Internet und Souveränität

Thiel, Thorsten

Preprint / Preprint
Sammelwerksbeitrag / collection article

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:
Hessische Stiftung Friedens- und Konfliktforschung (HSFK)

Empfohlene Zitierung / Suggested Citation:
Thiel, T. (2014). Internet und Souveränität. In C. Volk, & F. Kuntz (Hrsg.), *Der Begriff der Souveränität in der transnationalen Konstellation* (S. 215-239). Baden-Baden: Nomos. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-56142-3

Internet und Souveränität

Thorsten Thiel

> „Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather" (Barlow 1996).

Diese berühmten und viel zitierten Eingangssätze aus der 1996 von Perry Barlow veröffentlichten *Declaration of the Independence of Cyberspace* stehen emblematisch für eine über viele Jahre populäre Sichtweise auf das Internet. Sie wurden geschrieben in einer Stimmung und zu einer Zeit, als die Bedeutung des Staates und mit ihr das Konzept der Souveränität als im Schwinden begriffen wurden. Es galt nur noch als Frage weniger Jahre, bis sich andere Ordnungsmuster soweit würden durchgesetzt haben, dass souveräne Staatlichkeit als Anachronismus in den Geschichtsbüchern verschwände. Knapp zwanzig Jahre später wirkt diese Sichtweise selbst wie ein Anachronismus: Nicht zuletzt die Snowden-Enthüllungen haben überdeutlich gemacht, dass das Internet kein Raum ist, aus dem Staatlichkeit und Souveränität so einfach auszuschließen wären. Nunmehr wird die gesellschaftliche Vorstellung dominiert durch ein Bild, in dem digitale Kommunikation als der Türöffner erscheint, vollständige Überwachung zu realisieren. Der digitale Raum wird als ein Ort der Hypersouveränität gesehen, in dem alle Machtstrategien moderner Staatlichkeit kulminieren und die demokratische Zähmung der Souveränität verloren zu gehen droht. Beide Positionen zeigen zunächst einmal eins: Der *Cyberspace* ist ein politischer Raum und sollte auch als solcher thematisiert werden.

Wenn dies im Folgenden geschieht und genauer seziert wird, wie *Internet* und *Souveränität* diskursiv in ein Verhältnis gesetzt werden, so ist das Ziel der Ausarbeitung nicht, eine abgeschlossene Definition eines der beiden Konzepte zu liefern oder eine theoretische Großdeutung zu unternehmen, in welche Richtung sich *das* Netz oder *die* Souveränität entwickeln wird.[1] Vielmehr soll in der Aufarbeitung und Systematisierung der Debatte(n)

[1] In dieser Untersuchung werden die beiden zentralen Konzepte – Internet und Souveränität – nicht vorab bestimmt. Bezüglich des Internetbegriffs verwende ich ein sehr weites Verständnis, welches sich nicht nur auf das weltweite Computernetzwerk als technische Infrastruktur bezieht, die durch die Nutzung des TCP/IP Protokolls Datenübertragung und Datenaustausch ermöglicht, sondern auch den gesamten Bereich der Ideen und Kommunikationen dahinter meint, wie er unter dem noch abstrakteren und hier synonym verwendeten Begriff

aufgedeckt werden, welche begrifflichen Perspektiven im Netzdiskurs auf Souveränität eingenommen werden, wie sich diese Perspektiven verändern und wie sie zueinander in Beziehung stehen. Drei Dimensionen der netzpolitischen Debatte(n) werden dabei analytisch unterschieden: Erstens, die Debatte um die politische Ordnung als solche und damit die Idee, dass Netzwerke als Ordnungsform jene Ordnungsform ablösen, die mit Staatlichkeit, Souveränität und Hierarchie gleichgesetzt wird. Zweitens die Debatte um Recht und Rechtsdurchsetzung, in einer sich ins Virtuelle entziehenden, unweigerlich globalisierten Welt. Drittens, die Debatte um Staatlichkeit und Gewalt im Netz, mit den Manifestationen von *Cyberwar* und *Cyberterrorismus* und dem Versuch souveräne Kontrolle im digitalen Raum zu etablieren.[2] Die drei Debatten oszillieren dabei zwischen akademischer Auseinandersetzung und öffentlichem/politischem Diskurs, was jeweils in den Ausführungen mit reflektiert werden soll.[3]

In allen drei hier untersuchten Debattensträngen sind es dabei zunächst ähnliche Vorstellungen von Dezentralität, Globalität und Anonymität, die die Diskussion um die Auflösung geographisch bestimmter Räume in Gang bringen. Aus diesen werden Rückschlüsse auf den Wandel von Hierarchie, Staatlichkeit, Kontrolle oder Gewalt gezogen, was sich jeweils in der Hypothese verdichtet, dass das Internet das Grundprinzip von Staatlichkeit in Frage stellt (den Staat als einheitlich verfassten und kontrollierten Raum und damit als souveräne Entität). Über diese Ausgangshypothese hinausgehend werde ich aber für jede der drei Debatten nachzeichnen, wie die Argumente, Einschätzungen und empirischen Beobachtungen sich in sehr unterschiedliche Richtungen differenziert haben. Aus den drei Einzelbetrachtungen entsteht so ein Panorama, welches nicht nur eine lokale Sortierung und Systematisierung des Netzdiskurses darstellt, sondern auch auf die weitere Debatte um Transnationalisierung und Souveränität verweist. Das Internet steht dabei nicht nur als Beispiel für Entgrenzungs- und Wandlungsprozesse, sondern digitale Vernetzung selbst stellt eine treibende Kraft in Transnationalisierungsprozessen und der Neuformierung normativer Ordnungen dar. Dies zu reflektieren und die Beobachtungen

---

Cyberspace eingeschlossen ist. Souveränität wird hingegen gar nicht vorab zu umgrenzen, sondern direkt aus der Verwendung in den untersuchten Debatten abzulesen versucht.

[2] Es gibt selbstverständlich noch weitere souveränitätsrelevante Debatten, etwa jene um die Regulierung von Privatheit oder die Definition von Eigentum. Solche Debatten aber, in denen der Begriff der *Souveränität* eher indirekt eine Rolle spielt, sollen aus Platzgründen ausgespart bleiben. Ebenfalls ausgeblendet werden Untersuchungen, die über das Internet als öffentliches digitales Netzwerk hinausgehen und etwa durch die Digitalisierung hervorgebrachte private digitale Netzwerke (etwa in der Finanzindustrie) in den Blick nehmen. Eine Untersuchung, die beide Formen im Blick hat, ist: Sassen (2006).

[3] Dies zumal, weil ich davon ausgehe, dass die Weise, wie und mit welchen Begriffen wir uns den abstrakten Raum des Digitalen vorstellen, mitbestimmt wie sich unser normatives Verständnis von diesem Raum entwickelt. Vgl. Singh (2013) für eine Studie zur begriffsformenden Wirkung des Internetdiskurses als *Meta-Power*.

im weiteren Rahmen der politikwissenschaftlichen Souveränitätsdiskussion einzuordnen, schicken sich die abschließenden Bemerkungen des Artikels an.

1. *Das Netz als Netzwerk: Eine alternative Ordnung des Politischen*

Die erste Dimension der netzpolitischen Debatte um Ordnung und Souveränität ist jene, die den Wandel sozialer Praktiken und Ordnungsmuster in den Fokus rückt und die bereits im Eingangszitat des Artikels angesprochen wurde. Hierin werden die emergenten Praktiken digitaler Selbstorganisation abgegrenzt von Souveränität als einer hierarchisch stratifizierten Form der Organisation von Gesellschaft. Die plakative Feststellung, dass „the world of bits is not the same as the world of atoms" (Johnson et al. 2004: 6), dient als Ausgangspunkt, um die Legitimität von Regierungsformen auf den Prüfstand zu stellen: „We reject: kings, presidents and voting. We believe in: rough consensus and running code" (Clarke 1992).

Die Diskussion hat zunächst einen technischen Ursprung, der im Verständnis des Netzwerks als nicht-hierarchischer Ordnungsform begründet ist.[4] Diese Sichtweise formt die Überzeugungen der frühen Netzpioniere, die eine mal libertäre, mal hippieske, mal technokratische, stets aber anti-autoritäre Erwartung an die Entwicklung des Politischen im Zuge der Ausweitung digitaler Kommunikation formulieren[5]. Von der Architektur des Netzes wird angenommen, dass sie in besonderer Weise der Realisierung politischer Freiheit entgegenkommt. Durch sie könne man auf zentralisierte Infrastrukturen verzichten und sei in der Lage, bedarfsgerechte und spontane Assoziationen zu bilden. Auch wird erwartet, dass die Risiken von Kontrolle, Machtmissbrauch und Monopolbildung durch Netzwerke effizient gemindert werden. Diese gelten als variable und vielgestaltige Entitäten, die Heterogenität durch Verbindung ermöglichen, anstatt, wie der Staat, auf Schließung und Homogenität setzen zu müssen.[6] Netzwerke würden so den Anforderungen moderner Gesellschaften weit eher gerecht als sämtliche traditionelle Formen der politischen Organisation.[7] Souveräne Staatlichkeit wird als eine Krücke interpretiert, die zu einem

---

[4] Begrifflich fällt hier eine Resonanz mit politikwissenschaftlichen Debatten auf, in denen eine Dreiteilung von Regierung, Markt und Netzwerken eine hohe Verbreitung gefunden hat. Gerade in der *Global-Governance*-Debatte der 90er Jahre wurde dabei die Netzwerk-Form normativ wie funktional häufig präferiert. Während die politikwissenschaftliche Netzwerkdebatte jedoch hauptsächlich auf die Einbindung advokatorischer, privater Organisationen in die Zusammenhänge komplexen Regierens untersucht, ist die Debatte um technische Netzwerke mehr auf den Einbezug von Individuen konzentriert.

[5] Zur Geschichte dieser Verbindung vgl. Turner (2006).

[6] Zur medientheoretischen Einsortierung des Netzwerksbegriffs und der Entwicklung des Internets vgl. Warnke (2011).

[7] Die Entgegensetzung der organischen Metapher von Staatlichkeit mit der ephemeren Metapher von Netzwerken wird in einer anschaulichen Weise am Ende der Betrachtung zur Metapher des Staatskörpers von Koschorke et. al. (2007) artikuliert. Popularisiert wurde die Netzwerkmetapher natürlich zudem durch Manuel Castells (2010) Arbeiten zur Netzwerkgesellschaft, wobei diese zwar das Organisationsprinzip und dessen verändernde Kraft hochhalten,

bestimmten historischen Zeitpunkt notwendig gewesen sein mag, um Probleme kollektiven Handelns in großen Gesellschaften zu überwinden, die jedoch ihre Pflicht getan habe und die nun, da sie strukturell unvereinbar sei mit Demokratie und Freiheit, verworfen werden müsse.[8] Jetzt, da die Möglichkeit existiere, Gesellschaft mittels technischer Mittel anders und gerechter, nämlich dezentral, zu organisieren, sei Souveränität als Ordnungsprinzip verzichtbar: „The world's information is being liberated, and so, as a consequence, are we" (Katz 1997).

Fraglos ist das in diesem Verständnis artikulierte Bild von Souveränität unterkomplex, dessen normative Wertung einseitig und wenig reflektiert. Doch ist hier zunächst einmal interessant, welche Elemente als anti-souverän identifiziert und unmittelbar mit charakteristischen Eigenschaften digitaler Kommunikation (in Abgrenzung zu analoger Kommunikation) in Verbindung gebracht werden. Diese sind: Die Erreichbarkeit großer, nicht festgelegter Gruppen ohne Angewiesenheit auf Gatekeeper; die Möglichkeit der verlustfreien Speicherung und Vervielfältigung von Kommunikationsinhalten; die Marginalisierung von Kosten für Kooperation, Austausch und Information; die Übermittlung, Verarbeitung und Filterung von sehr großen Mengen an Informationen in sehr kurzer Zeit und die Reduktion der Bedeutung räumlicher Faktoren. Durch diese Merkmale digitaler Kommunikation sollen variable Verbindungen nahezu beliebiger Zahl und Ausdehnung möglich werden, was Individuen von der Abhängigkeit zentraler Koordinationsstellen befreit und sich unmittelbar in Selbstbestimmung übersetzen lassen soll. Die Idee einer *per definitionem* liberalen, dezentralen Netzwerkarchitektur, in der man sich, zudem durch Maßnahmen wie Anonymität und Verschlüsselung, aktiv und wirkungsvoll gegen den Staat zu wehren können weiß, wird dabei durch das Schlagwort der horizontalen Vernetzung mit Demokratie gleichgesetzt.

Als technische Utopie hatte diese Vorstellung von der Wirkung digitaler Netzwerke nicht lange Bestand. Zu offensichtlich ist, dass ungeachtet der potentiellen Qualitäten von Netzwerken eine Vielzahl von Wirkungen existiert, die die nivellierend-egalitäre Qualität konterkariert: So sind digitale Netzwerke schon deshalb weit weniger inklusiv als propagiert, da Zugangschancen in hohem Maße durch technische Ausstattung und Kompetenz bestimmt sind - *digital divide* (Jacob/Thomas 2014). Gewichtiger noch ist, dass die Entwicklung dezentraler Netzwerke Impulse für eine weitreichend ökonomische Umformung dieser Netze gesetzt hat, die wiederum

---

Netzwerke jedoch sehr umfassend soziologisch verstanden und nicht diametral der souveränen Staatlichkeit entgegengesetzt werden. Auch im weiteren Internetdiskurs findet diese Entgegensetzung häufig eher implizit statt.

[8] Besonders drastisch drückt dies Nicholas Negroponte aus, wenn er schreibt: „Like a mothball, which goes from solid to gas directly, I expect the nation-state to evaporate without first going into a gooey, inoperative mess, before some global cyberstate commands the political ether. Without question, the role of the nation-state will change dramatically and there will be no more room for nationalism than there is for smallpox." (Negroponte 1996: 238)

der Egalität von Netzwerkstandards entgegenwirken. Zentrale Server – wie beispielsweise Suchmaschinen – gewinnen durch die exponentiell ansteigende Komplexität und deren notwendige Reduktion auch in völlig offenen Netzwerkarchitekturen disproportional an Bedeutung. Die Entwicklung des Internets zeigt daher alsbald monopolistische Tendenzen, welche wiederum Anreize zu einer immer stärkeren staatlichen und wirtschaftlichen Regulierung setzen (Goldsmith/Wu 2006; Wu 2010b). Die Refinanzierungszwänge der keineswegs kostenlosen Netzwerkarchitektur bringen ökonomische Strategien hervor, die eine deutliche Abkehr von den Prinzipien des dezentralen Netzwerks bedeuten.[9] Dies führt zu einer hochgradig stratifizierten Wirklichkeit des Netzes, die die normativ aufgeladene Behauptung der Egalität horizontaler Netzwerke gegenüber vertikaler Souveränität naiv erscheinen lässt.

Auf einer allein technischen Basis lässt sich das Argument des Netzwerks als Alternative zu staatlicher Souveränität daher bereits früh nicht mehr halten. Und doch stellt die Ernüchterung nicht das Ende der Debatte dar. Vielmehr taucht die Entgegensetzung von Staat und Netzwerk in (mindestens) zweierlei Debatten – wenn auch in modifizierter, sehr viel moderaterer Form – wieder auf: Im Diskurs um die durch soziale Netzwerke entstehende Selbstorganisationsfähigkeit gesellschaftlicher Gruppen (1) und in der Auseinandersetzung um die Foren der politischen Regulierung des Internets (2).[10]

1) Der Aufschwung sozialer Netzwerke ist eines der zentralen Kennzeichen der Entwicklung des Internets in den 2000er Jahren. Chiffren wie *Web 2.0* oder *Social Media* bringen dabei die Überzeugung zum Ausdruck, dass Vernetzung sich in die Richtung Kollaboration und Interaktion bewegt.[11] *Many-to-many*-Kommunikation, wie sie von Howard Rheingold (Rheingold 2002) und Clay Shirky (Shirky 2008) beschrieben wurde, gilt als zentrales Merkmal digitaler

[9] Nach Jaron Lanier (2013) ist es das Zusammenspiel von freier Netzwerkideologie und dem Anwachsen von Verarbeitungskapazitäten, welche das Aufkommen sogenannter *Sirenen*-Server möglich gemacht hat. Sirenen-Server sind Spitzen eines Netzwerks, die aufgrund überlegener Verarbeitungskapazität, extreme Informationsasymmetrie schaffen und damit Kommerz und Kommunikation nach Belieben zu dominieren in der Lage sind. Eine ebenfalls die dezentrale Infrastruktur problematisierende, aber nicht ökonomische, sondern von Netzwerksicherheit geprägte Diagnose stellt Jonathan Zittrain (2009). In der deutschen Diskussion hat Sascha Lobo (2014) im Anschluss an die Snowden-Leaks und mit großem öffentlichen Nachhall das Ende der Internet-Utopie ausgerufen.

[10] Etwas weniger auf die Produktion kollektiv verbindlicher Entscheidungen abstellend, jedoch ebenso politisch und gesellschaftlich weitreichend sind Arbeiten, die sich über die Veränderung von Arbeit, Wertproduktion und Eigentum Gedanken machen, allen voran Yochai Benklers (2006) enorm einflussreiches *The Wealth of Networks*. Ich werde aus Platzgründen in diesem Aufsatz diese Linie von Texten ganz aussparen, ihre diagnostische Kraft wie ihre Bedeutung für den Internetdiskurs als Ganzen dürften aber beispielsweise die Diskussionen um Politisierung durch soziale Netzwerke deutlich übertreffen.

[11] Soziale Netzwerke sind sehr viel zugänglicher als die Netzwerkarchitektur des *Web 1.0*. Die technischen Hürden massenhafter Beteiligung sind in ihnen reduziert, auch die Komplexität von Kommunikation wird durch die Unterstützung von Algorithmen tendenziell gebändigt. Allerdings werden diese Vorzüge auf Kosten der dezentralen Grundstruktur realisiert. Eine Vielzahl der Eigenschaften, die die *demokratisierende* Wirkung des Internets im ursprünglichen Diskurs begründet haben, sind in der kommerziellen Struktur sozialer Netzwerke nicht vorhanden oder haben sich ins Gegenteil verkehrt, beispielsweise der (weitgehende) Verzicht auf Anonymität, die Abhängigkeit von zentralen Plattformen oder die Neutralität der Informationsselektion.

Kommunikation und wird in Verbindung gebracht mit einer Vielzahl demokratietheoretischer Diagnosen über die Wirkungen des Internet. Im Kontext der hier analysierten Souveränitätsdebatte sind dabei vor allem jene Ansätze interessant, die über einen reformistischen Blick hinaus gehen und das Netz als Raum der Realisierung alternativer Ordnungsmodelle interpretieren. Hierbei wird zumeist die Möglichkeit zivilgesellschaftlicher Selbstorganisation jenseits etablierter Autoritäten stark gemacht und das Potential für sozialen Protest gegen eben jene Autoritäten betont. Die Renaissance politischer Protestbewegungen und deren Wandel zu präfigurativen – nicht themenbezogenen, sondern Plattformen schaffenden (zumal häufig transnationalen) – Organisationsformen wird unter Rückgriff auf die gestiegenen Organisationsmöglichkeiten durch Vernetzung erklärt.[12] Der Anspruch, eine demokratische Alternative zum souveränen Nationalstaat wie zur kapitalistischen Wirtschaft zu schaffen, wird hier direkt mit der Organisation durch digitale Netzwerke verknüpft:

> „[…] in order to think democracy within networks, it is necessary to develop in conceptual and practical ways idioms for non- or post-representative democracy. Such a task does not abandon the concept or possibility of democracy, but rather it recognizes democracy as an ongoing project that, in a historical sense, is an idiom that has undergone numerous transformations" (Rossiter 2006: 51).

Eine Vorstellung, die auch deshalb von großer Popularität ist, da Ereignisse wie der arabische Frühling oder die Aktivitäten von WikiLeaks oder Anonymous unter dieser Theorieperspektive ausgedeutet wurden. Auch die ganz allgemeine Erwartung, dass das Internet demokratisch-zivilgesellschaftliche Tendenzen fördert und für autoritäre Regime eine Gefahr darstellt, speist sich aus solchen Überlegungen. Freie Netzkommunikation gilt hier als Antithese zu den geschlossenen Strukturen autoritärer Staatlichkeit.[13]

In dieser Weise das Netz als demokratiefördernde Alternative zur staatlich-repräsentativen Demokratie zu verstehen, ist charmant und hat doch viel und zu Recht Widerspruch geerntet. Die Annahme, dass Instrumente zur Selbstorganisation quasi automatisch das Potential von Macht und Dominanz verringern oder gar eine emanzipatorische Alternative zur Organisation der Demokratie darstellen, blendet eine Vielzahl von Risiken und Manipulationsmöglichkeiten

[12] Theoretische Analysen in Bezug auf das *radikaldemokratische* Potenzial des Medienwandels finden sich in: Dahlberg/Siapera (2007); stärker empirisch-sozialwissenschaftliche, jedoch insgesamt zurückhaltendere Einschätzungen liefern zum Beispiel: Bennett (2003); Bennett/Segerberg (2013), Juris (2012), Earl/Kimport (2011), Castells (2012).

[13] Empirische Untersuchungen haben jedoch schon länger nachgewiesen, dass diese Sichtweise differenziert werden muss und insbesondere auf die ebenfalls ansteigenden Kontroll- und Manipulationsmöglichkeiten verwiesen. Vgl. etwa: Kalathil/Boas (2003); Morozov (2011); Howard (2010); Deibert et al. (2008, 2010, 2012).

aus. Schon vor dem Bekanntwerden der umfangreichen Spionageprogramme westlicher Geheimdienste gab es eine Vielzahl empirischer Evidenzen, dass die Kommunikation über soziale Netzwerke keineswegs von Machtrelationen entkoppelt ist und es eine große Zahl von Möglichkeiten der Beeinflussung und Manipulation in und durch diese Instrumente gibt.[14] Ohne diese sehr umfangreiche Literatur hier umfassend würdigen zu können, sei zudem auch noch auf das sehr eindimensionale Verständnis von Demokratie in diesen Ansätzen verwiesen. Dieses erschöpft sich hauptsächlich in der Annahme, dass umfangreiche Partizipationsmöglichkeiten egalitäre Partizipation hervorbringen und dauerhaft zu erhalten imstande sind. Weder wird darin ernst genommen, dass Partizipation auch zu Apathie, Kritik und Fragmentierung führen kann, zudem schwierig über Zeit aufrecht zu halten ist und in vielen Politikfeldern unwahrscheinlich und sehr anspruchsvoll ist, noch wird die prozedurale Logik repräsentativer Demokratie und das Konzept von Bürgerschaft und Wahlen in ihren Vorzügen analysiert. So aber wird ein triviales Ausspielen von repräsentativer Demokratie/souveränem Staat gegen horizontale Basisdemokratie versucht, das zwar zunächst viel Aufmerksamkeit erzeugt, aber die Defizite einer aktivistischen Demokratiekonzeption nicht hinreichend erfasst.

2) Demokratietheoretisch unambitionierter und weniger normativ aufgeladen, nichtsdestotrotz aber höchst aufschlussreich im Bezug auf den Wandel von Staatlichkeit und die Wirkungen des Internets, ist der Diskurs um *Internet Governance*. *Internet Governance*, die Entwicklung und Anwendung geteilter Normen, Regeln und Prozeduren zur Pflege und Entwicklung des Internets, hat sich in einer Weise entwickelt, in der privaten Akteuren und technokratisch legitimierten Eliten eine hervorgehobene Rolle zukommt (Mathiason 2009; Hofmann 2005; 2009; DeNardis 2013). Gerade in der Frühphase des Netzes wurde angenommen, dass dieses als globales Phänomen in einer Weise reguliert werden müsse, die von großer Neutralität zeuge. Anders könne der nötige Konsens für die Weiterentwicklung überhaupt nicht erreichen werden. Hieraus wird die Notwendigkeit einer schwachen, entpolitisierten Rolle souveräner Staaten gefolgert, da diese ansonsten mit ihren kurzsichtigen, egoistischen Interessen die Ausweitung von Netzwerken behindern würden.[15] Auch in diesem Debattenstrang wird also diskursiv die Opposition von Netzwerklösungen und Staatlichkeit/Souveränität zu erzeugen gesucht.[16] Es wird ein Regime porträtiert, welches sich abhebt von den etablierten Institutionen und welches Transnationalität

[14] Vgl. nur die einflussreichen Diagnosen: Morozov (2011) und Lovink (2012).
[15] Es sei direkt eingewendet, dass diese Beschreibung übersieht, dass gerade die westlichen Staaten ein Interesse an der Konstruktion hatten und haben und man argumentieren kann, dass sie stets über eine indirekte Kontrolle verfügten, vgl. Drezner (2004).
[16] Das zentrale Buch, das sich mit der Unterscheidung und den Fallstricken/Simplifizierungen auseinander setzt und die komplexe Konstellation moderner *Internet Governance* differenziert darstellt, ist: Mueller (2010); vgl. zudem Ziewitz/Pentzold (2012) für einen Überblick über wissenschaftliche Ordnungsversuche des analytischen Felds.

an die Stelle staatsdominierter Internationalität setzt. Zugleich wird die Gefahr betont, die droht, wenn souveräne Staaten mehr Einfluss auf die Netzentwicklung erhalten - *die Balkanisierung des Netzes* (Grassegger 2014).

Das Bemühen, funktionalistische und normative Argumente für die Prävalenz der Netzwerkform vorzubringen (Reagle 1999), stößt aber schon deshalb auf Schwierigkeiten, da im Zuge der stark wachsenden politischen und ökonomischen Bedeutung des Netzes seit Mitte der 90er Jahre, die Leistungsfähigkeit und Effektivität der zunächst etablierten Institutionen an ihre Grenzen stößt und zugleich starke Gegenkräfte erwachsen. Nationalstaaten – autoritäre wie liberale – versuchen in zunehmendem Maße auf die Entwicklung und Regulierung des Internets Einfluss zu nehmen, die vormals gewahrte Diskretion nimmt ab und es gibt vielfältige Versuche zu *klassischen* Formen zwischenstaatlicher Aushandlung zurückzukehren.[17] Auch ist die Beteiligung zivilgesellschaftlicher Akteure in den entstandenen Governance-Arrangements sehr viel skeptischer und differenzierter zu sehen als zunächst propagiert und stellt sich bei näherem Hinsehen, nach Meinung vieler Beobachter, als Feigenblatt oder gar Einfallstor für Elitenkontrolle heraus (Dany 2012; Chenou 2014). Die beiden Formen – Netzwerk und Hierarchie – erweisen sich also auch in dieser Perspektive nicht als ausschließende oder normativ eindeutige Optionen, sondern als überlappend und ambivalent. Das sich derzeit etabliert habende Set an Institutionen ist äußerst umkämpft und ob es als Erfolgsmodell gelten darf, ist umstritten (DeNardis 2014). In jedem Fall lässt sich aber sagen, dass Souveränität durch die emergenten Institutionen der *Internet Governance* nicht als Konzept gefährdet ist. Maximal unterliegt die Art, wie Staaten Einfluss nehmen, einem gewissen Wandel (nicht einmal unbedingt einer Schwächung). Dieser Wandel zeichnet sich allerdings ganz allgemein in der internationalen Politik ab und er ist mit der post-westfälischen Situation und dem *Governance*-Begriff schon in anderen Zusammenhängen umfassend beschrieben (Shahin 2007).

In der nunmehr zunächst abgeschlossenen Betrachtung der Verzweigungen des ersten Strangs der Internetdebatte hat sich gezeigt, dass die auf die Ordnungsform des Netzwerks bezogenen Ansätze zwar mittels der dichotomen Abgrenzung von Netzwerk zu Souveränität viel Aufmerksamkeit erzeugen konnten, die Behauptung von Andersheit und Überlegenheit jedoch nach und nach zurückgenommen werden musste. Dies liegt zum einen daran, dass das Netz selbst sich verändert hat. Die dem Netzwerk zugeschriebenen egalisierenden Eigenschaften sind unter dem Druck von Kommerzialisierung und zunehmender staatlicher Regulierung weniger

[17] Drezner (2004); zur speziellen Rolle von *rising powers* in diesem Kontext vgl. Ebert/Maurer (2013).

beständig, als dies von den Pionieren des Netzes prognostiziert wurde.[18] Zum anderen muss aber eine (normative) Überschätzung des Netzwerkkonzepts konstatiert werden, da dieses keineswegs einfach mit Horizontalität und Partizipation gleichgesetzt werden darf und wesentlich anfälliger für Dominanzrelationen ist als zunächst behauptet. Der sich vollziehende mediale und gesellschaftliche Wandel ist insofern zwar tiefgreifend, seine normative Bewertung muss aber sehr viel differenzierter erfolgen. Die in der Debatte vollzogene Hochrechnung einzelner Entwicklungen auf das zu erwartende Ganze der neuen Ordnung hat zu einer Überschätzung von Ausmaß und Art des Wandels geführt und ist gegenwärtig einer Ernüchterung gewichen, die just in jenem Moment besonders schwer wiegt, wo viele positive Errungenschaften des Netzes tatsächlich auf der Kippe stehen und sich die Tendenz zur Schließung der offenen Strukturen durchzusetzen droht (Wu 2010b).

2. *Das Netz als Rechtsraum: Territorialität und Regulierung*

Neben der ordnungstheoretischen Dimension lassen sich noch zwei weitere Debatten unterscheiden, die die gesellschaftlichen Veränderungen durch digitale Kommunikation als Herausforderung für das Konzept von Souveränität verstehen. In diesen ist es jedoch nicht das Netz als Alternative zum Staat, sondern die Frage der Adäquatheit der Bedingungen und Mittel souveräner Staatlichkeit, aus der die Argumente entstehen. In der ersten Debatte ist die Rolle von Recht und Territorialität der Aufhänger, in der zweiten die Frage nach Gewalt und Sicherheit.

Die Debatte, der wir uns nun zunächst zuwenden wollen, stellt das Verhältnis von *Cyberspace* und Rechtsraum in den Mittelpunkt. Sie wurde in der zweiten Hälfte der 90er Jahre virulent, als das Internet ein Massenphänomen wurde und dessen Einsatz sich aus dem ursprünglichen wissenschaftlichen und militärischen Kontext weitgehend löste und immer stärker in kommerzielle Zusammenhänge entwickelte, die weit stärkeren Regulierungserwartungen unterliegen. Technische Annahmen über das Wesen von Netzwerken sind auch hier zentral, allerdings ist es nicht die aus der Konnektivität gefolgerte Idee einer hierarchiefreien Selbstregierung, sondern die im Zusammenhang mit Globalität und Anonymität postulierte Unregierbarkeit des *Cyberspace*, die entscheidend ist.

Souveränität wird in dieser Debatte als eine politisch-rechtliche Praxis zwischen Staaten interpretiert. Eine Praxis, die eine räumliche Zuteilung von Zuständigkeiten voraussetzt und aus

[18] Es ist allerdings darauf hinzuweisen, dass viele der Vordenker des Internets nicht so deterministisch argumentieren, wie es heute oft dargestellt wird. Dass die technische Infrastruktur nur einen Impuls liefert, die soziale Formierung aber ebenso wichtig ist und gegen bestehende Mächte erkämpft und stetig erhalten werden muss, wird beispielsweise durch Lessig (2002); Rheingold (2002) und Shapiro (1999) ausgeführt.

historisch-funktionalen Gründen hauptsächlich als Steuerung durch Recht gedacht wird. Damit Souveränität in diesem Sinne funktionieren kann, ist es nötig, dass die Staaten jeweils selbstständig in der Lage sind, Recht zu kreieren und durchzusetzen. Rechtsräume und die Einflüsse aufeinander müssen deswegen entweder separiert oder hierarchisiert werden. Für überlappende Räume und Interdependenzen müssen Regime wechselseitiger Anerkennung oder Kollisionsregeln entwickelt werden, welche wiederum die Souveränität der einzelnen Einheiten bestätigen. Die effektive Kontrolle von Grenzen ist demzufolge unerlässlich.[19]

Genau dies aber ist einer frühen, zunächst aber sehr prominenten Diagnose zufolge unmöglich geworden. Das Internet wird als ein grenzenloser und folglich rechtsfreier Raum interpretiert. Der *Cyberspace* wird als Kollaps der Möglichkeit von Grenzziehung interpretiert (Vgl. Johnson/Post 1996; Post 2002; 2007; 2009; McGregor 1999; Lessig 2002). Zwei Gründe werden angeführt: Zum einen, dass die dezentrale Netzwerkarchitektur erlaubt, sich im Netz unerkannt und nicht lokalisierbar zu bewegen – in den Worten der berühmten, schon 1993 veröffentlichten Karikatur des New Yorkers: „On the Internet, nobody knows you're a dog" –, wodurch eine Attribution von Handeln und Verantwortung schwer bis unmöglich wird. Zum anderen, dass Kommunikation permanent, intentional oder nicht-intentional eine Vielzahl von Grenzen überschreitet und in konkurrierenden Rechtsräumen Bedeutung erlangt. Nationalstaatliche Regulierung müsse daher notgedrungen scheitern, der Versuch, sie trotzdem durchzusetzen, bringe repressive, zugleich aber ineffektive Ergebnisse hervor.[20]

Ähnlich wie schon in der Debatte um das Netz als eigenständige Ordnungsform zeigt sich auch in der Debatte um die Wirkung des Internets auf Recht und Grenzen bald, dass die anfänglichen Hypothesen unterkomplex und häufig irreführend sind. Zu schnell wird von angenommenen

[19] Diese explizit territoriale, durch Recht induzierte Dimension von Souveränität wird auch in einem hier nicht weiter zu verfolgenden Nebenstrang deutlich. Der Regulierung des Wirkens globaler Internetunternehmen. Durch den Umstand, dass diese Unternehmen verhältnismäßig wenige Arbeitskräfte beschäftigen oder lokal gebundene Ressourcen benötigen, können sie sich staatlichen Einflussnahmen verhältnismäßig wirkungsvoll entziehen. Die Politik steht daher immer wieder vor dem Problem, wie einzelne Ansprüche gegen die Firmen durchgesetzt werden können (diskutiert wird dies zum Beispiel mit Blick auf die Verantwortung großer Internetunternehmen für Inhalte zu haften, aktuell beispielsweise bezüglich des *Recht auf Vergessen*). Solche Probleme des Umgangs von Staaten mit großen privaten Unternehmen in einer globalen Wirtschaft sind allerdings nicht netzspezifisch, was sich auch daran zeigt, dass es hier viele Analogien zu den Bemühungen gibt, just diese Konzerne in nationale Steuersysteme einzubeziehen. Auch sind Staaten – und dies hat die Globalisierungs- und Transnationalisierungsforschung nachdrücklich herausgearbeitet - insgesamt nicht so wehrlos, wie oftmals von diesen selbst behauptet.

[20] Dies wurde zu der Zeit besonders häufig durch die wild tobende Debatte um *File Sharing* und *Peer-to-Peer-Netzwerke* artikuliert. In dieser zeigte sich die offensichtlich disruptive Wirkung auf Industrien, im speziellen Fall die Musikindustrie, welche eine Allmacht der digitalen Entwicklung zu belegen schien. Gerade die Probleme mit Rechtsdurchsetzung und der Anwendung des Rechtskonzepts von Eigentum schien die exzpetionalistische These zu belegen. Neben Anonymität und Globalität als Prinzipien des Austauschs ist in dieser Diskussion zudem noch die Logik der Kopie ein wichtiges Merkmal der Andersheit und utopischen Potentialität digitaler Kommunikation (Bunz 2004).

strukturellen Eigenheiten auf eine vorgezeichnete Entwicklung geschlossen.[21] Da ist zunächst die Annahme, dass Staaten hilflos gegenüber der Abwanderung von Akteuren in den Cyberspace wären, da sie der Mittel von Kontrolle und Regulierung beraubt seien. Dies erwies sich schon deshalb als falsch, da diesem Argument eine naive, weil vollständige Trennung von online- und offline-Welt zu Grunde liegt. Gerade aber weil niemand nur im Cyberspace lebt, sondern über physische Infrastrukturen und notwendige Intermediäre (von Internetprovidern bis hin zu Banken) permanent Ankerpunkte für Regulierungsansätze bestehen, wären selbst dann, wenn Netzkommunikation sich wirklich überwiegend global und anonym vollzöge, noch Regulierungsmöglichkeiten vorhanden (Goldsmith/Wu 2006).

Ganz generell lässt sich jedoch festhalten, dass auch Globalität und Anonymität als Merkmale der Netzwerkarchitektur in der Weiterentwicklung des Internets deutlich zurückgegangen sind. Bezüglich der Globalität ist das erste Beispiel für diese Tendenz die deutlich erhöhte Geosensibilität des Netzes, wie sie durch die zunehmend genaue Ortung von IP-Adressen und die Regulierung von Kommunikation an zentralen Schnittstellen erreicht wird. Das zweite Beispiel ist die immer stärkere Abschottung nationaler Netze. Die Hoffnung, dass die Fluidität des Netzes ein wirksames Mittel gegen dessen *Balkanisierung* bilden würde, ist in technischer wie politischer Hinsicht enttäuscht worden.[22] Auch bezüglich der Anonymität ist eine ähnliche Entwicklung auszumachen: Das Nutzungsverhalten und die Logik der Angebote, die unsere Netzerfahrung strukturieren, haben das Prinzip der Anonymität weitgehend obsolet gemacht. Kommerzielle wie staatliche Kräfte haben Wege gefunden zumindest die breite Masse des Internetverkehrs, ungeachtet der exponentiell gestiegenen Zahl von Kommunikationen und Geräten, ortbar zu machen.[23] Wichtig ist dabei auch immer zu sehen, dass Staaten nicht allein auf die Form rechtlicher Regulierung beschränkt sind. Im Internet spielt *Code*, und damit die technische Möglichkeit der Regulierung, eine ebenso große Rolle. Auch dieser erweist sich aber als direkt oder indirekt staatlichen Entitäten zugänglich und er stellt angesichts seiner technischen, meist verborgenen Natur ein vielleicht sogar noch wirkungsvolleres Instrument von Regulierung dar (Lessig 2006). Schließlich sei auch noch eingewendet, dass im Gegeneinander-

[21] Für die frühe Debatte vgl. nur Wu (1997); Goldsmith (1998); Perritt (1998); Sassen (1998); einen aktualisierten Überblick über realistische Positionen und Einwände gibt Hansel (2010).

[22] Meist wird dies exemplifiziert an der *Great Firewall of China*, doch ließe sich dies ebenso gut an den mittlerweile sehr umfassenden Filtermaßnahmen des Netzes in Großbritannien belegen.

[23] Die Idee des der Autorität entzogenen, zutiefst anonymen Netzes lebt heute noch in Strukturen wie dem *Deep Web* weiter. Zu diesem sind allerdings die technischen Zugriffshürden sehr viel höher (und dessen Anonymität wurde aller Voraussicht nach auch mehrfach kompromittiert). Das Bemühen um mehr Kryptographie und andere auf individueller Basis ansetzende Versuche ein konsequent dezentrales Netz zu schaffen, sind zwar wichtige (und nach derzeitigem Stand keineswegs vergebliche) Anstrengungen, negative Freiheitsrechte zu sichern. Diese Anstrengungen stehen jedoch in Konkurrenz zu den mit deutlich mehr ökonomischer und politischer Macht ausgestatteten Bemühungen staatlicher und privatwirtschaftlicher Akteure, das Netz entlang ihrer Interessen zu formen.

Ausspielen von territorial gebundenem Recht und virtuell konstruiertem Cyberspace die performative Wirkung von Recht unterschätzt wird (Kamis 2014).

Die rechtstheoretische und rechtswissenschaftliche Debatte um das Internet hat sich somit seit der frühen Diskussion um *Internet Exceptionalism* insgesamt stark verschoben. Die These vom Internet als quasi natürlichem Hindernis nationalstaatlicher Souveränitätsausübung darf heute als widerlegt gelten (Kozinski/Goodfoot 2010; MacCarthy 2010; Wu 2010a). Recht und andere Formen staatlicher Regulierung haben sich auf die Gegebenheiten eingestellt und sind weitgehend wirksame Mittel zur Regulierung von Kommunikation und Austausch im Internet. Das Interesse im Diskurs hat sich daher verstärkt den Quellen von Autorität und Recht zugewendet sowie der Frage nach den Standards und Normen, die Regulierung anleiten sollen. Die Frage ist nun nicht mehr, ob die Prinzipien des Netzes per se der Belagerung durch die Prinzipien der Souveränität standhalten (sie tun es nicht), sondern vielmehr, ob und wie trotzdem offene Netzstandards erhalten und vor dem Missbrauch durch staatliche und kommerzielle Stellen geschützt werden können. Mit einer oft zitierten Wendung von Goldsmith und Wu muss festgehalten werden, dass die Besonderheit des Internets eine Frage der (gesellschaftlichen) Wahl, keine des (technischen) Schicksals ist (Goldsmith/Wu 2006: 90).[24] Die Kräfte, die das Netz in einem offeneren Zustand belassen wollen, stehen dabei heute sehr viel stärker unter Druck als zu jener Zeit, als der *Cyberspace* als souveränitätsaverser Raum gedacht wurde.

3. Das Netz als Gefahrenraum: Krieg, Kontrolle und entfesselte Souveränität

Der dritte Debattenstrang ist noch einmal anders strukturiert: Offenheit wird hier selbst in der Frühphase nicht als ein befreiendes Potential konzipiert, sondern als ein strategisches Problem gesehen. Souveränität und Staatlichkeit werden nicht hinterfragt, sondern in der Pflicht gesehen. Und während die beiden ersten Diskurse akademische Ursprünge haben, aber früh die öffentliche Imagination prägten, ist dieser dritte Diskurs zunächst und vorrangig ein politisch institutioneller Diskurs, der erst nach und nach und insgesamt sehr viel später durch den anschwellenden Sicherheitsdiskurs in den öffentlichen Raum getragen und dort verankert wird.[25]

Der Blick auf Souveränität und Internet wird in dieser Debatte durch das Aufzeigen von Missbrauchspotentialen und Risiken der Netzwerkkommunikation geprägt. Der *Cyberspace* gilt als ein gefährlicher Raum, als ein möglicher Schauplatz von Kriegen, Terrorismus und Verbrechen. Und diesem Raum wird eine extrem gesteigerte Bedeutung zugeschrieben, da moderne

[24] Vgl. hierzu auch Cohen (2007).

[25] Das jüngste Beispiel hierfür sind die programmatischen Anmerkungen des Innenministers Thomas de Maizière (2014), die im Vorfeld der Vorstellung der IT-Sicherheitsgesetze in der FAZ veröffentlicht wurden und die ganz explizit den Staat als Garant des offenen und freien Internets verstehen.

Gesellschaften von ihm abhängig und an dieser Stelle zutiefst verletzlich sind (Achillesferse). Dies erzwinge den Schutz dieses Raumes durch die Etablierung eines umfassenden Sicherheitssystems (Dunn Cavelty 2007). Staatliche Macht, das Poolen der Ressourcen zur Ausübung von Gewalt und Kontrolle, ist hierfür die klassische, ja meist gleichsam für natürlich gehaltene Lösung.[26] Der Staat wird als in seiner Kernaufgabe, der Gewährleistung kollektiver Sicherheit, gefordert gesehen und es wird explizit die Annahme formuliert, dass Sicherheit der Freiheit vorausgeht und erst etablierte Staatlichkeit Demokratie und andere liberale Güter ermöglicht.[27]

Auf den ersten Blick haben wir es daher in diesem Debattenstrang mit der Rückkehr eines sehr alten Souveränitätsverständnisses zu tun. Souveränität meint hier höchstranginge Handlungskompetenz, sie verweist auf Ressourcen und Gewaltmittel und wird als deckungsgleich mit den existierenden staatlichen Entitäten begriffen. Das Bedeutungswachstum des Internets unterstreicht demzufolge nur die Notwendigkeit von Staatlichkeit und mindert sie nicht etwa. Insofern scheint wenig überraschend, dass der Staat mitnichten ein Auslaufmodell ist – dies war ja auch schon ein Ergebnis der Betrachtung der ersten beiden Debatten –, sondern das Internet in mancherlei Hinsicht zu dessen Wiedererstarken beiträgt.[28]

Schaut man genauer hin, lassen sich auch in diesem Diskurs Behauptungen finden, die von einer transformativen Wirkung des *Cyberspace* auf das Konzept der Souveränität ausgehen (Herrera 2007). Die Veränderungen werden hier aber in der Ausrichtung und Tiefe von Souveränität festgemacht. Es wird eine *quantitative* Veränderung erwartet, die jedoch durchaus auch *qualitative*

[26] Vgl. den klassischen Aufsatz über den Zusammenhang von Staatsbildung und Kriegsführung: Tilly (1985).

[27] Der politische Diskurs, in dem Souveränität eine Forderung ist, wird dabei von zwei weitgehend getrennten akademischen Diskursen begleitet. Der erste dieser akademischen Diskurse beschäftigt sich mit den Ausprägungen des *Cyberwars*. Dabei ist höchst umstritten, was *Cyberwar* eigentlich ist und wie ernst man ihn nehmen sollte. Bereits früh wurde eine besondere Gefahr aus dem Netz ausgemacht und der Cyberspace als neue *Domain* der Kriegsführung (neben Boden, Wasser, Luft und Weltraum) beschrieben (Arquilla/Ronfeldt 1993; zur *Frühgeschichte* staatlicher Sicherheitsabwägungen generell vgl. Warner 2012). Während eine Vielzahl politikberatender Thinktanks und privater Sicherheitsfirmen nachdrücklich vor den Risiken des *Cyberspace* warnen und insbesondere den Gedanken einer passiven oder rechtlichen Hegung dieser Gefahr verwerfen, betonen andere Autoren, dass auch nach Jahren seiner Propagierung *Cyberwar* ein theoretisches Szenario geblieben ist, hauptsächlich das Wachstum des militärisch-industriellen Komplexes vorangetrieben hat und maximal in einem konventionellen Kriegsfall eine relevante Dimension darstellen würde: Rid (2013); Gartzke (2012); Brito/Watkins (2011). Der zweite akademische Diskurs ist eine eher kritische Begleitung. Hier wird der diskursanalytisch und zumeist unmittelbar mit Bezug auf die Versicherheitlichungstheorien der Kopenhagener Schule nachgezeichnet, wie der Sicherheitsdiskurs Raum greift, welche Begründungsmuster sich in ihm unterscheiden lassen und wie dies zum Wiedererstarken des Staats führt. Studien, die direkt durch die Kopenhagener Schule inspiriert sind, sind: Conway (2008), Dunn Cavelty (2008); (2013); Nissenbaum (2004); (2005); Hansen/Nissenbaum (2009). Mit einer ähnlichen argumentativen Ausrichtung, methodisch jedoch anders gelagert: Deibert/Crete-Nishihata (2012); Deibert/Rohozinski (2010a); (2010b); Deibert (2013); Kamis/Thiel (i.E.).

[28] Wie Deibert/Rohzinski (2010a) anmerken, muss man eigentlich zwei Typen von Gefahr-Reaktions-Schemata unterscheiden. Risiken *für* den Cyberspace werden tendenziell mittels gemeinsamer Abkommen und Zusammenarbeit einzuschränken versucht, Risiken *durch* den Cyberspace hingegen befördern die Tendenz zur unilateralen, meist nationalstaatlichen Abschottung. Letztere bewirken die Einschränkung der offenen und umfassenden Architektur des Netzes wie oben beschrieben, erstere sind eher im Zusammenhang mit der ebenfalls bereits beschriebenen Herausbildung des Regimes von *Internet Governance* zu interpretieren.

(und das heißt hier normative) Folgewirkungen für das Konzept der Souveränität als solcher haben kann. Die Annahme ist, dass die *westfälische* Konstellation einer abgegrenzten, überwiegend reaktiven und durch negative Freiheitsrechte innerstaatlich hegbaren Souveränität durch die Strukturmerkmale des Internets verunmöglicht wird. Souveräne Abgrenzung und das Verlassen darauf, dass staatliche Entitäten Gewalt global zu monopolisieren und zwischen sich aufzuteilen in der Lage wären, gelten als nicht länger bedingungslos voraussetzbar (Vgl. Brenner 2014).[29] So wird mit Blick auf *Cyberwar* behauptet, dass das digitale Kriegsszenario schon deswegen entschieden anders strukturiert ist, da die Attribution von Cyberattacken und die Möglichkeit der Vergeltung im Falle einer solchen jeweils schwierig sind. Es wird auf die große Wahrscheinlichkeit asymmetrischer Angriffe verwiesen und aus den Besonderheiten insgesamt die Unumgänglichkeit des Aufbaus präemptiver Kapazitäten gefolgert. Offensive Kapazitäten und Abschreckungspotentiale gelten als die im digitalen Krieg entscheidende Kapazität, die Möglichkeit von dessen rechtlicher oder politischer Hegung hingegen, werden als stark eingeschränkt begriffen (Clarke/Knake 2012; Goldsmith 2013). Souveräne Machträume können sich daher nicht länger wie im westfälischen System in Abgrenzung zueinander stabilisieren, sondern unterliegen einer Tendenz, sich wieder sehr viel stärker hegemonial oder imperial zu strukturieren.[30]

Diese Tendenz ist auch noch in einer zweiten, höchst souveränitätsrelevanten Dimension gut zu beobachten: den Geheimdiensten. Hier haben nicht zuletzt die Enthüllungen Edward Snowdens gezeigt, dass seit Jahren eine Entgrenzung der Überwachungsapparate stattfindet. Der Unterschied zwischen innen und außen, der für das klassische Konzept staatlicher Souveränität zentral ist, wird immer stärker verwischt. Etwa, wenn umfassend und global Metadaten gesammelt oder eine vollständige Erfassung der Netzkommunikation versucht wird. Eine umfangreiche und konkreten Verdachtsmomenten vorgelagerte Überwachung ist dabei nicht nur möglich geworden, sie wird geradezu zum Gebot erklärt. Zugleich zeigen die von Snowden geleakten Dokumente sowie die Vielzahl von Enthüllungen in deren Folge, dass die prozeduralen Kontroll- und Verantwortungsmechanismen in sämtlichen etablierten westlichen Demokratien nahezu wirkungslos gegenüber der technisch imprägnierten Begründung der Ausweitung von Überwachung waren. Insbesondere demokratisch legitimierte Parlamente haben deutlich an Boden verloren, die Ausübung von Souveränität sich sehr stark an exekutive Instanzen verlagert.

[29] Auch hierzu gibt es selbstverständlich nicht-netzbezogene Parallelen wie das Phänomen der neuen Kriege, Terrorismus oder zerfallende Staatlichkeit. Diese Phänomene sind jeweils eng verbunden und in ihren Wirkungen auf die Entwicklung von Rechtsstaatlichkeit und Demokratie ähnlich zu beurteilen. Vgl. etwa: Frankenberg (2010).

[30] Aus diesem Grunde argumentiert Sandro Gaycken (2012), dass *Entnetzung* der einzig effiziente Weg wäre, nationalstaatliche Souveränität im Feld elektronischer Kriegsführung wiederherzustellen.

Macht verschwindet nicht, aber sie entzieht sich und verliert ihre demokratische Hegung – was eine bedeutende Umkehr der Demokratisierung nationalstaatlicher Souveränität darstellt.[31]
Dies wird durch eine weitere Entwicklung nochmals verstärkt, die Zygmunt Bauman et al. wie folgt beschreiben:

> „[…], we see the transformation of a reason of state through the emergence of a digitized reason of state performed by a heterogeneous complex of professionals, of sensitive information hybridizing private and public actors. The transnational nature of gathering information that crosses the boundaries of states dissociates the discursive, homogeneous nature of national security interests while reconstructing an aggregate of professionals" (Baumann, et al. 2014: 126).

Diese hier als neue Normalität beschriebene Privatisierung von staatlichen Aufgaben und deren Immunisierung gegenüber Kontrolle lässt sich dabei für den Überwachungsapparat wie für die digitale Kriegsführung nachvollziehen (Deibert/Rohozinski 2010a; Gaycken 2014). Souveränitätstheoretisch impliziert die zunehmende Abhängigkeit staatlicher Akteure von privaten Firmen und Dienstleistern, dass dem Staat zunehmend die Kompetenzen verloren gehen, überhaupt in technischen Bereichen wie dem Internet eigenständig oder auch nur regelsetzend tätig zu werden. Eine Entwicklung mit weitreichenden normativen und demokratietheoretischen Folgen.[32]

Souveränität und Internet: Einige einordnende Bemerkungen

Der nun erarbeitete Überblick über die drei zentralen Debatten zum Verhältnis von Internet und Souveränität hat mehrere Dinge offenbart: Zunächst lässt sich festhalten, dass die unter dieser Überschrift geführten Diskurse im Laufe der Zeit eine deutliche Ausweitung und Differenzierung erfahren haben. In allen drei Debattensträngen ist es zu einer *Versachlichung* gekommen. Die Vorstellung des *Cyberspace* als Antithese zur Souveränität hat sich nicht halten können. In jeder der drei hier nachgezeichneten Debatten wurde die Annahme einer durch Technik determinierten gesellschaftlichen Entwicklung als unterkomplex zurückgewiesen und im Umkehrschluss die Rolle gesellschaftlicher und politischer Faktoren und Akteure herausgearbeitet.

[31] Eine umfassende, wenn auch keineswegs neutrale Beschreibung liefert: Greenwald (2014).
[32] Am bekanntesten formuliert in Colin Crouchs (2004) These von der Postdemokratie und der Unterhöhlung demokratischer Institutionen.

Eine der wichtigsten Thesen im Netzdiskurs – und über die drei Debattenstränge hinweg – ist daher die *Wiederkehr des Staates*. Dessen Kompetenz zu Rechtssetzung, Regulierung und Ordnungsbildung hat sich als beständiger und notwendiger erwiesen, als von den Internetpionieren behauptet und dessen demokratietheoretischen Meriten – insbesondere die durch repräsentative Institutionen realisierte Volkssouveränität – sind nicht so obsolet wie zunächst angenommen, zumal die Alternative(n) bei näherer Betrachtung deutlich an Überzeugungskraft verloren haben. Auch die als staatliche Kernaufgabe verstandene Gewährleistung kollektiver Sicherheit wurde im öffentlichen Diskurs zunehmend mit der digitalen Sphäre assoziiert, was bewirkt, dass heute der Aufbau von Kontroll- und Überwachungsressourcen sowie die nationale Filterung und Abschottung von Netzen als Bedingung eines freiheitlichen Internets dargestellt werden kann. Die *Realisten* haben insofern klar Oberwasser, die *Andersheit* des Netzes ist heute diskursiv wie faktisch stark zurückgegangen. Dass heute die dritte Debatte, jene um Sicherheit und Kontrolle, klar dominanter ist als die stärker *utopisch* dominierten Debattenkontexte eins und zwei, ist ein weiterer Ausdruck dieser Entwicklung.

Die *Wiederkehr des Staates* heißt jedoch nicht, dass nicht auch ein *Wandel von Staatlichkeit* stattgefunden hätte beziehungsweise immer noch stattfindet. Diese Erkenntnis ist in der Rekonstruktion der drei Debatten bisher nur partiell aufgeblitzt, soll hier aber noch einmal hervorgehoben werden: So hat sich in der Debatte um das Internet als Ordnungsform gezeigt, dass zwar nicht das Netzwerk per se der Hierarchie entgegengesetzt werden kann, dass aber sowohl im Bereich politischer Selbstorganisation als auch mit Blick auf die durch Netzwerkbildung erfolgende *Internet Governance* innovative Ergänzungen zu klassischen Ordnungsformen entstanden sind, die nicht nur politisch höchst relevant sind, sondern sich auch als relativ beständig sowie als Vorbild in andere Kontexten erwiesen haben. Nicht vergessen werden darf zudem, dass digitale Vernetzung Transnationalisierungsprozesse von Öffentlichkeit und zivilgesellschaftlichen Akteuren befördert, die wiederum den ganz analogen Wandel von Staatlichkeit verstärken. Auch bezüglich der Art und Weise wie staatliche Institutionen auf den *Cyberspace* zugreifen und diesen zu regulieren versuchen, haben sich *neue* Strategien und Instrumente herausgebildet, so beispielsweise die indirekte Regulierung von sich nationalstaatlichem Zugriff entziehenden Akteuren mittels privater Intermediäre oder die Vielzahl neuer Governance-Arrangements, die sich insbesondere durch die Einbeziehung technischer Experten und zivilgesellschaftlicher Akteure auszeichnen. Ein Wandel von Staatlichkeit lässt sich schließlich auch im sicherheitspolitischen Feld ausmachen. Aus normativer

Sicht sind hier allerdings größere Bedenken angebracht, da der Wandel hauptsächlich in einer Ausdehnung und teilweisen Immunisierung von Akteuren der staatlichen Exekutive besteht, die in Verbindung mit privaten Akteuren die ansteigenden Kapazitäten zu Überwachung und Kontrolle auszunutzen verstehen und damit dazu beitragen, dass sich das staatliche System zunehmend weniger durch souveräne Abgrenzung stabilisiert, stattdessen imperiale Ordnungsmuster an Bedeutung gewinnen.

Sowohl die *Wiederkehr des Staates* wie auch der *Wandel von Staatlichkeit* machen deutlich, dass die Debatte um Internet und Souveränität nicht abgekoppelt werden kann und sollte von der viel weiteren allgemeinen politikwissenschaftlichen Diskussion zu Souveränität und Transnationalisierung. Die Synchronität mit dem weiteren Diskursverlauf in der Disziplin, etwa mit Blick auf die Entwicklung von Global Governance, ist augenfällig. Die hier unternommene Zusammenstellung dreier zentraler Debattenkontexte kann daher auch als Aufforderung gelesen werden, sich aus der Perspektive der Politikwissenschaft als Ganzer oder noch spezieller der Politischen Theorie sehr viel intensiver in diesem, oft für fachfremd gehaltenen, Diskurs einzumischen. Dabei gibt es viel zu lernen, da das Internet als *Fallbeispiel* nicht nur hochgradig relevant ist, sondern sich an ihm auch eine Vielzahl von Phänomenen besonders deutlich studieren lassen. Grund hierfür ist, dass die Sprache des Diskurses, die institutionelle Form der Politik und die Kraft rechtlicher und sozialer Normen noch nicht sonderlich festgefügt ist. Politiktheoretisch zu erfassen, inwiefern sich in und durch dieses Politikfeld die Bedingungen moderner Politik verändern und welche institutionellen und normativen Schlussfolgerungen daraus zu ziehen sind, wird daher eine wichtige Aufgabe sein und bleiben – eine Aufgabe, die gerade im deutschen Sprachraum noch nicht hinreichend erkannt und angenommen ist.

Literatur

Arquilla, John/Ronfeldt, David 1993: Cyberwar is coming, in: Comparative Strategy 12: 2, S. 141-165.

Barlow, John Perry 1996: A Declaration of the Independence of Cyberspace. in: https://projects.eff.org/~barlow/Declaration-Final.html, 13.08.2014.

Baumann, Zygmunt/Bigo, Didier/Esteves, Paulo/Guild, Elspeth/Jabri, Vivienne/Lyon, David/Walker, R. B. J. 2014: After Snowden: Rethinking the Impact of Surveillance, in: International Political Sociology 8: 2, S. 121-144.

Benkler, Yochai 2006: The Wealth of Networks: How Social Production Transforms Markets and Freedom, New Haven.

Bennett, Lance W. 2003: Communicating Global Activism, in: Information, Communication & Society 6: 2, S. 143-168.

Bennett, Lance W./Segerberg, Alexandra 2013: The Logic of Connective Action: Digital Media and the Personalization of Contentious Politics, Cambridge.

Brenner, Susan W. 2014: Cyberthreats and the Decline of the Nation State, London.

Brito, Jerry/Watkins, Tate 2011: Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy, in: Mercatus Center Working Paper. No. 11-24.

Bunz, Mercedes 2004: Die Utopie der Kopie, in: Maresch, Rudolf/Rötzer, Florian: Rennaissance der Utopie. Zukunftsfiguren des 21. Jahrhunderts, Frankfurt am Main, S. 156-171.

Castells, Manuel 2010: The Rise of the Network Society, 2nd edition, Cambridge, Mass.

Castells, Manuel 2012: Networks of Outrage and Hope: Social Movements in the Internet Age, London.

Chenou, Jean-Marie 2014: From Cyber-Libertarianism to Neoliberalism: Internet Exceptionalism, Multi-stakeholderism, and the Institutionalisation of Internet Governance in the 1990s, in: Globalizations 11: 2, S. 205-223.

Clarke, David D. 1992: A Cloudy Crystal Ball - Visions of the Future, in: Davies, Megan, et al.: Proceedings of the Twenty-Fourth Internet Engineering Task Force, Cambridge.

Clarke, Richard A./Knake, Robert K. 2012: Cyber War: The Next Threat to National Security and What to Do About It, New York.

Cohen, Julie E. 2007: Cyberspace as/and Space, in: Columbia Law Review 107, S. 210-256.

Conway, Maura 2008: Media, Fear and the Hyperreal: The Construction of Cyberterrorism, in: Dunn Cavelty, Myriam/Kristensen, Kristian Soby: Securing the Homeland: Criticial Infrastructure, Risk, and (In)Security, London, S. 109-129.

Crouch, Colin 2004: Post-Democracy, Cambridge.

Dahlberg, Lincoln/Siapera, Eugenia 2007: Radical Democracy and the Internet. New York.

Dany, Charlotte 2012: Ambivalenzen der Partizipation. Grenzen des NGO-Einflusses auf dem Weltgipfel zur Informationsgesellschaft, in: Zeitschrift für Internationale Beziehungen 19: 2, S. 71-99.

Deibert, Ronald J. 2013: Black Code. Sureveillance, Privacy and the Dark Side of the Internet, Toronto.

Deibert, Ronald J./Crete-Nishihata, Masashi 2012: Global Governance and the Spread of Cyberspace Controls, in: Global Governance 18, S. 339-361.

Deibert, Ronald J./Palfrey, John/Rohozinski, Rafal/Zittrain, Jonathan 2008: Access Denied: The Practice and Policy of Global Internet Filtering. Cambridge, MA.

Deibert, Ronald J./Palfrey, John/Rohozinski, Rafal/Zittrain, Jonathan 2010: Access Controlled: The

Shaping of Power, Rights, and Rule in Cyberspace. Cambridge, MA.

Deibert, Ronald J./Palfrey, John/Rohozinski, Rafal/Zittrain, Jonathan 2012: Access Contested: Security, Identity and Resistance in Asian Cyberspace. Cambridge, MA.

Deibert, Ronald J./Rohozinski, Rafal 2010a: Risking Security: Policies and Paradoxes of Cyberspace Security, in: International Political Sociology 4: 1, S. 15-32.

Deibert, Ronald/Rohozinski, Rafal 2010b: Liberation vs. Control. The Future of Cyberspace, in: Journal of Democracy 21: 4, S. 43-57.

de Maizière, Thomas 2014: Das Netz - Raum der Chancen und der Freiheit, in: Frankfurter Allgemeine Zeitung, 18.08.2014, S. 6.

DeNardis, Laura 2013: The Emerging Field of Internet Governance, in: Dutton, William H.: Oxford Handbook of Internet Studies, Oxford.

DeNardis, Laura 2014: The Global War for Internet Governance, New Haven.

Drezner, Daniel 2004: The Global Governance of the Internet: Bringing the State Back In, in: Political Science Quarterly 119: 3, S. 477-498.

Dunn Cavelty, Myriam 2007: Is Anything Ever New? - Exploring the Specifities of Security and Governance in the Information Age, in: Dunn Cavelty, Myriam, et al.: Power and Security in the Information Age. Investigating the Role of the State in Cyberspace, Aldershot, S. 19-44.

Dunn Cavelty, Myriam 2008: Cyber-Terror - Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate, in: Journal of Information Technology & Politics 4: 1, S. 19-36.

Dunn Cavelty, Myriam 2013: From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse, in: International Studies Review 15: 1, S. 105-122.

Earl, Jennifer/Kimport, Katrina 2011: Digitally Enabled Social Change, Boston.

Ebert, Hannes/Maurer, Tim 2013: Contested Cyberspace and Rising Powers, in: Third World Quarterly 34: 6.

Frankenberg, Günter 2010: Staatstechnik. Perspektiven auf Rechtsstaat und Ausnahmezustand, Berlin.

Gartzke, Erik 2012: The Myth of Cyberwar. Bringing War on the Internet Back Down to Earth, in: International Security 38: 2, S. 41-73.

Gaycken, Sandro 2012: Cyberwar, München.

Gaycken, Sandro 2014: Mehr Staat fürs Netz, in: IP - Internationale Politik 12: 4, S. 100-106.

Goldsmith, Jack 1998: Against Cyberanarchy, in: University of Chicago Law Review 65.

Goldsmith, Jack 2013: How Cyber Changes the Laws of War, in: European Journal of International Law 24: 1, S. 129-138.

Goldsmith, Jack/Wu, Tim 2006: Who Controls the Internet? Illusions of a Borderless World, Oxford.

Grassegger, Hannes 2014: Staaten steigen aus dem Web aus, in: Neue Zürcher Zeitung, 09.02.2014.

Greenwald, Glenn 2014: No Place to Hide. Edward Snowden, the NSA and the Surveillance State, London.

Hansel, Michael 2010: Neue und alte Barrieren: Herrschaft und politische Partizipation im Cyberspace, in: Zeitschrift für Außen- und Sicherheitspolitik 3: 3, S. 357-378.

Hansen, Lene/Nissenbaum, Helen 2009: Digital Disaster, Cyber Security, and the Copenhagen School, in: International Studies Quarterly 53, S. 1155-1175.

Herrera, Geoffrey L. 2007: Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space, in: Dunn Cavelty, Myriam, et al.: Power and Security in the Information Age. Investigating the Role of the State in Cyberspace, Aldershot, S. 67-94.

Hofmann, Jeanette 2005: Internet Governance: Zwischen staatlicher Autorität und privater Koordination, in: Internationale Politik und Gesellschaft 3, S. 10-29.

Hofmann, Jeanette 2009: Formierung und Wandel des Politischen in der Regulierung des Internet, in: Bergermann, Ulrike, et al.: Das Planetarische. Kultur - Technik - Medien im postglobalen Zeitalter, München.

Howard, Philip N. 2010: The Digital Origins of Dictatorship and Democracy, Oxford.

Jacob, Daniel/Thomas, Manuel 2014: Das Internet als Heilsbringer der Demokratie?, in: Aus Politik und Zeitgeschichte 64: 22-23, S. 35-39.

Johnson, David R./Crawford, Susan P./Palfrey, John 2004: The Accountable Internet: Peer Production of Internet Governance, in: Virginia Journal of Law & Technology 9: 9, S. 3-33.

Johnson, David R./Post, David G. 1996: Law and Borders - The Rise of Law in Cyberspace, in: Stanford Law Review 48, S. 1367-1402.

Juris, Jeffrey S. 2012: Reflections on #Occupy Everywhere: Social media, public space, and emerging logics of aggregation, in: American Ethnologist 39: 2, S. 259-279.

Kalathil, Shanthi/Boas, Taylor C. 2003: Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule, Washington.

Kamis, Ben 2014: Res in Media: the post-national territorialisation of cyberspace through international law, in: unveröffentl. Research Paper, WISC-Konferenz 2014 (Frankfurt).

Kamis, Ben/Thiel, Thorsten i.E. (voraussichtliches Erscheiungsdatum?): The Orignial Battle Trolls: How States Represent the Internet as a Violent Place, (in der Begutachtung/ Vorversion gehalten auf der ECPR General Conference 2013, Bordeaux).

Katz, Jon 1997: The Birth of a Digital Nation, in: WIRED. 5.

Koschorke, Albrecht/Lüdemann, Susanne/Frank, Thomas/de Mazza, Ethel Marala 2007: Der fiktive Staat. Konstruktionen des politischen Körpers in der Geschichte Europas, Frankfurt.

Kozinski, Alex/Goodfoot, Josh 2010: A Declaration of the Dependence of Cyberspace, in: Szoka, Berin/Marcus, Adam: The Next Digital Decade, Washington, S. 169-178.

Lanier, Jaron 2013: Who Owns The Future?, New York.

Lessig, Lawrence 2002: The Future of Ideas, New York.

Lessig, Lawrence 2006: Code Version 2.0, New York.

Lobo, Sascha 2014: Abschied von der Utopie. Die digitale Kränkung des Menschen, in: Frankfurter Allgemeine Sonntagszeitung, 12.01.2014.

Lovink, Geert 2012: Networks Without a Cause. A Critique of Social Media, Oxford.

MacCarthy, Mark 2010: Internet Exceptionalism Revisited, in: Szoka, Berin/Marcus, Adam: The Next Digital Decade, Washington, S. 209-236.

Mathiason, John 2009: Internet Governance. The New Frontier of Global Institutions, New York.

McGregor, Heather 1999: Law on a Boundless Frontier: The Internet and International Law, in: Kentucky Law Journal 88, S. 967-986.

Morozov, Evgeny 2011: The Net Delusion, London.

Mueller, Milton 2010: Networks and States: The Global Politics of Internet Governance, Cambridge, MA.

Negroponte, Nicholas 1996: Being Digital, New York.

Nissenbaum, Helen 2004: Hackers and the Contested Ontology of Cyberspace, in: New Media & Society 6: 2, S. 195-217.
Nissenbaum, Helen 2005: Where Computer Security Meets National Security, in: Ethics and Information Technology 7: 2, S. 61-73.

Perritt, Henry H. 1998: The Internet as a threat to sovereignty? Thoughts on the Internet's role in strengthening national and global governance, in: Indiana Journal of Global Legal Studies 5: 2, S. 423-442.

Post, David G. 2002: Against 'Against Cyberanarchy', in: Berkeley Technology Law Journal 17: 1365-1387.

Post, David G. 2007: Governing Cyberspace: Law, in: Santa Clara High Technology Law Journal 24: 4, S. 884-913.

Post, David G. 2009: In search of Jefferson's moose: notes on the state of cyberspace, Oxford; New York.

Reagle, Joseph 1999: Why the Internet is Good. Community governance that works well, in: Berkman Center for Internet; Society, Harvard Law School (working paper).

Rheingold, Howard 2002: Smart Mobs. The Next Social Revolution, Cambridge, MA.

Rid, Thomas 2013: Cyber War will not take place, London.

Rossiter, Ned 2006: Organized Networks. Media Theory, Creative Labour, New Institutions, Rotterdam.

Sassen, Saskia 1998: On the Internet and Sovereignty, in: Indiana Journal of Global Legal Studies 5: 2, S. 545-559.

Sassen, Saskia 2006: Territory, Authority, Rights: From Medieval to Global Assemblages, Princeton.

Shahin, Jamal 2007: The Reassertion of the State: Governance and the Information Revolution, in: Dunn Cavelty, Myriam, et al.: The Resurgence of the State. Trends and Processes in Cyberspace Governance, Aldershot, S. 9-34.

Shapiro, Andrew L. 1999: The Control Revolution. How The Internet Is Putting Individuals In Charge And Changing The World We Know, New York.

Shirky, Clay 2008: Here Comes Everybody, London.

Singh, J.P. 2013: Information Technologies, Meta-power, and Transformations in Global Politics, in: International Studies Review 15: 1, S. 5-29.

Tilly, Charles 1985: War Making and State Making as Organized Crime, in: Evans, Peter, et al.: Bringing the State Back In, Cambridge, S. 169-187.

Turner, Fred 2006: From Counterculture to Cyberculture. Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism, Chicago.

Warner, Michael 2012: Cyber-Security: A Pre-History, in: Intelligence and National Security 27: 5, S. 781-799.

Warnke, Martin 2011: Theorien des Internets, Hamburg. (im Text nicht verwendet)

Wu, Tim 1997: Cyberspace Sovereignty - The Internet and the International System, in: Harvard Journal of Law & Technology 10, S. 648-666.

Wu, Tim 2010a: Is Internet Exceptionalism Dead?, in: Szoka, Berin/Marcus, Adam: The Next Digital Decade, Washington, S. 179-188.

Wu, Tim 2010b: The Master Switch. The Rise and Fall of Information Empires, New York.

Ziewitz, Malte/Pentzold, Christian 2012: In search of internet governance: Performing order in digitally networked environments, in: New Media & Society 16: 2, S. 306-322.

Zittrain, Jonathan 2009: The Future of the Internet. And How to Stop It, London.