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

UNIVERSITÄT
HEIDELBERG
ZUKUNFT
SEIT 1386

Journal of Self-Regulation and Regulation

Volume 01 (2015)

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

DOI: 10.11588/josar.2015.0.23487

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.initiatived21.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

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