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)

Gibt es Souveränität im Cyberspace?

Milton L. Mueller

Abstract

Dieser Beitrag behandelt die Frage, ob es staatliche Souveränität im Cyberspace geben kann. Er kommt zu einem differenzierten Ergebnis: Zunächst muss Souveränität *im* und Souveränität *über* den Cyberspace unterschieden werden. Letzteres stellt die Kontrolle über den Cyberspace in Form staatlicher Strukturen dar. Demgegenüber meint Souveränität im Cyberspace ein Äquivalent zur Souveränität, das mit virtuellen Mitteln erreicht werden kann, also im Sinne eines Gewaltmonopols im virtuellen Raum. Zu beiden Typen fällt die Bilanz skeptisch aus. Über ein Gewaltmonopol im Cyberspace verfügen Staaten offenbar nicht. Demgegenüber ist staatliche Souveränität über den Cyberspace technisch zwar durchaus möglich, sie würde aber das Ende des Internets, wie wir es kennen, bedeuten. Der virtuelle Raum würde eine erhebliche Fragmentierung erfahren. Diese ist keineswegs wünschenswert, denn sie würde das Innovationspotential der Internetentwicklung hemmen. Dies beträfe nicht zuletzt auch die gesellschaftlichen Entwicklungsmöglichkeiten. Wenn Normen durch Fragmentierung geschützt werden, müssen sie sich nicht mehr international durchsetzen. Das Internet bedroht zwar das klassische Konzept territorialer Souveränität. Allerdings könnte die Internetgemeinde gerade aus dieser Krise heraus eine neue Form transnationaler demokratischer Souveränität etablieren.

Keywords

Souveränität, Cyberspace, Territorialität, Fragmentierung, Autonome Systeme

DOI: 10.11588/josar.2015.0.23483

Gibt es Souveränität im Cyberspace?

Milton L. Mueller[1]

1 Einleitung

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

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

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

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

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

2 Das Souveränitätskonzept in der Politikwissenschaft

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

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

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

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

3 Souveränität und Territorialität

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

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

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

4 Volkssouveränität

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

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

5 Souveränität ‚im' und ‚über den' Cyberspace

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

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

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

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

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

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

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

6 Die Debatte Souveränität vs. Fragmentierung

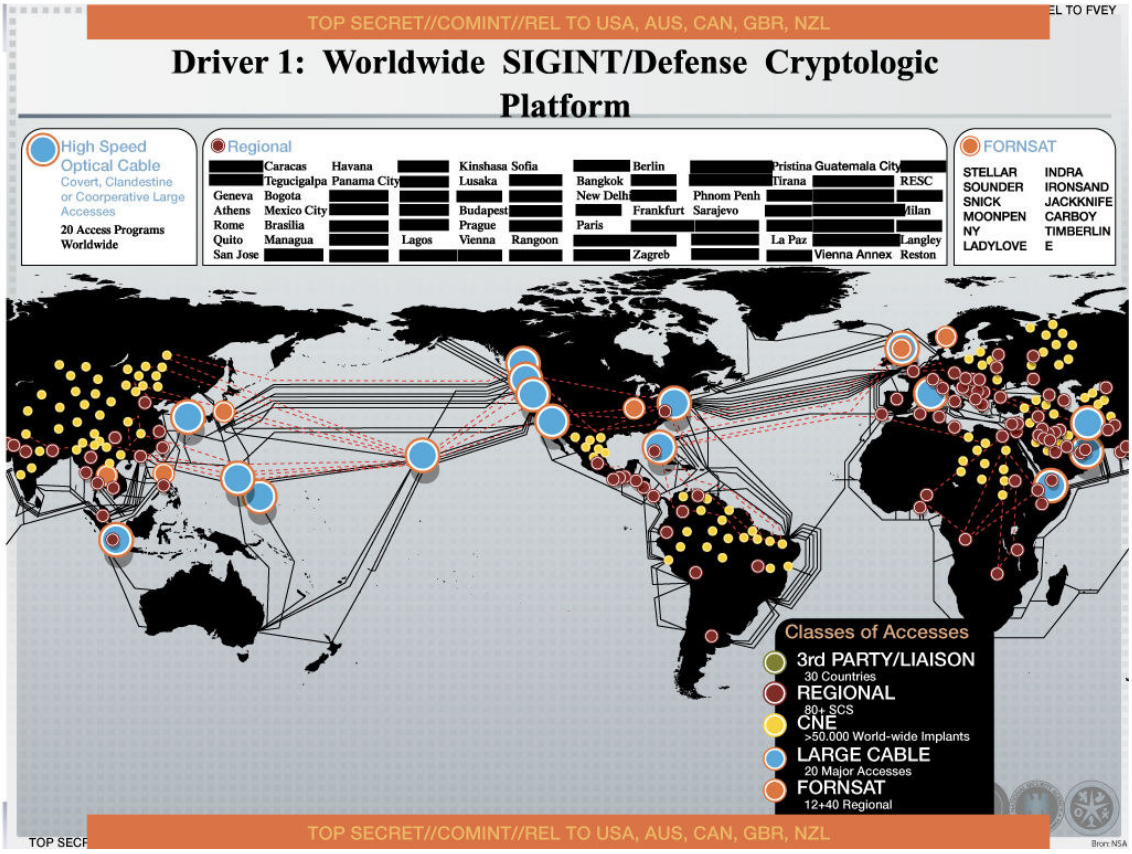
Das, was an den Snowden-Enthüllungen für viele schockierend war, ist doch, dass der Raum, der von den US-amerikanischen Sicherheitsbehörden als „ihr" zu schützender Cyberspace ausgegeben und konzipiert wird, keineswegs territorial begrenzt, sondern global ist. Die Karte in Abb. 1 stammt aus den von Snowden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

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

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

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

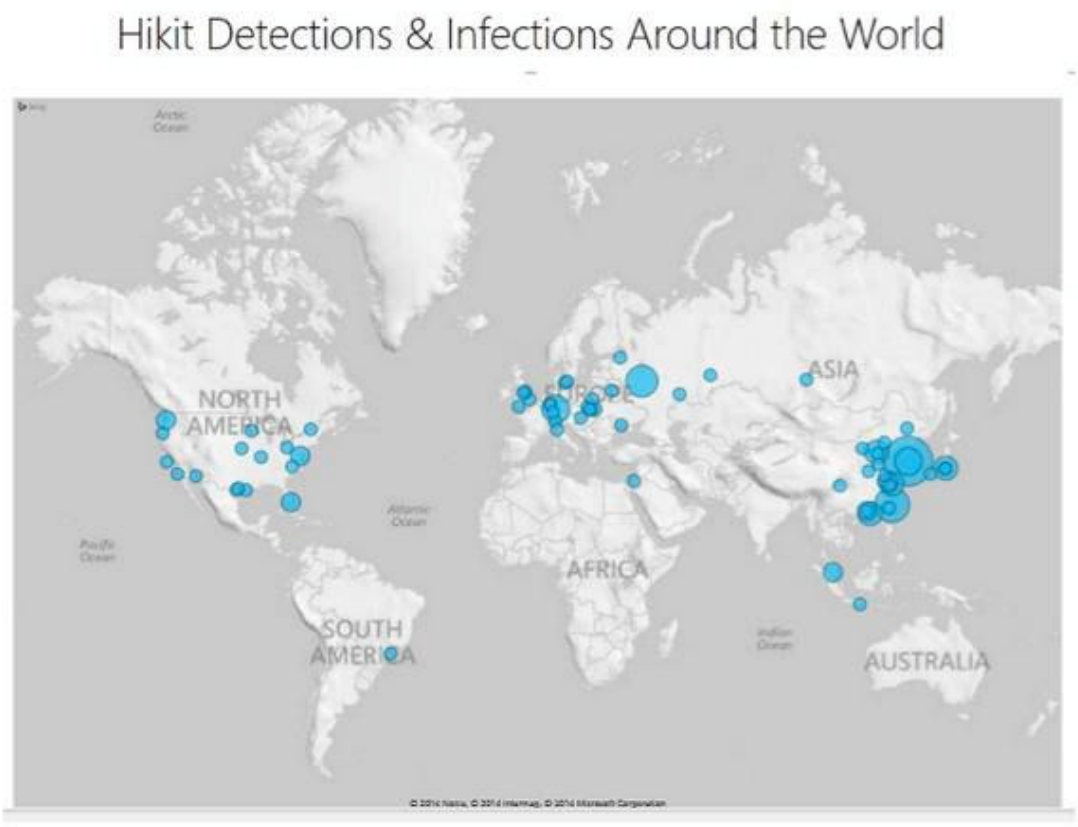
Abbildung 1: NSA-Dokument – Worldwide SIGINT/Defense Cryptologic Platform



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

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

Abbildung 2: Hikit Detections and Infections Worldwide



Quelle: Novetta Inc. 2014: 8.

7 Die wirklichen souveränen Einheiten des Internets

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

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

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

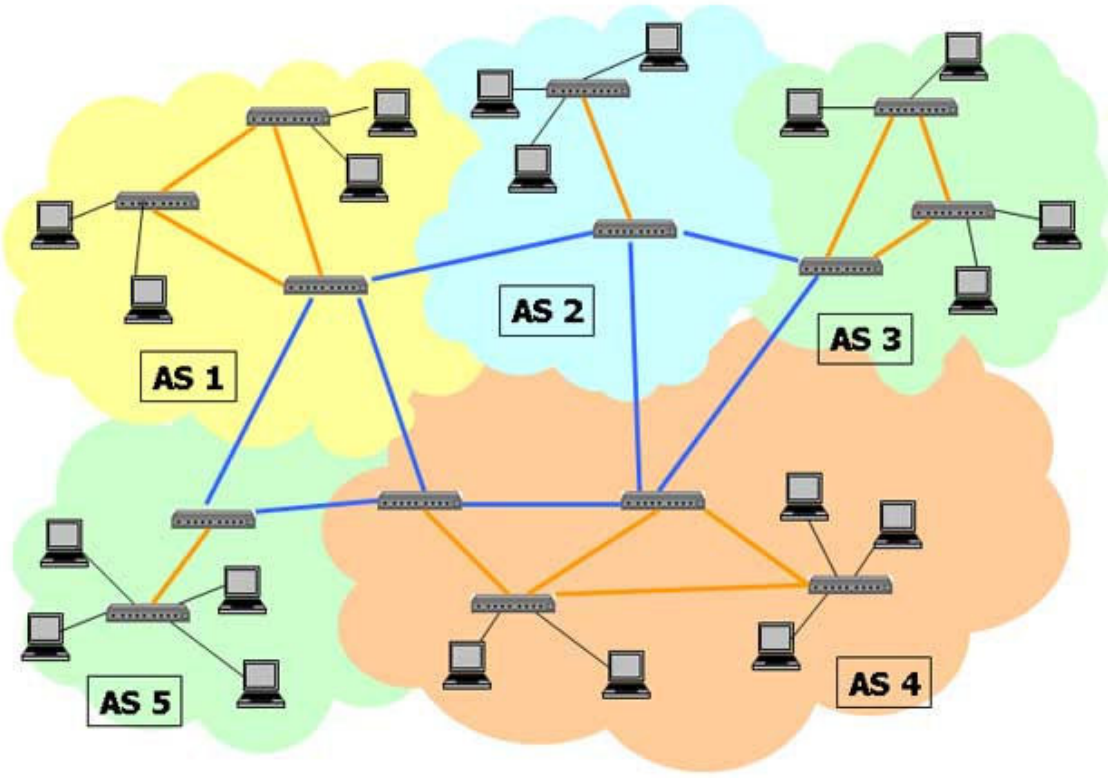
Auch wenn das Konzept des „kill switch", welches die Internetkonnektivität faktisch durch den Beschluss einer höheren Autorität vorübergehend aussetzt, noch darüber hinausgehen mag, so ist es im Regelfall das Autonome System, das „über den Ausnahmezustand entscheidet"(Schmitt 2009 [1922]: 13). Abb. 3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

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

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

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

Abbildung 3: Autonome Systeme (AS) im Cyberspace



Quelle: eigene Darstellung.

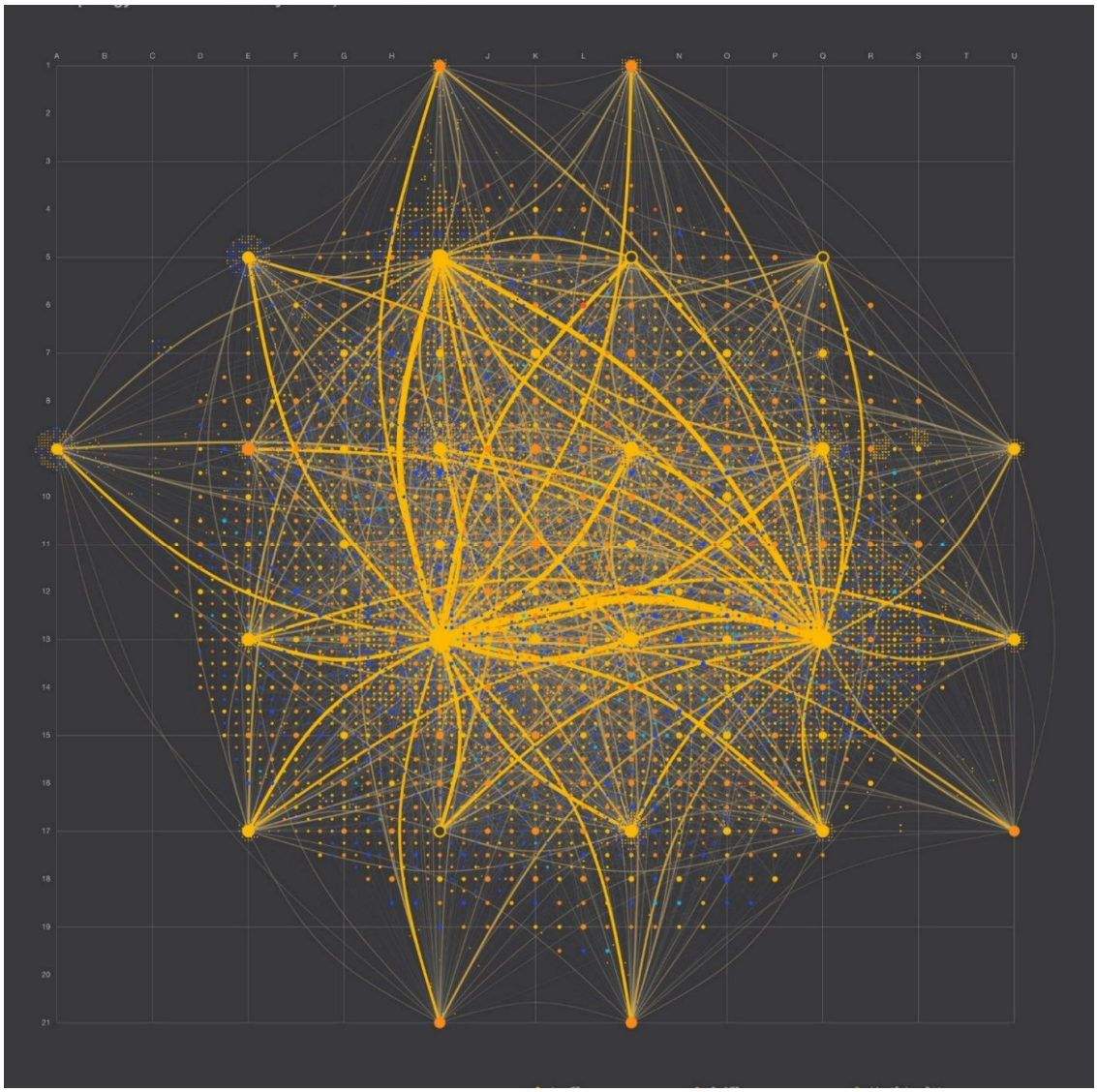
Auch muss der Staat, wenn er das Autonome System in seine Strukturen integriert hat, in der Lage sein, seine Politiken gegenüber allen Nutzern seines nationalen Netzwerks durchzusetzen. Diese Kontrolle hängt dabei nicht nur vom Netzwerkzugang ab, sondern von allen Geräten, dem Betriebssystem und den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

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

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

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

Abbildung 4: Einheiten des Cyberspace – Netzwerkdarstellung



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

9 Schlussbetrachtung

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

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

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

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

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

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

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

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

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

Literatur

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

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

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

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

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

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

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

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

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

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

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

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

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

Autor

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

DOI: 10.11588/josar.2015.0.23483

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