Das Aufdecken der Abhörpraxis verschiedener westlicher Partnerstaaten wie den USA und Großbritannien hat diesbezüglich eine Sensibilisierung erreicht, die zuvor in Bezug auf die Verwendung persönlicher Daten eher niederschwellig war (und in großen Teilen der Bevölkerung weiterhin ist). „Datenschutz ist im Kommunikationszeitalter das, was Umweltschutz für die Industrialisierung war" (Zeh 2013). Das Aufdecken der NSA-Abhöraktivitäten hat gleichwohl zu einer teils skeptischeren Haltung beigetragen und die Debatte um Datensicherheit und Datenschutz intensiviert.

Die Frage nach der Wirkmächtigkeit des Netzes im politischen Bereich erfordert ein umfassendes Forschungsprogramm. Hier können daher nur sehr skizzenhaft einige Aspekte angerissen werden, von der generellen Frage geleitet, welche Leistungen digitale Medien erbringen und welche intendierten oder nicht-intendierten Wirkungen sie entfalten. Ein Diskursstrang geht davon aus, dass das technische Potenzial des Netzes, vor allem sozialer Netzwerke, dazu in der Lage ist, substanzielle Defizite im Funktionieren der heutigen demokratischen Systeme auszumerzen und Verbesserungen zu erreichen. Ein anderer Diskursstrang nimmt dagegen an, dass aufgrund der Funktionslogik sozialer Medien Dysfunktionalitäten im demokratischen Gefüge entstehen, die nicht nur einer Erneuerung der repräsentativen Demokratie entgegenstehen, sondern sogar kontraproduktive Effekte hervorbringen (vgl. Kneuer 2012, 2013).

Die folgenden Überlegungen basieren auf der nüchterneren, so genannten netzrealistischen Annahme, dass das Web 2.0 – so wie im Übrigen jedwede technologische Neuerung – Ambivalenzen aufweist und insofern sowohl funktionale als auch dysfunktionale Effekte haben kann. Funktionale Effekte digitaler Kommunikation und Interaktion wären demnach solche, die die Qualität demokratischer Prozesse im Hinblick auf Transparenz, Partizipation und Responsivität von Meinungs- und Willensbildung und Entscheidungen verbessern und damit auch die demokratische Legitimation erhöhen können; dysfunktionale Effekte würden eine Belastung dieser Prozesse bedeuten oder deren demokratische Qualität gar verschlechtern (zur detaillierten Herleitung vgl. Kneuer 2013, 2014). Dahlgren beschreibt diese Ambivalenz mit der Metapher von Kraftfeldern, in denen sich die Spannung zwischen diesem demokratiestärkenden und demokratiemindernden Charakter des Netzes abbildet (Dahlgren 2013: 36-64). Vor dem Hintergrund dieser spannungsreichen Kraftfelder ergeben sich etwa für die Partizipation im Netz oft gegensätzliche Dynamiken wie etwa Sozialität versus „netbullying", das zu Stress führen oder auch polizeiliche Maßnahmen erforderlich machen kann. Eine andere solche gegensätzliche Dynamik besteht in der Individualisierung und dem Aktivismus. Einerseits ist Netzkommunikation als personalisierte und „dünne" Kommunikation zu begreifen, die reich an Identitäts- und Lifestyle-Narrativen ist (Bennett 2003a: 145-151). So betont Castells zwei zentrale Charakteristika des Internets,

nämlich zum einen eher schwache als starke Verbindungen zu entwickeln und zu fördern sowie zum anderen die „Privatisierung der Soziabilität“ (Castells 2000: 389) – Entwicklungen, die Wellman als „vernetzten Individualismus“ (Wellman 1999) und Bennett als Personalisierung von politischer Kommunikation beschreiben (Bennett 2003a). Zugleich bieten digitale Medien wie nie zuvor die Möglichkeit, für politische Projekte Sympathisanten zu finden und zu mobilisieren. Virtuelle Aktivisten müssen sich weder am gleichen Ort befinden, noch von dem gleichen Grundproblem bedroht sein (Bennett 2003b: 28). Damit werden neue Bereiche politischen Wettbewerbs und der Kontroverse eröffnet, zugleich aber wirft dies auch neue Probleme auf wie etwa die geschwächte politische Effizienz oder auch das Meiden der Konfrontation mit den traditionellen Machtzentren (Dahlgren 2013: 52). Noch gibt es durch empirische Studien keine ausreichend robuste Basis, um eine abschließende Einschätzung in Bezug auf das demokratiebereichernde Potenzial (oder das Gegenteil) vornehmen zu können. Zugleich liegen wenige konzeptionelle Zugänge zur systematischen Bearbeitung vor. Ein Ansatz ist die zentralen demokratischen Kategorien auf die möglichen Effekte von Online-Kommunikation und Interaktion zu prüfen, nämlich Transparenz, Partizipation, Responsivität und Legitimation. Dabei stehen folgende Fragen im Vordergrund: Welche politischen Prozesse können durch das Internet unterstützt werden und Transparenz, Partizipation und Responsivität erhöhen? Für welche politischen Prozesse erweist sich die Funktionslogik des Internets eher als Belastung des demokratischen Prozesses und insofern als eher dysfunktional in Bezug auf Transparenz, Partizipation und Responsivität?

In den folgenden Abschnitten wird zunächst dargestellt, welche Nutzungsprofile Regierungen anbieten und Bürger annehmen können (2.) und welche dieser Möglichkeiten Bürger tatsächlich nutzen (3.). Auf dieser Grundlage wird abschließend eine tentative Einschätzung vorgenommen, ob tatsächlich mit Verbesserungen demokratischer Qualität durch netzbasierte Kommunikation und Interaktion gerechnet werden kann.

2 Das Internet, seine technischen Nutzungsmöglichkeiten und Nutzungsangebote von Regierungen

Zweifelsohne stellen digitale Medien, vor allem soziale Netzwerke, ein Instrument dar, dessen Wirkkraft alle bisherigen medialen Informations-, Mobilisierungs- und Vernetzungsmöglichkeiten überschreitet. Auf diese Wirkkraft können demokratische Gruppen zur Überwindung autokratischer Systeme jedoch ebenso zurückgreifen wie nichtdemokratische Gruppen oder Autokratien, um Opposition und Protest zu kontrollieren, zu infiltrieren und zu unterminieren (Kneuer et al. 2012). Soziale Medien haben nicht per se ein inhärentes Demokratisierungspotenzial; die Nutzung sozialer Medien führt nicht automatisch zu mehr Deliberation oder Partizipation in der Demokratie. Zwar bergen sie das technische Potenzial neuer Kommunikationslogiken (Interaktivität, Echtzeit, Ortlosigkeit) und andersartiger Handlungslogiken (Vernetzung, Transnationa-

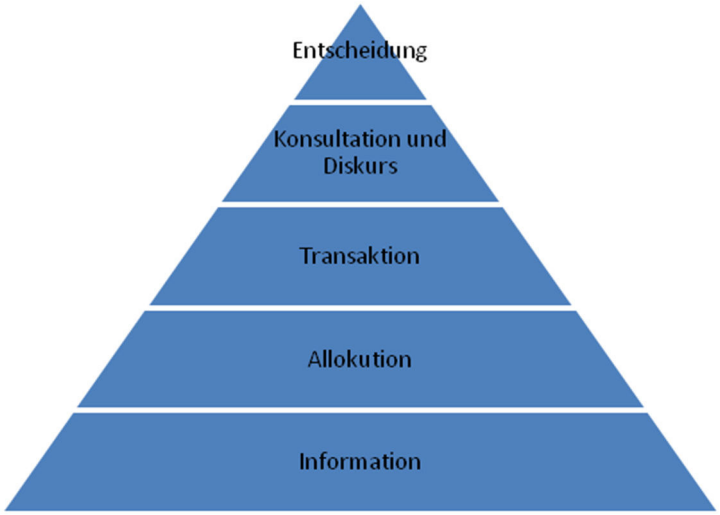
lität, Konnektivität). Soziale Medien operieren aber nicht im sozialen Vakuum und liefern keine einfachen Lösungen für die Probleme der Demokratie (Dahlgren 2013: 34). Ob die Nutzung sozialer Netzwerke demokratieförderlich oder -hinderlich ist, hängt von den Akteuren, der Art der Nutzung (Was wird wie kommuniziert?) ebenso ab wie von den Nutzungsmotiven und -zielen (Warum wird mit welchem Ziel kommuniziert?) sowie dem sozialen Kontext, in dem sie agieren. Das Gleiche gilt für die Handlungslogiken politischer Akteure.

Soziale Medien haben daher eine ermöglichende, aber keine verursachende Wirkung auf demokratische Handlungsweisen. Ob sie eine demokratisierende Kraft entfalten oder eher zur repressiven Kontrolle demokratischer Kräfte im Land eingesetzt werden; ob das Netz zur Bildung von neuartigen Foren der Deliberation oder zur Initiierung von Kampagnen oder Shitstorms genutzt wird; ob sich alternative Möglichkeiten der Partizipation ergeben (elektronische Petitionen und Unterschriftenlisten), mit denen mehr Menschen und vor allem solche eingebunden werden können, die sonst eher von politischer Teilhabe ausgeschlossen sind, oder ob eher mehr Ungleichheiten entstehen, da Vielen entweder die *hardware* oder die Netzkompetenz fehlt; ob Politiker sich durch neue Wege der Bürgeransprache responsiver zeigen oder ob sie sich getrieben von dem Diktat der digitalen Online-Kommunikation fühlen – all diese hier etwas plakativ als Gegensätze konstruierten Möglichkeiten hängen von mehreren Faktoren ab: nämlich a) in welchen Kontexten, b) in welcher Form, c) mit welchen Botschaften und Zielen und d) von welchem Akteur solche Kommunikation oder Maßnahmen initiiert und durchgeführt werden.

Der Bürger nimmt jedenfalls in unterschiedlichen Kommunikationskontexten unterschiedliche Rollen ein. Das drückt die untenstehende Graphik aus, indem sie unterschiedlichen Ebenen von Angebot und Nutzung wiedergibt. Die größten Möglichkeiten – dies galt bereits für das Web 1.0 – haben politische Akteure in Bezug auf die *Bereitstellung von Informationen* und die Bürger hinsichtlich der *Informationsbeschaffung* und des *Informationskonsums*. Zweifelsohne kann der Bürger so viele Informationen wie nie zuvor abrufen und Kenntnisse über mehr politische Vorgänge denn je erlangen. Jede Regierung, jedes Ministerium, alle Parteien, Verbände oder sonstigen Interessengruppen haben Websites, auf denen Informationen angeboten werden und abgerufen werden können (Dokumente, Reden, Pressemittelungen, Links). Gleichzeitig bedeutet das, dass sich der Bürger einer enorm großen Flut an Informationen gegenübersieht, die in ihrer Unüberschaubarkeit erhebliche Systematisierungs- und Orientierungsleistungen erfordert. Eine weitere Rolle des Bürgers ist inzwischen, dass er Ansprechpartner von Politikern, Parteien oder Interessengruppen geworden ist (*Allokution*). Die Bundeskanzlerin richtet wöchentlich Videobotschaften an die Bürger, Politiker unterhalten Blogs, in denen sie sich gezielt an den Bürger wenden. Hier ist der Bürger zunächst Informationskonsument. Er kann freilich auch in den Dialog mit dem Politiker, Parteienvertreter oder Vertreter von anderen Organisationen treten. Dies kann von den Politikern ausgehen (*Konsultation*), dann nutzen diese den Dialog mit dem Bürger,

um dessen Meinung, Interessen und Wünsche zu erfahren. Oder der Bürger tritt aus eigenem Antrieb in einen *Diskurs* mit Politikern. Dies ist über soziale Netzwerke (z.B. Facebook und Twitter) im Sinne eines horizontal vernetzten Online-Diskurses möglich. Eine andere Rolle kommt dem Bürger zu, wenn es um *Transaktionen* geht (Online-Steuererklärung, Online-Kfz-Anmeldung etc.). Hier handelt der Bürger als Kunde und Politik oder Verwaltung als Dienstleister. Die höchstwertige – nicht allein konsumtive, sondern konstitutive – Rolle von Bürgern besteht letztlich darin, an *politischen Entscheidungen* beteiligt zu werden, entweder bei Wahlen (e-voting) oder in Abstimmungsprozessen (e-referenda); auch deliberative Entscheidungsprozesse (Town Meetings, Deliberative Polling, Bürgerhaushalte etc.) können digital umgesetzt werden.

Abbildung 1: Netzbasierte Nutzungstypen von Bürgern



Quelle: eigene Darstellung.

Zunächst aber hängt das Potenzial, ein Mehr an Transparenz, Partizipation und Responsivität über internetbasierte Wege zu erlangen, von den Nutzungsvoraussetzungen ab sowie davon, ob und wie Staaten online verfügbare Angebote machen und ob und wie Bürger diese nutzen.

Nimmt man die weltweite Entwicklung der Nutzungsvoraussetzungen in den Blick, so offenbaren sich erhebliche Unterschiede. Die Vereinten Nationen messen seit 2011 die sogenannte „E-Government-Entwicklung“ anhand dreier Indikatoren, nämlich der technischen Infrastruktur, der von den Staaten online zur Verfügung gestellten Dienste und der Bildung (UN E-Government Survey 2014). Es ist kein überraschendes Ergebnis, dass hier die Länder mit hohem Einkommen einen klaren Vorteil haben und eine höhere E-Government-Entwicklung aufweisen. Des Weiteren aber machen die Daten und Rangfolgen der neuesten Studie der UN deutlich, welche Dynamik in diesem Bereich liegt. Während vor allem Länder Südostasiens und Ozeaniens (Australien, Japan, Singapur) in den letzten Jahren stark aufgeholt haben und nun an den Spitzenreiter Südkorea herangerückt sind, haben die vormals traditionell gut aufgestellten skandinavi-

schen Länder deutlich verloren. Deutschland nahm bislang ohnehin keinen Platz in der Spitzengruppe ein, rutschte aber ebenfalls etwas ab, auf Platz 24.

E-Government stellt sozusagen die schwächste Form der Einbeziehung des Internets in politische Prozesse dar, denn es geht zuvorderst um das „internetgestützte Abwickeln interner und externer administrativer Vorgänge mit größerer Geschwindigkeit und Interaktivität“ (Grundwald et al. 2006: 62). Der Bürger wird hier als Kunde betrachtet, dem eine bürgerfreundliche Verwaltungsleistung in Form der Online-Abwicklung behördlicher Vorgänge wie etwa das deutsche Elster-Verfahren bei der Steuererklärung ermöglicht werden soll. Zudem spielt die Kostensenkung für Bürger und Unternehmen eine Rolle. Die Leistung des Netzes wird hier weniger im Sinne demokratiebelebender Aspekte gesehen, vielmehr ist das Ziel die effektivere und dezentrale Bearbeitung von Dienstleistungen und Problemen, wenngleich freilich auch eine erhöhte Transparenz erreicht werden kann.

Die entwicklungsoptimistische Lesart der Vereinten Nationen impliziert, dass E-Government von Regierungen zugleich genutzt werden kann, um Bürger zu befähigen und sie am politischen Leben zu beteiligen. Dies geschieht etwa durch einen besseren Zugang zu Informationen, zu Dienstleistungen und die Möglichkeit, ihre Interessen gegenüber politischen Entscheidungsträgern hörbar zu machen. *E-Participation* – oft als *E-Democracy* bezeichnet – bezieht sich auf den weitergehenden Ansatz, via Internet neue und breitere Mitwirkungsmöglichkeiten zu schaffen. Auf dieser Entwicklungsstufe dient das Netz als Träger für zentrale Funktionen des demokratischen Prozesses – wie etwa Information, Kommunikation, Interessenartikulation und –aggregation sowie schließlich auch die Entscheidung in Form von Deliberation ebenso wie durch Wählen oder Abstimmen (Hagen o.J.; Hagen 1997). Umfassender als e-government und e-participation ist e-democracy zu verstehen. Das Konzept elektronischer Demokratie kann daher, so Zittel, als „Programm zur Reform repräsentativer Demokratie begriffen werden” (Zittel 2001: 173) mit dem Ziel von mehr Partizipation und einer Veränderung des Verhältnisses von Bürger und Staat.

Angestoßen durch die neuen Online-Interaktionsformen wie *liking* und *sharing* bei Facebook oder entsprechend *favoriting* und *retweeting* bei Twitter etwa mehren sich Stimmen, die nach Anpassungen klassischer Definitionen von Partizipation fragen bzw. diese auch in Frage stellen, etwa wenn es darum geht, festzulegen, ob etwa das Setzen eines Hakens in einer *Liking-Box* bereits Partizipation darstellt (Buchstein 1996; Voss 2014). Jedenfalls erscheint es für Forscher zunehmend notwendig, anzugeben, ob mit Partizipation eine eher niederschwellige Form, die bereits Information einschließt, oder ob eine höherschwellige Beteiligung gemeint ist, die aktive Beteiligung impliziert.

Die Vereinten Nationen fassen unter *e-participation* die drei Stufen *e-information, e-consultation* und *e-decision-making* (UN 2010: 83–84), die in dem oben dargestellten Dreieck (siehe Abb. 1) als jeweils eigene und voneinander unterschiedene Nutzungstypen verstanden werden. Für den e-participation-Index werden die Angebote der Regierungen aller 193 UN-Mitglieder ausgewertet (UN 2014: Annexes). Informationen

müssen demnach so gestaltet sein, dass sie Bürger zur Partizipation einladen (etwa durch Ankündigung von Ereignissen, an denen sie teilhaben können). Bei Konsultationen werden alle interaktiven Diskursmöglichkeiten betrachtet (Online-Umfragen, chat rooms, web logs, newsgroups etc.). Zu den Entscheidungsinstrumenten zählen online verfügbare öffentliche Ausschreibungen ebenso wie die öffentliche Bekanntmachung ihrer e-participation policy oder die Richtlinien für den Informationszugang bis hin zu e-petitions und e-voting.

Vergleicht man die letzten drei UN-Studien von 2010, 2012 und 2014, so fällt als erstes die Dynamik auf, mit der unterhalb des unangefochtenen Spitzenreiters Südkorea die Ränge wechseln. Steile Aufstiege (Vereinte Arabische Emirate, Uruguay, Costa Rica) sind ebenso möglich wie steile Abstiege (Russland, Schweden, Deutschland). Beobachtet werden sollten daher insbesondere Aufsteiger, die sich halten (Kolumbien, Chile). Zweitens ist bemerkenswert, dass demokratische und einkommensstarke Staaten in dieser Spitzengruppe dominieren; dennoch bieten autoritäre Regime wie Bahrein, Singapur, Kasachstan und die Vereinten Arabischen Emirate ganz offensichtlich mit einiger Kontinuität ebenso bürgerorientierte Websites und Online-Interaktionsformen an.[2]

Betrachtet man all jene Regierungen, die sich im oberen Drittel von e-participation-Angeboten befinden, so ergibt sich ein sehr uneinheitliches Bild in Bezug auf die einzelnen Nutzungstypen: Information, Konsultation und Entscheidung. Während ein durchaus beachtlicher Anteil an Regierungen sich in Bezug auf elektronische Informationsangebote im oberen Bereich befindet, nämlich insgesamt 84 Länder (entspricht 43,5% aller UN-Mitglieder), sieht die Zahl bei e-consultation bereits ganz anders aus: In intensiver Weise schalten weltweit nur 19 Länder (9,8%) solche Angebote. Möglichkeiten zur Beteiligung an Entscheidungen (e-decision-making) eröffnen letztlich von den 193 UN-Mitgliedern überhaupt nur 44 Länder, also weniger als ein Viertel; lediglich neun Länder liegen im oberen Drittel (4,6%)[3]. Interessant ist, dass soziale Medien das von Regierungen (immerhin 71) am meisten genutzte Instrument zur Konsultation darstellt; gefolgt von Online-Foren (51), Online-Umfragen (39). Abstimmungen und Petitionen führen dagegen nur jeweils 18 Regierungen durch (UN 2014: 69).

Fasst man diesen kurzen Blick auf die internationale Situation der Online-Interaktionsfelder zusammen, die Regierungen zur Verfügung stellen, so spiegelt sich die oben eingeführte Pyramide (siehe Abb. 1) empirisch wider: Es gibt ein breites Angebot zur Informierung der Bürger, wenn es aber um den horizontalen Diskurs oder gar um das Eröffnen von Beteiligung an politischen Entscheidungen geht, reduziert sich weltweit die Gruppe der Länder auf eine Minderheit. In diesem Sinne lesen sich die Zahlen für die Bundesrepublik Deutschland: In der Bereitstellung von Informationen

2 Kolumbien, Marokko und Malaysia zählen zu den nicht vollständig konsolidierten Demokratien.

3 Kolumbien, Japan, Südkorea, USA (Spitzengruppe), Australien, Frankreich, Niederlande, Großbritannien, Russland, Uruguay. Interessanterweise ist Kasachstan, das 2010 noch mit Südkorea und Australien die Spitzengruppe ausmachte, sehr stark abgerutscht.

erreicht es zwar fast 100% und befindet sich somit in der Spitzengruppe, bei Konsultationsangeboten liegt Deutschland allerdings nur im Mittelbereich und in Bezug auf e-participation unter den Schlusslichtern. Nach dem guten Rang 8 im Jahr 2012 ist Deutschland 2014 auf Platz 24 abgerutscht.

Abbildung 2: Spitzengruppe des E-Participation-Index der UN (2010, 2012 und 2014)

Rang	2010	2012	2014
1	Südkorea	Südkorea, Niederlande↑↑	Südkorea, Niederlande
2	Australien		
3	Spanien	Kasachstan↑↑↑, Singapur↑	Uruguay↑↑↑
4	Neuseeland		Frankreich↑, Japan↑, UK
5	UK	UK, USA	
6	Japan, USA		
7		Israel↑↑↑	Australien↓, Chile↑↑
8	Kanada	Australien↓, Estland, Deutschland↑	
9	Estland, Singapur		USA
10			Singapur↓
11	Bahrein	Kolumbien↑↑↑, Finnland↑↑↑, Japan↓, **Ver. Arabische Emirate**↑↑↑	Kolumbien
12	Malaysia		Israel↓
13	Dänemark		Ver. Arabische Emirate
14	Deutschland		Bahrein↑, **Costa Rica**↑↑↑, Kanada↓
15	Frankreich	Kanada↓, Ägypten↑↑↑, Norwegen↑, Schweden↑	
16	Niederlande		
17	Belgien		Griechenland↑↑↑, Marokko↑↑↑
18	Kasachstan		
19	Litauen	Bahrein↓, Chile↑↑↑, **Russland**↑↑↑	Neuseeland↑, Spanien↑↑, Italien↑↑↑
20	Slowenien		

Quelle: eigene Zusammenstellung.
Länder, die in ihrer Bewertung seit der vorhergehenden Studie um 5 und mehr Ränge gestiegen oder gefallen sind, sind mit einem Pfeil, um 10 und mehr Ränge mit zwei Pfeilen, um 15 und

mehr Ränge mit drei Pfeilen gekennzeichnet. Länder, die über 30 Ränge gestiegen oder gefallen sind, sind zusätzlich fett gesetzt.

3 Nutzung von Online-Angeboten durch die Bürger

Wie bereits erwähnt, sind Studien rar, zumal umfassende und differenzierte, die Aufschluss über die Nutzung des Internets zu politischen Zwecken geben. Dem folgenden Abschnitt liegen die Studie von Emmer, Vowe und Wolling aus dem Jahr 2011 sowie die jüngeren Untersuchungen vom Institut für Demoskopie Allensbach aus 2011, Ritzi, Schaal und Kaufmann aus 2012 und die Partizipationsstudie des Alexander von Humboldt Instituts für Internet und Gesellschaft (AHIIG) von 2014 zugrunde.[4]

Anders als die UN-Studie wird der Begriff der Partizipation hier nicht gleich umfassend gebraucht; d.h. als Dachbegriff für e-information, e-consultation und e-decision-making. Es macht vielmehr Sinn, diese Interaktionsformen differenziert zu betrachten, denn sie beinhalten unterschiedliche *Handlungsformen* (e-information = Abfrage von Informationen; e-consultation oder e-discourse = kommunikativer interaktiver Austausch mit Politikern; e-decision-making = Beteiligung an politischen Entscheidungsprozessen), die mit unterschiedlichem zeitlichen und sonstigem *Aufwand* verbunden sind und schließlich auch unterschiedliche *Ziele* haben können. So lässt sich in Bezug auf e-information unterstellen, dass die Nutzer nach Informationsgewinn suchen, bei e-consulation/discourse die eigene Meinungsbildung oder die Beteiligung an kollektiven Meinungsbildungsprozessen eine Rolle spielen sowie bei e-decision-making die Beteiligung und Einflussnahme auf politische Entscheidungsprozesse im Vordergrund steht.

Auf der Grundlage der empirischen Befunde wird im Folgenden versucht, eine Antwort darauf zu finden, inwieweit die Internetnutzung der Bürger auf eine mögliche Verbesserung in den Bereichen Transparenz, Partizipation und Responsivität hindeutet. Transparenz wird dabei angenommen, wenn Bürger die Informationsangebote via Internet annehmen und so einen potentiellen Gewinn an Kenntnissen über politische Prozesse und Hintergründe erlangen. Eine Verbesserung der Partizipation würde darin bestehen, wenn Bürger verstärkt onlinebasierte Beteiligungsformen nutzen. Schwieriger ist die Messung der Responsivität anhand der vorliegenden Studien; daher werden sich die Aussagen lediglich auf den politischen Diskurs und den politischen Austausch mit Politikern beschränken, was ein Element von Responsivität sein kann, aber die Kategorie freilich nicht in der Gänze erfasst.

4 Die Analysen sind in ihrer Ausrichtung und ihrem Umfang recht unterschiedlich. Die Studie von Emmer et al. bietet zweifelsohne den breitesten und zugleich differenziertesten Ansatz; für die Bewertung der heutigen Situation müssen allerdings Einschränkungen gemacht werden aufgrund des 2009 endenden Datensatzes. Die Studie von Ritzi et al. beschränkt sich auf das Bevölkerungssegment der 21-35-jährigen und erlaubt somit nur begrenzte Aussagen. Daher bietet die Partizipationsstudie des AHIIG zurzeit den wohl aktuellsten Bick, wobei hier die Fragestellung auf Partizipation zugeschnitten ist (also weitaus enger als bei Emmer et al.), was wiederum andere Bereiche (Konsultation, Diskurs etc.) ausnimmt.

3.1 Informationsgewinnung: mehr Transparenz?

Ohne Zweifel hat das Internet als Quelle politischer Information an Bedeutung gewonnen. Gleichwohl beziehen die Bürger ihre politischen Informationen weiterhin über klassische Medien oder sogar über persönliche Gespräche weit vor sozialen Netzwerken, Internetseiten und -portalen, selbst vor Online-Angeboten von Zeitungen. Auch bei der Informierung über das aktuelle politische Geschehen spielt das Internet nur eine marginale Rolle. Weniger als ein Drittel nutzt das Internet (mindestens 2-3 Mal die Woche), um sich über Politik zu informieren (Köcher et al. 2011: 16). Dies sieht allerdings anders aus, wenn man nur die jüngere Generation in den Blick nimmt; hier ist der Anteil derjenigen, für die das Internet eine wichtige politische Informationsquelle darstellt, deutlich höher (50%; ebd.: 24). In der Studie von Ritzi et al. finden sich zudem recht hohe Zahlen für die Informationsabfrage von 21-35-jährigen auf Nachrichtenseiten (96,2%), dem Empfangen von Newslettern (46,7%) und auch bei der Nutzung von Behörden-Websites (41,6%; Ritzi et al. 2012: 22). Bereits bei der Informationsabfrage kristallisieren sich Kluften heraus zwischen Geschlecht, Alter, Ausbildungs- sowie Einkommensniveaus. Generell nutzen Frauen, insbesondere aber Ältere das Internet weniger zur Informierung.

Die weit ausdifferenzierte Studie von Emmer et al. (2011) bringt die Nutzung bestimmter Informationsquellen mit soziodemographischen Daten in Verbindung und zeigt auf diese Weise, dass die Nutzung von journalistischen Online-Angeboten über politisches Geschehen deutlich zugenommen hat, dass zugleich aber starke Unterschiede im Bildungsstand bestehen. Ältere Onliner jedoch haben stark aufgeholt und fast gleichgezogen. Beim Lesen politischer Weblogs – eine Nutzungsform, die noch vor dem Lesen von Politiker-Internetseiten liegt – scheinen Bildungsunterschiede interessanterweise weniger relevant. Hier liegt die Gruppe mit mittlerer Bildung vorne (Emmer et al. 2011: 135–137). Viele Informationsmöglichkeiten – wie etwa das Anfordern von Informationsmaterial oder das Ansehen von Videos – werden kaum genutzt oder auf einem niedrigen und nicht wachsenden Niveau (podcasts) (ebd.: 139–141).

Eine wichtige Erkenntnis hinsichtlich der Internetnutzung zum Informationszugewinn ist, wie Köcher/Büttel (2011: 18) festhalten, dass Informierung im Internet „interessens- und ereignisgetrieben“ ist. Das heißt, das Internet wird weniger genutzt, um sich fortlaufend und ohne konkreten Anlass über das aktuelle Geschehen und Politik zu informieren, als vielmehr dazu, gezielte Informationssuche zu bestimmten Themen oder Ereignissen zu unternehmen. Interessant zu untersuchen wäre, inwieweit diese stark fokussierte und verengte Online-Informationssuche komplementär zu einer allgemeinen und breiten Informierung über Politik offline geschieht oder letztere ersetzt.

Letztlich ist eine Mehrheit der Bürger der Meinung, dass das Internet die Informationsmöglichkeiten über Politik verbessert (36% sehr, 33% etwas; ebd.: 34), auch wenn sie andere Medien primär für Informationen nutzen.

3.2 Diskurs und Austausch: mehr Responsivität?

Fragt man die Bürger, ob das Internet zu einem lebendigeren politischen Diskurs führen kann, so ist davon weniger als ein Drittel überzeugt. Hier liegen wiederum die Zahlen für die jüngere Generation höher (Köcher et al. 2011: 35). Dennoch wünscht sich eine Mehrheit, bei lokalen Belangen (68%) oder auch bei allgemeinen Themen und Gesetzesvorhaben (63%) mitreden zu können (ebd.: 38).

Wird das Internet für den politischen Diskurs genutzt, also bilden soziale Medien neue Foren für solche Diskurse? Die Zahlen für den Zeitraum von 2002 bis 2009 (Emmer et al. 2011: 143–160) sind da eher ernüchternd: Gespräche im Internet über Politik führten etwa 5% aller Befragten; bei den Onlinern liegt die Zahl etwas höher (10%), wenngleich der Trend nicht steigend ist. Diese Zahlen werden von der jüngeren Studie bestätigt, nach der ebenfalls nur 10% politische Debatten in sozialen Netzwerken führen bzw. Debattenbeiträge verfassen (Köcher et al. 2011: 42; AVIIG 2014: 28). Noch niedriger sind die Anteile von Bürgern, die eine E-Mail an einen Abgeordneten schreiben – hier sind die Älteren übrigens aktiver –, nämlich etwa 7%, einen politischen Beitrag in einem Chatroom verfassen (6%), sich auf einer eigenen Homepage, einem Blog oder über Twitter äußern (2%; ebd.: 42–44). Allerdings unterscheiden sich hier wieder die Jüngeren von den Älteren. In dieser Gruppe liegt der Austausch über politische Themen in sozialen Netzwerken bei den Online-Aktivitäten an der Spitze (39%). Das belegt, dass das Internet für diese Generation zuvorderst ein Medium des Austausches ist.

3.3 Neue Formen der Beteiligung: mehr Partizipation?

Das Internet hält zwei Vorteile im Bereich der Partizipation bereit: Zum einen ist es für bereits bestehende alternative Partizipationsformen – wie Unterschriftenaktionen und Petitionen – eine schnellere, effektivere und kostengünstigere Durchführungsart, die zudem für den Nutzer meist einen niedrigeren Aufwand bedeutet. Zum anderen bieten die technischen Möglichkeiten interaktiver Echtzeitinteraktion neue Formen der Beteiligung, wie Online-Konsultationen. Welche alten oder neuen Formen unkonventioneller Partizipation aber nutzen die Bürger tatsächlich und wie tun sie es?

Um die im Großen und Ganzen konsensuellen Befunde der verschiedenen Studien vorwegzunehmen: Die Online-Formen des Engagements ersetzen im Allgemeinen nicht die traditionellen Partizipationsformen, sondern ergänzen sie eher; nur dort, wo das Internet eine starke Vereinfachung bietet, kann es auch zu Verdrängungseffekten kommen. Die Bürger, insbesondere auch die Jüngeren, nutzen online – ähnlich wie offline – stark die Form von Online-Petitionen sowie Abstimmungen über politische Sachverhalte (Köcher et al. 2011: 44; Ritzi et al. 2012: 23; AVIIG 2014: 28–29). Ein Grund mag darin liegen, dass beides sich relativ einfach und mit geringem Zeitaufwand bewerkstelligen lässt. Die Messung von Reichweite und Zeitaufwand in der Partizipationsstudie (AVIIG 2014: 31) belegt sehr deutlich, dass Nutzungsformen mit hohen Nut-

zerzahlen bei geringem Zeitaufwand (Online-Petitionen Zeichnen, politische Sachverhalte Abstimmen) Nutzungsformen gegenüberstehen, in die wenige Nutzer einen hohen Zeitaufwand stecken (über Bürgerhaushalte beraten, an Online-Konsultationen teilnehmen, Online-Petitionen erstellen). Insofern deutet Einiges auf eine sich abzeichnende Beteiligungslücke („*participatory divide*“) hin. Ritzi et al. (2012) beziehen dies in der Betrachtung der Nutzungsmotive auf den Umstand, dass es mehr Menschen um symbolische Partizipation geht – nämlich ein Zeichen zu setzen – denn um instrumentelle Partizipation – im Sinne eines Engagements, das auf politische Einflussnahme zielt (ebd.: 26). Das heißt, die junge Generation nutzt die Beteiligungsmöglichkeiten nicht, um den politischen Entscheidungsprozess zu beeinflussen, sondern um politische Zeichen zu setzen. Deswegen – so die Autoren – kann „mehr Partizipation im Netz nicht die Partizipationsdefizite in der realen Welt kompensieren“ (ebd.: 35). Ein weiterer *participatory divide* kann – ebenfalls für die jüngere Generation – darin bestehen, dass die allgemeine Nutzung der Partizipationsformen negativ korreliert mit dem damit verbundenen Aufwand: Je anspruchsvoller die Beteiligungsform ist, desto weniger wird sie genutzt (ebd.: 23). Dies unterstützt die Ergebnisse der Studie von Emmer et al., die alle Aktivitäten, bei denen man eigene Beiträge (eigene Homepage, Beiträge in Bild oder Film, Blogs) abzufassen hat, gering sind (2011: 161–198). Das bedeutet, dass nur derjenige, der in einer Aufwand-Nutzen-Kalkulation den Aufwand hintanstellt, sich in dieser „anspruchsvolleren“ Form beteiligen wird. Dies setzt die Bereitschaft voraus, sich länger mit einer politischen Frage oder einer Interaktionsform auseinanderzusetzen. Es steht zu befürchten, dass gerade bei jüngeren Onlinern jedoch die schnelle und niederschwellige Aktion im Vordergrund steht, zumal wenn man den Befund miteinbezieht, dass das Zeichen-Setzen dominiert. Ernüchternd ist auch eine weitere Facette dieses *participatory divide*: Dass nämlich die höheren Bildungsschichten das Internet wesentlich konsequenter für die Verbesserung ihrer Information und Meinungsbildung nutzen, während die unteren Bildungsschichten das Netz primär für im Alltag einsetzbare „Nutzwertinformation“, d.h. Kommunikation und Unterhaltung nutzen (Köcher et al. 2011: 40).

Zusammengefasst lässt sich sagen, dass keine wachsende Zahl online politisch aktiver Bürger erkennbar war, sondern Bürger, die zusätzlich den Online-Weg zu dem ohnehin genutzten Strauß an Offline-Aktivitäten gehen (Emmer et al. 2011: 158). Internetbasierte Formen des politischen Engagements ersetzen also nicht die analogen, sie ergänzen sie. Politische Beteiligung im Netz scheint eher neue Kluften widerzuspiegeln – Stichwort *participatory divide* –, als dass sie neue Bevölkerungskreise erfasst oder neue Wege politischer Einflussnahme aufzeigt.

4 Conclusio

Unbestreitbar bietet das Internet erhebliche Möglichkeiten der Information, des interaktiven Austausches und der Organisation von politischer Teilhabe und Einflussnahme

für interessierte Bürger und Politiker. Allerdings hat dieser Beitrag eine differenziertere, „netzrealistische" Betrachtungsweise eröffnet. Zwei Aspekte standen dabei im Fokus der vorangegangenen Argumentation: Erstens hängen die in der Pyramide (Abb. 1) skizzierten Interaktionsfelder von der Bereitstellung durch den Staat und die politischen Akteure ab (Angebotsstruktur). Neben technischen Voraussetzungen (Netzzugang) und rechtlichen Bedingungen (Zensurfreiheit etc.) spielen – darauf wurde hier nicht eingegangen – zudem die Nutzungskompetenzen eine zentrale Rolle. Soll aber zudem der Diskurs zwischen Bürgern und Politikern intensiviert werden, bedarf es hierzu spezifischer Kanäle, die die Regierungen, Parteien etc. bereitstellen und pflegen müssen. Hier gibt es freilich weltweit noch etliche weiße Flecken, aber auch in Europa und selbst in Deutschland besteht weiterhin erheblicher Raum, das Angebot auszuweiten.

Zweitens, ist die Nachfrage entscheidend, also die Wege und die Intensität der Nutzung durch die Bürger. Dabei erzeugen nicht nur die allseits bekannten *digital divides* erhebliche Ungleichheiten in der Nutzung und Wirkung, die die Wirksamkeit des Mediums Internet insbesondere im Sinne eines breiteren diskursiven Austausches und einer intensiveren politischen Beteiligung in Frage stellen. Beachtenswert ist zudem, dass sich in den Bevölkerungssegmenten, in denen sich stärkere Nutzung finden lässt, neue problematische Entwicklungen abzeichnen. Die unter dem Stichwort *participatory divide* gefassten Phänomene – die Beschränkung auf symbolische Partizipation, auf niederschwellige Partizipationsformen und gezielte Nutzung der Ressourcenstärkeren – weisen auf eine gespaltene Kommunikationskultur hin, die eine optimistisch geprägte Interpretation des Internets als Allheilmittel zur Belebung der repräsentativen Demokratie eher Lügen straft.

Zudem zieht sich ein Befund durch alle Studien: Die Wirkungen des Online-Zugangs sind sozial selektiv. Mobilisierend wirkt der Zugang vor allem bei Jüngeren. Die Mobilisierung ist da sehr differenziert entlang der drei Kommunikationstypen zu betrachten: In Bezug auf die Information kann man sagen, dass hier via Internet der Nutzerkreis ausgeweitet werden konnte und zugleich aber eine Verstärkung der Nutzung bei denen zu erkennen ist, die vorher bereits aktiv waren. In Bezug auf den Diskurs bleibt die Mobilisierung moderat und findet vorwiegend bei Jüngeren statt, kaum dagegen im Hinblick auf neue Nutzerschichten. In Bezug auf politische Online-Partizipation ist keine signifikante Mobilisierung erkennbar (Emmer et al. 2011: 302). Hier scheint das Internet bislang keine Effekte aufzuweisen, die darauf hindeuten, dass sich durch die neuen technischen Möglichkeiten die politische Beteiligung substantiell steigern lässt.

Kurzum: Allein über elektronische Wege lassen sich keine Lücken in der politischen Partizipation von selbst schließen. Insbesondere die ungleichen Beteiligungschancen ressourcenschwacher und -starker Bevölkerungsteile beinhalten eher Legitimationsprobleme, als dass bestehende aufgelöst werden könnten. Dennoch ist eine Ergänzung und Bereicherung repräsentativer Demokratie mit Elementen digitaler Kommunikation und Vernetzung zur Verbesserung der Teilhabe von Bürgern denkbar. Insbesondere im

kommunalen Bereich, etwa im Rahmen kommunaler Planungsprozesse, versprechen Online-Verfahren Legitimitätsempfindlichkeiten von Bürgern entkräften zu können und haben zudem das Potenzial, auch ansonsten eher inaktive oder gar gänzlich von traditioneller politischer Partizipation (Wahlen, direktdemokratische Elemente) Ausgeschlossene (nicht-deutsche Staatsbürger, Menschen unter 18 Jahren) zu inkludieren.

Dennoch bleiben offene Fragen: Sind Bürger, die Online-Angebote nutzen und sich an Meinungsbildungs- oder Entscheidungsprozessen beteiligen, zufriedener mit den Entscheidungen (und mit dem Funktionieren von Demokratie)? Auch wenn die Prozesse unbefriedigend ablaufen und das Ergebnis den Interessen zuwiderläuft? Und wie empfinden staatliche oder lokale Behörden netzbasierte Verfahren, die angeboten und nicht nachgefragt werden? Welcher Strategien bedarf es zur „Motivation" zur Teilhabe? Was passiert, wenn Möglichkeiten zur Beteiligung eröffnet werden und Verfahren auf intensive Bürgerbeteiligung zugeschnitten werden, und diese nicht stattfindet?

Die Vorstellung jedenfalls, allein die Existenz neuer technischer Wege sei dazu in der Lage, Defizite oder Fehlentwicklungen in der repräsentativen Demokratie zu beheben, muss als naiv bewertet werden. Auch die Vision einer elektronischen Selbstregierung der Bürger ist nicht nur nicht umsetzbar, sondern steht mindestens einer – allerdings sehr hohen – Hürde gegenüber: der fehlenden Gleichheit des Zugangs, der Netzkompetenz und der Stimme des einzelnen Bürgers. Das heißt, nur wenn garantiert sein könnte, dass alle Bürger gleichermaßen informiert sind, alle gleichermaßen am Deliberationsprozess teilnehmen könnten und würden und dann alle eine gleichgewichtige Stimme bei der Entscheidungsfindung hätten, könnte dieses Ideal erreicht werden.

Bei der genauen Betrachtung einer Verbesserung demokratischer Qualität durch digitale Medien ist es geboten, sowohl die Angebots- als auch die Nachfrageseite in den Blick zu nehmen. Eine Erhöhung demokratischer Qualität schließt ein, dass die netzbasierten demokratischen Prozesse von beiden Seiten aktiv gestaltet werden. Eine realistische Variante zielt daher auf die Einbindung partizipativer Elemente in die repräsentative Demokratie, die weder letztere ersetzt noch zu einem „elektronischen Athen" stilisiert wird, bei dem die Bürger mit einem Beteiligungsdiktat konfrontiert werden. Vorstellbar ist dagegen vielmehr, die repräsentative Demokratie zu ergänzen und mit Elementen digitaler Kommunikation und Vernetzung zu bereichern, dort wo dem Wunsch der Bürger nach mehr Teilhabe entsprochen werden soll. Dort, wo solche Teilhabe – sinnvoll – eingebaut wird, kann das Internet tatsächlich wenig aufwändig und effektiv die Willensbildung und Entscheidungsfindung verbessern. Das trifft zum Beispiel auf Ergänzungen partizipativer Formen insbesondere im Rahmen kommunaler Planungsprozesse zu: Bürger können sich die Planungsalternativen herunterladen, haben Zugang zu den einschlägigen Dokumenten und können sich auch in Foren an den Diskussionen beteiligen.

Solche elektronischen Reformen der repräsentativen Demokratie beinhalten gleichwohl zunächst Aufgaben, die der Staat bzw. die nationale Regierung zu erfüllen hat, um diesen Modernisierungsprozess zu steuern. Die erste Voraussetzung besteht in

einem Netzzugang für alle Bürger, die zweite in sicheren Netzen. Nur wenn Netzsicherheit gewährleistet ist, sind überhaupt Formen elektronischer Teilhabe denkbar. Ein dritter Aspekt, die Netzkompetenz, beinhaltet nicht nur die Fähigkeit, mit dem Medium Internet umzugehen, sondern auch die Formen und Regeln des Netzdiskurses zu erlernen. Dazu wäre etwa eine grundlegende Hinführung bereits in den Schulen vonnöten.

Konkrete Schritte zur Verbesserung der demokratischen Qualität sind also denkbar im Sinne einer Ergänzung des repräsentativen Demokratiemodells durch responsive oder partizipative Elemente – Vorländer spricht in diesem Zusammenhang von einem „gemischten Regime“ (2011), das über die Gewaltenteilungs- und Kontrollsysteme der traditionellen Repräsentativdemokratie hinausgeht. Solche Reformschritte können durch die zusätzlichen Wege der Informierung und Allokution, der Konsultation und der Beteiligung qua Internet gestützt werden. Dabei muss allerdings darauf geachtet werden, dass die Institutionen der repräsentativen Demokratie nicht geschwächt werden und die repräsentativ-demokratischen Prozesse nicht unterspült werden von plebiszitären Vorkehrungen, die zum Beispiel das Parlament schwächen oder die Steuerungskapazität der Exekutive reduzieren könnten. Insbesondere müssen auch mögliche Dysfunktionalitäten im Blick bleiben. So können zu viele *e-consultation*- oder *e-referenda*-Elemente etwa eine weitere Verlangsamung der Entscheidungsprozesse nach sich ziehen, was Frustrationseffekte von Bürgern eher erhöhen als reduzieren dürfte und zudem einer größeren Transparenz oder Übersichtlichkeit der Entscheidungen ebenso wenig zuträglich wäre.

Literatur

Alexander von Humboldt Institut für Internet und Gesellschaft (2014): Partizipationsstudie 2014, http://www.hiig.de/online-mitmachen-und-entscheiden-die-partizipationsstudie-2014/ (18.04.2015).

Bennett, W. Lance (2003a): Lifestyle Politics and Citizen-Consumers: Identity, Communication, and Political Action in Late Modern Society, in: Corner, John, Pels, Dick (Hrsg.): Media and the Restyling of Politics: Consumerism, Celebrity and Cynicism, Sage: London.

Bennett, W. Lance (2003b): Communicating Global Activism. Strength and Vulnerabilities of Networked Politics, http://ccce.com.washington.edu/projects/assets/working_papers/communicatingglobalactivism.pdf (22.02.2015).

Castells, Manuel (2000): The Information Age: Economy, Society, and Culture. Volume 1. The Rise of the Network Society, Wiley-Blackwell: Malden.

Dahlgren, Peter (2013): The Political Web: Media, Participation and Alternative Democracy, Palgrave Macmillan: Basingstoke.

Emmer, Martin / Vowe, Gerhard / Wolling, Jens (2011): Bürger online. Die Entwicklung der politischen online-Kommunikation in Deutschland, UVK-Verlagsgesellschaft: Bonn.

Grunwald, Armin / Banse, Gerhard / Coenen, Christopher / Hennen, Leonhard (2006): Netzöffentlichkeit und digitale Demokratie: Tendenzen politischer Kommunikation im Internet, Edition sigma: Berlin.

Hagen, Martin (o.J.): A Typology of Electronic Democracy, http://martin-hagen.net/publikationen/elektronische-demokratie/typology-of-electronic-democracy/ (28.1.2012).

Hagen, Martin (1997): Elektronische Demokratie. Computernetzwerke und politische Theorie in den USA, LIT: Hamburg.

Hindman, Matthew (2009): The Myth of Digital Democracy, Princeton University Press: Princeton/Oxford.

Köcher, Renate / Bruttel, Oliver (2011): 1. Infosys-Studie: Social Media, IT and Society 2011, Infosys Limited: Frankfurt.

Kneuer, Marianne (2012): Demokratischer durch das Internet? Potenzial und Grenzen des Internets für die Stärkung der Demokratie, in: Politische Bildung, 2012:1, 28–54.

Kneuer, Marianne (2013): Bereicherung oder Stressfaktor? Überlegungen zur Wirkung des Internets auf die Demokratie, in: Kneuer, Marianne: (Hrsg.): Das Internet: Bereicherung oder Stressfaktor für die Demokratie?, Nomos: Baden-Baden, 7–35.

Kneuer, Marianne (2014): Mehr oder weniger demokratische Qualität durch das Internet?, in: Der Bürger im Staat. Politik und Internet, 64:4, 196–205.

Kneuer, Marianne / Demmelhuber, Thomas (2012): Die Bedeutung Neuer Medien für die Demokratieentwicklung. Überlegungen am Beispiel des Arabischen Frühlings, in: Informationen zur Politischen Bildung Bd. 35, 30–38.

Kneuer, Marianne / Richter, Saskia (2015): Soziale Medien in Protestbewegungen. Neue Wege für Diskurs Organisation und Empörung, Campus Verlag: Frankfurt am Main.

Rheingold, Howard (1993): The Virtual Community: Homesteading at the Electronic Frontier. MIT Press: New York.

Ritzi, Claudia / Schaal, Gary S. / Kaufmann, Vanessa (2012): Zwischen Ernst und Unterhaltung. Eine empirische Analyse der Motive politischer Aktivität junger Erwachsener im Internet, Universität der Bundeswehr Hamburg: Helmut-Schmidt Universität.

UN 2010: E-Government Survey (2010), http://unpan3.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2010 (18.04.2015).

UN 2014: E-Government Survey (2014), http://unpan3.un.org/egovkb/Reports/UN-E-Government-Survey-2014 (18.04.2015).

Wellman, Barry (1999): The Network Community, in: Wellman, Barry (Hrsg.): Networks in the Global Village. Life in Contemporary Communities, Westview Press: Oxford, 1–47.

Wilhelm, Anthony G. (2000): Democracy in the Digital Age. Challenges to Political Life in Cyberspace, Routledge: New York, London.

Zeh, Juli (2013): Mein digitaler Zwilling gehört mir, in: Frankfurter Allgemeine Zeitung, 7.9.2013: 35.

Autorin

Prof. Dr. Marianne Kneuer

Professorin für Politische Wissenschaft und Geschäftsführende Direktorin des Instituts für Sozialwissenschaften

Universität Hildesheim

Universitätsplatz 1

DE-31141 Hildesheim

kneuer@uni-hildesheim.de

DOI: 10.11588/josar.2015.0.23481

Gibt es Souveränität im Cyberspace?

Milton L. Mueller[1]

1 Einleitung

Gibt es Souveränität im Cyberspace? – Das ist eine Frage, die mich in den vergangenen fünf Jahren beschäftigt und fasziniert hat, in einer Phase der Internetentwicklung, in der sich die einst sehr verschiedenen Politikbereiche der Internet Governance, Außenpolitik und der nationalen Sicherheit deutlich angenähert haben. Das ist durchaus überraschend für diejenigen, die sich schon seit langem mit der Internetwirtschaft, mit Domain names, mit Zensur und Internetfreiheiten, mit Bürgerrechten befassen. Zwar hat das Verhältnis zwischen Staaten und dem Cyberspace, oder *Networks and States* (Mueller 2010), wie der Titel meines jüngsten Buches lautet, die Debatten über die Regulierung des Internets seit Mitte der 1990er Jahre bewegt. Aber mit dem Einzug nationaler Sicherheit und Außenpolitik in dieses Feld, erhält es eine neue, bislang wenig erforschte Dimension.

Freilich hat dieses Thema gerade in jüngerer Zeit, nach den Enthüllungen durch den Whistleblower Edward Snowden, an politischer Relevanz und gesellschaftlicher Aufmerksamkeit gewonnen, doch schon zuvor war über das Problemfeld Cybersicherheit eine Verknüpfung zwischen dem Internet und der nationalen Sicherheit gegeben. Nach Snowden werden nun explizite Forderungen nach Datensouveränität, technologischer Souveränität oder anderen wohlklingenden und kreativ benannten Visionen eines staatlichen oder justiziellen Überbaus für Computernetzwerke formuliert. Es geht dabei aus meiner Sicht darum, das Internet zu „souveränisieren“. Daher haben diese Neuerfindungen oder Wiederbehauptungen des klassischen Souveränitätskonzepts auf der anderen Seite Gegenstimmen und Warnungen vor einer Fragmentierung oder einer ‚Balkanisierung‘ des Internets ausgelöst.

Gibt es Souveränität im Cyberspace? Da dies ein akademischer Vortrag und kein Mystery-Roman ist, werde ich nicht im Ungewissen lassen, wie ich diese Frage beantworte: Ich glaube, dass staatliche Souveränität im Cyberspace möglich ist; doch je gründlicher wir erfassen, was es erfordern würde, sie zu etablieren, desto klarer würden wir uns, dass sie nicht kompatibel ist mit dem Internet: Weder mit seinen technologischen Strukturen, noch mit den Normen und Vorteilen, die mit der bisherigen Internetentwicklung einhergehen. Man könnte also, zu einem hohen Preis und mit erheblichen Schwierigkeiten, Souveränität im Internet durchsetzen, aber dies würde auch das Internet, wie wir es kennen, zerstören. Auf der anderen Seite bringt die Ent-

1 Dieser Text wurde von Wolf J. Schünemann aus dem Englischen übersetzt.

wicklung des Internets zur Ausschöpfung seines vollen Potentials zwar eine Gefährdung und Einschränkung *nationaler* Souveränität mit sich, aber, so mein Argument hier, dadurch könnten wir eine neue Form demokratischer Souveränität erlangen.

2 Das Souveränitätskonzept in der Politikwissenschaft

Die nähere Betrachtung des Souveränitätskonzepts in der Politischen Wissenschaft kann von Max Webers berühmter Definition des Staates ihren Ausgang nehmen: „Staat ist diejenige menschliche Gemeinschaft, welche innerhalb eines bestimmten Gebietes – dies: das ‚Gebiet', gehört zum Merkmal – das Monopol legitimer physischer Gewaltsamkeit für sich (mit Erfolg) beansprucht" (Weber 1992: 6). Es ist diese Kombination von gewaltsamer Durchsetzungsmacht und Legitimität, immer beschränkt auf ein bestimmtes und gegebenes Territorium, das den Souverän ausmacht.

Beim britischen Politikwissenschaftler Robert Jackson heißt es: „Sovereignty is a foundational idea of politics and law that can only be properly understood as, at one and the same time, both an idea of *supreme* authority in the state, and an idea of the political and legal *independence* of geographically separate states" (Jackson 2007: x). Es geht also nicht allein um Autorität und Vorrang innerhalb eines Staates, sondern zugleich um Unabhängigkeit und Selbstbestimmung gegenüber anderen Staaten. Stephen Krasner (1999) unterscheidet dabei vier distinkte Typen von Souveränität:

1. „International legal sovereignty": die wechselseitige Anerkennung unter Staaten mit formaler juristischer Unabhängigkeit;
2. „Westphalian sovereignty": den Ausschluss externer Akteure von den staatlichen Ordnungsstrukturen innerhalb eines Territoriums und die Exklusivität politischer Institutionen;
3. „Domestic sovereignty": die Fähigkeit staatlicher Behörden zur Ausübung effektiver Kontrolle;
4. „Interdependence sovereignty": die Fähigkeit staatlicher Behörden Informationsflüsse, den Verkehr von Ideen, Gütern, Personen, Kapital etc. in das eigene Territorium und hinaus zu kontrollieren.

Mit Ausnahme der letzten beiden Typen, die ich nach gründlicher Überlegung im Wesentlichen für dasselbe halte, stimme ich mit dieser Typologie überein. Da in allen genannten Souveränitätsdefinitionen, das Staatsgebiet oder Territorium eine entscheidende Rolle spielt, möchte ich mich im folgenden Abschnitt auf die Betrachtung dieses Aspekts konzentrieren.

3 Souveränität und Territorialität

In Jacksons Definition sind Unabhängigkeit, rechtlicher Vorrang (Suprematie) und Territorialität aufeinander bezogen. Die logische Konsequenz ist, dass bindende Autorität durch eine geografische ‚Einschränkung' notwendig bedingt ist. Oder in den Worten

Jacksons: „a world based on state sovereignty is a world of mutually exclusive territorial jurisdictions; a world without overlapping jurisdictions" (Jackson 2007: 8).

Diese enge Verbindung von Souveränität und Territorialität scheint mir besonders interessant. Tatsächlich ist es schwierig, eine theoretische Grundlage für die notwendige Territorialität des Souveräns zu finden; vielmehr muss man auf pragmatische Erwägungen zurückgreifen. Wenn der Staat zum Beispiel über ein natürliches Monopol legitimer physischer Gewaltsamkeit verfügt, es also nur diesen einen Inhaber oberster Autorität über ein gegebenes Gebiet geben kann, warum sollte dann nicht die gesamte Welt eine einzige souveräne Regierung haben (können)? Wenn man die Antwort darauf in einer Gleichsetzung einer politischen Gemeinschaft mit einem linguistischen, ethnischen oder kulturellen Kollektiv, einem „Volk" sucht, macht man zwangsläufig die Erfahrung, dass solche Definitionen selten gelingen und niemals perfekt sind (Yuncker 2011). In einigen Fällen ergibt eine solche Reifizierung offensichtlich keinen Sinn. Die Vereinigten Staaten etwa sind nicht eine ethnische oder kulturelle Einheit. Umgekehrt gibt es mit Süd- und Nordkorea zwei Staaten mit einer ethnisch relativ homogenen Population. Zudem macht es das internationale System zunehmend schwieriger, die territorialen Grenzen nach ethnischen oder nationalen Unterschieden zu ziehen. Man könnte die Erklärung für die Territorialität auch mit Blick auf Kommunikationstechnologien und die damit verbundenen Kontrollmöglichkeiten suchen. In dem Maße, in dem unsere technischen Kontrollmöglichkeiten wachsen, lassen sich unter Umständen die Grenzen für territoriale Herrschaft ausweiten. Während dadurch Aufstieg und Bedeutung von großen politischen Systemen wie den USA, der EU oder Chinas erklärt werden können, würde dies doch nicht für die Persistenz vieler sehr kleiner Staaten und die Auflösung manch größerer Staaten und Imperien gelten. Diese Frage ist von großer Bedeutung, denn gerade die Spannung oder die Unvereinbarkeit zwischen dem ‚Internet-Territorium' und dem politischen Territorium bildet den Ausgangspunkt der aktuellen Debatte über ‚technologische Souveränität' oder die Souveränität im und über das Netz.

4 Volkssouveränität

Der Begriff der Volkssouveränität markiert einen radikalen Wandel im Souveränitätskonzept, der mit dem Aufkommen und der Entwicklung moderner Demokratien einherging. Er ist daher zentral für eine Analyse des Verhältnisses zwischen dem Cyberspace und dem Staat. In Jacksons Worten bricht die Volkssouveränität mit der Doktrin „that final authority rests with an individual or an oligarchy or some other segment of the population of a country" (Jackson 2007: 82) und legt die politische Autorität in die Hände „des Volks". Allerdings, so fügt Jackson hinzu, „the notion of popular sovereignty is not as straightforward as it might seem to be", denn „the people have to be called into existence by somebody". Damit sei das Volk in einer repräsentativen Demokratie „creatures of the constitutional arrangements of the state; they do not and cannot

exist on their own“ (ebd.: 92). Es kann nicht für sich selbst existieren. Es kann von sich aus kein politisches Gemeinwesen konstituieren, ohne konstitutionelle und demokratische Arrangements, die ihm die Macht geben, ein politisches Gemeinwesen zu konstituieren. Mithin kreiert sich ein demokratisches Gemeinwesen erst durch den Akt der längerfristigen Selbstbindung in einer Verfassung. Aber wie bringen wir Volkssouveränität mit politischer Autorität im Cyberspace in Einklang?

5 Souveränität ‚im' und ‚über den' Cyberspace

Der Begriff Cyber-Souveränität hat seit seiner ersten Nutzung eine 180-Grad-Wende vollzogen. In seinem Ursprungskontext sprachen vor allem diejenigen von Cyber-Souveränität, die dachten, der Cyberspace selbst sei souverän und solle auch weiterhin unabhängig vom Einfluss der Staaten bleiben, so wie z.B. John Perry Barlow in seiner Unabhängigkeitserklärung für den Cyberspace (Barlow 1996). In diesem Sinne definierte Timothy Wu (1997) Cyber-Souveränität als den Glauben, dass der „cyberspace ought not to be regulated, or is impossible to regulate“. Heutzutage werden Komposita aus „Cyber-“ („Daten-“, „Netzwerk-“ oder „technologische“) und Souveränität hingegen in der Regel von jenen gebraucht, die das Internet an die Grenzen und Regeln territorialer Staatlichkeit zurückbinden wollen. Doch selbst wenn wir so eine klassische Definition anwenden möchten, müssten wir meines Erachtens zwischen Souveränität *im* Cyberspace und Souveränität *über den* Cyberspace unterscheiden.

Mit einem Begriffsverständnis im Sinne von Souveränität im Cyberspace betrachten wir diesen als eine separate und distinkte Sphäre, eine virtuelle Welt und formulieren die Frage nach einem Äquivalent von Souveränität, das mit rein virtuellen Mitteln innerhalb dieses Raumes erreicht werden kann. Souveränität über den Cyberspace meint hingegen, dass die hergebrachten Souveräne aus der materiellen Welt ihre territorialstaatliche Souveränität auf den virtuellen Raum, d.h. auf die Sphäre von Computern, EDV-Geräten und Netzwerken übertragen oder verlängern können, sei es durch die Kontrolle der Akteure selbst oder sei es die Kontrolle ihrer technischen Anlagen und Standards.

Im Hinblick auf die Souveränität im Cyberspace stellt sich mithin die Frage, ob wir ein Äquivalent des Monopols legitimer physischer Gewaltsamkeit beobachten können. Das ist eine komplizierte Frage. Für das Internet als global vernetzten virtuellen Raum gilt zumindest theoretisch, dass jeder potentiell unbeschränkten Zugang zu jedem anderen im und am Netz hat. Und das gilt ungeachtet dessen, dass Netzwerke sich natürlich gegen Zugriffe von Dritten sichern können, etwa über Benutzerkonten und Passwörter. Worin soll aber der begrenzte „Raum“ bestehen, für den ein Staat ein Monopol der Gewaltsamkeit beanspruchen könnte? Wenn militärische Akteure davon sprechen, *ihren* Luftraum zu verteidigen, *ihre* Hoheitsgewässer oder *ihr* Land, dann wissen wir, was sie meinen. Wenn das US Cyber Command hingegen sagt, es verteidige *unseren* Cyberspace, wenn ein offizieller Bericht, erstellt vom Center for Strategic and In-

ternational Studies für Präsident Obama, vom Cyberspace als „a vital national asset" spricht (CSIS 2008: 1), aber auch wenn die russische Regierung behauptet, sie würde das „nationale Segment" des Internets verteidigen, ist mir nicht klar, was das bedeuten soll. Freilich gibt es Staaten und privatwirtschaftliche Akteure, die über mehr Cyber-Macht verfügen als andere. Wenn die NSA zum Beispiel eine Distributed-Denial-of-Service-Attacke (DDos) auf den von mir betriebenen Internet-Governance-Blog starten würden, hätten sie wahrscheinlich sehr schnell Erfolg, während ich mit einem Angriff auf das NSA-Datenzentrum in Utah vermutlich scheitern würde. Aber wem würden wir einen legitimen Gebrauch von DDoS-Attacken, Zero-day-Exploits oder Cyber-Sabotage zusprechen? Wir wissen in der Regel weder, ob die Gewalt, die im Internet ausgeübt wird, begrenzt ist, noch ob sie legitim ist. Im Hinblick auf Gewalt im Cyberspace macht Thomas Rid (2012) das treffende Argument, dass die Rede vom „Cyberkrieg" normalerweise die Gleichsetzung von Cyber-Fähigkeiten mit tatsächlicher physischer Gewaltsamkeit impliziert. Nehmen wir das prominente Beispiel Stuxnet: Anstatt die iranischen Urananreicherungsanlagen zu bombardieren, sabotierten wir sie über Netzwerktechnik.[2] Wenn es mithin so etwas wie Souveränität oder auch nur militärische Überlegenheit im Internet gibt, dann scheint damit keine Territorialität verbunden zu sein.

Im Hinblick auf die Souveränität über den Cyberspace stellt sich ebenso die Frage, wie sich staatliche Souveränität abbilden lässt. Wie sollte diese aussehen und wie funktionieren? Abgesehen von der Frage, ob sie möglich ist, stellt sich auch die Frage der Erwünschtheit. Wenn wir die Fähigkeit des Staates diskutieren, Souveränität über das Internet herzustellen, ist es zunächst wichtig klarzustellen, dass staatliche Souveränität nach klassischem Muster unabhängig von der Internetentwicklung durch eine Reihe anderer Faktoren, nicht allein das Internet, herausgefordert wird. Krasner zum Beispiel konstatiert für die von ihm definierten Souveränitätstypen eins und zwei, dass diese in der Geschichte regelmäßig verletzt worden seien; keiner von beiden erwies sich also als stabiles Gleichgewicht. Es gab vielmehr immer Akteure, die einen Anreiz verspürten, von der gegebenen Ordnung abzuweichen. Deswegen kann Souveränität nach Krasner bestenfalls als „organisierte Hypokrisie" (Krasner 1999) verstanden werden – politische Führer und Regenten binden sich an die Norm der Souveränität, wenn es ihnen Ressourcen und Unterstützung bietet, sie weichen davon bereitwillig ab, wenn der Normbruch ihnen Gewinne verspricht. Jüngere Forschungsliteratur zeigt zudem, dass die Typen drei und vier (domestische und Interdependenzsouveränität) zunehmend kontingent werden. Obwohl unter den Mitgliedern des Staatensystems ein wachsendes Interesse am Erhalt territorialer Integrität identifizierbar ist, wurde Staaten, die hinsichtlich der Souveränitätstypen drei und vier Schwächen aufwiesen, doch deutlich gemacht, dass ihre Souveränität bedingt sei und durch externe Kräfte miss-

2 Die Attribution von Cyberangriffen ist keineswegs trivial (vgl. Rid/Buchanan 2015). Für den Fall „Stuxnet" gibt es aber hinreichend eindeutige Indizien, die den Angriff staatlichen Akteuren westlicher Regierungen zuordnen (vgl. Lindsay 2013).

achtet werden könne, etwa im Namen der Schutzverantwortung, der Menschenrechte, der Nichtverbreitung von Massenvernichtungswaffen, der Terrorismusbekämpfung oder anderer transnationaler Angelegenheiten (Ramos 2013).

6 Die Debatte Souveränität vs. Fragmentierung

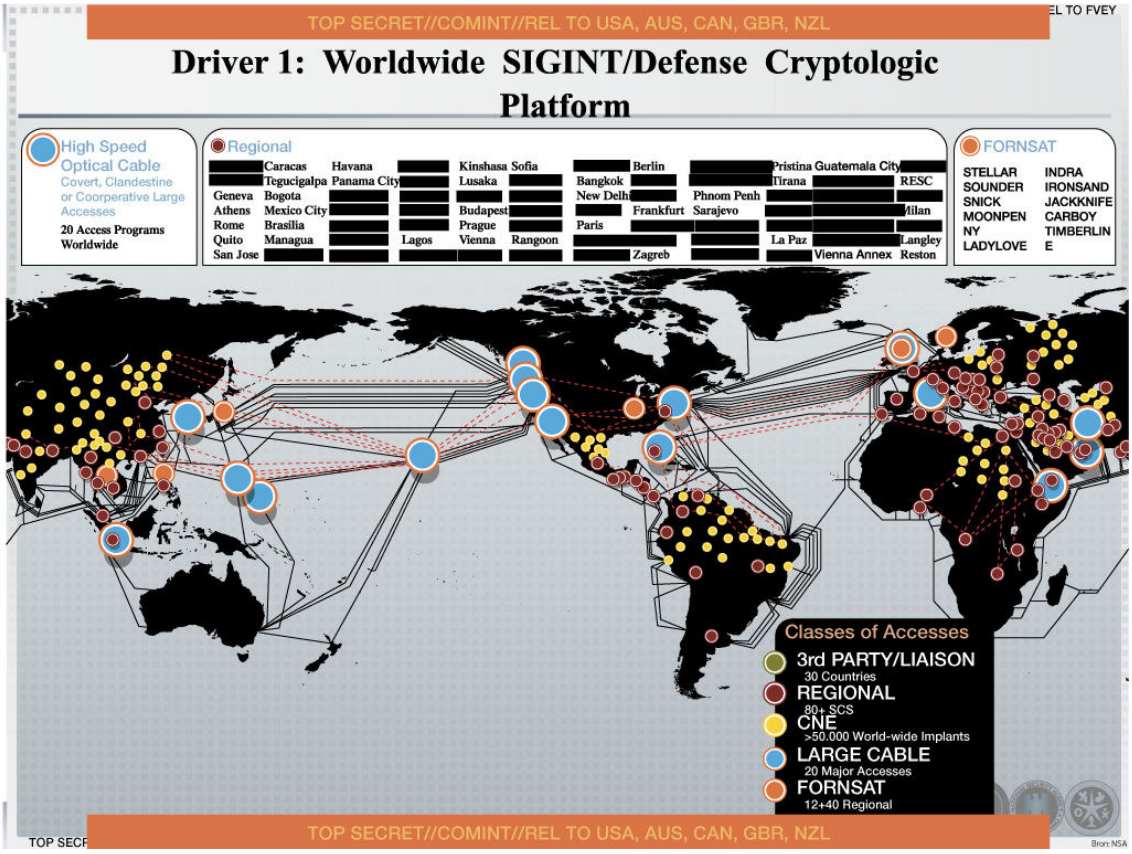
Das, was an den Snowden-Enthüllungen für viele schockierend war, ist doch, dass der Raum, der von den US-amerikanischen Sicherheitsbehörden als „ihr" zu schützender Cyberspace ausgegeben und konzipiert wird, keineswegs territorial begrenzt, sondern global ist. Die Karte in Abb. 1 stammt aus den von Snowden enthüllten Dokumenten. Sie zeigt die sog. Crypotologic Platform der NSA. Die gelben Punkte sind sogenannte Computer Network Exploitations (CNE). Dort sind die Techniker der NSA in Netzwerke eingedrungen, haben Trojaner installiert oder ähnliche Angriffe auf Netzwerke vollzogen, die im traditionellen Sinn nicht zu ihrem Handlungsbereich zählen. Man könnte nun einwenden, dass das nur ein Zeugnis davon ist, dass die US-amerikanische militärische Macht ohnehin globalisiert ist. Ein Blick auf Abb. 2 zeigt allerdings für die Computer Network Exploitations von China (blaue Punkte), genauer diejenigen mit dem Trojaner Hikit, auch ein transnationales Muster.

Die Snowden-Enthüllungen dieser globalisierten Expansion staatlicher Aktivitäten haben eine Debatte über Souveränität losgetreten, und die Bundesrepublik hat sich hier neben Brasilien als einer der stärksten Befürworter für so etwas wie technologische Souveränität ausgesprochen. Die Vertreter dieser „souveränistischen Linie", die sogenannten Souveränisten, denken, sie würden größere Kontrolle über Daten und das Internet gewinnen, aber können sie das wirklich? Wenn die NSA tatsächlich weltweit Spionage über Computernetzwerke betreiben kann, vorausgesetzt sie hat die Instrumente dafür, in welchem Ausmaß kann dann eine Erklärung über Datensouveränität tatsächlich irgendetwas schützen?

Wir können in der gesamten Debatte über Souveränität im Cyberspace einen positiven ‚Spin' mit Begriffen wie Datensouveränität, Netzwerksouveränität oder technologischer Souveränität beobachten, aber auch eine negative Betrachtungsweise derselben Phänomene und Lösungsansätze mit Konzepten wie Datensezession, Balkanisierung oder Fragmentierung. Die Fragmentierung ist hierbei eines der zentralen Argumente gegen staatliche Maßnahmen zur (Wieder-)Herstellung ihrer Souveränität. Allerdings müssen wir auch hier fragen, was Fragmentierung überhaupt bedeuten soll. Meint Fragmentierung etwa, dass ein Staat die Verbindung zum Internet auflöst? Zumindest für 99 Prozent der Zeit kann es das nicht heißen. Kein Staat möchte wirklich von der Welt abgekoppelt sein. Das als sog. „kill switch" bezeichnete regelrechte Abschalten des Internets von Seiten einer Regierung, mit den Beispielen Ägyptens, wo das Netz für mehrere Tage nicht verfügbar war, oder Venezuelas, dessen Regierung das Netz für einige Stunden gesperrt hat, – und das wäre Fragmentierung, wenn ein Netzwerk also gewissermaßen herunter gefahren wird – , ist nur in absoluten Ausnah-

mefällen angewendet worden, in legitimer Weise oder nicht. Ein anderer Weg echter Fragmentierung wäre die Entscheidung, TCP/IP nicht mehr zu nutzen, sondern ein eigenes Internetprotokoll zu entwickeln, das nicht kompatibel ist mit TCP/IP. Was meinen Sie, wie viele Akteure das tun (könnten)?

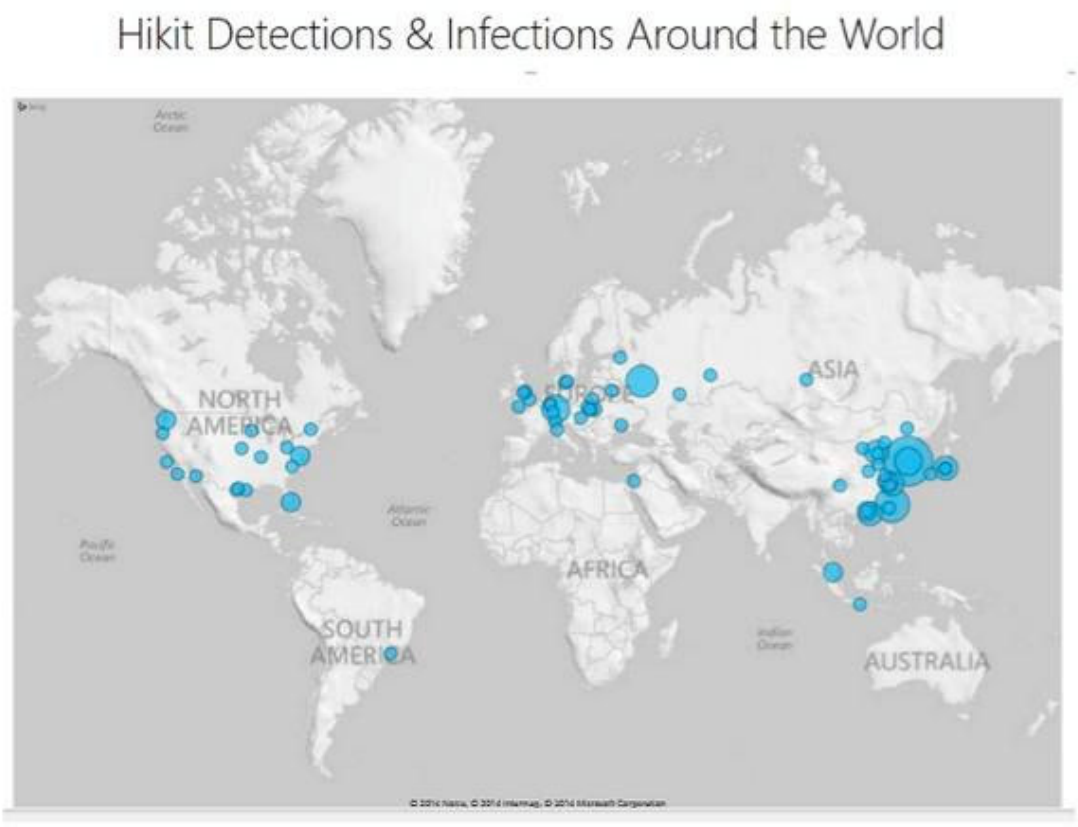
Abbildung 1: NSA-Dokument – Worldwide SIGINT/Defense Cryptologic Platform



Quelle: https://edwardsnowden.com/de/2013/11/23/worldwide-sigintdefense-cryptologic-platform/ (25.05.2015).

Auch auf staatlicher Ebene greift der sogenannte Netzwerkeffekt, d.h. die allerwenigsten Staaten könnten damit leben, vom eigentlichen, viel genutzten Internet abgekoppelt zu sein. Eine letzte Möglichkeit zur Fragmentierung bestünde in einer nationalen Positivliste, die autoritativ für den gesamten Internetverkehr des Landes Anwendung fände. Nicht einmal die Regierung der Volksrepublik China macht so etwas. Sie benutzen eine Negativliste, um Inhalte und Verkehr auszusperren. Allein die Pflege und Aktualisierung einer solchen Negativliste produziert aber einen erheblichen Aufwand, vom Aufwand, den eine Positivliste und ihre Fortschreibung mit sich bringen würde, einmal ganz zu schweigen.

Abbildung 2: Hikit Detections and Infections Worldwide



Quelle: Novetta Inc. 2014: 8.

7 Die wirklichen souveränen Einheiten des Internets

Neben den unterschiedlichen potentiellen Fragmentierungspfaden gibt es eine weitere, grundlegende Unklarheit in der Fragmentierungsdebatte: Was ist die eigentliche Kontrolleinheit, über die wir sprechen? Das Internet ist nie ein homogener und voll integrierter virtueller Raum gewesen und war auch niemals so angelegt. Stattdessen war es von Beginn an als Netzwerk der Netzwerke konzipiert und umgesetzt. Autonomes System (AS), so lautet der technische Begriff für die individuellen Netzwerke, welche die grundlegenden Einheiten dieses Netzwerks der Netzwerke bilden. Worin besteht dann aber der Paradigmenwechsel der Internettechnologie? In einer unbeschränkten Zahl von Netzwerken, in privater oder öffentlicher Hand. Anstelle einer von einer nationalen Behörde festgelegten Anzahl von Lizenzen für eine kleine Zahl von Diensteanbietern haben wir es hier mit einem offenen Standard zu tun, der von Anfang an globale Konnektivität für jeden versprach, der sich mit einem selbsterklärten Netzwerk anschließen wollte.

Es gibt heute etwa 50.000 registrierte AS-Nummern (ASN) für das Internet. Im Hinblick auf die Netzwerke ist also das AS die Einheit, die sich am ehesten analog zur ‚territorialen' Einheit fassen lässt, weil diese AS über vorrangige und exklusive Autorität darüber verfügen, wie das Gesamtnetzwerk funktioniert. Das AS besitzt übergeordnete

und exklusive Autorität innerhalb seines Routing-Bereichs. Es ist auch unabhängig von anderen AS. Die AS erkennen sich wechselseitig als Netzwerke an, etwa als Ursprung oder als Ziel eines Datenpakets. Autonome Systeme sind also die technischen und administrativen Einheiten, die Grenzen im Cyberspace bilden und definieren, wenngleich ihre Grenzen nicht geografisch, sondern virtuell oder logisch sind. Sie sind auch die Einheiten, die die Politiken bestimmen, nach denen der Eingang oder Ausgang von Datenpaketen über Grenzen hinweg geregelt wird. AS brauchen eine einzige Quelle für Routing-Entscheidungen. Diese Quelle muss einheitlich und exklusiv sein, so wie die autoritative Entscheidungsinstanz eines Souveräns. AS müssen einander wechselseitig anerkennen, wenn Interoperabilität ohne Konflikt oder Störung gegeben sein soll; sie kommunizieren miteinander über den gemeinsamen Gebrauch des BGP (Border Gateway Protocol), also des Protokolls für das Internet-Routing, sowie Peering-Vereinbarungen, die Beteiligung am Internetaustausch etc.

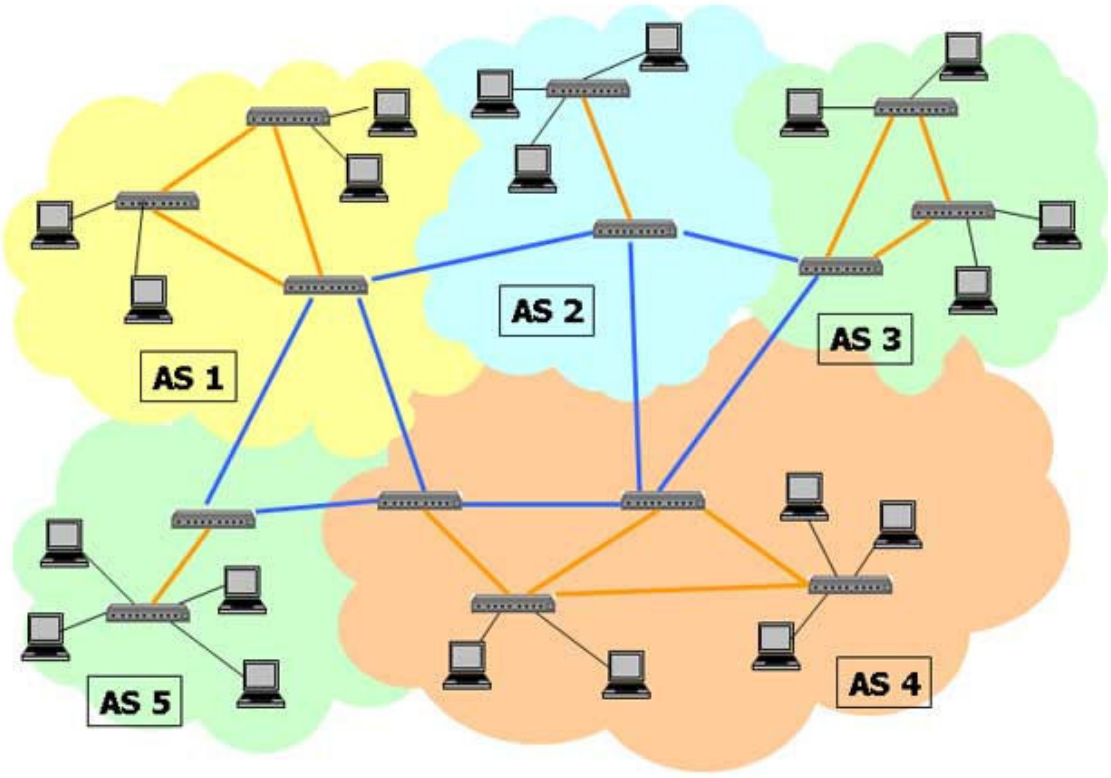
Auch wenn das Konzept des „kill switch", welches die Internetkonnektivität faktisch durch den Beschluss einer höheren Autorität vorübergehend aussetzt, noch darüber hinausgehen mag, so ist es im Regelfall das Autonome System, das „über den Ausnahmezustand entscheidet"(Schmitt 2009 [1922]: 13). Abb. 3 übertreibt die Analogie zur Staatenwelt insofern, als sie die AS territorial erscheinen lässt. Das hat aber nur mit den Anforderungen an eine zweidimensionale Grafik zu tun. AS sind nicht physisch territorial verfasst. Die zweite Karte (Abb. 4), die aus einer Netzwerkanalyse hervorgegangen ist, ist passender.

Wie lässt sich ein derartiger ‚Raum', ein Netzwerk mit dem Konzept der territorialstaatlichen Souveränität in Einklang bringen? Zwar könnten Staaten Souveränität herstellen, indem sie Autonome Systeme regulieren, aber diese erstrecken sich eben nicht zwingend nur innerhalb einer nationalstaatlichen Jurisdiktion. Schwieriger noch: Selbst ein lokales AS fungiert als Ziel- oder Ursprungsnetzwerk für globalen Kommunikationsverkehr. An einem bestimmten Punkt im Netzwerk zu *sein*, bedeutet, dass man irgendwo in der Welt *sein* kann.

Der Diskurs über die staatliche Souveränität im Internet ist buchstäblich eine Abkehr von der bisherigen Machtverteilung im Feld der Netzwerk- und Informationstechnologie. Die Kompetenzübertragung an individuelle Akteure und Märkte, die mit der Entstehung von AS, die über TCP/IP kommunizieren, einherging, wird relativiert und an staatlichen Hierarchien orientiert. Politische Souveränität auf den Cyberspace zu übertragen, würde in Extremform einen kompletten Isomorphismus bedeuten, also eine perfekte Angleichung zwischen den rechtlich gesetzten Grenzen des Nationalstaats und den operational definierten Grenzen des Autonomen Systems. Es würde die perfekte Integration der obersten Entscheidungsinstanz des Staates mit derjenigen des Autonomen Systems erfordern. Zu diesem Zweck wäre es nötig, den globalisierten virtuellen Raum, der auf der gemeinsamen Verwendung von TCP/IP-Protokollen basiert, mit nationalen Gateways und Verbindungspunkten nachzurüsten. Schließlich würde ein solcher Schritt bedeuten, die Anzahl der Autonomen Systeme von mehreren Zehn-

tausend ohne eingebaute Wachstumsgrenze und mit ungebremstem Wachstum auf etwa 200 zu begrenzen.

Abbildung 3: Autonome Systeme (AS) im Cyberspace



Quelle: eigene Darstellung.

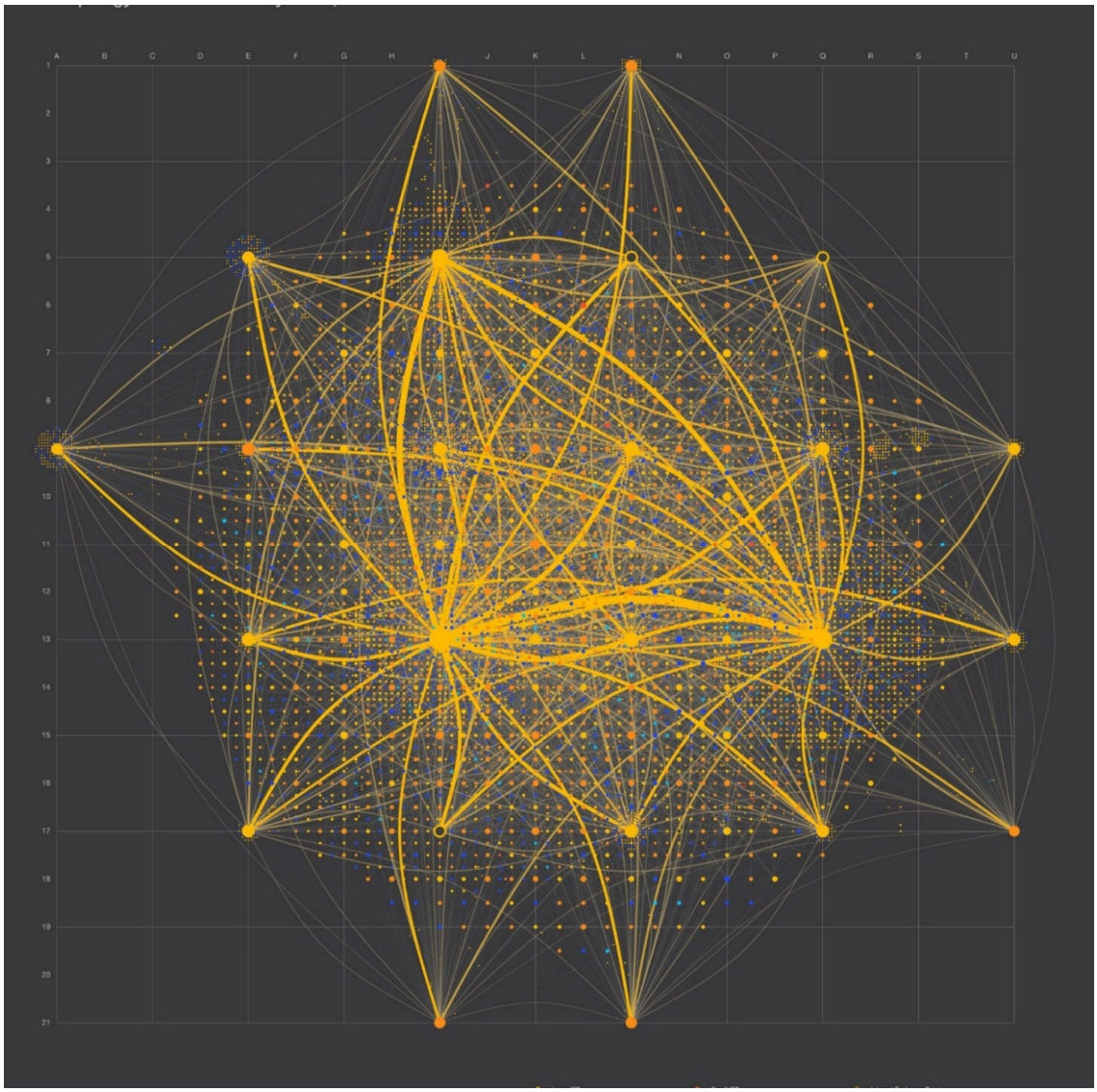
Auch muss der Staat, wenn er das Autonome System in seine Strukturen integriert hat, in der Lage sein, seine Politiken gegenüber allen Nutzern seines nationalen Netzwerks durchzusetzen. Diese Kontrolle hängt dabei nicht nur vom Netzwerkzugang ab, sondern von allen Geräten, dem Betriebssystem und den Programmen, die die Nutzer anwenden.

Ferner ist auch im Hinblick auf die Kontrolle der Datenströme festzuhalten: „Tracking all copies of data, without total control of the network, is a […] very hard problem“, wie es in einem aktuellen Forschungspapier ausgedrückt ist (Peterson et al. 2011). Das Papier behandelt die Schwierigkeiten und Unzulänglichkeiten der Geolokationsbestimmung von IP-Adressen und fügt hinzu:

> „Beyond the limitations of geolocating an IP address, there currently exist no techniques that effectively (let alone securely) bound the geographical location of some data stored in the cloud. […] A class of related technologies – which we describe collectively as provable data possession (PDP) – can be used to efficiently audit remote data stores, without requiring the client or the server to retrieve the entire file. PDP, however, only provides proof of the existence of data, not its location“ (Peterson et al. o.J.).

Das entscheidende Argument ist hier, dass, wenn das ganze System darauf angelegt ist, dass sich die Daten darin bewegen können, sich vielleicht allenfalls dann ermitteln lässt, dass Daten sich innerhalb eines bestimmten Rechtsgebiets befinden, aber nicht, ob sie sich nicht auch schon außerhalb des Systems bewegt haben und vielleicht 700 Kopien irgendwo anders in der Cloud bestehen.

Abbildung 4: Einheiten des Cyberspace – Netzwerkdarstellung



Quelle: Peer1 Hosting (2011).
Goldener Punkt: großer Internet Service Provider (ISP)/Autonomes System (AS); orangener Punkt: kleiner ISP/AS; leerer Kreis: Internet Exchange Point (IXP); blauer Punkt: Organisationsnetzwerk (etwa Universitäten); roter Punkt: Network Information Center.

Zuletzt würde ich auch die Idee infrage stellen und ablehnen, dass besserer Datenschutz und informationelle Privatsphäre in einer global vernetzten Welt durch die Wiederherstellung oder Akzentuierung territorialer rechtlich-politischer Strukturierung erreicht werden könnte. Es gibt keine Inseln im Internet. Datenschutzkonzepte müssen, sofern sie öffentliche und nicht private Politiken begründen wollen, im Wettstreit

divergenter Vorstellungen bestehen, um dadurch Deutungshoheit und Anwendung im gesamten Cyberspace zu finden. Es sollte also nicht versucht werden, isolierte Brückenköpfe in einem fragmentierten Netz zu etablieren, wenngleich es schon jetzt fragmentierte Räume innerhalb des Cyberspace gibt: So finden wir sie bspw. auf operativer Ebene, d.h. innerhalb eines bestimmten AS. Der einzige sichere Weg nationale Regeln des Privatsphären- und Datenschutzes innerhalb eines AS effektiv durchzusetzen bestände darin, dessen Konnektivität dramatisch einzuschränken, wenn nicht gar komplett vom Datenfluss mit anderen AS abzuschneiden.

8 Fallstudie: Country code Top-level-domains (ccTLD)

In diesem Abschnitt möchte ich mich einem konkreten Beispiel für die Schwierigkeiten im Verhältnis zwischen staatlicher Souveränität und dem Cyberspace zuwenden: dem Fall der Country code Top-level-domains (ccTLD). Diese länderspezifischen Domänen zeigen einen sehr interessanten Nexus zwischen traditionellen Konzepten von Souveränität und dem globalen Internet auf.

Der Ursprung der ccTLDs geht auf eine Anfrage für länderspezifische Top-level-Domains von Seiten Großbritanniens im Jahr 1984 zurück. Jon Postel, der das Domain-Name-System (DNS) vor Etablierung der ICANN 1998 autoritativ verwaltete, hatte in der Gründungsphase des Domain-Name-Systems lediglich sieben generische Top-Level-Domains vorgesehen (etwa .org, .com., .gov). Dennoch ging Postel auf den Wunsch Großbritanniens ein, eine nationale TLD einzurichten. Allerdings wollten Postel und seine Mitstreiter nicht darüber entscheiden, welche Staaten Anspruch auf welche Top-Level-Domains hatten, und welche Antragsteller überhaupt als Staaten zu werten seien. Um sich also vor unangenehmen (politischen) Entscheidungen zu bewahren, griff er auf einen externen Standard zurück, um zu definieren, was als Staat im Raum der Domainnamen anerkannt werden konnte, nämlich die ISO-Kodierliste (ISO-3166)[3] mit Codes aus zwei Buchstaben für geografische Einheiten. Vor dieser Entscheidung waren ccTLDs auch noch an Vertreter vergeben worden, die Postel aus globalen Wissenschafts- und Forschungsnetzwerken kannte. Während bei diesen Vergabeverfahren im Regelfall eine Verbindung zu einem Territorium, zumindest einem Aufenthaltsland bestanden hatte, hat die Vergabepraxis damals eigentlich keine Verbindung zum Staat oder politischen Gemeinwesen per se. Nationale Regierungen wussten in der Mitte der 1980er Jahre nichts von Internet-Domains oder sie interessierten sich nicht dafür. Wenngleich die Kartografie der ISO-3166-Liste im Hinblick auf die nationalstaatlichen Territorien ebenfalls nicht perfekt war, hatten Postels Vergabepraktiken eine rein semantische Kopplung vom Raum der Domain-names und dem ‚Territorium' hergestellt. Die Betonung liegt hierbei auf semantisch im Gegensatz zu real.

Postel hinterließ uns also ein gemischtes Vergabesystem, in dem ccTLDs ursprünglich privaten Akteuren übertragen waren, die meisten aus dem wissenschaftlichen

3 Liste findet sich in der Wikipedia: https://de.wikipedia.org/wiki/ISO-3166-1-Kodierliste (24.5.2015).

Non-Profit-Bereich oder aus Forschungsnetzwerken, einige darunter aber auch Unternehmer. Als das Internet allerdings Mitte der 1990er Jahre an Bedeutung, vor allem als wirtschaftlicher Raum, gewann, entdeckten es auch die Regierungen für sich und zeigten Interesse daran, wer die Vergabe der ccTLDs, die für die nationale Gemeinschaft im Cyberspace stehen, kontrolliert. Postel veröffentlichte 1994 das RFC 1591 (Request for comments)[4], um diese Probleme anzugehen. Darin findet sich das Konzept dualer Treuhänderschaft beschrieben. Gemeint ist damit, dass der Inhaber der ccTLD als Treuhänder nicht nur für die nationalstaatliche Gesellschaft, sondern zugleich auch für die globale Internetgemeinde fungiert. Die zentrale Autorität für die Vergabe der ccTLDs wurde bei Jon Postel bzw. der IANA verortet.

Zudem begannen Regierungen, die Souveränität über Territorien beanspruchen konnten, und die in der ISO-Liste enthalten waren, wie etwa diejenige der Isle of Man in der Irischen See (.IM), die entsprechenden Domains zur Verwaltung anzufordern. Bis ins Jahr 2000 kam so ein buntes Mischsystem zustande, einige ccTLDs waren in privater Hand, andere wurden von Regierungen gehalten und verwaltet. In den 2000er Jahren erhielten die Staaten mit dem Governmental Advisory Committee (GAC) sogar eine institutionelle Vertretung im Rahmen der ICANN. Sie wurden also Mitentscheider im Prozess um die TLDs, allerdings waren es auch weiterhin die US-Regierung und die ICANN, die als zentrale und autoritative globale Entscheidungsinstanzen im Endeffekt über die Domain-Vergabe entschieden.

Dementsprechend heißt es im Prinzipienkatalog der US-amerikanischen NTIA: „We own the root and intend to hang on to it“ (U.S. Commerce Department NTIA 2005). Allerdings fand mit dem World Summit on the Information Society (WSIS) 2005 auch die folgende Formulierung Eingang in das Abschlussdokument, wonach Regierungen „legitimate interest in the management of their country code top level domains (ccTLD)“ haben. Weiter lautet es hier:

> „The United States recognizes that governments have legitimate public policy and sovereignty concerns with respect to the management of their ccTLD. As such, the United States is committed to working with the international community to address these concerns, bearing in mind the fundamental need to ensure stability and security of the Internet's DNS.“

Wir sehen also einen hierarchischen Souveränitätsanspruch über die ccTLDs, wobei die USA gewissermaßen die Souveränität über das globale DNS letztinstanzlich für sich beanspruchen, aber davon abgeleitet den übrigen Staaten partielle Souveränität über ihre ccTLDs zugestehen. Um es an dieser Stelle aber noch einmal klarzustellen: Die Verbindung zwischen einer ccTLD und einem staatlichen Territorium ist rein semantisch. Es gibt keine andere Verbindung dazwischen als die sprachlich-referentielle. Die „root“ ist nicht in einem Land, der Name, „.cn“, „.de“, ist nicht der Handelsname eines Landes.

4 Abrufbar unter: https://www.ietf.org/rfc/rfc1591.txt (24.05.2015).

Die Frage einer hierarchischen Souveränität im Cyberspace führt natürlich zum spannenden Thema in der internationalen Internet Governance in diesem Jahr: der Übertragung der sog. IANA-Funktionen. Die USA haben die globale ‚Souveränität' über das Domain-Name-System, also die Verwaltung der Nummern und Namen im Internet. Sie führen sie über ihre Verträge mit der ICANN sowie dem privatwirtschaftlichen Unternehmen Verisign aus. Verisign veröffentlicht die Domainnamen und ICANN verwaltet die Root-Zone-Datei. Zwar bestimmt ICANN, welche Domainnamen existieren. Die mittelbare, unilaterale Kontrolle des DNS durch die USA widerspricht aber dem klassischen Konzept völkerrechtlicher Souveränität. Wenn beispielsweise der Iran eine Änderung des Beauftragten für seine ccTLD wünscht, muss es zu einer Institution mit vertraglicher Bindung an die US-amerikanische Regierung herantreten und in letzter Konsequenz die Zustimmung der US-amerikanischen Regierung erhalten, um diesen Wechsel zu vollziehen. Das steht also in einer Spannung zum Grundsatz völkerrechtlicher Souveränität. Zur gleichen Zeit verletzt die US-Regierung aber auch ihre politische Selbstverpflichtung auf eine privatwirtschaftlich betriebene Multistakeholder-Governance des Internets hinzuwirken. Einerseits behauptet die US-Regierung, man bräuchte keine Regierungen, keine UN, keine ITU, um das Internet zu regieren. Andererseits wird die eigene Stellung im DNS davon ausgenommen: Wir haben ein Recht und Befugnis, diese Angelegenheiten zu regeln, und niemand sonst hat diese Rechte. Das ist natürlich eine sehr widersprüchliche Position. Als Reaktion auf die Snowden-Enthüllung haben die USA nun versprochen, ihre dominante Rolle in diesem Feld aufzugeben und die IANA-Funktionen an das Multistakeholder-System zu übertragen. Dieser Prozess ist aktuell im Gange und es gibt sehr viele, auch manche widersprüchliche Informationen hierzu von den beauftragten Stellen und Gremien.[5]

9 Schlussbetrachtung

Wenn Souveränität im Cyberspace bedeuten soll, dass wichtige Strukturen und Kontrollparameter des Internets den nationalstaatlichen Strukturen anzugleichen sind, dann halte ich das aus normativer Perspektive für eine katastrophale Idee. Ich vermute, dass die Leute, die in Bezug auf Informationstechnologien von Souveränität sprechen, nicht besonders gründlich über die Auswirkungen entsprechender Reformbemühungen nachgedacht haben. Souveränität über den Cyberspace bedeutet nicht allein die Territorialisierung der Netzwerkprotokolle und -operationen in einer Weise, die ihrem technischen Design, ihrem wirtschaftlichen und sozialen Potential in diametraler

5 Informationen zu und von der IANA Stewardship Coordination Group: https://www.icann.org/stewardship/coordination-group (25.5.2015); Prozesse zur Ausarbeitung von Vorschlägen in den Bereichen: a) Names (CWG-IANA): https://community.icann.org/x/37fhAg (25.5.2015); b) Numbers (CRISP): https://www.nro.net/nro-and-internet-governance/iana-oversight/consolidated-rir-iana-stewardship-proposal-team-crisp-team (25.5.2015); Protocols (IETF IANAPlan working group): http://www.ietf.org/iana-transition.html (25.5.2015). Interventionen des US-amerikanischen Kongresses: http://www.internetgovernance.org/2014/12/12/u-s-congressman-in-the-middle-attack-on-iana-transition/ (25.5.2015).

Weise entgegensteht. Vielmehr würde ein solcher Schritt – um wirklich effektiv zu sein – ebenfalls erfordern, eine nationale Zertifizierung von Hardware und Software vorzunehmen. Denn es könnten ja Cybersicherheitsprobleme bestehen, wenn chinesische Hardware in US-amerikanischen Systemen eingebaut wäre, und umgekehrt könnte es aus Sicht der chinesischen Regierung problematisch sein, US-amerikanische Hard- und/oder Software zu verwenden. Alle generischen Top-Level-Domains müssten aufgegeben werden. Domaininhabern müsste es untersagt werden, Domains mit in unterschiedlichen Rechtsräumen befindlichen Systemen zu besitzen. Im Ergebnis müssten in die gesamte Wertschöpfungskette informationeller Güter und Dienstleistungen nationale Strukturen eingezogen und somit auch 30 bis 40 Jahre der Globalisierung und Liberalisierung rückgängig gemacht werden.

Gibt es also Souveränität im Cyberspace? Nein, nicht wirklich. Der Cyberspace ist ein neuer Raum, und dort gibt es viele transnationale Streitfragen und Konflikte. Gibt es Souveränität über den Cyberspace? Nein, offensichtlich nicht. Sollte es Souveränität über den Cyberspace geben? Es ist im Vorangegangenen hoffentlich deutlich geworden, dass ich nicht behaupten möchte, Cyber-Souveränität sei gänzlich unmöglich, sondern dass sie im eigentlichen wie im übertragenen Sinn einen sehr hohen Preis hätte – und deshalb alles andere als wünschenswert wäre. Die potentiellen Gewinne – außer der Tatsache, dass Staaten ihre Kontrollmöglichkeiten verbessern – sind die Kosten und Opfer aus meiner Sicht nicht wert.

Zuletzt soll noch die Frage nach einer möglichen Alternative behandelt werden. Ein besserer Weg wäre es aus meiner Sicht, die ursprüngliche Idee von Cyber-Souveränität zu neuem Leben zu erwecken. Es ist eben nicht so, dass der Cyberspace nicht reguliert werden könnte. Doch er kann es nur als unabhängiger, autonomer Raum mit genuinen Governance-Strukturen und -Prozessen. Warum betrachten wir daher nicht die globale Internetgemeinde als ein politisches Gemeinwesen? Warum versuchen wir nicht, politische Strukturen und Governance-Arrangements zu schaffen, die dieses Gemeinwesen betreffen und vertreten? Wozu dient die Bindung an kleinere territorialstaatlich verfasste Einheiten, wenn es ein globaler Raum ist, den es zu regieren gilt?

Volkssouveränität besagt im Wesentlichen, dass politische Herrschaft und Autorität nur dann legitim sind, wenn sie auf dem Einverständnis der Beherrschten beruhen. Mit diesem Prinzip lassen sich sogar Eingriffe in die nationale Souveränität legitimieren, nämlich insofern, als Menschen und Völker nicht ihre eigenen Rechte entäußern können.

Es liegt mithin nichts Verrücktes oder Problematisches in der Vorstellung einer Internetgemeinde als politischem Gemeinwesen. Vielmehr stellt das Internet tatsächlich die mediale Plattform für eine Gemeinschaft mit eigenen Interessen, einer entstehenden Identität, eigenen Normen und Werten, und schließlich neuen Formen des Zusammenlebens dar. Und es ist nur ein kleiner Schritt von einem Gemeinwesen zu einer Nation, denn eine Nation ist nichts anderes als ein Gemeinwesen, das seinen eigenen Staat fordert. Folglich ist die Frage gar nicht von großer Bedeutung, ob die existieren-

den Souveräne machtvoll genug sind, um der Internetgemeinde ihre Regeln aufzuzwingen. Worauf es wirklich ankommt, ist, ob die Internetgemeinde so organisiert werden kann, dass sie in der Lage ist, ihre Unabhängigkeit zu erklären und zu erlangen.

Es sind Verfassungen, die Volkssouveränität möglich machen. Auch das Internet hat eine globale Verfassung: die Protokollstandards und die organisch entwickelten Institutionen der Internet Governance.

Literatur

Barlow, John Perry (1996): A Declaration of the Independence of Cyberspace, 07.08.2004, https://projects.eff.org/~barlow/Declaration-Final.html (13.03.2015).

Jackson, Robert H. (2007): Sovereignty. Evolution of an idea, Polity: Cambridge.

Krasner, Stephen D. (1999): Sovereignty. Organized hypocrisy. Princeton University Press: Princeton, N.J.

Mueller, Milton L. (2010): Networks and states. The global politics of internet governance, MIT Press (Information revolution and global politics): Cambridge, Mass.

Novetta Inc. (2014): Operation SMN: Axiom Threat Actor Group Report, https://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf (18.06.2015).

PEER 1 Hosting (2011): The Internet - Topology of Autonomous Systems. PEER 1 Hosting, http://www.peer1.com/map-of-the-internet-infographic (25.06.2015).

Peterson, Zachary N.J. / Gondree, Mark / Beverly, Robert (2011): A Position Paper on Data Sovereignty: the importance of geolocating data in the cloud, http://znjp.com/papers/peterson-hotcloud11.pdf (07.07.2015).

Rid, Thomas (2012): Cyber War Will Not Take Place, in: Journal of Strategic Studies 35:1, 5–32.

Schmitt, Carl (2009 [1922]): Politische Theologie. Vier Kapitel zur Lehre von der Souveränität, Duncker & Humblot: Berlin.

U.S. Commerce Department NTIA (2005): U.S. Principles on the Internet's Domain Name and Addressing System, http://www.ntia.doc.gov/other-publication/2005/us-principles-internets-domain-name-and-addressing-system (18.06.2015).

Weber, Max (1992): Politik als Beruf, Reclam (Universal-Bibliothek, 8833): Stuttgart.

Wu, Timothy: Cyberspace Sovereignty? The Internet and the International System, in: Harvard Journal of Law and Technology, 10:3 (Summer 1997), 647–666.

Yuncker, James A. (2011): The Idea of World Government: From ancient times to the twenty-first century, Routledge: New York.

Autor

Prof. Milton L. Mueller
Georgia Institute of Technology
School of Public Policy
685 Cherry Street
Atlanta, GA 30332 USA
milton.mueller@pubpolicy.gatech.edu

DOI: 10.11588/josar.2015.0.23483

Wer besteuert das Internet? Die Steuersparmodelle von Amazon, Google & Co. als juristische Reformimpulse

Ekkehart Reimer

1 Einführung

1.1 Das Problem

Warum zahlen wir unentrinnbar unsere Steuern, während Unternehmen das umso weniger tun, je größer, globalisierter und virtualisierter sie sind? Oder kürzer: Uns besteuert der Staat. Aber wer besteuert das Internet? Ob man das Problem wirklich so formulieren darf, ob also die in der Frage transportierten Thesen stimmen und wie diese Frage ggf. zu beantworten ist, ist Gegenstand der nachfolgenden Darstellung.

Vorab ist klarzustellen, dass es bei der Besteuerung des Internets nicht generell um das Problem einer Minderbesteuerung geht, die unvermeidlich auftritt, nur weil jemand im Internet und durch das Internet Geld verdient; darauf wird gleichwohl noch zurückzukommen sein. Problematisch sind aber die Grenzüberschreitungen in klassisch-territorialer Hinsicht, genauer: die Kumulation von Virtualisierung und Globalisierung. Das Problem globaler Minderbesteuerung stellt sich hier umso mehr und umso drängender, je weniger fassbar die unternehmerische Geschäftstätigkeit oder jedenfalls die Geheimnisse ihres Erfolgs sind. So hat wohl noch niemand das Original des angeknabberten Apfels in der Hand gehabt, denn dieses Original gibt es gar nicht. Doch wir zahlen viel Geld, um ein Telefon zu kaufen, das dieses Symbol zeigt. Auf immateriellen geistigen Schöpfungen beruht also reale Wertschöpfung. Wenn sich das Steuerrecht darauf einlässt (was es muss), dann wird es zugleich anfällig für Verträge oder Gestaltungsmodelle, die auf weiteren immateriellen Vorgängen aufbauen: auf der Schöpfung und Verlagerung von geistigem Eigentum, Marken, good-will, unternehmerischen Chancen und Risiken. Das ist alles nur sehr schwer zu fassen und zu bewerten – es sind eben geistige Schöpfungen (*intellectual property*, IP), aber sie haben Konsequenzen für die reale Wertschöpfung und damit für ein modernes Steuerrecht postindustrieller Gesellschaften.

1.2 Die Steuer: Ein Kind des Rechts in interdisziplinärer Diagnostik

Mit der Steuer partizipiert der moderne Staat am Erfolg privaten Wirtschaftens. Dieser Lehrsatz ist zentral für den akademischen Unterricht. Er ist historisch tief verankert, hat aber auch eine normative Seite: Hier gründet er in den Wirtschaftsgrundrechten, etwa den Artikeln 14 Abs. 1, 12 Abs. 1 und 2 Abs. 1 des Grundgesetzes. Um die Grund-

rechte bestmöglich zur Geltung zu bringen, verzichtet der Staat darauf, seinen Bedarf anders als (nur) durch Abgaben zu decken. Zentrales Steuerungsmittel für die Steuern ist ebenfalls – wie so oft – das Recht.

Die Fragen, wer wie das Internet besteuert, lassen sich deshalb mehr als nur annäherungsweise durch Einblick in Gesetze, unionale Richtlinien und völkerrechtliche Verträge, also mit den etablierten juristischen Methoden beantworten. Nur sehr eingeschränkt lässt sich mit juristischen Methoden dagegen beobachten, ob das Recht auch beachtet wird, und noch schwieriger ist es für Juristen, die Frage zu beantworten, ob das Recht auch sinnvoll ist. Hier ist die multidisziplinäre Perspektive unabdingbar, wie sie in diesem Band eingenommen wird. Das gilt gerade in einem Sachbereich wie dem Steuerrecht, in dem unterschiedliche Wissenschaften unterschiedliche, aber durchgehend wertvolle Einsichten beitragen.

Immerhin wissen aber das Recht und die Rechtswissenschaft um die Verletzlichkeit des Rechts. Mit juristischen Mitteln lässt sich nachzeichnen und analysieren, wann und wie das Recht aus dem Lot gerät. Juristen sehen, wie alte Normen auf neue Paradigmen der ökonomischen Wertschöpfung reagieren, und sie können den Erfindungsreichtum und die Sorgfalt kundiger Berater nachvollziehen, die Lücken des geltenden Rechts identifizieren, die ihre Mandanten vor vermeidbaren Steuerbelastungen schützen und die damit zugleich den Anlass für Nachjustierungen des geltenden Rechts setzen.

1.3 Gang der Untersuchung

Die nachfolgende Darstellung skizziert zunächst kurz die Grundstrukturen und Determinanten des Steuerrechts in der elektronischen Welt (0). Auf diesen normativen Teil folgt ein harter Schwenk auf die Wirklichkeit: Vorgestellt werden typische Bauelemente, sog. Steuersparmodelle. Dabei ist zu fragen, wie v.a. die global operierenden Internetunternehmen zu einer erheblichen Senkung ihrer Steuerbelastung gelangen (0). Darauf baut eine Art Synthese auf: Sie behandelt die Frage, wie sich die Probleme bewältigen lassen, was sinnvolle Ziele und inhaltliche Strategien einer Steuerpolitik für das Internet wären. Vor allem aber: „Wer besteuert das Internet?“ Wer sind die maßgeblichen Akteure? Von welchen Institutionen können wir eine Abhilfe der Probleme erwarten, die zuvor deutlich geworden sind, und welche Verfahren und Handlungsformen können diese Akteure wählen (0)?

2 Grundstrukturen: Das Steuerrecht der elektronischen Welt

2.1 Virtualisierung ohne Globalisierung

Vor 15 Jahren waren viele führende Praktiker des Internationalen Steuerrechts und die sie beobachtenden und begleitenden Wissenschaftler fast durchgehend der Auffassung, die Nutzung des Mediums Internet an sich sei steuerrechtlich bereits hochproblematisch. Die Besteuerung des E-Commerce wurde zum Modethema, und manches

klang wie die ärztlichen Warnungen vor zu hoher Geschwindigkeit, als 1835 der „Adler“ schnaufend von Nürnberg nach Fürth raste. Heute ist klar, dass Steuern auch schuldet, wer über Internet-Plattformen handelt, das Manuskript eines literarischen Bestsellers per E-Mail an den Verlag schickt, bei einer Direkt-Bank online Geld anlegt und dafür Zinsen erhält, wer eine Sportwette im Internet abschließt oder wer Bitcoins kauft und sie einige Monate später mit Gewinn wieder veräußert. Schwierigkeiten gibt es gelegentlich noch im Bereich der Umsatzsteuer, aber auch sie sind lösbar.

Heute sind die Schwierigkeiten der Besteuerung des E-Commerce in rein innerstaatlichen Sachverhalten fast vollständig überwunden. Das Internet ist ein Medium, das auch die Finanzverwaltung im Interesse einer effizienten Datenerhebung und damit im Interesse der Gleichmäßigkeit der Besteuerung erfolgreich nutzt. Das Internet ist also im rein innerstaatlichen Fall für sich genommen kein Problem. Man kann also sagen: In diesem ersten Fall – Virtualisierung ohne Globalisierung – ist das Steuerrecht vollständig in der Spur, wir haben keine Angst mehr vor Hochgeschwindigkeit.

2.2 Globalisierung ohne Virtualisierung

Komplementär dazu gilt der zweite, nun etwas ausführlichere Blick der Globalisierung ohne Virtualisierung: Wie reagiert das staatengebundene Steuerrecht traditionell auf das staatenübergreifende, d.h. real grenzüberschreitende Wirtschaften? Wie werden internationale Kapitalströme besteuert?

2.2.1 Parlamentarische Gesetzgebung als Zentrum steuerlicher Normsetzung

Das Internationale Steuerrecht, das hiermit angesprochen ist, beruht weiterhin in erster Linie auf den nationalen Belastungsgesetzen (in Deutschland also etwa dem Einkommensteuergesetz, dem Körperschaftsteuergesetz, dem Umsatzsteuergesetz oder dem Erbschaftsteuergesetz), die parlamentarisch legitimiert sind und die das Parlament auch jederzeit wieder ändern kann.

Darüber hinaus haben wir es aber mit einer Vielfalt weiterer Rechtsquellen zu tun. Zu nennen sind zunächst eine Reihe innerstaatlicher Normen, die die Regelungen ergänzen, die die Stammgesetze für grenzüberschreitende Sachverhalte treffen. So gibt es in Deutschland mit dem Außensteuergesetz (AStG) von 1973 ein Querschnittsgesetz, das eine Reihe unliebsamer oder missbräuchlicher Gestaltungen aufgreift, in denen die Grenzüberschreitung an sich zu niedrigeren steuerlichen Gesamtbelastungen geführt hätte. Der AStG-Gesetzgeber bemüht sich hier um eine Inlands-Auslands-Neutralität, d.h. um die Aufrechterhaltung des Belastungsniveaus, das für den reinen Inlandsfall gegolten hätte, auch für den grenzüberschreitenden Fall. Hier finden sich deshalb Regelungen über die Anpassung unangemessener Konzernverrechnungspreise, unrealistischer Gewinnaufteilungen zwischen inländischem Stammhaus und Auslandsbetriebsstätten in grenzüberschreitend tätigen Einheitsunternehmen (§ 1 AStG), die Fortdauer einer sog. „erweiterten beschränkten Steuerpflicht“ nach dem Wegzug deutscher

Staatsbürger in Niedrigsteuerländer (Hierzu instruktiv: Stahl 2013), die Besteuerung stiller Reserven großer Aktienpakete bei einem Wegzug des Anteilseigners in das Ausland (§6 AStG), aber auch die sog. Hinzurechnungsbesteuerung, durch die zwischengeschaltete passive Auslandsgesellschaften, mit denen inländische Investoren ihre Auslandsgewinne vor dem deutschen Fiskus abschirmen, diese Abschirmwirkung verlieren (§§ 7–14. AStG).

2.2.2 Unionsrecht

Daneben spielen in der grenzüberschreitenden Besteuerung Normen des europäischen Rechts eine wichtige Rolle (Überbick: Schaumburg/Englisch 2015). Die Mehrwertsteuer, die in Deutschland traditionell Umsatzsteuer heißt, ist seit dem großen Systemwechsel von 1968 in der ganzen EWG harmonisiert (anschaulich: Storbeck 2006). Seit 1990 treten Teilregelungen für das Recht der Konzernbesteuerung hinzu: zunächst für die Besteuerung grenzüberschreitend gezahlter Dividenden bei verbundenen Unternehmen (Mutter-Tochter-Richtlinie), nach 2000 zusätzlich für die steuerliche Behandlung konzerninterner Zinsen und Lizenzgebühren (Zins-Lizenzgebühren-Richtlinie) und für die steuerliche Behandlung von Umstrukturierungen (steuerliche Fusions-Richtlinie). Diese materiellrechtlichen Regelungen werden durch zwei verfahrensrechtliche Richtlinien flankiert; sie erlauben und gebieten den zwischenstaatlichen Informationsaustausch (Amtshilferichtlinie) und die grenzüberschreitende Vollstreckung von Steuerforderungen (Beitreibungsrichtlinie).

Mindestens ebenso wichtig und wirksam ist die etwa 1995 einsetzende und seither sehr aktive Rechtsprechung des Europäischen Gerichtshofs zu den Grundfreiheiten des AEUV. Sie bietet Schutz gegen grenzüberschreitende Diskriminierungen. Der grundfreiheitliche Schutzanspruch der Steuerpflichtigen richtet sich gleichermaßen gegen den Zielstaat (Schutz der Grundfreiheiten für Inlandsinvestitionen EU-ausländischer Unternehmen) und gegen ihren Heimatstaat (Schutz der Grundfreiheiten für EU-Auslandsinvestitionen inländischer Unternehmen).

Ergänzend tritt das Verbot staatlicher Beihilfen in Form von Steuersubventionen hinzu (Vertrag über die Arbeitsweise der Europäischen Union: Art. 107, 108). Es enthält Besserstellungsverbote und wirkt damit komplementär zu den Grundfreiheiten. Die Mitgliedstaaten dürfen keine selektiven Vorteile (zur Bedeutung des Selektivitätskriteriums zuletzt: Ismer et al. 2015: 257ff.) für Unternehmen gewähren, die den grenzüberschreitenden Handel mit Waren und Dienstleistungen aktuell oder potenziell verzerren. Wie die Grundfreiheiten betrifft auch das Beihilfenverbot gleichermaßen das materielle Steuerrecht und das Steuerverfahrensrecht, die Rechtsetzungsebene und den Steuervollzug (dazu näher unter 3.7).

Das alles zeigt, wie sehr das Internationale Steuerrecht für die in der EU-28 zusammengeschlossenen Staaten durch ein spezifisches Europäisches Steuerrecht überlagert und ergänzt wird.

2.2.3 Doppelbesteuerungsabkommen als Kern des Steuervölkerrechts

Von höherer Anciennität als das Europäische Steuerrecht sind die seit über 100 Jahren bestehenden Doppelbesteuerungsabkommen (DBA). Bei ihnen handelt es sich um klassisches Völkerrecht, fast ausnahmslos in Form bilateraler Staatenverträge. Heute bestehen weltweit etwa 3.000 DBA; allein Deutschland ist mit rd. 100 ausländischen Staaten durch bilaterale DBA verbunden.

Diese Doppelbesteuerungsabkommen zielen im Kern auf die Bewältigung von zwei Problemen. Erstens schützen sie den Steuerpflichtigen davor, dass er doppelt belastet wird; zweitens schützen sie die Staaten davor, dass der Steuerpflichtige dadurch, dass er grenzüberschreitend investiert oder konsumiert, weniger Steuern zahlt, als er gezahlt hätte, wenn er nur im einen Staat oder nur im anderen Staat tätig geworden wäre. Auf den Begriff gebracht: Die DBA dienen der Vermeidung von Doppelbesteuerung und der Vermeidung von Doppelnichtbesteuerung (eindrucksvoll: Valta, 2014: 223).

Die Gründe dafür, dass wir es praktisch ausschließlich mit bilateralen Handlungsformen zu tun haben, liegen darin, dass die Abkommen keinen gestaltend-formenden Einfluss auf die nationalen Rechtsordnungen haben. Die nationalen Gesetzgeber bleiben frei, ihre Steuerrechtsordnungen so zu schreiben und auszugestalten, wie sie es ökonomisch für opportun halten und wofür sich demokratische Mehrheiten finden lassen. Die völkerrechtliche Koordination dient lediglich der Abgrenzung an Inlands-Auslands-Schnittstellen. Das Völkerrecht überlagert als eine Art zweite Schicht das innerstaatliche Recht, ohne aber die Gesetze zu verändern. Diese zweite Schicht befindet nach Art einer Schablone darüber, welches Pflänzchen nach oben wachsen darf – welcher nationale Steueranspruch aufrechterhalten bleibt und welcher nicht. Daher müssen die DBA immer beide nationalen Rechtsordnungen in ihrem jeweiligen Zustand so präzise aufeinander abstimmen, dass es weder Überschneidungen noch Lücken gibt. Wir haben es mit Millimeterrecht zu tun. Die Regelwerke der DBA sind daher technisch außerordentlich anspruchsvoll; es ist kaum möglich, je mehr als zwei Rechtsordnungen so aufeinander abzustimmen, dass sich Überlappungen von Steueransprüchen und Lücken vermeiden lassen, die Staaten aber zugleich die *iustitia commutativa,* die horizontale Aufteilungsgerechtigkeit aufgeben müssen (ebd.: passim).

Ein zweiter, nicht generell juristischer, sondern polit-ökonomischer Grund für die Bilateralität ist, dass jeder Staat in den Abkommensverhandlungen zugleich gibt und nimmt, dieses Geben und Nehmen aber juristisch in sehr abstrakte Formulierungen gelegt wird, die sich immer umkehren lassen: die ein Staat genauso gegen sich gelten lassen muss wie der andere Staat im spiegelbildlichen Fall. In den Abkommen steht also nicht: „Deutschland darf – Frankreich darf"; die Rede ist immer nur von „dem Ansässigkeitsstaat" bzw. dem „anderen Vertragsstaat", so dass sich die Regelungen eines DBA immer umkehren lassen. Sie passen sich – bildlich gesprochen – dem Stand der Kompassnadel an. Diese Reziprozität des Rechts hat einen Gerechtigkeitsgehalt – zwischenstaatlich ebenso wie im Staat-Bürger-Verhältnis. Sie macht es im Grunde unmög-

lich, dass man in Dreiecksfällen, wenn also drei Staaten ein solches Abkommen schließen wollten, ein bestimmtes Aufkommensergebnis, das die Verhandelnden anstreben, nachhaltig erzielt. Deswegen ist es fast eine Art Naturgesetz, dass diese zwischenstaatliche Kooperation – von wenigen Ausnahmen abgesehen – bilateral geblieben ist.

Diese Bilateralität hat aber ihrerseits eine feste Verankerung im supranationalen Bereich. Die völkerrechtlichen Doppelbesteuerungsabkommen beruhen auf Blaupausen, auf Formularen, die die Staaten auf Ebene der OECD erarbeiten und verbessern. Die OECD und in ihrem Fahrwasser auch der Steuerausschuss der Vereinten Nationen (siehe Kap. 4-2.2) haben einen hohen technischen Sachverstand angesammelt, einerseits im Rat, in seinen Ausschüssen und deren Arbeitsgruppen, auf der anderen Seite aber vor allem im Sekretariat. Das Sekretariat der OECD, das Center for Tax Policy and Administration (CTPA), ist der beste und auch nachhaltigste *think tank*, der das Internationale Steuerrecht prägt. Durch dieses epistemische Netzwerk gewinnt die OECD entscheidenden Einfluss auf das heutige Internationale Steuerrecht. In dem Maße, in dem sich die OECD Schwellenländern wie insbesondere den BRICS-Staaten öffnet, ist das Interesse vor allem des Sekretariats, aber auch des Rates, immer stärker darauf gerichtet, dass auch das Steuervölkerrecht den Interessen der Schwellenländer entspricht – und nicht mehr nur den Interessen der Kapitalexporteure in der Nordatlantikregion. Diese Öffnung der OECD führt dazu, dass das Steuervölkerrecht in aller Regel dem Quellenstaat den Vorrang vor dem Ansässigkeitsstaat gibt.

2.2.4 Sonstiges Völkerrecht mit Relevanz für das Steuerrecht

Erstaunlich gering ist demgegenüber die Relevanz des klassischen Wirtschaftsvölkerrechts, bilateraler Investitionsschutzabkommen, aber auch des Seerechts, des Internationalen Transportrechts oder des Internationalen Umweltrechts für das Steuerrecht. Allenfalls sehr vereinzelt haben Garantien der unter dem Dach der WTO versammelten Vertragswerke mit ihren Diskriminierungsverboten, Meistbegünstigungsgeboten, Beihilfeverboten und Amts- und Rechtshilfeklauseln Einfluss auf die Besteuerung (Reimer 2006: 41; Trottmann 2010). Entsprechend gering ist die Bedeutung investitionsschutzrechtlicher Schiedsklauseln für die Steuerpolitik.

2.3 Überlagerung von Globalisierung und Virtualisierung

Im Folgenden sind nun beide Teilperspektiven zusammenzubringen: Wie reagiert die Steuerrechtsordnung auf die Kombination von Virtualisierung und Globalisierung? Lassen sich die alten Muster für die Zuweisung der primären Besteuerung an Quellen- oder Ansässigkeitsstaat aufrechterhalten, wenn es nun nicht mehr um realwirtschaftliche, d.h. mit einer physischen Verlagerung von Personen oder Waren verbundene Leistungen geht, sondern wenn elektronische Dienstleistungen erbracht, Wertschöpfungen in der virtuellen Welt realisiert werden?

Hier fällt die Antwort gespalten aus. Einerseits erweisen sich die bestehenden Regelwerke als stabil und auch als überraschend leistungsfähig, was – vereinfacht gesprochen – den arglosen Steuerpflichtigen angeht, der Wirtschaftsvorgänge, die früher aus echten Lieferungen oder physischen Leistungen bestanden, ganz oder teilweise in den elektronischen Geschäftsverkehr verlagert. Solange das Internet Medium und Hilfsmittel dessen ist, was sich weiterhin physisch-real erfassen lässt, sind allenfalls technische Anpassungen erforderlich. Derartige Anpassungen finden sich im Recht der indirekten Steuern, in Europa v.a. in der Mehrwertsteuer (Umsatzsteuer) in größerer Zahl als bei den direkten Steuern (exemplarisch: Henschel 2005; Meinke 2012). Hier wie dort bleiben aber die alten Muster zur Zuweisung von Besteuerungsrechten im Wesentlichen intakt.

Andererseits aber transformiert das Internet die Produktion und Verfrachtung von Waren in elektronische Dienstleistungen, macht diese Dienstleistungen hochfungibel und erschwert so ihre räumliche Ortung. Hier schlägt die mediale Vereinfachung in ein qualitatives Novum um. Geradezu sprunghaft nehmen Prozesse einer Wertschöpfung aus der Nutzung immaterieller Wirtschaftsgüter zu. Dass Patente, Know-how, aber selbst die Ertragskraft kompetenter Teams von Entwicklern als solche zum Gegenstand von Entstrickungs- und Verstrickungsprozessen, Versicherungen, Rückversicherungen und anderen Derivaten werden und dass die so entstehenden Stammrechte – zumal im Binnenmarkt – an anderer Stelle angesiedelt sein können als dort, wo sie genutzt werden, ist neu. Das Steuerrecht entwickelt nur langsam, tastend und unter Inkaufnahme von Genauigkeitsverlusten Regeln zur Behandlung immaterieller Wirtschaftsgüter und der aus ihnen gezogenen Nutzungen.

3 Typische Steuersparmodelle: Funktionsweise, Bauformen, Ursachen

Diese Schwierigkeiten schlagen sich in einer Reihe neuer Steuersparmodelle nieder, die seit einigen Jahren im grellen Licht der Öffentlichkeit diskutiert werden (besonders klar: Pinkernell 2014). Sie bestehen aus zahlreichen, i.d.R. miteinander kombinierten Bausteinen. Die wichtigsten dieser Bausteine zeigen exemplarisch die Herausforderungen, vor denen nationale Steuergesetzgeber und die die Staaten verklammernden und unterstützenden supra- und internationalen Organisationen und Akteure gegenwärtig stehen.

3.1 Aufbau und Nutzung mehrstöckiger Unternehmensstrukturen

Die Errichtung eines Steuersparmodells ist zunächst nichts anderes als die Ausübung der grundrechtlich (Art. 14 Abs. 1, 12 Abs. 1, 9 Abs. 1, 2 Abs. 1 GG) abgesicherten Privatautonomie. Der Steuerpflichtige bedient sich der Mittel des Zivilrechts, um mehrstufige Strukturen aus einzelnen Kapitalgesellschaften, Stiftungen oder *trusts* in unterschiedlichen Staaten zu errichten. Die Unternehmensgegenstände dieser einzelnen

Rechtsträger sind dabei nicht identisch; die einzelnen Gesellschaften sind i.d.R. nicht volle Landesgesellschaften, die das Gesamtgeschäft oder auch nur den Vertrieb der Gruppe übernehmen und in ihrem Geschäftsgegenstand nur territorial auf ihren jeweiligen Ansässigkeitsstaat begrenzt sind. Vielmehr bildet die Gesamtstruktur ein stark arbeitsteiliges Vorgehen ab. Ein Teil der beteiligten Rechtsträger ist nicht aktiv tätig und hat deshalb kaum Personal, sondern bündelt nur Beteiligungen, Liquidität, Darlehensforderungen und/oder Verbindlichkeiten. Charakteristisch ist aber v.a. die Nutzung derartiger passiver Gesellschaften mit dem Geschäftsgegenstand Erwerb und Hinaus-Lizenzierung geistigen Eigentums, v.a. von Patenten und Marken (dazu noch unter 3.4).

3.2 Nutzung eines „hybrid mismatch" in persönlicher Hinsicht

Während die aktiv (operativ) tätigen Gesellschaften sich in der Regel einem Staat sehr klar zuordnen lassen, weil sie dort zugleich ihren Sitz und ihre tatsächliche Geschäftsleitung haben, werden als passive Finanzierungs-, Beteiligungs- und IP-Gesellschaften oftmals sog. hybride Gesellschaften verwendet, für die zwei Formen zu unterscheiden sind.

Einerseits können Gesellschaften dadurch hybrid sein, dass sie aus Sicht eines Staates als eigenständige Steuersubjekte, d.h. als „intransparent" wahrgenommen werden, während ein anderer Staat in ihnen nur die Bündelung der wirtschaftlichen Interessen der hinter ihr liegenden Gesellschafter sieht, die Gesellschaft daher als „transparent" ansieht und nicht sie selber, sondern die hinter ihr liegenden Gesellschafter besteuert.

Im (heute kaum noch vorkommenden) Extremfall kann das zu einer Art negativem Besteuerungskonflikt führen: Wenn – etwa aufgrund der Regelungen des zwischen den Staaten abgeschlossenen DBA – die Konstellation so ist, dass der Sitzstaat der Gesellschafter für die (nicht ausgeschütteten) Gesellschaftsgewinne dem Intransparenzkonzept folgt und daher allein den Sitzstaat der Gesellschaft abkommensrechtlich als zur Besteuerung befugt ansieht, während umgekehrt der Sitzstaat der Gesellschaft dem Transparenzkonzept folgt und meint, die Zinsen oder Lizenzgebühren, die die passive Gesellschaft erlangt, seien allein auf Ebene der – gebietsfremden – Gesellschafter zu erfassen, kommt es jedenfalls solange zu einer Doppelnichtbesteuerung, wie die Gesellschaft diese Gewinne nicht an ihre Gesellschafter ausschüttet. Ist es umgekehrt (Gesellschaftsstaat nimmt Intransparenz, Gesellschafterstaat Transparenz der Gesellschaft an), kommt es – spiegelbildlich – zu einer Doppelbesteuerung.

Andererseits können Gesellschaften in territorialer Hinsicht hybrid werden: Wenn sie zwar nach dem Recht eines Staates gegründet und in diesem Staat z.B. in ein Handelsregister eingetragen sind, während aber die zentralen betrieblichen Entscheidungen in einem anderen Staat getroffen werden, klaffen der (zivilrechtliche) Sitz und die (tatsächliche) Geschäftsleitung auseinander. Da die Steuerrechtsordnungen und die DBA aber nur teilweise an den zivilrechtlichen Sitz, sogar überwiegend dagegen an den

Ort der tatsächlichen Geschäftsleitung anknüpfen (Art. 4 Abs. 1 und Abs. 3 OECD-MA. Hierzu: Ismer et al. 2015: Art. 4 Rn. 49–36, 118–133), um die Ansässigkeit eines Rechtsträgers und damit auch die Zuweisung der Besteuerung zu bestimmen, kommt es wiederum zu bilateralen Zuordnungskonflikten (dem *hybrid mismatch*) und zu der Gefahr von Doppelbesteuerung oder Doppelnichtbesteuerung.

3.3 Gewinnverlagerung durch Gesellschafterfremdfinanzierung

Soweit „Schlupflöcher" mit dem Ziel einer Doppelnichtbesteuerung genutzt werden, besteht allerdings immer noch die Gefahr von Steuerbelastungen, sobald die hinter einer Gesellschaft stehenden Anteilseigner (oft innerhalb ein und desselben Konzerns) Dividenden dieser Gesellschaft beziehen oder durch Anteilsveräußerungen den Wert der in den Beteiligungen verkörperten Altgewinne realisieren. Tatsächlich lassen sich aber auch diese echten Vermögensmehrungen auf Gesellschafterebene wiederum steuerfrei (oder jedenfalls mit einer nur sehr niedrigen Steuerbelastung) vereinnahmen. Eines der Instrumente, die dazu genutzt werden, ist die Fremdfinanzierung der Zielgesellschaft: Wenn sie nicht – wie es dem gesellschaftsrechtlichen Leitbild entspricht – durch ein Grund- oder Stammkapital ausfinanziert ist, sondern zur Ergänzung eines nur geringen Grund-/Stammkapitals Darlehen aufnimmt, wird sie durch die Zinslasten, die sich aus den Darlehensverbindlichkeiten ergeben, gleichsam ausgezehrt. Dieser Ersatz von Eigen- durch Fremdkapital ist dann kein Nachteil für die Gruppe mehr, wenn das Darlehen nicht von einer externen Bank stammt, sondern innerhalb der Gruppe selber ausgereicht wird – etwa von einer in einem Niedrigsteuergebiet ansässigen Finanzierungstochter. Dann bleiben die Zinsen gleichsam „innerhalb der Familie". Die operativ erfolgreiche Konzerngesellschaft, die in einem Hochsteuerstaat hohe Erträge erzielt (Beispiel: Apple Deutschland), muss diese Erträge in Form steuerlich abziehbarer Zinsausgaben an Konzerngesellschaften im Ausland abgeben. Sie wird mit diesen konzerninternen Fremdfinanzierungen also gleichsam „auf null" gesetzt und entgeht einer Steuerbelastung in ihrem Sitzstaat.

Diese klassische Form der Gewinnverlagerung (*profit shifting*), die aus Sicht des Ansässigkeitsstaats der ertragreichen Landesgesellschaft zu einer Kürzung der inländischen Bemessungsgrundlage (*base erosion*) führt, hat allerdings in vielen Staaten Gegenreaktionen der nationalen Gesetzgeber hervorgerufen. Viele Steuerrechtsordnungen sehen vor, dass es bei einer unangemessen hohen Fremdkapitalquote (beruhend auf einem Vergleich des Fremd- zum Eigenkapital der betroffenen Landesgesellschaft) oder bei einem unangemessen hohen Zinsaufwand (beruhend auf einem Vergleich des Netto-Zinsaufwands mit den zinsbereinigten Roherträgen dieser Gesellschaft) dazu kommt, dass die Zinsen nicht mehr steuerwirksam sind, d.h. für Zwecke der Bildung der steuerlichen Bemessungsgrundlage nicht länger als Betriebsausgaben abgezogen werden dürfen.

Für Deutschland markiert die Einführung der sog. Zinsschranke (§§ 4h EStG, 8a KStG) den bislang letzten Schritt in der langen und erstaunlich wechselvollen Geschichte der Abwehrgesetzgebung. Charakteristisch für diese Zinsschranke ist, dass sie – im Gegensatz zu Vorläuferregelungen über die Gesellschafterfremdfinanzierung – im Kern auf einem Vergleich des Zinssaldos (Überschuss abfließender gegenüber zufließenden Zinsen) mit dem sog. EBITDA (den *earnings before interest, taxes, depreciation and amortization*) der inländischen (Tochter-)Gesellschaft beruht, aber dem Abzugsverbot seine krisenverschärfende Wirkung dadurch nimmt, dass die – bei gleichbleibendem Lohn- und Gehaltsaufwand – in Depressionsjahren nahezu zwangsläufige Versagung jedes Zinsabzugs durch ein Unterschreiten der maßgeblichen Schwellenwerte in vorangegangenen oder nachfolgenden Jahren verhindert oder jedenfalls ex post beseitigt werden kann. Dadurch und durch eine Reihe weiterer normativer Vorkehrungen (insbesondere den sog. Eigenkapitalvergleich als Ausschlusstatbestand) trägt die deutsche Zinsschranke dem genuin betriebswirtschaftlich-operativ begründeten Fremdfinanzierungsbedürfnis der inländischen Unternehmen hinreichend Rechnung, ohne ihr steuerpolitisches Ziel – die Eindämmung von *base erosion and profit shifting* (BEPS) – aus den Augen zu verlieren.

3.4 Insbesondere: Verlagerung immaterieller Wirtschaftsgüter

Die Steuerplanungsindustrie hat auf die Einführung derartiger Institute allerdings rasch reagiert, indem sie schlicht das Medium der Fremdfinanzierung ausgetauscht hat: An die Stelle von Darlehen in Geld (die zu Zinsaufwand bei der fremdfinanzierenden Konzerngesellschaft führen) tritt die Überlassung immaterieller Wirtschaftsgüter zur Nutzung durch diese Gesellschaft. Dazu werden immaterielle Wirtschaftsgüter – wie oben skizziert – in Gesellschaften verlagert, die in Staaten mit einem niedrigen Steuerniveau angesiedelt sind. Dieses niedrige Steuerniveau kann sich aus dem Fehlen jeder Körperschaftssteuer (Bermudas), alternativ aus sehr niedrigen Steuersätzen (Irland, Malta, Niederlande) oder aber der Aufrechterhaltung nominell hoher Steuersätze bei gleichzeitiger Gewährung großzügiger Freibeträge, hoher (teils virtueller) Abschreibungen oder anderer fiktiver Betriebsausgaben für Aktivitäten im Bereich von Forschung und Entwicklung ergeben (Dänemark, Österreich; vgl. Spengel 2009: 73). Ähnliche Strategien verfolgen Staaten, die präferenzielle steuerliche Regime für die (sc. Aktive) Forschungs- und Entwicklungstätigkeit anbieten und damit gezielte Anreize für die Hereinverlagerung derartiger Tätigkeiten setzen (Belgien, Frankreich, Niederlande, Spanien, Schweiz, Vereinigtes Königreich: Evers 2015).

In allen diesen Fällen überlässt die IP-Gesellschaft Patente und Markenrechte den in Hochsteuerländern operativ tätigen Konzerngesellschaften und bezieht als Gegenleistung marktübliche Lizenzgebühren. Diese Lizenzgebühren nehmen nun strukturell den Platz ein, den in den Gesellschafterfremdfinanzierungsfällen (siehe Kap. 3.3) traditionell die Zinsen hatten: Sie mindern die Bemessungsgrundlage im Sitzstaat der ope-

rativ tätigen Landesgesellschaft; aus den genannten Gründen führen sie aber nicht zu einer korrespondierenden (substanziellen) Belastung im Staat der die Lizenzgebühren empfangenden IP-Gesellschaft.

Hier zeigt sich BEPS in einer besonders wirksamen Ausbaustufe: Die *base erosion* ist nicht mehr (isoliert) nur auf einen Staat beschränkt; vielmehr verschwinden Gewinne gleichsam global, d.h. auch in der Gesamtbetrachtung über mehrere Staaten hinweg. Immer stärker klaffen damit die den Kapitalmärkten berichteten Ergebnisse großer Konzerne und ihre globale steuerliche Bemessungsgrundlage auseinander; die Kapitalmärkte wiederum feiern niedrige Konzernsteuerquoten als operativen Erfolg. Daher sind in vielen international tätigen Unternehmen heute die dem Finanzvorstand (CFO) zugeordneten Steuerabteilungen oft besonders ertragreiche *profit center*.

3.5 Nutzung eines „hybrid mismatch" in sachlicher Hinsicht

Ein weiteres Gestaltungselement sind hybride Finanzierungen, die eingesetzt werden, wo zwei beteiligte Staaten unterschiedliche Kriterien für die Abgrenzung von Dividenden von Zinsen anwenden. Dividenden sind regelmäßig aus versteuertem Einkommen der ausschüttenden (Tochter-)Gesellschaft zu zahlen, werden aber auf Ebene der empfangenden (Mutter-)Gesellschaft nicht oder allenfalls sehr gering erneut belastet. Zinsen mindern dagegen – in den Grenzen der oben (Kap. 3.3) skizzierten Zinsschranken oder sog. *thin cap rules* – den Gewinn der Schuldnergesellschaft, während sie empfängerseitig voll zu erfassen und zu besteuern sind. Wenn nun durch Genussrechte, Beteiligungsdarlehen (*profit-sharing loans*) oder andere strukturierte Derivate Gesellschaftsfinanzierungen ins Werk gesetzt werden, die der Sitzstaat der Schuldnergesellschaft als Zins, der Sitzstaat der Gläubigergesellschaft als Dividende oder auch als steuerfreien Veräußerungsgewinn qualifiziert, kommt es wiederum zu Phänomenen einer Doppelnichtbesteuerung oder jedenfalls einer globalen Minderbesteuerung.

3.6 Mehrfacher Aufwands- oder Verlustabzug

Ein sechstes Element, das ebenfalls oft Verwendung findet, ist der *double dip*: Durch die Berücksichtigung ein und desselben Aufwands (bestimmter Betriebsausgaben) in mehr als einem Staat können selbst dann, wenn sämtliche Erträge einmal steuerlich erfasst werden, globale Konzerngewinne in globale Konzernverluste verwandelt werden, die am Ende jede Besteuerung ausschließen. Entsprechendes gilt für die – über den Veranlagungszeitraum aggregierte – Größe des Jahresverlusts: Durch bestimmte stabile Strukturen können im Einzelfall bereits laufende Verluste mehrfach verwertet werden – einmal im ausländischen Betriebsstättenstaat oder im Sitzstaat einer ausländischen Tochtergesellschaft, ein zweites Mal auf Ebene des Stammhauses oder im Sitzstaat der Muttergesellschaft. Vor allem aber lassen sich *double-dip*-Phänomene durch geschickte Umwandlungen ins Werk setzen, die auch unterschiedliche Stichtage (über-

lappende Steuerjahre) oder unterschiedliche Realisierungszeitpunkte (Verlustentstehungstage) nutzen.

3.7 Rulings

Ein letztes, nun aber nicht mehr dem materiellen Recht mit seinen Gestaltungsoptionen, sondern dem Verfahrensrecht zuzuordnendes Element sind verbindliche Auskünfte (*rulings*), die zahlreiche Staaten bereitwillig erteilen, um Unternehmen im Vorfeld ein hohes Maß an Investitionssicherheit zu bieten. Rechtsstaatlich ist gegen Rechtssicherheit nichts einzuwenden. Es ist richtig und wichtig, dass auch das deutsche Recht verbindliche Auskünfte (§ 89 Abs. 2 AO) und zusätzlich – im Anschluss an Betriebsprüfungen – verbindliche Zusagen (§§ 204ff. AO) kennt und dass die Finanzbehörden des Bundes und der Länder diese Rechtsinstitute auch nutzen. Darüber hinaus sind bilaterale Vorabverständigungen zwischen zwei Staaten möglich (Art. 25 OECD-MA, Art. 24 dVG). Alle diese Regelungen dienen dazu, die Ungewissheiten, die mit der Anwendung eines hochkomplexen Systems wie des Internationalen Steuerrechts so wirksam zu beseitigen, dass der Steuerpflichtige schon vor einer Transaktion weiß, welche Staaten diese Transaktion mit welchen Beträgen belasten.

Allerdings zeigt sich in der *ruling*-Praxis einiger europäischer Staaten (genannt werden v.a. Belgien, Irland, Luxemburg und die Niederlande, teilweise aber auch Frankreich und Österreich), dass die Behörden nicht in allen Fällen das geltende Gesetzes- und Abkommensrecht strikt anwenden, um die Gleichmäßigkeit des Vollzugs zu gewährleisten, sondern dass sie mit Duldung der Regierungen Standortpolitik betreiben. Die EU-Kommission hat eine Reihe von Beihilfeprüfungsverfahren eingeleitet: zunächst im Juni 2014 gegen Irland, Luxemburg und die Niederlande; im Dezember 2014 dann – vielfach als Entlastungsangriff des luxemburgischen Kommissionspräsidenten gedeutet – gegen alle 28 EU-Staaten. Diese Untersuchungen haben allerdings unterschiedliche Intensität; so hat die EU-Kommission im Februar 2015 mitgeteilt, die belgische Praxis einer besonders eingehenden Überprüfung zu unterziehen (European Commission 2015).

3.8 Steuerhinterziehung als Ausnahmefall

Nur selten tritt zu diesen – durchweg nicht verbotenen – Gestaltungselementen die echte Illegalität hinzu. Typischerweise sind BEPS-Gestaltungen aber nicht mit (sc. verbotener und sogar strafbarer) Steuerhinterziehung verbunden. Im Gegenteil: Die Unternehmen legen alles offen, was die beteiligten Fisci – gedeckt durch nationales Verfahrensrecht – an Informationen benötigen und anfordern. Nicht selten wissen daher alle beteiligten Finanzverwaltungen, wie das Modell in seiner Gänze aussieht. Daneben gibt es allerdings bis heute zahlreiche Modelle, in denen Informationsdefizite der beteiligten Fisci, also der Finanzverwaltungen, mitursächlich dafür werden, dass es nicht zu einer symmetrischen, normalen Besteuerung kommt.

Anders ist es im Bereich der organisierten Kriminalität. Hier werden Geschäftsvorfälle verschleiert oder vorgetäuscht. Das beginnt bei Vermögensanlagen von Diktatoren in der Schweiz oder in Singapur und zieht sich über den sog. Karussellbetrug in der Umsatzsteuer (statt aller: Huschens 2012; Heuermann 2015) bis zum Handel mit an sich bereits verbrauchten Emissionszertifikaten.

3.9 Bündelung

Diese Gestaltungselemente werden je unterschiedlich kombiniert und verbunden. In vielen Fällen werden dadurch Null- oder Minimalbesteuerungen der Gewinne aus der Auslandstätigkeit ermöglicht. Dagegen zahlen viele international tätige Unternehmen im Heimatstaat des Konzerns oder der Gruppe auf die dort erzielten (Absatz-)Gewinne durchaus reguläre Steuern; sie erscheinen politökonomisch als eine Art Preis für den wirtschafts- und auch steuerpolitischen Schutz, denen ihnen der Heimatstaat gewährt. Es sind meist die ausländischen (Absatz-)Gewinne, die global unversteuert bleiben oder jedenfalls extrem niedrigen Belastungen ausgesetzt sind. Diese Asymmetrie zeigt sich besonders deutlich für die IP-starken US-Konzerne, von denen stellvertretend Amazon, Apple, Google, Microsoft, aber auch Coca Cola, General Electrics oder Starbucks zu nennen sind. In der Tendenz sind sie aber auch den in Deutschland ansässigen Unternehmen nicht gänzlich fremd. Auch hierzulande weisen die Konzernsteuerabteilungsleiter gegenüber Finanzpolitikern fast vorwurfsvoll darauf hin, man erziele im Inland nur ein Fünftel der globalen Gewinne und habe hier nur ein Drittel des globalen Lohnaufwands; von den globalen Steuern entfielen aber zwei Drittel auf den deutschen Fiskus.

Das alles ist indes nur eine Seite der Medaille. Der Konzernbesteuerung steht die Konsumbesteuerung gegenüber. Hier wandelt sich das Bild: Denn auf jeden Kauf eines ausländischen Produkts durch einen inländischen Konsumenten im Inland wird im Inland Umsatzsteuer (Mehrwertsteuer) in Höhe von grundsätzlich 19 Prozent erhoben. Das gilt gerade auch für die Waren und Dienstleistungen der oben genannten US-amerikanischen Unternehmen. Diese Steuern stehen in voller Höhe dem inländischen Fiskus zu. Diese Belastung auf den gesamten Konsumentenumsatz begründet auch nominell eine viel erheblichere Belastung als es die Konzernbesteuerung (die ja nicht auf den Umsatz, sondern immer nur auf den Gewinn geht) jemals könnte.

Parallel dazu ist ferner die hohe inländische Steuerbelastung der hier gezahlten Löhne und Gehälter zu konstatieren. Auch die ausländischen Unternehmen, die durch Betriebsstätten oder Tochtergesellschaften im Inland präsent sind, führen für den hier entstehenden Lohn- und Gehaltsaufwand in voller Höhe Lohnsteuer an den inländischen Fiskus ab. Dieser Teil der Wertschöpfung, der mit dem Kauf eines ausländischen Produkts im Inland verbunden ist, wird also ebenfalls regulär im Quellenstaat versteuert. Auch hier sind jedenfalls nicht in nennenswertem Umfang Phänomene einer *base erosion* zu erkennen.

Insofern kann man in der Summe nicht davon sprechen, dass das Internet nicht besteuert wird. Defizite zeigen sich nur in der ersten – und ökonomisch ohnehin am wenigsten bedeutsamen – Dimension des klassischen Unternehmenssteuerrechts, nämlich bei der Besteuerung der unternehmerischen Margen.

4 Problembewältigung: Akteure und Handlungsformen

Gleichwohl sind mit dieser Diagnose die Probleme benannt, die es gegenwärtig zu lösen gilt. In den vorstehenden Analysen ist deutlich geworden, dass die Minderbesteuerung grenzüberschreitender Unternehmensgewinne ein besonderes Problem derjenigen Branchen und Unternehmen ist, die in hohem Maße geistiges Eigentum anbieten oder benötigen: know-how, Patente, aber auch Marken und einen besonderen Goodwill, ihren guten Namen bei den Kunden. Deshalb ist die Problembewältigung, die nun in den Blick rückt, vor allem auf die steuerliche Behandlung des geistigen Eigentums zu konzentrieren.

Im Vorfeld aller inhaltlichen Überlegungen sind aber zunächst Akteure und Handlungsformen zu betrachten – also diejenigen Institutionen und rechtlichen Instrumente, die Lösungen des Problems hervorbringen könnten.

4.1 Materielle Ziele

Die Ziele ihres Handelns sind schnell benannt: Aus der Perspektive einer der Bewältigung des BEPS-Problems verpflichteten Internationalen Steuerpolitik geht es um die Wahrung einer Gleichmäßigkeit der Besteuerung durch ein möglichst hohes Maß an Steuerneutralitäten: Die Steuerbelastung soll – möglichst unmerklich – der Wertschöpfung folgen, dabei Inbound-Investitionen ausländischer Investoren gegenüber inländischen Investitionen heimischer Investoren ebenso wenig benachteiligen wie Outbound-Investitionen heimischer Investoren gegenüber inländischen Investitionen derselben Investoren. Zugleich dürfen und sollen Steuern der Preis variabler öffentlicher Güter sein. Es gibt kein weltweit einheitliches Set öffentlicher Aufgaben und kein einheitliches Niveau ihrer Erfüllung. Daher sind unterschiedliche Steuerbelastungen der natürliche, im Wettbewerb der Staaten um die beste Politik nachgerade notwendige Ausdruck unterschiedlicher Output-Strategien.

Zentral erscheinen aber Transparenz und Vorhersehbarkeit der Besteuerung, ihre strikte Gesetzesbindung und damit ein möglichst lückenloser Gesetzesvollzug.

4.2 Institutionen

Doch bereits die Frage nach den Institutionen, die diese Ziele und Sub-Ziele erreichen oder jedenfalls fördern können, ist vergleichsweise komplex.

4.2.1 Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD)

Die größte Sachkompetenz und Prägekraft für das internationale Steuerrecht liegt seit über 50 Jahren bei der OECD. Auch für den BEPS-Prozess ist ihre Rolle schlechthin zentral. Dabei vertritt diese – früher oft als Kartell der Industriestaaten diskreditierte – Internationale Organisation heute längst nicht mehr nur Interessen klassischer Kapitalexporteure. Zwar wird die OECD weiterhin durch zahlreiche große EU-Staaten, die USA und Japan dominiert. Ihr gehören aber aus dem amerikanischen Raum inzwischen auch Kanada, Mexiko und Chile, aus dem asiatisch-pazifischen Raum Korea, Australien und Neuseeland, ferner Norwegen, die Schweiz, die Türkei und Israel an.

Vor allem aber kann man die heutige OECD in ihrem institutionellen Handeln nur verstehen, wenn man das in Paris angesiedelte Sekretariat und seine institutionellen Interessen auch isoliert in den Blick nimmt. Hier besteht ein starker Drang nach Erweiterungen der OECD um die BRICS-Staaten und weitere Schwellenländer. Dadurch ändert sich die Problemsicht des Sekretariats und seines *Center of Tax Policy and Administration* (CTPA) signifikant; auch Interessen großer Kapitalimporteure schlagen sich in den Vorschlägen des CTPA sichtbar nieder. Alle Vorschläge des CTPA erlangen zwar rechtliche Relevanz erst durch die Zustimmung sämtlicher 34 Mitgliedstaaten; hier gilt ein Einstimmigkeitserfordernis. Die Schreibrechte, also die sachverständige Ausgestaltung und Vorjustierung aller Vorschläge, bleibt aber Sache des CTPA und kleiner Arbeitsgruppen aus Vertretern einzelner Staaten. Die großen Runden – allen voran der Rat (*Council*) der OECD auf Botschafterebene – werden dadurch faktisch zu Ratifikationsorganen.

4.2.2 Vereinte Nationen

Die Vereinten Nationen, die der globalste aller Akteure sein könnten, haben sich insgesamt erst sehr spät in die Auseinandersetzung um BEPS und die Bemühungen um die Glättung und Optimierungen des Internationalen Steuerrechts eingebracht. Bis heute ist der Steuerausschuss der Vereinten Nationen im Kielwasser der OECD unterwegs. Was die VN an Blaupausen für den Abschluss bilateraler Doppelbesteuerungsabkommen liefern, entspricht zu etwa 98 Prozent textlich den Vorlagen der OECD. Nur an einigen wenigen Stellschrauben – etwa einem Recht des Quellenstaats zur satzmäßig begrenzten Besteuerung abfließender Lizenzgebühren – kommt es zu Abweichungen von den Standards der OECD. Diese Abweichungen bilden die Mehrheiten in Mitgliederstruktur und Vollversammlung der VN ab, die bei den Entwicklungs- und Schwellenländern liegt. In der Summe lässt sich sagen, dass die Präferenz zugunsten des jeweiligen Quellenstaates im Musterabkommen der Vereinten Nationen noch deutlicher zum Tragen kommt als bei der OECD. Ein substantieller Akteur im BEPS-Prozess sind die VN aber nicht geworden.

4.2.3 G20

Zwischen Vereinten Nationen und OECD steht als sehr junger Akteur das Forum der G20. Im Frühsommer 2013 haben sich die dort vertretenen Staats- und Regierungschefs in ihren informellen Gesprächen darauf verständigt, dem BEPS-Problem entgegentreten zu wollen. Dazu haben sie der OECD einen Arbeitsauftrag erteilt, obwohl die Mitgliedschaften in OECD und G20 nicht kongruent sind. Die OECD hat 34 Mitglieder, darunter nicht alle G20-Staaten.

Trotzdem sind die G20 das Forum, das die Gewähr dafür bietet, dass seit dem Sommer 2013 höchst intensiv an globalen Konzepten zur Bewältigung von BEPS gearbeitet wird. Diese Arbeit hat sehr schnell, nämlich noch 2013, eine erste Frucht hervorgebracht: einen Aktionsplan, der 15 Maßnahmen benennt, die die Staaten – einzeln, bilateral oder multilateral – ins Werk setzen sollen, damit die oben (Kap. 3) genannten Schwierigkeiten, namentlich die unterschiedlichen Formen eines *hybrid mismatch* und die gravierenden Informationsdefizite bekämpft werden können.

Von diesen 15 Maßnahmen sind einige sehr konkret, andere abstrakt. Einige beziehen sich auf die Veränderungen im Völkerrecht selbst, namentlich in den bilateralen DBA, zum Teil auch in multilateralen Informationsaustauschverträgen. Andere zielen lediglich auf Veränderungen des innerstaatlichen Rechts ab – auf das, was *Eberhardt Schmidt-Aßmann* Determinationsrecht nennt: Metaregeln, die im Wege supranationaler Empfehlungen, unionaler Richtlinien, völkerrechtlicher Verträge und gelegentlich auch nur von soft law auf die nationale Gesetzgebung einzuwirken suchen.

Dieser Maßnahmenplan aus dem Jahr 2013 wird gegenwärtig *peu à peu* abgearbeitet. Der Abarbeitungsprozess hat 2014 intensiv begonnen. Er setzt sich 2015 fort und soll Ende 2016 abgeschlossen sein.

4.2.4 Europäische Union

Deutlich geringer erscheint die Bedeutung der EU in der Bekämpfung der globalen Minderbesteuerung. Ihre Rolle ist sogar regelrecht ambivalent: Insbesondere aus US-amerikanischer Sicht erscheint der europäische Binnenmarkt sogar als begünstigender Faktor bei der Entstehung von BEPS. Da es in der EU auf dem Gebiet der direkten Steuern keine umfassende Harmonisierung gibt, die einzelnen Mitgliedstaaten – auch und gerade die kleinen und mittleren: Belgien, Estland, Lettland, Luxemburg, die Niederlande, Österreich – ihre eigene Steuerpolitik machen können, ohne dass sich die großen Industriestaaten innerhalb der EU dagegen abschotten dürften, eröffnet die EU den in einem Mitgliedstaat ansässigen Unternehmen beträchtliche Möglichkeiten für die Steuervermeidung. Die oben skizzierten Modelle wären kaum möglich gewesen, wenn die typischen Ansässigkeitsstaaten – neben Deutschland insbesondere auch Frankreich und die USA – Gewinne, die in Belgien, Irland, Luxemburg oder den Niederlanden nicht ausreichend vorbelastet worden sind, gleichsam nachholend besteuern dürften. Dem steht aber die Rechtsprechung des Europäischen Gerichtshofs in Luxem-

burg zur Bedeutung der binnenmarktlichen Niederlassungsfreiheit nach bisheriger Lesart entgegen.[1]

Nicht zu verkennen sind allerdings auch die zahlreichen gegenläufigen Bemühungen. Auch die EU und hier namentlich die Europäische Kommission bemühen sich aktiv um eine Eindämmung des sog. schädlichen Steuerwettbewerbs zwischen den Mitgliedstaaten. Diese Bemühungen haben bereits in den 1990er Jahren eingesetzt. Sie stützen sich teilweise auf hartes Recht, insbesondere die primärrechtlichen Vorschriften zum Beihilfenverbot (siehe Kap. 2.2.2 und 3.7). Diese Vorschriften kann die Kommission durchsetzen, und zwar prinzipiell allein – also ohne Zutun der Mitgliedstaaten, und ohne mitgliedstaatlichen Veto-Spielern ausgeliefert zu sein.

Einen Meilenstein markiert sodann der 1997 im ECOFIN-Rat verabschiedete Verhaltenskodex zur Unternehmensbesteuerung, mit dem der Rat und zusätzlich die Vertreter der mitgliedstaatlichen Regierungen, die im Rat versammelt sind, insoweit aber intergouvernemental handeln, steuerliche Maßnahmen als unstatthaft markieren, die zu einer Steuerbelastung führen, die erheblich geringer ist als die Normalsteuerbelastung in dem betroffenen Mitgliedstaat. Eine Expertengruppe unter der Leitung der britischen Staatssekretärin Dawn Primarolo hat sich nach Verabschiedung dieses Verhaltenskodex an dessen Umsetzung gemacht und 1999 einen ersten Bericht vorgelegt, in dem 66 einzelne Maßnahmen von Mitgliedstaaten als potentielle Verstöße gegen den Verhaltenskodex benannt wurden. Da der Verhaltenskodex nur soft law ist, gaben nur wenige dieser Maßnahmen Anlass für förmliche Vertragsverletzungsverfahren (v.a. Beihilfeprüfungsverfahren) durch die Kommission; sie haben aber zu wirksamen politischen Bemühungen im ECOFIN-Rat geführt. Nahezu keine der im *Primarolo*-Bericht kritisierten Maßnahmen bestehen in dieser Form heute noch fort.

Mit Blick auf neuartige Elemente eines schädlichen Steuerwettbewerbs hat die Kommission aber ihre eigenen Bemühungen um die Sicherung von Besteuerungsrechten im Binnenmarkt auch in den letzten Jahren fortgesetzt. 2012 hat sie einen Aktionsplan für ein effektiveres Vorgehen der EU gegen Steuerhinterziehung und Steuerumgehung vorgelegt. Er enthält einen umfassenden Katalog von Maßnahmen, die es den Mitgliedstaaten ermöglichen sollen, das ihnen zustehende Steuersubstrat effektiv zu nutzen. Auf diese Weise möchte die Kommission einen Mehrertrag der 28 nationalen Fisci in Höhe von 1 Billion Euro realisieren.

Praktisch folgen aus dem Aktionsplan zwei Empfehlungen: Erstens möchte die EU entschiedener gegen Steueroasen in Drittstaaten vorgehen. In diesem Bemühen reiht sie sich in die sehr wirksame Politik der OECD zum Abschluss von Informationsaustauschabkommen ein. Die zweite Empfehlung zielt nach innen: Die Mitgliedstaaten und die Kommission selbst sollen stärker gegen „Rechtstricks und Steuerschlupflöcher" vorgehen, die Unternehmen nutzen, um sich ihren Steuerpflichten zu entziehen. Dazu

1 Problematisch in dieser Perspektive v.a. die Rechtsprechungslinie Cadbury Schweppes, die auf das Urteil des EuGH v. 12.09.2006, Rs. C-196/04, Slg. 2006, I-7995, zurückgeht.

möchte die Kommission gestaltenden Einfluss auf die DBA nehmen. Außerdem sollen die Mitgliedstaaten unilateral Missbrauchsbekämpfungsklauseln in ihre nationalen Steuerrechtsordnungen einfügen.

Im Unterschied zu den klugen, technisch sehr feingliedrigen und mit fachlicher Autorität ausgestatteten 15 Maßnahmen der OECD bleibt der EU-Aktionsplan allerdings bis heute in einer Aufmerksamkeitsnische gefangen. Das liegt auch an der Retardierung des Handelns der Kommission. Als G20 und OECD längst an der Umsetzung des BEPS-Aktionsplans arbeiteten, gab die Generaldirektion Steuern der EU-Kommission im Dezember 2014 erst einmal eine externe Studie in Auftrag, die im Oktober 2015 vorgestellt werden und mit der nun überhaupt erst eruiert werden soll, welche Mitgliedstaaten Rechtsregeln bereitstellen, auf denen Unternehmen ihre Modelle einer sog. aggressiven Steuerplanung stützen. Auch die Möglichkeiten, die die Kommission als ständige Beobachterin bei den Arbeiten der OECD zu BEPS und auch auf dem *Global Forum* der OECD zu Verrechnungspreisfragen hat, nutzte sie kaum aus.

Insgesamt lässt sich also sagen: Es gibt in Brüssel nur einige wenige, eher nachvollziehende Reflexionen. Das erstaunt umso mehr, als das Europäische Recht sehr konkrete, juristisch harte Instrumente kennt, die auf OECD-Ebene erst entwickelt werden müssten. Wiederum ist exemplarisch das Beihilfenrecht zu nennen, über das die Kommission als Beihilfenaufsicht wacht. Es wäre gut geeignet, einen Teil der Bausteine, auf denen Steuersparmodelle beruhen, durch zielgenaue und doch maßvolle hoheitliche Maßnahmen in den Griff zu bekommen. Doch die Mühlen der Kommission mahlen langsam.

4.2.5 Bündelung

In alldem zeigt sich, dass die Staaten weiterhin die treibenden Akteure bei der Entstehung und Bekämpfung von BEPS sind. Zahlreiche Staaten, allen voran die USA, arbeiten sogar gleichzeitig an der Entstehung und an der Bekämpfung von BEPS. Erklärbar wird das durch das Bestreben, der heimischen Wirtschaft gegen die internationale Konkurrenz zu helfen; erklärbar wird es aber auch durch enorme Divergenzen zwischen US-Regierung und amerikanischem Kongress. *Mutatis mutandis* sind derartige Ambivalenzen aber auch in Deutschland zu erkennen.

4.3 Verfahren und Handlungsformen

Der letzte Blick gilt den Verfahren und Handlungsformen der oben genannten Akteure. Nicht alle Staaten sind zu Verschärfungen ihres innerstaatlichen Rechts bereit, ließen sich aber völkerrechtlich mindestens teilweise einbinden. Umgekehrt steht aber das Unionsrecht den rein völkerrechtlich fundierten Maßnahmen gegen BEPS entgegen. Hier wie dort – im Völkerrecht wie in weiteren Schritten einer unionalen Harmonisierung des Steuerrechts – bestehen aber Einstimmigkeitserfordernisse. Sie treffen auf eine höchst unterschiedliche Bereitschaft der Staaten, BEPS überhaupt als Problem zu

bezeichnen und die Bewältigungsstrategien auch zu Lasten der heimischen Unternehmen durchzusetzen. Daraus ergeben sich gravierende Dilemmata.

Deshalb ist für die EU-Staaten der Blick auf das Beihilfenrecht, seine Fortentwicklung und v.a. die gleichmäßige und damit sachgerechte Effektuierung seines Vollzugs durch die Europäische Kommission von zentraler Bedeutung.

Die weitere unionale Harmonisierung begegnet dagegen institutionellen Grenzen. Wir Deutschen wissen nicht, ob wir das Einstimmigkeitserfordernis aufgeben könnten, ohne das Grundgesetz und seine Integrationsschranken zu verletzen. Und doch ist die Dysfunktionalität, die von dem Einstimmigkeitserfordernis ausgeht, gravierend. Das gilt insbesondere für spätere Änderungen eines einmal erzielten Kompromisses: Darf es hier 28 Vetospieler geben? Diese Bestandsaufnahme (siehe Kap. 3) hat überdeutlich gezeigt, dass gerade im Steuerrecht jeder Rechtsetzer darauf angewiesen ist, sehr schnell zu reagieren, sobald die Beratungsindustrie neue Gestaltungsmodelle anbietet. Diese Möglichkeit der schnellen Reaktion stößt schon im Bundesstaat an ihre Grenzen; insbesondere die USA lähmen sich selbst. Noch viel schwieriger wären Anpassungsreaktionen auf europäischer Ebene: Das Initiativrecht für die (Steuer-)Gesetzgebung ist bei der Kommission monopolisiert; und einem Kommissionsvorschlag müssten sodann alle Vertreter der Mitgliedstaaten im ECOFIN-Rat zustimmen. Deshalb wird es auch langfristig nicht ohne zwischenstaatliche Kooperation gehen. Die Insuffizienzen der Vergangenheit leben fort; das Netz der Doppelbesteuerungsabkommen ist aber wandlungsfähig. Deswegen ist der derzeit gewählte Weg, den die G20 mit starker Unterstützung aus Frankreich, Deutschland und dem Vereinigten Königreich beschreiten, die intergouvernementale Koordination auf den beiden Ebenen der G20 und der OECD.

5 Fazit

Zieht man das Fazit aus diesen Überlegungen, so zeigt sich einerseits, wie präzise und sicher die Netzwerke einer globalen Koordination die Probleme des materiellen Rechts lösen könnten, wenn man dem Sachverstand seinen Lauf ließe. Die Erkenntnismöglichkeiten der Finanzverwaltungen sind hoch; dadurch lassen sich sehr klar und mit sehr hoher Auflösung die Mechanismen ermitteln, die den unfairen Steuerwettbewerb in den letzten Jahren ermöglicht haben. Zugleich lassen sich die Überwirkungen identifizieren, die nationale Steuerpolitik auf grenzüberschreitende Fälle hat.

Viel schwieriger – und zwar bereits normativ, nicht erst politisch schwierig – ist dagegen die Frage zu beantworten, in welchen Fällen derartige Überwirkungen gewissermaßen gegen Rechtsnormen verstoßen oder in Zukunft verstoßen sollten. In vielen Fällen sind es schlicht Größenvorteile oder auch bestimmte wirtschaftsstrukturelle Gegebenheiten, die es einem kleinen Staat leicht machen, mit niedrigen Steuersätzen auf industrielles Handeln abstrakt-generelle Regeln einzuführen, die im innerstaatlichen Fall genauso gelten wie im grenzüberschreitenden Fall. Wer traditionell keine eigene Industrie hat (Bermudas, Irland, Niederländische Antillen), hat keine Schwierig-

keiten mit einer großflächigen Absenkung des Besteuerungsniveaus, kann sich aber umgekehrt gerechtigkeitstheoretisch nicht vorwerfen lassen, etwas falsch zu machen, weil er ja abstrakt-generell alle gleich behandelt, auch den innerstaatlichen Fall. Darin liegt das normative Problem der Identifikation von Überwirkungen.

Gefordert bleibt daneben die Verdichtung des Informationsflusses zur Behebung des Problems von Steuerhinterziehungen durch eine grenzüberschreitende Zusammenarbeit zwischen Finanzbehörden. Sinnvoll ist die Einführung neuer Pflichten zur Offenlegung von Steuersparmodellen im Staat-Bürger-Verhältnis und zur Offenlegung der steuerlichen Verhältnisse desselben Unternehmens in anderen Staaten (*country by country reporting*). Perspektivisch sind deshalb v.a. die Informationsasymmetrien, die heute bestehen, zu vermeiden. Hier bestehen politisch die größten Erfolgsaussichten. Die Pointe könnte darin liegen, dass das Internet das Medium zur Bewältigung der steuerlichen Probleme ist, die es selber geschaffen hat.

Literatur

European Commission (2015): State aid: Commission opens in-depth investigation into the Belgian excess profit ruling system, 3.02.2015, http://europa.eu/rapid/press-release_IP-15-4080_en.htm (10.08.2015).

Evers, Lisa K. (2015): Intellectual Property (IP) Box Regimes. Tax Planning, Effective Tax Burdens, and Tax Policy Options, PhD Thesis: University of Mannheim BusinessSchool Mannheim.

Henschel, Lars (2005): Umsatzsteuerliche Behandlung des sog. E-Commerce, Verlag Dr. Otto Schmidt: Köln.

Heuermann, Bernd (2015): Mit Italmoda auf den Schultern von Larenz, in: DStR [Deutsches Steuerrecht], 1416–1420.

Huschers, Ferdinand (2012): Umsatzsteuerrechtliche Karussellgeschäfte und deren Auswirkungen, in: SteuK [Steuerrecht kurzgefasst], 479–483.

Ismer, Roland / Piotrowski, Sophia (2015): Selektivität von Beihilfen: Dogmatische Grundfragen am Beispiel von IP-Boxen, in: Internationales Steuerrecht 8, 257–266.

Ismer, Roland / Riemer, Katharina (2015): Kommentierung des Art. 4 OECD MC, in: Reimer, Ekkehart Reimer / Rust, Alexander (Hrsg.): Klaus Vogel on Double Taxation Conventions Bd.1 , Kluwer Law International: Aalphen aan den Rijn.

Meinke, Christopher (2012): Grenzüberschreitende Online-Umsätze im Umsatzsteuerrecht, in: Interdisziplinäres Zentrum für Internationales Finanz- und Steuerwesen der Universität Hamburg, Interdisziplinäres Zentrum für Internationales Finanz- und Steuerwesen: Hamburg.

Pinkernell, Reimar (2014): Internationale Steuergestaltung im Electronic Commerce. Institut Finanzen und Steuern: Berlin.

Reimer, Ekkehart (2006): Steuerrechtliche Bezüge der völkerrechtlichen Meistbegünstigungspflichten, in: Cordewener / Enchelmaier / Schindler (Hrsg.): Meistbegünstigung im Steuerrecht der EU-Staaten. Mit Diskussionsbeiträgen eines Münchener Symposions, C.H. Beck: München, 41–76.

Schaumburg, Harald / Englisch, Joachim (2015): Europäisches Steuerrecht, Verlag DR. Otto Schmidt: Köln.

Spengel, Christoph (2009): Steuerrechtliche Förderung von Forschung und Entwicklung (FuE) in Deutschland. Ökonomische Begründung, Handlungsbedarf und Reformbedarf, Springer: Berlin.

Stahl, Christian (2013): Die Reichweite der erweiterten beschränkten Steuerpflicht nach § 2 AStG.: Ein Beitrag zur Struktur der Steuerpflicht, Duncker & Humblot: Berlin.

Storbeck, Olaf (2006): Mehrwertsteuer: Geburt eines Goldesels, in: Handelsblatt 2006: 60 Jahre deutsche Wirtschaftsgeschichte, 28.12.2006, http://www.handelsblatt.com/archiv/60-jahre-deutsche-

wirtschaftsgeschichte-mehrwertsteuer-geburt-eines-goldesels/v_detail_tab_print/2749888.html (10.8.2015).

Trottmann, Christian (2010): Gleichbehandlung und Neutralität im internationalen Ertragsteuerrecht aus Sicht des Welthandelsrechts (WTO). Die Vorgaben der Subventions- und Diskriminierungsverbote für die Besteuerung des grenzüberschreitenden Warenverkehrs, Nomos: Baden-Baden.

Valta, Matthias (2014): Das Internationale Steuerrecht zwischen Effizienz, Gerechtigkeit und Entwicklungshilfe, Mohr Siebeck: Tübingen.

Autor

Prof. Dr. Ekkehart Reimer
Direktor des Instituts für Finanz- und Steuerrecht
Inhaber des Lehrstuhls für Öffentliches Recht, Europäisches und Internationales Steuerrecht
Universität Heidelberg
Friedrich-Ebert-Anlage 6-10
DE-69117 Heidelberg
reimer@uni-heidelberg.de

DOI: 10.11588/josar.2015.0.23484

Das Internet: ein umfassendes Überwachungssystem

William Binney[1]

1 Einleitung

Der vorliegende Beitrag beschreibt die (Aus-)Nutzung des Internets durch die National Security Agency (NSA) zum Zweck der Individual- und Massenüberwachung von US-Bürgern und Nicht-US-Bürgern. Auf vier Punkte wird hierbei besonderes Gewicht gelegt. So soll zunächst (Abschnitt 2) auf die besonderen Möglichkeiten und Zugangspunkte der massenhaften Datenüberwachung und das jeweilige Vorgehen der NSA eingegangen werden. Hierbei wird Einblick in die drei am häufigsten angewandten Methoden gegeben und diese werden anhand der Überwachungspraktiken auf der nationalen und internationalen Ebene exemplifiziert. Danach (Abschnitt 3) werden weitere Methoden der Überwachung aufgezeigt und die Ineffizienz des gesamten Überwachungssystems verdeutlicht. In Abschnitt 4 folgt die Kontrastierung einer ursprünglich von uns – einer früheren Riege von Mitarbeitern der NSA, der ich angehörte – mitentwickelten, zielgerichteten und rechtlich unbedenklichen Überwachung sozialer Netzwerke mit jener der NSA. Diese Analyse wird ergänzt durch eine Einschätzung über die Anpassung des Überwachungsprogramms seit den Enthüllungen durch Edward Snowden. Schließlich werden in Abschnitt 5 die weiteren, problematischen Folgen der Massenüberwachung angesprochen. Es wird gezeigt, wie das NSA-Überwachungssystem bereits über die reine geheimdienstliche Arbeit hinausgreift und bestehendes Recht und Gesetz bricht.

Alle verwendeten Materialien und Dokumente, auf die sich dieser Artikel stützt, stammen aus frei zugänglichen Quellen, aus öffentlich zugänglichen und legalen Seiten im Internet. Der überwiegende Anteil – wenngleich nicht ausschließlich – entstand rund um die Enthüllungen des Whistleblowers Edward Snowden. Sie wurden für den vorliegenden Beitrag erklärend aufgearbeitet und mit eigenen Analysen ergänzt. Das Bild, das sich hieraus abzeichnet, macht deutlich, dass die NSA nicht nur erheblichen Einfluss auf das Internet besitzt, sondern das Internet bereits kontrolliert. Dies gilt zumindest, was den Zugang zu den Daten betrifft.

2 Die Massenüberwachung der NSA

Die NSA überwacht nahezu den gesamten Internetverkehr, immer auf der Suche nach relevanten Informationen. Als relevante Informationen oder zumindest potentiell rele-

1 Der Text beruht auf einem Vortrag. Er wurde von Stefan Artmann erstellt.

vante Informationen werden von der NSA dabei inzwischen nahezu alle Daten angesehen: Entweder weil sie aus sich selbst heraus interessant sind oder durch die intelligente oder automatisierte Kombination mit anderen Datenbeständen zu einem lückenlosen Informationsbild beitragen; oder weil sie für die Abwehr bereits bekannter Gefahren oder noch unbekannter Gefahren eingesetzt werden können. Dieses Informationsinteresse beginnt bereits bei den so genannten Metadaten, also Informationen die über die Inhaltsdaten hinausgehen. Bei einer E-Mail beispielsweise ist der Inhalt der geschriebene Text. Die Metadaten hingegen umfassen Informationen über den Absender, das Absendedatum, den Empfänger, die Größe der E-Mail, aber auch die Betreffzeile der Nachricht. Derartige Informationen sind vielfach sogar von größerem Nutzen für die Geheimdienste, da sie einfachere, schnellere und spezifischere Rückschlüsse über eine Person zulassen, als dies die Inhaltsdaten bei gleichem Aufwand erlauben würden. Diese Metadaten sind daher oftmals auch das begehrtere Gut für die NSA.

Das starke Interesse der NSA für Metadaten ist darauf zurückzuführen, dass ein jeder Mensch, der den Cyberspace nutzt, hierin über den Besitz und die Nutzung von elektronischen Geräten Spuren hinterlässt, mit deren Hilfe sich nahezu lückenlose Bewegungsprofile generieren lassen. Hierbei ist die Nutzung des Cyberspace in einem breiten Sinne zu verstehen. Darunter fallen nicht nur die offensichtlichen Praktiken wie die Nutzung von PCs, Smartphones oder ähnlichen Geräten, sondern auch der Umgang mit vielen weiteren, alltäglichen Geräten. So nutzen EC- und Kreditkartensysteme für die Abrechnung den Cyberspace genauso, wie ein Großteil der heutigen Telefonkommunikation digital verläuft. Dies betrifft dabei nicht nur Smartphone-Gespräche, selbst vermeintlich analoge Festnetzanschlüsse werden, dank Voice-over-IP-Technologie, inzwischen ebenfalls vielfach vollautomatisch in digitale Datenpakete umgewandelt und über den Cyberspace abgewickelt.

Geheimdienste, wie die NSA, haben somit ein hohes Interesse diesen Datenverkehr aufzufangen, abzuhören und auszuwerten. Die bisher von Edward Snowden veröffentlichten Dokumente machen dabei bereits jetzt deutlich, dass die NSA in ihrer Informationsbeschaffung einem Stufenmodell folgt. Diese Stufen sollen im Folgenden vorgestellt werden.

2.1 Die drei Stufen der Überwachung

Die Online-Überwachung der NSA folgt einem Drei-Stufenmodell, das abhängig nach Zugangsmöglichkeit des Ziels und der Kooperationsbereitschaft der jeweiligen Betreiber ausgeführt wird. Die drei Stufen schließen sich in ihrer Anwendung dabei nicht gegenseitig aus. Sie können vielmehr auch parallel Anwendung finden, wobei jedoch die Kosten für die NSA mit jeder Stufe ansteigen.

Auf der ersten und untersten Stufe steht die direkte Zusammenarbeit mit einem Unternehmen, etwa einem Internet Service Provider oder Internetdienstanbieter (ISP). Gerade bei US-Unternehmen oder Unternehmen, die auf US-amerikanischem Territo-

rium technische Einrichtungen besitzen, ist dies vielfach der erste und gängigste Weg. Die Unternehmen werden mit finanziellen Anreizen, zum Teil in Verbindung mit rechtlichem, richterlich durchgesetztem Zwang zur Kooperation verpflichtet. In der Abfolge übernehmen sie dann, im direkten Auftrag der NSA, Sammelaufgaben, leiten die Suchergebnisse entsprechend weiter und richten generell Zugangsmöglichkeiten für die NSA ein. Das NSA-Überwachungsprogramm „Prism" ist hierfür wohl das inzwischen bekannteste Beispiel, und doch steht es nur exemplarisch für eine ganze Reihe einer inzwischen nahezu unüberschaubaren Anzahl derartiger Systeme.

Wenn die interessanten Informationseinrichtungen außerhalb des US-amerikanischen Hoheitsgebietes liegen, so wird die zweite Stufe eingeführt. Hierbei baut die NSA auf die Kooperation mit Partnerstaaten bzw. deren Geheimdiensten. Auf dieser Stufe werden die Geheimdienste dieser Partnerstaaten als Intermediäre gebraucht, die, in Abbildfunktion der Methoden der NSA in den USA, die Kooperation mit den Unternehmen in ihren jeweiligen Ländern koordinieren und die Ergebnisse an die NSA weiterreichen. Die NSA besitzt, durch ihre zentrale Stellung als Informationsbeschaffer für Geheimdienste in vielen Drittstaaten, unterschiedliche Anreize und Möglichkeiten der Gegenleistung wie auch der Druckausübung, mit denen sie sich die Gefolgschaft der Partnerländer und deren Geheimdienste sichern kann. Dabei wird nicht jedes Land von der NSA gleich behandelt. So ist den Snowden-Dokumenten zu entnehmen, dass die USA 37 „approved SIGINT [Signals Intelligence; Anm. d. Verf.] partners" besitzen, die sie in unterschiedliche Gruppen (sogenannte parties) einteilen. Die erste Party oder Gruppe bezeichnet dabei die USA selbst. Zur zweiten Gruppe (second party) zählen Australien, Kanada, Neuseeland und das Vereinigte Königreich, also alle primär englischsprachigen Staaten. Die erste und zweite Gruppe bilden zusammen die inzwischen berühmt gewordenen *Five Eyes*, einen Verbund jener fünf Staaten, die seit dem Zweiten Weltkrieg besonders eng geheimdienstlich zusammenarbeiten. Deutschland zählt zusammen mit 33 anderen Staaten – zu denen die meisten europäischen Länder gehören – zur „third party", also einer Staatengruppe, mit der reger Geheimdienstaustausch stattfindet, die aber nicht ohne Vorbehalte betrachtet wird.

Die dritte Stufe ist der unilaterale Weg. Er wird von der NSA verwendet, wenn Unternehmen und/oder die entsprechenden Regierungen der Länder nicht gewillt sind, sich den Wünschen der NSA zu beugen und die entsprechenden Informationen und Zugänge bereitzustellen – oder eine Kooperation sehr unwahrscheinlich ist bzw. sich die Spionage gar gegen die betreffenden Länder selbst richtet. In diesem Fall handelt die NSA im Alleingang und ohne Kenntnis der entsprechenden Unternehmen oder Regierungen und besorgt sich die benötigten Informationen mit anderen geheimdienstlichen Methoden. Diese Informationsbeschaffung kann über verschiedene Wege erfolgen, etwa über das direkte Anzapfen der Glasfaserkabel und das „Abhören" der Kommunikation. Eine andere Möglichkeit ist die gezielte Manipulation der Technik, entweder durch Einspeisung von Schadsoftware zur geheimen Kontrollübernahme jener Techniken oder über die physische Einfügung veränderter oder additiver Hardware in

bestehende Systeme. Der Fall der Cisco-Router ist hierbei aufschlussreich. Diese Router wurden von der NSA im Versand heimlich abgefangen und mit entsprechender Hardware „nachgerüstet", bevor sie an ihre eigentlichen Empfänger zugestellt wurden (Greenwald 2014).

Dass sich die drei Stufen nicht gegenseitig ausschließen, sondern je nach Erkenntnisinteresse auch parallel erfolgen können, macht der Fall Google deutlich. So gewährte das Unternehmen Google im Rahmen des PRISM-Übereinkommens[2] der NSA bereits Einblick in ihre Daten. Dies hinderte die NSA jedoch nicht daran, sich zusätzlich zu dem bereits durch Google bereitgestellten Zugang noch einen weiteren und geheimen Zugang zu verschaffen (Gellman et al. 2013), um noch weitreichendere Informationen als die bereits von Google zur Verfügung gestellten zu gewinnen.

Diese Doppelstrategie der NSA, sich nicht nur auf das eine Programm Prism zu verlassen, sondern darüber hinaus auch andere Methoden anzuwenden, macht wohl am deutlichsten, dass Prism zwar das bekannteste Tool darstellt, letztlich aber weder das einzige, noch das wichtigste ist. Viel entscheidender ist womöglich die sogenannte Upstream Collection. Hierbei werden die Kommunikationsleitungen direkt am Backbone und anderen zentralen Leitungen angezapft und die anfallenden Daten und Metadaten direkt mitgeschnitten. Die rechtliche Grundlage für dieses Verfahren, mit dem auch die meiste Kommunikation innerhalb der USA überwacht wird, bietet bereits die *Executive Order 12333* des damaligen Präsidenten Ronald Reagan aus dem Jahr 1981. Ausgeweitet und auf den Stand der heutigen Massenüberwachung gebracht, wurde diese jedoch erst deutlich später. Dies lässt sich nicht nur mit der verbesserten Computertechnologie und dem Wandel vom Nischenphänomen Internet in eine Massentechnologie begründen. Beide mögen Bedingungen sein, die entscheidende Variable, das formative Ereignis, liegt hingegen bei den Anschlägen vom 11. September 2001. Der Schock, der durch die terroristischen Anschläge ausgelöst wurde, ermöglichte die Einführung umfassender Gesetzgebungen, die den verfassungsrechtlich verbrieften Freiheitsrechten entgegenstehen und die Befugnisse der US-Regierung massiv ausweiteten: USA-Patriot Act, FISA Amendement Act und andere Regelungen sind den meisten interessierten Bürgern zumindest vom Namen her bekannt und seit ihrer Einführung mehrfach verlängert, vereinzelt sogar verschärft worden. Durch diese und andere Regelungen genossen und genießen die US-Geheimdienste seit den Anschlägen vom 11. September 2001 nahezu alle Freiheiten bei der massenhaften Überwachung von Bürgern der USA und anderer Staaten. Ob dies indes mit der US-Verfassung vereinbar ist, daran gibt es nicht nur ernsthafte Zweifel: So hat am 7. Mai 2015 im Fall ACLU v. Clapper das Gericht entschieden, dass zumindest die „bulk collection" (massenhafte Sammlung) der Telefondaten von US-Bürgern illegal ist (Aclu v. Clapper 2015). Diese Praxis musste in seiner bestehenden Form ausgesetzt werden.

2 Zu dieser Gruppe gehörten neben Google noch Microsoft, Yahoo, Facebook, PalTalk, AOL, Skype, Youtube und Apple.

Dennoch: Welche Formen und Auswirkungen die Überwachungen bereits angenommen haben, und dies sowohl auf nationaler als auch auf internationaler Ebene, darüber sollen die beiden folgenden Unterabschnitte einen kurzen Einblick geben.

2.2 Nationale Ebene

Für die „Upstream Collection" also das bereits angesprochene direkte Abhören an großen Datenleitungen auf amerikanischem Boden, ist das sogenannte Fairview-Programm eines der umfangreichsten, auf das im Folgenden eingegangen werden soll.

Tabelle 1: Netzknoten vier großer ISPs in den USA

Major Communications Cables

– Points of Convergence – USA

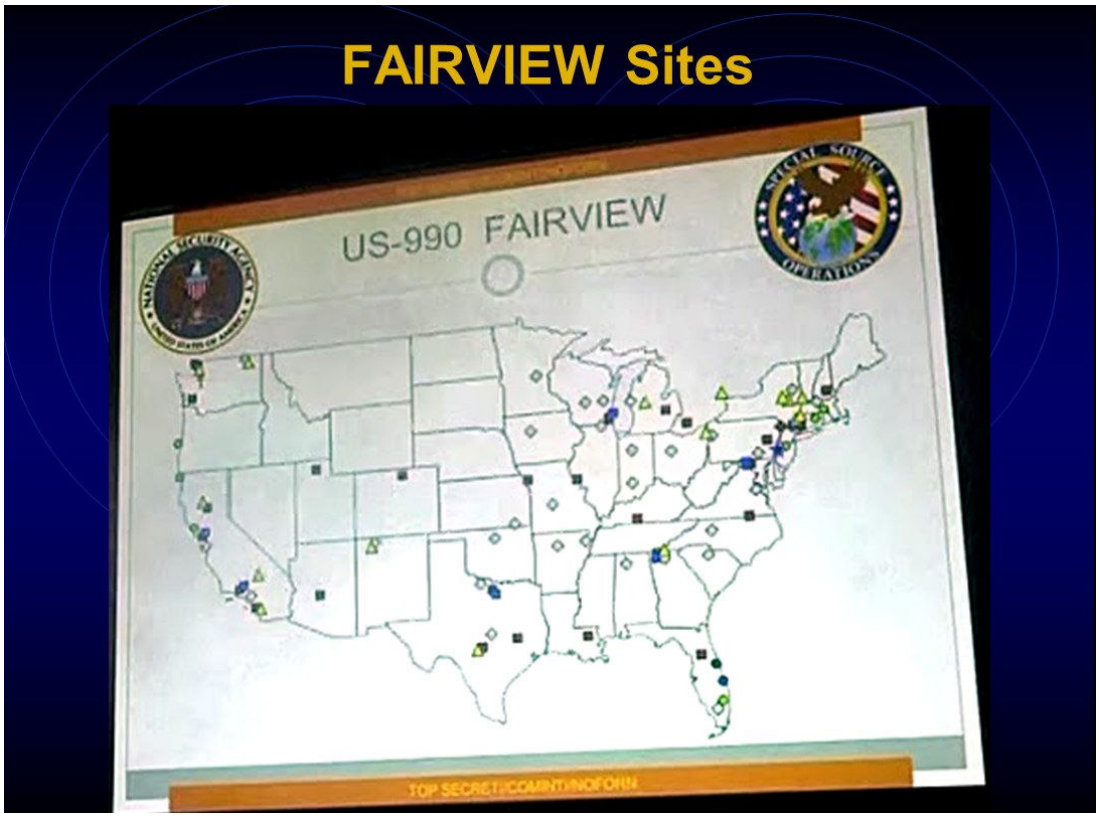
AT&T	**Verizon**	**British Telecom**	**T-Mobile**
New York	New York	New York	New York
Chicago	Chicago	Chicago	Chicago
Los Angeles	Los Angeles	Los Angeles	Los Angeles
Salt Lake City	Salt Lake City	Salt Lake City	
Denver	Denver	Denver	
Phoenix	Phoenix	Phoenix	
Kansas City	Kansas City	Kansas City	
Atlanta	Atlanta	Atlanta	
Miami	Miami	Miami	
Washington DC	Washington DC	Washington DC	
Seattle	Seattle	Seattle	
San Francisco	San Francisco		San Francisco
Dallas	Dallas		Dallas
San Joese	San Joese		
San Diego	San Diego		
St Loius	St Loius		
Orlando	Orlando		
Boston	Boston		
Newark	Newark	Newark	
		Houston	
	Philadelphia		Philadelphia
Nashville	Portland	Sunnyvale	
Cleveland	San Diego	Burbank	
	Las Vegas	Tucson	
	Detroit	Tampa	
	Charlotte NC	Eckington	
	Richmond		

Quelle: eigene Darstellung.

Ideale Standorte für eine effiziente Abhörung des Upstreams sind jene Orte, an denen möglichst viele Datenstränge zahlreicher Internetdienstanbieter sich kreuzen, die sogenannten (Internet-)Knotenpunkte. Die nachfolgende Tabelle 1 führt die Knotenpunk-

te vier großer Internetdienstanbieter (ISP) in den USA auf, jene von AT&T, Verizon, British Telecom und T-Mobile.

Abbildung 1: Map of FAIRVIEW SIGAD



Quelle: NSA 2013a.

Auf einer durch Edward Snowden veröffentlichen Landkarte (Abbildung 1) sind die Vereinigten Staaten übersät mit einer Vielzahl von unterschiedlich gefärbten kleinen Kreisen, Dreiecken und Quadraten, die jeweils verschiedene Aktivitäten sowie Speicher- und Leistungsfähigkeit einzelner Abhöreinrichtungen im Rahmen des Fairview-Programms symbolisieren. Jede dieser Anlagen kostet dabei zwischen 10 und 100 Millionen US-Dollar.[3] Untersucht man die Standorte der schwarzen Quadrate genauer und vergleicht ihre kartographische Verortung mit den Netzknoten von AT&T, so ist auffällig, dass sie nahezu deckungsgleich sind. Dies ist vermutlich kein Zufall, sondern Anzeichen dafür, dass die NSA für jeden der großen AT&T-Netzknoten einen Zugriffspunkt unterhält. Schließt man die übrigen Symbole der Karte noch in ähnliche Überlegungen mit ein, so ergibt sich daraus die begründete Vermutung, dass die NSA die Fähigkeit besitzt, quasi den gesamten relevanten US-Web-Verkehr abzuhören (d.h. Chat, Video, E-Mail etc.). Darüber hinaus kann die NSA – Schätzungen zufolge – auch 80 Prozent

3 Die großen Speicherzentren, wie in Fort Mead oder Utah, die allein im Bau bereits Milliarden US-Dollar kosteten, sind hierbei noch gar nicht mit eingerechnet.

aller Telefongespräche für 20 bis 30 Tage speichern; im Bedarfsfall und für Einzelfälle natürlich noch länger, gar unbegrenzt.

Der Erfassung und Speicherung dieser unfassbar großen Datenmenge stehen dabei nicht nur rechtliche und ethische Bedenken gegenüber, sondern auch ganz pragmatische. So sind 10.000 bis 20.000 Analysten mit der Auswertung der täglichen Massenüberwachung betraut. Diese Zahlen erscheinen zunächst sehr hoch, doch zugleich nehmen sie sich geradezu gering aus, wenn man sie den gut 300 Millionen US-Bürgern entgegenstellt, von denen sie Daten erhalten. Selbst mit den besten Analysetools fällt hierbei noch immer eine nicht zu bewältigende Datenmenge an. Es ist zu vergleichen mit einer beliebigen Google-Anfrage, die man bis zur letzten Seite überprüfen und durcharbeiten müsste. Die Folge dieser Massenanhäufung ist ein „Datenmasseversagen“ (bulk data failure). Die Geheimdienste versagen, nicht weil sie zu wenig Daten haben, sondern weil sie in den Datenmassen versinken.

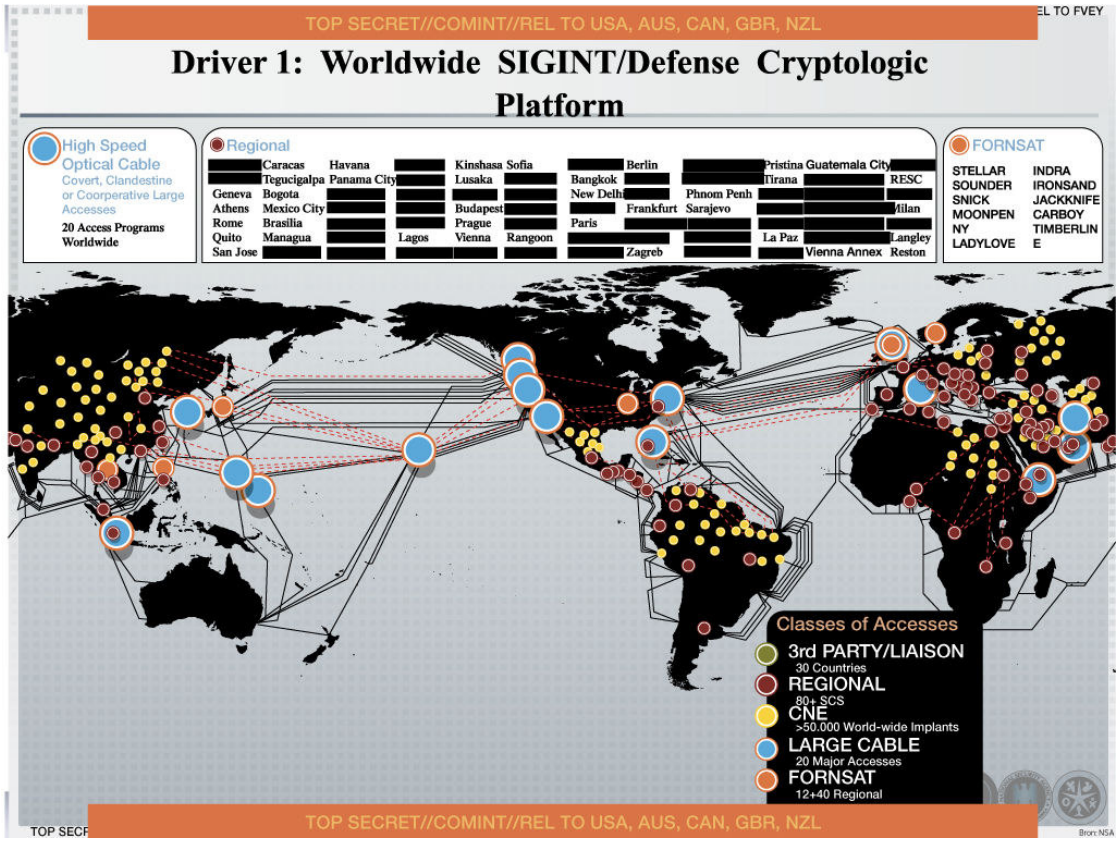
2.3 Internationale Ebene

Betrachten wir nun die Überwachung der internationalen Datenströme, also das Anzapfen an Orten außerhalb der USA, so zeigt sich ein kaum besseres Bild. Zwar wurden die Unterlagen Snowdens in der Worldwide SIGINT/Defense Cryptologic Platform (vgl. Abbildung 2) nur stark zensiert veröffentlicht und enthalten deshalb keine Informationen über die First Party (USA), noch zeigen sie die Zusammenarbeit mit Second (UK, Kanada, Australien, Neuseeland) oder Third Party Mitgliedern (Deutschland etc.); obgleich dies in der Vorschaugrafik angekündigt wird. Dennoch lässt sich Vieles über die internationale Zusammenarbeit der NSA aus der Grafik und den im Kontext veröffentlichten Informationen herauslesen. Von besonderem Interesse sind dabei die Computer Network Exploitations (CNE), d.h. Maßnahmen zur Ausnutzung von Computernetzwerken. Dabei gelingt der NSA das Abfangen und Abgreifen von Informationen am einfachsten über die Implementierung von zusätzlicher Soft- und/oder Hardware von Geräten und Anlagen in Schlüsselpositionen, wie es etwa in dem bereits erwähnten Fall der Cisco-Router erfolgte. Durch die Einbringung derartiger Soft/Hardware (so genannte Implants), schafft sich die NSA Hintertüren (Backdoors), die es ihr ermöglichen direkten Zugang zu den entsprechenden Computernetzwerken zu erhalten und sie zu deren eigentlichen Herren zu erheben. Die Hintertür befähigt die Agency alle für sie interessanten Informationen live einzusehen, mitzuschneiden und eine Kopie für spätere Untersuchungen abzuspeichern.

Wie viele derartige Implants die NSA tatsächlich installiert hat und wie viele der Geräte auch tatsächlich noch im Betrieb sind, ist weiterhin Teil wilder Spekulationen in der Netzgemeinde und der weiteren Öffentlichkeit. Erste Schätzungen und Berichte gingen von 50.000 derartigen Implants aus. Andere reichen aber bis zu einer Million und mehr. Am wahrscheinlichsten ist meiner Ansicht nach eher der niedrigere Wert, so dass es vermutlich „nur“ zwischen 50.000 und 100.000 Implants sind, die auch tatsäch-

lich zur Anwendung kommen. Dies ist jedoch kein Grund zur Erleichterung. Diese Anzahl – an den richtigen Schlüsselpositionen platziert – ist mehr als ausreichend, um eine nahezu lückenlose Überwachung zu gewährleisten und die elektronische Kommunikation jeder beliebigen Zielperson, gleich wo sie sich auf der Erde befindet, egal zu welcher Zeit und an welchem Ort, verfolgen zu können.

Abbildung 2: Worldwide SIGINT



Quelle: NSA 2013b.

Ein anderes NSA-Programm, das diese Massenüberwachung nutzbar machen soll, nennt sich Treasuremap. Es verspricht eine Kartierung des gesamten Internets, zumindest nach den veröffentlichten NSA-Dokumenten von Snowden: „Map the entire Internet – Any device, anywhere, all the time“ (Horchert 2014).

Den ungefähren Standort eines Gerätes zu bestimmen, ist dabei nicht sonderlich schwierig. Für das herkömmliche Telefonnetz lässt sich zumindest die Landesherkunft leicht erkennen, da das gesamte System durch das Global Public Service Telephone Network Switching System (PSTN) unterteilt ist. Nordamerika hat etwa die Eins, Westeuropa die Drei und Osteuropa die Vier.[4] Das System gliedert sich dann auf und lässt einige Rückschlüsse über die Herkunft des Anrufers zu. Ähnlich in der Art, aber in technischer Hinsicht deutlich zu unterscheiden, ist die Strukturierung des World Wide Web.

4 Den meisten Telefonnutzern dürfte diese Einteilung durch die gleichlautende Vorwahl für internationale Gespräche vertraut sein.

Im WWW besitzt jedes Gerät einen Machine Access Code (MAC) und eine Internetprotokoll-Adresse (IP). Jedes Gerät muss eine eigene, einzigartige Nummer besitzen, wenn es sich mit dem Internet verbinden möchte. Dies erfolgt über IPv4- oder IPv6-Nummern. Diese Nummern werden den Endgeräten von den ISPs zugeteilt, sind also nicht frei wählbar. Und auch den ISPs werden die IP-Adressen nur zugewiesen. Oberste Vergabestelle der IP-Adressen ist die Internet Corporation for Assigned Names and Numbers (ICANN) mit ihrer Internet Assigned Numbers Authority (IANA), die die IP-Adressen in Paketen an verschiedene Anbieter herausgibt.[5] Allein an der IP-Adresse und ihrer Zugehörigkeit zu einem bestimmten Paket lässt sich somit viel über den Aufenthalt einer Person oder zumindest ihres elektronischen Gerätes aufzeigen. Über die IP-Adresse und die Vergabe der Provider lässt sich somit der ungefähre geografische Standort des Benutzers verorten.[6] Für alles Weitere können dann die MAC-Adresse, GPS-Daten oder sonstige relevante Infos aus den Inhaltsdaten und Metadaten der Kommunikation herangezogen werden, um den exakten Standort der Person ausfindig zu machen.

Hierdurch ist aber nur angedeutet, was machbar ist. Welche Probleme sowohl in rechtlicher Hinsicht als auch in ganz pragmatischer Hinsicht mit dem Umgang dieser Datenmengen entstehen, davon handelt das nächste Kapitel.

3 Ineffizienz und rechtliche Bedenken

Prism, Treasuremap oder Fairview sind nur einige der führenden Programme, mit denen die NSA US-Bürger und Bürger anderer Nationen abhört und überwacht. Und der Wunsch der Agency nach noch mehr Zugriff, noch mehr Einblick und nach noch mehr Kompetenzen ist ungestillt. In den Folgen der Anschläge vom 11. September 2001 erhielten die Geheimdienste nahezu freie Hand und wurden in einer geradezu panischen Reaktion mit hohen Geldsummen und weitreichenden Befugnissen ausgestattet, ohne sich mit tiefergehenden Fragen nach Sinn oder Unsinn der Entwicklung aufzuhalten. Was folgte, war ein aufgeblähter, aus meiner Sicht völlig ineffizienter Geheimdienstapparat, der seine neue Macht nutzen und Kompetenzen rechtfertigen musste, ohne dabei aus den Fehlern zu lernen, die man nach den Anschlägen des 11. September eigentlich hätte ziehen müssen.

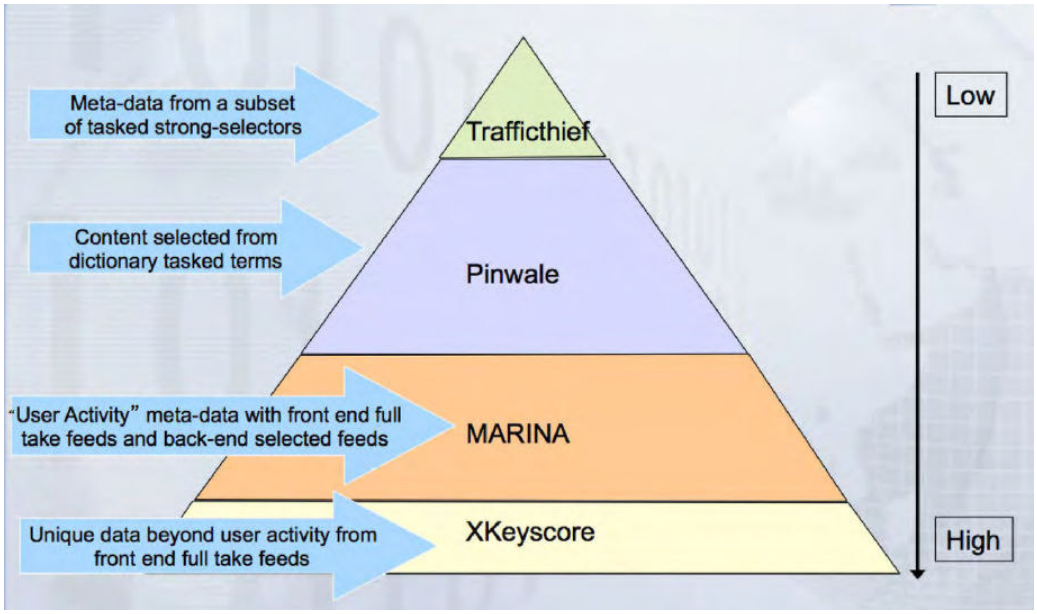
5 ICANN vergibt IP-Adressen an fünf internationale Registraturen (Regional Internet Registries, RIR), die zuständig sind für Afrika (AfriNIC), Nordamerika (ARIN), Lateinamerika und den Karibikraum (LACNIC), Europa, den Nahen Osten und Zentralasien (RIPE NCC) und den asiatisch-pazifischen Raum (APNIC). Diese RIR verteilen dann ihrerseits wieder IP-Adressen an Local Internet Registries (LIR) oder National Internet Registries (NIR), die sie an die Internet Service Provider (ISP) weiterreichen. Diese geben die Adressen schließlich an die Endnutzer aus. Jeder Zwischenhändler erhält die durch ihn zu vergebenden IP-Adressen natürlich nicht einzeln, sondern in größeren Paketen, je nach Ebene von einigen zehntausend für die ISPs bis zu Paketen von mehreren Millionen für die RIRs.

6 Natürlich gibt es auch hier technische Möglichkeiten, eine andere IP vorzutäuschen. Das resultierende technische Katz-und-Maus-Spiel soll hier aber nicht weiter diskutiert werden (vgl. etwa Stein 2010).

Die Anschläge von 9/11 konnten nicht deswegen nicht verhindert werden, weil nicht genügend Geheimdienstinformationen vorlagen. Im Gegenteil: Es lagen nahezu alle Informationen vor, die es ermöglicht hätten, die Terroristen rechtzeitig zu stoppen. Und noch weit mehr. Und genau hierin liegt das Problem: Die Anschläge konnten nicht verhindert werden, weil die Menge an Informationen so groß war und die Kommunikation unter den Diensten so gering, dass die Zusammenhänge nicht rechtzeitig erkannt wurden. Allein der 9/11 Commission Report von 2004 widmet diesem Versagen ein ganzes Kapitel, das unter der Überschrift „the system was blinking red" (Kean et al. 2004: Kapitel 8) steht. Die Anstrengungen sind zu vergleichen mit der Suche nach der Nadel im Heuhaufen.

Nach dem 11. September, nachdem man die Nadel übersehen hatte, wurden die Suchmannschaften verstärkt. Doch statt effizienter das Heu zu durchsuchen, wurde die Arbeitskraft nun darauf abgestellt, noch mehr Heu herbeizuschaffen. Die NSA-Überwachungen sind somit nicht nur ungesetzlich und verstoßen – meiner Ansicht nach – gegen die US-Verfassung, sondern sie erfüllen noch nicht einmal ihren angestrebten Zweck eines erkennbaren Sicherheitszuwachses. Die NSA erstickt förmlich in all den für sie nutzlosen Daten und ist derart angewachsen, dass sie ihre Arme überall hinaus ausstreckt, jedoch an zielgerichteter und gebündelter Schlagkraft für die Gefahrenabwehr eingebüßt hat.

Abbildung 3: DNI Discovery Options



Quelle: Bildausschnitt nach NSA 2014.

Wie fehlgeleitet die Perspektivität ist, entlarvt auch eine Dreiecksgrafik der NSA, bei der verschiedene Programme aufgeführt werden und deren „Erkenntnisgewinn" von Low (die Spitze des Dreiecks) zu High (seine Hypotenuse) bewertet wird (vgl. Abbildung 3). Die beiden obersten Stufen des Dreiecks, also der Bereich mit dem vermeintlich

geringsten Erkenntnisgewinn, genügen im Folgenden bereits, um die Verirrungen der NSA deutlich zu machen und ihre fehlgeleitete Gleichsetzung von Datenmenge mit Informationsgewinn zu verdeutlichen.

3.1 Bulk Data Failure: Weniger ist mehr

Auf einer Grafik der NSA wurden verschiedene Programme zusammengefasst und in Form eines Dreicks hinsichtlich ihres Nutzens gruppiert (vgl. Abbildung 3). An der Spitze und damit an der Stelle des geringsten Erkenntnisgewinns, steht „Trafficthief“, ein Programm das Metadaten nach einer Auswahl spezifischer Selektoren sammelt. Die NSA erwartet hierbei wenig Gewinn, es handelt sich um Daten von einem sehr engen Personenkreis. Sie verkennt, dass es genau dieser enge Personenkreis ist – ein Personenkreis von bereits Verdächtigen und mit tatsächlich bereits gesuchten Personen –, bei dem die Chance ausgesprochen hoch ist, weitere gefährliche Personen aufzufinden. In der bereits verwendeten Analogie gesprochen: Dieser Heuhaufen ist klein, und es wurde darin bereits eine oder mehre Nadeln gefunden.

Wird nun der direkte Vergleich mit der zweiten Stufe, mit „Pinwale“, gezogen, wird das Missverhältnis noch deutlicher. Pinwale operiert mit Inhalten die mit Hilfe von Schlagwörtern, d.h. Wörterbucheinträgen, operiert. Hierbei werden also Suchwörter ausgewählt und wann immer diese Suchwörter irgendwo bei Personen auftauchen, schlägt das Programm Alarm. Es ist im Grunde nichts anderes als eine Google-Suche, die eine scheinbar endlose Zahl an Treffern generiert, die aber dennoch überprüft werden muss, wenn man damit womöglich eine neue, unter Umständen tatsächlich gefährliche Person ausfindig machen möchte.

Wie häufig hierbei ein Fehlalarm ausbrechen muss, wie absurd das Vorgehen der NSA geworden ist, wird allein schon dadurch deutlich, wenn man sich die Suchbegriffe genauer anschaut. Eine solche mehrere hundert Wörter umfassende Selektorenliste musste das DHS bereits 2012 veröffentlichen (US Department of Homeland Security 2011: 20ff.). Zwar galt die damalige Liste nur der Überprüfung sozialer Medienseiten, für das Projekt Pinwale dürfte die Liste aber ähnlich, wenn nicht gar noch umfassender ausgesehen haben. Auf dieser Liste findet sich dabei eine ganze Reihe von Suchwörtern, die die Anzahl von zu überprüfenden Personen in astronomische Höhen treiben dürften, ohne tatsächlich signifikanten Mehrwert zu produzieren. So steht auf dieser Liste unter anderem das Wort „pork“ (Schweinefleisch). Dies heißt, wann immer – zumindest in diesem Fall innerhalb sozialer Medien – jemand das Wort „pork“ verwendet, verzeichnet die Suchmaske einen Treffer, und es muss untersucht werden, ob der Produzent der Äußerung sich im Kontext terroristischer Kreise bewegt.

Wenn wir beim Heuvergleich bleiben, so wird die Nadel nicht länger in einem Heuhaufen gesucht, sondern während der Heuernte, und es besteht keine Möglichkeit auch nur ansatzweise die täglich auflaufenden Mengen an neuem Heu zu überprüfen und abzuarbeiten. Doch auch bei einer spezifischeren Untersuchung, der Überwachung

von sozialen Netzwerken, zeigen sich das überaus bedenkliche Vorgehen der NSA und ihre gleichzeitige Verblendung.

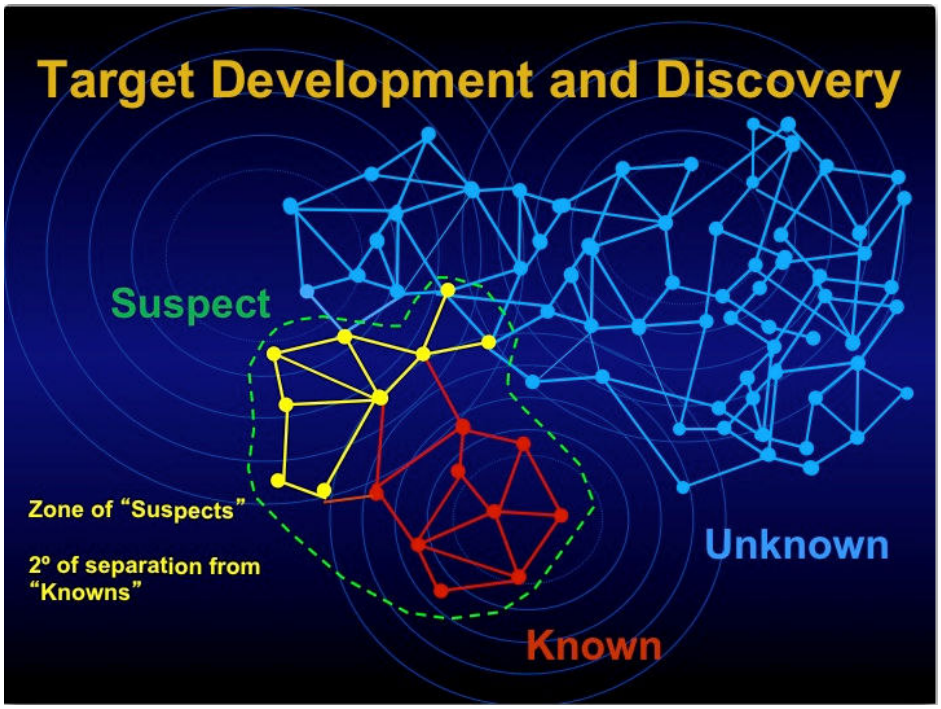
4 Überwachung sozialer Netzwerke

Programme wie jene im vorangegangenen Abschnitt beschriebenen sind ausgerichtet auf die anlasslose Überwachung vieler Menschen sowohl von US-Bürgern als auch Nicht-US-Bürgern. Das Ziel dahinter ist, die Möglichkeit zu besitzen, möglichst viele Menschen gleichzeitig und live zu überwachen. Die derzeitigen Fähigkeiten der NSA, dies effektiv zu tun, dürften sich indes auf einige wenige Millionen Nutzer belaufen. Das gesamte Überwachungssystem ist somit aufgrund der schieren Datenmasse bereits im Vorfeld zum Scheitern verurteilt. Viel nutzbringender wäre es natürlich nur diejenigen zu überwachen, die tatsächlich eine potentielle Gefahr darstellen, bzw. Personen zu identifizieren, bei denen dieses Potential signifikant ist. Die Frage ist klar: Wie kann man herausfinden, ohne alle Nutzer permanent zu überwachen, wer eine Gefahr für die Sicherheit darstellt? Eine Antwort darauf ist die „target development and discovery"-Methode, die in einer eingeschränkten und funktionalen Form von uns bereits in den 1990er Jahren vorgeschlagen wurde und die bei der NSA in einer anderen, einer pervertierten und dysfunktionalen Form Anwendung findet.

4.1 Eine theoretische Alternative

Die Idee hinter der „target development and discovery"-Methode ist es nicht, alle Menschen zu überwachen. Vielmehr geht es darum, ausgehend von bekannten Personen, die eine Gefahr für die Sicherheit darstellen, deren soziale Netzwerke zu überprüfen und dort nach weiteren verdächtigen Personen zu suchen. Dies erfolgt rein über die Metadaten und vollautomatisch, ohne dass ein Beamter Einblick in die Daten erhält. Auch die Inhaltsdaten der Personen werden nicht berührt oder gesammelt, und nur bei einem vermeintlichen Treffer wird diese Person genauer untersucht. In diesem Fall und nur in diesem Fall werden Inhaltsdaten erhoben, ausgewertet und die Person entweder als Bedrohung eingestuft und somit genauer observiert, einschließlich ihrer Kontakte, oder sie wird als falsch-positiver Befund auf eine Sperrliste gesetzt, so dass sie vom System unter den gleichen Verhaltensweisen und Parametern nicht mehr aufgefunden wird. Die gesamte Überprüfung des sozialen Netzwerks sollte dabei einer sog. Zwei-Sprung-Regelung folgen, das heißt, dass nicht nur Personen überprüft werden, die direkten Kontakt mit der bekannten Gefahr haben, sondern auch all jene Personen, die im sozialen Umfeld mit dem sozialen Umfeld der bekannten Gefahr stehen. Hierdurch kann das Problem von Mittelsmännern und indirekten Kontakten umgangen werden und eine größere Aufklärung erreicht werden (vgl. Abbildung 4).

Abbildung 4: Target Development and Discovery



Quelle: eigene Darstellung.

4.2 Die praktische Anwendung

Der NSA ging dieser Vorschlag aber damals nicht weit genug. Sie wählte eine Form, die den klaren Zuschnitt des vorgeschlagenen Programms pervertierte und schließlich auch nutzlos werden ließ. Dies liegt hauptsächlich an zwei Gründen: Zunächst einmal verwendeten die Analysten der Behörde für die Überprüfung des sozialen Umfelds keine Zwei-Sprung-Regelung, sondern eine Drei-Sprung-Regelung. Dies klingt zunächst wie ein geringfügiger Unterschied, der Zuwachs ist jedoch exponentiell. Gehen wir der Einfachheit halber davon aus, dass eine Person im weitesten Sinne 100 Menschen kennt – ein geringer Wert, doch soll er für das Beispiel genügen – so müssen bei einer Zwei-Sprung-Regelung 100^2 Menschen oder 10.000 Personen überprüft werden. Bei einer Drei-Sprung-Regelung sind es 100^3 oder 1.000.000 Menschen. Die Idee einer schlanken, zielgerichteten Methode wird somit zerstört.

Nach Bekanntwerden der Praktiken der NSA durch Edward Snowden kam auch gegen dieses Vorgehen der Überwachung vereinzelt Kritik auf und nach einiger Diskussion und Verhandlungen einigte sich die US-Regierung mit den Behörden Anfang 2014 auf eine Reduzierung der Regelung auf die Zwei-Sprung-Marke. Dies wurde als großer Erfolg gefeiert und als Zugeständnis an die Freiheitsrechte. Der Prozess dorthin erfolgte dabei erstaunlich widerstandsarm. Weder die NSA noch das FBI, CIA, DHS, DOD oder irgendeine andere Einrichtung bezog vehement gegen diese Einschränkung Position. Dieses Eingeständnis der benannten Institutionen sagt jedoch nichts über ihre jeweili-

ge Positionierung zugunsten der Freiheitsrechte aus. Es hat mit einem zweiten Grund zu tun, der die Einschränkung von Drei- zu Zwei-Sprüngen bedeutungslos werden lässt.

Anders als im propagierten Verfahren sind im NSA-Verfahren Personen innerhalb des sozialen Netzwerks nicht nur als Menschen gemeint, sondern auch juristische Personen, also Einrichtungen, Firmen, Unternehmen und dergleichen mehr. Dies hat zur Folge, dass jeder Kontakt eines Pizzalieferanten Teil der Sprungkette ist, genauso wie die eigene Regierung und auch Internetunternehmen. Allein durch Google, mit seinem Kundenkreis von monatlich deutlich über einer Milliarde Nutzern, wird so faktisch im Alleingang die Vollüberwachung nahezu aller Menschen legitimiert.

Vollüberwachung heißt in diesem Fall die Erfassung aller Metadaten und – ohne signifikante Hürden zumindest für nicht US-Bürger – auch aller Inhaltsdaten. Dies ist ein weiterer Unterschied zwischen dem vorgeschlagenen Entwurf und dem in Kraft getretenen Verfahren. Im vorgeschlagenen Verfahren wäre die Erstellung der Analyse der sozialen Netzwerke vollauf automatisiert erfolgt. Die Verbindungen wären maschinenbasiert erfolgt und die Daten und Metadaten verschlüsselt gewesen. Die NSA und ihre Mitarbeiter hätten keine direkte Einsicht in die Informationen, sondern nur dann, wenn das System auf Grundlage des Algorithmus eine möglicherweise verdächtige Person ausmacht.[7] Die NSA hätte dann mittels eines Antrags bei Gericht und Kongress die Entschlüsselungsrechte und somit Einblick in die Metadaten erhalten und bei einem dadurch erhärteten Verdacht auch Einsicht in die Inhaltsdaten bekommen. Dieses Vorgehen hätte sich prinzipiell für alle erfassten Nutzer anwenden lassen, zumindest aber für US-Bürger, deren Privatrechte im amerikanischen Recht deutlich besser geschützt sind als jene von Nicht-US-Bürgern.

Bedauerlicherweise kam dieses Verfahren nie zur Anwendung. Die Versuchung an derart viele Daten und somit vermeintlich auch an alle Informationen zu kommen, war einfach zu groß. Viel zu viel lässt sich damit bewerkstelligen. Die NSA ist dabei nicht die einzige Einrichtung, die Gefallen an einer derartigen Datenfülle gefunden hat. Auch bei anderen Einrichtungen wurden diesbezüglich Interessen geweckt.

5 Die weiteren Folgen der Massenüberwachung

Für das Auffinden neuer potentieller Straftäter sind Treasuremaps, Prism etc. wie auch die meisten anderen Verfahren denkbar ungeeignet, wie in den vorangegangenen Abschnitten gezeigt wurde. Für das Ausspähen bereits identifizierter Ziele sowohl rückwirkend, dank der umfassenden Speicherung, als auch im Rahmen einer Live-Verfolgung ist die Datenfülle und die Dichte des Abhörnetzes umso geeigneter. Die NSA arbeitet daher mit Nachdruck an Verfahren, alle abgefangenen Informationen zusammenzuführen, zu systematisieren und die Daten in eine personalisierte Timeline

7 Als verdächtig hätte noch nicht die Verbindung mit einer bereits identifizierten und als gefährlich eingestuften Person gezählt. Erst wenn ein doppelter Treffer, das heißt der Kontakt zu zwei bereits Bekannten und als Bedrohung registrierten Personen vorgelegen hätte, hätte das System eine Überprüfung veranlasst.

zu überführen. Dies gelingt bereits in vielfacher Form, so dass die NSA Programme nutzt, die Listen generiert, mit denen nicht nur alle Informationen, sowohl Metadaten und – wo vorhanden – auch Inhaltsdaten aus den verschiedenen Quellen, einzelnen Personen zugeordnet werden, sondern darüber hinaus auch die Kontakte zwischen den einzelnen Einträgen aufgezeigt werden können. Es lässt sich also mittlerweile minutiös nachzeichnen, wann eine Person im – elektronischen – Kontakt mit einer anderen stand und für wie lange. Und dies gilt für nahezu alle Menschen, also auch für jeden Kongressabgeordneten, jedes Mitglied eines Parlaments und jeden Regierungschef und jede Regierungschefin der Erde.

Eine derartige Masse an Daten über jeden Menschen, seien es auch „nur" Metadaten von US-Bürgern oder Meta- und Inhaltsdaten von Nicht-US-Bürgern, gebündelt in den Händen einer einzelnen Organisation, der NSA, ist bereits für sich selbst genommen mehr als besorgniserregend. Sie lässt sich aus meiner Sicht durch keine Antiterrorstrategie oder geheimdienstliche Aufklärung rechtfertigen. Doch wird es noch schlimmer: Die Erhebung der Daten durch die NSA soll dem Schutz des Landes vor terroristischen Bedrohungen dienen, doch eine derartige Datenfülle schafft auch Begehrlichkeiten bei weiteren Einrichtungen. So sind die Geheimdienste allein schon durch die reine Datenmenge nicht in der Lage, tatsächliche Vorhersagen zu treffen. Für den Bereich der strafrechtlichen Forensik, also das Auffinden von Straftätern nach begangener Tat, sind sie aber umso interessanter! Und die NSA scheint Anfragen von Ermittlungsbehörden nach Einsicht nur allzu gern nachzukommen. So können Polizei und Ermittlungsbehörden nach einem erfolgten Anschlag die Daten verwenden, um den oder die Täter zu finden. Doch war diese Nutzungsart nie Rechtfertigung noch Aufgabe der geheimdienstlichen Massenüberwachung. Sie wurden gegründet um terroristische Anschläge zu verhindern, nicht um nachträglich bei ihrer Aufklärung zu helfen.

Doch damit nicht genug. Auch hier hat die Begehrlichkeit nach den Datensätzen das Ermittlungsziel zur Aufklärung von Terroranschlägen und vergleichbaren Angriffen auf die nationale Sicherheit überholt und längst weitere Bereiche ergriffen, die nie Teil der Überwachungsaufgaben hätten sein sollen. So berichtete die Nachrichtenagentur Reuters bereits im August 2013 von einem Sondereinsatzkommando (SOD), das privilegierten Zugang zu den Daten der NSA hat und diese zur Aufspürung krimineller Aktivitäten nutzt (Shiffman et al. 2013). Innerhalb dieses Sondereinsatzkommandos finden sich Beamte sowohl der NSA, des FBI (Federal Bureau of Investigation; Bundespolizei/Inlandsgeheimdienst), der CIA (Central Intelligence Agency; der Auslandsgeheimdienst) wie auch des DHS (Department of Homeland Security; Heimatschutzministerium), aber auch der IRS (Internal Revenue Service; Bundessteuerbehörde) und des DEA (Drug Enforcement Agency; Drogenvollzugsbehörde), die alle nach verdächtigen Personen oder auffälligen Mustern suchen. Und dies in allen von ihnen angestrebten Bereichen, also auch im Drogenkampf oder bei der Suche nach Steuersündern. Die Daten sind vorhanden, also will man möglichst viel Nutzen daraus ziehen. Dabei kann eine Person bereits als verdächtig angesehen werden, wenn sie zu einer bestimmten religi-

ösen Gruppe zählt oder es sich etwa um einen Sympathisanten der Occupy-Bewegung oder ein Mitglied einer bestimmten politischen Partei handelt. All dies erfolgt ohne einen zuvor erstellten Haft- oder Untersuchungsbefehl und ohne Kontrolle durch den US-Kongress oder eine richterliche Anordnung. So stehen nach SOD alle Menschen unter Schuldverdacht, bis ihre Unschuld zweifelsfrei bewiesen ist. Und nicht umgekehrt, wie es nach geltendem Recht in den Vereinigten Staaten der Fall sein müsste.

Dies verstößt nicht nur gegen die amerikanische Verfassung. Es ist auch hinsichtlich der Ermittlungstechnik höchstproblematisch, was sowohl die NSA als auch das Sondereinsatzkommando zumindest geahnt zu haben scheinen. So zeigen die Snowden-Dokumente (RT 2013), dass die Ermittlungsbehörden für die Verfolgung von Verdächtigten und eine daran angeschlossene Anklage strengen Regeln unterlagen, die jedoch nicht dem Schutz der angeklagten Personen galten, sondern der Wahrung der Geheimhaltung der Massenüberwachung. Wie durch die Dokumente klar wurde, durften Informationen, die durch den Einsatz des Sondereinsatzkommandos gewonnen wurden, nicht mit anderen geteilt werden, nicht an die Öffentlichkeit gelangen und selbst bei einem angeschlossenen Prozess nicht den zuständigen Richtern, Verteidigern oder Staatsanwälten zugänglich gemacht werden, noch durften diese über die Daten in Kenntnis gesetzt werden; vom Informationsaustausch im Rahmen internationaler Rechtshilfe ganz zu schweigen. Die beteiligten Institutionen wurden vielmehr dazu aufgerufen, Parallelkonstruktionen zu schaffen. So sollten sie, auf Grundlage der bereits erfolgten Vor-Verurteilung durch die Daten der Massenüberwachung, mit konventioneller Ermittlungsarbeit neue und andere Beweise zusammentragen, die dann vor einem Gericht und der Öffentlichkeit Verwendung finden durften. Hierdurch ist weder ein ausgewogenes Sammeln von Beweisen, noch eine vorurteilsfreie Beurteilung dieser möglich, da die Schuld scheinbar bereits bewiesen wurde und nur noch auf anderem Wege vorgetragen werden muss.

Dieses Vorgehen, das laut Aussage des damaligen Direktors des FBI, Robert Mueller, bereits seit 2001 Verwendung fand, soll nun immerhin eingeschränkt werden. Präsident Obama hat diesbezüglich versprochen, dass fortan alle Angeklagten über die Quellen der Anklage informiert werden, so dass sie sich im Rahmen eines ordentlichen Verfahrens gegen die Anschuldigungen wehren können. Wie es eigentlich auch Rechtsvorschrift ist. Allein, es wurde weiterhin keine Aussage über all diejenigen getroffen, die im Rahmen dieses Überwachungssystems, ohne Kenntnis der Praxis und somit ohne Möglichkeit einer fairen Verteidigung, in den Jahren seit 2001 verurteilt wurden. Noch besteht irgendein Ansatz zur Änderung der weltweiten Überwachung. Das Überwachungssystem der NSA besteht also fort.

6 Konklusion

Der vorliegende Beitrag stellte die Überwachungstechniken der NSA im Cyberspace vor, wie sie durch den Whistleblower Edward Snowden bekannt geworden sind und

lieferte eine anschließende Untersuchung und kritische Bewertung der verwendeten Praktiken. Im Fokus der Kritik stand hierbei die rechtlich problematische Überwachung bei gleichzeitigem Vorwurf der Ineffizienz des Programms. Komplementiert wurde die Kritik durch die Skizzierung eines funktionalen Gegenentwurfs, der eine effizientere Geheimdiensttätigkeit unter höchstmöglicher Wahrung individueller Freiheitsrechte ermöglichte.

Innerhalb des Beitrags wurden eine Reihe von Überwachungsmethoden der NSA vorgestellt und ihre Umsetzung wie auch Auswirkung genauer untersucht. Dabei wurden die Praktiken der Überwachung dem Drei-Stufenmodell der NSA zugeordnet, bei dem sich die Überwachungs- und Informationsbeschaffungsmaßnahmen anhand der Einbindung Dritter orientieren. Sie reichen von der Zusammenarbeit mit (US-) Unternehmen (1), über die Kooperation mit befreundeten Regierungen oder deren Geheimdiensten (2) bis hin zum eigenmächtigen Vorgehen der NSA (3). Hierbei wurde sowohl auf die unterschiedlichen rechtlichen Positionen von US-Bürgern gegenüber Nicht-US-Bürgern in der Überwachung eingegangen als auch auf den verschiedenartigen Gehalt von Inhaltsdaten und Metadaten hinwiesen.

In der Bewertung der Überwachungspraktiken zeigte der Beitrag, dass die angewandten Methoden aus vielfacher Hinsicht höchst problematisch sind. So wurde auf die eklatante Schieflage von Sicherheitsrechten zu Ungunsten von Freiheitsrechten eingegangen sowie eine Anzahl (verfassungs-)rechtlicher Bedenken als auch bereits gerichtlich bestätigter Übertretungen angeführt. Diese Vorwürfe wiegen umso schwerer, als sie sich nicht einmal über den scheinbaren Mehrwert an Sicherheitszuwachs rechtfertigen lassen. Es wurde gezeigt, dass die Überwachungsprogramme in höchstem Maße ineffizient arbeiten, da sie sich mit einem Übermaß an unwichtigen Informationen konfrontiert sehen, die den Blick auf die wirklich wichtigen Daten verstellen.

Letztlich verdeutlichte der Beitrag, dass, obgleich die Enthüllungen Edward Snowdens eine Welle der Empörung bezüglich der Praktiken der NSA auslöste, sich in der Tätigkeit der Überwachung durch die NSA kein fundamentaler Wandel abzeichnet. Die Reaktionen sind minimal und vielfach kaum mehr als kosmetischer Natur. Für einen echten Wandel bedarf es vielmehr der stärkeren Kontrolle durch Gerichte und Parlamente sowie einer informierten und kritischen Öffentlichkeit, die sich der Freiheit des Einzelnen verpflichtet fühlt.

Literatur

ACLU v. Clapper (2015): Second Circuit Court of Appeals Ruling in ACLU v. Clapper (Docket No. 14-42-cv), USCourts.gov. 2015-05-07. (25.07.2015).

Gellman, Barton / Soltani Ashkan (2013): NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say, in: The Washington Post, 30.10.2013, https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html (12.07.2015).

Greenwald, Glenn (2014): Glenn Greenwald: how the NSA tampers with US-made internet routers, in: The Guardian, 12.05.2014, http://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden (07.07.2015).

Horchert, Judith / Grothoff, Christian / Stöcker, Christian (2014): NSA-System Treasuremap: „Jedes Gerät, überall, jederzeit", in: Spiegel Online, 17.09.2014, http://www.spiegel.de/netzwelt/netzpolitik/nsa-wie-der-geheimdienst-mit-dem-system-treasuremap-daten-sammelt-a-991496.html (20.07.2015).

US Department of Homeland Security (2011): Analyst's Desktop Binder, http://de.scribd.com/doc/82701103/Analyst-Desktop-Binder-REDACTED (20.07.2015).

NSA (2013a): Map of FAIRVIEW SIGAD, in: wikipedia.org: https://commons.wikimedia.org/wiki/File%3AUS-990_Fairview_Map_-_crop.jpg (20.07.2015).

NSA (2013b): Worldwide SIGINT/Defense Cryptologic Platform, in edwardsnowden.com, https://edwardsnowden.com/de/2013/11/23/worldwide-sigintdefense-cryptologic-platform/ (20.07.2015).

NSA (2014): DNI Discovery Options, in ACLU.org, https://www.aclu.org/foia-document/dni-discovery-options (20.07.2015).

RT (2013): DEA agents use NSA intercepts to investigate Americans – report, in: RT Question more, 05.08.2013, http://www.rt.com/usa/dea-agents-nsa-evidence-067 (20.07.2015).

Shiffman John / Cooke Kristina (2013): Exclusive: U.S. directs agents to cover up program used to investigate Americans, in Reuters.com, 05.08.2013, http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805 (20.07.2015).

Stein, Thomas (2010): Intrusion Detection System Evasion durch Angriffsverschleierung in Exploiting Frameworks, Diplomica Verlag: Hamburg.

Kean, Thomas H. / Hamilton, Lee (2004): The 9/11 Commission Report. Final report of the National Commission on Terrorist Attacks upon the United States. Official government: Washington, D.C.

Autor

William Binney

Ehemaliger Technischer Direktor der National Security Agency und US-amerikanischer Nachrichtendienst-Mitarbeiter

DOI: 10.11588/josar.2015.0.23485

From Anonymity to Identification

A. Michael Froomkin

1 Introduction

This is not a cheerful paper, which mirrors the lecture from which it is adapted.[1] It is not cheerful because the prognosis for effective online anonymity has become progressively less and less cheerful.

By anonymity, I mean something strong: the ability to speak without anybody being able to identify you. This untraceable anonymity is the highest level of technical protection for speech (cf. Froomkin 1995). That it is untraceable brings with it the ability to speak without fear of jail, harm, or other retaliation. This strong version of anonymity is controversial. The arguments for why untraceable anonymity is a good thing include the idea that it contributes to human flourishing; people want to experiment, and the ability to experiment with less fear contributes to human self-realization. In places that are less free, avoiding retribution for saying the wrong thing may be a matter of life and death. Political dissidents, ethnic minorities, religious splinter groups, people campaigning for women's rights or gay rights, and many others are, or have been, subject to the risk of genuine and very palpable violence. If they wish to speak or write for their causes they need a means to protect themselves. Anonymity is one such tool.

For those of us who do not face the danger of personal violence in retaliation for our writings, there are nonetheless other more subtle dangers. One is the danger of profiling. Profiling enables stereotypical discrimination on the basis of sexual orientation, political opinion, or other characteristics. Less serious, but annoying, is the effort commercial entities make to profile for marketing purposes.

Anonymity is a way to defend against that profiling, a protection that is desirable not just because some find it creepy or uncomfortable to be profiled, but also because the people doing the profiling could actually exercise market power by doing price discrimination (DeLong et al. 2000).

When the Internet started, one byproduct of the architecture of the Internet was that online anonymity was easy to achieve. It required only minimal technical knowledge, or fairly simple tools, or assistance from the right people. In those days you

1 The lecture from which this paper is adapted was delivered at the University of Heidelberg on Dec 11, 2015, under the auspices of the Netzpolitik AG of the University of Heidelberg. I am very grateful to Dr. Wolf J. Schünemann and all my hosts for the invitation and the warm welcome. Unless otherwise noted, this paper attempts to reflect legal and technical developments up to May 1, 2015.

could be anonymous and have a great deal of faith in being successfully untraceable. Cryptography made this possible. PGP – "Pretty Good Privacy" – was one of the early and important tools, perhaps the first consumer-oriented cryptography. Another very important tool was the secure anonymous remailer (cf. Froomkin 1997: 129).

An anonymous remailer works as follows: Alice sends out an email destined for Bob which contains within it one or more layers. Each layer consists of an encrypted message, which I will call the payload, and unencrypted delivery instructions, making the entire message something like a sealed paper letter with an address written on the front. Although destined for Bob, Alice addresses the message to a remailer operator. The remailer operator strips off the headers of Alice's email – the part that identified it as coming from her – and forwards the payload message as directed. Alice could direct that the payload go to a second remailer, who would decrypt the payload only to find in it another layer of address and (to him) unreadable payload. By chaining the message in this manner through two or more remailers, Alice could ensure that before the message reached Bob its origins would be thoroughly obfuscated. What is more, if Alice and Bob used encryption to exchange messages, then none of the remailer operators would ever know what Alice was saying. Even if Bob was not so sophisticated, only the last remailer in the chain would be capable of reading the cleartext, and that person would have no way of finding out who originally sent the message unless every remailer in the chain kept logs and cooperated in unraveling the message's path.

Sending messages this way was never easy, and would be harder today because there are fewer reliable remailers. Remailers ran into two serious problems. The first is that spammers abused the remailer network. Strangely, a small amount of spam is a good thing for the remailer network because the spammers can be relied on to create a certain volume of traffic and this makes it harder for any observer to trace the genuine messages as they move through the network (ib.). But in short order the volume of spam increased to the point that so much spam went through the network as to first burden it and then choke many of the remailers entirely (Canter 2003).

Worse, the remailers faced a serious legal problem. The end point in any chain of remailers – the exit node – carries legal risk for misuse of the network. If, for example, your computer was used to send a death threat to the US President, ignorance of the message's content was not a comforting defense, and certainly was no shield against an investigation. To say that the entire process was automated did not necessarily provide a sufficient defense either.[2] As governments and police departments became more technologically savvy, the email operators increasingly decided it was just too unsafe to run a remailer, or at least to run an exit node. As fewer and fewer remailers were willing to be exits, the ones that persisted became overwhelmed with all the

2 Notably, the protections of the CDA against civil liability for third-party postings do not apply to criminal law. 47 U.S.C. §230(e)(1).

spam that sought release into the greater Internet, thus accelerating the network's death spiral.

Almost all these anonymity systems depended on some kind of cryptography. Western governments, and in particular the U.S. government, worked very hard to slow the spread of consumer cryptography. Governments were basically able to restrict the spread of cryptography, originally through export control (Froomkin 1996: 15–75). By preventing standardization, they made it easier to maintain the wiretapping and interception capabilities of both national security services and ordinary law enforcement. For many years this project of prevention was successful, and consumer cryptography was rare; indeed, only specialists used it – the presence of strongly encrypted traffic was sufficiently unusual to raise the possibility that observers might use it as a signal that one had something to hide, drawing extra attention from the authorities.

All these things undermine access to anonymity (in the strong sense). We can divide the history of Internet communications into three periods when using anonymity as a yardstick. In the first period, as noted above, anonymity was easy if you knew what you were doing, but it was not available easily to the consumer. This period ended when the remailers died off and strong anonymity was reduced to what I would call a 'safety valve' technology. That is, although it was no longer as easy for the technologically adept to achieve strong anonymity, it was still technically feasible. That mattered: if you were, for example, a sufficiently motivated dissident organization – you could be anonymous if you had to be. But for most people anonymity was either not available at all or it was foreseeably traceable: it was predictable that governments or others could trace the author without extraordinary effort. Today, anonymity online is not even a safety valve: it is increasingly difficult, sometimes impossible, for everyone.

2 The source of the demise of anonymity

Today the outlook for online anonymity is much worse than it has ever been before, and there is, I fear, little hope for improvement. The sources of this change extend well beyond the government surveillance revealed in the Snowden revelations (Strohm et al. 2014; Greenwald 2013; Kelion 2013; ib. 2014; Gellman 2013; Ball 2014; cf. Ball et al. 2013). There are in fact five reasons for this development. First, there is a widespread ideology that says anonymity is a bad thing in itself and ought not to be allowed. A second source is the profit motive. It turns out that there is quite a lot of profit in not having anonymity. The next two things are technological. Both governments and the private sector built a series of tools that greatly improve their abilities to track users online. These technologies are synergistic with other tools that enhance the linkages between online and off-line tracking. Off-line tracking is already prevalent and still growing, which means that it is ever harder to be anonymous online. Where in the past we observed the online world intruding into, and altering, the real world, now we

see the reverse: the real world invades and affects the online. And last – because it was somewhat late to the party – is the law, both at the national and the supra-national level.

Powerful motives animate the effort to make anonymity traceable, or indeed impossible. The most visible of these motives is the felt needs of national security, an argument pressed with increasing energy since 9/11. This concern over security is fueled by the fear that bad actors are using (or will use) this technology to inspire others to do harmful things, and that it empowers communications among terrorists who will be working in secret. The spies and policeman, it is claimed, will be left defenseless.

It is easy to imagine the anonymity issue from the point of view of a government official. A reasonable official might well believe that if she refrained from deploying some available technology of surveillance, and then something terrible happened, everybody would blame her. This scenario is what many officials actually believe, and this belief therefore pushes the people in government towards ever-increasing surveillance (Baker 2010: 5, 72).

This tendency in government, to push for technologies of identification in fear of not being able to catch someone doing something bad, is a truly global phenomenon. It is found in the UK (c.f. UK Identity Cards Act 2006: c.15), Australia (Parliament of Australia 2015), and in Pakistan (Computer Science and Telecommunications Board 1996: 438). Iran recently announced mandatory identification for everybody who goes online – as soon as they can figure out how to do it (The Economic Times 2011; Sharma 2011). India has been monitoring electronic communications for many years. It has a very elaborate and expensive centralized monitoring system, aimed at the Internet, called the "Lawful Intercept and Monitoring System" (Singh 2013).

The Indian story is instructive as it shows some of the limits of the law as a tool for combatting even government surveillance. Indian courts said that the Indian government needed a warrant to access email and telephonic communications (Prakash 2013). As a condition of receiving a license to operate, all internet service providers (ISPs), and all telecom providers, are required to provide the Indian government direct access to all communications passing through their systems, and must do so without a warrant (Freedom House 2014). India also requires that the carriers make sure that only weak encryption is used with their equipment in order to ensure that everything they carry is very easily accessible to authorities (Verma 2015). Furthermore, privacy safeguards built into the "Lawful Intercept and Monitoring System" appear to be ignored (Singh 2013).

Some other countries are not spending quite as much money as India and are not quite as strong in their licensing requirements, but they are enforcing identification nonetheless. In many countries, a major method of access to Internet is through cyber cafés. To destroy anonymity, governments pass a law that says cyber cafés must ask for ID and keep a log of who is using which machine at what time. This creates a record

that the government can always access if it traces a message's IP number to a particular machine in a cybercafé, thus allowing it to link the message to a person.

In the United States, the view that anonymity is dangerous is associated with Justice Scalia of our Supreme Court, who wrote in a 1995 dissent that anonymity is generally dishonorable because "[i]t facilitates wrong by eliminating accountability, which is ordinarily the very purpose of the anonymity" (McIntyre 1994: 514 U.S. 334, 385). To create legal protection for anonymous communication absent a reason to expect "threats, harassment, or reprisals," he argued, "seems to me a distortion of the past that will lead to a coarsening of the future" (ib.: 334, 385). However, in the *McIntyre* case as well as in other recent decisions (cf. Watchower Bible 2001: 536 U.S. 150, 166), the Supreme Court has found that there is a right to anonymous speech in the US Constitution. That means US citizens and permanent residents are protected against US laws criminalizing or otherwise preventing anonymous speech. We are not protected against government actions that have the side effect of making anonymous speech impossible nor against anonymity-blocking actions in the private sector. Thus, although we have a constitutional right, it turns out not to be as meaningful as it probably sounds.

In other countries, such as the UK, identification is incentivized by liability rules. The UK Defamation Act 2013 amended the UK's libel laws to stop the problem of people going to the UK and suing for Internet speech that originated somewhere else. The new Act provides that it is a defense for a website operator to show that she was not the author of the challenged material, but only if the identity of the real author is readily apparent, or if the website operator has complied with regulations concerning how to respond to notices of alleged defamation (Defamation Act, 2013: c. 26 U.K.). This puts pressure on the website owner. If the website owner cannot identify the speaker, then she has 48 hours following notice of the libel claim to take down the post or the speech is treated as her own (ib.). The United States, of course, is at the other extreme. Section 230 of the Communications Decency Act immunizes the owner of the website for almost all hosted third party speech unless the plaintiff can show that the website owner said it himself. Most other countries do not take that view, and a website operator is responsible for policing whatever speech appears there.

The United States, and other countries, also adhere to another important ideological view that has worked against anonymity, an ideology of responsibility that is rooted in feminist ideas. Numbers of feminists, including one of my colleagues (Franks 2011: 224–261; ib. 2012: 655–704), think it is tremendously important to punish people harming women online. Feminists point to “revenge porn,” the posting of nude pictures of ex-girlfriends as a form of oppression that they want to eliminate, and have ignited a movement sweeping the US to require website operators either to identify the source of the picture or be held responsible for it themselves (Peterson 2015). The consequences for anonymity are obvious. If you are creating a website capable of hosting photographs posted by others, you cannot know in advance what sort of photo-

graphs will be posted there. Therefore, under this regime, you have to be able to find everybody who uses your website for fear they might post one of these pictures.

3 The technological drivers of the demise of anonymity

Other technologies neither give people notice nor a choice as to how they will be identified. “Trusted computing” is a set of technologies designed to serve the needs of digital rights management (DRM). The theory is that users cannot be trusted, and hence content providers need to know exactly who is accessing their content. Manufacturers put an identification chip into a device, and design the operating system to allow third parties to see the ID, but prevent the device’s owner from masking the ID (Woodford 2004: 253–280). Content providers love this, as it permits them to append a unique identifier to every licensed download that encodes the user’s ID without the machine owner’s knowledge. That way, if a digital copy of the content should turn up on somebody else’s machine, the rights-owners will know who to sue.

The protection of intellectual property rights is a globally accepted norm. The problem with ‘trusted computing’, however, is that the same technology that enables strong DRM can easily be accessed by other applications designed to identify the user. The fundamental design feature of ‘trusted computing’ is that the user can have no control over it, or at most very limited control over it (Anderson 2011).

The profit motive obviously drives DRM; it also drives other attempts to ensure that customers are identified. Recently, MasterCard made a submission to Australian regulators in a formal procedure in which the Australian government was trying to decide how and whether to regulate BitCoin, a somewhat anonymous payment technology (Hajdarbegovic 2014). MasterCard made a very strong submission to the Australian regulator which said, we are regulated and have to know our customers and therefore no one else should be allowed to provide anonymous payment services. "[A]ll participants in the payments system that provide similar services to consumers should be regulated in the same way to achieve a level playing field for all" (ib.). And that level playing field should involve maximal consumer transparency, thus "consumer protection, anti-money laundering (AML), counter-terrorist financing (CTF) and stability should be the cornerstones of any regulation of electronic payments, including digital currencies"(ib.).

MasterCard’s sole proposal was that nobody should have privacy by law, and no one should be allowed to offer it. That is a disturbing indicator suggesting that the desire to protect the profit and business models of companies that heavily invested in identification technology has set off a race to the bottom in which regulations will be invoked to limit competing privacy-enhanced products. One would have much preferred to see a so-called ‘struggle to the top’ in which firms competed to provide privacy-enhanced products.

Indeed, identifying technologies are already widespread. Some are operated at the ISP level, some are in telephones, and some operate at the legal level. You cannot talk today about any online issue without talking about telephones. Predictions are that telephones will be eclipsing PCs very shortly as a means to get online (Standage 2013). Telephones come configured as a privacy wasteland. Because the engineering of the cell phone network is entirely about identifying the user, your phone is constantly providing data about you and that information is used to identify you and link to offline databases.

In the United States, if a person walks into a store it is perfectly legal for the store to detect the wi-fi signal that their phone emits as it tries to connect to a network. That signal has a unique identifier. It permits the store to track customers as they move around the store, and it links to that record if the customer ever revisits the store. Linking the customer to a past purchase may make it possible to send the customer advertisements or discount coupons.

From a strictly pocketbook point of view, this might be a good thing for consumers as they get offered a discount. Indeed, this is the method by which most phone-based technology, most apps, convince people not to be too concerned. The surveillance is sold to consumers as empowering, in the sense that it makes possible the functionality of the app. But one need only look at a modern smart phone to see the great breadth of the permissions which installed apps require in order to function. It is common on installation to see a great mismatch between the permissions that the app asks for and what it actually needs to function. On my phone, apps commonly demand to have access to my location, even though they are not a name- or location-based service. The choice is to take it or leave it. And we take it. And thus there is no privacy if you use your phone.

4 Political drivers of the demise of anonymity

But it gets worse. If you are using a cell phone, or an old fashioned telephone, or a computer, to access the internet, there is probably one – if not several – government-sponsored data collection devices monitoring your communication. This is one of the things we learned from Edward Snowden, and even before him, where people had stumbled upon these strange rooms in ISPs company where there were far more computers, recorders and wires than had any right to be there (Hepting 2008; In re NSA 2008). We know from statistics that came out in the Snowden revelations that as of May 2012, US security services and their allies had collected technical information on about 70 percent of the cell phone networks in the world. They had data on 701 out of 985 known cell phone networks (Ferranti 2014). As for the physical undersea cables that move communications transnationally, it is believed that every one of those cables has a tap attached to it (Khazan 2013), which is why some countries now want to

build their own undersea cables (Scola 2014), which I interpret, perhaps cynically, to mean they want to own the taps.

The information architectures we use route our information via strange places, such as "the cloud", further undermining our privacy. One could encrypt all one's data so that tapping the cloud would be less useful, but few people do that. And even encryption has become an uncertain friend. This is another thing we have learned from the Snowden revelations: that the US National Security Administration (NSA) has worked quite hard in two known cases – and, we fear, in others that we don't know about – to weaken encryption standards in a way which makes them easier to break (Arthur 2013). These decryption projects still take some computation, but much less than would be required if the algorithms had not been engineered to carry hidden defects. The tools meant to protect us and protect our information are no longer reliable. It is no longer reasonable to have faith in even those international standard-making processes that had been the gold standard for reliable cryptography, because very subtle changes were introduced into these processes via government employees supposedly working independently in a private capacity (The Economist 2013). As investigators and analysts discover these weaknesses, they propose new and one hopes better standards. But that still leaves a large unpatched installed base which can take a long time to catch up to the new versions, if indeed they are capable of being patched and the new versions are compatible.

In contrast, sometimes the things that would identify us are put out in the open for everyone to see, but that can provoke resistance. An example comes from the Domain Name System (DNS), which uses what are called IP numbers. IPv4 is the old system and the address space is nearly used up. It has only 2^{32} numbers, or about four billion possible numbers, which is fewer than the number of people on the planet. The internet is in the process of moving to IPv6, which offers us 2^{128} numbers, which is about 340 decillion, enough in theory to give every person on earth several octillions of IP numbers and still have plenty left over (Goldman 2012). The original IPv6 specification for email required that every email packet would include the MAC number in the header, uniquely identifying the device that sent the packet. As a result, every packet sent would be immediately traceable to the device that sent it. This created such a furor that the Internet Engineering Task Force (IETF) came out with an alternate, if optional, standard which includes privacy enhancements (Narten et al. 2007).

It remains possible that by going to the public library, or to the university, or to the cyber café, one can avoid being linked to a message – so long one does not have to show ID to use the public computer, and so long as there is no camera there watching who is using the equipment. But today, both government and private security cameras are ubiquitous indoors and out, making it nearly impossible to be anonymous offline.

5 Self-Surveillance as a driver of the demise of anonymity

And then there is self-surveillance. Twitter, Instagram, Facebook, all offer opportunities to sabotage one's own privacy. Using a decent camera and increasingly accurate of facial recognition software, we have now gotten to a point where if you have a Facebook account, there is a 75% chance that a computer can match a picture taken of you to your Facebook account in less than 2 seconds (Acquisti et al. 2014). Not having a Facebook account is little protection. If somebody else on Facebook took a picture of you and tagged it, it is the same as doing it yourself.

The public and private data collectors are almost merged outside of the EU, practically the only place where there are significant limits on data re-use. In the rest of the world, and especially in the US, they are all sharing with each other. In the United States all sorts of government information, including some disclosures required to obtain certain permits, is for sale. Meanwhile the marketers are selling their data to the government, which uses it for ID authentication among other things. In the name of national security, the US is also building ever-larger databases, which brings us to the world of big data. The internet of things means that we will have all sorts of devices that talk to each other on the internet, so your refrigerator will know when you are home, it will know what you are eating and it will tell your insurance company about your diet. Your life insurance rates will be adjusted according to whether you ingest too much cholesterol.

6 Law and the demise of anonymity

So where does law fit into all this? The common-law nations have approached the Internet with a three-step procedure. The first step has been to look at some of the activity on the internet, like email and electronic documents, and to try to categorize those things, or those activities, as akin to something familiar, both because this is how lawyers think and because it is less work.

When that approach failed to cover all the new phenomena, or just could not be made to fit because that internet thing was too different, the next step was to create new categories or in some cases to create new institutions like ICANN.

Meanwhile, there was a third step: a bold attempt to turn back the clock. New channels of speech, new channels of commerce, and of course new methods of copying and sharing content, each discomfited and disrupted established practices or threatened profitable business models belonging to powerful institutions. In the case of law enforcement, common investigative techniques seemed to be at risk. These institutions sought to prohibit the new things that endangered the established order. For a long time the best example of this was the campaign by Big Copyright for DRM. Copyright interests carried out a successful campaign to enact new copyright restrictions, to protect against digital technologies, and to get the law to make copyright violation an increasingly serious offense (Digital Millennium Act 1998). The *loi Hadopi*

was an example of this in France (Dejean et al. 2010), until it was struck down (Conseil Constitutionnel 2009), although even then copyright interests secured passage of a corrective, known as "Hadopi 2"(Loi 2009-1311 du 28 octobre 2009).

7 A goldfish bowl society

The push against anonymity has had even greater success than the push against copyright violations. Copyright violations are still ongoing; we need only consider the cases of torrent sites, or the notorious Pirate Bay (Cook 2014), to see that. But for those seeking to speak anonymously, there really is no place to go. There is more identification and more surveillance online – especially through the linking of the online and offline – than I think has ever before existed in human history. We have radically overcompensated. The Internet plus cellphones, plus sensors, equals basically a goldfish bowl society, and we are the goldfish.

The state can use this privacy-compromising technology in all kinds of overt and subtle ways. The subtle ones may be worse than the overt ones because people become nervous about doing things, the so-called chilling effect. We have seen examples of this in New York City where the police created a Facial Recognition Unit to identify suspects – and demonstrators – via Instagram and Facebook (Weis 2013). Ukraine had a demonstration recently, and the government set up a fake cell tower – stingray is the name of the technology – collecting information on cellphones held by the people in the area. It then sent text messages, "Hello, we are the police. Your position has been reported and being at an illegal demonstration, just thought you'd like to know we know" (Merchant 2014). This is a way of keeping people home. It works.

In the West, we have used the law to enlist key intermediaries as our identity collectors. Here the template was the banking system, which has for many years been subject to "know your customer" rules in which banks and other financial intermediaries must collect information about people before accepting their deposits and processing their payments. ISPs, the choke points in the internet ecology, were next. There has been a gradual effort to get ISPs to collect as much information about their customers, and their customer's communications, as the cellphone company gathers. As is well known, U.S. law has special Constitutional protections for speech (US Constitution Amendment I), and supposedly against government searches (US Constitution Amendment IV). It is worth pointing out when you mix the adoption of encryption with the legal protection of anonymous speech, it creates a major tension that U.S. law has not yet resolved. The legal problem exists because every packet of encrypted digitized data looks alike from the outside. If the legal system imagines that there might be any class of disfavored and thus unprotected speech, whether it is pirated movies, terrorist conspiracies, obscenity, or revenge porn, widespread encryption undermines the ability to control the spread of that content. And if a key element of that control involves finding the party responsible for the bad speech, cryptography-based anonymity tech-

nology becomes a major problem. The technological measures necessary to be able to pierce anonymity must be applied to every packet on the network or it is meaningless. Either we allow as much anonymity as users want, or we allow none at all.

8 Safeguarding anonymity

Can anonymity online be saved? The question currently makes sense only for computers, because for cellphones the game is fully lost. To protect identities in the cell phone world would take a whole new hardware, a whole new architecture, and given the size and value of the installed base and the power of incumbent carriers, one has to ask if this is even possible. Even for the world wide web, reclaiming space for real anonymity would take many changes. It would take the full encryption of the web transport mechanisms (Casaretto 2014).[3] It would require the repeal of all laws that enable digital inspections, in which the government can look inside the packet to tell whether it is a bad packet or a good packet. It would require control of ongoing efforts of national security agencies to collect and store all the metadata information that describes where the packet came from and where it is going. And, crucially, it requires standards we can trust. This is the biggest barrier, because that trust requires relying on a mathematical expertise that only a small number of people have.

To make email anonymity real, we would need many things we do not have at present. To start, we would need a widely shared encryption tool; in addition we would need an infrastructure of remailers, a thing that is quite unlikely for all of the reasons mentioned above, notably the spam and the legal risks.

More generally we would need a deeper and broader understanding of what privacy means and why it matters. Because ultimately the anonymity problem is converging with the big data problem: the more that governments and firms place sensors everywhere and collect masses of information about everyone online and off and then use it to build profiles about us, the less there is any place to hide. Thus, we must now ask whether there are the legal or social solutions to the problem of these profiles.

9 Data retention

It is true that on the data retention question alone we have relatively good results, especially in the EU. There was a major decision by the European Union Court of Justice in April 2014 annulling the proposed data retention rules (Digital Rights Ireland 2014), and it did so on the basis of the European Convention of Human Rights, and on case law from the European Court of Human Rights, which importantly opens the doors to linking these two sets of law. Henceforth, in the EU data retention cannot be general but must be necessary and proportionate. Data collected for one purpose can only be re-used for law enforcement if there is a link to a specific threat to public safe-

3 Although growing quickly, current https traffic remains a small fraction of total web traffic, being only 3.8% in North America in 2014, 6.1% in Europe, and 10.37% in Latin America.

ty and the risk of stigmatization stemming from inclusion in the police data basis is limited. Either before this decision, or as a result of it, the national courts in many countries of the EU have struck down data retention. Many more countries have challenges pending.

But outside Europe it is a different story. In Australia, data retention is proceeding apace. Indeed outside of Europe and the U.S. we don't have at the moment mandatory data retention, we just have an open door. A number of Latin American countries are discussing data retention laws. To the extent that some people look to the Inter-American Convention on Human Rights (Inter-American Commission on Human Rights 1969), there is a little relevant case law. And then in Asia, and especially in China, there tends to be even less scope for anonymity.

In the United States as a formal matter, we do not have a data retention mandate at present. But there is a terribly fictional element to that claim as we have learned that our government is already gathering and storing massive amounts of communications traffic (Ball 2014).

10 Some unintended consequences of the Snowden revelations

This brings us to yet another perversity in privacy and security policy. In addition to all their positive effects, the Snowden revelations may have two other unanticipated negative effects. Let me not be misunderstood; so far, the consequences have been positive. But we need to understand what all the consequences may be. One likely consequence is that a number of governments will now officially make legal what was previously done secretly. We are already seeing this in Ireland which is setting up a new system of surveillance in which ISPs and telephone companies can be required to provide data to the government and if they are unwilling there is a new secret court to make them – in effect creating a whole new judicial system (Lillington 2014). The second thing is that we now know that the NSA has been collecting data domestically on a large scale. This was a major secret, so much so that it greatly constrained the NSA's willingness to share data with civilian law enforcement authorities although it did not completely prevent it (Fakhoury 2013). The NSA apparently feared that information about its capabilities and activities might come out in court, and the NSA considered this knowledge to be a national secret of too high value to take that risk.

Now we find ourselves in a different place. We now have evidence that the NSA and its companion agencies in several other countries have been capturing communications and sharing them with each other (Corera 2013). As a result, it seems only logical that the NSA and other nations' security agencies too, will become much more willing to share the fruits of their communications acquisition with domestic law enforcement agencies. If and when this comes to pass, privacy actually might become weaker as a result of Snowden's exposure of these surveillance technologies.

11 The limited potential of International Human Rights law

Lawyers naturally wish to find solutions to social problems in the law. After all, if access to anonymity is so closely tied to the preservation of autonomy and personal privacy, and if this problem is indeed global in scope, that sounds as if it should be an international human rights problem. Can International Human Rights (IHR) law do the job here? Again, I have a rather pessimistic assessment. There is no real sign that IHR law provides the tools to address this problem, and if it could, the enforcement mechanisms outside the EU are notoriously weak. Although there is some basis in IHR law to seek protection for privacy, broadly defined, it is not the same as anonymity and indeed it is fairly clear in most of the relevant instruments that anonymity is something they wish to exclude from protection. Indeed, a rare clear discussion of the protection of anonymity in IHR law is found in the Council of Europe's Declaration of Freedom of Communication on the Internet of 2003 where it says on article 7, principle 7:

> In order to ensure protection against online surveillance and to enhance the free expression of information and ideas, member states should respect the will of users of the Internet not to disclose their identity. This does not prevent member states from taking measures and co-operating in order to trace those responsible for criminal acts, in accordance with national law, the Convention for the Protection of Human Rights and Fundamental Freedoms and other international agreements in the fields of justice and the police (Council of Europe, Committee of Ministers 2003).

So even there, in what is perhaps the high watermark for protection of anonymous speech in IHR law, we see major carve-outs and limitations.

But this is still more than we find in other instruments. Article 19 in the Universal Declaration in Human Rights provides that "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers" (UN 1948). Similar protections of communicative freedom appear in other important international agreements, for example Article 19 of the International Covenant on Civil and Political Rights (UN 1976), but in every case either implicitly or more commonly explicitly the relevant rights are hedged with the idea that *ordre publique* or something similar justifies finding the identity of the speaker – that it is important to ensure that communicative freedom is not used for crime. Thus the International Covenant on Civil and Political Rights provides for a number of important communicative freedoms and then qualifies them by saying that they "may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary" whether for the "respect of the rights or reputations of others" or "for the protection of national security or of public order, or public health or morals" (ib.; Grisby 2014).[4] Those are very broad categories.

4 On November 25, 2014, the third committee of the UN General Assembly adopted a resolution that calls on states to "respect and protect the right to privacy" in the digital age. Surveillance of digital communications "must be conducted on the basis of a legal framework". The final Report, however, removed text from an earlier draft that said surveillance needed to conform with principles of pro-

The EU idea is better, but only somewhat. The EU seems to believe that large amounts of personal data may be collected, but once the data are collected it is possible to impose limits on reuse. From my pessimistic perspective, proportionality means that the information is going to be available, waiting to be analyzed, waiting to be used, if a government body finds that there are sufficient grounds to do so. One is asked to trust the people holding the information, despite what we have learned from Snowden.

12 Conclusion and outlook

That trust approach is different from the appeal of anonymity in the strong sense. Anonymity is a safety valve technology when trust is absent or the future uncertain. In a world of increasing surveillance we have never needed that safety valve more than we do today. It provides a mechanism, one at present complex and not utterly reliable, from which we derive some hope of blocking the growth of profiling, and some hope of communicating without it necessarily being traced back to us – because otherwise everything can be traced back to us. Neither in domestic law nor in international law do we see a strong commitment to anonymous speech at a time when it is so much in need of protection. I think that Justice Scalia spoke for many people, particularly those in power, when he said he thought there was something fundamentally dishonorable about anonymous speech (McIntyre v. Ohio Elections Comm'n 1995).

Many governments simply do not trust their people and are afraid of honest speech because it might lead to something revolutionary. Others may not fear revolution but they fear crime, hate speech, or the theft of intellectual property. So the combination of these things means there is basically no constituency for anonymity at the international level nor at the government level other than a few NGOs – but they do not get to make national, much less international, law. Add in the bilateral and multilateral trade treaties that often create new protections for intellectual property, and recall that many of these protections will require identification in order to be effective. The bottom line is that anonymity online is not just in danger, but on life support.

The plight of online anonymity can no longer be seen as just a technical issue. It is political. The anonymity issue is an inextricably interconnected with technical issues for the standards for phones and for computers, for apps, for 'trusted technology', for intellectual property. It is connected to strong market-based incentives because there is money to be made from identification and profiling. Anonymity also suffers from its connection to very powerful imperatives and bureaucratic incentives in the name of national security.

The anonymity issue has merged into the online privacy issue, and the online privacy issue is merged into the offline privacy issue, and in fact has become just the privacy

portionality, legitimacy, and necessity—principles that are not [explictly] contained in the International Covenant on Civil and Political Rights (ICCPR) (ib.).

issue with no adjectives. The question therefore is really to what extent consumers and voters are going to decide they care about privacy. And the history so far suggests that the answer is that they care a little bit, not zero, but not enough to push against all the other forces deployed in this arena. I continue to believe that the lack of panic is primarily because most people do not truly understand how much they are being surveilled – because surveillance, especially online, remains mostly invisible. I think there is still hope; if we can make surveillance more visible, there is hope that enough people will get excited about the issue to matter. But this is only a hope and in no way a certainty.

In the process of offering anonymity as a response to surveillance, it will be important to deal with the very legitimate, and if not legitimate certainly honestly and deeply felt, concerns of people who think that there is something wrong with anonymity, that it encourages people to be bad. Part of that solution will be to devise other ways to deal with the bad things people do online. So, for example, if we had a consensus for ridicule and social ostracism of people who are the sources of revenge porn (most of whom will be known to the victims), and also for those who enable them, this might help prevent it and reduce the calls for ubiquitous deployment of identification technology.

Although not all is lost yet, realistically one must conclude that the prognosis for strong anonymity is fairly grim. I invite you to prepare to enjoy swimming in the digital goldfish bowl.

Bibliography

Acquisti, Allessandro / Gross, Ralph / Stutzman, Fred (2014): Face Recognition and Privacy in the Age of Augmented Reality, in: Journal of Privacy and Confidentiality 6:2, 1, http://repository.cmu.edu/jpc/vol6/iss2/1/ (24.07.2015).

Anderson, Ross (2011): Trusted Computing 2.0, in: Light Blue Touchpaper), https://www.lightbluetouchpaper.org/2011/09/20/trusted-computing-2-0/ (26.06.2015).

Arthur, Charles (2013): Academics criticize NSA and GCHQ for weakening online encryption, http://www.theguardian.com/technology/2013/sep/16/nsa-gchq-undermine-internet-security (22.06.2015).

Baker, Stewart A. (2010): Skating on Stilts, Hoover Institution Press: Stanford, CA.

Ball, James / Ackerman, Spencer (2013): NSA loophole allows warrantless search for US citizens' emails and phone calls, http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls (15.07.2015).

Ball, James (2014): NSA collects millions of text messages daily in 'untargeted' global sweep, http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep (15.07.2015).

Canter, Sheryl (2003): Hiding Your Identity, PC Magazine, http://www.pcmag.com/article2/0,2817,1230752,00.asp (14.07.2015).

Casaretto, John (2014): The Internet strikes back, Global encrypted SSL traffic booms, http://siliconangle.com/blog/2014/05/20/the-internet-strikes-back-global-encrypted-ssl-traffic-booms/ (26.06.2015).

Computer Science and Telecommunications Board (1996): Cryptography's Role in Securing the Information Society, National Academy Press: Washington, D.C.

Conseil Constitutionnel (2009): Décision n° 2009-580 DC du 10 juin 2009, http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/2009/decisions-par-date/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html (24.07.2015).

Cook, James (2014): The Pirate Bay Speaks Out About the Police Raid That Shut It Down: 'We Couldn't Care Less', http://www.businessinsider.com/the-pirate-bay-speaks-out-about-the-police-raid-we-couldnt-care-less-2014-12 (22.06.2015).

Corera, Gordon (2013): Spying Scandal: Will the 'five eyes' club open up?, http://www.bbc.com/news/world-europe-24715168 (22.06.2015).

Council of Europe, Committee of Ministers (2003): Declaration on Freedom of Communication on the Internet, article 7, principle7, https://wcd.coe.int/ViewDoc.jsp?id=37031 (24.07.2015).

Defamation Act, (2013): chapter 26 (U.K.), http://www.legislation.gov.uk/ukpga/2013/26/contents/enacted (15.07.2015).

Dejean, Sylvain / Pénard Thierry / Suire, Raphaël (2010): Une première évaluation des effets de la loi Hadopi sur les pratiques des Internautes français, http://www.marsouin.org/IMG/pdf/NoteHadopix.pdf (17.08.2015).

DeLong, J.B. / Froomkin, A.M. (2000): Speculative Microeconomics for Tomorrow's Economy, in: Internet Publishing and Beyond: The Economics of Digital Information and Intellectual Property, http://www.law.miami.edu/~froomkin/articles/spec.htm (14.07. 2015).

Digital Millennium Act (1998): 17 U.S.C. §512, 1201 to 1205, 1301 to 1332, 28 U.S.C. §4001.

Digital Rights Ireland Ltd v Minister for Communication (2014): Joined Cases C-293/12 & C-594/12, 11-16 (Ct. Justice E.U. Apr. 8, 2014), http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=161279 (26.06.2015).

Fakhoury, Hanni (2013): EFF, DEA and NSA Team Up to Share Intelligence, Leading to Secret Use of Surveillance in Ordinary Investigations, https://www.eff.org/deeplinks/2013/08/dea-and-nsa-team-intelligence-laundering (24.07.2015).

Ferranti, Marc (2014): NSA Spy Program Targets Mobile Networks Worldwide, http://www.pcworld.com/article/2856352/nsa-spy-program-targets-mobile-networks-worldwide.html (22.06.2015).

Franks, Marry Anne (2011): Unwilling Avatars: Idealism and Discrimination in Cyberspace, in: Columbia Journal of Gender and Law 20: 224–261.

Freedom House (2014): India, Freedom on the Net, https://freedomhouse.org/report/freedom-net/2014/india (15.07.2015).

Franks, Marry Anne (2012): Sexual Harassment 2.0, in: Maryland Law Review 71: 655–704.

Froomkin, A. Michael (1995): Anonymity and Its Enmities, in: Journal of Online Law Article 4, http://groups.csail.mit.edu/mac/classes/6.805/articles/anonymity/froomkin.html (14.07.2015).

Froomkin, A. Michael (1996): It Came From Planet Clipper, in University of Chicago Law Forum.

Froomkin, A. Michael (1997): The Internet As A Source Of Regulatory Arbitage, in: Kahin, Brian / Nesson, Charles (eds.): Borders In Cyberspace, MIT Press: Cambridge, Mass.

Gellman, Barton (2013): NSA broke privacy rules thousands of times per year, audit finds, http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html (15.07.2015).

Goldman, David (2012): The Internet Now has 340 Trillion Trillion Trillion Addresses, http://money.cnn.com/2012/06/06/technology/ipv6/ (22.06.2015).

Greenwald, Glenn (2013): NSA collecting phone records of millions of Verizon customers daily, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (15.07.2015).

Grisby, Alex (2014): UN Committee Adopts Resolution on Right to Privacy in the Digital Age, in: Council on Foreign Relations: Net Politics, http://blogs.cfr.org/cyber/2014/12/01/un-committee-adopts-resolution-on-right-to-privacy-in-the-digital-age/ (26.06.2015).

Hajdarbegovic, Nermin (2014): MasterCard Seeks 'Level Playing Field' for Bitcoin Regulation, http://www.coindesk.com/mastercard-seeks-level-playing-field-bitcoin-regulation/ (22.06.2015).

Hepting v. AT&T, 539 F.3d 1157 (9th Cir. 2008).

In re National Security Agency Telecommunications Records Litigation, 564 F. Supp.2d 1109 (N.D.Cal. 2008).

Inter-American Commission on Human Rights (1969): http://www.cidh.oas.org/basicos/english/basic3.american%20convention.htm (26.06.2015).
Khazan, Olga (2013): The Creepy, Long-Standing Practice of Undersea Cable Tapping, http://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/ (16.07.2015).
Kelion, Leo 2013: Q&A: NSA's Prism internet surveillance scheme, http://www.bbc.com/news/technology-23027764 (15.07.2015).
Kelion, Leo (2014): Edward Snowden: Leaks that exposed US spy programme, http://www.bbc.com/news/world-us-canada-23123964 (15.07.2015).
Legal Information Institute (n.y.): 47 U.S. Code § 230 - Protection for private blocking and screening of offensive material, https://www.law.cornell.edu/uscode/text/47/230 (15.07.2015).
Lillington, Karlin (2014): Surveillance by a Government-sponsored secret system, The Irish Times, http://www.irishtimes.com/business/technology/surveillance-by-a-government-sponsored-secret-system-1.2033443 (26.06.2015).
Loi 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet, http://legifrance.gouv.fr/eli/loi/2009/10/28/JUSX0913484L/jo/texte (26.06.2015).
McIntyre, Joseph (1994): Certiorari to the Supreme Court of Ohio No. 93-986. Argued October 12, 1994-Decided April 19, https://supreme.justia.com/cases/federal/us/514/334/case.html (15.07.2015).
McIntyre v. Ohio Elections Comm'n (1995): 514 U.S. at 385 (Scalia, J. dissenting), https://supreme.justia.com/cases/federal/us/514/334/case.html (24.07.2015).
Merchant, Brian (2014): Maybe the Most Orwellian Text Message a Government's Ever Sent, Motherboard, http://motherboard.vice.com/en_ca/blog/maybe-the-most-orwellian-text-message-ever-sent (26.06.2015).
Narten, Thomas / Draves, Rich / Krishnan, Subramanian (2007): Privacy Extensions for Stateless Address Autoconfiguration in IPv6, RFC 4941, http://www.ietf.org/rfc/rfc4941.txt (26.06.2015).
Parliament of Australia (2015): Telecommunications (Interception and Access) Amendment (Data Retention) Bill, http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5375 (15.07.2015).
Peterson, Andrea (2015): Activists in the war against revenge porn are finally seeing results, in: The Washington Post, http://www.washingtonpost.com/blogs/the-switch/wp/2015/02/20/activists-in-the-war-against-revenge-porn-are-finally-seeing-results/ (26.06.2015).
Prakash, Pranesh (2013): How Surveillance Works in India, in: The New York Times, http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/?_r=1 (15.07.2015).
Scola, Nancy (2014): Brazil Begins Laying Its Own Internet Cables To Avoid U.S. Surveillance, https://www.washingtonpost.com/news/the-switch/wp/2014/11/03/brazil-begins-laying-its-own-internet-cables-to-avoid-u-s-surveillance/ (22.06.2015).
Singh, Shalini (2013): Govt. violates piracy safeguards to secretly monitor Internet traffic, in: The Hindu, http://www.thehindu.com/news/national/govt-violates-privacy-safeguards-to-secretly-monitor-internet-traffic/article5107682.ece?homepage=true, (26.06.2015).
Sharma, Amol (2011): RIM Facility Helps India in Surveillance Efforts, in: Wall Street Journal, http://online.wsj.com/article/SB10001424052970204505304577001592335138870.html (15.07.2015).
Standage, Tom (2013): Live and Unplugged, http://www.economist.com/news/21566417-2013-internet-will-become-mostly-mobile-medium-who-will-be-winners-and-losers-live-and (22.06.2015).
Strohm, Chris / Wilber, Del Quentin (2014): Pentagon Says Snowden Took Most U.S. Secrets Ever, Bloomberg Business, http://www.bloomberg.com/news/articles/2014-01-09/pentagon-finds-snowden-took-1-7-million-files-rogers-says (15.07.2015).
The Economic Times (2011): RIM gives India access to Messenger services, http://articles.economictimes.indiatimes.com/2011-01-14/news/28430015_1_security-architecture-corporate-email-blackberry-enterprise-server (15.07.2015).
The economist (2013): Cracked Credibility, http://www.economist.com/news/international/21586296-be-safe-internet-needs-reliable-encryption-standards-software-and (22.06.2015).
UK Identity Cards Act (2006): chapter 15, http://www.legislation.gov.uk/ukpga/2006/15/pdfs/ukpga_20060015_en.pdf (15.07.2015).

UN (1948): The Universal Declaration of Human Rights, Article 19.
UN (1976): International Covenant on Civil and Political Rights, Article 19.
US Constitution Amendment I, http://www.usconstitution.net/xconst_Am1.html (24.07.2015).
US Constitution Amendment IV, http://www.usconstitution.net/xconst_Am4.html (24.07.2015).
Verma, Vivek Kumar (2015): Digital Encryption Laws in India, https://indiancaselaws.wordpress.com/2015/02/10/digital-encryption-laws-in-india/ (26.06.2015).
Watchower Bible & Tract Society of New York, Inc., et al. v. Village of Stratton et al. (2001): Certiorari to the United States Court of Appeals for the Sixth Circuit No. 00-1737. Argued February 26, 2002-Decided June 17, 2002, https://supreme.justia.com/cases/federal/us/536/150/case.html (15.07.2015).
Weis, Murray (2013): High-Tech NYPD Unit Tracks Criminals Through Facebook and Instagram Photos, http://www.dnainfo.com/new-york/20130325/new-york-city/high-tech-nypd-unit-tracks-criminals-through-facebook-instragram-photos (27.06.2015).
Woodford, Chad (2004): Trusted Computing or Big Brother? Putting the Rights Back in Digital Rights Management, in: University of Colorado Law Review 75, 1253–1317.

Author

Prof. A. Michael Froomkin
Laurie Silvers & Mitchell Rubenstein Distinguished Professor of Law
University of Miami
School of Law
1311 Miller Drive, Coral Gables, FL 33146
froomkin@law.miami.edu

DOI: 10.11588/josar.2015.0.23480

Im Netz der Geheimdienste – strafrechtliche Aspekte der Massenüberwachung im Internet

Kai Cornelius

1 Einleitung

Wer regiert das Internet? Im November 2014 wurde die Aufdeckung der Spionagesoftware Regin gemeldet. Diese wurde im laufenden Betrieb analysiert. Damit können Daten kopiert, Tastatureingaben protokolliert, die Kamera eingeschaltet oder gleich die vollständige Kontrolle über den Rechner übernommen werden (vgl. Symantec 2014: 14–15). Wer über ein so mächtiges Werkzeug verfügt, dem kommt aufgrund der nahezu allumfassend anmutenden Wissensherrschaft eine unerhörte Macht zu (vgl. Boehme-Neßler 2014: 825 unter Verweis auf das Francis Bacon 1597 zugeschriebene „scientia est potenzia"). Dieser Drang nach Wissen ist nichts Besonderes: Seit es Menschen gibt, gibt es Geheimnisse. Und genauso lange gibt es Menschen, die hinter die Geheimnisse der anderen kommen möchten, sei es aus wirtschaftlichen, militärischen oder politischen Gründen (vgl. Kloepfer 2002: § 1 Rn. 55 zum Einsatz von Informationen als Herrschaftsmittel). Ein Mittel dafür ist die Spionage. Nicht wenige Forscher bezeichnen die Spionage als „zweitältestes Gewerbe der Welt" (vgl. Stürmer 2006: 21; Reinhard 2007: 234). Dabei stellt sich in einem demokratischen Rechtsstaat immer wieder die Frage der Kontrolle und Rechtskonformität des verdeckten Erlangens der Informationen.

Dem wird sich der nachfolgende Beitrag unter zwei Aspekten widmen – einerseits der Massenüberwachung im Internet durch Geheimdienste, bekannt geworden durch *Edward Snowden,* jedoch noch weitgehender, wie das Aufdecken von *Regin* zeigt.[1] Andererseits wird untersucht, wie sich das Strafrecht dazu verhält. Dabei wird folgender Struktur gefolgt: Nach einigen einleitenden Worten zum rechtstatsächlichen Hintergrund der Massenüberwachung werden die verfassungsrechtlichen Vorgaben zum Fernmeldegeheimnis dargestellt. Daran schließt sich der Hauptteil mit den strafrechtlichen Implikationen an, die von der Vorgehensweise von Hackern (mit einem Szenario zu *Treasuremap*) über das Eindringen in informationstechnische Systeme (mit einem Szenario zu *Regin*) bis zur strategischen Telekommunikationsüberwachung des Bundesnachrichtendienstes (BND) mit einem Szenario zu *Eikonal* (vgl. zu diesem Szenario Cornelius 2015a: 693ff.) untersucht werden. Ein abschließendes Fazit rundet den Bei-

1 Eine begriffliche Unterscheidung zwischen Nachrichtendiensten und Geheimdiensten soll hier nicht erfolgen, zumal sie bezüglich der inländischen Geheimdienste keine Stütze in der deutschen Rechtsordnung findet (ebenso Lampe 2015: 363).

trag ab. Dabei sei betont, dass die strafrechtsdogmatische Analyse anhand der hier vorgestellten Szenarien erfolgt, da wegen der ungesicherten Faktenlage endgültige Aussagen über die Strafbarkeit einer erfolgten Massenüberwachung nicht möglich sind. Allerdings ist es auf diese Weise möglich, jene Grenzen aufzuzeigen, bei deren Überschreiten eine Strafbarkeit von Mitarbeitern der Nachrichtendienste gegeben ist.

2 Fakten zur Massenüberwachung

Die Enthüllungen von *Edward Snowden* im Juni 2013 haben zu einer „Globalen Überwachungs- und Spionageaffäre“ geführt. *Snowden* hatte von 2009 bis 2013 auf Top-Secret-Dokumente der NSA zugegriffen, er kopierte etwa 1,7 Mio. Dateien und begann diese an ausgewählte Presseorgane zu versenden. Dadurch wurde ein weltweites Netz von Spionagesystemen durch die NSA, das GCHQ und engste Partner (Nachrichtendienste Neuseelands, Kanadas und Australiens – die *Five Eyes*) aufgedeckt (Zeit Online 2015). Nach Aussage *Snowdens* handele es sich um die „größte verdachtsunabhängige Überwachung in der Geschichte der Menschheit“, die einen schwerwiegenden Verstoß gegen Menschenrechte und Verfassungen darstelle. Die betroffenen Geheimdienste wehren sich mit dem Argument, dass die Aktivitäten zum „Kampf gegen den internationalen Terror“ notwendig seien. Als Rechtsgrundlagen für die Massenüberwachung waren im Gefolge des Anschlags auf das World-Trade-Center am 11. September 2001 in den USA der Patriot Act und in Großbritannien der Regulation of Investigatory Powers Act geschaffen worden.

2.1 Echelon

Allerdings ist die Tatsache einer umfassenden Überwachung von Telekommunikation nicht neu. So wurde bereits im Jahr 2001 durch das *Europäische Parlament* ein Bericht zur Existenz eines globalen Abhörsystems erstellt (vgl. Schmid 2001). Darin wurde festgestellt, dass „es auf der Grundlage der durch den Nichtständigen Ausschuss eingeholten Informationen keinen Zweifel mehr daran gibt, dass ein globales Abhörsystem existiert, das unter Beteiligung der Vereinigten Staaten, des Vereinigten Königreichs, Kanadas, Australiens und Neuseelands im Rahmen des UKUSA-Abkommens betrieben wird“ (vgl. ebd.: 18).[2] Außerdem wird angenommen, dass „das System, oder Teile davon, zumindest für einige Zeit, den Decknamen ‚ECHELON‘ trugen“ (vgl. ebd.: 14). Zum Zweck des Echelon-Systems wird darüber hinaus festgehalten, dass „nunmehr kein Zweifel mehr daran bestehen kann, dass das System nicht zum Abhören militärischer, sondern zumindest privater und wirtschaftlicher Kommunikation dient“, wobei es insbesondere auf dem „globalen Abhören von Satellitenkommunikation aufbaut“ (ebd.). In Gebieten mit „hoher Kommunikationsdichte“ werde die Kommunikation allerdings

2 Als UKUSA-Abkommen wird ein 1948 unterzeichnetes Abkommen zwischen Großbritannien (United Kingdom, UK), den Vereinigten Staaten (USA) sowie Australien, Kanada und Neuseeland bezeichnet (hierzu ausführlich Schmid 2001: 63 ff.).

nur zu einem kleinen Teil mittels Satelliten vermittelt und so könne „der überwiegende Teil der Kommunikation nicht durch Bodenstationen […], sondern nur durch Anzapfen von Kabeln und Abfangen von Funk“ geschehen, was jedoch wiederum nur in eng gesteckten Grenzen möglich sei (ebd.: 14, 33–34.). Zusammen mit dem erheblichen Personalaufwand, der für eine Auswertung der Daten erforderlich sei, kommt der Echelon-Abschlussbericht daher zum Ergebnis, dass die UKUSA-Staaten letztlich nur auf einen geringen Teil der kabel- und funkgebundenen Kommunikation Zugriff haben und darüber hinaus eine gründliche Auswertung aller gewonnenen Daten nicht machbar erscheine (ebd.: 14). Dieser Bericht lässt damit bereits Strukturen der globalen Überwachungs- und Spionageaffäre erkennen, und es wird deutlich, dass weniger das Sammeln der Daten als eine entsprechende Auswertung derselben das Problem war. Konsequenzen wurden aus diesem Bericht nicht gezogen. Vielmehr fiel er den Zeitläuften nach den Terroranschlägen auf das World-Trade-Center am 11. September 2001 in New York zum Opfer, die im Rahmen der Terrorabwehr zu einer erheblichen Ausweitung nachrichtendienstlicher Befugnisse führten (siehe auch den Beitrag von Beckedahl in diesem Band).

2.2 PRISM, X-Keyscore und Tempora

Für die umfassende Überwachung der elektronischen Kommunikation stehen solche Programme wie PRISM, Boundless Informant, Xkeyscore, Tempora Mail Isolation Control and Tracking, FAIRVIEW, Genie, Bullrun und CO-TRAVELER Analytics. Das wohl bekannteste Programm PRISM soll einen direkten Zugang zu zentralen Servern von Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL, Apple und anderen führenden US-Internetfirmen gewähren (vgl. Computerwoche 2013a). Dennoch wird dieses Phänomen nachfolgend nicht weiter verfolgt werden. Denn nach dem in § 3 StGB niedergelegten Territorialitätsprinzip gilt das deutsche Strafrecht für alle Taten, die im Inland begangen werden. Den Tatort bestimmt das Ubiquitätsprinzip des § 9 Abs. 1 StGB. Danach begründen sowohl der Handlungs- als auch der Erfolgsort eine Strafbarkeit (Cornelius 2013a: Rn. 56; Ambos 2011: § 9 Rn. 1). Bei PRISM ist jedoch nicht bekannt, dass die entsprechenden Überwachungshandlungen in Deutschland vorgenommen wurden oder der Erfolg eines Datenzugriffs in Deutschland eingetreten ist. Da außerdem – das wird hier einmal unterstellt – keine Strafbarkeit nach US-Recht vorliegt, ist die Anwendbarkeit deutschen Strafrechts auch nicht gem. § 7 StGB möglich. Denn die Voraussetzung hierfür ist, dass die Tat am Tatort mit Strafe bedroht ist (ebd.). Eine Anwendbarkeit deutschen Strafrechts kommt damit nur nach § 5 Nr. 4 StGB für Straftaten des Landesverrats und der Gefährdung der äußeren Sicherheit (§§ 94 bis 100a StGB) und nach § 5 Nr. 7 StGB bei der Verletzung von Betriebs- oder Geschäftsgeheimnissen in Betracht. Da insoweit eine umfassende strafrechtliche Betrachtung wegen der stark eingeschränkten Anwendbarkeit deutschen Strafrechts nicht möglich ist, soll PRISM hier nicht weiter verfolgt werden. Denn dieser Beitrag beschäf-

tigt sich explizit mit der *Massenüberwachung*. Damit geht es nicht um solche speziellen Szenarien, bei denen die Ausspähung von Staatsgeheimnissen oder von Wirtschaftsgeheimnissen verwirklicht wird, sondern um die Ausspähung der Allgemeinheit.

Bei *X-Keyscore* scheint diese auf den ersten Blick stärker betroffen. Dieses Tool dient der Auswertung der Datenmenge, die im Kommunikationsverkehr (Telefon und Internet) abgeschöpft wird. Mittels *X-Keyscore* können die großen Datenmengen gefiltert und in Echtzeit analysiert werden (Computerwoche 2013b). Es wurde auch an das *Bundesamt für Verfassungsschutz* weitergegeben, damit dieses die NSA unterstützen konnte (vgl. Spiegel Online 2014d). Damit kommt in Betracht, dass ein Tatort für potentiell strafbare Handlungen in Deutschland liegen kann. Dennoch soll auch dies hier nicht weiter verfolgt werden, da die eigentliche Erhebung der Daten durch die Massenüberwachung einer Auswertung durch *X-Keyscore* vorgelagert ist.

Ferner soll Berichten zufolge das Spähprogramm *Tempora* den Zugang zu bis dato 200 Glasfaserkabeln ermöglichen, die von Großbritannien aus ins Meer führen. Hierbei kann eine Komplettdatenspeicherung von Kommunikationsinhalten (aus dem weltweiten Telefon- und Internet-Verkehr) von bis zu drei Tagen und eine Speicherung von Metadaten von bis zu 30 Tagen vorgenommen werden (vgl. Spiegel Online 2013). Da das Anzapfen in internationalen Gewässern erfolgt und damit der Tatort nicht in Deutschland liegt, gelten die bereits bei *PRISM* dargestellten Einschränkungen zur Anwendbarkeit deutschen Strafrechts, so dass auch *TEMPORA* nicht weiter verfolgt werden soll.

2.3 Treasuremap, Regin und Eikonal

In einer internen Präsentation der NSA zu *Treasuremap* wird der Einsatzbereich dieser Datenbank wie folgt beschrieben: „Kartografiert das gesamte Internet, jedes Gerät, überall, jederzeit“ (vgl. Spiegel Online 2014c). Diese Karte soll von den groben bis hin zu den feinsten Strukturen des Netzes möglichst alles abbilden. Sie enthält Informationen darüber, wie Netzwerke aufgebaut sind, wo ihre Engpässe und Schwachstellen liegen und wie man Daten unauffällig von A nach B bringt. Das betrifft nicht nur Netzverbindungsstellen, sondern auch Router und Informationen über einzelne Endgeräte, verschlüsselte private Netzwerke (VPN-Netze) und WLAN-Netzwerke (vgl. The New York Times 2013). Eine wichtige Datenquelle ist dabei die Ablaufverfolgung für das Versenden von Datenpaketen über das Internet (sogenannte Traceroutes). Dies bedeutet, dass wie bei einem „roten Faden“ der Weg abgebildet wird, den die Datenpakete von Rechner eins zu Rechner zwei inklusive aller Zwischenschritte, also der dabei durchquerten Netzwerk-Knotenpunkte, nehmen (vgl. Spiegel Online 2014c). Wegen dieser kartografischen Darstellung wird *Treasuremap* auch als das „Google Earth für das Internet“ bezeichnet (vgl. Süddeutsche Zeitung 2014c). Dabei scheint Deutschland eine besondere Rolle zu spielen: Nach einem Dokument aus dem Fundus von *Edward Snowden* besteht die Möglichkeit, dass sich die NSA Zugriff auch auf Netzwerke der

Deutschen Telekom und des Kölner Providers *Netcologne* verschafft hat. Beide Anbieter sind auf einer Karte wie *Treasuremap*, die Verknüpfungen zwischen den Netzwerken einzelner Provider darstellt, mit einem roten Punkt markiert. Einem weiteren Dokument zufolge soll dieser rote Punkt bedeuten, dass es in diesem Netzwerk einen „Sigint collection point" gibt (vgl. Spiegel Online 2014c). Dieser lässt sich mit einem Spionagewerkzeug wie dem eingangs beschriebenen *Regin* nutzen, um in die Systeme einzudringen und Informationen zu sammeln. Ob dies stimmt, kann derzeit nicht verifiziert werden. Nachträgliche Untersuchungen der *Deutschen Telekom* und von *NetCologne* konnten dies nicht bestätigen (vgl. Süddeutsche Zeitung 2014c). Allerdings war genügend Zeit für die NSA, etwaige Spuren zu verwischen. Da die Datenströme nicht in den Grenzen des Nationalstaates kanalisierbar sind (bzw. dies zumindest nicht erfolgt ist), kann das Abgreifen der notwendigen Daten vielleicht auch außerhalb Deutschlands erfolgt sein, so dass sich jedoch wieder die Frage nach der Anwendbarkeit des deutschen Strafrechts stellen würde.

Anders sieht es bei dem in Köln ansässigen Unternehmen *Stellar* aus. In einem GCHQ-Dokument zu *Treasuremap* fand sich eine Tabelle, die zeigte, welche Stellar–Kunden über welchen Satellitentransponder kommunizierten; nach dem Bekanntwerden der Malware *Regin* ist vorstellbar, dass diese Daten über einen Zugriff auf das Firmennetzwerk erlangt wurden. Bei *Stellar* handelt es sich um ein Teleportunternehmen, das entlegene Orte, wie Ölplattformen, via Satellit mit Internet versorgt. Da für die Kommunikation über Satellitentransponder keine Glasfaserleitungen genutzt werden, ist es vorstellbar, dass entsprechende Angriffe bei *Stellar* selbst, also auf deutschem Boden, ausgeführt worden sind, so dass die Anwendbarkeit deutschen Strafrechts kein Problem darstellt. Die Staatsanwaltschaft Köln hat folgerichtig auch ein Ermittlungsverfahren gegen Unbekannt wegen des Verdachts auf das Ausspähen von Daten (§ 202a StGB) eingeleitet (vgl. Spiegel Online 2014b).

Für die deutschen Behörden selbst ist jedoch die „Operation Eikonal" von höchster Brisanz. Bei dieser arbeiteten die NSA und der BND jahrelang zur Überwachung von Telekommunikationsdaten zusammen (Süddeutsche Zeitung 2014a). Zwischen 2004 und 2008 zapfte der BND einen der wichtigsten Kommunikationsknotenpunkte der Welt, DE–CIX, in Frankfurt an und gab die so gewonnenen Rohdaten an die NSA weiter. Zwar sollte die Telekommunikation deutscher Personen vorher herausgefiltert werden, jedoch funktionierte der vom *BND* eingesetzte Filter DAFIS nur unzulänglich: So konnten 2003 nur 95 % der übermittelten Daten von deutschen Rohdaten bereinigt werden (Süddeutsche Zeitung 2014b). Dabei bemerkte der *BND* im Rahmen der Operation, dass durch die NSA auch nach Daten von Firmen wie der EADS (jetzt *Airbus Group*), *Eurocopter* (jetzt *Airbus Helicopters*) sowie von französischen Behörden gesucht wurde (Süddeutsche Zeitung 2014a).

Für die Betrachtung der strafrechtlichen Implikationen der Massenüberwachung bieten sich Szenarien in Anlehnung an *Treasuremap* (als „Karte des Internets") (vgl. Spiegel Online 2014c), *Regin* als Spionagetool zum Eindringen in Systeme und insbe-

sondere *Eikonal* (Süddeutsche Zeitung 2014a) als Beispiel für die Durchführung der strategischen Telekommunikationsüberwachung an. Anhand von *Treasuremap* und *Regin* lässt sich das Vorgehen bei einem „Einbruch“ in ein informationstechnisches System darstellen und *Eikonal* ist ein Paradebeispiel für die Massenüberwachung. Der direkte Bezug zu Deutschland ist auch gegeben, so dass die Anwendbarkeit deutschen Strafrechts uneingeschränkt möglich ist. Es gibt also mehr als nur vage Anhaltspunkte, dass wir es in der Praxis mit einer Massenüberwachung zu tun haben. Nachfolgend werden zunächst der verfassungsrechtliche Rechtsrahmen (Fernmeldegeheimnis sowie Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme) im Hinblick auf eine Massenüberwachung der Telekommunikation durch Geheimdienste dargestellt. Anschließend wird anhand von Szenarien zu Treasuremap, Regin und Eikonal eine strafrechtliche Bewertung vorgenommen.

3 Rechtsrahmen der Massenüberwachung

3.1 Fernmeldegeheimnis

Das Fernmeldegeheimnis ist unverletzlich. So sagt es unsere Verfassung (Art. 10 Abs. 1 GG). Einfachgesetzlich geregelt ist dann, was alles unter das Fernmeldegeheimnis fällt. Nach § 88 Abs. 1 TKG sind dies der Inhalt der Telekommunikation und ihre näheren Umstände. Das bezieht auch die Beteiligung an einem Telekommunikationsvorgang ein. Ein Eingriff in das Fernmeldegeheimnis liegt damit vor, wenn die öffentliche Gewalt vom Inhalt und den Umständen der geschützten Kommunikation Kenntnis nimmt (BVerfGE 67, 157 (172); 100, 313 (358); 125, 260 (309); 130, 151 (179); Gärditz et al. 2014: 217, damit sind auch die Verbindungsdaten umfasst; Cornelius, Kai 2013b: 167).

Warum gibt es überhaupt einen Schutz des Fernmeldegeheimnisses? Dies hat das *Bundesverfassungsgericht* treffend mit der Feststellung auf den Punkt gebracht, dass der Meinungs- und Informationsaustausch mittels Telekommunikationsanlagen nicht deswegen unterbleiben oder nach Form und Inhalt anders verlaufen soll, weil die Beteiligten damit rechnen müssen, dass staatliche Stellen sich in die Kommunikation einschalten und Kenntnisse über die Kommunikationsbeziehungen oder Kommunikationsinhalte gewinnen (BVerfG 30.4.2007: 2752). Dies erfordert die Möglichkeit eines „privaten, vor der Öffentlichkeit verborgenen Austausches von Informationen“, zumal wenn die Telekommunikationsverbindung „wegen der räumlichen Distanz zwischen den Beteiligten auf eine Übermittlung durch andere angewiesen ist und deshalb in besonderer Weise einen Zugriff Dritter – einschließlich staatlicher Stellen – ermöglicht“ (BVerfGE 115, 166 (182).

Da es beim Fernmeldegeheimnis damit um den Schutz und die näheren Umstände der Telekommunikation geht, ist jetzt noch die Frage zu beantworten, was darunter – bei normativer Betrachtung – zu verstehen ist. Nach § 3 Nr. 22 TKG ist Telekommunikation der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen. Diese sind wiederum technische Einrichtun-

gen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können (§ 3 Nr. 23 TKG). Dieses Herunterbrechen auf die technische Ebene bedeutet, dass jeder Dienst (jede Nachrichtenübermittlung), der diese technische Ebene (durch Kommunikationsanlagen) benutzt, davon erfasst und vom Fernmeldegeheimnis geschützt ist. Deshalb werden alle Formen der Nachrichtenübermittlung unter Überwindung des Raumes in nicht körperlicher Weise und mittels technischer Einrichtungen unter dem Begriff der Telekommunikation subsumiert (Schwabenbauer 2013: 57; Cornelius 2015a: 697). Das bezieht also nicht nur Telefon, Telefax und E-Mail ein, sondern auch SMS, MMS, Skype, WhatsApp, Internetkommunikation über Satellit etc. (Roggan 2012: § 1 Rn. 11; Cornelius 2015a: 697).

Dieses nach Abs. 1 des Art. 10 GG eigentlich unverletzliche Fernmeldegeheimnis kann nach dem Gesetzesvorbehalt des Art. 10 Abs. 2: 1 GG aufgrund eines „einfachen" Gesetzes eingeschränkt werden. Nun wurde bereits dargestellt, dass die Gewährleistung des Fernmeldegeheimnisses unverletzlich ist und dass dazu nicht nur der Inhalt der Kommunikation, sondern auch die Umstände des Zustandekommens (also die Metadaten) zählen. Allerdings ist nach Art. 10 Abs. 2: 2 GG ein heimlicher Eingriff nur für den Schutz der freiheitlich-demokratischen Grundordnung oder den Bestand bzw. die Sicherung des Bundes oder eines seiner Länder zulässig (Cornelius 2015a: 697). Genau um diese Gemengelage geht es bei der Frage der strafrechtlichen Bewertung der Massenüberwachung.

3.2 Vertraulichkeit und Integrität informationstechnischer Systeme

Neben dem Fernmeldegeheimnis ist das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) in seiner Ausprägung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07) berührt, wenn die Kommunikation durch den Zugriff auf ein Endgerät des Telekommunikationsteilnehmers überwacht wird und die Daten nicht nur auf der Übertragungsstrecke abgefangen werden (Cornelius 2015a: 697). Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen (BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07). Diese Vorgaben des *Bundesverfassungsgerichts* hat der Gesetzgeber bei den Regelungen des § 20k BKAG zu Online-Durchsuchungen[3] berücksichtigt. Diese sind danach bei Vorliegen einer *konkreten Gefahr* für die enumerativ aufgeführten Rechtsgüter Leib, Leben oder Freiheit einer Person oder Güter der Allgemeinheit, deren Bedro-

3 Unter einer Online-Durchsuchung wird der heimliche staatliche Zugriff auf Datenbestände des Zielrechners durch Einschleusen von Überwachungssoftware wie Trojanern oder Backdoor-Programmen verstanden (vgl. Beulke et al. 2007: 60, 64; Cornelius 2007: 798; Soiné 2012: 1585, 1586; Jahn et al. 2007: 58).

hung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt, zulässig. Eine konkrete Gefahr liegt nach der Rechtsprechung des *Bundesverfassungsgerichts* und des *Bundesverwaltungsgerichts* dann vor, wenn die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ein Schaden für ein betroffenes Rechtsgut eintreten wird (BVerwG 1970: 1892; BVerwG 1991). Diese Wahrscheinlichkeitsprognose muss auf Tatsachen basieren, die über vage Anhaltspunkte oder bloße Vermutungen ohne greifbaren, auf den Einzelfall bezogenen Anlass hinausgehen (BVerfGE 100, 313 (395); 120, 274 (328); Soiné 2012: 1586). Eine anlassunabhängige Massenüberwachung der Telekommunikation im Internet kann diesen hohen Vorgaben des *Bundesverfassungsgerichts* nicht genügen (Cornelius 2015a: 697).

Allerdings ist eine Besonderheit zu beachten: Wenn der Zugriff auf das Endgerät ausschließlich auf die Überwachung einer laufenden Telekommunikation beschränkt und dies durch entsprechende technische Vorkehrungen und rechtliche Vorgaben sichergestellt ist, dann muss die hoheitliche Maßnahme „nur" den Anforderungen des Fernmeldegeheimnisses (Art. 10 GG) genügen (BVerfGE 120, 274). Obwohl bei dieser Quellen-TKÜ[4] wegen der Infiltration des Endgerätes der Schutzbereich des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme eröffnet ist, sind solche Eingriffe damit nicht an den hohen Vorgaben des „IT-Grundrechts" zu messen (Buermeyer 2013: 473; Hoffmann-Riem 2008: 1021–1022.). Deshalb sollen die Vorgaben des „IT-Grundrechts" hier nicht weiter vertieft werden. Dafür spricht auch ein weiteres Argument: Wenn schon die Messlatte des Art. 10 GG mit seinen geringeren Vorgaben gerissen wird, dann gilt dies erst recht für die höheren Vorgaben des „IT-Grundrechts".[5]

4 Szenario zu Treasure Map

Da es in der Natur der Sache liegt, dass geheimdienstliche Tätigkeiten regelmäßig nicht bekannt sind, werden für die nachfolgende strafrechtliche Bewertung ausschließlich Szenarien als Modelle der Abfolge von möglichen Ereignissen zugrunde gelegt, ohne dass damit die Aussage verbunden ist, dass der Sachverhalt *tatsächlich* so gegeben ist. Das heißt, es wird nicht behauptet, dass die Sachlage so war, sondern nur, dass es sich *möglicherweise* so zugetragen haben könnte.

Das Szenario zu *Treasure Map* besteht darin, dass ein Projekt zu analysieren ist, das sich mit der Kartografierung des gesamten Internets beschäftigt. So können nachfol-

4 Als Quellen-TKÜ wird die behördliche Überwachung von verschlüsselter Telekommunikation „direkt an der Quelle" – also noch vor der Verschlüsselung – durch Infektion des verwendeten Endgerätes mit einem Trojaner bezeichnet (vgl. Buermeyer 2013: 470).

5 An dieser Stelle sei jedoch ausdrücklich klargestellt, dass damit nicht eine Stellungnahme des Autors verbunden ist, dass eine Quellen-TKÜ nach den Vorschriften für eine Telekommunikationsüberwachung zulässig ist. Hierfür ist es nämlich nach den skizzierten Anforderungen notwendig, dass ein entsprechendes Infiltrationstool auch technisch dahingehend „beschränkt" ist, dass nur die laufende Telekommunikation und nicht etwa auf dem Endgerät gespeicherte Inhalte ausgespäht werden (instruktiv hierzu Buermeyer: 2013: 470ff.).

gende Computerangriffe, Spionageaktionen aber auch die Verteidigung von Computernetzwerken besser geplant werden. Die zu beantwortende Frage lautet dahin, ob mit der Planung von Angriffen verbundene Handlungen strafbar sind, wenn auch Netzwerke in Deutschland von dieser Kartografierung betroffen sind. Da das strategisch verfolgte Ziel letztlich das unberechtigte Eindringen in Computer- oder Netzwerksysteme ist, bietet sich hierbei ein Vergleich mit der Vorgehensweise von Hackern an.

Denn unter „Hacken" wird das unberechtigte Eindringen in Computer- oder Netzwerksysteme verstanden. Die ursprünglichen Hacker haben ihre Fähigkeiten dazu genutzt, die Stärke und Integrität von Computersystemen zu testen und zu verbessern. Nach und nach hat es sich eingebürgert, den Begriff „Hacker" für Eindringlinge zu verwenden, die illegal auf Computer(systeme) zugreifen (Ernst 2003: 3233).

Der Hacker wird – ebenso wie dies regelmäßig ein Einbrecher macht, bevor er in ein Objekt eindringt – zunächst Erkundigungen über das anzugreifende System einziehen. Hierzu wird er die Netzwerkinfrastruktur durch Zusammenstellung leicht erhältlicher Informationen (wie die Namen von Personen/Rechnern/Domänen, IP-Adressen) auskundschaften, um eine Abbildung des zunächst vollkommen unbekannten Systems zu erhalten.

Diese Informationen kann er beispielsweise durch Whois-Abfragen, die Nutzung von Internet-Verzeichnissen (www.arin.net), die Untersuchung des HTML-Quelltextes von Webseiten einschließlich der entsprechenden Kommentare erhalten. Die Nutzung solcher öffentlich verfügbaren Informationen – auch wenn sie mit dem Ziel eines späteren rechtswidrigen Eindringens in ein fremdes System erfolgen – sind zunächst nur Vorbereitungshandlungen und nicht strafbar (zu den Quellen zur Informationssammlung: vgl. Hadagny 2011: 58ff.). Dies ist – um das Bild des Einbrechers aufzugreifen – mit einer Sondierung der Lage und der Umgebung eines Gebäudes vergleichbar, in welches später eingebrochen werden soll.

Kritischer wird es, wenn die Angriffsvorbereitungen in die nächste Phase treten und nicht nur öffentlich verfügbare Informationen abgefragt, sondern Reaktionen von aktiven Systemen provoziert werden. So werden beim *Network Mapping* ganze Adressbereiche angepingt, um festzustellen, welche Systeme erreichbar sind. Wenn ein System aktiv ist, gibt es auf die Ping-Anfrage ein Echo, so dass die sendende Person die Adresse erkennen kann. Die Namensauflösung selbst kann Hinweise auf die Einsatzbereiche geben. Auch dies ist zunächst nur eine straflose Vorbereitungshandlung und – um bei dem Bild mit dem Einbrecher zu bleiben – mit dem Ablesen der Namensschilder vergleichbar.

Sobald das Zielsystem identifiziert ist, geht es darum, die Schwachstellen dieses Systems zu erkennen, um einen Zugriff darauf zu erleichtern. Hierfür kann beispielsweise die Methode des *Port-Scannings*[6] oder des damit verwandten *OS Fingerprinting*[7]

6 Unter dem Port-Scanning wird der Identifizierungsprozess offener Ports auf einem oder mehreren Hosts verstanden (vgl. Singh et al. 2010: 222).

genutzt werden. Auch hierbei wird das System durch PING-Anfragen gescannt, um festzustellen, welche Ports[8] offen sind. Eine bestimmte Kombination von offenen Ports lässt darauf schließen, welche Applikationen beziehungsweise auch welches Betriebssystem laufen. Sobald dies bekannt ist, ist es in einem zweiten Schritt möglich, eine Schwachstellenanalyse durchzuführen[9] und die beste Form des Eindringens zu finden (Rinker 2002: 663). Diese Vorgehensweise ist noch nicht mit einem Eindringen in das System verbunden, so dass es an dem Tatbestandsmerkmal des Überwindens einer Zugangssicherung fehlt, um zu einer Strafbarkeit wegen des Ausspähens von Daten (§ 202a StGB) gelangen zu können.[10] Vielmehr handelt es sich um das Erlangen von Informationen an der Außengrenze eines Systems, die noch nicht geschützt sind (Heghmanns 2012: Teil 6.1 Rn. 32). Bei einem Einbrecher wäre dies vergleichbar mit dem Schauen durch ein Schlüsselloch oder dem Rütteln an der Haustür oder dem Kellerfenster, um zu überprüfen, ob diese offen sind (Rinker 2002: 665). Zwar soll es nach – umstrittener (ablehnend: Hillenkamp 2007: § 22 Rn. 28, 99, 103) – Rechtsprechung bereits für eine Versuchsstrafbarkeit ausreichen, wenn der Täter die Tauglichkeit einer Sache für einen im *unmittelbaren* zeitlichen Anschluss beabsichtigten strafbaren Angriff untersucht (BGHSt 22, 80). Allerdings kann dies hier dahinstehen, da nach dem Szenario zu *Treaseuremap* nur eine Karte für *spätere* Angriffe angefertigt werden soll. Selbst nach dieser extensiven Rechtsprechung wäre diese Handlung noch eine straflose Vorbereitungshandlung, auch wenn sie mit dem Ziel durchgeführt wird, genaue Angriffsvorbereitungen zu ermöglichen. Dies ist hier nicht weiter zu vertiefen, da für das Ausspähen von Daten schon keine Versuchsstrafbarkeit angeordnet ist.

5 Szenario zu Regin

Anders verhält es sich, wenn es tatsächlich zu einem Eindringen *in* ein Computersystem kommt – also zu einem Hackerangriff. Für die strafrechtliche Betrachtung wird wieder wegen der fehlenden Verifizierungsmöglichkeiten bezüglich des tatsächlichen Geschehens von einem Szenario ausgegangen: Die Kunden eines Teleportanbieter nutzen das Internet über Satellit. Die Server der Firma stehen in Köln und sind durch eine

7 Von *OS-Fingerprinting* ist die Rede, wenn man ein Zielsystem anhand seiner spezifischen Eigenschaften auf Protokollebene identifizieren möchte. Anhand von kleinen Abweichungen gegenüber den Standards und weiteren einzigartigen Merkmalen, kann unter Umständen ein exakter „Fingerabdruck“ des Betriebssystems und evtl. dessen Version angelegt werden (vgl. Dirscherl 2010).

8 Ein Port ist ein virtueller Briefkasten zur Kommunikation eines Programms bzw. einer bestimmten Programmfunktion.

9 Beispielsweise kann nach – selbst dem Hersteller noch unbekannten – Schwachstellen gesucht werden. Für solche Zero-Day-Exploits existiert ein regelrechter Markt und es wird auch den Geheimdiensten immer wieder vorgeworfen, sich solche Schwachstellen nutzbar zu machen (vgl. Grüter 2013: 181 im Hinblick auf *Stuxnet*; Johnigk et al. 2014: 105 zur Entwicklung von Zero-Day-Exploits im Projekt *Quantum Insert* der NSA).

10 Zutreffend: Bär kommt zu einer Strafbarkeit nach § 202a StGB, sieht aber das Portscanning als Unterfall des Hackings, ohne sich damit auseinanderzusetzen, dass durch die Abfrage der Ports noch nicht in das System eingedrungen wird (vgl. Bär 2014: 14. Kap., Rn. 80; Marberth-Kubicki 2008: 17).

unternehmenseigene Firewall und Passwortabfragen gesichert. Ein ausländischer Geheimdienst verschafft sich Zugang zu dem System und erlangt die vollständigen Verbindungsdaten, die zeigen, welcher Kunde über welchen Satellitentransponder kommuniziert hat.[11] Die Firma stellt Strafantrag.

5.1 Materiell-strafrechtliche Betrachtung

Die Server des Teleportanbieters stehen in Deutschland, so dass die Anwendbarkeit deutschen Strafrechts bei diesem Szenario kein Problem darstellt. Obwohl der Schutz des Fernmeldegeheimnisses die Verbindungsdaten umfasst, liegt keine nach § 206 StGB strafbare Verletzung des Post- und Fernmeldegeheimnisses vor, da den Mitarbeitern eines ausländischen Geheimdienstes regelmäßig die Täterqualität für dieses Sonderdelikt fehlt. Gleichfalls liegt kein Verstoß gegen das Abhörverbot nach §§ 148, 89 TKG vor, da nicht die Telekommunikation durch Überwachung des Satelliten ausgeforscht wird, sondern leitungsgebunden in die Server eingedrungen wird (zu den Voraussetzungen des Abhörverbotes: vgl. Cornelius 2015a: 695). Ebenso scheidet eine Verletzung der Vertraulichkeit des Wortes nach § 201 StGB aus, da nicht die Gespräche selbst mitgeschnitten werden, sondern nur die Verbindungsdaten erlangt werden (zu den Voraussetzungen des § 201 StGB: vgl. ebd.).

Allerdings kommt eine Datenausspähung nach § 202a StGB in Betracht. Diese Vorschrift schützt die formelle Verfügungsbefugnis des Berechtigten, über die Zugänglichkeit der Daten zu bestimmen, also sein individuelles Geheimhaltungsinteresse (ebd.). Die Zuordnung von Daten an einen Berechtigten erfolgt dabei grundsätzlich danach, wer die Speicherung oder Übermittlung der Daten initiiert, also den Skripturakt vorgenommen hat (ebd.). Dagegen sind die Eigentumsverhältnisse oder der Personenbezug (hierfür ist § 43 BDSG einschlägig: Lenckner et al. 2014: § 202a Rn. 1.) unerheblich für die Bestimmung der Berechtigteneigenschaft. Bei der Zugrundelegung dieser Kriterien ist der Berechtigte im Sinne des § 202a StGB der Teleportanbieter, der die Daten auf seinem System speichert. Dieser kann darüber entscheiden, wer auf die Daten zugreifen darf. Das ist jedenfalls nicht der ausländische Geheimdienst, so dass die erlangten Verbindungsdaten nicht für ihn bestimmt sind (zu diesem Erfordernis: vgl. Kilian et al. 2013: Teil 10, Rn. 19).

Des Weiteren erfordert der Tatbestand der Datenausspähung, dass eine Zugangssicherung überwunden wird. Darunter ist jedes Hindernis zu verstehen, das den tatsächlichen Zugriff auf Daten nicht ganz unerheblich zu erschweren geeignet und dafür bestimmt ist (Cornelius 2015a: 695). Grundsätzlich ist davon auszugehen, dass eine Firma

11 Nach einem Dokument aus dem Fundus von *Edward Snowden* besteht die Möglichkeit, dass sich die NSA und GCHQ Zugriff auf Netzwerke der Deutschen Telekom und des Kölner Providers Netcologne verschafft haben (vgl. Spiegel Online 2014c). Die *Staatsanwaltschaft Köln* hat folgerichtig ein Ermittlungsverfahren gegen Unbekannt wegen des Verdachts des Ausspähens von Daten (§ 202a StGB) eingeleitet (vgl. Spiegel Online 2014b).

ihr Netzwerk gegen unberechtigte Zugriffe von außen sichert, wie es auch hier im Szenario vorgesehen ist. Damit ist auch dieses Tatbestandsmerkmal erfüllt.

Ferner muss sich der ausländische Geheimdienst den Zugang zu Daten verschafft haben, wobei ein erfolgreicher Systemeinbruch ausreichend ist. Das Verschaffen des Zugangs zu Daten ist in jedem Fall dann erfüllt, wenn der Täter die tatsächliche Herrschaftsmacht über die Daten erlangt (Kargl 2013: § 202a Rn. 12). Dies ist spätestens mit dem Abspeichern der Verbindungsdaten der Fall.

Das Verschaffen des Zugangs zu Daten ist dem tatsächlichen Verschaffen der Daten zeitlich vorgelagert. Deshalb ist es nach Überwindung der Zugangssicherung nicht mehr erforderlich, dass sich der Täter die Daten durch reproduzierbare Kenntnisnahme oder durch Erlangen der Herrschaftsmacht tatsächlich verschafft. Bereits die Möglichkeit hierzu ist ausreichend. Dann hat der Täter schon *Zugang* zu den Daten. Damit kommt es nicht mehr darauf an, dass die Strafverfolgungsbehörden dem Täter nachweisen müssen, dass er tatsächlich die Herrschaftsgewalt über Daten erlangt hat oder diese zumindest reproduzierbar zur Kenntnis genommen hat (Kilian et al. 2013: Teil 10, Rn. 31).

Das außerdem erforderliche Merkmal der Unbefugtheit ist gegeben, da weder ein Einverständnis des Berechtigten vorliegt noch ein Rechtfertigungsgrund greift. Strafprozessuale Ermächtigungsgrundlagen (wie §§ 94, 100a StPO) und Maßnahmen der präventiven Gefahrenabwehr scheiden für einen ausländischen Geheimdienst als Rechtfertigungsgrund bereits *per se* aus. Für eine Notwehr nach § 32 StGB ist ein „gegenwärtiger Angriff“ erforderlich. Dieser ist „als punktuelles Ereignis“ erst dann anzunehmen, wenn die Gefahr unmittelbar in eine Rechtsgutsverletzung umzuschlagen droht (Erb 2011: § 32 Rn. 105), wobei auch späte Vorbereitungsphasen einbezogen werden, wenn diese bereits den konkreten Lebensvorgang eingeleitet haben (ebd.: § 32 Rn. 108). Diese Gegenwärtigkeit liegt bei einer einzelfallunabhängigen[12] Überwachung der Allgemeinheit nicht vor, da dieses Konzept mit dem großflächigen Ansatz gerade keinen Überwachungsanlass benötigt (vgl. zu diesem Konzept: Bäcker 2014: 556; Cornelius 2015a: 696). Im Übrigen kann die Notwehr nur einen Eingriff in die Rechtsgüter des Angreifers rechtfertigen (vgl. Erb 2011: § 32 Rn. 122). Selbst für den Fall, dass der ausländische Nachrichtendienst Anhaltspunkt für einen unmittelbar bevorstehenden Angriff (beispielsweise einen terroristischen Anschlag) hat, könnte damit nur die gezielte Überwachung bestimmter Kommunikationsverbindungen, nicht aber die Erlangung sämtlicher Verbindungsdaten gerechtfertigt werden.

Die Voraussetzungen des § 34 StGB liegen gleichfalls nicht vor. Hierzu bedarf es einer gegenwärtigen, nicht anders abwendbaren Gefahr für ein Rechtsgut im Sinne des § 34 StGB. Selbst wenn die Gegenwärtigkeit der Gefahr teilweise schon dann bejaht

12 Wegen dieser Einzelfallunabhängigkeit scheitert selbst die Effizienzlösung, nach welcher eine Gegenwärtigkeit schon beim Verstreichenlassen der „letzten oder sichersten Abwehrchance“ vorliegen soll, ebenso ist die Möglichkeit einer Präventivnotwehr abzulehnen (vgl. Hillenkamp 1995: 152–153).

wird, wenn der Eintritt eines drohenden Schadens erst in der Zukunft zu erwarten ist, aber nur durch sofortiges Handeln abgewendet werden kann (Perron 2014: § 34 Rn. 17; Erb 2011: § 34 Rn. 85 lässt schon ein erhöhtes Fehlschlagsrisiko genügen), liegt dies bei der einzelfallunabhängigen umfassenden Telekommunikationsüberwachung gerade noch nicht vor. Denn die Überwachung der Telekommunikation erfolgt planmäßig und wird über einen längeren Zeitraum zur Informationsbeschaffung begangen, ohne dass ein Anlass dafür gegeben sein muss.[13]

5.2 Prozessuale Betrachtung

Die materielle Seite ist somit kein Problem – aber die Strafverfolgung. Ein Rechtshilfeersuchen wird keinen Erfolg haben, denn die Voraussetzung der gegenseitigen Strafbarkeit dürfte regelmäßig nicht gegeben sein. Der NSA-Mitarbeiter wird sich darauf berufen, dass seine Handlungen nach dem US-amerikanischen Recht zulässig sind (vgl. Wolf 2013: 1040ff.). Differenzierter gestaltet sich die Rechtslage mit Blick auf *Großbritannien*. Dieses ist ein Mitgliedsstaat der *Europäischen Union* und dort gibt es das besondere Instrument des Europäischen Haftbefehls. Grundsätzlich gilt auch für diesen das Prinzip der gegenseitigen Strafbarkeit, aber es gibt Ausnahmen, u.a. für Delikte der Cyberkriminalität – das ist die Datenausspähung – die im ausstellenden Staat im Höchstmaß mit einer Freiheitsstrafe von 3 Jahren bedroht ist. Auch diese Voraussetzung ist hier gegeben, da § 202a StGB einen Strafrahmen bis zu drei Jahren vorsieht. Damit käme also tatsächlich eine erfolgversprechende Strafverfolgung in Betracht, wenn entsprechend dem hier unterstellten Szenario ermittelt werden kann (vgl. Cornelius 2015a: 694). Das ist natürlich die schwierigste Aufgabe!

Außerdem gibt es ggf. noch eine andere Hürde. *Großbritannien* ist in einem Ablösungsprozess von der *Europäischen Union* begriffen (vgl. Brodowski 2013: 458). Dies führte u.a. dazu, dass das Vereinigte Königreich mit Schreiben vom 24. Juli 2013 zum 1. Dezember 2014 entsprechend einer im Rahmen der Verhandlungen zum Lissabon-Vertrag zugestandenen Ausstiegsklausel aus 133 Regelungen zur gemeinsamen europäischen Innen- und Justizpolitik ausstieg (Europäische Union 2012: Art. 10 Abs. 4: 322). 35 davon wollte die Regierung beibehalten und wieder einführen.[14] Darunter ist auch der Europäische Haftbefehl. Bei der Abstimmungsvorlage im Unterhaus waren aber nur 11 der 35 Regelungen (darunter auch nicht der Europäische Haftbefehl) enthalten, so dass sich die Frage stellt, ob dieser nun wiedereingeführt wurde oder nicht. Innenministerin *Theresa May* geht (zumindest noch) davon aus, dass die Abstimmung für alle 35 Regelungen und damit auch den Europäischen Haftbefehl gilt (vgl. Frankfurter Allgemeine Zeitung 2014).

13 Vgl. die Argumentation des OLG Düsseldorf 2013: 593 zur Einschleusung von Vertrauensleuten in kriminelle Organisationen, die im Hinblick auf die fehlende Gegenwärtigkeit einer Gefahr vergleichbar ist mit einer umfassenden anlasslosen Telekommunikationsüberwachung.

14 Diese Möglichkeit räumt Art. 10 Abs. 5: 1 ein (Europäische Union 2012: 322).

Dann stellt sich jedoch noch ein zusätzliches Problem: Grundsätzlich ist die Staatsanwaltschaft verpflichtet, bei Vorliegen eines Anfangsverdachts ein Ermittlungsverfahren einzuleiten und bei einem hinreichenden Tatverdacht Anklage zu erheben. Allerdings wird dieses Legalitätsprinzip eingeschränkt durch das Opportunitätsprinzip. So kann die Staatsanwaltschaft bei Taten, deren Erfolgsort zwar in Deutschland liegt, deren zum Erfolg führende (menschliche) Handlung aber außerhalb von Deutschland im Ausland vorgenommen wurde, auch das Verfahren einstellen (§ 153c III StPO) (Cornelius 2015a: 694). Voraussetzung hierfür ist, dass die Durchführung des Verfahrens die Gefahr eines schweren Nachteils[15] für die Bundesrepublik Deutschland herbeiführen würde oder wenn der Verfolgung sonstige überwiegende öffentliche Interessen[16] entgegenstehen.

6 Szenario zu Eikonal

In diesem Szenario wird davon ausgegangen, dass der *BND* zwischen 2004 und 2008 einen der wichtigsten Kommunikationsknotenpunkte der Welt, den DE–CIX, in Frankfurt anzapfte und die durch diese *strategische Telekommunikationsaufklärung* gewonnenen Daten an einen amerikanischen Geheimdienst weiterleitete. Zwar sollte die Telekommunikation deutscher Personen vorher herausgefiltert werden, jedoch funktionierte der vom *BND* eingesetzte Filter nur unzulänglich: Es konnten nur 95 % der übermittelten Daten von deutschen Rohdaten bereinigt werden.[17] Machen sich die Mitarbeiter des BND strafbar, wenn sie sich an einer solchen Aktion beteiligen? Die Antwort auf diese Frage ist: Ja![18]

6.1 Verwirklichte Straftatbestände

Zwar scheiden die Strafvorschriften des TKG (§§ 148 i.V.m. 89 TKG) nach diesem Szenario aus, da in den Schutzbereich dieser Vorschriften nur über Funk erfolgende Nachrichtenübermittlung fallen (Altenhain 2015: § 148 TKG Rn.; 6; Cornelius 2015a: 695). Ebenso wenig ist der Tatbestand des Ausspähens von Daten (§ 202a StGB) erfüllt. Freilich haben sich die Mitarbeiter des BND nach dem vorgestellten Szenario den Zugang zu Daten verschafft, die nicht für sie bestimmt waren. Es ist außerdem davon auszugehen, dass ein so bedeutender Internetknotenpunkt nicht ohne eine adäquate Zugangssicherung betrieben wird. Jedoch ist der Betreiber unter den Voraussetzungen des

15 Die Gefahr eines schweren Nachteils kann die äußere Sicherheit betreffen, aber auch das innere oder sonstige (z.B. das wirtschaftliche) Wohl, den inneren politischen Frieden etc.

16 Dies kann jedes sonstige öffentliche Interesse sein, so dass durchaus auch Erwägungen zur Verhinderung des Zusammenbruchs der Zusammenarbeit mit GCHQ oder NSA und den deutschen Geheimdiensten vorstellbar sind (vgl. zu diesen Erwägungen: Hettel et al. 2014: 349).

17 Zu den tatsächlichen Hintergründen für dieses Szenario vgl. Süddeutsche Zeitung 2014a, b.; Spiegel Online 2014a; Golem.de 2014.

18 Ausführlich wurde die Frage der Strafbarkeit bei der strategischen Telekommunikationsüberwachung untersucht (Cornelius 2015a: 693ff.), weshalb nachfolgend nur die wichtigsten Überlegungen widergegeben werden.

G10-Gesetzes verpflichtet, dem BND zur Durchführung der strategischen Telekommunikationsüberwachung den Zugriff zu gewähren, vgl. § 2 G 10 Gesetz und unterliegt diesbezüglich auch einem Mitteilungsverbot, § 17 G 10 Gesetz. Deshalb ist davon auszugehen, dass kein Überwinden einer entsprechenden Zugangssicherung vorliegt. Dies muss an dieser Stelle nicht weiter vertieft werden, denn selbst wenn keine Zugangssicherung überwunden wird und damit eine Strafbarkeit nach § 202a StGB ausscheiden würde, wären zumindest die Voraussetzungen des § 202b StGB (Abfangen von Daten) gegeben, da es sich bei privater Telekommunikation um eine nichtöffentliche Datenübermittlung handelt, die sich der BND unter Anwendung technischer Mittel verschafft. Das ist schon dann gegeben, wenn der Datenstrom in Gestalt einer Verdoppelung dem *BND* zugeleitet wird.[19] Je nach der Art der abgehörten Daten kommt daneben noch die Verletzung der Vertraulichkeit des Wortes (§ 201 StGB) in Betracht. Dies betrifft Sprachnachrichten (alle abgefangenen Telefonate), nicht dagegen Textnachrichten wie E-Mails. Da es sich bei den Mitarbeitern des BND regelmäßig um Amtsträger oder für den öffentlichen Dienst besonders verpflichtete Personen handeln wird, ist dann sogar die Qualifikation des § 201 Abs. 3 mit einem Strafrahmen von bis zu fünf Jahren Freiheitsstrafe gegeben (ausführlich: Cornelius 2015a: 695).

6.2 Keine strafrechtlichen Rechtfertigungsgründe

Die Verwirklichung eines Straftatbestandes ist jedoch nicht gleichzusetzen mit einer Strafbarkeit. Diese ist vielmehr dann ausgeschlossen, wenn sich der BND auf eine Berechtigung berufen kann, die Telekommunikation aufzeichnen und überwachen zu dürfen. Die allgemeinen Rechtfertigungsgründe kommen aus den bereits zur umfassenden Telekommunikationsüberwachung durch einen ausländischen Geheimdienst dargelegten Gründen auch für den BND nicht in Betracht. Bei der strategischen Telekommunikationsüberwachung wird es regelmäßig an der Gegenwärtigkeit eines Angriffs bzw. einer Gefahr fehlen (vgl. Erb 2011: § 32 Rn. 105, 108).

6.3 Keine Wahrnehmung amtlicher Befugnisse

Allerdings kann die rechtmäßige Wahrnehmung amtlicher Befugnisse die Verwirklichung von Straftatbeständen rechtfertigen. Dies wird im Grundsatz weder in der Rechtsprechung noch in der Lehre bestritten (Evers 1987: 155; Lampe 2015: 367–368; Rönnau 2007: Vor § 32 Rn. 21; Roxin 2006: § 14 Rn. 32; Lenckner et al. 2014: vor § 32 Rn. 4; Hoyer 2009: Vor §§ 32ff. Rn. 41), obgleich die Anforderungen im Einzelnen um-

19 Zu dieser Vorgehensweise im Rahmen der strategischen Telekommunikationsbeschränkung (vgl. BVerwG 2014: 1668, Rn. 24); bei diesem Vorgehen kommt es damit nicht mehr darauf an, welche Daten nach dem Einsatz von Suchworten für eine weitere Verarbeitung herausgefiltert werden (vgl. zur parallelen Erwägung für einen Eingriff in das Fernmeldegeheimnis: ebd.: 997., Rn.32; mit Anm. Gärditz 2014: 1000; der aber a.a.O. vor einer Individualisierung der im Rahmen der strategischen Überwachung gewonnenen Daten einen Grundrechtseingriff in Art. 10 Abs. 1 GG ablehnt (ebd.: 1002).

stritten sind (vgl. OLG Düsseldorf 2013: 591, wo das Gericht den Rechtfertigungsgrund der Wahrnehmung amtlicher Befugnisse prüft, § 3 BNDG i.V.m. § 8 Abs. 2 BVerfSchG letztlich aber nicht durchgreifen lässt; vgl. auch Frisch 2003: 200; Hofmann et al. 2014: 178–188). Nur wenn die in der öffentlich-rechtlichen Ermächtigungsnorm konkret genannten Eingriffsvoraussetzungen objektiv erfüllt sind, kommt eine Rechtfertigung in Betracht (Lenckner et al. 2014: Vor § 32 Rn. 84; Cornelius 2015a: 696).

6.3.1 Öffentlich-rechtliche Rechtswidrigkeit als notwendige Bedingung einer Strafrechtswidrigkeit

Dies soll jedoch nicht heißen, dass eine öffentlich-rechtliche Rechtswidrigkeit immer zu einer Strafrechtswidrigkeit eines Verhaltens führt. Im Gegenteil kann ein Verhalten in einer außerstrafrechtlichen Teilrechtsordnung rechtswidrig sein, ohne dass es auch strafrechtswidrig ist (Günther 1983: 73; Erb 2011: Vor §§ 32ff. Rn. 2–3; vgl. Lehleiter 1995: 97; vgl. auch Schenke et al. 2014: § 1 BNDG Rn. 12ff., § 3 BNDG Rn. 30 zum Grundsatz der differenzierten Rechtmäßigkeit bzw. Rechtswidrigkeit in unterschiedlichen Rechtsgebieten). Damit ist bei der strafrechtlichen Bewertung staatlicher Maßnahmen auf Grund öffentlich-rechtlicher Eingriffsbefugnisse gegenüber dem Bürger die öffentlich-rechtliche Rechtswidrigkeit eine notwendige, nicht aber hinreichende Bedingung für die Strafrechtswidrigkeit (Felix 1998: 306–307; Günther 1983: 101; Lehleiter 1995: 93).[20] Eine Verletzung von Straftatbeständen durch eine staatliche Maßnahme kann nur dann zulässig sein, wenn eine *hinreichend konkrete* Ermächtigungsgrundlage in Form einer Befugnisnorm einschlägig ist und die entsprechenden Anforderungen erfüllt sind (OLG Düsseldorf 2013: 591; Lampe 2015: 368, 371; vgl. Roxin 2006: § 14 Rn. 31–32, wonach eine öffentlich-rechtliche Erlaubnis die Strafrechtswidrigkeit eines Verhaltens ausschließt). Deshalb ist in einem ersten Prüfungsschritt zu untersuchen, ob die Telekommunikationsüberwachung nach dem *Eikonal*-Szenario durch öffentlich-rechtliche Erlaubnisvorschriften gedeckt ist oder nicht. Wenn dies gegeben ist, dann gilt die Rechtfertigung für die gesamte Rechtsordnung (Lampe 2015: 368). Nur wenn dies nicht der Fall ist, muss in einem zweiten Schritt untersucht werden, ob die öffentlich-rechtliche Rechtswidrigkeit auch zur strafrechtlichen Verantwortlichkeit des jeweils handelnden Beamten führt (vgl. zu dieser Vorgehensweise: Felix 1998: 307 unter Rückgriff auf BVerfGE 88, 203 (258)).

20 Lehleiter weist zu Recht darauf hin, dass dieser Rechtswidrigkeitsbegriff im Hinblick auf die Rechtsfolgen funktionsbestimmt rechtsdogmatisch zu verstehen ist. Da es im Rahmen dieses Beitrages um die strafrechtliche Rechtfertigung durch öffentlich-rechtliche Eingriffsbefugnisse geht, kommt es auf die Diskussion zur Verallgemeinerung des Stufenverhältnisses der Rechtswidrigkeitsbegriffe nicht an (vgl. beispielsweise zur Ungleichbehandlung des untauglichen Versuchs im Deliktsrecht und im Strafrecht: Hellmann 1986: 88).

6.3.2 Spezialgesetzliche Eingriffsbefugnisse

Der BND ist keine Ermittlungsbehörde, so dass er sich nicht auf die Ermächtigungsgrundlagen zur Strafverfolgung stützen kann (vgl. §§ 94, 100a StPO). Zwar soll er – wie die Polizei – auch zur Gefahrenabwehr tätig werden. Allerdings ist er nach dem verfassungsrechtlich nicht ausdrücklich normierten, aber vor den unterschiedlichen Aufgabenzuweisungen anerkannten Trennungsgebot eine selbständige nicht der Polizei zuordenbare Behörde (Schwabenbauer 2013: 17–18), was einfachgesetzlich in §§ 1 Abs. 2, 2 Abs. 3 BNDG zum Ausdruck kommt (Schenke et al. 2014: § 1 BNDG Rn. 12 ff., § 2 BNDG Rn. 33). Deshalb kann sich der *BND* auch nicht auf etwaige Ermächtigungen in den Polizeigesetzen (wie zum Beispiel die Generalklauseln) berufen (vgl. Pawlik 2010: 696; Zöller 2007: 767). Gleichfalls scheidet eine Berufung auf § 9 Abs. 1 i.V.m. § 8 Abs. 2 BVerfSchG für die geheime Erhebung von Telekommunikationsdaten aus. Denn für eine Ermächtigungsgrundlage in entsprechende Eingriffe des Art. 10 GG wäre es gemäß dem Zitiergebot des Art. 19 Abs. 2: 1 GG notwendig, dass die Möglichkeit von Einschränkungen des Fernmeldegeheimnisses explizit erwähnt wird, was wegen der abschließenden Regelung des G10-Gesetzes für die heimliche Post- und Telekommunikationsüberwachung nicht erfolgt ist (Schenke et al. 2014: § 8 BVerfSchG Rn. 39; Lampe 2015: 366).

Eine Rechtfertigung der Telekommunikationsüberwachung durch den BND käme damit nur nach den spezialgesetzlichen Vorschriften im Gesetz zur Beschränkung des Brief-, Post - und Fernmeldegeheimnisses (G10-Gesetz) bzw. dem BNDG in Betracht.

6.3.3 Überwachung inländischer Telekommunikation

Der BND ist ein Auslandsgeheimdienst. Konsequenterweise hat er keine Befugnis, die Telekommunikation zwischen zwei deutschen Teilnehmern im Rahmen der strategischen Telekommunikationsüberwachung zu überwachen (Bäcker 2014: 557; Cornelius 2015a: 698). Wenn – wie in diesem Szenario unterstellt – die Filter nicht ordnungsgemäß funktionieren und damit auch die Daten einer rein deutschen Kommunikation weitergegeben werden, ist keine Rechtfertigung – weder für die Erhebung noch für die Weitergabe – denkbar. Allerdings ist eine Strafbarkeit wegen fehlenden Vorsatzes solange ausgeschlossen, wie die Mitarbeiter des BND davon ausgingen, dass der Filter ordnungsgemäß funktioniert.

6.3.4 Überwachung internationaler Telekommunikation

Die Rechtslage gestaltet sich komplizierter bei Telekommunikationsbeziehungen zwischen einem Teilnehmer in Deutschland und einem zweiten Teilnehmer im Ausland. Die Überwachung solcher internationalen Telekommunikationsverbindungen soll unter bestimmten Voraussetzungen nach § 5 G 10 G zulässig sein (Huber 2013: 2573).[21] Da-

21 Mit Betonung auf der Beschränkung der Eingriffsermächtigung für Telekommunikationsverbindungen mit einem Bezugspunkt (Anfangs- oder Endpunkt) zu Deutschland.

bei geht es um die frühzeitige Erkennung von Gefahren für die Sicherheit der Bundesrepublik Deutschland, weshalb nicht die Identität der Kommunikationsteilnehmer, sondern die Inhalte der Telekommunikation im Vordergrund stehen (Schwabenbauer 2013: 62). Deshalb bedarf es für die strategische Telefonüberwachung keiner tatsächlichen Anhaltspunkte für eine konkrete Gefahr (BVerfGE 100, 313 (383)). Dennoch sind die verfassungsrechtlichen Vorgaben, welche das *Bundesverfassungsgericht* konkretisiert hat, streng. Danach ist eine Ermächtigung zur strategischen Überwachung internationaler Telekommunikation nur bei einschränkenden Vorgaben im Hinblick auf Gegenstand, Ausmaß und Modalitäten der Überwachung verfassungsgemäß (BVerfGE 100, 313 (376, 377, 384)). Es ist jedoch äußerst zweifelhaft, ob diese einschränkenden Vorgaben mit der weiten Formulierung des § 5 G 10 G erfüllt werden, weshalb tendenziell davon auszugehen ist, dass diese Vorschrift keine ausreichende Ermächtigungsgrundlage ist (ausführlich: Cornelius 2015a: 698–699). Da es in diesem Beitrag um die strafrechtlichen Verantwortlichkeiten geht, soll an dieser Stelle erst einmal die Feststellung ausreichen, dass die Rechtslage bezüglich der öffentlich-rechtlichen Bewertung höchst unklar ist.

6.3.5 Überwachung ausländischer Kommunikation

Der *Europäische Gerichtshof für Menschenrechte* hat sich mit der strategischen Überwachung ausländischer Kommunikation (d.h. beide Kommunikationsteilnehmer befinden sich im Ausland) befasst und hatte zu entscheiden, ob diese einen unerlaubten Eingriff in die Souveränität der ausländischen Staaten darstellt, in denen die überwachten Personen wohnen (EGMR 2007: 1433ff.). Dies hat er deshalb abgelehnt, da kein ausreichender Vortrag seitens der Beschwerdeführer erfolgte, dass ein Eingriff in die völkerrechtlich geschützte territoriale Souveränität ausländischer Staaten vorliege, zumal sich die Überwachungsanlagen auf deutschem Gebiet befanden und die Daten in Deutschland verwendet wurden (ebd.: 1435).

Bezüglich ausländischer Telekommunikationsüberwachung beruft sich der BND selbst auf die Aufgabenzuweisungsnorm des § 1 Abs. 2 BNDG (BT-Drs.17/9640: 6, 10; BT-Drs. 17/14739: 14; BVerfGE 100, 313 (337, 338); Huber 2001: 3298; Bäcker 2014: 560). Danach müsse die Datenerhebung lediglich dazu dienen, Erkenntnisse von außen- und sicherheitspolitischer Bedeutung zu beschaffen. Dieser Rechtsansicht hat die Bundesregierung in einer Stellungnahme vor dem *Bundesverfassungsgericht* dahingehend zugestimmt, dass diese Überwachung des „offenen Himmels“ nicht unter das G10-Gesetz falle (vgl. die Stellungnahme der Bundesregierung im Verfahren über das G10-Gesetz: BVerfGE 100, 313 (339)). Die Verletzung von Straftatbeständen durch diese Überwachungsmaßnahmen kann jedoch nicht auf eine allgemeine Aufgabenzuweisungsnorm ohne eine *hinreichend konkrete* Ermächtigung gestützt werden (vgl. OLG Düsseldorf 2013: 591; Lampe 2015: 368, 371), wenn die ausländische Kommunikation durch das Fernmeldegeheimnis des Art. 10 GG geschützt wird (Bäcker 2014: 560; Cor-

nelius 2015a: 699). Das *Bundesverfassungsgericht* hat in dem Verfahren zum G 10 bereits darauf hingewiesen, dass der Schutz des Fernmeldegeheimnisses jedenfalls bei einem territorialen Bezug zu Deutschland greift, der bereits dann besteht, wenn ausländische Telekommunikation mit Überwachungsanlagen aufgezeichnet wird, die sich auf deutschem Boden befinden (BVerfGE 100, 313 (363, 364). Dies ist bei unserem Beispiel zu Eikonal mit der Überwachung des DE-CIX gegeben. Der territoriale Bezug liegt vor, so dass der Schutzbereich des Fernmeldegeheimnisses eröffnet ist, also eine ausdrückliche Befugnisnorm als Ermächtigungsgrundlage erforderlich ist. Diese kann nicht in der allgemeinen Aufgabenzuweisungsnorm des § 1 Abs. 2: 1 BNDG gesehen werden (vgl. Huber 2013: 2575).[22]

6.3.6 Strafrechtswidrigkeit

Damit ist die notwendige Voraussetzung für eine Strafrechtswidrigkeit – nämlich eine mangelnde öffentlich-rechtliche Befugnisnorm – gegeben. Da weder die strafrechtlichen Rechtfertigungsgründe (§§ 32, 34 StGB) noch spezielle Eingriffsnormen greifen, ist nun in einem zweiten Schritt zu prüfen, ob diese öffentlich-rechtliche Rechtswidrigkeit auch zu einer Strafrechtswidrigkeit führt. Dies ist im Hinblick auf den einzelnen Mitarbeiter des BND dann ausgeschlossen, wenn er sich auf eine zwar rechtswidrige, aber verbindliche dienstliche Anordnung berufen kann.

Nach § 63 BBG ist eine Anordnung auch strafbaren Inhalts selbst dann verbindlich, wenn der konkrete Weisungsempfänger nicht erkannt hat und nach seinem Wissens- und Erfahrungshorizont auch nicht erkennen konnte, dass das, was von ihm verlangt wird, „strafbar“ ist (Lenckner 1993: 227). Bei dem hier zugrunde gelegten *Eikonal*-Szenario kann nicht davon ausgegangen werden, dass die Strafbarkeit so evident ist, dass der ausführende Beamte dies zumindest zweifelsfrei hätte erkennen können. Bei der Überwachung der internationalen Telekommunikation wurde herausgearbeitet, dass die Rechtslage unklar ist. Dies schließt die evidente Erkennbarkeit einer diesbezüglichen Strafbarkeit aus. Zwar stellt sich dies bei der strategischen Überwachung ausländischer Telekommunikation anders dar, da das Ergebnis einer fehlenden Ermächtigungsgrundlage eindeutig ist. Dennoch kann aus der Sicht eines BND-Mitarbeiters nicht von einem Evidenzfall ausgegangen werden, da sowohl die Rechtsabteilung des BND als auch die Bundesregierung der Auffassung sind bzw. waren, dass die strategische Überwachung ausländischer Telekommunikation allein aufgrund der Aufgabenzuweisungsnorm des § 1 Abs. 2 BNDG zulässig und damit eine entsprechende Strafbarkeit ausgeschlossen ist. Damit handelte es sich bei einer entsprechenden Weisung des jeweiligen Vorgesetzten an den ausführenden Mitarbeiter um eine verbindliche Anordnung, deren Durchführung dem jeweiligen Mitarbeiter nicht strafrechtlich zu

22 Huber weist darauf hin, dass die Aufzeichnung, Auswertung und die Entscheidung über die Weitergabe der Informationen auf deutschem Boden erfolgen.

einem Vorwurf gemacht werden kann (ausführlich zu diesen Erwägungen: Cornelius 2015a: 700–701).

Dies gilt jedoch nur für die Person des Ausführenden, nicht aber für das von dem Weisungsgeber zu verantwortende staatliche Handeln, welches im Außenrechtsverhältnis rechtswidrig bleibt (vgl. Lenckner 1993: 224–225; Erb 2011: § 34 Rn. 43; Paeffgen 2013: Vor §§ 32 Rn. 192). Das führt dazu, dass der Vorgesetzte, welcher sich nicht mehr auf eine verbindliche Weisung stützen kann, als mittelbarer Täter für die im Außenverhältnis begangene Tat haftet (Weißer et al. 2014: § 25 Rn. 34). Zumindest der Vorgesetzte, der den eigentlichen Einsatz von *Eikonal* angeordnet hat, kann sich nicht mehr auf die Verbindlichkeit einer rechtswidrigen Anweisung berufen.

6.3.7 Verbotsirrtum, § 17 StGB

Jedoch kommt in Betracht, dass eine strafrechtliche Verantwortlichkeit dieses Vorgesetzten wegen eines Verbotsirrtums nach § 17 StGB ausscheidet. Die herrschende Meinung geht davon aus, dass schon bei einem bedingten Unrechtsbewusstsein kein Verbotsirrtum vorliegt – also eine entsprechende Unrechtseinsicht vorhanden ist. Wenn es der Täter bei einer unklaren Rechtslage auch nur für möglich hält, dass sein Verhalten verboten sein könnte (vgl. BGH 1953: 431; OLG Karlsruhe 2000: 61) und er lediglich darauf hofft, dass sein Verhalten nicht gegen das Strafgesetz verstoße (Fischer et al. 2015: § 17, Rn. 9c), reicht dies also schon aus, um einen Unrechtsausschluss zu verneinen (Cornelius 2015a: 701; Cornelius 2015b: 106). Solche Zweifel müssten von den Juristen der Rechtsabteilung des BND bei einer sachgemäßen Prüfung der Rechtslage angesichts der G10-Entscheidung des *Bundesverfassungsgerichts* den verantwortlichen Mitarbeitern beim BND zur Kenntnis gebracht werden. Jedoch ist darauf hinzuweisen, dass die Rechtsprechung selbst – in Abkehr von den dogmatischen Grundsätzen zum Verbotsirrtum – eine Anwendung von § 17 StGB bei unbehebbaren Unrechtszweifeln zugesteht (ebd.; kritisch hierzu: Cornelius 2015b: 106 mit einem Lösungsvorschlag zur verfassungskonformen Auslegung). Ein solcher kommt in Anbetracht der unklaren Rechtslage zwar im Hinblick auf die Überwachung internationaler Telekommunikation in Betracht, ist aber angesichts der Rechtsprechung des Bundesverfassungsgerichts und auch der ganz herrschenden Meinung in der Literatur zur begrenzten Reichweite einer Aufgabenzuweisungsnorm bei der strategischen Überwachung ausländischer Telekommunikation ausgeschlossen.

7 Fazit

Die Herstellung einer Karte vom Internet wie *Treasuremap* ist selbst dann nicht strafbar, wenn das Angriffsvorbereitungen für ein späteres Eindringen in informationstechnische Systeme sind. Dagegen ist ein Vorgehen ausländischer Geheimdienste mit einem solchen Spionagetool wie *Regin* bereits von allgemeinen Vorschriften zur Computerkriminalität erfasst, ohne dass es – auf je nach Tatfrage ggf. auch mitverwirklichte –

Vorschriften zum Schutz von Staatsgeheimnissen oder von Betriebs- und Geschäftsgeheimnissen ankommt. Das eigentliche Problem besteht in der faktischen Unmöglichkeit der Strafverfolgung amerikanischer Geheimdienstbeamter. Bei den britischen ist dies wegen des fehlenden Erfordernisses der gegenseitigen Strafbarkeit im Bereich der Cyberkriminalität im Rahmen des Europäischen Haftbefehls leichter. Allerdings stellt sich dann die Frage, inwieweit tatsächlich ein Wille zur Strafverfolgung vorhanden ist, da nach dem Opportunitätsprinzip auch von einer Strafverfolgung abgesehen werden kann.

Im Hinblick auf die einzelfallunabhängige, anlasslose (strategische) Telekommunikationsüberwachung, die von den deutschen Geheimdiensten allein dem BND gestattet ist, ist die Überwachung inländischer und ausländischer Telekommunikation unzulässig. Nach dem Willen des Gesetzgebers soll dagegen die strategische Überwachung internationaler Telekommunikation zulässig sein. Diese normative Vorgabe aus § 5 G10-Gesetz ist technisch jedoch nicht umsetzbar. Allein deshalb ergibt sich schon dringend ein Neuordnungsbedarf im Bereich des Sicherheitsrechts.

Eine Rechtfertigung des staatlichen Handelns im Verhältnis zwischen betroffenem Telekommunikationsanbieter bzw. Bürger scheidet (im Außenrechtsverhältnis) aus. Jedoch kommt in Betracht, dass sich die ausführenden Beamten auf eine rechtswidrige verbindliche Anweisung eines Vorgesetzten berufen können mit der Folge, dass diese selbst kein strafrechtliches Unrecht verwirklicht haben. Der Vorgesetzte, der sich nicht mehr auf die Verbindlichkeit einer wenn auch rechtswidrigen Anweisung stützen kann, ist dagegen strafrechtlich verantwortlich. Eine dann zu erwägende Berufung auf einen Verbotsirrtum ist zwar Tatfrage, dürfte aber nur bei der Überwachung internationaler Telekommunikation in Betracht kommen. Aufgrund der Rechtsprechung des *Bundesverfassungsgerichts* und der damit übereinstimmenden weitaus herrschenden Meinung in der verfassungsrechtlichen Literatur, dass eine Überwachung auch ausländischer Telekommunikation von deutschem Boden ein Eingriff in das Fernmeldegeheimnis darstellt, dürfte er dagegen relativ geringe Chancen auf Erfolg im Hinblick auf die strategische Überwachung des „offenen Himmels“ haben. Denn daraus resultiert unmittelbar, dass konkrete Eingriffsbefugnisse für einen solchen Eingriff normiert sein müssen, die mit einer allgemeinen Aufgabenzuweisungsnorm wie § 1 Abs. 2:1 BNDG nicht vorliegen. Allerdings ist bei §§ 202a, b StGB zu beachten, dass diese relative Antragsdelikte sind. Dagegen ist die Qualifikation des § 201 Abs. 3 StGB im Hinblick auf das Abfangen von Sprachnachrichten ein Offizialdelikt, was ohne einen entsprechenden Antrag von der Staatsanwaltschaft zu verfolgen ist.

Unabhängig von der Strafverfolgung kommt der Feststellung einer nach deutschem Recht rechtswidrigen Erhebung für eine Verwendung der daraus gewonnenen Erkenntnisse in einem deutschen Strafverfahren Bedeutung zu (Gärditz 2014: 999; Gercke 2013: 754; Zöller 2007: 770–771). Das gilt sowohl für die Erkenntnisse ausländischer als auch inländischer Geheimdienste. Denn Strafverfolgungsbehörden können nur dann auf solche Erkenntnisse zurückgreifen, wenn die Daten durch eine vergleich-

bare Maßnahme in Übereinstimmung mit den strafprozessualen Vorschriften hätten erlangt werden können (vgl. BVerfGE 100, 313 (394); Schünemann 2008: 326; Zöller 2007: 771).

Der rechtstatsächliche Hintergrund der Massenüberwachung im Internet zeigt, dass es jetzt viel besser als früher möglich ist, jeden Einzelnen zu analysieren, zu vermessen und fast schon die Gedanken vorherzusagen. Damit scheint unsere Gesellschaft mittlerweile dem vom Jeremy Bentham entworfenen Panopticon – jener Vollzugsanstalt, deren ringförmige Bauweise die lückenlose Überwachung der Gefangenen ermöglicht – zu gleichen (vgl. zu diesem Gleichnis: Fischer-Lescano 2014: 965). Die Wirkung einer nicht sichtbaren Überwachung ist permanent, auch wenn ihre Durchführung nur sporadisch ist. Das Internet ist hervorragend geeignet, dieses Konzept einer durch die Architektur ermöglichten Überwachung zu verwirklichen (vgl. das Erfordernis von Technologien für den „hierarchischen Blick" bei: Foucault 1977: 221ff.). Die möglichen Auswirkungen hat das *Bundesverfassungsgericht* bereits im Volkszählungsurteil beschrieben: „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen" (BVerfGE 65, 1 (43)).

Was zur Verhinderung von Kriminalität vielleicht begrüßenswert erscheinen mag (vgl. Bayerisches Staatsministerium des Innern für Bau und Verkehr 2014),[23] ist mit Blick auf die Gedankenfreiheit des Einzelnen beängstigend. Hier ist eine Debatte notwendig! Abwehrmaßnahmen können nicht darin bestehen, die Zeit zurückzudrehen (vgl. Süddeutsche Zeitung 2014d).[24] Vielmehr sind die Rahmenbedingungen anzupassen. Dazu gehört einerseits die Neuausrichtung des Sicherheitsrechts. So ist die Unterscheidung zwischen Inlands- und Auslandsüberwachung nicht mehr zeitgemäß (Huber 2013: 2577; Schmahl 2014: 226). Andererseits ist die rechtspolitische Diskussion zu führen, wieweit eine Überwachung angemessen ist, um dadurch auch Terroranschläge zu verhindern.

Literatur

Altenhain, Karsten (2015): Telekommunikationsgesetz (TKG) Auszug: Normzweck, in: Heintschel-Heinegg, Bernd von (Hrsg.): Münchener Kommentar zum StGB. Nebenstrafrecht II, Bd. 7, C.H. Beck: München, 1377–1404.

Ambos, Kai (2011): § 9, in: Heintschel-Heinegg, Bernd von (Hrsg.): Münchener Kommentar zum Strafgesetzbuch: StGB, Bd 1: §§ 1-37 StGB, C.H. Beck: München, 261–277.

Bäcker, Matthias (2014): Strategische Telekommunikationsüberwachung auf dem Prüfstand, in: Kommunikation und Recht 33, 556–561.

23 Zum Einsatz der Prognosesoftware Precobs, um die Wahrscheinlichkeit der Begehung von Straftaten berechnen zu können.

24 Zu den Überlegungen im NSA-Untersuchungsausschuss, anstatt Computern mechanische Schreibmaschinen einzusetzen.

Bär, Wolfgang (2014): Computer- und Internetkriminalität, in: Wabnitz, Heinz-Bernd / Janovsky, Thomas (Hrsg.): Handbuch Wirtschafts- und Steuerstrafrecht, C.H. Beck: München, 813–908.

Bayerisches Staatsministerium des Innern für Bau und Verkehr 2014: Bayernweite Kontrollaktion gegen Diebes-banden, 26.11.2014, http://www.stmi.bayern.de/med/aktuell/archiv/2014/20141126sonderkontrollaktion/ (16.08.2015).

Beulke, Werner / Meininghaus, Florian (2007): Heimliche Online-Durchsuchung eines PC, in: Strafverteidiger 2, 60–65.

BGH (1953): Verbotsirrtum, in: Neue Juristische Wochenschrift 11, 431–433.

BGH (1968): Beginn der Gebrauchsentwendung durch Untersuchung des KfZ, in: BGHSt 22, 80–82.

Boehme-Neßler, Volker (2014): Das Recht auf Vergessenwerden – Ein neues Internet-Grundrecht im Europäischen Recht, in: Neue Zeitschrift für Verwaltungsrecht 13, 825–830.

Brodowski, Dominik (2013): Strafrechtsrelevante Entwicklungen in der Europäischen Union – ein Überblick, in: Zeitschrift für Internationale Strafrechtsdogmatik 8:11, 455–472.

Buermeyer, Ulf (2013): Zum Begriff der »laufenden Kommunikation« bei der Quellen-Telekommunikationsüberwachung (»Quellen-TKÜ«), in: Strafverteidiger 7, 470–476.

BVerfG (2007): Unzulässige Telefonüberwachung des Anwalts von El Masri, in: Neue Juristische Wochenschrift 38, 2752–2753.

BVerfGE 65, 1 (43); 67, 157 (172); 88, 203 (258); 100, 313 (337, 338, 339, 358, 363, 364, 376, 377, 383, 384; 394, 395); 115, 166 (182); 120, 274 (328); 125, 260 (309); 130, 151 (179).

BVerfG, Urteil vom 27.02.2008 – 1 BvR 370/07.

BVerwG (2014): Feststellungsklage gegen strategische Überwachung durch den BND, in: Neue Zeitschrift für Verwaltungsrecht 2014, 1666–1670.

BVerwG, Urteil vom 02.07.1991 – 1 C 21.89.

BVerwG (1970): Lagerung von Heizöl im engeren Schutzbereich eines Wasserschutzgebietes; nicht zu besorgende Verunreinigung des Grundwassers i.S. des § 34 Abs. 2 WHG, in: Neue Juristische Wochenschrift 42, 1890 – 1893.

Computerwoche (2013a): US-Regierung schnüffelt in Rechnern von Internet-Firmen, 07.06.2013, http://www.computerwoche.de/a/us-regierung-schnueffelt-in-rechnern-von-internet-firmen,2539842 (13.08.2015).

Computerwoche (2013b): Die Spionage-Werkzeuge der NSA, 01.08.2013, http://www.computerwoche.de/a/die-spionage-werkzeuge-der-nsa,2543728 (13.08.2015).

Cornelius, Kai (2015a): Strafrechtliche Verantwortlichkeiten bei der Strategischen Telekommunikationsüberwachung, in: Juristen Zeitung 70:14, 693–702.

Cornelius, Kai (2015b): Die Verbotsirrtumlösung zur Bewältigung unklarer Rechtslagen - ein dogmatischer Irrweg, in: Goltdammer's Archiv für Strafrecht 2, 101–124.

Cornelius, Kai (2013a): Besonderheiten des Strafrechts und Strafprozessrechts in der Informationstechnologie (Teil 10), in Leupold, Andreas / Glossner, Silke (Hrsg.): Münchener Anwaltshandbuch IT-Recht, C. H. Beck: München, 963–1080.

Cornelius, Kai (2013b): Zum strafrechtlichen Schutz des Fernmeldegeheimnisses und der Untreuerelevanz datenschutzrechtlicher Verstöße, in: Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht, 166–170.

Cornelius, Kai (2007): Verdeckte Online-Durchsuchung-Anmerkung zum Beschluss des BGH vom 31.1.2007 – StB 18/06, in: Juristen Zeitung, 62: 15–16, 796–800.

Deutscher Bundestag (2013): BT-Drs. 17/14739, http://dip21.bundestag.de/dip21/btd/17/147/1714739.pdf (16.08.2015).

Deutscher Bundestag (2012): BT-Drs.17/9640, http://dip21.bundestag.de/dip21/btd/17/096/1709640.pdf (16.08.2015).

Dirscherl, Hans-Christian (2010): Fingerprinting: Betriebssysteme identifizieren, 08.06.2010, http://www.pcwelt.de/ratgeber/Fingerprinting-Betriebssysteme-identifizieren-Netzwerk-Sicherheit-und-Nmap-171343.html (14.08.2015).

EGMR (2007): 29. 6. 2006 - 54934/00: Abhörmaßnahmen nach dem G 10-G, in: Neue Juristische Wochenschrift 20, 1433–1439.

Erb, Volker (2011): § 32 Notwehr, in: Heintschel-Heinegg, Bernd von (Hrsg.): Münchener Kommentar zum StGB. §§ 1 - 37 StGB, Bd. 1, C.H. Beck: München, 1435–1547.

Ernst, Stefan (2003): Hacker und Computerviren im Strafrecht, in: Neue Juristische Wochenschrift 45, 3233–3238.

Europäische Union (2012): Protokoll (Nr. 36) über die Übergangsbestimmung, in: Amtsblatt der Europäischen Union C 326, 55, 322–328, https://www.ecb.europa.eu/ecb/legal/pdf/c_32620121026de.pdf (15.08.2015).

Evers, Hans (1987): Sprengung an der Celler Gefängnismauer: Darf der Verfassungsschutz andere Behörden und die Öffentlichkeit täuschen?, in: Neue Juristische Wochenschrift 4, 153–159.

Felix, Dagmar (1998): Einheit der Rechtsordnung. Zur verfassungsrechtlichen Relevanz einer juristischen Argumentationsfigur, Mohr Siebeck: Tübingen.

Fischer, Thomas / Schwarz, Otto / Dreher, Eduard / Tröndle, Herbert (2015): Strafgesetzbuch: StGB mit Nebengesetzen, C.H. Beck: München.

Fischer-Lescano, Andreas (2014): Der Kampf um die Internetverfassung, in: Juristen Zeitung 69: 20, 965–974.

Foucault, Michel (1977): Überwachen und Strafen, Suhrkamp: Frankfurt am Main.

Frankfurter Allgemeine Zeitung (2014): Mit wehenden Frackschößen, 11.11.2014, http://www.faz.net/aktuell/politik/europaeische-union/london-heftige-debatte-im-unterhaus-13260875.html (15.08.2015).

Frisch, Peter (2003): V-Leute im Strafverfahren und im Verbotsverfahren, in: Deutsche Richterzeitung 81, 199–203.

Gärditz, Ferdinand (2014): Anmerkung, in: Juristen Zeitung 69: 20, 998–1002.

Gärditz, Ferdinand / Stuckenberg, Carl-Friedrich (2014): Vorratsdatenspeicherung à l'américaine – Zur Verfassungsmäßigkeit der Sammlung von Telefonverbindungsdaten durch die NSA, in: Juristen Zeitung 69:5, 209–219.

Gercke, Marco (2013): PRISM, TEMPORA und das deutsche Strafverfahren – Verwertbarkeit der Erkenntnisse ausländischer Nachrichtendienste, in: Computer und Recht 11, 749–754.

Golem.de (2014): Operation Eikonal: NSA wollte die DE-CIX-Daten des BND nicht mehr, 08.10.2014, http://www.golem.de/news/operation-eikonal-nsa-wollte-die-de-cix-daten-des-bnd-nicht-mehr-1410-109715.html (15.08.2015).

Grüter, Thomas (2013): Offline! Das unvermeidliche Ende des Internets und der Untergang der Informationsgesellschaft, Springer Spektrum: Berlin.

Günther, Hans-Ludwig (1983): Strafrechtswidrigkeit und Strafunrechtsausschluß. Studien zur Rechtswidrigkeit als Straftatmerkmal und zur Funktion der Rechtfertigungsgründe im Strafrecht, Carl Heymanns Verlag: Köln.

Hadagny, Christopher (2011): Kunst des Human Hacking: Social Engineering, mitp Verlags GmbH & Co. KG: Wachtendonk.

Heghmanns, Michael (2012): Straftaten gegen die betriebliche Datenverarbeitung, in: Achenbach, Hans / Ransiek, Andreas / Mosbacher, Andreas (Hrsg.): Handbuch Wirtschaftsstrafrecht, 741–816.

Hellmann, Uwe (1986): Die Anwendbarkeit zivilrechtlicher Rechtfertigungsgründe im Strafrecht, Carl Heymann: Köln.

Hettel, Alexander / Kirschhöfer, Max Phillip (2014): Aus aktuellem Anlass: Die Strafbarkeit geheimdienstlicher Spionage in der Bundesrepublik Deutschland, in: Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht 9, 341–349.

Hillenkamp, Thomas (2007): §§ 22 StGB, in: Laufhütte, Heinrich Wilhelm / Rissing-van Saan, Ruth / Tiedemann, Klaus (Hrsg.): Leipziger Kommentar zum StGB (LK-StGB), Bd. 1, de Gruyter: Berlin, Rn. 28, 99, 103.

Hillenkamp, Thomas (1995): In tyrannos - viktimodogmatische Bemerkungen zur Tötung des Familientyrannen, in: Kühne, Hans-Heiner (Hrsg.): Festschrift für Koichi Myazawa. Dem Wegbereiter des japanisch-deutschen Strafrechtsdiskurse, Nomos: Baden-Baden, 141–159.

Hofmann, Manfred / Ritzert, Silke (2014): Zur Strafbarkeit des Einsatzes nachrichtendienstlicher V-Personen in terroristischen Vereinigungen, extremistischen Organisationen und verbotenen Gruppierungen, in: Neue Zeitschrift für Strafrecht 4, 177–182.

Hoffmann-Riem, Wolfgang (2008): Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, in: Juristen Zeitung 63:21, 1009–1022.

Hoyer, Andreas (2009): Vorbemerkungen vor §§ 32ff. (Unrechtslehre), in: Wolter, Jürgen (Hrsg.): Systematischer Kommentar zum Strafgesetzbuch: SK-StGB, Carl Heymanns: Köln, Rn. 41.

Huber, Bertold (2013): Die strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefugnisse und Regelungsdefizite, in: Neue Juristische Wochenschrift 35, 2572–2576.

Huber, Bertold (2013): Das neue G 10-Gesetz, in: Neue Juristische Wochenschrift 45, 3296–3301.

Jahn, Matthias / Kudlich, Hans (2007): Die strafprozessuale Zulässigkeit der Online-Durchsuchung, in: Juristische Rundschau 2, 57–61.

Johnigk, Sylvia / Nothdurft, Kai (2014): Internet als Domäne von Militär und Geheimdiensten, in: Bittner, Peter / Hügel. Stefan / Kreowski, Hans-Jörg / Meyer-Ebrecht, Dietrich / Schinzel, Britta (Hrsg.): Gesellschaftliche Verantwortung in der digital vernetzten Welt, Lit Verlag: Berlin, 101–124.

Kargl, Walter (2013): § 202a Ausspähen von Daten, in: Kindhäuser, Urs / Neumann, Ulfrid / Paeffgen, Hans-Ullrich (Hrsg.): Nomos-Kommentar zum StGB (NK-StGB), Bd. 2, Nomos: Baden-Baden, 1402–1417.

Kilian, Wolfgang / Heussen, Benno / Cornelius, Kai (2013): Computerrechts-Handbuch, C.H. Beck: München.

Kloepfer, Michael (2002): Informationsrecht, C. H. Beck: München.

Lampe, Joachim (2015): Die Schwierigkeiten mit der Rechtfertigung nachrichtendienstlicher Tätigkeit, in: Neue Zeitschrift für Strafrecht 7, 361–372.

Lehleiter, Gunther (1995): Der rechtswidrige verbindliche Befehl. Strafrechtsdogmatische Untersuchung, demonstriert am Beispiel des militärischen Befehls, Peter Lang Verlag: Frankfurt am Main.

Lenckner, Theodor / Eisele, Jörg (2014): Verletzung des persönlichen Lebens- und Geheimbereichs (§§ 201–206), in: Schönke, Adolf / Schröder, Horst (Hrsg.): StGB. Kommentar, C.H. Beck: München, 1921–1996.

Lenckner, Theodor / Sternberg-Lieben, Detlev (2014): Vorbemerkungen vor § 32, in: Schönke, Adolf / Schröder, Horst (Hrsg.): StGB. Kommentar, C.H. Beck: München, RN 4.

Lenckner Theodor (1993): Der "rechtswidrige verbindliche Befehl" im Strafrecht - nur noch ein Relikt?, in: Küper, Wilfried (Hrsg.): Beiträge zur Rechtswissenschaft. Festschrift für Walter Stree und Johannes Wessels zum 70. Geburtstag, C.F. Müller: Heidelberg, 223–240.

Marberth-Kubicki, Annette (2008): Neuregelungen des Computerstrafrechts, in: IT-Rechtsberater, 17–19.

OLG Düsseldorf (2013): 6. 9. 2011 - 5 Sts 5/10: Vereinigungsmitglied als BND-Informant, in: Neue Zeitschrift für Strafrecht 10, 590–593.

OLG Karlsruhe (2000): 18. 10. 1999 - 2 Ws 51/99 : Gewerbliche Abgabe von Frischkäse in einer Gaststätte, in: Neue Zeitschrift für Strafrecht-RechtsprechungsReport 2, 60–62.

Paeffgen, Hans-Ullrich (2013): Notwehr und Notstand: Vorbemerkungen zu den §§ 32 ff, in: Kindhäuser, Urs / Neumann, Ulfrid / Paeffgen, Hans-Ullrich (Hrsg.): Nomos-Kommentar zum StGB (NK-StGB), Bd. 1, Nomos: Baden-Baden, 1247–1489.

Pawlik, Michael (2010): Zur strafprozessualen Verwertbarkeit rechtswidrig erlangter ausländischer Bankdaten, in Juristen Zeitung 65:14, 693–702.

Perron, Walter (2014): § 34 Rechtfertigender Notstand, in: Schönke, Adolf / Schröder, Horst (Hrsg.): StGB. Kommentar, C.H. Beck: München, 293–302.

Reinhard, Wolfgang (2007): Geheimnis und Fiktion als politische Realität, in: Reinhard, Wolfgang (Hrsg.): Krumme Touren – Anthropologie kommunikativer Umwege, Böhlau Verlag GmbH & Co. KG: Wien, 221–272.

Rinker, Mike (2002): Strafbarkeit und Strafverfolgung von „IP-Spoofing" und „Portscanning", in: MultiMedia und Recht 10, 663–665.

Rönnau, Thomas (2007): Vor § 32, in: Laufhütte, Heinrich Wilhelm / Rissing-van Saan, Ruth / Tiedemann, Klaus (Hrsg.): Leipziger Kommentar zum StGB (LK-StGB), Bd. 2, de Gruyter: Berlin, 1–352.

Roggan, Fredrik (2012): G-10-Gesetz, Nomos: Baden-Baden.

Roxin, Claus 2006: Strafrecht Allgemeiner Teil Band I: Grundlagen. Der Aufbau der Verbrechenslehre, C.H. Beck: München.

Schenke, Wolf-Rüdiger / Graulich, Kurt / Ruthig, Josef (2014) (Hrsg.): Sicherheitsrecht des Bundes. BPolG, BKAG, ATDG, BVerfSchG, BNDG, VereinsG, C.H. Beck: München 2014, § 1 BNDG Rn. 12 ff., § 3 BNDG Rn. 30.

Schmahl, Stefanie (2014): Effektiver Rechtsschutz gegen Überwachungsmaßnahmen ausländischer Geheimdienste?, in: Juristen Zeitung 69:5, 220–228.

Schmid, Gerhard (2001): Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem Echelon), EP, A5–0264/200,

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//DE (13.08.2015).

Schünemann, Bernd (2008): Prolegomena zu einer jeden künftigen Verteidigung, die in einem geheimdienstähnlichen Strafverfahren wird auftreten können, in: Goltdammer's Archiv für Strafrecht 155:5, 314–334.

Schwabenbauer, Thomas (2013): Heimliche Grundrechtseingriffe. Ein Beitrag zu den Möglichkeiten und Grenzen sicherheitsbehördlicher Ausforschung, Mohr Siebeck: Tübingen.

Singh, Himanshu / Chun, Robert (2010): Distributed Port Scan Detection, in: Stavroulakis, Peter / Stamp, Mark (Hrsg.): Handbook of Information and Communication Security, Springer: Heidelberg, 221–234.

Soiné, Michael (2012): Eingriffe in informationstechnische Systeme nach dem Polizeirecht des Bundes und der Länder, in: Neue Zeitschrift für Verwaltungsrecht 24, 1585–1589.

Stürmer, Michael (2006): Welt ohne Weltordnung, Murmann: Hamburg 2006.

Spiegel Online (2014a): Operation "Eikonal": Grüne und Linke verlangen Aufklärung über NSA-BND-Kooperation, 6.10.2014, http://www.spiegel.de/netzwelt/netzpolitik/eikonal-bnd-soll-daten-von-bundesbuergern-an-nsa-uebergeben-haben-a-995602.html (15.08.2015).

Spiegel Online (2014b): Britischer Geheimdienst GCHQ: Staatsanwaltschaft ermittelt nach mutmaßlichem Cyberangriff auf deutsche Firma, 21.09.2014, http://www.spiegel.de/netzwelt/netzpolitik/gchq-ermittlungen-nach-cyberangriff-auf-stellar-a-992903.html (13.08.2015).

Spiegel Online (2014c): NSA-System Treasuremap: "Jedes Gerät, überall, jederzeit", 17.09.2014, http://www.spiegel.de/netzwelt/netzpolitik/nsa-wie-der-geheimdienst-mit-dem-system-treasuremap-daten-sammelt-a-991496.html (13.08.2015).

Spiegel Online (2014d): Snowdens Deutschland-Akte: Die Dokumente im PDF-Format, 18.06.2014, http://www.spiegel.de/netzwelt/web/snowdens-deutschland-akte-alle-dokumente-als-pdf-a-975885.html (13.08.2015).

Spiegel Online (2013): Britische Internet-Überwachung: Freund liest mit, 22.06.2013, http://www.spiegel.de/netzwelt/netzpolitik/internetueberwachung-tempora-geheimdienst-zapft-glasfaserkabel-an-a-907283.html (13.08.2015).

Süddeutsche Zeitung (2014a): Codewort Eikonal - der Albtraum der Bundesregierung, 04.10.2014, http://www.sueddeutsche.de/politik/geheimdienste-codewort-eikonal-der-albtraum-der-bundesregierung-1.2157432 (13.08.2014).

Süddeutsche Zeitung (2014b): BND leitete Daten von Deutschen an NSA weiter, 03.10.2014, http://www.sueddeutsche.de/politik/spaeh-affaere-bnd-leitete-daten-vondeutschen-an-nsa-weiter-1.2157406 (13.08.2015).

Süddeutsche Zeitung (2014c): NSA kann offenbar direkt auf Telekom-Netz zugreifen, 13.09.2014, http://www.sueddeutsche.de/digital/neue-enthuellung-aus-snowden-dokumenten-nsa-kann-offenbar-direkt-auf-telekom-netz-zugreifen-1.2128313 (13.08.2015).

Süddeutsche Zeitung (2014d): Schreibmaschine soll für sichere Kommunikation sorgen, 14.07.2014, http://www.sueddeutsche.de/politik/nsa-untersuchungsausschuss-schreibmaschine-soll-fuer-sichere-kommunikation-sorgen-1.2045675 (16.08.2015).

Symantec (2014): Security Response. Regin: Top-tier espionage tool enables stealthy surveillance, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf (7.08.2015).

The New York Times (2013): N.S.A. Report Outlined Goals for More Power, 22.11.2013, http://mobile.nytimes.com/2013/11/23/us/politics/nsa-report-outlined-goals-for-more-power.html?hp=&pagewanted=all&_r=4 (13.08.2015).

Weißer, Bettina / Heine, Günter (2014): Täterschaft und Teilnahme (§§ 25–31), in: Schönke, Adolf / Schröder, Horst (Hrsg.): StGB. Kommentar, C.H. Beck: München, 478–570.

Wolf, Joachim (2013): Der rechtliche Nebel der deutsch-amerikanischen ,,NSA-Abhöraffäre“, in: Juristen Zeitung 68:21, 1039–1046.

Zeit Online (2015): Alles Wichtige zum NSA-Skandal. Welche Daten sammelt die NSA, was ist Prism und wie reagieren die Überwachten? Aktuelle Entwicklungen und ein Überblick über die Snowden-Enthüllungen seit Juni 2013, 02.07.2015, http://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal (13.08.2015).

Zöller, Mark (2007): Der Rechtsrahmen der Nachrichtendienste bei der „Bekämpfung“ des internationalen Terrorismus, in Juristen Zeitung 62:15/16, 763–771.

Autor

PD Dr. Kai Cornelius, LL.M.
Lehrstuhlvertreter an der Humboldt-Universität zu Berlin – Juristische Fakultät
Lehrstuhl für Strafrecht, Strafprozessrecht und Urheberrecht
Unter den Linden 6
D-10099 Berlin
cornelius@rewi.hu-berlin.de

DOI: 10.11588/josar.2015.0.23482

Die materiellen Ursachen des Cyberkriegs
Cybersicherheitspolitik jenseits diskursiver Erklärungen

Myriam Dunn Cavelty

1 Einleitung

Euphoriker des Informationszeitalters sprachen Staaten jahrelang die Fähigkeit ab, ihre Macht im virtuellen Raum entfalten zu können. Zu hierarchisch, langsam und unflexibel seien sie, um auf die entfesselte Dynamik des Cyberspace[1] und dessen Nutzung adäquat reagieren zu können (siehe z.B. Barlow 1996; Rosenau 1998). Jüngste Entwicklungen in der internationalen Politik zeigen jedoch, dass das Gegenteil zutrifft: Der Cyberspace wird als strategische Domäne angesehen, deren Aufbau und Steuerung nicht mehr nur nichtstaatlichen Akteuren überlassen werden kann. Staaten begegnen den von ihnen zunehmend ernst genommenen Cyberunsicherheiten, indem sie im Namen der nationalen Sicherheit mit wachsender Durchsetzungskraft Aspekte des virtuellen Raums ihrer Kontrolle unterwerfen (Schneier 2012, 2013; Meinrath et al. 2011). Da die Cyber-Domäne zu 100 Prozent menschengemacht ist und aufgrund von physischer Infrastruktur wie Kabeln und Servern auch gezwungenermaßen einer geographisch nationalstaatlichen Logik unterworfen ist, ist staatliche Machtausübung relativ einfach möglich – wenn auch zu einem bestimmten Preis (vgl. den Beitrag von Milton Mueller in diesem Band).

Auf Sicherheit zielende staatliche Interventionen, die diesen Raum nun einer nationalen Sicherheitslogik unterwerfen wollen, kollidieren häufig direkt mit rivalisierenden Vorstellungen, wie der Cyberspace ausgestaltet werden soll. Dies verursacht beträchtlichen Widerstand gegenüber nationalen Regulierungsversuchen, mit hohen Kosten für alle Beteiligten. Konkret führt die Bereitschaft von Staaten, Sicherheitsbedürfnisse über andere Bedürfnisse zu stellen, dazu, dass staatliche Kontrolle über Informationsflüsse und Bestrebungen, nationale Cyberräume zu bauen, sprunghaft zugenommen haben: Autoritäre Regime begrüßen dies, um ihre Macht weiter zu festigen (Deibert et. al. 2008, 2010; Deibert 2013). Auch in demokratischen Staaten gibt es mehr staatliche Überwachung und Zensur als je zuvor. Und je mehr sich der Diskurs um solche Kontrollversuche dreht, desto deutlicher geht es um physische Infrastrukturen, die den

1 In diesem Beitrag wird der Begriff Cyberspace anstelle des Begriffs Internet verwendet. Im populären Sprachgebrauch werden die zwei Begriffe oft als Synonyme gebraucht, in der sozialwissenschaftlichen Forschung aber wird das Internet als Teilaspekt des Cyberspace verstanden (vgl. Deibert et al. 2010). Der Cyberspace hat sowohl eine „virtuelle“ wie auch eine „physische“ Dimension.

Prinzipien der Territorialität und Souveränität unterworfen werden können und sollen (Dunn Cavelty 2015).

Im Zusammenhang mit der Zuspitzung, die das Thema der Cybersicherheit in den letzten Jahren erfahren hat, geht dieser Beitrag der folgenden Frage nach: Aufgrund von welchen Unsicherheitsfaktoren lässt sich der Anstieg von staatlicher Macht im Cyberspace erklären und welche Konsequenzen ergeben sich dadurch? Im Gegensatz zu der existierenden Forschung wird in diesem Beitrag das Argument entwickelt, dass es nicht nur diskursive Prozesse sind, die eine verstärkte Verknüpfung des Cyberspace mit der nationalen Sicherheit vorantreiben, sondern auch grundlegende technisch-materielle Faktoren und Praktiken, die sich der sozialwissenschaftlichen Forschung bisher weitgehend entziehen. Diese Dimension muss vermehrt beachtet werden, wenn wir politische Cybersicherheitsprozesse und ihre Konsequenzen (politischer, sozialer und wirtschaftlicher Natur) umfassender verstehen wollen.

Der Beitrag umfasst vier Teile. Im ersten wird die dominante Theorie in der Cyber-Sicherheitsforschung (*Securitization Theory*) kritisch im Hinblick auf ihre Erklärungskraft betrachtet und einige weiterführende theoretische Überlegungen angestellt, die zusätzliche Aspekte von Cybersicherheitspolitik in den Fokus rücken. Es wird eine Ergänzung der gängigen Analysen von eliteproduzierten, öffentlich zugänglichen Dokumenten durch den Einbezug von materiellen Unsicherheitsfaktoren und Sicherheitspraktiken propagiert. In einem zweiten Teil werden materielle Faktoren der Unsicherheit und ihr Einfluss auf die Cybersicherheitspolitik skizziert. In einem dritten Abschnitt werden drei Arten von auf diesen Faktoren beruhenden Konzeptionen des Cyberkriegs beschrieben. Dabei wird gezeigt, dass die Macht dieses Begriffs nicht nur in der Politik des „Worst Case" zu finden ist (vgl. Dunn Cavelty 2013a), sondern in seiner allumfassenden, andere Begrifflichkeit integrierenden/inkorporierenden Wirkung, die zu einem großen Teil auf materielle Unsicherheiten baut. Im letzten Teil werden die Wirkungen dieser Konzeptionen für die Cybersicherheit und allgemein die internationale Sicherheit aufgezeigt, die sich auch am besten auf materieller Ebene erschließen.

2 Theorie und Cybersicherheit

Einen genauen Zeitpunkt für den Anstieg von staatlicher Machtausübung im Cyberspace festzumachen, ist schwierig. Grund dafür ist unter anderem, dass es bisher keine zweckmäßigen Indikatoren gibt, die Dynamik staatlicher Macht in der Cyberdomäne über einen genügend langen Zeitraum zu messen.[2] Darüber hinaus zeichnen sich Cybersicherheitsdiskurse dadurch aus, dass es darin keinen einheitlichen, klar dominierenden Deutungsrahmen gibt. Stattdessen findet sich zu jeder Zeit eine Vielzahl von nebeneinander laufenden Diskursen, die sich auf unterschiedliche Aspekte der Prob-

2 Ein möglicher – aber nicht sehr valider – Indikator ist der Grad an „Internet freedom" (also Netzfreiheit), der z.B. von der Institution Freedom House erhoben wird (siehe: https://freedomhouse.org/issues/internet-freedom#.VVG9imP2P7Y). Das Problem dabei ist jedoch, dass staatliche Macht hier immer als Gegensatz zu Netzfreiheit verstanden wird.

lematik beziehen (Cyberkriminalität, Cyberterror, Cyberspionage, Cyberkrieg) und die unterschiedliche Lösungsansätze nach sich ziehen – die meistens einen Mix von staatlicher und nicht-staatlicher „Machtausübung“ beinhalten (Dunn Cavelty 2012). Wie im ersten Unterkapitel beschrieben wird, heißt das, dass eine der prominentesten Sicherheitstheorien, die Sekuritisierungstheorie der „Kopenhagener Schule” (Buzan et al. 1998), die sich mit den Wirkungen von Gefahrendarstellungen im politischen Prozess auseinandersetzt, nur sehr beschränkt Erklärungen für die Gründe für und Konsequenzen der Cybersicherheitspolitik liefert. Obwohl die Theorie in den letzten Jahren konstant weiterentwickelt und angepasst wurde, hat sie einige grundsätzliche Schwächen, die es verunmöglichen, dass sie die Dynamik der Cybersicherheitspolitik adäquat erklären kann. In einem zweiten Unterkapitel wird daher ein Vorschlag gemacht, welche Art von Theorie besser geeignet wäre.

2.1 Securitization Theory +

Die *Securitization Theory* sagt, dass die erfolgreiche *Securitization* (Versicherheitlichung) eines Themas den Einsatz aller verfügbaren Mittel rechtfertigt – insbesondere solche, die normale politische Spielregeln außer Kraft setzen. Um eine Versicherheitlichung zu erzielen, muss vorgängig eine mobilisierende diskursive Rechtfertigung für diesen außerordentlichen Zustand präsentiert werden, welche dann im politischen Prozess akzeptiert oder abgelehnt werden kann. Dies geschieht in der narrativen Darstellung der drohenden Gefahr (oder eines Risikos) und des dadurch bedrohten Referenzobjekts, in Form eines Sprechakts. Dabei erkennt die Theorie grundsätzlich nur eine Logik von Sicherheit an: eine Sicherheit, ohne die das Überleben (*survival*) (eines wertvollen Objekts, meist des Staats) gefährdet ist und die zu erreichen daher immer den Einsatz von außerordentlichen, den demokratischen Prozess sprengenden Maßnahmen rechtfertigt (vgl. Corry 2012).

Die Theorie (und diverse Abwandlungen davon) sind vereinzelt schon auf Cyberthemen angewandt worden (Bendrath 2003; Hansen et al. 2009; Lawson 2011). Dabei stand die Frage im Zentrum, ob der Themenkomplex Cybersicherheit insgesamt versicherheitlicht ist oder nicht. Die Literatur hat darauf keine einheitliche Antwort entwickelt: Je nach Schwerpunkt entweder auf die „multi-dimensional cyber disaster scenarios“ (Hansen et al. 2009: 1164) oder die tatsächlich umgesetzten Lösungen (Bendrath 2003) kommen die Autoren zu unterschiedlichen Schlüssen: erstere dazu, dass der Komplex versicherheitlicht ist; zweitere dazu, dass er es nicht ist. Allerdings sollte die Frage gestellt werden, ob die Feststellung, ob etwas versicherheitlicht ist oder nicht, überhaupt relevant ist, ohne dass die konkreten Konsequenzen der Versicherheitlichungsversuche aufgezeigt werden können. Die Theorie hat nämlich Mühe, heterogene Prozesse und über verschiedene Politikfelder fragmentierte Antworten auf Gefahren zu erklären, die nicht durchgehend der einen an „dem physischen Überleben (survival)“ geknüpften Logik von Sicherheit folgen (Neal 2009; Huysmans 2011).

Verschiedene Wissenschaftler haben über die Jahre versucht, diese Schwäche der Kopenhagener Schule durch Zusätze zu überwinden, die auch für Teilaspekte der Cybersicherheit relevant sind. Einige seien hier knapp skizziert. Jackson zum Beispiel (2006) hat das Konzept der „rhetorischen Versicherheitlichung" als eine Art Unterkategorie von gescheiterten Versicherheitlichungen eingeführt, bei der ein Sicherheitsproblem zwar als solches akzeptiert wird, dieser Prozess aber zu keiner außergewöhnlichen Maßnahme in der Politik führt. In der Tat finden wir die Cybersicherheit längst in nationalen Sicherheitsstrategien wieder – und doch ist es schwierig, den gesamten Themenkomplex als versicherheitlicht zu bezeichnen, insbesondere, wenn „außergewöhnliche“ Maßnahmen als ausschlaggebendes Kriterium angesehen werden, an denen es oftmals mangelt (Bendrath 2001; 2003). Andere Forschende haben festgestellt, dass der Prozess der Versicherheitlichung in einer bestimmten sozio-politischen Gemeinschaft nicht nur auf eine Arena und eine Art von Publikum beschränkt ist, sondern auch aus sich überlappenden Prozessen besteht (Balzacq 2005, 2008; Léonard et al. 2011). Damit ließen sich die Unterschiede in den Versicherheitlichungdynamiken für verschiedene Cybergefahrenkategorien bestimmen.

Andere wiederum schauen sich den zeitlichen Ablauf von Versicherheitlichungsprozessen an, um die Fixierung der Kopenhagener Schule auf einen bestimmten performativen Moment zu überwinden (Salter 2008: 575ff.). Versicherheitlichung ist dann vielmehr ein nie abgeschlossener Prozess, während dessen ständig neue Vorstöße gemacht werden und etablierte Versicherheitlichungslogiken aufrechterhalten werden müssen. Ähnliche Ansätze, die sich auf Versicherheitlichung als Prozess konzentrieren, entlang dessen Entscheidungsträger Herausforderungen kategorisieren können (von nicht-politisiert, zu politisiert, zu versicherheitlicht), lassen unterschiedliche und damit auch unterscheidbare „Grade“ von Versicherheitlichung zu (Haacke und Williams 2008; McDonald 2008). Mit einem solchen Ansatz ließen sich die unterschiedlichen (historischen) Phasen der Cybersicherheit und unterschiedliche Gefahrenkategorien und deren Wirkung besser verstehen und erklären, ohne den einen, ausschlaggebenden Moment der Versicherheitlichung identifizieren zu müssen.

2.2 Sicherheitspraktiken und die „little security nothings“

Mit den eben beschriebenen Zusätzen zur klassischen *Securitization Theory* können Dynamiken in der Cybersicherheitspolitik also teilweise erklärt werden. Der Theorie ist aber noch ein weiterer einschränkender Faktor zu Eigen. Wie fast alle diskurstheoretischen Ansätze schaut die Kopenhagener Schule fast ausschließlich auf „sichtbare” Sprechakte von politisch-öffentlichen Akteuren, die durch ein spezifisches Publikum akzeptiert werden können oder nicht (Huysmans 2011: 371). Securitization-Untersuchungen konzentrieren sich oft auf offizielle Aussagen von Staatsoberhäuptern, hochrangigen Beamten oder Leitern von internationalen Institutionen (Hansen 2006: 64). Dabei wird zumeist auf öffentlich zugängliche Dokumente (Reden, offizielle

Berichte, teilweise auch Bildmaterial etc.) zurückgegriffen, was aufgrund der einfachen Verfügbarkeit zu Vorteilen, aber auch durchaus zu einem „selection bias“ (einer Stichprobenverzerrung) führen kann. Solch ein Untersuchungsfokus vermag daher primär die konstitutive Wirkung von diskursiven Praktiken privilegierter Sprecher in der (Welt-)Politik aufzuzeigen. Was hingegen häufig kaum beachtet wird, ist wie diese diskursiven Praktiken durch zeitlich vorgelagerte sprachliche und nicht-sprachliche Praktiken von diesen und anderen Akteuren, die weniger leicht erkennbar oder attribuierbar sind, erleichtert oder vorbereitet werden.

Tatsächlich kann die Cybersicherheit als (sicherheits-)politisches Phänomen nur verstanden werden, wenn sie nicht nur mit Situationen von größter Dringlichkeit in Zusammenhang gebracht wird. Vielmehr geht es bei der Herstellung von Sicherheit im Cyberspace in erster Linie um alltägliche, „normale“ Routineprozesse und Verfahren, die entwickelt wurden, um Netzwerke, Computer, Programme und Daten vor Angriffen, Schäden oder unberechtigtem Zugriff zu schützen.[3] In Bezug auf die sicherheitsrelevanten Praktiken in bürokratischen Einheiten hat Jef Huysmans den Begriff der „little security nothings“ eingeführt (Huysmans 2011). So verstanden wird Cybersicherheit mitproduziert von jedem privaten Computerbenutzer, von IT-Support-Mitarbeitenden in den Serverräumen dieser Welt, von Programmierern, von Chief Information Officers (CIOs) oder Chief Executive Officers (CEOs), die Entscheide über Cybersicherheitsinvestitionen fällen, von IT-Spezialisten, die Regierungsnetzwerke sichern, von Sicherheitsberatern, von Cyberforensikern, von Regulierungsbehörden – und erst am Ende der cybersicherheitspolitischen Handlungskette von Politikern und anderen Regierungsbeamten, die Cybervorfälle interpretieren und auf sie mit verbalisierten Erwartungen und Befürchtungen und später auch Politiken reagieren.

Mit nicht klar eingrenzbaren politischen Phänomenen und solchen „little security nothings“ umzugehen weiß die Gouvernementalitätsforschung (vgl. Lemke et al. 2000). Gouvernementatlität ist ein Begriff, der auf Michel Foucault zurückgeht. Er versteht darunter

> „die Gesamtheit, gebildet aus den Institutionen, den Verfahren, Analysen und Reflexionen, den Berechnungen und den Taktiken, die es gestatten, diese recht spezifische und doch komplexe Form der Macht auszuüben, die als Hauptzielscheibe die Bevölkerung, als Hauptwissensform die politische Ökonomie und als wesentliches technisches Instrument die Sicherheitsdispositive hat“ (Foucault 2005: 171).

3 Cybersicherheit wird unter Experten nicht als Zustand, sondern als Prozess verstanden, der die Risiken, die aus dem Cyberraum jetzt und in Zukunft erwachsen, unter Berücksichtigung der IT-Schutzziele und unter Berücksichtigung der nötigen Funktionalität durch entsprechende Gegenmaßnahmen technischer, organisatorischer, rechtlicher und politischer Natur laufend auf ein gesellschaftlich akzeptiertes Maß zu reduzieren sucht. Die IT-Schutzziele im engen Sinne sind: Vertraulichkeit, Integrität, Verfügbarkeit, Authenzitität. Im erweiterten Sinne kommen hinzu: Zurechenbarkeit, Verbindlichkeit/Nicht-Abstreitbarkeit, Nicht-Anfechtbarkeit und in bestimmten Kontexten, wie z. B. im Internet, Anonymität. Die Basis für Cybersicherheit ist dabei in erster Linie die IT-Sicherheit und ihre Maßnahmen.

In den europäischen Sicherheitsstudien werden Gouvernementalitätsansätze seit einigen Jahren gewinnbringend auf komplexe und heterogene Probleme wie z.B. Terrorbekämpfung angewendet (siehe z.B. Aradau et al. 2007; Amoore et al. 2005). Ein solcher Ansatz erlaubt eine viel breitere Erfassung von Problemen, Konzepten, Techniken und Handeln in Bezug auf ein politisches Problem, als sie der Ansatz der Kopenhagener Schule ermöglicht. Forschende müssen sich nicht auf einen Teilaspekt und nicht nur auf eine Logik von Sicherheit beschränken. Insbesondere das Konzept des „Risikos" hat so verstärkt in der Sicherheitsforschung Fuß gefasst (Petersen 2012).

Methodisch-empirisch ergeben sich durch einen solchen Ansatz neue Herausforderungen. Nach wie vor können öffentlich zugängliche Dokumente studiert werden, dabei muss aber nicht auf Sprechakte geschaut werden. Häufig wird auch auf die historische Methode der sogenannten „Genealogie" à la Foucault zurückgegriffen, um das Entstehen und die Normalisierung von spezifischen Sicherheitsdispositiven zu erklären. Was jedoch als zusätzliches Element in den Blickpunkt rückt, sind Sicherheitspraktiken von Nicht-Eliten. Für die Forschung im Bereich der Cybersicherheit bedeutet dies, dass das Studium von öffentlich zugänglichen Dokumenten unbedingt und ganz im Sinne des „practice turns" (Schatzki et al. 2001) durch das Studium von Praktiken, soweit diese zugänglich sind,[4] ergänzt werden muss. Darüber hinaus erscheint es gewinnbringend, den Fokus auf die soziopolitischen Prozesse zu richten, die sich rund um Cybervorfälle (Schadsoftware, aber auch Hacktivismus- und Hackingkampagnen) abspielen.

2.3 Die technische Voraussetzung für Cyberunsicherheit

Dieser Beitrag kann dem Anspruch nach einer vertieften Analyse unter Einbezug von materiellen Faktoren und alltäglichen Praktiken nicht gerecht werden. Zumindest aber will er technisch-materielle Faktoren der Unsicherheit hervorheben und gleichwertig (oder ergänzend) neben Sprechakte stellen. Damit soll nicht behauptet werden, dass materielle Faktoren außerhalb und über politischen Entscheidungen und diskursiven Prozessen stehen. Dennoch bilden sie eine fundamentale Voraussetzung für die Art und Weise, wie die sicherheitspolitische Dimension der Cybersicherheit in Sprechakten etabliert werden kann. Neben einer Reihe von Trends im Bereich der Cybergefahren, die diese verstärkte Beachtung verursacht haben (vgl. z.B. Dunn Cavelty 2012b; 2015 – und siehe den folgenden Abschnitt), gibt es einige relativ konstant bleibende Faktoren der Unsicherheit, die mit den Technologien und deren Nutzung einhergehen, welche den virtuellen Raum ermöglichen und für diverse Akteure so attraktiv machen.

Fakt ist, dass digitale Technologien über die Jahre auf dem denkbar unsichersten Niveau im Cyberspace zusammengewachsen sind. Das hat teils historische Gründe, denn zu der Zeit, als das Internet für den wissenschaftlichen Datentransfer gebaut

4 Spätestens seit den Enthüllungen von Edward Snowden ist klar, dass die Geheimdienste und das Militär (oftmals in Kombination) zentrale Akteure im Bereich der Cybersicherheit sind. Ihre Praktiken bleiben jedoch bislang weitgehend unerforscht.

wurde, legten die Netzwerk-Designer mehr Gewicht auf die Robustheit und Ausfalltoleranz des Netzwerks als auf Sicherheitsaspekte. Aufgrund der wenigen (großen) Maschinen, die miteinander vernetzt waren, gab es dafür wenig Anlass. Die heutige Computernetzwerkumgebung ist deshalb so anfällig, weil sie aus der gleichen (unsicheren) Netzwerk-Technologie von damals besteht, diese aber mit viel offeneren (sprich ebenfalls unsicheren) Systemen kombiniert, die untereinander zudem stärker vernetzt sind (Libicki 2000; Warner 2012). Zudem hat die fortlaufende Globalisierung von Informationsnetzwerken zu einer drastischen Erhöhung der Komplexität geführt. Je komplexer ein IT-System aber ist, desto mehr Fehler enthält es; und desto schwieriger ist es, die IT-Sicherheit des Systems zu kontrollieren, zu gewährleisten oder zu verwalten. Das gleiche gilt für die verwendete Software.

Hinzu kommen ökonomische Gründe: Sehr schnelle Innovationszyklen bei IT-Produkten sind hinderlich für die Einführung von Sicherheitsmaßnahmen, denn sie wirklich sicher zu machen, dauert häufig länger als die Entwicklung der IT-Nachfolgegeneration selbst, so dass der angestrebte (oder erstrebenswerte) Sicherheitsstandard nie erreicht wird. Zudem haben Sicherheitsstandards oft einen negativen Effekt auf die Funktionalität und Benutzerfreundlichkeit (Andersson 2001). Auch ist der Softwaremarkt wegen des so genannten Netzwerkeffekts (der Nutzen an einem Produkt wächst, wenn dessen Nutzerzahl größer wird) geprägt von der Winner-takes-it-all-Logik und daraus hervorgehenden (Quasi-)Monopolen. In dem herrschenden hohen Kosten- und Zeitdruck bei der kommerziellen Software-Entwicklung wird daher meist nur auf die Funktionalität und eine schnelle Auslieferung geachtet. Qualitätskriterien, gerade in Bezug auf Sicherheit, spielen dabei eine untergeordnete oder gar keine Rolle. In den meisten Programmen und Betriebssystemen befinden sich daher unzählige (häufig nicht einmal bekannte) Sicherheitslücken, die zu ganz unterschiedlichen Zwecken missbraucht werden können – und werden.

Viele Attacken – die wirkungsvollsten bleiben häufig lange oder sogar für immer unerkannt – „beuten“ Sicherheitslücken aus, um auf das angegriffene System zugreifen zu können. Hat ein Angreifer Zugriff aus das Innenleben des Systems, kann er die sich darin befindenden Informationen zum Beispiel kopieren, korrumpieren, zerstören, abändern, stehlen, usw. (Waltz 1998). Abhängig vom Wert oder der Bedeutung der Informationen haben solche Aktionen unterschiedlich schwerwiegende Auswirkungen. Es ist daher unumstritten, dass Cyberangriffe Konsequenzen in der Form von z.B. Kosten haben. Das Beachtenswerte aus analytischer Sicht ist also nicht, dass den möglichen Gefahren des Cyberspace im politischen Prozess Beachtung geschenkt wird oder dass Überlegungen angestellt werden, ob der jeweilige Staat zusätzliche Anstrengungen zu ihrer Bekämpfung unternehmen soll. Hingegen ist bemerkens- und untersuchenswert, was oder wer zu welcher Zeit und durch wen die meiste Aufmerksamkeit (und welche Art von Ressourcen) erhält.

Dass Cybersicherheit als sicherheitspolitisches Problem angesehen wird, ist nicht selbsterklärend oder selbstverständlich, obwohl eine solche Deutung heute kaum

mehr hinterfragt wird. Es lässt sich beobachten, wie seit den 1980er Jahren im politischen Prozess verschiedene diskursive Verknüpfungen zwischen Cyberspace und anderen Themen und Objekten vorgenommen wurden, die zu dieser sicherheitspolitischen Deutung beigetragen haben – also z.B. neue Gefahrenkategorien wie Cyberterror geschaffen wurden. Eine große Rolle dabei spielte die „Form" des Cyberspace. Diese Prozesse sollen nicht Fokus dieses Beitrags sein, denn sie wurden anderswo bereits beschrieben (vgl. Dunn Cavelty 2010). Für die Ausführungen hier ist vor allem die Kopplung zwischen Computern (oder Informationsinfrastrukturen) und so genannten kritischen Infrastrukturen ausschlaggebend.

Unter dem Begriff Infrastrukturen – bestehend aus den beiden Wörtern „infra" („unterhalb") und „Struktur" („Gefüge, Bau, Aufbau") – versteht man Anlagen, Einrichtungen, Organisationen, aber auch Prozesse, Produkte, Dienstleistungen und Informationsflüsse, die den „Unterbau" für das reibungslose Funktionieren der Gesellschaft, der Wirtschaft und des Staates bilden. Als kritisch werden jene Infrastrukturen bezeichnet, die bei einem Ausfall zu gravierenden politischen oder wirtschaftlichen Schäden führen können (Dunn Cavelty et al. 2008; Collier et al. 2008).[5] Nach deren weitgehenden Privatisierung in den 1980er und 90er Jahren befinden sich viele dieser für die nationale Sicherheit wichtigen Objekte derzeit in privater Hand. Obwohl in vielen Sektoren Regulierungen bestehen, die auch die Sicherheit betreffen (häufig jedoch nicht direkt nationale Sicherheit, sondern eher die „Safety"),[6] folgen die Betreiber von kritischen Infrastrukturen grundsätzlich den Regeln des freien Markts und streben nach Gewinnmaximierung.

Neben klassischen Risiken wie Naturkatastrophen oder Feuer bilden Cybergefahren seit einigen Jahren eine neue Risikogruppe für kritische Infrastrukturen. Der Grund dafür ist, dass im Zuge von Automatisierungs- und Effizienzsteigerungsprozessen kritische Infrastrukturen häufig computerisiert wurden.[7] Ehemals isolierbare Geräte, wie industrielle Steuerungssysteme und Fabrikmonitore, die nun digital steuerbar und zugänglich gemacht werden, sind aber nie dafür entwickelt worden, mit dem Cyberspace verknüpft zu werden. Mit der steigenden Zahl von eingebetteten Systemen und mit deren wachsender Vernetzung untereinander (drahtlos wie auch kabelgebunden) er-

5 In diese Kategorie fallen gemeinhin die Energieversorgung, die Kommunikation, das Gesundheitswesen, der Verkehr oder die öffentliche Sicherheit. Die Bestimmung, was kritisch ist und was nicht, ist ein diskursiver Prozess, wohingegen die Verknüpfung von ehemals analogen Systemen mit digitalen Komponenten keiner ist.

6 „Safety" und „Security" werden auf Deutsch beide mit Sicherheit übersetzt und auch auf English sind die beiden Wörter sehr eng miteinander verbunden. In der technischen Community wird traditionellerweise das Wort „Safety" für Betriebssicherheit verwendet und das Wort „Security" für Angriffssicherheit (vgl. englische Übersetzung der Nationalen Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie; Bundesministerium des Innern 2009: 3): „Sicherheitsstandard und die Ausfallsicherheit Kritischer Infrastrukturen" übersetzt als „safety standard and failure safety of critical infrastructure".

7 Es gibt sogar kritische Infrastrukturen, die sich mehr über Daten und Prozesse charakterisieren lassen, als über physische Komponenten (z.B. Finanzwesen) – eine solche Unterscheidung soll hier aber nicht gemacht werden.

höht sich damit objektiv gesehen deren Verwundbarkeit. Mit Hilfe von Suchmaschinen wie Shodan haben Forscher festgestellt, dass Millionen von Geräten, einschließlich solchen, die hochsensible Prozesse steuern, über das Internet zugänglich sind und dass 25–30 Prozent davon schlecht oder gar nicht gesichert werden und damit anfällig für Malware-Attacken sind (Jackson Higgins 2013).

Natürlich ist eine Schwachstelle in einem Computersystem, das kritische Prozesse steuert, noch nicht per se eine Bedrohung für die nationale Sicherheit. Das Wissen um diese Verwundbarkeiten und die Gewissheit, dass sie von böswilligen Akteuren ausgenutzt werden könnten, ist jedoch ein zentraler Bestandteil für die sicherheitspolitische Deutung der Cybersicherheit. Diskursive Prozesse setzen hier ein – die technische Unsicherheit ist die Basis dafür.

3 Drei Facetten des Cyberkriegs

Der Grund, warum Staaten heute mehr als früher bestrebt sind, Macht im Cyberspace auszuüben, ist in der Kombination von technisch-materiellen Faktoren und deren diskursiven Deutung/Verwertung im politischen Prozess zu finden. Seit jeher zeichnen sich Cybersicherheitsdiskurse nämlich dadurch aus, dass Cybervorfälle – die durch Schadsoftware oder DDoS-Attacken[8] hervorgerufen werden – herangezogen werden, um den Ernst der Lage für einen Akteur zu unterstreichen und um dann spezifische Ressourcen zu mobilisieren. Dabei ist es vor allem der Begriff des Cyberkriegs, der in vielen Facetten die Debatte dominiert. Bemerkenswert an diesem Begriff ist, dass damit weitaus nicht nur kriegsähnliche Formen der Cyberaggression bezeichnet werden; vielmehr sind es quasi alle Aggressionsformen, bei denen das Einwirken eines staatlichen Akteurs vermutet werden kann. Dadurch besetzt der Begriff „Cyberkrieg“ im Cybersicherheitsdiskurs eine hegemoniale Position, so dass alle daran Beteiligten und davon Betroffenen gezwungen sind, sich ihm ständig zu widmen, auch wenn sie ihn ablehnen. Der Begriff wird so laufend in seiner andere Logiken inkorporierenden Position bestärkt.

Die Effekte dieser Überdeterminierung liegen zum einen in der ständigen Mobilisierung von „Worst Case“-Szenarien als Beweis für die Dringlichkeit des Problems und in der Etablierung militärischer Zuständigkeit für Cyberfragen, was u.a. konkrete budgetäre Konsequenzen hat. Die Cyberverteidigung ist dann auch der eine Bereich, in dem die Ausgaben auch in Zeiten der allgemeinen militärischen Budgetkürzungen stetig steigen (Brito et al. 2011; Deibert et al. 2011). Zum anderen aber entsteht die Möglichkeit, die unterschiedlichsten Arten von Cybervorfällen als Cyberkrieg zu bezeichnen, eben durch die zuvor beschriebene technisch-materielle Logik. In den folgenden drei Unterabschnitten wird das Zusammenspiel zwischen technisch-materiellen Unsicherheitsformen und den diskursiven, politischen Elementen exemplarisch an drei „For-

8 DDoS-Attacke=Distributed Denial-of-service. Dabei wird ein Netzwerkdienst durch Überlastung nicht-verfügbar gemacht.

men“ des Cyberkriegs aufgezeigt. Das erste schaut sich den Cyberkrieg als Hacktivismus an. Das zweite die militärische Debatte zu Kriegsformen im Cyberspace. Das dritte analysiert „Advanced Persistent Threats“ (APTs), denen seit rund fünf Jahren besonders viel Aufmerksamkeit gewidmet wird.

3.1 Hacktivismus und seine sichtbaren Effekte

Der „Hacktivismus“ – ein Kofferwort aus „Hacking“ und „Aktivismus“ – hat sich spätestens seit der Kosovo-Intervention von 1999 als Form des politischen Protests etabliert: Heutzutage weist quasi jeder politische, wirtschaftliche und militärische Konflikt eine Cyberkomponente auf, die die eigentlichen Konflikthandlungen begleitet. Da der Hacktivismus neben unterschiedlichen Formen der Cyberkriminalität die weitaus häufigste Form von Cyberaggression ist, kommt ihm im allgemeinen Gefahrendiskurs eine sehr große Rolle zu. Durch die virtuelle Veränderung oder Zerstörung von Inhalten, wie z.B. dem Hacken von Webseiten oder dem Ausschalten eines Servers durch Datenüberflutung (DDoS-Attacke), kreiert der Hacktivismus „sichtbare“ Effekte (u. a. der Unterbrechung), die häufig, ganz im Sinne der Hacktivisten, medial ausgeschlachtet und aufgebauscht werden. Dabei steht er im Gegensatz zu anderen Cyberaggressionsformen, die keine sichtbaren Effekte kreieren, weil die Schadsoftware, die dahintersteckt, verborgen bleiben möchte.

Auch wenn eine systematische und empirisch saubere Auswertung von Hacktivismuskampagnen bisher fehlt, lässt sich doch festhalten, dass die Auswirkungen auf den eigentlichen Konflikt und dessen Verlauf fast ausschließlich marginal sind und der tatsächlich entstandene Schaden klein bis sehr klein bleibt. Der weitaus größere Effekt dieser digitalen Proteste entsteht im politischen Prozess, der Hacktivismus als Form des Cyberkriegs etabliert hat, auch wenn die Rolle von staatlichen Akteuren meistens unklar oder sogar fragwürdig bleibt.[9] Wie aber ist es möglich, dass dem Hacktivismus ein solcher Status in der sicherheitspolitischen Debatte zukommt?

Ein Fokus auf den Versicherheitlichungsprozess zeigt, wie die Vorfälle in Estland (2007) zum Beispiel[10] herangezogen werden, um die Realität des Cyberkriegs im Hier und Jetzt zu beweisen. Bemerkenswert dabei ist, dass die Details oder Annahmen hin-

9 Auch die Aktionen von WikiLeaks und der Hackerkollektive Anonymous oder LulzSec haben dem Hacktivismus unlängst sehr viel Aufmerksamkeit beschert – sie seien hier aber nur am Rande erwähnt. WikiLeaks handeln unter der Hackermaxime „Informationen sollten frei sein“ und rütteln an der Macht von Staaten, gewisse Informationen im Namen der nationalen Sicherheit unter Verschluss zu halten. Die Hackerkollektive greifen aufgrund der Medienwirksamkeit oft Ziele an, die als „kritische Infrastrukturen“ gelten und liefern so die Vorlage, um als nationales Sicherheitsproblem definiert zu werden (vgl. Dunn Cavelty et al. 2015).

10 Estland 2007 bezeichnet DDoS-Attacken auf Estland, die sich u.a. gegen das estnische Parlament, Banken, Ministerien und Rundfunksender richteten. Diese Attacken waren eine Begleiterscheinung eines Aufruhrs von russischen Esten, die gegen die Umstellung eines Denkmals protestierten. Der „cui bono“-Logik folgend, wurde die russische Regierung als Drahtzieher oder zumindest als Auftraggeber der Angriffe etabliert. Auch wenn eine Beteiligung nie bewiesen werden konnte, hält sich diese Attribution hartnäckig.

ter diesem Vorfall nicht mehr erläutert werden müssen: Es reicht, dass „Estland 2007“ gesagt wird, um ein Versicherheitlichungsargument zu machen. Das Wissen (und Nichtwissen) in Bezug auf diesen Vorfall hat sich im politischen Prozess zu einer spezifischen Wahrheit verdichtet, die Akteure wie Intentionen und Konsequenzen beinhaltet. Die Logik, die dabei zum Tragen kommt, ist die „cui-bono“-Logik. Die als „wem zum Vorteil“ zu übersetzende lateinische Frage drückt aus, dass der Verdacht am ehesten auf denjenigen fallen sollte, der durch eine (Straf-)Tat den größten Nutzen davonträgt. Im Falle von Estland 2007 weist die cui-bono Logik auf Russland hin, das mit Hilfe von nicht klar ihm zuordenbaren Aktivitäten im Cyberspace, die auf kritische Infrastrukturen abzielen, eine Machtdemonstration vornehmen will. Damit (staatlicher Akteur, der kritische Infrastrukturen angreift) lassen sich Aussagen von hochrangigen NATO-Generälen erklären, die sofort von einem potenziellen Bündnisfall sprachen.

Die „cui-bono“-Logik kann in diesem Diskurs nur eine so starke Stellung einnehmen, weil die technisch-materiellen Spielregeln des Cyberspace die gesicherte „Attribution“ (in etwa: Zuordnung) eines Angriffs äußerst schwierig, in gewissen Fällen sogar unmöglich machen. Das heißt: Clevere Gegner können sich vollkommen in der Anonymität des technischen Systems verbergen und gut gemachte Angriffe sind unmöglich einem exakten Ursprung zuzuordnen (Gaycken 2011: 80–90). Wenig erstaunlich: Das Attributionsproblem von Cyberattacken ist eines der Hauptthemen in der Cybersicherheitsdebatte, weil es die Logik der (militärischen und strafrechtlichen) Abschreckung fast gänzlich außer Kraft setzt (Rid et al. 2015). So lassen sich auch die „Lösungsansätze“ erklären, die auf technischer Ebene die Attribution ermöglichen wollen, was gleichzeitig fast immer die Aufgabe von Anonymität im Cyberspace bedeuten würde.

3.2 Vom strategischen und operativen Cyberkrieg

Eine fachspezifischere Debatte zum Cyberkrieg spielt sich in strategisch ausgerichteten amerikanischen Fachjournalen ab. In öffentlichen Versicherheitlichungsprozessen sind solche Diskussionen nicht abgebildet, sie sind jedoch äußerst relevant, um gegenwärtige militärische Pläne und den Einsatz militärischer Mittel zu verstehen. In der Debatte wird zwischen dem strategischen und dem operationellen Cyberkrieg unterschieden. Der strategische Cyberkrieg bezeichnet einen Krieg, der ausschließlich mit Cybermitteln geführt wird oder bei dem andere Kampfhandlungen zumindest der Cyberdimension untergeordnet werden. Er wird wie folgt definiert: „hostile actions in cyberspace that have effects that amplify or are equivalent to major kinetic violence“ (Nye 2011: 21). In diesem Bereich befinden sich die klassischen Cyber-doom-Szenarien der 1990er Jahre, in denen vollkommen unsichtbare Feinde einem Land z.B. quasi per Knopfdruck den Strom abstellen und es so in die Knie zwingen.

Grundsätzlich hat sich bei den Experten die Meinung durchgesetzt, dass ein strategischer Cyberkrieg in der nahen Zukunft sehr unwahrscheinlich ist (Sommer et al. 2011; Rid 2011; Gartzke 2013). Dafür werden etwa die unsicheren Resultate eines virtuellen

Angriffs, die fehlende Motivation auf der Seite der möglichen Angreifer und deren gemeinsames Unvermögen, sich gegen einen Gegenschlag zu wappnen, genannt: alles Faktoren, die auf materielle Effekte hinweisen. Darüber hinaus werden unkontrollierbare Rückkopplungseffekte im stark vernetzten virtuellen Raum genannt, die beträchtliche Risiken auch für einen angreifenden Staat/Akteur bergen. Dieser Faktor ist umso wichtiger, als diejenigen Staaten, die das technologische Know-how für strategischen Cyberkrieg am ehesten besitzen oder entwickeln können, besonders abhängig von ihren eigenen Informationsinfrastrukturen und damit in einem potentiellen IT-Krieg sehr verletzlich sind. Aufgrund unkontrollierbarer Nebeneffekte wäre ein Cyberkrieg wohl auch mit einer langfristigen Destabilisierung des Vertrauens in den Cyberspace verbunden, was negative Folgen für die Weltwirtschaft und damit ebenfalls für alle Beteiligten nach sich ziehen könnte (Rathmell 2001).

Technisch-materielle Faktoren sind auch dafür verantwortlich, dass in strategischen Zirkeln der operative Cyberkrieg viel mehr Aufmerksamkeit findet. Der operative Cyberkrieg wird definiert als militärische Operationen begleitendes Phänomen, bei dem es zu staatlichen Cyberattacken auf militärische und zivile bzw. Dual-use-Infrastrukturen kommt (z.B. Telekommunikationseinrichtungen, die von zivilen Stellen unterhalten werden, jedoch für zivile und militärische Zwecke genutzt werden) und sich eine Beeinträchtigung auch auf die zivile Supply-Chain (bspw. zivile Auftragnehmer für Logistik) erstrecken könnte. Ein solches Szenario ist am sinnvollsten, wenn es um darum geht, militärische Reaktionen unmittelbar vor oder während einer konventionellen Kampfhandlung zu verlangsamen oder zu verunmöglichen (Libicki 2009: 82). Ganz spezifisch wird im US-Militär einem „Fait Accompli“-Szenario im Zusammenhang mit einer Konfrontation zwischen China und den USA wegen Taiwan am meisten Aufmerksamkeit geschenkt. In dieser spezifischen Cyberkriegsdebatte spielen Verwundbarkeiten in der Infrastruktur („Vulnerabilities“) die größte Rolle – die Einschätzung dessen ist der Hintergrund für konkrete Szenarien, die in die Planung für begleitende Kriegsführung im Cyberspace einfließen.

3.3 Advanced Persistent Threats

Die dritte Art des Cyberkriegs ist nicht zerstörerisch, sondern geheim und stetig. Gewisse Aspekte dieser dritten Art werden im öffentlichen Raum besprochen, andere hingegen vor allem in der technischen Fachdebatte. Die Cybersicherheitsdebatte hat sich seit 2010 beträchtlich zugespitzt, nicht zuletzt, weil sich beobachtbare Angriffsmuster substantiell verändert haben. In Gefahrenberichten von öffentlichen Stellen wie auch Privatunternehmen wird vor allem von der steigenden Professionalisierung auf dem kriminellen Markt berichtet, der längst nicht mehr von Einzeltätern, sondern von der organisierten Kriminalität beherrscht wird.

Diese Beobachtungen der Professionalisierung gehen einher mit einer Verschiebung der Aufmerksamkeit von Massenereignissen hin zu gezielten Angriffen („targeted

attacks“). Zum einen sind in den letzten Jahren vermehrt so genannte „Mega Hacks“ bekannt geworden, in denen große Datenmengen aus Firmen und regierungsnahen Einrichtungen gestohlen wurden. Auf der anderen Seite liegt der Schwerpunkt der Debatte jetzt auf sogenannten *Advanced Persistent Threats* (APTs) – Schadsoftware (und neu auch Hackingkampagnen), die relativ komplex sind und die nicht die massenhafte Ausbreitung zum Ziel haben (wie z.B. Spam oder normale Viren), sondern vor allem für das Eindringen in ein spezifisches Ziel (System) geschrieben wurden (Dunn Cavelty 2015).[11]

In der gesamten Malwareumgebung machen APTs nur einen kleinen Prozentsatz aus (Maillart et al. 2010), aber auf Grund ihrer Auswirkungen und ihrem Link zu strategischer Nutzung des Cyberspace erhalten sie große Aufmerksamkeit – wenn sie entdeckt werden. APTs ermöglichen schleichende und kontinuierliche Cyberoperationen, die bestimmte Informationen oder Funktionen von spezifischen Unternehmen oder Organisationen zum Ziel haben. Sie sind „advanced“ (fortgeschritten), da das Programmieren der Malware ein gewisses technisches Können voraussetzt. Sie sind „persistent“ (anhaltend), weil es eine ständige Überwachung der Malware von außen und oft eine konstante Extraktion von Daten gibt. Und sie werden in Übereinstimmung mit dem Vokabular der IT-Sicherheit als „threats“ (Bedrohung) bezeichnet, da sie von einem menschlichen Akteur orchestriert werden.

Für die meisten sind die technischen Determinanten von APTs der Beweis, dass Staaten die Anonymität des Cyberspace dazu ausnutzen, Cyberspionage durchzuführen. Erstens werden die Kosten für das Programmieren von APTs (und vor allem den gezielten Einsatz) als relativ hoch eingeschätzt, während es beim Hacktivismus sehr niedrige finanzielle und technische Eintrittsbarrieren gibt. Um bei Cyberoperationen einen kontrollierten Effekt zu erzielen, muss der „Angreifer“ Wissen über spezifische, bisher nicht bekannte und/oder nicht-gepatchte Schwachstellen besitzen und auch über die Fähigkeiten, diese mit Hilfe einer dafür geschriebenen Malware auszunutzen. Beides erfordert einen relativ hohen Organisationsgrad. Der Preis für strategisch wertvolle Schwachstellen liegt derzeit bei rund 200.000 bis 300.000 US-Dollar (Miller 2007; Böhme 2005). Diese lassen sich auf einem Graumarkt kaufen, auf dem Berichten zufolge auch Regierungen Kunden sind (Perlroth et al. 2013). Ein Bericht schätzt, dass z.B. die NSA im Jahr 2013 zwischen 100 und 625 Schwachstellen gekauft hat (Frei 2013:

11 Im als „Bundestag-Hack“ bekannt gewordenen Cyber-Vorfall (entdeckt im Mai 2015) wurde gemäß der zur Verfügung stehenden Informationen ein sogenannter Trojaner verwendet, der mit einem Klick auf einen Link in einer Email installiert wurde. Die Schadsoftware hat Daten aus dem IT-System des Bundestags kopiert und an Unbekannt versandt; typischerweise ist aber bisher noch nicht vollständig klar, welche Daten es waren und wie groß der Umfang war. Als Täter werden „östliche“ (bzw. russische) Geheimdienste vermutet. Über die technischen Details des Angriffs ist nicht viel bekannt (siehe aber Beuth 2015), aber da es sich um eine gezielte und wohl auch über eine Zeit andauernde Attacke handelt, gehört der Bundestag-Hack in die Kategorie APT. Die Aufklärung des Vorfalls dürfte lange dauern, mit ungewissem Ausgang (siehe etwa Bewarder et al. 2015; Gebauer et al. 2015).

15). Gemäß der Washington Post hat sie dafür über 25 Millionen Dollar bezahlt (Fung 2013). Darüber hinaus braucht es nicht nur gute Programmierkenntnisse, sondern auch „Labore“, in denen die Ziele simuliert werden können. Darüber hinaus scheint es plausibel, dass viele APTs physisch in die Zielsysteme eingeführt werden, also durch geschultes Personal vor Ort.

Bei dieser dritten Form des Cyberkriegs stehen also wieder Verwundbarkeiten in der Infrastruktur im Zentrum, aber auch die eigentliche Schadsoftware, die zu deren Ausnutzung eingesetzt wird. Aufgrund dieser Schadsoftware – und der sich um sie herum verdichteten Wahrheiten – wird wiederum gemäß der cui-bono-Logik auf die Akteure geschlossen, die dahinter stehen. Da hier große Verwundbarkeiten und staatliche Gegner mit ausreichenden Ressourcen und böswilliger Absicht verknüpft werden, kann die zunehmende Versicherheitlichung direkt mit dem Wissen um APTs einhergehen.

4 Der Cyberkrieg jenseits des Diskurses – Schlussbemerkungen

Von Hacktivismus bis APTs, aufsehenerregende Cybervorfälle sind heute an der Tagesordnung und finden zunehmend Beachtung auf höchster politischer Ebene. Wie im vorherigen Abschnitt exemplarisch aufgezeigt, werden dabei sehr unterschiedliche Formen von Cybervorfällen als Cyberkrieg bezeichnet. Die soziopolitischen Prozesse, die dabei zum Tragen kommen, sind nur teilweise gut erschlossen, gehen aber in fast allen Fällen weit über den „Sprechakt“, auf den sich der Sekuritisierungsansatz der Kopenhagener Schule gründet, hinaus. Die Gegenmaßnahmen, die diskutiert und umgesetzt werden, sind dabei äußerst vielschichtig und beinhalten technische, organisatorische, gesetzliche, außenpolitische und klassisch sicherheitspolitische Strategien und Instrumente. Analysen, die nur darauf schauen, wie über den Cyberkrieg „gesprochen“ wird, werden so nie die gesamte Breite der Cybersicherheitspolitik erfassen können.

Dies zeigt deutlich, dass die Forschung nicht nur darauf achten sollte, wer was zum Cyberkrieg sagt – sondern auch darauf, wer was tut und was die Konsequenzen dieser Taten sind. Einige dieser „Taten“ sind klar sichtbar und können mit traditionellen Ansätzen der internationalen Beziehungen erforscht werden. So können wir z.B. beobachten, dass trotz beträchtlicher Unterschiede zwischen herkömmlichen Sicherheitsproblemen und den neueren Herausforderungen der Cybersicherheit Staaten auf traditionelle Werkzeuge der Diplomatie setzen, um den Cyberspace international zu regulieren (Nye 2014). Während des Kalten Krieges entwickelte Instrumente werden verwendet, um politische Interaktion in und durch den Cyberspace zu stabilisieren und gleichzeitig das Eskalationspotential von Cyberkonflikten zu verringern. Der Schwerpunkt liegt auf dem Aufbau von Transparenz und Vertrauen bildenden Maßnahmen im Rahmen der OSZE sowie der Ausgestaltung von völkerrechtlichen Normen für kriegerische Auseinandersetzung im Cyberspace (Dunn Cavelty 2015). Wie und warum sich

welche Normen herausbilden und wer dabei welche Rolle spielt, bietet sich als Forschungsfrage regelrecht an; mittlerweile ist auch genügend Material vorhanden, um diese Normen-, vielleicht sogar eine internationale Regimebildung auch empirisch zu untersuchen.

Andere Praktiken sind weitaus schwieriger zu erforschen. Dazu gehören vorneweg geplante und bereits umgesetzte Konzepte der (operativen) Kriegsführung in und durch den Cyberspace. Während gewisse Grundideen in öffentlich zugänglichen Dokumenten abgebildet sind (z.B. in der im April 2015 veröffentlichten DoD Cyber Strategy), sind andere Sicherheitspraktiken nur über indirekte Zugänge erforschbar, auch wenn sie potentiell diejenigen sind, die einen direkten Einfluss auf die materielle Unsicherheit haben.

Es gibt viele Hinweise darauf, dass die rasante Entwicklung von militärischen und geheimdienstlichen Cyberkapazitäten gegenwärtig stärker wächst als das zivile Verständnis und die Möglichkeiten zu ihrer Kontrolle. Während Nachrichtendienste oft das Budget wie auch die nötigen technologischen Ressourcen besitzen, um auf Cyberbedrohungen reagieren zu können, löst ihre Rolle nicht erst seit Edward Snowdens Enthüllungen öffentliches Unbehagen aus. Solches Unbehagen ist nicht unbegründet: Im Namen der nationalen Sicherheit führen Praktiken dieser Akteure nämlich zu weniger Cybersicherheit – und so auch zu weniger Sicherheit für das Individuum. Das heimliche Einschleusen von Schadsoftware für Spionagezwecke in den Wirkungskreis von Nachrichtendiensten, aber auch bei Akteuren aus der Industrie hat bisher keinen sichtbar positiven Einfluss. Vielmehr scheint es so, als ob die nachrichtendienstliche Ausnutzung von Schwachstellen im Cyberbereich (z.B. durch APTs) jene Stabilität untergräbt, die durch die einsetzende internationale Normenbildung eigentlich erst noch erreicht werden soll. Absichtlich offen gehaltene Schwachstellen im globalen Cyberspace reduzieren die Sicherheit des gesamten Systems – für jedermann. Der strategisch nutzbare virtuelle Raum voller Schwachstellen und der sichere, robuste Cyberspace schließen sich gegenseitig aus. Darüber hinaus ist es äußerst besorgniserregend, wie leicht die gegenwärtig stattfindende Untergrabung der Freiheitsrechte (inkl. Privatsphäre) im Namen der Sicherheit zu rechtfertigen ist, ohne dass der Nutzen der Untergrabung nachgewiesen werden muss.

Die politikwissenschaftliche Cybersicherheitsforschung hat sich bisher vor allem mit Versicherheitlichungsprozessen durch Sprechakte befasst. Solche Analysen zeigen deutlich, welcher Stellenwert Cybergefahren im sicherheitspolitischen Prozess zukommt. Was diese Analysen aber nicht zeigen können, sind bereits existierende Praktiken, die Grund für, aber auch Konsequenz von solchen politischen Prozessen sind. Die hier entwickelte Perspektive soll es hingegen möglich machen, diese konkreten, bereits existierenden Auswirkungen auf die Sicherheit des gesamten Cyberspace in den Blick zu nehmen.

Literatur

Amoore, Louise / De Goede, Marieke (2005): Governance, Risk and Dataveillance in the War on Terror, in: Crime, Law and Social Change 43:2–3, 149–173.

Anderson, Ross (2001): Why Information Security is Hard – An Economic Perspective, in: IEEE Computer Society (Hrsg.): Proceedings of the 17th Annual Computer Security Applications Conference, IEEE Computer Society: Washington D.C., 358–365.

Aradau, Claudia / van Munster, Rens (2007): Governing Terrorism through Risk: Taking Precautions, (un)Knowing the Future, in: European Journal of International Relations 13:1, 89–115.

Balzacq, Thierry (2005): The Three Faces of Securitization: Political Agency, Audience and Context, in: European Journal of International Relations 11:2, 171–201.

Balzacq, Thierry (2008): The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policies, in: Journal of Common Market Studies 46:1, 75–100.

Barlow, John Perry (1996): A Declaration of the Independence of Cyberspace, https://homes.eff.org/~barlow/Declaration-Final.html (07.07.2015).

Bendrath, Ralf (2001): The Cyberwar Debate. Perception and Politics in US Critical Infrastructure Protection, in: Information & Security: An International Journal 7, 80–103.

Bendrath, Ralf (2003): The American Cyber-Angst and the Real World – Any Link?, in: Latham, Robert (Hrsg.): Bombs and Bandwidth: The Emerging Relationship between IT and Security, The New Press: New York, 49–73.

Beuth, Patrick (2015): Hackerangriff im Bundestag, in: Zeit Online, 12. Juni 2015, http://www.zeit.de/digital/datenschutz/2015-06/bundestag-hack-karlsruher-firma-aufklaerung (07.07.2015).

Bewarder, Manuel / Clauß, Ulrich (2015): Verfassungsschutz verfolgt Spur nach Russland, in: Die Welt, 11.06.2015, http://www.welt.de/politik/deutschland/article142372328/Verfassungsschutz-verfolgt-Spur-nach-Russland.html (07.07.2015).

Böhme, Rainer (2005): Vulnerability Markets – What is the economic value of a zero-day exploit? Paper given at the 2005 Chaos Communication Congress Berlin, Germany, https://events.ccc.de/congress/2005/fahrplan/attachments/542-Boehme2005_22C3_VulnerabilityMarkets.pdf (07.07.2015).

Brito, Jerry / Watkins, Tate (2011): Loving the Cyber Bomb? The Dangers of Threat Inflation, in: Cybersecurity Policy, Mercatus Center George Mason University, Working Paper No. 11–24.

Bundesministerium des Innern (2009): Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), http://www.bmi.bund.de/cae/servlet/contentblob/544770/publicationFile/27031/kritis.pdf (03.08.2015).

Buzan, Barry / Wæver, Ole / de Wilde, Jaap (1998): Security: A New Framework for Analysis, Lynne Rienner: Boulder.

Collier, Stephen / Lakoff, Andrew (2008): The Vulnerability of Vital Systems: How Critical Infrastructure Became a Security Problem, in: Dunn Cavelty, Myriam / Kristensen, Kristian Søby (Hrsg.): The Politics of Securing the Homeland: Critical Infrastructure, Risk and Securitization, Routledge: London, 17–39.

Corry, Olaf (2012): 'Securitisation' and 'Riskification': Second-order Security and the Politics of Climate Change, in: Millennium – Journal of International Studies 40:2, 235–258.

Deibert, Robert / Rohozinski, Rafal (2010): Risking Security: Policies and Paradoxes of Cyberspace Security, in: International Political Sociology 4, 15–32.

Deibert, Ronald (2013): Black Code: Surveillance, Privacy and the Dark Side of the Internet, Random House: New York.

Deibert, Ronald / Palfrey, John G. / Rohozinski, Rafal / Zittrain, Jonathan (2008) (Hrsg.): Access Denied: The Practice and Policy of Global Internet Filtering, MIT Press. Cambridge.

Deibert, Ronald / Palfrey, John G. / Rohozinski, Rafal / Zittrain, Jonathan (2010) (Hrsg.): Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace, MIT Press: Cambridge.

Deibert, Ronald / Rohozinski, Rafal (2011): The New Cyber Military-Industrial Complex. The Globe and Mail, March 28, in: http://www.theglobeandmail.com/news/opinions/opinion/the-new-cyber-military-industrial-complex/article1957159/ (04.12.2012).

Dunn Cavelty, Myriam (2010): Cyber-security, in: Burgess, Peter (Hrsg.): The Routledge Companion to New Security Studies, Routledge: London, 154–162.

Dunn Cavelty, Myriam (2012): The Militarisation of Cyberspace. Why Less May Be Better, in: Czosseck, Christian / Ottis, Rain / Ziolkowski, Katharina (Hrsg.): Proceedings of the 4th International Conference on Cyber Conflict, Tallinn, 141–153.

Dunn Cavelty, Myriam (2013a): Der Cyber-Krieg der (so) nicht kommt – Erzählte Katastrophen als (Nicht)Wissenspraxis, in: Hempel, Leon / Bartels, Marie (Hrsg.): Aufbruch ins Unversicherbare – Zum Katastrophendiskurs der Gegenwart, Transcript Verlag: Bielefeld.

Dunn Cavelty, Myriam (2013b): From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse, in: International Studies Review 15:1, 105–122.

Dunn Cavelty, Myriam / Kristensen, Kristian Søby (2008): Introduction: Securing the Homeland – Critical Infrastructure, Risk, and (In)Security, in Dunn Cavelty, Myriam / Kristensen, Kristian Søby (Hrsg.): The Politics of Securing the Homeland: Critical Infrastructure, Risk and Securitisation, London: Routledge, 1–14.

Dunn Cavelty, Myriam / Jaeger, Mark Daniel (2015): (In)visible Ghosts in the Machine and the Powers that Bind: The Relational Securitization of Anonymous, in: International Political Sociology 9:2, 176–195.

Foucault, Michel (2005): Analytik der Macht, Suhrkamp: Frankfurt am Main.

Frei, Stefan (2013): The Known Unknowns. Empirical Analysis of Publicly Unknown Security Vulnerabilities, https://www.nsslabs.com/reports/known-unknowns-0 (07.07.2015).

Fund, Brian (2013): The NSA hacks other countries by buying millions of dollars' worth of computer vulnerabilities, The Washington Post, 31 August 2013, https://www.washingtonpost.com/news/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities/ (07.07.2015).

Gartzke, Eric (2013): The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth, in: International Security 38:2, 41–73.

Gaycken, Sandro (2011): Cyberwar: Das Internet als Kriegsschauplatz, München.

Gebauer, Matthias / Meiritz, Annett / Stöcker, Christian (2015): Cyberangriff auf Parlament: IT-Spezialisten können Bundestagstrojaner nicht stoppen, Spiegel Online, 21.05.2015, http://www.spiegel.de/netzwelt/netzpolitik/bundestag-experten-koennen-trojaner-nicht-stoppen-a-1035006.html 07.07.2015).

Haacke, Jürgen / Williams, Paul D. (2008): Regional Arrangements, Securitization, and Transnational Security Challenges: the African Union and the Association of Southeast Asian Nations Compared, in: Security Studies 17:4, 775–809.

Hansen, Lene / Nissenbaum, Helen (2009): Digital Disaster, Cyber Security, and the Copenhagen School, in: International Studies Quarterly 53, 1155–1175.

Huysmans, Jef (2011): What's in An Act? On Security Speech Acts and Little Security Nothings, in: Security Dialogue 42:4–5, 371–383.

Jackson Higgins, Kelly (2013): 'Project SHINE' Illuminates Sad State Of SCADA/ICS Security on the Net, Information Week, 16 October 2013. http://www.darkreading.com/vulnerabilities---threats/project-shine-illuminates-sad-state-of-scada-ics-security-on-the-net/d/d-id/1140691 (07.07.2015).

Jackson, Nicole J. (2006): International Organizations, Security Dichotomies and the Trafficking of Persons and Narcotics in Post-Soviet Central Asia: A Critique of the Securitization Framework, in: Security Dialogue 37:3, 299–317.

Lawson, Sean (2011): Beyond Cyber-doom. Cyberattack Scenarios and the Evidence of History, in: Mercatus Center George Mason University Working Paper, No 11–01.

Lemke, Thomas / Krasmann, Susanne / Bröckling, Ulrich (2000): Gouvernementalität. Neoliberalismus und Selbsttechnologien. Eine Einleitung, in: Lemke, Thomas / Krasmann, Susanne / Bröckling, Ulrich (Hrsg.): Gouvernementalität der Gegenwart: Studien zur Ökonomisierung des Sozialen, Suhrkamp: Frankfurt am Main, 7–40.

Léonard, Sarah / Kaunert, Christian (2011): Reconceptualizing the Audience in Securitization Theory, in: Balzacq, Thierry (Hrsg.): Securitization Theory. How Security Problems Emerge and Dissolve, Routledge: London, 57–76.

Libicki, Martin (2000): The Future of Information Security, Institute for National Strategic Studies: Washington.

Libicki, Martin (2009): Cyberdeterrence and Cyberwar, RAND Corporation: Santa Monica.

Maillart, Thomas / Sornette, Didier (2010): Heavy-Tailed Distribution of Cyber-Risks, in: The European Physical Journal B, 75:3, 357–364.

McDonald, Matt (2008): Securitization and the Construction of Security, in: European Journal of International Relations 14:4, 563–587.
Meinrath, Sascha D. / Losey, Hames / Pickard, Victor (2011): Digital Feudalism: Enclosures and Erasures from Digital Rights Management to the Digital Divide, in: The CommLaw Conspectus: Journal of Communications Law and Policy 19:2, http://scholarship.law.edu/commlaw/vol19/iss2/6/ (07.07.2015).
Miller, C. (2007): The legitimate vulnerability market: the secretive world of 0-day exploit sales. In 6th Workshop on the Economics of Information Security (WEIS 2007), http://www.econinfosec.org/archive/weis2007/papers/29.pdf (07.07.2015).
Neal, Andrew W. (2009): Securitization and Risk at the EU Border: The Origins of FRONTEX, in: Journal of Common Market Studies 47:2, 333–356.
Nye, Joseph (2011): Nuclear Lessons for Cyber Security? in: Strategic Studies Quarterly 5:4, 18–38.
Nye, Joseph (2014): The Regime Complex for Managing Global Cyber Activities. Global Commission on Internet Governance, http://dash.harvard.edu/bitstream/handle/1/12308565/NyeGlobalCommission.pdf?sequence=1 (07.07.2015).
Perlroth, Nicole / Sanger, David E. (2013): Nations Buying as Hackers Sell Flaws in Computer Code. New York Times, 13 July 203, http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html?partner=rss&emc=rss&smid=tw-nytimes&_r=1& (07.07.2015).
Peterson, Karen Lund (2012): Risk Analysis – a Field within Security Studies?, in: European Journal of International Relations 18:4, 693–717.
Rathmell, Andrew (2001): Controlling Computer Network Operations, in: Information & Security: An International Journal 7, 121–144.
Rid, Thomas (2011): Cyberwar Will Not Take Place, in: Journal of Strategic Studies 33:5, 727–758.
Rid, Thomas / Buchanan, Ben (2015): Attributing Cyber Attacks, in: Journal of Strategic Studies, 38:1–2, 4–37.
Rosenau, James (1998): Global Affairs in an Epochal Transformation, in: Henry, C. Ryan / Peartree, Edward C. (Hrsg.): Information Revolution and International Security, Center for Strategic and International Studies Press: Washington D.C., 33–57.
Salter, Mark B. (2008): Securitization and Desecuritization: A Dramaturgical Analysis of the Canadian Air Transport Security Authority, in: Journal of International Relations and Development 11:4, 321–349.
Schatzki, Theodore R. / Knorr, Cetina Karin / von Savigny, Eike (2001): The Practice Turn in Contemporary Theory, Routledge: London.
Schneier, Bruce (2012): When It Comes to Security, We're Back to Feudalism. Wired, http://www.wired.com/2012/11/feudal-security/ (07.07.2015).
Schneier, Bruce (2013): The Battle for Power on the Internet. The Atlantic, http://www.theatlantic.com/technology/archive/2013/10/the-battle-for-power-on-the-internet/280824/ (07.07.2015).
Sommer, Peter / Brown, Ian (2011): Reducing Systemic Cyber Security Risk. Report of the OECD's International Futures Project, IFP/WKP/FGS(2011)3: Paris.
Waltz, E. (1998): Information Warfare: Principles and Operations, Artech House: Boston.
Warner, M. (2012): Cybersecurity: A Pre-History, in: Intelligence & National Security 27:5, 781–799.

Autorin

Dr. Myriam Dunn Cavelty
Dozentin für Schweizerische und Internationale Sicherheitspolitik
Departement Geistes-, Sozial- und Staatswissenschaften
Eidgenössische Technische Hochschule Zürich
Haldeneggsteig 4
CH-8092 Zürich
dunn@sipo.gess.ethz.ch

DOI: 10.11588/josar.2015.0.23486

Wer regiert das Internet? – Sechs Thesen und einige Tendenzen

Sebastian Harnisch und Wolf J. Schünemann

1 Einleitung

„Wer regiert das Internet?“ ist nur auf den ersten Blick eine einfache Frage, denn sie wirft eine Vielzahl weiterführender Fragen auf, die in die verschiedenen Winkel des Makrokosmos (Kleinwächter 2015) der Internetregulierung verweisen. Welchen Regeln und Strukturen sind Netzarchitektur und -nutzung unterworfen? Stoßen Nationalstaaten im Umgang mit der virtuellen Welt an die Grenzen ihrer Steuerungskapazitäten? Welche Rolle spielen internationale Regime und Organisationen, inklusive NGOs, bei der Regulierung des virtuellen Raums? Welche Macht besitzen transnationale Unternehmen? Wie wirkt das Nutzerverhalten auf Strukturen und Möglichkeiten der Netzregulierung? In welchem Verhältnis stehen die Anstrengungen der Governance-Akteure zur Selbstbestimmung digitaler Bürger auf der individuellen Ebene? Diese und weitere Fragen markieren die gesellschaftspolitischen Herausforderungen des digitalen Wandels. Sie sind in den vorangegangenen Beiträgen ausführlicher behandelt worden.

Diese Bilanz hat sich die Aufgabe gestellt, die behandelten Themen, Fragen und die gegebenen Antworten sowie die verschiedenen Forschungsstränge wieder zusammenzuführen. Dies wird nur teilweise gelingen. Zu groß ist die Fülle und Bandbreite der vorgestellten Überlegungen und Ansätze. Dennoch unternehmen wir einen beherzten Versuch, indem wir sechs Thesen zur Netzpolitik vorstellen, die die in diesem Band ausgelegten Fäden aufgreifen, zusammenführen, eigene Überlegungen einführen und zuspitzende Aussagen formulieren. Der Beitrag gliedert sich nach den Thesen in sechs thematische Abschnitte, denen die titelgebende These jeweils vorangestellt ist, sowie eine Konklusion.

2 Die verzögerte Politisierung des Netzes (These 1)

> Das Internet entzieht sich als politischer Raum in seiner jetzigen dynamischen Entwicklungsphase der politischen und rechtlichen Regulierung: Akteursinteressen bilden sich noch heraus, Koalitionen werden erst geschmiedet. Zudem greifen beschränkte Regulation und die Konstitution des entstehenden Politikfelds ineinander, sodass sich (bis auf weiteres) konfliktäre Wechselbeziehungen mit der analogen Welt ergeben.

Die erste These bezieht sich direkt auf unsere übergeordnete Fragestellung: „Wer regiert das Internet?“ Auf der einen Seite gibt sie eine abschlägige Antwort. Auf der anderen Seite weicht sie der Frage aber auch aus, indem sie nicht auf das Wer antwortet, sondern das Ob in den Fokus rückt: Kann das Internet überhaupt regiert werden? –

Nein, nicht wirklich oder nicht so, wie wir es gewohnt sind. Betrachten wir die vorangegangenen Beiträge, so fällt auf, dass sich in keiner dieser Annäherungen ein klares, unproblematisches und realistisches Angebot für einen Regenten oder besser: Regulierer des Internets findet. Markus Beckedahl (in diesem Band) liefert zwar einen umfassenden Überblick über jene netzpolitisch relevanten Politikfelder, die eine politische Gestaltung und Regulierung dringend erforderlich machen. Die Frage danach, wer diese Regulierungsanstrengungen anstoßen und effektiv durchsetzen kann, beantwortet er aber nicht. Auf den internationalen Umgang mit den kritischen Ressourcen der Technologie gerichtet, stellt Jeanette Hofmann (in diesem Band) das Internet explizit als einen schwer regierbaren Raum dar, als *Moving Target* und fluiden Gegenstand. Deshalb müssten sich die Bemühungen einer internationalen Internet Governance notwendig als eine Art „Suchprozess" ausnehmen (siehe auch Hofmann 2005: 26–27). In jüngeren Arbeiten spricht sie in diesem Zusammenhang auch vom Modus „reflexiver Koordination", durch den sich die Governance in diesem Feld auszeichne (Hofmann et al. 2014).

In Milton Muellers Beitrag zur territorialstaatlichen Souveränität im Internet wird deutlich, dass von den Nationalstaaten als klassischen Regulierungsinstanzen und Machtakteuren internationaler Politik keine Gestaltungsmacht und Strukturierungsleistung zu erwarten ist, die mit der bislang entwickelten Architektur des Internets vereinbar wäre. Während Mueller seine Hoffnung in eine neue Form postterritorialer Volkssouveränität legt, macht der Beitrag von Marianne Kneuer (in diesem Band) zumindest für den nationalen Raum die große Lücke zwischen Anspruch und Wirklichkeit im Hinblick auf Online-Beteiligungen von Bürgern sichtbar. Sie vertritt eine empirisch gesättigte skeptische Perspektive auf das Wechselverhältnis von Demokratie und Internet (Kneuer 2013a; Kneuer 2013b; siehe auch den folgenden Abschnitt).

Angesichts des Befundes, dass es offensichtlich keine klare Regulierungsinstanz für das Internet gibt und sich die Etablierung einer Volkssouveränität im Netz schwierig gestaltet, stellt sich die Frage, welche Kräfte dafür sorgen, dass sich noch keine spezifischen Strukturen der politischen Steuerung im und für das Netz herausgebildet haben. Aus unserer Sicht geschieht dies vornehmlich aus zwei Gründen: Zum einen befindet sich das Internet im Hinblick auf seine gesellschaftspolitische Ausgestaltung nach wir vor im Werden: Konstitutive Fragen und Herausforderungen stehen immer noch im Vordergrund der netzpolitischen Debatte. Die ständige Neuerfindung und Erweiterung des Netzes erschwert eine Verstetigung und Verfestigung von Akteurskoalitionen mit festen Präferenzen, die danach streben, institutionelle Strukturen zu ihrem eigenen Vorteil auf Dauer zu stellen. Vielmehr greifen netzpolitisch aktive Akteure auf bestehende institutionelle Arrangements aus der Offline-Welt zurück, um aufwändige Aushandlungsprozesse zu vermeiden und erwartbare Verteilungseffekte bestehender Institutionen zu realisieren.

Zum anderen muss konstatiert werden, dass der Netznutzer vornehmlich als Konsument, interessiert an Informationen und Kontakten, teils auch als Produzent, u.U. als

Krimineller in das Netz eintritt. Eindrücklich wird dies bestätigt in den Beiträgen von Reimer, Cornelius sowie den Analysen von Beckedahl und Kneuer, welche den katalytischen Effekt des Netzes für mehr oder minder legale Steuersparmodelle, die schwache Nutzung von deliberativen Instrumenten in den Bereichen E-Government (Bürgerhaushalte) und E-Participation (Organisation anstatt Deliberation) betonten. Der Netz-Citoyen, der Internet-Bürger, der Mitsprache und Mitgestaltungsrechte geltend macht und der aktiv den netzpolitischen Raum gestalten will, bleibt trotz aller Appelle der netzpolitisch aktiven Gemeinschaft eine seltene Spezies in der stetig wachsenden Internetpopulation.

Dass sich dieser aus demokratietheoretischer Sicht beklagenswerte Zustand schnell ändern kann, zeigen die Offenlegungen Edward Snowdens und anderer Whistleblower. Sie haben nicht nur große Aufmerksamkeit in den Vorträgen der Ringvorlesung erregt (vgl. bspw. die Veranstaltungen mit William Binney und Kai Cornelius) und zum Teil erbitterte Kritik an den Überwachungspraktiken der National Security Agency (NSA) hervorgerufen. Sie haben auch eine breitere gesellschaftliche Debatte über die Risiken staatlicher Überwachung und insbesondere US-amerikanischer Ausspähpraktiken ausgelöst. So wurde in der Diskussion mit Michael Froomkin deutlich, dass die großen US-amerikanischen Internet-Service-Provider aufgrund massiver Umsatzverluste im Zuge der Snowden-Veröffentlichungen, die US-Exekutive zur Mäßigung aufgerufen haben, weil sie ihre Geschäftsmodelle in Gefahr gebracht sehen, insofern sie nicht als Dienstleister für ihre Kunden sondern als Helfershelfer einer ungeregelt spionierenden Regierung angesehen würden. Ob die aktuell bereits schwächelnde Aufmerksamkeit und Empörung aber in eine nachhaltige Politisierung des Internets übergeht, ist sehr zu bezweifeln.

3 Das Netz wirkt nicht (nur) demokratisierend (These 2)

> Es gibt keine gerichtete Beziehung zwischen Internetnutzung und der Entwicklung politischer Regime: (a) Durch das Internet können autokratische Regime ebenso gestützt wie gestürzt werden; (b) die Bürger regieren das Internet nicht, sie konstituieren es mehr als Marktbürger denn als digitale Citoyens, sodass die Kommerzialisierung vieler Lebensbereiche, nicht aber die Demokratisierung der Gesellschaft die Folge ist; (c) der Netizen ist demografisch, funktional und situativ sehr speziell und repräsentiert nur einen kleinen Teil der realen Gesellschaften (digital divide); (d) das Netz funktioniert primär als Katalysator von Protestbewegungen, als Medium für kurzfristige Mobilisierung und in einigen Ausnahmefällen als Vetospieler; e) andere politische Prozesse (Deliberation oder Repräsentation) werden bisher nicht effektiv im Netz umgesetzt.

Unsere These zur Demokratieentwicklung kommt als ein Bündel von Annahmen daher, die unterschiedliche Aspekte und Bezugspunkte des Verhältnisses von Internet und Herrschaftstypus berühren. Insbesondere die frühe Internetforschung zeichnete sich durch utopische Annahmen eines direkten und positiven Zusammenhangs von Internet und Demokratisierung aus (Ferdinand 2000; Negroponte 1995; Rheingold 1994), indem das Netz zuallererst als „Web of the Free“ charakterisiert wurde (Shiffrin et al. 2005). Diese fortschrittsoptimistischen Visionen wurden zwar immer wieder grundlegend in

Frage gestellt (Hindman 2009; Kneuer 2013a; Morozov 2011), doch in Form des Mitmach-Netzes (Web 2.0: Bruns 2009; Reynolds 2006; Shirky 2008) oder Katalysators vermeintlicher „Twitter-“ und „Facebook-Revolutionen“ hat diese unhaltbare These auch noch in jüngerer Zeit sichtbare Aktualisierungen erfahren (Shirky 2011; Diamond 2012; Howard et al. 2011).

In Abgrenzung zu dieser fortschrittsoptimistischen Position argumentieren wir auf der Grundlage der Beiträge in diesem Band, dass es bislang keinen klaren Nachweis für einen gerichteten Zusammenhang zwischen Internetnutzung und Demokratie oder – allgemeiner gesprochen – politischer Regimebildung, politischer Performanz oder der Persistenz von politischen Regimen gibt. Wir führen diese zentrale Annahme auf fünf Beobachtungen zurück:

Zum Ersten (a) stellt sich die Frage, welche Effekte die Internetnutzung auf die Stabilität von Autokratien und Demokratien, auf ihre Performanz und Persistenz hat. Die Antwort ist uneinheitlich. Durch das Internet können autokratische Regime ebenso gestützt wie gestürzt werden (Schünemann 2012: 29). Es lassen sich zwar Indizien dafür finden, dass Internettechnologien und die dadurch ermöglichte Online-Kommunikation autokratische Regime unter Druck setzen können, z.B. durch die internetgestützte Organisation von Massenbewegungen. Nicht zuletzt die großen Anstrengungen autokratischer Regime, das Internet zu kontrollieren, deuten auf eine entsprechende, tief verwurzelte Sorge hin. Mit Blick auf die Volksrepublik China lässt sich aber auch feststellen, dass autokratische Regime ebenso von der Internetentwicklung profitieren können (vgl. die Beiträge von Kneuer und Froomkin), autokratische Regime das Netz für sich nutzen können und die Technologie somit auch systemstabilisierende Wirkung entfalten kann (für weiterführende Informationen siehe Greitens 2013; Morozov 2011; Stier 2015).

Unser zweiter Befund (b) sollte nicht als reflexhafte Kulturkritik missverstanden werden. Er knüpft vielmehr an die Beobachtungen des Netzpolitikers Markus Beckedahl an, woraus dieser einen wohlbegründeten Appell zum politischen Engagement für die Gestaltung des Internets ableitet. In der Tat ist grundlegend und abstrakt die Frage zu stellen, welche Art von Bürger wir im Netz vorfinden? Wie verhalten sich Menschen im Netz? Aktuell, so scheint es, wird das Internet vornehmlich von Markt- oder Wirtschaftsbürgern bevölkert. Dieser Bürger- oder Nutzertyp prägt das Netz als Produzent von Inhalten und in jedem Fall von Daten (siehe den folgenden Abschnitt; auch Froomkin in diesem Band) sowie Konsument von Informationen und Waren. Dabei wird der so genannte ‚produser‘ oder ‚Prosument‘ durch seine Geschäftigkeit im Netz selbst zum Datengeschäft. Demgegenüber ist der digitale Citoyen, der als Staatsbürger agiert und aktiv für seine Freiheits- und bürgerlichen Rechte eintritt, allenfalls als Heranwachsender im Netz erkennbar. Diese Identitätsfindungsphase von Netizens geht auch mit einer beschränkten Fähigkeit zur Bildung von persistenten Gruppen einher. Netizens treten den gesellschaftlichen Systemen von Markt und Staat in der Regel als einzelne Nutzer gegenüber. Sie beteiligen sich selektiv und interessenbasiert. Die

Ubiquität und Spontaneität vieler Internetangebote überhöhen und verstärken die individuellen Bedürfnisse des Einzelnen. Soziale Netzwerke können den individuellen Geltungsdrang schüren, sodass das Kollektiv als Publikum nicht aber als Handlungsarena wahrgenommen wird.

Der Nutzer als Prosument verkehrt auf diese Weise die Demokratisierungslogik der Internetoptimisten in ihr Gegenteil: Konsum und Selbstentäußerung gehen häufiger – aber nicht immer – mit Individualisierung und Entpolitisierung einher. Dass die bewusste Abwendung von als problematisch erkannten Angeboten – etwa im Hinblick auf den Datenschutz – kaum gelingt, hat mit der starken Sogwirkung der Netzwerkeffekte zu tun. Nirgendwo wird dies so deutlich wie im Bereich der sozialen Netzwerke (vgl. Lanier 2014). Wer wagt es noch, etwa aus Gründen des Datenschutzes ein soziales Netzwerk wie Facebook zu verlassen, wenn er im gleichen Moment die Vernetzung mit einer Vielzahl seiner ‚Freunde', wenn er deren ‚digitale Anerkennung' aufgeben muss? Welches kleine oder mittlere Unternehmen kann es sich leisten, die Angebote des Internetkaufhauses Amazon auszuschlagen, wenn es die wachsenden Marktanteile des E-Commerce damit faktisch weitgehend abschreiben muss?

Unsere dritte Teilthese (c) betrifft die soziale Schichtung der Internetnutzung. Sie ist von den Anfängen der digitalen Ära bis heute als sog. digital divide sichtbar. Empirische Befunde zeigen deutlich, dass Netizens und Onliner – d.h. besonders kompetente und aktive Bürger des Netzes – in demografischer Hinsicht sehr spezielle Typen sind. Im Regelfall ist der Onliner jung, männlich, gut gebildet und wohlsituiert. Er lebt eher in der Stadt als auf dem Land. Tatsächlich nutzten 2014, laut dem aktuellen Digital-Index der Initiative D21 (2014), zwar 76,8 Prozent der Deutschen das Internet – also immer noch etwa ein Viertel der Bevölkerung nicht –, aber nur knapp 60 Prozent taten dies über schnelle Breitbandverbindungen. Diese Studie weist aus, dass 81,8 Prozent der befragten Männer zu den kompetenten Internetnutzern gehören, also jenen, die mit verschiedenen Anwendungen über E-Mail, Informationssuche und Online-Shopping hinaus umzugehen wissen. Im Unterschied dazu gehören nur 71,9 Prozent der Frauen zu dieser Gruppe. Unter den 20- bis 29-Jährigen gaben 98,1 Prozent an, zu den Onlinern zu gehören, unter den 60- bis 69-Jährigen waren es hingegen nur 64,5 Prozent. Eine besonders deutliche Kluft ergibt sich mit Blick auf die sozioökonomische Schichtung. Die Befragten mit einem Haushaltseinkommen unter 1000 Euro ließen sich zu 54,1 Prozent als Onliner einstufen, bei denjenigen mit einem Einkommen von über 3000 Euro waren es hingegen 93,7 Prozent.

Der Netizen ist nicht nur soziodemografisch besonders, er ist auch funktional und situativ sehr speziell. Bis heute scheint sich die aufklärerische Dualität von Citoyen und Bourgeois noch nicht voll entfaltet und sicher nicht auf die gesamte Nutzerpopulation übertragen zu haben. Zumindest ist aber kein „digitaler Strukturwandel der Öffentlichkeit" (Bieber 2002) erkennbar geworden, der identifizierbare Demokratisierungseffekte gezeitigt hätte (siehe den Beitrag von Kneuer in diesem Band).

Welchen demokratisierenden Effekt hat das Netz aber, wenn überhaupt, auf seine

Nutzer, die Gesellschaften der Welt und die Weltgesellschaft? Aus der Perspektive der empirischen politikwissenschaftlichen Forschung zeigen sich bisher allenfalls Beschleunigungseffekte auf die politische Protestkultur, verbunden mit redistributiven Effekten in Krisensituationen. Über die Internetkommunikation erreichen politischer Protest und Erregung rascher eine breite öffentliche Aufmerksamkeit und gewinnen dadurch womöglich an Intensität, sodass der Entscheidungsdruck auf die politischen Akteure wachsen kann. So wird möglich, dass die politische Online-Kommunikation (d) tatsächlich als eine Art Katalysator von Protestbewegungen, als Medium für kurzfristige Mobilisierung verstanden werden und in Ausnahmefällen auch einen Supervetospieler konstituieren kann (siehe das Beispiel ACTA: Matthews et al. 2013; vgl. auch Kneuer in diesem Band).

In der Online-Kommunikation sind die Themenkonjunkturen allerdings merklich kurzatmiger geworden, sodass Protestbewegungen – aber auch internetorientierte Parteien und andere längerfristige, institutionalisierte Organisationsformen – bislang keine nachhaltige Bindungskraft haben entfalten können. So dient das Internet bisher kaum als wirksames Medium in politischen Konflikt- oder Deliberationsprozessen. Jüngere Forschungsarbeiten zeigen auf, dass nicht nur der erhoffte demokratisierende Strukturwandel der Öffentlichkeit im Sinne von Shirkys Diktum: „Here comes everybody“ (Shirky 2008) ausbleibt; es sind auch nur bedingt transnationale Vergesellschaftungsprozesse nachweisbar (Schünemann et al. 2016, i.E.).

In den vorangegangenen Beiträgen ist zuletzt (e) deutlich geworden, dass die hoffnungsvoll erwarteten direkt(er)demokratischen Politikformate in Form neuartiger Partizipations- und Repräsentationsverfahren in den meisten Fällen nicht effektiv umgesetzt werden, wie etwa Studien über verschiedene Bürgerhaushalte und andere Aktivitäten zeigen (vgl. insbesondere den Beitrag von Kneuer). So kommt es auf den beiden Seiten des Angebots und der Nachfrage politischer Beteiligung zu einer Art von Scheinpartizipation. Dies betrifft online verfügbare Beteiligungsangebote, die keinerlei nachweisbare Wirkung entfalten, weil die tatsächlichen Entscheidungsprozesse nicht hinreichend mit den neuen Verfahren verzahnt sind. Dies belegen auch die sehr niedrigen Beteiligungsquoten bei Partizipationsverfahren, weil die Nachfrage nach Online-Mitsprache und -Mitwirkung höher eingeschätzt wird, als sie sich tatsächlich niederschlägt. Wenige ernsthafte Angebote gehen also häufig mit einer geringen und einseitigen Nutzung einher, so dass „Internet-gestützte Beteiligungsfassaden“ entstehen können (im Sinne der „simulativen Demokratie“: Sarcinelli 2014; siehe auch Sarcinelli 2012). Demgegenüber kann mit Kneuer (in diesem Band) festgestellt werden, dass Deliberation und offener Argumentationsaustausch im Netz nur sehr eingeschränkt stattfinden. Insofern fällt das Internet als Medium der politischen Willensbildung zwar keineswegs aus. Ein direkter oder indirekter Demokratisierungseffekt – wie von den Fortschrittsoptimisten erhofft – ist aber eindeutig nicht nachweisbar.

4 Vom Datenschutz zur Sicherung der Privatsphäre (These 3)

> Die Virtualisierung (insbes. die Diffusion und Vorhaltung) von Kommunikation führt dazu, dass Privatheit nicht mehr allein durch Individuen definiert und hergestellt werden kann; vielmehr muss sie zunehmend durch Dritte (oft Firmen) abgesichert werden, um virtuelle Privatheit herzustellen. So wird das Grundrecht auf Privatsphäre im Offline-Raum zum kommodifizierbaren Bedürfnis im virtuellen Raum.

Die dritte These greift die Rollendifferenzierung zwischen Bourgeois und Citoyen im virtuellen Raum auf und vermisst ihre Bedeutung für den liberalen Schutzraum des Privaten. Abstrakt lässt sich die Leitfrage wie folgt formulieren: Welche Effekte hat das Netz auf die bürgerlichen Grundrechte, im deutschen Kontext auf die „informationelle Selbstbestimmung“ des Bürgers (BVerfGE 65,1; zur politischen Genese siehe auch Busch et al. 2011)?

Ausgangspunkt unserer Argumentation ist die Feststellung u.a. Michael Froomkins, dass die Digitalisierung und Virtualisierung von Kommunikation, verstärkt durch die zunehmende Nutzung sozialer Netzwerke sowie Cloud-Diensten zu einem massiven Verlust der Verfügungshoheit von Individuen über ihre Privatsphäre führen. Zum einen sind die heutigen Nutzungsformen mit der langfristigen Speicherung von Kommunikationsdaten (sowohl Meta- als auch Inhaltsdaten) an ‚Orten‘ und unter Bedingungen, die vom Einzelnen kaum noch durchschaut oder kontrolliert werden können, verbunden. Darin unterscheidet sich der virtuelle Raum vom materiellen Raum. Das international anerkannte Kernbegehren des Privatsphärenschutzes, im eigentlichen Sinn des Wortes, *allein* gelassen zu werden (vgl. Ziemele 2009), lässt sich im materiellen Raum ungleich besser herstellen, als im virtuellen, denn letzterer beruht ja gerade auf Vernetzungsleistungen und -plattformen („intermediaries of our Internet experiences“: Deibert 2013: 36), die sich der Nutzerkontrolle notwendigerweise entziehen.

Zum anderen schafft die Internetnutzung erst die Grundlage für den Rollenwechsel des Nutzers zum Prosumenten, denn er produziert ständig neue Informationen – z. B. Nutzungsprofile – die von Internetunternehmen vermarktet werden können. Wenn aber Informationen und Daten der Nutzer für den Geschäftsprozess eine essentielle Rolle spielen, dann ist klar, dass die Geschäftsinteressen der Datenmakler und Datenverwerter den Schutzinteressen der Bürger entgegenstehen. Die Selbstaufgabe der Privatsphäre ist gewissermaßen Grundbedingung für die Beziehung zwischen dem Internetnutzer und seinem Dienstleister, dem Internetunternehmen. Wie das Beispiel der hilfreichen Smartphone-Apps zur Navigation zeigt, wird der Marktbürger, der nach einem Restaurant sucht, wie selbstverständlich durch den Bezug und die Auswertung von Geolokationsdaten zum Gegenstand, zur Bezugsgröße von Konsum- oder Bewegungsprofilen sowie zum potentiellen Kunden von gezielten Werbeangeboten. Während das Aktivieren oder Verhindern dieser Option in den Bereich des Selbstdatenschutzes (zu Term und Techniken siehe Karaboga et al. 2014; Baumann 2013: 39) fällt, müssen der Schutz personenbezogener Daten und allgemeinverbindliche Datenschutznormen gegenüber Sozialen Netzwerken auf individueller Nutzerebene und kollektiver

politischer Ebene hart erkämpft werden. So muss bei Eintritt in solche Netzwerke jedem Nutzer klar sein, dass die Möglichkeit, in sehr großen Netzwerken zu kommunizieren und daraus große soziale Vernetzungseffekte zu schöpfen mit dem Kontrollverzicht auf Inhalts- (z.B. Bilder) sowie auf Kommunikationsdaten erkauft werden.

Neben starken Unternehmensinteressen führt auch die Entterritorialisierung von Diensten dazu, dass ausländische Anbieter von Internetdiensten oft nur sehr schwer auf die Einhaltung nationaler oder lokaler Standards zu verpflichten sind (vgl. die Beiträge von Cornelius und Reimer in diesem Band). Eine wichtige kollektive Anstrengung ist die intensiv diskutierte Datenschutzgrundverordnung der Europäischen Union, die sich derzeit noch in der Rechtsetzung, konkret in den Trialog-Verhandlungen, befindet. Wesentliche Normentscheidungen des vorgeschlagenen Rechtsetzungspakets, wie das Marktortprinzip, das „Recht auf Vergessenwerden“ oder das Prinzip der Datensparsamkeit deuten darauf hin, dass transnational operierenden Internetunternehmen zum Schutz gesellschaftlicher Datenschutznormen einheitliche Regeln vorgeschrieben werden sollen. Traditionell ist Europa Vorreiterin in den Bereichen des Privatsphären- und Datenschutzes (siehe Froomkin in diesem Band). Kommt es ihrer Vorreiterrolle in der internationalen Normentwicklung auch in diesem Fall nach, dann könnten sich die Handlungsspielräume von Internetunternehmen im europäischen Binnenmarkt bald deutlich verengen.

Gelingt dies jedoch nicht, dann steht zu befürchten, dass das Grundrecht auf Privatsphäre in der digitalen Kommunikation tatsächlich zu einem kommodifizierbaren Bedürfnis, zu einem wirtschaftsfähigen Gut degradiert wird (vgl. den Beitrag von Froomkin in diesem Band; Sevignani 2013). Privatsphäre lässt sich dann eben auch scheibchenweise oder in Paketen veräußern: Ein besonderer Trend sind etwa Fitnessarmbänder, mit denen der eigene Körper und seine Funktionen im Sinne des ‚Quantified Self‘ vermessen werden, etwa wie viele Schritte der Träger zurücklegt, wie lange er schläft, welchen Pulsschlag er zu welchem Zeitpunkt hat. Diese Daten werden in der Regel an ein Online-System des Herstellers übertragen, der die Datenauswertung übernimmt, in die der Kunde wiederum über eine App des Anbieters Einblick hat. Diese Daten aber liegen auf dem Server des Anbieters und sind durch diesen weiter verwertbar. So wird bereits darüber diskutiert, ob Krankenversicherungsunternehmen Zugriff auf solche Datenbestände erhalten sollten, um Versicherten mit nachweislich gesundem Lebenswandel Beitragsrabatte und/oder Prämien einräumen zu können. Mit der Datenweitergabe erhält der Marktbürger also auch neue Möglichkeiten, sein verfügbares Einkommen aufzustocken und ggfs. seine Lebensqualität zu verbessern. Gleichzeitig verliert der Marktbürger aber auch jene privaten Rückzugsräume des politischen Bürgers, dessen Lebenswandel und Weltanschauung frei und unkontrolliert von staatlichen und privaten Kontrollen sind und bleiben müssen.

So nimmt die Fremd- und Selbstkontrolle in einer vernetzten Welt dem Einzelnen die Möglichkeit, Dinge geheim zu halten (und sei es die eigene Identität, siehe Froomkin in diesem Band). Gesellschaftspolitisch kann daraus tatsächlich eine Transparenz-

norm erwachsen, die im Modus einer zunächst unverdächtigen, individualistischen Kombination von Konsum und Lifestyle eine totalitäre Gesellschaftsform entstehen lässt (Baumann 2014). Vor derartigen Tendenzen kann, bei aller Unsicherheit der Prognosen, nur gewarnt werden.

5 Mit Sicherheit unsicherer? (These 4)

> Sekuritisierungsprozesse verschieben das normative Spannungsgefüge zwischen Freiheit und Sicherheit zugunsten letzterer in der Cybersicherheitspolitik. So droht Sicherheit als transzendentaler Wert („Supergrundrecht") zum Vehikel von diversen Geheimdiensten zu werden, indem die allumfassende und anlasslose Überwachung zu ihrer Kernaufgabe deklariert wird. Dieser stetige Normbruch könnte, verstärkt durch die Verstrickung Dritter (Politik und Unternehmen) und Gewöhnungseffekte, zum Regelfall werden.

Neben Datenhandel und Selbstüberwachung wurde die Internetentwicklung in den vergangenen Jahren zunehmend durch die geheimdienstliche Massenüberwachung geprägt, die, sofern durch Enthüllungen bekannt, fraglos totalitäre Züge gezeigt hat (Crampton 2014; Deibert 2013; Greenwald 2014: 47). Im Vergleich zum Privatsphären- und Datenschutz, wo eine große Lücke in der sozial- und politikwissenschaftlichen Auseinandersetzung klafft, fügen sich die Erkenntnisse über die Auswüchse der staatlich sanktionierten Geheimdiensttätigkeit in eine lange Reihe von Beispielen, die intensiv durch politikwissenschaftliche Analysen zur Cybersicherheit untersucht worden sind. Ein Großteil dieser Studien geht vom konstruktivistischen Theorieangebot der Kopenhagener Schule, konkret: dem Sekuritisierungsansatz, aus (vgl. Dunn Cavelty 2013 sowie in diesem Band; Guitton 2013; Hansen et al. 2009; Nissenbaum 2005).

Die vielfach und in dramatisierendem Ton beschriebenen diffusen Bedrohungen von Cyberkrieg und Cyberterror (eindrückliche Bspe. in Singer et al. 2014: 37) wurden und werden zur Legitimation von Maßnahmen beispielloser Massenüberwachung genutzt. Dabei stellt sich die Frage, ob Freiheit oder Sicherheit als das transzendentale Gut angesehen werden kann, also als das Bedürfnis, das erfüllt sein muss, damit alles Weitere sinnvoll zu wünschen ist. Empirische Beispiele zeigen, dass Sekuritisierungsprozesse auf diesem schwierigen normativen Terrain sehr gut gedeihen. Ein häufiges Beispiel sind die terroristischen Anschläge auf das World Trade Center im September 2001. Sie haben unmittelbar zu einer Verschärfung der Gesetzeslage auch auf dem Feld der Cybersicherheit geführt. Der US Patriot Act hat die ausufernden Überwachungspraktiken der Geheimdienste ermöglicht (vgl. Deibert 2013: 3–5). Auch die aktuelle Entwicklung der Gesetzgebung im von den Anschlägen auf das Satiremagazin Charlie Hebdo und einen jüdischen Supermarkt im Januar 2015 schwer getroffenen Frankreich deuten in diese Richtung.[1]

1 So verabschiedete die französische Nationalversammlung am 24. Juni 2015 einen Gesetzesvorschlag (Nr. 2669), der den nationalen Geheimdiensten sehr weitgehende Befugnisse zur Aufklärung und Überwachung von Internetkommunikation erteilt: http://www.assemblee-nationale.fr/14/pdf/projets/pl2669.pdf (26.6.2015).

Die Beispiele deuten darauf hin, wie Geheimdienste und andere sicherheitspolitische Akteure Bedrohungen und Risiken als Begründung verwenden, um bürgerliche Freiheit und Grundrechte einzuschränken. Ein viel beachtetes Zitat aus dem deutschen Kontext, in dem die Transzendentalisierung der Sicherheit buchstäblich wird, ist das umstrittene Diktum des damaligen Bundesinnenministers Friedrich, der im Juli 2013 von einem „Supergrundrecht Sicherheit" sprach (Krempl et al. 2013). Der Vollständigkeit halber sollte gesagt werden, dass Friedrich nachschob, dass für die Sicherheit nicht die Freiheit aufzugeben sei. Dennoch bringt seine Wortwahl eine Prioritätensetzung im Sinne der Sekuritisierung zum Ausdruck. Bis heute werden durch ähnliche Einlassungen immer wieder Aufklärungswiderstände im Rahmen der Ermittlungen des NSA-Untersuchungsausschusses begründet (siehe aktuell zum Umgang mit der sogenannten Selektorenliste: Bundespresseamt 2015).

Die Befunde über die ab 2001 erfolgte massive Ausweitung der geheimdienstlichen Überwachungstätigkeit in den USA (siehe Binney in diesem Band) zeigen deutlich, dass die permanente, globale, anlasslose und massenhafte Sammlung von Daten im Rahmen technischer Überwachung zu einer Kernaufgabe der Geheimdienste, nicht nur in den USA, gemacht wurde (Dickow 2015: 1). Warner und Mahner aus Sicherheitskreisen bilden die Speerspitze dieses Prozesses. Vertreter von IT-Unternehmen sekundieren hier nur allzu häufig, ohne dabei die Vermarktung der eigenen Produkte aus dem Blick zu verlieren. Es scheint, dass angesichts dieser „Marktmacht" die Politik oftmals nicht über eine ausreichend unabhängige Expertise verfügt, um wichtige Details nachzuvollziehen, wie in einer Resolution der Parlamentarischen Versammlung des Europarats von April 2015 festgehalten ist:

> „In several countries, a massive 'Surveillance-Industrial Complex' has evolved, fostered by the culture of secrecy surrounding surveillance operations, their highly technical character and the fact that both the seriousness of alleged threats and the need for specific counter-measures and their costs and benefits are difficult to assess for political and budgetary decision-makers without relying on input from interested groups themselves. These powerful structures risk escaping democratic control and accountability and they threaten the free and open character of our societies" (Europarat 2015).

Ob sich der hier konstatierte Normbruch verfestigen wird, wird auch davon abhängen, wie lange die Enthüllungen Snowdens und anderer eine gesellschaftliche Debatte sowie Gegenbewegungen hervorbringen und formieren. Indizien deuten darauf hin, dass das Thema „ungeregelte Massenüberwachung" zwar einer beschleunigten Themenkonjunktur unterliegt, sich aber auch hier zunehmend eine Haltung der ohnmächtigen Bequemlichkeit durchsetzt (vgl. auch Deibert 2013: 7).

Praktische Durchsetzungsprobleme ergeben sich aus territorial verfassten Ordnungsansprüchen (Heumann et al. 2014: 14–18; Neumann 2014: 11). Denn das von westlichen Geheimdiensten, so auch dem deutschen BND, etablierte Kooperationsgeflecht gleicht einem Ringtauschsystem, in dem jeder beteiligte Geheimdienst die nationale Grundrechtslage unterwandern kann, indem er die gewünschten Daten heimischer Grundrechtsträger vorbei an parlamentarischer und/oder richterlicher Kontrolle

vom Partnergeheimdienst erhält (Neumann 2014: 24; siehe auch Rudolf 2014: 29; „Schattendiplomatie“: Dickow 2015: 1–2). Der einzelne Bürger kann in einer solchen Umgebung kaum je eine Exekutive, gar einen ausländischen Geheimdienst, verantwortlich halten. Auch das verschiedentlich dokumentierte Scheitern von Versuchen deutscher und französischer Behörden, so genannte „No-Spy-Abkommen“ mit der US-amerikanischen Regierung zu verhandeln, weist darauf hin, dass der Grundrechtsschutz in einer Demokratie durchaus mit dem Grundrechtsbruch in einer anderen Demokratie einhergehen kann und möglicherweise dauerhaft -gehen wird (vgl. Rudolf 2014: 30). Es ist daher denkbar, wenn nicht gar plausibel, wenn sich ob dieser Entwicklung eine Mentalität und Praxis der gesellschaftlichen Selbstzensur verbreitete (Greenwald 2014).

Die passive Selbstzensur, die das Wissen um permanente Überwachung präventiv in das Verhalten einschreibt, kann abstrakt und theoretisch mit dem Bild des Panoptikums bei Bentham (2003 [1791]) illustriert werden. Jeder fühlt sich überwacht und passt deshalb sein Verhalten an (siehe hierzu auch Cornelius und Binney in diesem Band). Diese Erwartung ist auch in eine Negativutopie steigerungsfähig, wenn sich nämlich die Überwachungspraxis und ohnmächtige Haltung in eine Art Transparenzgebot (siehe oben) transformiert und derjenige sich verdächtig macht, der etwas zu verbergen hat.

Die Tendenz zur Entterritorialisierung und die Praxis geheimdienstlichen Ringtausches fordern die Frage nach internationalen und globalen Standards heraus. Entsprechende Anstrengungen sind, wie etwa die zitierte Resolution des Europarates (Europarat 2015), erkennbar. In ihrem Forderungskatalog finden sich z.B. ein Verbot der gezielten Schaffung von Backdoors in Sicherheitsarchitekturen, nationale Kontrollmechanismen auf Basis ausreichender unabhängiger Expertise; Schutz für Whistleblower bis hin zum Asyl; Schutz ausländischer Bürger wie eigener; Förderung von nutzerfreundlichen Datenschutztechnologien; Verbot von Exporten von Ausspähsoftware an autokratische Regime. Jüngere Dokumente des internationalen digitalen Menschenrechtsschutzes sind auch der Bericht der Menschenrechtsbeauftragten der Vereinten Nationen sowie die Resolution der UN-Generalversammlung zum Recht auf Privatheit im digitalen Zeitalter (Pillay 2014; Generalversammlung der Vereinten Nationen 2014). Ob in solchen Versuchen die Herausbildung tragfähiger Normen für die internationale Gemeinschaft erkennbar wird, wird sich noch erweisen müssen.

6 Die schwierige Restitution staatlicher Souveränität (These 5)

In seiner Entstehungsphase überließen die Staaten die Regulierung des Internets den Erfindern und Pionieren. Je mehr das Netz zum Feld wirtschaftlicher Aktivität und politischer Auseinandersetzung geworden ist, haben die klassischen politischen und rechtlichen Regulierungsinstanzen (insbesondere Regierungen) ihren Zugriff verstärkt. Sie fordern und fördern die territoriale Vergrenzung des Cyberspace.

Der Gründungsmythos des Internets kennt mindestens zwei Erzählweisen. Sie schauen auf unterschiedliche Akteursgruppen, um die Ursprünge der Internettechnologie zu identifizieren. Zum einen ist da das US-amerikanische Verteidigungsministerium, konkret: die ARPA (Advanced Research Projects Agency, heute DARPA), die um ein ausfallsicheres Informations- und Kommunikationsnetz zwischen militärischen Einheiten zu etablieren, Forschung im Bereich der Netzwerktechnologie gezielt und umfangreich förderte (Singer et al. 2014: 13). Zum anderen sind es die so geförderten Wissenschaftler und Entwickler, die ein möglichst funktionales Netz mit entsprechenden Standards kreierten. Diese Protokolle und Standards setzen gesellschaftsrelevante Nutzungsrahmen, sind per se gewissermaßen Regulierung (vgl. Lessig 1999; Deibert 2013: 5–8; DeNardis 2014: 7). Darüber hinaus gab es jenseits der initialen Förderung allerdings kaum regulierende Eingriffe von außen oder gar von staatlicher Seite.

Selbst als das Internet durch die Erfindung des WWW Anfang der 1990er Jahre rasant an Bedeutung gewann, wurde das Netz nicht sofort einer starken Regulierung unterworfen. Vielmehr wehrten sich die Internetpioniere nach Kräften gegen jegliche staatliche Einmischung, erklärten die territorialstaatlich gebundenen politischen Gemeinwesen gar für überholt und lehnten jegliche Kontrolle durch die für überkommen erklärten Souveräne ab (siehe etwa Barlow 1996). In dieser Phase traten die Staaten dem Internet in erster Linie als Nutzer entgegen: Sie verlagerten viele Tätigkeiten in den virtuellen Raum, um Verwaltungen effizienter zu machen. Basierend auf den Lehren des New Public Management orientierten sie sich an Vorbildern aus dem Bereich des E-Commerce (OECD 2003; Accenture 2007; United Nations 2008). Regulierungsbemühungen wurden allenfalls dann unternommen, wenn es um die Verwaltung des Domain-Name-Systems ging. Dies betraf zuvörderst die heikle Frage der Vergabe von Top-Level-Domains (TLDs), insbesondere der Country-Code Top-Level-Domains (ccTLDs), welche Ende der 1990er Jahre der informellen Verwaltung durch den Internetpionier Jon Postel entzogen und einer privatwirtschaftlichen Einrichtung unter Vertrag mit der US-Regierung übertragen wurde.

Die Entwicklung der ccTLDs eignet sich als gutes Beispiel, um die fortbestehende Wirkung territorialstaatlichen Denkens auch auf die Internetarchitektur und die konstitutive Dimension der Internetregulierung zu verstehen (vgl. den Vortrag und die Diskussion Milton Mueller). Die Ursprungsidee der Ingenieure und Pioniere, das grundlegende Ordnungsprinzip des Online-Adressraums war die der allgemeinen, der generischen Top-Level-Domains, etwa gov, com, edu, org, mil, net oder int. Mittlerweile sind weitere, auch umstrittene, hinzugekommen (DeNardis 2014: 44).[2] Diese internetarchitektonische Ausgangsidee ging mit postterritorialen Visionen einher: Jedes Handelsunternehmen der Welt sollte sich unter .com registrieren, jede Universität unter .edu

2 Der XXX-Fall ist mit Blick auf die Frage staatlichen Einflusses, vor allem der USA, aber durchaus über das GAC, sehr erhellend. Aufgrund innenpolitischen Widerstands hatte die US-amerikanische Regierung die Etablierung der TLD XXX für pornographische Inhalte blockiert (Mueller 2010: 71–73).

(Postel 1992). Die Realität der Internetentwicklung hielt diesen Visionen aber nicht Stand: Während die generischen TLDs für US-amerikanische Inhaber zur Regel wurden, zogen Einrichtungen jenseits der USA eine Registrierung unter der jeweiligen länderspezifischen Kennung vor. Diese waren zwar Anfang der 1980er Jahre als TLDs eingeführt worden,[3] sie sollten nach dem Willen der Pioniere aber keine große Bedeutung erlangen. Den Nationalstaaten ist es allerdings gelungen, der Konstitution des virtuellen Raums zumindest ihre territorialstaatliche Ordnung aufzuzwingen. Mueller (in diesem Band) zeigt zwar, dass die technische Struktur des Internets als Netzwerk der Netzwerke sich der territorialstaatlichen Ordnung weiterhin entzieht: Die sogenannten Autonomen Systeme (AS), welche die tatsächlichen souveränen Einheiten des Internets darstellen, decken sich keineswegs mit staatlichen Einheiten. Eine komplette Deckungsgleichheit (Isomorphie) von AS und Staaten als übergeordnetes Reformziel wäre nicht nur sehr unwahrscheinlich, sie würde das Internet, wie wir es kennen, auch existentiell gefährden. ccTLDs hätten aus Muellers Sicht allenfalls semantische Bedeutung. Daraus abzuleiten, dass es sich dabei aber lediglich um ein unbedeutendes Kürzel im Adressfeld eines Browsers handelt, könnte zu weit gehen. Denn der Hinweis auf den bloß semantischen (besser: semiotischen) Charakter der ccTLDs lässt sich auf alle konventionalisierten Zeichensysteme übertragen (Saussure 2001), nicht zuletzt auch auf diejenigen staatlicher Symbolik. Empirische Studien zeigen, dass staatliche Symbolik nachhaltige sozialstrukturelle Effekte zeitigt (Schünemann et al. 2015).

Auch mit Blick auf die Organisationsstruktur der internationalen Internet Governance hat sich die multilaterale oder intergouvernementale Logik durchaus ihre Plätze erkämpft. Ein zentrales Datum ist hier der 2005 veranstaltete World Summit on the Information Society (WSIS), dem ein zweijähriger Konsultationsprozess vorausgegangen war und der mit der sog. Tunis-Agenda abgeschlossen wurde. Gipfel und Agenda markieren einen Wendepunkt hin zu größerer staatlicher Aufmerksamkeit und klarer artikulierten Hoheitsansprüchen im Bereich der Internet Governance. Aktuell läuft die Revision des Tunis-Agenda-Programms unter dem Titel WSIS +10. Dieser Prozess wird im Dezember 2015 in der Generalversammlung der Vereinten Nationen, also im klassischen zwischenstaatlichen Format, abgeschlossen. Schon mit dem ersten Gipfel zur Informationsgemeinschaft wurde mit dem Internet Governance Forum (IGF) eine erste permanente UN-Organisation zur Regulierung des Cyberspace etabliert.

Selbst der zentralen Organisation zur Verwaltung der kritischen Internet-Ressourcen, der ICANN, die klarer als vergleichbare Organisationen den Grundsatz des Multistakeholderism verkörpert und von staatlichen Regulierungen nur schwach betroffen ist, wurde mit dem Governmental Advisory Committee (GAC) ein intergouvernementales Gremium hinzugefügt (vgl. auch den Beitrag von Hofmann in diesem Band). Dieses ist pro forma zwar nur beratendes Gremium, aber wegen seiner unspezi-

3 Hinterlegt ist das ganze System in der ISO-3166-Liste, die Postel und sein Kreis zur Orientierung und Entlastung heranzogen, um Konflikten aus dem Weg zu gehen (Postel 1994).

fischen Kompetenzzuschreibung und seines faktischen Wirkens als Interessenvertretung der Nationalstaaten kommt es immer wieder zu problematischen Konflikten im intrainstitutionellen Gefüge der ICANN (vgl. Mueller 2010: 242–244).

Zuletzt gibt es mit den USA einen Nationalstaat, der sich als Gründungsnation des Internets und Treuhänder eines freien Netzes versteht (Web of the Free) und mit dieser Rechtfertigung bislang die Sonderrolle eines Prinzipals im Hinblick auf die IANA-Funktionen für sich beanspruchte. Doch ist diese Treuhänderrolle, auch aufgrund der steigenden Bedeutung des Internets für die weltweite Kommunikation, zunehmend von anderen Staaten, allen voran Russland, angefochten worden (Lewis et al. 2011: 4). So könnte die derzeit vieldiskutierte Transformation der IANA-Funktionen (Internet Assigned Numbers Authority, s. Hofmann in diesem Band) die Ordnungsstruktur in eine neue Richtung lenken. Allerdings hat die US-amerikanische Regierung dafür klare Bedingungen gesetzt: den Verbleib der Funktionen bei einer ausführenden Organisation mit Sitz innerhalb der USA sowie eine weitere Verpflichtung zum Multi-Stakeholder-Ansatz, sodass anderen Staaten ein größerer Einfluss im Sinne eines intergouvernementalen Aufbaus verwehrt bleiben dürfte.

Betrachten wir die regulative Dimension der Internet Governance, also die verschiedenen Problembereiche, die sich mit der Internetentwicklung herausgebildet oder neu zugespitzt haben, so stechen vermehrte staatliche Ordnungsansprüche ebenfalls ins Auge. Ein erster großer Konflikt hat sich auf dem Feld des Urheberrechts zugetragen. Später ging es um Jugendschutz und Netzsperren, Cybersicherheit und Datenschutz. In all diesen Bereichen stellt sich die Frage, wie sich Ordnungsansprüche durchsetzen lassen, wenn die klassischen Regulierungsinstanzen von Politik und Recht an ihre territorialstaatlichen Grenzen stoßen (vgl. die Beiträge von Reimer, Cornelius, Mueller und Froomkin in diesem Band).

Zuletzt finden wir staatlich regulierte Content-Regulierung in autokratischen Regimen, wo sie gravierende Formen der Zensur bedeuten (können), und auch in demokratischen Gemeinwesen, wo sie oft als umstrittene Maßnahmen zur Bekämpfung kinderpornografischer oder terroristischer Inhalte auftreten. Gerade im Hinblick auf dieses letzte Beispiel und die Kontroversen, die sicherheitspolitisch motivierte Akteure mit der Netzgemeinde darüber auszutragen hatten, stellen sich wichtige Grundsatzfragen: Inwieweit unterlaufen technische Hindernisse und einfache Umgehungsmöglichkeiten die Gültigkeit einer Norm? Lassen sich Handlungen nicht auch dann als rechtswidrig klassifizieren und im Fall von Verstößen verfolgen, wenn sie leicht möglich und nur schwerlich aufzudecken sind?

7 Vom Cyberkrieg, der niemals stattfand (These 6)

> Operationelle Cyberangriffe sind bereits Teil der konventionellen militärischen Einsatzführung in und zwischen industrialisierten Staaten. Sie werden in Zukunft zunehmend auch Teile der weniger vernetzten Welt betreffen. Den Cyberkrieg im Sinne strategischer Kriegführung, der eine vollständige Lähmung oder gar physische Auslöschung des Gegners umfasst, gibt es bislang nicht und er bleibt auf lange Frist unwahrscheinlich.

Das viel gebrauchte Wort des Cyberkriegs ist ganz offensichtlich eine Metapher (Rid 2012: 15). In seiner realweltlichen Bedeutung steht Krieg für Phänomene lang anhaltender organisierter Gewaltausübung zwischen Staaten, die anhand von qualitativen oder quantitativen Kriterien nach den politischen Zielen von Akteuren, der Wahl der Mittel, dem Ausmaß an Zerstörungen oder der Zahl der Todesopfer unterschieden werden können. Der Cyberkrieg als Sammelbegriff für verschiedenste Formen (oder auch bloßen Spuren) der offenen oder verdeckten netzbasierten Konfliktaustragung unterläuft all diese Definitionen. Auf der Ebene der Wortbedeutung kann also im strengen Sinne bislang in keinem Fall tatsächlich von einem Cyberkrieg die Rede sein.

Dennoch wird der Begriff, gelegentlich wohl auch in effekthascherischer Absicht, oft gebraucht (zu Ursprung und Verbreitung: Dunn Cavelty 2010: 82–183), sodass nach der politischen Wirkung des Metapherngebrauches zu fragen ist. Die politikwissenschaftliche Diskursforschung ist dazu geeignet, den Sprachgebrauch daraufhin zu untersuchen, inwiefern er bestimmtes politisches Handeln rechtfertigt und dadurch bspw. ermöglicht, dass drastische Präventions- und/oder Verteidigungsmaßnahmen von einem Gemeinwesen akzeptiert werden.

Es ist der starke, in Teilen alarmistische Begriffsgebrauch, der jenseits des Cyberkrieges weitere potente Analogien transportiert[4] und der zu einer verbreiteten Anwendung des sog. Sekuritisierungsansatzes der „Kopenhagener Schule“ geführt hat (Dunn Cavelty 2013; Guitton 2013; Hansen et al. 2009). Nach einer Phase der allgegenwärtigen Anwendung des Ansatzes ist die Cybersicherheitsforschung in diesem Forschungssegment insbesondere durch die Arbeiten von Myriam Dunn Cavelty vorangetrieben worden. Sie bemüht sich nicht nur um eine kritische Bestandsaufnahme und Reflexion von Versicherheitlichungsprozessen, indem sie wichtige Differenzierungen des Begriffs einführt, bspw. jene zwischen einem operationellen und einem strategischen Cyberkrieg. Ersteren, so Dunn Cavelty, gibt es, wird es immer geben und hat es – auf dem jeweiligen technischen Niveau – schon lange gegeben. Informationelle Kriegsführung und ‚Propagandakrieg‘ – auch das eine Metapher, die sich in ihrer eingegrenzten Bedeutung durchaus gut verstehen lässt – haben in früheren Konflikten vor der Entwicklung und massenhaften Nutzung von Computern und Netzwerktechnologien eine substantielle Rolle gespielt. Durch den Cyberspace verfügen diese Techniken nun über ein neues, und potentiell sehr potentes Anwendungsgebiet. Ähnliche Effekte sind für die Cyber-Spionage und Sabotage zu beobachten. Dies alles lässt sich aber zweifelsfrei der Kategorie operationeller Kriegsführung oder Konfliktaustragung zuordnen (siehe auch Nye 2011: 11).

Dem operationellen Cyberkrieg steht der strategische Cyberkrieg gegenüber. Für eine solche Art von netzbasierter Gewaltanwendung mit direkten und fatalen Folgen gibt es bisher keine Beispiele. Auch der Computerwurm Stuxnet erfüllt nicht die defini-

4 Beispiele wie „Cyber 9/11“, „Cyber Pearl Harbor“ oder „Cyber Hiroshima“ stellen nur die offensichtlichsten Beispiele dar (Bspe. dokumentiert etwa von Rid 2012: 6; Singer et al. 2014: 37).

torischen Kriterien eines Akts im Sinne der strategischen Kriegsführung (Rid 2012; abweichend Deibert 2013). Vielmehr ist selbst diese erfolgreiche und mit kinetischem Effekt implantierte Schadsoftware nur ein raffinierter Sabotageakt, der schon allein deshalb keinen Kriegsakt darstellt, weil es keinen völkerrechtlich anerkannten oder nur politisch erklärten Krieg zwischen den beteiligten Staaten gegeben hat. Einen Cyberkrieg im strategischen Sinn gibt es also bislang tatsächlich nicht und er ist auch für die Zukunft unwahrscheinlich (Dunn Cavelty 2010: 186–187; Lewis et al. 2011: 2; Rid 2012).

Anders verhält es sich mit der Metapher des Cyberterrorismus (Definitionen in Dunn Cavelty 2010: 182; Heickerö 2014: 554–557; Heugenbart 2014: 7). Zunächst ist der Begriff des Terrorismus per se unklarer als der Kriegsbegriff, und seine Deutung ist daher aufgeschlossener gegenüber der chronisch unklaren Attribution von Cyberangriffen (Rid et al. 2015). Anders auch als der politikwissenschaftliche Kriegsbegriff bemisst er sich nicht an quantifizierbaren Zerstörungs- oder Mortalitätsraten. Vielmehr steht die einschüchternde Wirkung des Terroraktes auf das Publikum, den interessierten Dritten, im Mittelpunkt eines sozialwissenschaftlichen Terrorismusbegriffes. In diesem Sinne können eine Reihe jüngerer Cyberangriffe durchaus als Cyberterrorismus bezeichnet werden, etwa die DDoS-Attacken und defacements gegen TV5Monde im April 2015. Die Totalausfälle von elf Spartenkanälen des französische Nationalidentität transportierenden Fernsehsenders, verbunden mit Bekennervideos und -texten der Terrororganisation Islamischer Staat, islamistischen Hassparolen und Drohungen, haben nur wenige Monate nach den Anschlägen auf das Satiremagazin Charlie Hebdo und einen jüdischen Supermarkt gesellschaftliche Ängste ausgelöst und verstärkt.

Cyberterrorismus oder Cyberkrieg: beide Begriffe haben ihre, wenn auch unterschiedliche, soziale und politische Wirklichkeit. Mit beiden müssen sich die Sozialwissenschaften auseinandersetzen, ohne bei der Dekonstruktion eines als alarmistisch empfundenen Begriffsgebrauchs stehen zu bleiben. Vielmehr müssen auch dessen soziokulturellen Bedingungen und die Eintrittswahrscheinlichkeiten von netzbasierten Gewaltakten systematisch und differenziert untersucht werden.

8 Konklusion

Mit unseren sechs Thesen haben wir den „Makrokosmos“ (Kleinwächter 2015) der Internet Governance durchschritten und dabei nur einige Winkel beleuchten können. Ausgangspunkt unserer Argumentation war die zögerliche Politisierung der Internetregulierung, die wir auf drei, teilweise verschränkte Faktoren zurückgeführt haben: 1. die anhaltende Herausbildung von cyberpolitischen Akteurs- und Interessenkonstellationen auf nationaler wie internationaler Ebene; 2. die dominante Selbstbeschränkung des Nutzers auf die Rolle als Marktbürger, der seine bürgerlichen Rechte und Freiheiten kaum wahrnimmt; 3. die territorialstaatliche politische und rechtliche Haftung der

klassischen Regulierungsinstanzen im Spannungsverhältnis mit drängenden transnationalen Regulierungsbedarfen.

Auf dieser Grundlage haben wir zweitens argumentiert, dass zumindest bislang demokratisierende Effekte des Internetgebrauchs kaum empirisch feststellbar sind. Einerseits zeigen die Autoren (insbesondere Kneuer, Froomkin und Binney), dass keine gerichtete Beziehung zwischen Regimetyp und -stabilität und der Internetentwicklung nachweisbar ist. So bietet das Internet auch demokratischen Regierungen die Chance zu ungezügelter Überwachung und Herrschaft. Hier schlägt sich auch die mangelnde Ausprägung einer digitalen Bürgerrolle negativ nieder. Zudem existiert nach wie vor eine auffällige soziale Schichtung (digital divide) in der Internetnutzung, die ein demokratieoptimistisches Fazit, welches die Repräsentanz der Nutzer im politischen Raum nicht ausreichend reflektiert, auf nationaler wie internationaler Ebene infrage stellen muss. So lassen sich empirisch nur bedingt Veränderungen der politischen Öffentlichkeit aufzeigen: Kurzatmige Online-Protestkulturen sind deutlicher erkennbar als nachhaltige Mobilisierungseffekte, sodass wir jenseits tragfähiger demokratischer Partizipation über das Netz eher deutliche Anzeichen einer netzbasierten Scheinpartizipation erkennen können.

Diese skeptische Bewertung der Befunde verschärft sich, wenn wir den Blick auf den Privatsphären- und Datenschutz lenken. Die Mehrzahl unserer Autoren (und auch wir) konstatieren eine besorgniserregende Aufweichung dieses Grundrechts. Die Privatsphäre im Netz wird immer mehr zu einem kommodifizierbaren Gut in der Internetwirtschaft und diese Entwicklung beeinträchtigt auch nachhaltig deren Schutz in der Offline-Welt (insbesondere Froomkin in diesem Band). Internationale Standards in diesem Bereich sind dringend erforderlich, stecken aber noch im Entwicklungsstadium.

Der Kommodifizierung durch Internetanbieter steht die Nivellierung durch geheimdienstliche globale Massenüberwachung in nichts nach. Theorien der Versicherheitlichung können gut erklären, wie es zur Legitimierung außergewöhnlicher Maßnahmen in diesem Bereich gekommen ist und weiterhin kommt. Aus demokratietheoretischer Sicht ist dies gleichwohl nicht weniger problematisch, denn der Normbruch scheint eher auf Dauer denn auf Abruf gestellt zu sein. Auch in diesem Bereich ist die internationale Normsetzung allenfalls in einem initialen Stadium befindlich.

Die Straffung des staatlichen Herrschaftsanspruchs über seine Bürger in Form von Kontrolle und Überwachung steht in einem Spannungsverhältnis zum Versuch der Restitution staatlicher Souveränität im Internet, denn diese ist mit der bestehenden technischen Architektur als eines Netzwerks der Netzwerke nicht vereinbar. Gleichwohl können wir steigende staatliche Ordnungsansprüche und wachsende Einflüsse auf die konstitutive, die regulative wie auch die institutionelle Dimension der Internet Governance beobachten. Dieser Trend wird oft verkürzt als Vergrenzung des Cyberspace begriffen. Er steht aber jenen Abgesängen auf den Nationalstaat entgegen, die Mitte der 1990er Jahre noch die Internetgemeinde beseelten. Dies gilt auch deshalb, weil staatliche Sicherheitsorgane im Angesicht immer neuer „Gefahren, Risiken und

Bedrohungen“ die Versicherheitlichung des Cyberspace betreiben und dabei *en passant* auch eigene Gestaltungsansprüche neu fromulieren. In Forschung und politischer Praxis bedarf es daher, wie Miriam Dunn-Cavelty es fordert, einer kritischen und differenzierten Debatte über den Gebrauch von irreführenden Metaphern wie dem Cyberkrieg, der in seiner strategischen Ausprägung kaum jemals eintreten wird.

Unsere Überlegungen sind noch keineswegs abgeschlossen. Aus unserer sozialwissenschaftlichen Perspektive scheint das Internet trotz seiner mittlerweile beträchtlichen ‚Lebenszeit‘ immer noch untererforscht. Die zukünftige politikwissenschaftliche Forschung sollte sich dabei mit angrenzenden Disziplinen, insbesondere aber auch mit dem Feld der Computerwissenschaften interdisziplinär vernetzen. Die Heidelberger Ringvorlesung und der vorliegende Sammelband sind im Sinne dieses Ziels konzipiert worden und sollen weitere Forschungs-, Diskussions- und Publikationsprojekte anstoßen.

Wir meinen, dass die nationale wie internationale Regulierung des Internets zu den spannendsten politischen Fragen dieser Zeit gehört. Sie wird auch mittel- und langfristig die nationale wie internationale Politik sowie die beteiligten Gesellschaften stark prägen. Eine entscheidende Frage wird dabei sein, wie sich der Netzbürger selbst definiert und reguliert, denn er bildet nicht nur den Souverän des Netzes, sondern sein Verhalten wirkt ganz entscheidend auf die Stellung von Unternehmen und Regierungen, die ihrerseits das Netz und seine Regeln bestimmen möchten.

Literatur

Accenture (2007): Leadership in Customer Service. Delivering on the Promise. Accenture.

Barlow, John Perry (1996): A Declaration of the Independence of Cyberspace (07.08.2004), https://projects.eff.org/~barlow/Declaration-Final.html (13.03.2015).

Baumann, Max-Otto (2013): Der politische Diskurs über Privatsphäre und Datenschutz in sozialen Netzwerken, in: Ackermann, Ulrike (Hrsg.): Im Sog des Internets. Öffentlichkeit und Privatheit im digitalen Zeitalter, Humanities: Frankfurt, 15–52.

Baumann, Max-Otto (2014): Die schöne Transparenz-Norm und das Biest des Politischen. Paradoxe Folgen einer neuen Ideologie der Öffentlichkeit, in: Leviathan 3, 398–419.

Bentham, Jeremy (2003 [1791]): Panopticon: or, the inspection-house. Containing the idea of a new principle of construction applicable to any sort of establishment, in which persons of any Description are to be kept under Inspection. and in particular to penitentiary-houses, prisons, Houses of Industry, Work-Houses, Poor-Houses, Manufactories, Mad-Houses, Hospitals, and Schools. With a plan of Management adapted to the Principle. In a series of letters, written in the Year 1787, From Crecheff in White Russia, to a Friend in England, Eighteenth Century Collections Online: Dublin, http://find.galegroup.com/ecco/infomark.do?&source=gale&prodId=ECCO&userGroupName=heidel&tabID=T001&docId=CW125793319&type=multipage&contentSet=ECCOArticles&version=1.0&docLevel=FASCIMILE (26.06.2015).

Bieber, Christoph (2002): Digitaler Strukturwandel der Öffentlichkeit?, in: Schatz, Heribert / Rössler, Patrick / Nieland, Jens-Uwe (Hrsg.): Politische Akteure in der Mediendemokratie. Politiker in den Fesseln der Medien?, Westdeutscher Verlag: Wiesbaden, 113–127.

Bruns, Axel (2009): Blogs, Wikipedia, Second Life and Beyond. From Production to Produsage, Peter Lang: New York.

Bundespresseamt (2015): Bundeskanzlerin "Sicherer durch Arbeit der Nachrichtendienste", BPAInternet, http://www.bundeskanzlerin.de/Content/DE/Artikel/2015/05/2015-05-04-merkel-bnd.html (26.06.2015).

Busch, Andreas / Jakobi, Tobias (2011): Die Erfindung eines neuen Grundrechts. Zu Konzept und Auswirkungen der "informationellen Selbstbestimmung", in: Hönnige, Christoph / Kneip, Sascha / Lorenz, Astrid (Hrsg.): Verfassungswandel im Mehrebenensystem, VS Verlag für Sozialwissenschaften: Wiesbaden, 297–320.

Crampton, Jeremy W. (2014): Collect it all: national security, Big Data and governance, in: GeoJournal, DOI: 10.1007/s10708-014-9598-y.

Deibert, Ronald (2013): Black code. Surveillance, privacy, and the dark side of the Internet, Trade paperback edition.

DeNardis, Laura (2014): The global war for internet governance, Yale University Press: New Haven/London.

Diamond, Larry (2012): The Coming Wave, in: Journal of Democracy 23: 1, 5–13.

Dickow, Marcel (2015): Außenpolitik der Dienste. Die strategische Kommunikationsüberwachung und ihre Folgen, in: SWP-Aktuell 18.

Dunn Cavelty, Myriam (2010): Cyber-threats, in: Dunn Cavelty, Myriam / Mauer, Victor (Hrsg.): The Routledge handbook of security studies, Routledge (Routledge handbooks): Milton Park, 180–189.

Dunn Cavelty, Myriam (2013): Der Cyber-Krieg, der (so) nicht kommt. Erzählte Katastrophen als (Nicht)Wissenspraxis, in: Hempel, Leon / Bartels, Marie (Hrsg.): Aufbruch ins Unversicherbare. Zum Katastrophendiskurs der Gegenwart, transcript (Sozialtheorie): Bielefeld, 209–233.

Europarat (21.04.2015): Resolution 2045: Mass Surveillance, http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21692&lang=en (26.06.2015).

Ferdinand, Peter (2000): The Internet, democracy and democratization, in: Democratization 7: 1, 1–17.

Generalversammlung der Vereinten Nationen (2014): Das Recht auf Privatheit im digitalen Zeitalter. Generalversammlung der Vereinten Nationen. New York (A/RES/69/166), http://www.un.org/depts/german/gv-69/band1/ar69166.pdf (01.07. 2015).

Greenwald, Glenn (2014): NSA: Die Schere im Kopf. Wie Massenüberwachung jeden Protest im Keim erstickt, in: Blätter für deutsche und internationale Politik 6, 47–58.

Greitens, Sheena Chestnut (2013): Authoritarianism online. What Can We Learn from Internet Data in Nondemocracies, in: Political Science & Politics 46: 2, 262–270.

Guitton, Clement (2013): Cyber insecurity as a national threat. overreaction from Germany, France and the UK?, in: European Security 20: 1, 21–35.

Hansen, Lene / Nissenbaum, Helen (2009): Digital Disaster, Cyber Security, and the Copenhagen School, in: International Studies Quarterly 53: 4, 1155–1175.

Hegenbart, Christine (2014): Semantics Matter. NATO, Cyberspace and Future Threats. NATO Defense College (Research Paper, 103), http://www.ndc.nato.int/download/downloads.php?icode=416 (01.07.2015).

Heickerö, Roland (2014): Cyber Terrorism: Electronic Jihad, in: Strategic Analysis 38: 4, 554–565.

Heumann, Stefan / Wetzling, Thorsten (2014): Strategische Auslandsüberwachung. Technische Möglichkeiten, rechtlicher Rahmen und parlamentarische Kontrolle (Policy Brief), http://www.stiftung-nv.de/sites/default/files/052014_snv_policy_brief_strategische_auslandsuberwachung.pdf (10.04.2015).

Hindman, Matthew Scott (2009): The myth of digital democracy, Princeton University Press: Princeton, NJ.

Hofmann, Jeanette (2005): Internet Governance. Zwischen staatlicher Autorität und privater Koordination, in: Internationale Politik und Gesellschaft 3, 10–29.

Hofmann, Jeanette / Katzenbach, Christian / Gollatz, Kirsten (2014): Between Coordination and Regulation: Conceptualizing Governance in Internet Governance, in: HIIG Discussion Paper Series 4, DOI: 10.2139/ssrn.2484463.

Howard, Philip N. / Hussain, Muzammil M. (2011): The Upheavals in Egypt and Tunisia. The role of digital media, in: Journal of Democracy 22: 3, 35–48.

Initiative D21 (2014): D-21-Digital-Index 2014. Die Entwicklung der digitalen Gesellschaft in Deutschland. Initiative D21. Berlin, http://www.initiative21.de/wp-content/uploads/2014/11/141107_digitalindex_WEB_FINAL.pdf (25.06.2015).

Karaboga, Murat / Masur, Philipp / Matzner, Tobias / Mothes, Cornelia / Nebel, Maxi / Ochs, Carsten et al. (August/2014): White Paper Selbstdatenschutz. Hrsg. v. Forum Privatheit. Karlsruhe.

Kleinwächter, Wolfgang (2015): Internet Governance Outlook 2015. Two Processes, Many Venues, Four Baskets, http://www.circleid.com/posts/20150103_internet_governance_outlook_2015_2_processes_many_venues_4_baskets/ (08.01.2015).

Kneuer, Marianne (2013a): Bereicherung oder Stressfaktor? Überlegungen zur Wirkung des Internets auf die Demokratie, in: Kneuer, Marianne (Hrsg.): Das Internet: Bereicherung oder Stressfaktor für die Demokratie?, Nomos (Veröffentlichungen der Deutschen Gesellschaft für Politikwissenschaft, 31): Baden-Baden, 7–31.

Kneuer, Marianne (2013b): "Mehr Partizipation durch das Internet?". Mainz: LpB (Zur Sache, 7).

Krempl, Stefan / heise online (2013): Friedrich erhebt Sicherheit zum "Supergrundrecht". Heise Medien, 17.07.2013, http://www.heise.de/newsticker/meldung/Friedrich-erhebt-Sicherheit-zum-Supergrundrecht-1919309.html (26.06.2015).

Lanier, Jaron (2014): Who owns the future?, Simon & Schuster trade paperback edition.

Lessig, Lawrence (1999): Code and other laws of cyberspace, Basic Books: New York.

Lewis, James A. / CSIS (2011): Cybersecurity two years later, Washington, DC.

Matthews, Duncan / Žikovská, Petra (2013): The Rise and Fall of the Anti-Counterfeiting Trade Agreement (ACTA). Lessons for the European Union, in: IIC 44: 6, 626–655.

Morozov, Evgeny (2011): The Net delusion. The dark side of internet freedom, PublicAffairs: New York.

Mueller, Milton L. (2010): Networks and states. The global politics of internet governance, MIT Press (Information revolution and global politics): Cambridge, Mass.

Negroponte, Nicholas (1995): Being digital, Knopf: New York.

Neumann, Peter (2014): Algorithmen und Agenten. Wo es gerade in Deutschland bei der Geheimdienstarbeit hapert, in: Internationale Politik Nov./Dez., 8–14.

Nissenbaum, Helen (2005): Where Computer Security Meets National Security, in: Ethics and Information Technology 7: 2, 61–73.

Nye, Joseph S. (2011): Diffusion and Cyberpower, in: Nye, Joseph S. (Hrsg.): The Future of Power, Public Affairs: New York, 113–152.

OECD (2003): The e-government imperative, OECD Organisation for Economic Co-operation and Development: Paris.

Pillay, Navanethem (2014): The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights. UNHCR. New York (A/HRC/27/37), http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (01.07.2015).

Postel, Jon (1992): The US Domain. Request for Comments (1386). Network Working Group (Request for Comments, 1386), https://www.ietf.org/rfc/rfc1386.txt (26.06.2015).

Postel, Jon (1994): Domain Name System Structure and Delegation. Request for Comments (1591). Network Working Group (Request for Comments, 1591), https://www.ietf.org/rfc/rfc1591.txt (26.06.2015).

Reynolds, Glenn H. (2006): An army of Davids. How markets and technology empower ordinary people to beat big media, big government, and other Goliaths. Nelson Current: Nashville, Tenn.

Rheingold, Howard (1994): Virtuelle Gemeinschaft. Soziale Beziehungen im Zeitalter des Computers, Addison-Wesley: Bonn, Paris, Reading, Mass.

Rid, Thomas (2012): Cyber War Will Not Take Place, in: Journal of Strategic Studies 35: 1, 5–32.

Rid, Thomas / Buchanan, Ben (2015): Attributing Cyber Attacks, in: Journal of Strategic Studies 38: 1–2, 4–37.

Rudolf, Peter (2014): Vertrauen wär' gut. …doch Amerika will Kontrolle: Zur Legitimität von Spionage, in: Internationale Politik Nov./Dez., 26–33.

Sarcinelli, Ulrich (2012): E-Partizipation in der 'Web 2.0-Demokratie'. Wege und Hindernisse demokratischer Teilhabe – ein Essay, in: Schünemann, Wolf J. / Weiler, Stefan (Hrsg.): E-Government und Netzpolitik im europäischen Vergleich, Nomos-Verlag: Baden-Baden, 435–448.

Sarcinelli, Ulrich (2014): Von der Bewirtschaftung der Aufmerksamkeit zur simulativen Demokratie? Politische Visionen – Von Platon zum Global Village, in: Zeitschrift für Politikwissenschaft 24: 3, 331–341.

Saussure, Ferdinand de (2001): Grundfragen der allgemeinen Sprachwissenschaft. Unter Mitarbeit von Herman Lommel, mit einem Nachw. von Peter Ernst, de Gruyter: Berlin New York.

Schünemann, Wolf J. (2012): E-Government und Netzpolitik – eine konzeptionelle Einführung, in: Schünemann, Wolf J. / Weiler, Stefan (Hrsgg.): E-Government und Netzpolitik im europäischen Vergleich, Nomos-Verlag: Baden-Baden, 9–38.

Schünemann, Wolf J. / Keller, Reiner (2015): Narrativer Nationalismus. Die Wissenssoziologische Diskursanalyse zur Untersuchung kultureller Kontexte der politischen Auseinandersetzung in Europa, in: Hofmann, Wilhelm (Hrsg.): Die andere Seite der Politik. Theorien der kulturellen Konstruktion des Politischen, Springer VS: Wiesbaden.

Schünemann, Wolf J. / Steiger, Stefan / Stier, Sebastian (2016, i.E.): Transnationalisierung politischer Öffentlichkeit über Soziale Medien. Ein Politikfeldvergleich. Manuskript, in: Zeitschrift für Vergleichende Politikwissenschaft Sonderheft: Web 2.0 – Demokratie 2.0 (hrsg. v. Kneuer, Marianne und Salzborn, Samuel).

Sevignani, Sebastian (2013): The commodification of privacy on the Internet, in: Science and Public Policy 40: 6, 733–739.

Shiffrin, Mark A. / Silberschatz, Avi (2005): Web of the Free, in: New York Times, 23.10.2005.

Shirky, Clay (2008): Here comes everybody. the power of organizing without organizations, Penguin Books: New York, NY.

Shirky, Clay (2011): The political power of social media, in: Foreign Affairs 90: 1, 28.

Singer, P. W. / Friedman, Allan (2014): Cybersecurity and cyberwar. What everyone needs to know (What everyone needs to know), Oxford University Press: USA.

Stier, Sebastian (2015): Political Determinants of E-Government Performance Revisited. Comparing Democracies and Autocracies, in: Government Information Quarterly 32: 3, 270–278.

United Nations (2008): E-Government Survey 2008. From E-Government to Connected Governance. Nations, United.

Ziemele, Ineta (2009): Privacy, Right to, International Protection (Max Planck Encyclopedia of Public International Law [MPEPIL]), 3/2009, http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e863?rskey=bTyyHI&result=2&prd=EPIL (26.06.2015).

Autoren

Prof. Dr. Sebastian Harnisch
Inhaber der Professur für Internationale Beziehungen und Außenpolitik
Institut für Politische Wissenschaft
Ruprecht-Karls-Universität Heidelberg
Bergheimer Straße 58
DE-69115 Heidelberg
sebastian.harnisch@uni-heidelberg.de

Dr. Wolf J. Schünemann
Mitarbeiter am Lehrstuhl für Internationale Beziehungen und Außenpolitik
Institut für Politische Wissenschaft
Ruprecht-Karls-Universität Heidelberg
Bergheimer Straße 58
DE-69115 Heidelberg
wolf.schuenemann@ipw.uni-heidelberg.de

DOI: 10.11588/josar.2015.0.23487

Abstracts

Die digitale Geselschaft – Netzpolitik, Bürgerrechte und die Machtfrage

Markus Beckedahl

Abstract

In diesem Beitrag werden in vier Teilen die wesentlichen netzpolitischen Streitfragen und Konfliktlinien zu der Frage „Wer regiert das Internet?“ aufgezeigt. Hierbei werden die früheren und aktuellen Praktiken der Massenüberwachung durch Staaten und Geheimdienste beleuchtet. Es erfolgen außerdem eine Ableitung der Netzneutralität aus den Ursprüngen der Internetentwicklung und ein Plädoyer für den Erhalt dieses Prinzips. Die Fallstricke und Unklarheiten eines territorial gebundenen Urheberrechts werden näher untersucht, ebenso wie die durch soziale Netzwerke vorangetriebene Privatisierung digitaler Öffentlichkeiten. Diese wird problematisiert und mit den modernen Malls in der analogen Welt verglichen. Es werden also die großen gesellschaftlichen Probleme aufgezeigt, die mit der Internetentwicklung verbunden sind und die nach gesellschaftspolitischer Gestaltung verlangen, um Netzpolitik als emergentes Politikfeld zu umreißen.

Keywords

NSA; Netzpolitik; Massenüberwachung; Netzneutralität; Urheberrecht

Internet Governance: Theoretische und empirische Annäherung an einen schwer fassbaren Gegenstand

Jeanette Hofmann

Abstract

Gemessen an der Bedeutung, die das Internet mittlerweile gewonnen hat, steckt die sozialwissenschaftliche Internetforschung, vor allem die Forschung zu Internetpolitik und -regulierung, in Deutschland immer noch in den Kinderschuhen. Vor allem die globale Regulierung des Netzes findet nur wenig Aufmerksamkeit. Um dieses Thema näher zu beleuchten, vergleicht dieser Beitrag Internet Governance mit dem multilateralen Regime der internationalen Telekommunikationspolitik, da sich die Verwaltung des Internets als transnationales Netz der Netze nämlich in bewusster Distanz zur internationalen Staatenwelt und seinen Institutionen entwickelte. Die Folge davon ist ein de-

zentrales, verteiltes Institutionengefüge auf kontinuierlicher Suche nach Legitimität. Außerdem wird der Governance-Begriff mit seiner uneinheitlichen Verwendung sozialwissenschaftlich diskutiert. Dabei liegt der Fokus auf der reflexiven Koordination, also auf der Koordination von Koordination, die dann auftritt, wenn etablierte Koordinationsmodi problematisch werden. Abschließend wird dieser Governance-Begriff anhand der jüngeren empirischen Entwicklung von Internet Governance nach den Snowden-Enthüllungen illustriert.

Keywords

Internet Governance, Governance, Regulierung, Multistakeholder, critical moments

Mehr demokratische Qualität im Cyberspace

Marianne Kneuer

Abstract

Unbestreitbar bietet das Internet erhebliche Möglichkeiten der Information, des interaktiven Austausches und der Organisation von politischer Teilhabe und Einflussnahme für interessierte Bürger und Politiker. Dieser Beitrag argumentiert, dass das Potenzial, ein Mehr an Transparenz, Partizipation und Responsivität über internetbasierte Wege zu erlangen, davon abhängt, ob und wie Regierungen und politische Akteure online verfügbare Angebote machen und ob und wie Bürger diese nutzen. Eine Erhöhung demokratischer Qualität schließt ein, dass die netzbasierten demokratischen Prozesse von beiden Seiten aktiv gestaltet werden. Die Vorstellung jedoch, allein die Existenz neuer technischer Wege sei dazu in der Lage, Defizite in der repräsentativen Demokratie zu beheben, muss als naiv bewertet werden.

Keywords

Internet, Soziale Medien, E-Government, E-Participation, Internetnutzung

Gibt es Souveränität im Cyberspace

Milton L. Mueller

Abstract

Dieser Beitrag behandelt die Frage, ob es staatliche Souveränität im Cyberspace geben kann. Er kommt zu einem differenzierten Ergebnis: Zunächst muss Souveränität *im* und Souveränität *über* den Cyberspace unterschieden werden. Letzteres stellt die Kontrolle

über den Cyberspace in Form staatlicher Strukturen dar. Demgegenüber meint Souveränität im Cyberspace ein Äquivalent zur Souveränität, das mit virtuellen Mitteln erreicht werden kann, also im Sinne eines Gewaltmonopols im virtuellen Raum. Zu beiden Typen fällt die Bilanz skeptisch aus. Über ein Gewaltmonopol im Cyberspace verfügen Staaten offenbar nicht. Demgegenüber ist staatliche Souveränität über den Cyberspace technisch zwar durchaus möglich, sie würde aber das Ende des Internets, wie wir es kennen, bedeuten. Der virtuelle Raum würde eine erhebliche Fragmentierung erfahren. Diese ist keineswegs wünschenswert, denn sie würde das Innovationspotential der Internetentwicklung hemmen. Dies beträfe nicht zuletzt auch die gesellschaftlichen Entwicklungsmöglichkeiten. Wenn Normen durch Fragmentierung geschützt werden, müssen sie sich nicht mehr international durchsetzen. Das Internet bedroht zwar das klassische Konzept territorialer Souveränität. Allerdings könnte die Internetgemeinde gerade aus dieser Krise heraus eine neue Form transnationaler demokratischer Souveränität etablieren.

Keywords

Souveränität, Cyberspace, Territorialität, Fragmentierung, Autonome Systeme

Wer besteuert das Internet? Die Steuersparmodelle von Amazon, Google & Co. Als juristische Reformimpulse

Ekkehart Reimer

Abstract

„Business goes global, taxes stay local“: Dieser Satz, der seit Ende der 1990er Jahre oft als pejorativ-karikierende Beschreibung verwendet wurde, trifft die Wirklichkeit des heutigen Internationalen Steuerrechts nur noch zum Teil. Steuern sind und bleiben zwar staatenbezogen, weil die Staaten Normgeber und Gläubiger sind. Normsetzung und Rechtsanwendung werden aber längst bilateral, supranational (unional) und international koordiniert.

Aus rechtswissenschaftlicher Perspektive zeigt der Beitrag für das Referenzgebiet der im Internet tätigen multinationalen Unternehmensgruppen (MNEs), deren Wertschöpfung im Wesentlichen auf immateriellen Wirtschaftsgütern beruht, wie diese Koordinationsmechanismen funktionieren. Er verdeutlicht zugleich, auf welche Herausforderungen die zwischenstaatliche und supranationale Koordination stößt und welche Perspektiven der Problembewältigung bestehen.

Im Zentrum steht das materielle Recht, das akteurszentriert entfaltet wird. Daneben kommen verfahrensrechtliche Potenziale zur Sprache. Die Erörterung gewinnt durch die in den Jahren 2013 bis 2016 mit Hochdruck vorangetriebenen Bemühungen der

G20-Staaten, der OECD und – nachrangig – der EU um die Eindämmung der base erosion and profit shifting (BEPS) hohe Aktualität.

Keywords

BEPS, Doppelbesteuerung, Europäisches Steuerrecht, OECD, Steuerbetrug, Steuerinformationsrecht, Steuerpolitik

Das Internet: ein umfassendes Überwachungssystem

William Binney

Abstract

Die Veröffentlichungen des Whistleblowers Edward Snowden enthüllten die systematische Massenüberwachung zahlloser Menschen durch die National Security Agency (NSA), die seit den Anschlägen vom 11. September 2001 quasi unkontrolliert und ohne Beschränkungen handeln konnte. Dieser Beitrag untersucht dabei die Funktions- und Wirkungsweise dieser Überwachungstätigkeit und stellt ihr eine kritische Betrachtung sowie eine funktionale Alternative entgegen.

Die NSA nutzt für die massenhafte Überwachung von US-Bürgern und Nicht-US-Bürgern nicht nur eigene Fähigkeiten, sondern geht in zahlreichen Fällen Kooperationen mit sowohl staatlichen wie auch nicht-staatlichen Akteuren zur Erreichung ihrer Ziele ein. Der Beitrag zeigt auf, dass diese massenhafte Überwachung nicht nur in vielfacher Weise gegen amerikanisches Gesetz und gegen die Verfassung verstößt, sondern darüber hinaus sogar dazu beiträgt, dass die NSA, aufgrund der nicht zu bewältigenden Datenmenge, an Effizienz und Sicherheitskompetenz einbüßt. Es wird dabei argumentiert, dass es zwar funktionale Alternativen zum vorherrschenden System gäbe – eine wird dabei skizziert – jedoch von Seiten der NSA keine Bestrebungen vorhanden sind, die einmal erhaltenen Befugnisse und Kompetenzen wieder einzuschränken. Im Gegenteil, so weckte der Datenbestand bereits Begehrlichkeiten anderer Einrichtungen, die diesen für ihre Zwecke heimlich missbrauchten.

Keywords

NSA; Massenüberwachung; PRISM; Metadaten; Target Development and Discovery

From Anonymity to Identification

A. Michael Froomkin

Abstract

This article examines whether anonymity online has a future. In the early days of the Internet, strong cryptography, anonymous remailers, and a relative lack of surveillance created an environment conducive to anonymous communication. Today, the outlook for online anonymity is poor. Several forces combine against it: ideologies that hold that anonymity is dangerous, or that identifying evil-doers is more important than ensuring a safe mechanism for unpopular speech; the profitability of identification in commerce; government surveillance; the influence of intellectual property interests and in requiring hardware and other tools that enforce identification; and the law at both national and supra-national levels. As a result of these forces, online anonymity is now much more difficult than previously, and looks to become less and less possible. Nevertheless, the ability to speak truly freely remains an important 'safety valve' technology for the oppressed, for dissidents, and for whistle-blowers. The article argues that as data collection online merges with data collection offline, the ability to speak anonymously online will only become more valuable. Technical changes will be required if online anonymity is to remain possible. Whether these changes are possible depends on whether the public comes to appreciate value the option of anonymous speech while it is still possible to engineer mechanisms to permit it.

Keywords

Internet, Privacy, Anonymity, Surveillance, Speech

Im Netz der Geheimdienste – strafrechtliche Aspekte der Massenüberwachung im Internet

Kai Cornelius

Abstract

Die anlasslose Ausspähung der Allgemeinheit im Internet ist aufgrund der Bedrohungsszenarien durch den internationalen Terrorismus und unterstützt durch die rasante technologische Entwicklung in einem bislang unvorstellbaren Maße ausgeufert. Dieser Beitrag untersucht anhand von drei Szenarien mit einem Bezugspunkt zu Deutschland, ob diesbezüglich eine Strafverfolgung in Betracht kommt. Dies betrifft die Vorbereitung des Eindringens in informationstechnische Systeme (mit einem Szenario zu *Treasuremap*), das Eindringen selbst (mit einem Szenario zu *Regin*) und die strategische

Telekommunikationsüberwachung des Bundesnachrichtendienstes (BND) mit einem Szenario zu *Eikonal*. Außerdem wird anhand dieser Ausführungen die Frage erörtert, ob das geltende Recht neu auszurichten ist. Dabei werden einerseits sicherheitspolitische Aspekte, aber andererseits auch der Schutz des Bürgers vor einer allumfassenden Überwachung in einem angemessenen Ausgleich berücksichtigt.

Keywords

Telekommunikationsüberwachung, Fernmeldegeheimnis, Strafbarkeit, Rechtfertigung, Verbotsirrtum

Die materiellen Ursachen des Cyberkriegs. Cybersicherheitspolitik jenseits diskursiver Erklärungen

Myriam Dunn Cavelty

Abstract

Optimisten des Informationszeitalters sprachen Staaten jahrelang die Fähigkeit ab, ihre Macht im virtuellen Raum entfalten zu können. Jüngste Entwicklungen in der internationalen Politik zeigen jedoch, dass das Gegenteil zutrifft: Der Cyberspace wird mittlerweile von einer wachsenden/Mehrheit (Zahl) staatlicher Akteure als strategische Domäne angesehen, deren Weiterentwicklung und Steuerung nicht mehr nur nichtstaatlichen Akteuren überlassen werden kann. Staaten begegnen den von ihnen zunehmend ernst genommenen Cyberunsicherheiten, indem sie im Namen der nationalen Sicherheit mit wachsender Durchsetzungskraft Aspekte des virtuellen Raums ihrer Kontrolle unterwerfen. Vor dem Hintergrund dieser Zuspitzung analysiert dieser Beitrag spezifische Unsicherheitsfaktoren, die staatliches Handeln im Namen der nationalen Sicherheit im Cyberspace erklären und geht auf sich daraus ergebende Konsequenzen ein. Im Gegensatz zu der bisherigen Forschung in den Politikwissenschaften wird das Argument entwickelt, dass es nicht nur diskursive Prozesse in der Form von Sprechakten sind, die eine verstärkte Verknüpfung des Cyberspace mit der nationalen Sicherheit vorantreiben, sondern auch grundlegende technisch-materielle Faktoren und Praktiken, die sich der sozialwissenschaftlichen Forschung bisher weitgehend entziehen. Diese Dimension sollte vermehrt beachtet werden, wenn wir politische Cybersicherheitsprozesse und ihre Konsequenzen umfassender verstehen wollen.

Keywords

Cyberkrieg, Cybersicherheit, Kopenhagener Schule, Gouvernmentalität, „material turn“

Wer regiert das Internet? – Sechs Thesen und einige Tendenzen

Sebastian Harnisch und Wolf J. Schünemann

Abstract

Das Kapitel analysiert die Ergebnisse von zwölf Vorträgen zum Regieren im und für das Internet in theoretischer Absicht. Basierend auf den fachdisziplinären Untersuchungen werden in Thesenform die Wechselwirkungen zwischen technologischer Entwicklung, politischer Regulation und Selbstregulierung der Nutzer kritisch diskutiert. Wir argumentieren, dass die verspätete Politisierung des Netzes auf den dynamischen technologischen Wandel und komplexere Interessensbildungsprozesse zurückgeführt werden kann. Diese Konstellationen bewirken, dass die Kommunikationsgewinne einzelner Nutzer nicht immer nur demokratisierend wirken, sondern durch staatliche Eingriffe und Manipulation auch erfolgreich zur Stabilisierung autokratischer Herrschaft genutzt werden. Neben staatlichen Eingriffen verändern Internetanbieter das Verhalten der Nutzer, indem sie deren Daten und Verhaltensprofile in einer dynamisch wachsenden Internetökonomie feilbieten, die den Netizen primär zum „Prosumenten“ werden lassen. Ökonomische Interessen und sicherheitspolitische Risiken bewirken sodann, dass Regierungen verloren geglaubte Regulierungsmöglichkeiten reklamieren, um Internetkriminalität und Angriffe auf IT-basierte kritische Infrastrukturen zu verhindern. Unsere Überlegungen zeigen schließlich, dass Regierungen selbst den Cyberspace zur Unterstützung konventioneller Kriegsführung und Angriffe auf strategische Infrastruktur nutzen, eine virtuelle Kriegsführung zur Ausschaltung eines realen Gegners oder Eroberung von Territorium findet aber weiterhin nicht statt.

Keywords

Netzpolitik, Internet Governance, Datenschutz, Cybersicherheit, Massenüberwachung

The **Journal of Self-Regulation and Regulation** is an open-access peer-reviewed journal serving as a potential outlet for edge-cutting interdisciplinary research on regulatory processes in individuals and organizations. It is published by the research council of Field of Focus 4 (FoF4) of Heidelberg University. The research council stimulates and coordinates interdisciplinary activities in research and teaching on self-regulation and regulation as part of the university's institutional strategy "Heidelberg: Realising the Potential of a Comprehensive University", which is funded by the Federal Government as part of the excellence initiative.

The *Journal of Self-Regulation and Regulation* publishes two volumes per year, regular volumes containing selected articles on different topics as well as special issues. In addition, the reader will be informed about the diverse activities of FoF4, uniting scientists of the faculty of behavioural and cultural studies, the faculty of social sciences and economics, as well as the faculty of law.

Imprint

Journal of Self-Regulation and Regulation Volume 01 (2015)

Research Council of Field of Focus 4, Heidelberg University
Forum Self-Regulation and Regulation
Hauptstr. 47–51
69117 Heidelberg, Germany

Fon: +49 (0)6221 / 54 – 7122
E-mail: fof4@psychologie.uni-heidelberg.de
Internet: https://www.uni-heidelberg.de/fof4

Publisher: Research Council of Field of Focus 4, Heidelberg University
Spokesperson: Sabina Pauen, Department of Psychology
Guest Editors: Wolf J. Schünemann, Department of Political Science
Sebastian Harnisch, Department of Political Science
Editorial Team: Melanie Bräunche, Sabine Falke

You can download the volumes of the *Journal of Self-Regulation and Regulation* free of charge at:
http://journals.ub.uni-heidelberg.de/index.php/josar/index

Contents

Publisher
Research Council of Field of Focus 4: Self-Regulation and Regulation, Heidelberg University