SWP

SWP-Studie

Daniel Voelsen

Risse im Fundament des Internets

Die Zukunft der Netz-Infrastruktur und die globale Internet Governance

Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

SWP-Studie 12
Mai 2019, Berlin

Das Fundament des Internets zeigt Risse. Zentrale Elemente der Netz-Infrastruktur gehen auf Entscheidungen zurück, die vor Jahrzehnten getroffen wurden. Seitdem aber hat sich der technische Kontext ebenso massiv verändert wie die politische Bedeutung des Internets.

Für die deutsche Digitalpolitik sind drei Konflikte um die Weiterentwicklung der Internet-Infrastruktur besonders bedeutsam. Der erste betrifft die Sicherheit und den Schutz der Privatsphäre im Adress-System des Internets, dem sogenannten Domain Name System (DNS). Zweitens schwelt ein Konflikt um die Sicherheit des Border Gateway Protocol (BGP) — jenes Protokolls, über das der Datenverkehr im Internet koordiniert wird. Drittens erweisen sich die Sicherheit und Verfügbarkeit der Unterseekabel als zunehmend problematisch, die das physische Rückgrat des globalen Internets bilden.

Bleiben diese Konflikte ungelöst, während zugleich weltweit die Anforderungen an das Internet weiter steigen, so wird dies zunehmend negative Folgen für Sicherheit, Privatsphäre und wirtschaftliche Entwicklung haben. Mehr noch: Es droht eine Spaltung des Internets bis auf die Ebene der Infrastruktur.

Dieses vielschichtige Konfliktfeld verlangt von der deutschen Politik ein klares strategisches Vorgehen. Ihren selbstgesetzten digitalpolitischen Ansprüchen gemäß sollte sie gleichermaßen das Ziel weltweiter Interoperabilität verfolgen und sich der beschriebenen Probleme im europäischen Rahmen annehmen. Die Herausforderung liegt darin, die Weiterentwicklung der Internet-Infrastruktur in Europa so zu gestalten, dass sie das gemeinsame globale Fundament des Internets ergänzt — und nicht weiter gefährdet.

SWP-Studie

Daniel Voelsen

Risse im Fundament des Internets

Die Zukunft der Netz-Infrastruktur und die globale Internet Governance

Stiftung Wissenschaft und Politik
Deutsches Institut für
Internationale Politik und Sicherheit

SWP-Studie 12
Mai 2019, Berlin

SWP-Studien unterliegen einem Verfahren der Begutachtung durch Fachkolleginnen und -kollegen und durch die Institutsleitung *(peer review)*, sie werden zudem einem Lektorat unterzogen. Weitere Informationen zur Qualitätssicherung der SWP finden Sie auf der SWP-Website unter https://www.swp-berlin.org/ueber-uns/qualitaetssicherung/. SWP-Studien geben die Auffassung der Autoren und Autorinnen wieder.

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3—4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-200
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1611-6372
doi: 10.18449/2019S12

Inhalt

Dr. Daniel Voelsen ist Wissenschaftler in der Forschungsgruppe Globale Fragen

Risse im Fundament des Internets. Die Zukunft der Netz-Infrastruktur und die globale Internet Governance

Die Lebensweise moderner Gesellschaften ist in wachsendem Maße darauf angewiesen, Informationen über das Internet auszutauschen. Dies gilt besonders für die Wirtschaft, immer mehr aber auch für Institutionen des Staates. Berichte über die politischen und wirtschaftlichen Folgen von Hacker-Angriffen illustrieren eindrücklich, wie unverzichtbar das Internet für öffentliche und private Institutionen geworden ist — und wie verletzbar sie dadurch sind.

Der Fokus liegt dabei meist auf den von Angriffen bedrohten Institutionen. Kaum beachtet wird in diesem Kontext dagegen die Infrastruktur des Internets. Eine Vielzahl von Protokollen und Standards bildet zusammen mit dem physischen Netz der Kabelverbindungen und Router diese Infrastruktur — und damit das globale Fundament des Internets. Ausgehend von den USA hat sich diese Infrastruktur im Laufe der 1990er Jahre weltweit entfaltet, und mit ihr das nicht minder komplexe Institutionengeflecht der globalen Internet Governance.

Zunehmend jedoch zeigen sich Risse im Fundament des Internets. Zentrale Elemente der Infrastruktur gehen auf Entscheidungen zurück, die vor Jahrzehnten getroffen wurden. Seitdem hat sich der technische Kontext ebenso massiv verändert wie die politische Bedeutung des Internets. Im Lichte der selbstgesetzten Ziele deutscher Digitalpolitik sind dabei drei Konflikte um die Internet-Infrastruktur von besonderer Bedeutung.

Erstens geht es um die Sicherheit des Domain Name System (DNS), also des technischen Systems zur Zuordnung von Domain-Namen und IP-Adressen. Entsprechende Konfigurationen, die einstmals sinnvoll waren, führen heute zu gravierenden Sicherheitslücken und bieten einfache Wege, um die Privatsphäre von Internet-Nutzern zu verletzen. Für diese Probleme existieren ausgereifte Lösungsvorschläge, die sich jedoch in den bisherigen Strukturen der Internet Governance nicht durchsetzen lassen.

Zweitens schwelt ein Konflikt um die Sicherheit des Routing-Systems. Das Border Gateway Protocol (BGP) stellt eine technische Möglichkeit bereit, um innerhalb der dezentralen Struktur des Internets den

Transport von Daten zu koordinieren. In den letzten Jahren jedoch häufen sich Fälle, in denen Staaten und private Akteure dieses Protokoll nutzen, um den Datenverkehr im Internet zu manipulieren. Auch hier gibt es Lösungsansätze, die nicht umgesetzt werden.

Drittens erweisen sich die Sicherheit und Verfügbarkeit von Unterseekabeln als zunehmend problematisch. Diese werden zum Großteil von Privatunternehmen betrieben, die sich in ihren Planungen in nachvollziehbarer Weise an wirtschaftlichen Kriterien orientieren. Allerdings hat dies zur Folge, dass einzelne Routen und Anlandepunkte häufig wiederverwendet werden — und so besonders verletzbare Knotenpunkte (»chokepoints«) entstehen. Zudem sind viele Entwicklungsländer nur unzureichend an das globale Netz der Unterseekabel angebunden. Hier besteht ein weithin verkannter Konflikt zwischen den Sicherheitsinteressen der Staaten und den Interessen der beteiligten Unternehmen.

Bleiben diese Konflikte ungelöst, während zugleich weltweit die Anforderungen an das Internet weiter steigen, so wird dies zunehmend negative Folgen für Sicherheit, Privatsphäre und wirtschaftliche Entwicklung haben. Zudem verweisen die Konflikte auf ein systemisches Problem der globalen Internet Governance. Prägend sind hier nichtstaatliche Akteure, allen voran private Unternehmen. In Form von Protokollen und Standards stellen sie wichtige öffentliche Güter bereit, doch haben sie weder wirtschaftliche Anreize noch die nötige Legitimation, um politische Konflikte durch autoritative Regelsetzung zu einem Ende zu bringen. Selbst dort, wo technisch ausgereifte Lösungen vorliegen, wird die Internet-Infrastruktur daher nicht in der notwendigen Weise weiterentwickelt.

Zwei Institutionen bieten sich im Prinzip dafür an, diese Lücke zu füllen: die Internet Corporation for Assigned Names and Numbers (ICANN) und die International Telecommunication Union (ITU). Beide jedoch erweisen sich bei genauerer Betrachtung als ungeeignet. In den aktuellen politischen Kontroversen um ICANN zeigt sich, dass die Organisation nicht über die erforderliche Legitimität verfügt, um jenseits eines begrenzten technischen Bereichs autoritative Vorgaben zu machen. Für die ITU als Sonderorganisation der Vereinten Nationen ist dieser Aspekt zwar weniger ein Problem; doch gibt es unter den Mitgliedstaaten der Institution einen fundamentalen Dissens in Fragen der Internet Governance, weshalb die ITU bei diesem Thema schon seit langem und wohl auch auf absehbare Zeit blockiert ist.

Vor diesem Hintergrund gewinnt die Sorge vor einer möglichen Spaltung des Internets besondere Brisanz. Auf Ebene der Internet-Dienste ist eine regulatorische Fragmentierung entlang staatlicher Grenzen schon heute praktische Realität. Die entscheidende Frage aber ist, ob diese Fragmentierung auf die Ebene der Internet-Infrastruktur übergreift. Die Unfähigkeit der heutigen Institutionen, die Probleme der globalen Internet-Infrastruktur zu lösen, schafft dafür einen Nährboden. So bieten etwa Unternehmen wie Google und Mozilla bereits jetzt eigene DNS-Dienste an. China und Russland signalisieren zudem immer wieder ihr Interesse, eine alternative Infrastruktur zu errichten. So wächst die Gefahr, dass aus den bisherigen Rissen im Fundament des Internets echte Brüche werden.

Diese Konfliktlage verlangt von der deutschen Politik eine klare strategische Ausrichtung. Den selbstgesetzten Zielen deutscher Digitalpolitik entsprechend sollte sie gleichermaßen das Ziel globaler Interoperabilität verfolgen *und* sich der beschriebenen Probleme im europäischen Rahmen annehmen. Die nicht triviale Herausforderung dabei ist, die Weiterentwicklung der Internet-Infrastruktur in Europa so zu gestalten, dass sie das gemeinsame globale Fundament des Internets ergänzt — und nicht weiter gefährdet.

Aus dieser Zielbestimmung ergeben sich drei Handlungsempfehlungen für die deutsche Politik. *Erstens* gilt es darauf hinzuwirken, ICANN auf jene technischen Kernfunktionen zu reduzieren, die für den Betrieb des DNS notwendig sind. Ein einheitliches DNS ist wesentlich für das Ziel globaler Interoperabilität, und in ebendiesem Bereich wird die Autorität von ICANN aus funktionalen Erwägungen weithin anerkannt. *Zweitens* sollte die deutsche Politik ihren Einfluss in der ITU und im Internet Governance Forum (IGF) nutzen, um »Multistakeholder«-Institutionen überall dort Rückhalt zu bieten, wo sie wichtige Beiträge zur technischen Weiterentwicklung der globalen Internet-Infrastruktur leisten. *Drittens* schließlich sollte Deutschland sich dafür einsetzen, jene Probleme dieser Infrastruktur, die auf globaler Ebene aktuell nicht lösbar sind, soweit wie möglich innerhalb der EU zu bewältigen. Dies sollte im wohlverstandenen Eigeninteresse geschehen, zugleich aber auch als Impuls für die globale Entwicklung.

Internet Governance als Aufgabe für die deutsche Politik

Der Begriff »Internet Governance« ist politisch umkämpft. Für die wissenschaftliche Analyse ist dies kein geringes Problem, ist damit doch schon der Gegenstand selbst umstritten.[1] Eine Möglichkeit, dem zu begegnen, besteht darin, den Begriff Internet Governance auch wissenschaftlich so weit zu fassen, dass er alle politischen Phänomene abdeckt, die irgendwie mit dem Internet zu tun haben.[2] In der vorliegenden Studie jedoch soll die Praxis der Internet Governance anhand einer enger gefassten analytischen Konzeption von Governance erschlossen werden, die zugleich die politische Bedeutung dieser Praxis hervorhebt.

Governance

Den Ausgangspunkt für das hier vorgeschlagene Verständnis von Internet Governance bildet eine Governance-Definition, wie sie in der jüngeren politikwissenschaftlichen Debatte prominent von Thomas Risse und Tanja Börzel aufgestellt wurde. Sie bestimmen Governance als institutionalisierte Formen politischer Steuerung, »die auf die Herstellung und Implementierung verbindlicher Regelungen bzw. auf die Bereitstellung kollektiver Güter abzielen«.[3] Legt man dieses Verständnis von Governance zugrunde, so definiert sich Internet Governance als die Summe all jener institutionalisierten Formen politischer Steuerung, die darauf abzielen, mit Bezug auf das Internet verbindliche Regeln zu setzen und/oder kollektive Güter bereitzustellen.

Bewusst offengehalten ist dabei, welche Akteure es sind, die Regeln setzen bzw. Güter bereitstellen, und auf welche Weise sie das tun. Dies soll insbesondere dafür sensibilisieren, dass Governance nicht immer nur Sache des Staates ist. Zugleich lenkt die Definition den Blick darauf, dass es um die *intentionale* Bereitstellung kollektiver *Güter* geht. Nichtintendierte Effekte sind demnach ebenso wenig als Governance zu bezeichnen wie die bewusste Koordination zur Verbreitung von Übeln (etwa in Form organisierter Kriminalität).[4]

In konkreten Governance-Konstellationen manifestieren sich dabei auch stets die Machtverhältnisse zwischen den beteiligten Akteuren. So erklärt sich, warum Governance immer rechtfertigungsbedürftig ist. Dies gilt in besonderem Maße für die Setzung und Durchsetzung kollektiv verbindlicher Regeln, also die Ausübung von Autorität. Doch auch bei der Bereitstellung kollektiver Güter entsteht Rechtfertigungsbedarf, wenn sie vor dem Hintergrund bestehender Machtasymmetrien erfolgt und diese fortzuführen droht.

Aufgaben und Ziele deutscher Politik

So technisch Internet Governance oftmals erscheinen mag, geht es hier im Kern doch um Grundfragen des Politischen. Welche Institutionen und Akteure haben das Recht, auf Basis welcher Verfahren Regeln zu setzen, also Autorität auszuüben? Welche Institutionen und Akteure sind dafür verantwortlich, welche kollektiven Güter bereitzustellen, und zu welchen Bedingungen? Welche Interessen werden dabei

1 Vgl. Jeanette Hofmann, »Internet Governance. Theoretische und empirische Annäherungen an einen schwer fassbaren Gegenstand«, in: *Journal of Self-Regulation and Regulation*, 1 (2015), S. 31–45; Julia Pohle/Maximilian Hösl/Ronja Kniep, »Analysing Internet Policy as a Field of Struggle«, in: *Internet Policy Review*, 5 (2016) 3, S. 1–21.

2 Vgl. etwa Laura DeNardis, *Protocol Politics. The Globalization of Internet Governance*, Cambridge/MA 2009, S. 14.

3 Anke Draude/Thomas Risse/Cord Schmelzle, *Grundbegriffe der Governanceforschung*, Berlin 2012 (SFB Governance Working Paper Series, Nr. 36), S. 6.

4 Tanja Börzel/Thomas Risse, »Governance without a State. Can It Work?«, in: *Regulation & Governance*, 4 (2010), S. 113–134 (115).

Box 1:
Öffentliche und kollektive Güter

Öffentliche Güter zeichnen sich in Abgrenzung zu privaten Gütern dadurch aus, dass (a) der Zugang zu ihnen allen gleichermaßen freisteht (Nicht-Ausschließbarkeit) und dass (b) die Nutzung des Gutes durch eine Person die Nutzung für andere nicht einschränkt. Beide Bedingungen beruhen auf politischen Vorgaben. Ob etwa Wissen als öffentliches oder privates Gut behandelt wird, ist keineswegs in der Sache selbst angelegt. Kollektive Güter unterscheiden sich von öffentlichen dadurch, dass nur eine dieser zwei Bedingungen erfüllt sein muss.[5]

verfolgt, und wie wirkt sich dies auf Machtbeziehungen aus?[6]

So wie das Internet ein globales Kommunikationsnetz ist, so haben auch diese Fragen globale Reichweite — und fallen somit immer auch in den Bereich der Außenpolitik. Traditionell jedoch wird Internet Governance in vielen Staaten vorrangig als wirtschaftspolitisches Thema behandelt. Auch in Deutschland liegt die entsprechende Federführung innerhalb der Bundesregierung beim Wirtschaftsministerium (BMWi). Insbesondere ist dieses dafür zuständig, Deutschland bei der ITU und bei ICANN zu vertreten; außerdem ist das BMWi dafür verantwortlich, das Internet Governance Forum (IGF) 2019 zu organisieren (siehe Box 3, S. 12). Regelmäßig beteiligt sind dabei das Bundesministerium für Verkehr und digitale Infrastruktur (BMVI), das Bundesministerium des Innern, für Bau und Heimat (BMI) und das Auswärtige Amt (AA). Dieser Ressortzuständigkeit entspricht auch der Umgang mit dem Thema im Bundestag; allerdings finden insbesondere Fragen der *globalen* Internet Governance hier nur wenig Aufmerksamkeit.

Da es bisher keine breitere Debatte über die globale Internet-Infrastruktur gibt, sind auch die öffentlichen Äußerungen zu den Zielen deutscher Politik begrenzt. Nichtsdestotrotz lassen sich aus den allgemeinen Grundsätzen deutscher Außenpolitik, aus der 2014 von der Bundesregierung veröffentlichten »Digitalen Agenda« sowie aus einzelnen Stellungnahmen vor allem des BMWi einige grundsätzliche Zielsetzungen ableiten:

- *#Z1: Förderung der digitalen Wirtschaft.* Über alle politischen Lager hinweg wird das Internet in Deutschland als Chance für die wirtschaftliche Entwicklung wahrgenommen. Zwar wird immer wieder auch auf die negativen Folgen des Internets für Teile des Arbeitsmarktes verwiesen, doch überwiegen die positiven Erwartungen. Zuletzt hat etwa das Schlagwort »Industrie 4.0« viel Aufmerksamkeit erfahren. In der »Digitalen Agenda« von 2014 findet sich ein expliziter Verweis auf das ordnungspolitische Ziel eines freien und fairen Wettbewerbs.[7] Im Kontext der politischen Diskussionen um die globale Internet Governance lässt sich dies als Zielsetzung verstehen, das Internet als weltweites Kommunikationsmedium für wirtschaftliche Aktivitäten zu erhalten und nach Möglichkeit weiter auszubauen.
- *#Z2: Verstärkung der Sicherheit von IT-Systemen.* Die Sicherheit von IT-Systemen nimmt hierzulande in der digitalpolitischen Debatte einen hohen Stellenwert ein. Viel Aufmerksamkeit hat das Thema in den letzten Jahren durch die publik gewordenen Hackerangriffe auf den Bundestag und das Netz der Bundesregierung erfahren. Hinzu kommen Klagen von Unternehmen über die Zunahme wirtschaftlich motivierter Angriffe. Das Ziel, die Nutzung des Internets für öffentliche Stellen und Unternehmen, aber auch für individuelle Bürgerinnen und Bürger sicher zu gestalten, lässt sich auf die Ebene der globalen Internet Governance ausweiten: Ein ausreichendes Maß an Sicherheit bei der globalen Internet-Infrastruktur ist Voraussetzung für die Sicherheit von Internet-Diensten, die sich dieser Infrastruktur bedienen.
- *#Z3: Schutz der Menschenrechte auch im digitalen Raum.* Die Menschenrechte gelten als einer der zentralen normativen Orientierungspunkte deutscher Außenpolitik. Gerade in den letzten Jahren wurde dabei von Seiten der Bundesregierung immer wieder hervorgehoben, dass dies auch den digitalen Raum betreffe. Ein deutliches Zeichen in diesem Sinne setzt Deutschland mit seinem Engagement in der Freedom Online Coalition (FOC). Im Fokus stehen dabei vor allem das Recht auf Privat-

5 Tanja Börzel/Thomas Risse/Anke Draude, »Governance in Areas of Limited Statehood. Conceptual Clarifications and Major Contributions of the Handbook«, in: Tanja Börzel u.a. (Hg.), *The Oxford Handbook of Governance and Limited Statehood*, Oxford 2018, S. 3—25.

6 Vgl. hierzu Laura DeNardis, *The Global War for Internet Governance*, New Haven/CT 2014.

7 Die Bundesregierung, *Digitale Agenda 2014–2017*, Berlin 2014, S. 4, <https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/digitale-agenda.pdf> (eingesehen am 14.3.2019).

sphäre sowie das Recht auf Meinungs- und Pressefreiheit.[8] Ende 2018 hat sich die Bundesregierung dem von Tim Berners-Lee vorgeschlagenen Entwurf für einen »Contract for the Web« angeschlossen, der den freien Zugang zum Internet und das Recht auf Privatsphäre betont.[9] Diesem wiederholten Bekenntnis zur Geltung der Menschenrechte im digitalen Raum lassen sich Ziele auch für die Ebene der Internet-Infrastruktur entnehmen. Schließlich werden hier die technischen Weichen dafür gestellt, ob und in welchem Maße etwa Zensur ermöglicht oder die Privatsphäre der Internet-Nutzer geschützt wird.

- *#Z4: Stärkung der »Multistakeholder«-Governance.* Speziell mit Blick auf den Kontext der globalen Internet Governance gibt es seit vielen Jahren ein explizites Bekenntnis der Bundesregierung zur Multistakeholder-Governance. So hat sich etwa das BMWi gemeinsam mit einer Reihe deutscher Interessengruppen 2015 klar dafür ausgesprochen, die Verwaltung des DNS (siehe Box 2, S. 12) an ICANN zu übergeben. Zur Begründung wurde gerade auch darauf verwiesen, dass diese Institution im Sinne des Multistakeholder-Modells organisiert sei.[10] Die Enquete-Kommission »Internet und digitale Gesellschaft« hat sich in einem Bericht von 2013 ebenfalls klar in diesem Sinne positioniert. Nicht zuletzt unterstützt die Bundesregierung prominent das IGF (siehe Box 3, S. 12), indem es das Forum 2019 im eigenen Land ausrichtet.
- *#Z5: Bewahrung von Interoperabilität.* Das Bekenntnis zu den bisherigen Strukturen der Multistakeholder-Governance ist meist verknüpft mit dem Ziel der Interoperabilität.[11] Gemeint ist damit schlicht die Möglichkeit, dass die verschiedenen Elemente des Internets bei aller technischen Vielfalt im Prinzip miteinander kommunizieren können. Das Internet besteht aus zahlreichen Teilnetzen, verbindet unterschiedlichste Gerätetypen und wird zu verschiedensten Zwecken genutzt. Nicht immer ist der Datenaustausch über diese vielfältigen Nutzungsformen hinweg erwünscht; im Prinzip ist er aber so lange möglich, wie alle dieselbe Infrastruktur nutzen. Der technische Begriff der Interoperabilität lässt sich mithin in das politische Ziel übersetzen, die weltweit einheitliche Infrastruktur des Internets zu erhalten.

8 Auswärtiges Amt, *Cyber-Außenpolitik*, <https://www.auswaertiges-amt.de/de/aussenpolitik/themen/cyber-aussenpolitik> (eingesehen am 14.3.2019).

9 Marie-Charlotte Matthes, »Schnelles und offenes Internet für alle: Bundesregierung unterzeichnet ›Contract for the web‹«, *netzpolitik.org (online)*, 28.11.2018, <https://netzpolitik.org/2018/schnelles-und-offenes-internet-fuer-alle-bundesregierung-unterzeichnet-contract-for-the-web/> (eingesehen am 14.3.2019).

10 BMWi, *Position deutscher Interessengruppen. Leitlinien und Handlungsempfehlungen zur Überleitung der Aufsicht über die IANA-Funktionen*, Berlin 2015.

11 Vgl. etwa Deutscher Bundestag, 17. Wahlperiode, Drucksache 17/12480, *Elfter Zwischenbericht der Enquete-Kommission »Internet und digitale Gesellschaft«. Internationales und Internet Governance*, 28.2.2013, S. 20.

Das bisherige Modell der Internet Governance

Die Ursprünge des Internets gehen auf erhebliche Investitionen der öffentlichen Hand zurück. Ein wesentlicher Treiber war dabei das Interesse des US-Militärs an einem dezentralen Kommunikationssystem. Zu Beginn der 1990er Jahre jedoch entschied sich die Clinton-Administration für eine weitreichende Politik der Privatisierung. Die Aufgabe, das Internet weiterzuentwickeln und eine entsprechende Infrastruktur für die breite Bevölkerung zu schaffen, wurde privaten Unternehmen anvertraut.[12]

Im Zuge der globalen Ausbreitung des Internets wurde dieses Modell von den meisten Staaten übernommen. So erfolgt der Zugang zum Internet in der Regel über private Internet Service Provider (ISP), die sich entweder direkt mit weltweit agierenden Netzbetreibern oder vermittelt über ebenfalls privat betriebene Internetknotenpunkte (IXP) mit dem globalen Netzwerk verbinden. Letzteres wiederum besteht aus einem Komplex an Glasfaser- und Satellitenverbindungen, der ebenfalls zum größten Teil in privater Hand liegt.

Diese hervorgehobene Rolle privater Akteure spiegelt sich auch in den heutigen Strukturen der Internet Governance. Zwar unterstehen ISPs, IXPs und ebenso die Anbieter von Internet-Anwendungen den gesetzlichen Vorgaben der Staaten, in denen sie ihre Dienste offerieren. Jene technischen Standards jedoch, die global und auch innerstaatlich die Grundlage für die Kommunikation im Internet schaffen, werden von privaten Akteuren entwickelt. Nichthierarchische Kooperation bildet hier die dominante Form von Governance (siehe S. 7), ergänzt um den sachlich eng begrenzten Autoritätsanspruch von ICANN (vgl. Tabelle 1).

12 Ev Ehrlich, »Thanks To Bill Clinton, We Don't Regulate the Internet Like a Public Utility«, *Forbes (online)*, 17.5.2014, <https://www.forbes.com/sites/realspin/2014/03/17/thanks-to-bill-clinton-we-dont-regulate-the-internet-like-a-public-utility/> (eingesehen am 19.12.2018).

Analytisch hilfreich ist dabei die Unterscheidung zwischen *Internet-Diensten* und *Internet-Infrastruktur*. Seit den 1990er Jahren ist eine Vielzahl an Internet-Diensten entstanden, von einfachen Websites und Chatrooms bis hin zu den sozialen Netzwerken und Messaging-Diensten von heute.

Die Funktionsweise des Internets basiert darauf, dass all diese verschiedenen Dienste letztlich auf einem überschaubaren Set von Basis-Protokollen zur Übertragung von Daten aufbauen. Diese Protokolle werden als *logische Infrastruktur* des Internets bezeichnet (wobei »logisch« hier im Wesentlichen als Verweis auf Software zu verstehen ist). Sie sollen es ermöglichen, die vielfältigen Nutzungsformen des Internets in einer einheitlichen technischen Struktur zusammenzuführen. Diese Struktur folgt einer geschichteten Architektur; die höheren Schichten (»layers«) enthalten dabei spezifischere Protokolle und fußen auf den unteren Schichten. Es ist heute üblich, die Gesamtheit der logischen Infrastruktur mit dem Modell des Transmission Control Protocol/Internet Protocol (TCP/IP) zu beschreiben. Hinzu kommt die *physische Infrastruktur* in Form von Kabelverbindungen, Routern und Servern.

Globale Standards

Die logische Infrastruktur des Internets besteht also aus einer Reihe von aufeinander aufbauenden Standards und Protokollen. Prominente Beispiele dafür sind etwa die Hypertext Markup Language (HTML) zur Darstellung von Websites oder auch der Unicode-Standard zur Zusammenführung verschiedener Schrift- und Zeichensysteme. Zum ganz überwiegenden Teil werden solche Standards und Protokolle von privaten Akteuren bereitgestellt.

Diese finden in Institutionen wie der Internet Engineering Task Force (IETF), dem Institute of Electrical and Electronics Engineers (IEEE) oder dem

Tabelle 1

Das Feld der globalen Internet Governance

	Autoritative Setzung von Regeln	**Bereitstellung öffentlicher/ kollektiver Güter**
Internet-Dienste	Staat: Gesetze	Zivilgesellschaft: z.B. creative commons, open source
Internet-Infrastruktur		
logisch (TCP/IP)		
application layer (z.B. http, ftp, DNS)	ICANN: DNS	IETF, W3C: Standards
transport layer (z.B. TCP, UDP)	—	IETF: Standards
network layer (z.B. IP)	—	IETF: Standards
network access layer (z.B. Ethernet)	—	IEEE, ITU: Standards
physisch		
Kabel, Router, Server (IXPs, ISPs)	Staat: Gesetze	IETF, IEEE: Standards

World Wide Web Consortium (W3C) zusammen. Im Prinzip steht die Teilnahme dabei allen Interessierten offen. Tatsächlich aber ist das technische Niveau, dessen es dazu bedarf, so hoch, dass sich hier vor allem Vertreter und Vertreterinnen aus einschlägigen Unternehmen sowie in begrenztem Umfang aus der Wissenschaft versammeln. Einen Eindruck von der üblichen Zusammensetzung solcher Institutionen bietet das Internet Architecture Board (IAB), das innerhalb der IETF in begrenztem Umfang eine Art Aufsichtsfunktion über die Prozesse der Standardsetzung ausübt. Von den zwölf Mitgliedern dieses Gremiums arbeiten aktuell zehn für Unternehmen aus der Internet-Branche, hinzu kommen zwei Wissenschaftler von Universitäten.[13]

Die Standards und Protokolle, die in Foren wie IETF, IEEE oder W3C entwickelt werden, sind öffentliche Güter (siehe Box 1, S. 8). Sie werden öffentlich zur Verfügung gestellt, sind für jeden frei nutzbar (Nicht-Ausschließbarkeit) und können von unbegrenzt vielen Leuten verwendet werden (Nicht-Rivalität). Tatsächlich ist es sogar im Interesse aller Beteiligten, dass diese öffentlichen Güter eine möglichst starke Nutzung erfahren.[14]

Entwickelt werden die Standards auf Basis freiwilliger Kooperation. Auch die Verbreitung der Standards erfolgt der Form nach freiwillig. Eine Institution wie IETF kann weder Staaten noch Unternehmen vorschreiben, welche Standards sie zu nutzen haben. In diesem Sinne handelt es sich hier um die nichthierarchische Bereitstellung eines öffentlichen Gutes (siehe Tabelle 1).

Die Abwesenheit formaler Hierarchien bedeutet jedoch nicht, dass es keine Machtbeziehungen gäbe. Insbesondere die jeweils betroffenen Unternehmen versuchen, in Gremien wie IETF ihre Interessen durchzusetzen. Ein aktuelles Beispiel dafür ist das starke Engagement des chinesischen Unternehmens Huawei bei der Ausgestaltung des neuen Mobilfunkstandards 5G.[15] Auch setzen Unternehmen immer wieder gezielt ihre Marktmacht ein, um bestimmten Standards zum Durchbruch zu verhelfen.

13 *Internet Architecture Board – Members*, <https://www.iab.org/about/iab-members/> (eingesehen am 18.4.2019).

14 Joseph S. Nye, *The Regime Complex for Managing Global Cyber Activities*, Waterloo: Global Commission on Internet Governance, 2014, S. 6, <https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf> (eingesehen am 14.9.2018).

15 Raymond Zhong, »China's Huawei Is at Center of Fight Over 5G's Future«, in: *The New York Times (online)*, 7.3.2018, <https://www.nytimes.com/2018/03/07/technology/china-huawei-5g-standards.html> (eingesehen am 6.2.2019). Siehe dazu auch Daniel Voelsen, *5G, Huawei und die Sicherheit unserer Kommunikationsnetze. Handlungsoptionen für die deutsche Politik*, Berlin: Stiftung Wissenschaft und Politik, Februar 2019 (SWP-Aktuell 5/2019).

Box 2:
Das Domain Name System (DNS)

Als globales Kommunikationsnetz basiert das Internet darauf, dass sich im Prinzip alle damit verbundenen Geräte untereinander austauschen können. Dies setzt voraus, dass alle Geräte über individuelle Adressen verfügen. Dazu wird jedem Gerät (zumindest temporär) eine numerische IP-Adresse zugewiesen. Das bisher übliche Format für solche IP-Adressen ist IPv4 (zum Beispiel 192.0.43.7). Der neue Standard IPv6 (zum Beispiel 2606:2800:220:1:248:1893:25c8:1946) bietet einen sehr viel größeren Adressraum und wird seit einigen Jahren parallel zum bisherigen Standard IPv4 eingeführt. Domain-Namen (z.B. www.example.com), die auf ebendiese IP-Adressen verweisen, sollen menschlichen Nutzern den Austausch im Internet erleichtern.

Das globale Adressverzeichnis des Internets verknüpft in diesem Sinne Domain-Namen und IP-Adressen. Es besteht aus einer Vielzahl von Datenbanken, die jeweils bestimmte Adressbereiche abdecken. Viele Internet Service Provider (ISP) halten zudem Kopien der für ihre Kunden wichtigsten Daten im eigenen Netzwerk bereit. Die Gesamtheit dieser Netzwerke wird als Domain Name System (DNS) bezeichnet. Entgegen der weitverbreiteten Rhetorik vom Internet als dezentralem Netzwerk ist das DNS streng hierarchisch organisiert. Die verschiedenen Teildatenbanken für einzelne Adressbereiche (wie zum Beispiel die Domain .de) sind über eine zentrale Datenbank miteinander verknüpft, die sogenannte DNS Root Zone.

Box 3:
Das Internet Governance Forum (IGF)

Die Vereinten Nationen haben die Idee der Multistakeholder-Governance prominent durch Gründung des Internet Governance Forum (IGF) aufgegriffen. Das IGF wurde im Rahmen des World Summit on the Information Society (WSIS) 2005 ins Leben gerufen; seither hat die UN-Generalversammlung das entsprechende Mandat zweimal verlängert. Im Kern besteht das IGF aus einer jährlichen Konferenz, zu der die verschiedenen Stakeholder aus aller Welt zusammenkommen. Es hat dabei explizit kein Mandat, um verbindliche Entscheidungen zu treffen. Vielmehr sollen die Diskussionen des Forums eine Grundlage für freiwillige Kooperation und für bindende Beschlüsse in anderen Institutionen bilden.

Nach anfänglichem Enthusiasmus befindet sich das IGF heute in einer schwierigen Situation. Sein Alleinstellungsmerkmal, die Anbindung an die Verfahren des UN-Systems, wird zunehmend als Einschränkung wahrgenommen. Das unter anderem von Milton Mueller gegründete Internet Governance Project (IGP) etwa kritisiert den großen Einfluss, den sich die Staaten dadurch sichern. Außerdem befürchtet IGP, dass zunehmend nur noch Staaten aus der OECD-Welt das Forum ausrichten könnten, weil die UN so hohe Anforderungen an den jeweiligen Gastgeber stellten.[17]

Symptomatisch waren vor diesem Hintergrund die Schwierigkeiten, ein Gastland für das IGF 2018 zu finden. Erst wenige Monate vor dem geplanten Termin zeigte sich Frankreich bereit, das Treffen auszurichten. Dabei konnten die Räumlichkeiten der UNESCO genutzt werden, um den Anforderungen für UN-Konferenzen gerecht zu werden. Der französische Präsident Emmanuel Macron verband die Veranstaltung zeitlich mit gleich zwei weiteren langgeplanten internationalen Digitalkonferenzen der französischen Regierung — und verlieh damit seiner Forderung Nachdruck, das IGF stärker an multilaterale Entscheidungsprozesse anzubinden.[18] 2019 ist Deutschland Gastgeber des IGF.

Autoritative Regelsetzung durch ICANN

Eine besondere Stellung im Gefüge der globalen Internet Governance nimmt die Internet Corporation for Assigned Names and Numbers ein. Zum einen setzt sie in autoritativer Weise kollektiv verbindliche Regeln für das Domain Name System (DNS, siehe Box 2). So legt ICANN fest, wie und zu welchen Bedingungen Domain-Namen und IP-Adressen im Internet vergeben werden.[16] Zum anderen stellt die Organisation ein für die globale Infrastruktur des

16 Ausführlicher hierzu siehe Daniel Jacob, *Mehr als nur ein Adressbuch. Wie ICANN politische Autorität ausübt und warum es darüber zunehmend Streit gibt*, 2018, <https://www.theorieblog.de/index.php/2018/06/mehr-als-nur-ein-adressbuch-wie-icann-politische-autoritaet-ausuebt-und-warum-es-darueber-zunehmend-streit-gibt/> (eingesehen am 25.6.2018).

17 International Governance Project (IGP), *International Internet Policy Priorities. IGP Advises the NTIA*, Atlanta/GA 2018, S. 1—14 (12ff), <https://www.ntia.doc.gov/files/ntia/publications/igp-comments.pdf> (eingesehen am 3.7.2018). Siehe auch Milton Mueller, *The Paris IGF: Convergence on Norms, or Grand Illusion?*, International Governance Project, 9.11.2018, <https://www.internetgovernance.org/2018/11/09/the-paris-igf-convergence-on-norms-or-grand-illusion/> (eingesehen am 14.11.2018).

18 Internet Governance Forum, »IGF 2018 Speech by French President Emmanuel Macron«, 13.11.2018, <https://www.intgovforum.org/multilingual/content/igf-2018-speech-

Internets zentrales öffentliches Gut bereit, indem sie die DNS Root Zone verwaltet, die zentrale Datenbank im Adress-System des Internets.[19]

Legitimation durch Multistakeholder-Governance

Wie jede Institutionenordnung ist auch das heutige System der globalen Internet Governance rechtfertigungsbedürftig. Zu seiner Legitimierung wird immer wieder auf die technische Expertise von Institutionen wie ICANN und IETF verwiesen, ebenso auf den freiwilligen Charakter der entwickelten Standards und Protokolle.[20]

Mit Blick auf die spezifisch politische Dimension der Internet Governance hat zudem die Idee der Multistakeholder-Governance weite Verbreitung gefunden. Grundgedanke ist dabei, all jene einzubeziehen, für die die weitere Entwicklung des Internets mit einem spezifischen »Einsatz« (stake) verbunden ist. In der Praxis werden hierzu üblicherweise Unternehmen, Staaten, die Wissenschaft sowie verschiedene Akteure der Zivilgesellschaft gezählt. Prägend für IETF und W3C etwa ist die offene und weitgehend informelle Einbeziehung von Unternehmen, unabhängigen Experten sowie Wissenschaftlern. Und auch ICANN hat eine Reihe von Beratungsgremien, die in formalisierten Verfahren an den Entscheidungen des ICANN-Vorstands beteiligt werden.

by-french-president-emmanuel-macron> (eingesehen am 13.12.2018).

19 Siehe hierzu <https://pti.icann.org> sowie <https://www.iana.org>.

20 Vgl. Monika Ermert, »Missing Link. Der Angriff auf das offene Internet und die Ethik des Netzes«, *heise online*, 5.8.2018, <https://www.heise.de/newsticker/meldung/Missing-Link-Der-Angriff-auf-das-offene-Internet-und-die-Ethik-des-Netzes-4129289.html> (eingesehen am 4.9.2018).

Konflikte um die globale Infrastruktur des Internets

Mit den bisherigen Strukturen der Internet Governance ist es gelungen, die Möglichkeiten zur Nutzung des Internets massiv auszuweiten. Zu den wichtigsten Veränderungen in jüngerer Zeit zählt der Zugang zum Internet über mobile Geräte. Hinzu kommen — nicht nur in sozialen Medien — Formen der interaktiven Nutzung, häufig umschrieben mit dem Schlagwort »Web 2.0«. Ein wichtiger Trend ist zudem die wachsende Bedeutung der »cloud«. Dabei verlagern sich Datenspeicherung und -verarbeitung weg vom Einzelgerät hin zu großen Datenzentren. Das mobile Internet und die »cloud« bilden die Grundlage für jene Entwicklung, von der erwartet wird, dass sie die nächsten Jahre prägen wird: die Vernetzung von immer mehr Geräten in Wirtschaft, Verwaltung und privaten Haushalten im Sinne des »Internets der Dinge«.

Doch zeigt sich auch, dass das bisherige Modell der Internet Governance bei genuin politischen Konflikten systemisch an seine Grenzen stößt. Erklärungen dafür finden sich in der politikwissenschaftlichen Governance-Forschung:

- #E1: Erstens wird die nichtstaatliche Governance durch die bloße Anzahl der beteiligten Akteure in ihren Möglichkeiten begrenzt. Freiwillige Koordination setzt ein Mindestmaß an Vertrauen voraus, gibt es doch keine Instanz, die Fehlverhalten autoritativ sanktionieren kann. In kleinen sozialen Gruppen schaffen persönliche Kontakte Vertrauen; zugleich gibt es hier Wege, durch verschiedene Formen sozialer Ächtung unerwünschtes Verhalten zu ahnden.[21] Betrachtet man die Geschichte der Internet Governance, so fällt auf, dass diese anfangs tatsächlich noch stark von persönlichen Beziehungen geprägt war. In der geläufigen Rede von den »Vätern des Internets« kommt ein entsprechend personalisiertes Verständnis von Governance zum Ausdruck — und zudem der Unwille, den Beitrag von Frauen wie Sharla Boehm oder Elizabeth »Jake« Feinler zur Entwicklung des Internets anzuerkennen.[22] Mit dessen globaler Ausweitung jedoch hat sich die Zahl der beteiligten Akteure deutlich erhöht. Auch wenn es sich empirisch schwer messen lässt, ist davon auszugehen, dass auf persönlichen Beziehungen basierendes Vertrauen entsprechend nachgelassen hat.
- #E2: Ein systematisches Problem für nichthierarchische Governance entsteht zweitens dann, wenn es keine Einigkeit über die zu erbringenden Leistungen gibt. In diesem Fall sinkt die Bereitschaft zu freiwilliger Kooperation, und es tritt schnell zutage, dass nichtstaatliche Formen von Governance oft nicht über die notwendige Legitimität für derartige Entscheidungen verfügen.[23] In der Internet Governance zeigt sich das Problem vor allem darin, dass immer mehr Staaten das Internet als Mittel zur Durchsetzung ihrer jeweiligen Interessen verstehen — und so untereinander sowie mit nichtstaatlichen Akteuren der Internet Governance in Konflikt geraten.
- #E3: Eng damit verbunden ist ein drittes Problem nichtstaatlicher Governance, dass diese — wenig überraschend — von den Interessen privater Akteure bestimmt wird. Im Falle der Internet Governance sind dies vor allem Unternehmen, deren primärer Organisationszweck die Mehrung des eigenen Profits ist. Eine solche nichtstaatliche Governance ist daher ungeeignet für Probleme, deren Lösung keinen Profit bringt oder gar Kosten

21 Anke Draude/Lasse Hölck/Dietlind Stolle, »Social Trust«, in: Börzel u.a. (Hg.), *The Oxford Handbook of Governance* [wie Fn. 5], S. 3–25.

22 Zur Frage nach den »Müttern des Internets« siehe die Antworten auf den folgenden Tweet: <https://twitter.com/d_voelsen/status/1098898783004446726>.

23 Daniel Jacob/Bernd Ladwig/Cord Schmelzle, »Normative Political Theory«, in: Börzel u.a. (Hg.), *The Oxford Handbook of Governance* [wie Fn. 5], S. 564–583.

verursacht. Ein Beispiel ist die noch immer geringe Ausbreitung von IPv6-Adressen (siehe Box 2, S. 12). Diese bieten eine Antwort darauf, dass die Zahl der nach dem bisherigen Standard IPv4 verfügbaren Adressen begrenzt ist und langfristig nicht ausreichen wird, um alle Geräte direkt mit dem Internet zu verbinden. Die Umstellung auf IPv6 ist politisch wenig umstritten, steht aber im Konflikt zu den wirtschaftlichen Interessen der Netzwerkbetreiber. Diese sind bisher nicht gewillt, für die Umstellung Kosten zu tragen, die sie ihren Kunden nicht vermitteln können.[24]

Sicherheit und Privatsphäre im Domain Name System (DNS)

Das DNS ist ein wesentliches Element der logischen Infrastruktur des Internets (siehe Box 2, S. 12). In seiner heutigen Form birgt dieses System allerdings erhebliche Schwachstellen. Aus Sicherheitsperspektive besteht das drängendste Problem im sogenannten »DNS poisoning«. Dabei werden die DNS-Informationen in einem Teilnetzwerk so manipuliert, dass eine Anfrage des Nutzers zu einer Domain auf eine andere als die eigentlich registrierte IP-Adresse verweist. Der Aufruf der Domain example.com würde dann etwa zu einer Seite führen, die für den Nutzer aussieht wie die Originalseite, tatsächlich aber eine Kopie ist, die dazu dient, Schadsoftware auf den Computer des Nutzers zu laden oder dort kritische Daten wie etwa Passwörter auszulesen.

Ein mittlerweile recht weit verbreiteter Versuch, diesem Problem zu begegnen, besteht in der Ausstellung verschlüsselter Zertifikate (siehe Box 4). Diese können für sich genommen »DNS poisoning« nicht verhindern, bieten aber doch einen gewissen Schutz vor entsprechenden Angriffen. Wird eine Anfrage an example.com auf eine andere IP-Adresse umgeleitet, kann der aufgerufene Server nicht das zu example.com gehörende SSL-Zertifikat senden — und es erscheint eine entsprechende Warnung im Browser. Das Problem ist allerdings, dass die heute existierenden SSL-Zertifikatssysteme eigene Sicherheitslücken aufweisen und noch immer nur auf 70 bis 80 Prozent aller Websites eingesetzt werden.[25] Hinzu kommt, dass viele Websites veraltete oder falsch konfigurierte Varianten des SSL-Protokolls verwenden.[26] Überdies ist es möglich, legitim wirkende SSL-Zertifikate auf »gefälschten« Websites einzubinden. Mit entsprechendem Aufwand kann ein Internet-Nutzer so auf eine Seite umgeleitet werden, die der Originalseite nicht nur ähnlich sieht, sondern auch vermeintlich sichere SSL-Verschlüsselung anbietet.[27]

Die sogenannten Domain Name System Security Extensions (DNSSEC) sollen direkt Abhilfe gegen »DNS poisoning« schaffen. Sie dienen dazu, DNS-Daten digital zu signieren. Damit soll sichergestellt werden, dass DNS-Daten von vertrauenswürdigen Quellen stammen. DNSSEC gilt allerdings als kompliziert und entsprechend fehleranfällig.[28]

In seiner bestehenden Form bietet das DNS zudem weitreichende Möglichkeiten, in die Privatsphäre von Internet-Nutzern einzugreifen. Alle Anfragen an das

Box 4: Verschlüsselung (TLS, SSL, HTTPS)

Daten verschiedener Art werden für die Übertragung durch das Internet mit dem Protokoll Transport Layer System (TLS) verschlüsselt. Dieses Protokoll ist der Nachfolger des lange genutzten Protokolls Secure Socket Layer (SSL). Bekannt ist die Nutzung von TLS bei der Darstellung von Websites; dazu wird das Protokoll Hypertext Transfer Protocol (HTTP) um eine Verschlüsselungskomponente ergänzt (HTTPS). Bietet ein Webserver derartige Verschlüsselung an, ist das an der Adresse der Website erkennbar. Diese beginnt dann mit »https« statt mit »http« (z.B. https://www.swp-berlin.org). Zudem weisen viele moderne Browser mittlerweile darauf hin, wenn eine Website nicht per https verschlüsselt ist. TLS kann aber auch für andere Zwecke genutzt werden, etwa zur Verschlüsselung des Zugriffs auf E-Mail-Server.

24 Brenden Kuerbis, »IPv6 Deployment around the World. A New Digital Divide?«, *CircleID*, 25.1.2018, <http://www.circleid.com/posts/20180125_ipv6_deployment_around_the_world_a_new_digital_divide/> (eingesehen am 23.8.2018).

25 Let's Encrypt, *Let's Encrypt Stats*, 2018, <https://letsencrypt.org/stats/> (eingesehen am 13.12.2018).

26 Monika Ermert, »TLS 1.2. Client-Zertifikate als Tracking-Falle«, *heise online*, 20.7.2018, <https://www.heise.de/security/meldung/TLS-1-2-Client-Zertifikate-als-Tracking-Falle-4117357.html> (eingesehen am 14.3.2019).

27 Siehe dazu Andy Greenberg, »Cyberspies Hijacked the Internet Domains of Entire Countries«, *Wired*, <https://www.wired.com/story/sea-turtle-dns-hijacking/> (eingesehen am 2.5.2019).

28 IANIX, *DNSSEC Downtime: List of Outages & Validation Failures*, 2018, <https://ianix.com/pub/dnssec-outages.html> (eingesehen am 13.12.2018).

DNS sind bisher unverschlüsselt; auch DNSSEC verschlüsselt DNS-Anfragen nicht. So lässt sich mit recht einfachen Mitteln erfassen, welche Domains ein Internet-Nutzer beim DNS anfragt. Viele Staaten machen sich dies zunutze, um bestimmte Domains gezielt zu blockieren.

Auch dieses Problem ist in der technischen Community seit längerem bekannt. So gibt es weitentwickelte Vorschläge dazu, DNSSEC mit Verschlüsselungsmechanismen zu kombinieren (vgl. Box 4, S. 15). Die Grundidee hierbei ist, DNS-Anfragen über verschlüsselte Verbindungen zu leiten (z.B. »DNS over TLS«, »DNS over HTTPS«). Demnach würden die Anfragen nur noch in verschlüsselter Form von zertifizierten Stellen bearbeitet. Eine solche Verbindung von Zertifizierung und Verschlüsselung würde »DNS poisoning« erheblich erschweren, die Privatsphäre der Internet-Nutzer stärker schützen und staatliche Zensur erschweren.[29]

Sicherheitsbehörden wollen bestehende Lücken im DNS vielfach für Zwecke der Strafverfolgung nutzen.

Die Problematik von Sicherheit und Datenschutz im DNS ist mithin bekannt, und Lösungsvorschläge liegen bereits vor. Es gelingt jedoch nicht, diese auf Ebene der globalen Infrastruktur flächendeckend umzusetzen. Erklären lässt sich das mit den im vorigen Abschnitt genannten Grenzen nichtstaatlicher Governance.

So ist *erstens* in historischer Perspektive festzustellen, dass das Sicherheitsproblem des »DNS poisoning« eine Folge der massiven Erweiterung des Internets ist. In dessen Gründungsphase gab es nur einen begrenzten Kreis an Institutionen, die DNS-Anfragen bearbeiteten. Diesen Institutionen konnte weitgehend ohne Rückgriff auf komplexe Zertifizierungsmechanismen vertraut werden (#E1). Eine solche Art der vertrauensbasierten Kommunikation ist heute jedoch nicht mehr möglich.[30]

Zweitens sind Maßnahmen zur Verbesserung von Sicherheit und Datenschutz im DNS politisch umstritten (#E2). Zwar haben im Prinzip alle Staaten ein Interesse an einer sicheren globalen Internet-Infrastruktur. Die Sicherheitsbehörden vieler Staaten wollen jedoch zugleich die bestehenden Sicherheitslücken im DNS für Zwecke der Strafverfolgung nutzen oder um den Zugang zu bestimmten Inhalten einzuschränken. Auch in demokratischen Rechtsstaaten werden DNS-basierte Filter verwendet, um etwa den Zugriff auf Kinderpornographie zu erschweren.

Drittens gilt sowohl für die Zertifizierung als auch für die Verschlüsselung von DNS-Anfragen, dass damit den Netzwerkbetreibern zusätzliche Kosten entstehen. Neben den direkten Kosten für die Einführung entsprechender technischer Vorkehrungen befürchten Netzwerkbetreiber indirekte Kosten, die dadurch anfallen, dass gängige Methoden des Datenverkehrsmanagements bei verschlüsselten DNS-Anfragen nicht mehr möglich sind. Da sich nur wenige Verbraucher und Unternehmen der Sicherheitsrisiken im DNS bewusst sind, gibt es für die Netzwerkbetreiber kaum eine Möglichkeit, diese Kosten an ihre Kunden weiterzugeben (#E3).

Einen Gegenpol hierzu bilden die Bemühungen von Mozilla, DNS-Anfragen auf Ebene des Browsers zu verschlüsseln. Dahinter steht das Bemühen, besonders datenschutzsensiblen Kunden mit dem Browser Firefox eine Alternative zum bisherigen System der DNS-Anfragen zu bieten. Im Rahmen der bisherigen Tests werden die verschlüsselten Anfragen von der US-Firma Cloudflare bearbeitet. Dass ein einzelner Anbieter alle DNS-Anfragen sammelt, hat viel Kritik ausgelöst. Als Reaktion ließ Mozilla verlauten, hier in Zukunft mit weiteren Firmen zusammenarbeiten zu wollen.[31] Auch Google lenkt in seinem Browser Chrome standardmäßig alle DNS-Anfragen zu seinem eigenen DNS-Dienst (per IPv4 erreichbar unter 8.8.8.8). Hier geht es allerdings nicht um Datenschutz; Google nutzt die Daten vielmehr, um Informationen zur Verbesserung der eigenen Dienste zu gewinnen, sowie möglicherweise auch für Werbezwecke.[32]

Die Aktivitäten von Mozilla und Google verweisen dabei auf ein strukturelles Problem der heutigen

29 Carsten Schmidt/Jürgen Strotmann, »DNS mit Privacy und Security vor dem Durchbruch«, in: *c't*, (2018) 14, S. 176–179.

30 Edward Lewis, *DNS. A Look Back at a Look Back*, Blog, 19.8.2018, <https://blog.apnic.net/2018/08/09/dns-a-look-back-at-a-look-back/> (eingesehen am 23.8.2018).

31 Monika Ermert, »DNS over HTTPS und die Privatsphäre der Nutzer: Mozilla will nicht nur einen Resolver«, *heise online*, 28.3.2019, <https://www.heise.de/newsticker/meldung/Mozilla-zu-DoH-Resolvern-Es-soll-nicht-nur-einen-geben-4354060.html> (eingesehen am 18.4.2019).

32 Vgl. <https://developers.google.com/speed/public-dns/privacy> und <https://policies.google.com/privacy?hl=en#whycollect>.

Internet Governance. Es gelingt nicht, die globale Internet-Infrastruktur weiterzuentwickeln. Dies lädt potente Akteure geradezu ein, eigene Lösungen zu entwickeln. Im Fall des DNS steht dabei nicht weniger auf dem Spiel als die Zukunft eines global einheitlichen Adress-Systems.

Sicherheit im Routing-System

Das Internet war ursprünglich darauf angelegt, dass alle verbundenen Geräte direkt miteinander in Austausch treten können. Die dezentrale Logik des Internets sieht daher bis heute vor, dass die wichtigsten Aufgaben bei der Übermittlung von Daten von den Endpunkten erfüllt werden, seien dies Endgeräte, Server oder auch Teilnetzwerke.

Eine Folge ist, dass es weder technisch noch rechtlich Vorgaben dazu gibt, entlang welcher Wegpunkte Daten (»packets«) durch das globale Internet geleitet (engl. »routing«) werden. Verschiedene Organisationen wie große Unternehmen, Regierungseinheiten und vor allem Internet Service Provider (ISP) betreiben Teilnetze des Internets, sogenannte Autonomous Systems. Als Betreiber dieser Teilnetze informieren sie andere Betreiber darüber, welche Verbindungen sie zu welchen Geschwindigkeiten anbieten können. Die Grundlage hierfür bildet das Border Gateway Protocol (BGP). Ein deutscher ISP würde also etwa signalisieren, dass er besonders schnelle Verbindungen zu Endpunkten in Deutschland und Frankreich anbieten kann. Indem alle Betreiber von Teilnetzen solche Informationen publik machen, entsteht eine Art Landkarte, auf der ersichtlich ist, welche Verbindungen zum jeweiligen Zeitpunkt am schnellsten sind.

Der entscheidende Punkt ist nun, dass dieser Austausch bisher ausschließlich auf Vertrauen basiert (#E1). Die Informationen der Betreiber von Teilnetzen werden nicht systematisch verifiziert. So ist es möglich, dass einzelne Betreiber falsche Angaben veröffentlichen und damit den globalen Datenverkehr verändern. Ursache kann schlicht ein Konfigurationsfehler sein. Doch gerade in letzter Zeit mehren sich Vorfälle, bei denen der Verdacht besteht, dass sie politisch motiviert sind. Die Logik dahinter ist einfach: Lenkt ein Staat den Datenverkehr über sein Territorium bzw. über Autonomous Systems unter seiner Kontrolle, erhält er damit die Möglichkeit, ihn auszuwerten oder zu filtern. Dieses Vorgehen wird als BGP Hijacking bezeichnet.[33] Die folgenden Beispiele illustrieren das Problem:

- Bereits im April 2010 hat das Unternehmen China Telecom für achtzehn Minuten etwa 15 Prozent des weltweiten Internet-Datenverkehrs über chinesische Server geleitet. Davon betroffen war unter anderem auch der Datenverkehr zu Domains der US-Regierung (.gov) und des US-Militärs (.mil).[34] Ein Ende 2018 veröffentlichter Bericht weist darauf hin, dass China Telecom seit 2016 in einer Reihe weiterer Fälle Datenverkehr aus den USA per BGP Hijacking über chinesische Server gelenkt hat.[35] Dazu wurden Niederlassungen des Unternehmens (»points of presence«) in den USA und Kanada genutzt.
- Wie den Enthüllungen des Whistleblowers Edward Snowden zu entnehmen ist, hat auch die NSA in der Vergangenheit die Methode des BGP Hijacking genutzt, um Datenverkehr gezielt umzuleiten. Detailliert wird in den Unterlagen der NSA am Beispiel des Jemen das entsprechende technische Vorgehen beschrieben, für das dort der euphemistische Begriff »traffic shaping« steht.[36]
- Am 30. Juli 2018 hat die Telecommunications Company of Iran (TCI) für den Zeitraum von etwa einer Stunde den Datenverkehr zu den Servern des im Iran sehr viel genutzten Messaging-Dienstes Telegram umgeleitet. Der unmittelbare Effekt bestand darin, dass Telegram zu diesem Zeitpunkt als Messaging-Dienst nicht mehr verwendbar war.[37]

33 Wobei es auch Fälle von BGP Hijacking gibt, die primär kommerziell motiviert zu sein scheinen. Vgl. Doug Madory, *BGP/DNS Hijacks Target Payment Systems*, 3.8.2018, <https://blogs.oracle.com/internetintelligence/bgp-dns-hijacks-target-payment-systems> (eingesehen am 7.8.2018).

34 Nate Anderson, »How China Swallowed 15% of 'Net Traffic for 18 Minutes«, in: *Ars Technica*, 17.11.2010, <https://arstechnica.com/security/news/2010/11/how-china-swallowed-15-of-net-traffic-for-18-minutes.ars> (eingesehen am 9.7.2018).

35 Chris Demchak/Yuval Shavitt, »China's Maxim — Leave No Access Point Unexploited. The Hidden Story of China Telecom's BGP Hijacking«, in: *Military Cyber Affairs*, 3 (2018) 1, S. 1–9.

36 Bruce Schneier, »More on the NSA's Use of Traffic Shaping«, *Blog*, 12.7.2017, <https://www.schneier.com/blog/archives/2017/07/more_on_the_nsa_2.html> (eingesehen am 14.11.2018).

37 GlobalVoices advox, *Iran's Telecommunications Company Illegally Rerouted Telegram App Traffic*, 2018, <https://advox.globalvoices.org/2018/08/06/irans-telecommunications-

Schon Anfang 2018 hatte die Regierung in Teheran mit verschiedenen Mitteln versucht, die Nutzung von Telegram innerhalb des Landes technisch zu unterbinden.

Auch wenn sich Fälle wie diese in letzter Zeit zu häufen scheinen, ist das Problem seit vielen Jahren bekannt.[38] Dabei mangelt es nicht an technischen Lösungsansätzen. So wie DNSSEC das DNS um Zertifizierungsmechanismen ergänzt, gibt es einen Vorschlag dazu, das BGP-Protokoll durch Zertifizierungsmechanismen abzusichern (BGPsec).[39] Eine Idee hierbei ist, dass die Betreiber von Autonomous Systems ihre Routing-Informationen mit einem Zertifikat absichern und selbst nur solche Informationen verwenden, die ebenfalls zertifiziert sind. Auf diese Weise wäre auch in einem dezentralen System jederzeit erkennbar, aus welcher Quelle die Routing-Informationen kommen und für wie zuverlässig die Quelle eingeschätzt wird. Darüber hinaus hat die Internet Society, eine im Bereich der Internet Governance einflussreiche NGO, einen Katalog praktischer Maßnahmen zur Absicherung des Routing-Systems erstellt — die Mutually Agreed Norms for Routing Security (MANRS). Sie werden bisher allerdings nur von wenigen Unternehmen unterstützt.[40]

Diese Vorschläge sind politisch nicht unumstritten (#E2). Wie beschrieben, haben die Nachrichtendienste einiger Staaten nachweislich ein Interesse daran, Sicherheitslücken nicht zu beheben. Erschwerend kommt hinzu, dass es für die Betreiber der Autonomous Systems mit erheblichen Kosten verbunden wäre, Änderungen am bisherigen System vorzunehmen (#E3). Zum einen müssten sie ihre eigene Infrastruktur aktualisieren; zum anderen fürchten sie die damit verbundene Transparenz. Wäre ein Betreiber verpflichtet, verifizierbar akkurate Daten über seine Verbindungskapazitäten öffentlich zu machen, würde ihm damit eine Möglichkeit genommen, den Datenverkehr durch sein Netzwerk zu steuern.[41]

Auch hier zeigen sich mithin die Grenzen nichthierarchischer Governance. Es ist bemerkenswert, dass sich sogar die Internet Society — ansonsten eher bekannt als Kritiker staatlichen Wirkens in der Internet Governance — beim Thema Routing-Sicherheit explizit an »Policymaker« richtet und diese zum Handeln auffordert: »Wenn sie mit gutem Beispiel vorangehen, die Kommunikation stärken und dazu beitragen, Anreize für mehr Sicherheit zu schaffen, können die politischen Entscheidungsträger dazu beitragen, das Ökosystem der Routing-Sicherheit zu verbessern.«[42]

Wie beim DNS zeigt sich auch hier die Gefahr einer Fragmentierung der globalen Internet-Infrastruktur. So heißt es in dem bereits erwähnten Bericht zu China Telecom, das BGP Hijacking durch die Firma habe wesentlich darauf basiert, dass sie seit Anfang der 2000er Jahre über mehrere »points of presence« in den USA verfügt. Eine solche Präsenz vor Ort erleichtert es, Datenverkehr in den USA bzw. Verkehr, der durch die USA geht, umzuleiten. Doch umgekehrt gibt es keine nichtchinesischen »points of presence« in China. Die Autoren des Berichts plädieren dafür, hier auf mehr Gegenseitigkeit zu dringen. Das Vorgehen Chinas zeigt aber auch die entgegengesetzte Möglichkeit auf, nämlich eine nationalstaatliche Abschottung. Gelingt es nicht, die Probleme der Routing-Sicherheit global zu lösen, steht zu befürchten, dass in Zukunft weitere Staaten diesen Weg wählen.

Sicherheit und Verfügbarkeit von Unterseekabeln

Die Rede vom Internet als »logischem Raum«, die Metapher von Datenwolken (»clouds«) und nicht zuletzt die enormen technischen Fortschritte im Bereich der kabellosen Datenübertragung mit WLAN, Bluetooth und Mobilfunknetzen — sie lassen bisweilen fast vergessen, dass das Internet auf eine ganz und

company-illegally-rerouted-telegram-app-traffic/> (eingesehen am 15.8.2018).

38 Vgl. Kim Zetter, »Revealed: The Internet's Biggest Security Hole«, *WIRED*, 26.8.2008, <https://www.wired.com/2008/08/revealed-the-in/> (eingesehen am 14.11.2018).

39 Vgl. M. Lepinski/K. Sriram, *RFC 8205: BGPsec Protocol Specification*, 2017, <https://tools.ietf.org/html/rfc8205>; Geoff Huston, »Securing the Routing System at NANOG 74«, *CircleID*, 16.10.2018, <http://www.circleid.com/posts/20181016_securing_the_routing_system_at_nanog_74/> (eingesehen am 17.10.2018).

40 *Mutually Agreed Norms for Routing Security*, <https://www.manrs.org/> (eingesehen am 19.12.2018).

41 Vgl. Russ White, »BGP Hijacks: Two More Papers Consider the Problem«, *CircleID*, 6.11.2018, <http://www.circleid.com/posts/20181106_bgp_hijacks_two_more_papers_consider_the_problem/> (eingesehen am 14.3.2019).

42 Internet Society, *Routing Security for Policymakers: An Internet Society White Paper*, Reston/VA 2018, <https://www.internetsociety.org/resources/doc/2018/routing-security-for-policymakers/> (eingesehen am 14.11.2018, Übersetzung durch den Autor).

gar handfeste physische Infrastruktur angewiesen ist. Dabei nehmen Unterseekabel eine hervorgehobene Stellung ein. Festlandgebundene Kabelverbindungen und Mobilfunknetze sind territorial begrenzt, ob auf einzelne Regionen, Staaten oder wie im Falle Europas den jeweiligen Kontinent. Die Verbindung zwischen diesen Gebieten erfolgt nur zu einem sehr geringen Teil über Satellitenverbindungen, ansonsten aber vor allem über Unterseekabel.

Bemerkenswert dabei ist, dass das weltweite Netzwerk an Unterseekabeln zu gut 95 Prozent in der Hand privater Unternehmen liegt.[43] Die Betreiber stellen die Übermittlungskapazitäten der Kabel in der Regel gegen Gebühren bereit. Zudem gibt es vertragliche Vereinbarungen, mit denen sich große Betreiber gegenseitig bestimmte Datenübertragungskapazitäten zur Verfügung stellen.[44] Erkennbar handelt es sich hierbei um ein privates — und eben nicht kollektives — Gut (siehe Box 1, S. 8). Auch gibt es in diesem Bereich bisher keine globale Institution, die den Anspruch erhebt, in spezifischer Weise kollektiv verbindliche Regeln zu setzen. Institutionen wie IETF und W3C beschäftigen sich ausschließlich mit Software-Protokollen, Institutionen wie IEEE und ITU allenfalls am Rande mit den technischen Herausforderungen von Kabelsystemen.[45]

»Chokepoints« als Sicherheitsbedrohung

Nur wenig Aufmerksamkeit finden so die spezifischen Bedrohungen, denen die Sicherheit dieses Teils der Internet-Infrastruktur ausgesetzt ist. Das bisherige Netz an Unterseekabeln weist eine hohe Konzentration von Routen und Landungsstellen auf; durch diese »chokepoints« entsteht eine erhebliche Verwundbarkeit.[46] Beispiele dafür sind der Suez-Kanal, durch den fast sämtliche Datenverbindungen zwischen Europa und Asien verlaufen, oder die Anlandestelle im brasilianischen Fortaleza, die von einem Großteil der Verbindungen zwischen Nord- und Südamerika genutzt wird (siehe Abb. 1, S. 20).

Diese Konzentration ergibt sich primär aus wirtschaftlichen Erwägungen (#E3). Hat ein Betreiber bereits Routen zu einem bestimmten Anlandepunkt entwickelt und entsprechende Verhandlungen mit dem betreffenden Staat geführt, ist es sehr viel kostengünstiger, für neue Kabel denselben Weg und dieselbe Anlandestelle zu verwenden, als neue Strecken zu erschließen.

Bedroht sind diese neuralgischen Punkte dabei aus verschiedenen Richtungen. Die meisten Schäden an Kabeln entstehen ganz undramatisch durch die hohen Belastungen, denen sie unter Wasser ausgesetzt sind, etwa aufgrund von Strömungen oder scharfkantigem Geröll am Meeresboden. Vor allem in küstennahen Gebieten werden die Kabel zudem immer wieder von der Fischerei gefährdet. Nach öffentlich verfügbaren Informationen sind dagegen gezielte militärische Maßnahmen zur Kappung von Unterseekabeln bisher nur eine potentielle Bedrohung. Dass russische U-Boote in der Nähe solcher Kabel gesichtet wurden, gab in der Vergangenheit Anlass zu entsprechenden Spekulationen; tatsächlich aber ist bislang kein Fall publik geworden, in dem ein Staat zu solchen Mitteln gegriffen hätte.[47]

Schon 2010 benannte der Bericht »Reliability of Global Undersea Cable Communications Infrastructure« (ROGUCCI-Report) die Gefahren. Zutreffend wurde hier darauf hingewiesen, dass ernsthafte Störungen auf Ebene der Unterseekabel zwar unwahrscheinlich seien, im Falle ihres Eintretens aber potentiell katastrophale Folgen hätten: »Die Auswirkungen eines solchen Versagens auf die internationale Sicherheit und die wirtschaftliche Stabilität könnten verheerend sein. Es ist unklar, ob die Zivilisation nach dem Scheitern einer Technologie, die so schnell ohne Backup-Plan eingeführt wurde, wieder zu ihrem vorherigen Zustand zurückfinden kann.«[48]

Ob die Zivilisation als solche durch Störungen der Unterseekabel bedroht wäre, mag zweifelhaft sein. Unschwer vorstellbar ist jedoch, welch enorme wirtschaftliche Schäden es mit sich bringen würde, wenn flächendeckend etwa die Verbindungen zwischen der

43 Douglas R. Burnett/Robert Beckman/Tara M. Davenport (Hg.), *Submarine Cables. The Handbook of Law and Policy*, Leiden 2013, S. 9.

44 Mick Green, »The Submarine Cable Industry. How Does It Work?«, in: Burnett u.a. (Hg.), *Submarine Cables* [wie Fn. 43], S. 42–60 (48).

45 Burnett u.a. (Hg.), *Submarine Cables* [wie Fn. 43], S. 10.

46 Nicole Starosielski, »Strangling the Internet«, in: *Limn*, (2018) 10, <https://limn.it/articles/strangling-the-internet/> (eingesehen am 14.3.2019).

47 Louis Matsakis, »What Would Really Happen If Russia Attacked Undersea Internet Cables«, *WIRED*, 1.5.2018, <https://www.wired.com/story/russia-undersea-internet-cables/> (eingesehen am 14.3.2019).

48 Karl Frederick Rauscher, *Reliability of Global Undersea Cable Communications Infrastructure*, 2010 (ROGUCCI report), S. 33, <http://www.ieee-rogucci.org/files/The%20ROGUCCI%20Report.pdf> (eingesehen am 14.3.2019, Übersetzung durch den Autor).

Abbildung 1

Größere, detailreichere Fassung dieser Karte unter http://bit.ly/SWP19S12Seekabel

Konzentration von Landungspunkten im weltweiten Netz der Unterseekabel

Die Darstellung zeigt Kabel, die aktuell in Betrieb sind oder voraussichtlich bis 2022 in Betrieb genommen werden.
Hervorgehoben sind Orte, in denen eine große Zahl von Kabeln anlandet.

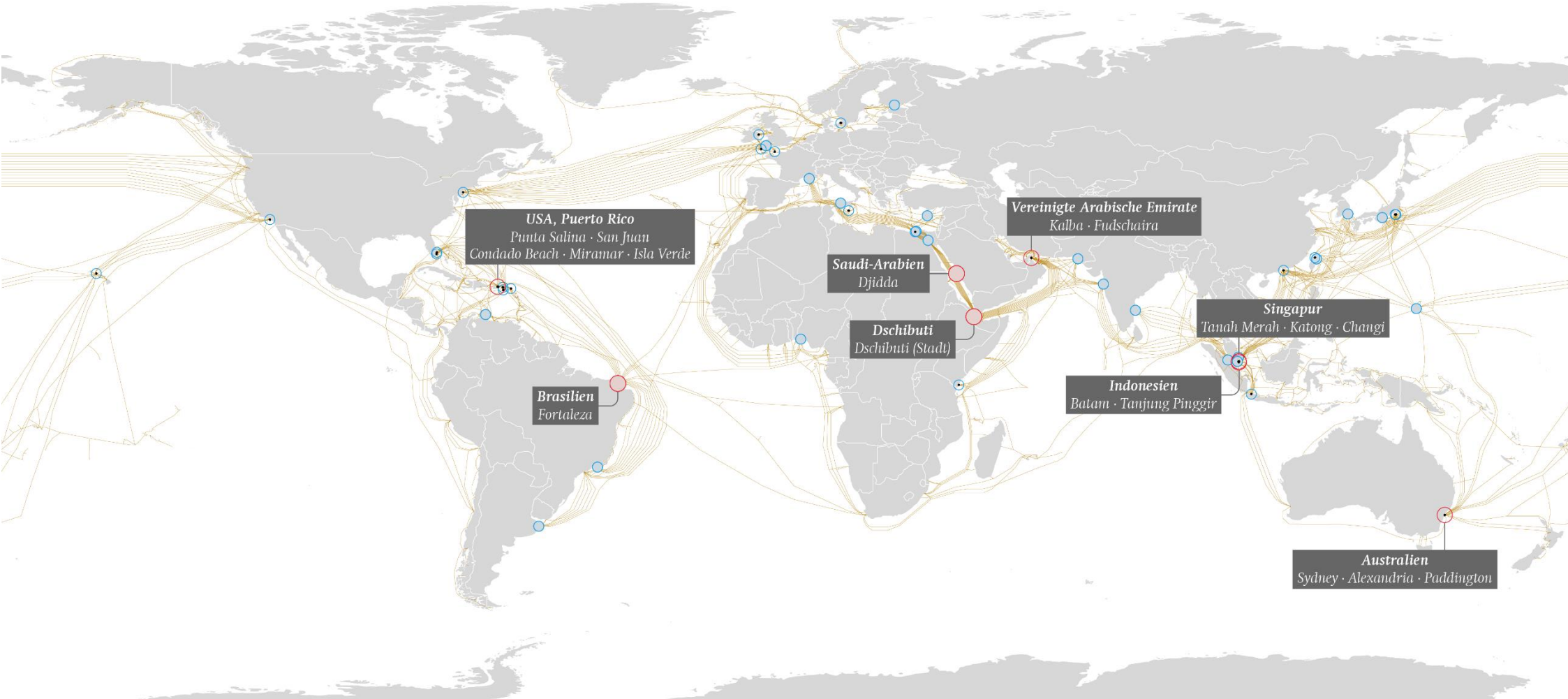
Kategorie 10
Orte, in denen an einem Anlandepunkt mehr als 10 Kabel ankommen *oder* mehrere Anlandepunkte im Abstand von jeweils nicht mehr als 10 km einen Cluster bilden, an dem mehr als 10 Kabel ankommen.

K10 Anlandepunkt **K10** Cluster

Kategorie 5
Orte, in denen an einem Anlandepunkt mehr als 5 Kabel ankommen *oder* mehrere Anlandepunkte im Abstand von jeweils nicht mehr als 10 km einen Cluster bilden, an dem mehr als 5 Kabel ankommen.

K5 Anlandepunkt **K5** Cluster

Quelle: TeleGeography, www.submarinecablemap.com



EU und den USA ausfallen würden. Das Finanzwesen oder auch der gesamte Bereich der internationalen Logistik sind heute darauf angewiesen, dass große Datenmengen fast in Echtzeit weltweit übermittelt werden. Schon temporäre Einschränkungen können hier erhebliche Folgewirkungen haben. Nimmt die Bedeutung dieser globalen Verbindungen in Zukunft weiter zu, so steigt damit auch die Verletzbarkeit. Zwar könnten auch großflächige Ausfälle von Unterseekabeln vorübergehend durch Umleitungen oder den Rückgriff auf Satellitenverbindungen ausgeglichen werden. Doch auch dann wären die unmittelbaren ökonomischen Konsequenzen beträchtlich.

Ein aktueller Fall zeigt die praktische Relevanz dieser Überlegungen. Die Insel Tonga im Südpazifik ist nur über ein einziges Unterseekabel mit dem Internet verbunden. Aus noch ungeklärten Gründen wurde dieses Kabel im Januar 2019 massiv beschädigt. Die Insel und ihre Bevölkerung waren für gut zwei Wochen nur noch über eine Satellitenverbindung an das Internet angeschlossen, deren begrenztes Datenvolumen dafür genutzt wurde, dass etwa Banken weiterhin Geld auszahlen konnten.[49]

Die Marktanreize für Kabelbetreiber stehen in Spannung zu den wirtschaftspolitischen Bedürfnissen von Entwicklungsländern.

Wie beschrieben, ist die Wahrscheinlichkeit gering, dass große Teile des Netzwerks an Unterseekabeln ausfallen. Dies erklärt, warum die meisten Staaten hier bisher nur wenig Handlungsbedarf sehen. Wenn überhaupt, nehmen sie ihr unmittelbares Umfeld in den Blick. So haben die USA in den letzten Jahren die Anforderungen für die Sicherung von Anlandestellen erhöht. Australien hat 2018 aktiv verhindert, dass das chinesische Unternehmen Huawei den Auftrag zur Verlegung eines Unterseekabels erhielt, das die Salomon-Inseln mit dem Kontinent verbinden soll.[50] Die globale Dimension des Problems wird bisher jedoch politisch nicht in den Blick genommen.

49 BBC, »Tonga Hit by Near-Total Internet Blackout«, *BBC (online)*, 23.1.2019 <https://www.bbc.com/news/world-asia-46968752> (eingesehen am 14.3.2019).

50 »Australia Keeps China Out of Internet Cabling for Pacific Neighbor«, *Reuters*, 13.6.2018, <https://www.reuters.com/article/us-australia-solomonislands-internet/australia-keeps-china-out-of-internet-cabling-for-pacific-neighbor-idUSKBN1J90JY> (eingesehen am 20.6.2018).

Dabei schwelt hier ein Konflikt, der im Kern ähnlich strukturiert ist wie die Auseinandersetzungen um die logische Infrastruktur des Internets. Auch wenn viele Regierungen die Bedeutung des Themas noch nicht erkannt haben, ist es im Interesse aller Staaten, dass das Netzwerk der Unterseekabel vor flächendeckenden Ausfällen geschützt ist. Notwendig dafür wäre vor allem, redundante Strukturen bei den gewählten Kabelverbindungen und Anlandestellen zu schaffen, ebenso Diversität bei der genutzten Kabel- und Netzwerktechnologie. Solche Maßnahmen sind jedoch mit erheblichen Kosten verbunden. Es überrascht nicht, dass die privaten Betreiber der Unterseekabel diesen finanziellen Aufwand zu vermeiden suchen (#E3).

Die entwicklungspolitische Bedeutung

Der Konflikt zwischen Staaten und Unternehmen zeigt sich jenseits von Sicherheitsfragen schon heute deutlich bei der Frage, welchen Zugang die Entwicklungsländer zum Netz der Unterseekabel erhalten. Dieser Faktor ist von großer Bedeutung, wenn es darum geht, das wirtschaftliche Potential der Digitalisierung nutzen zu können. Im Netzwerk der Unterseekabel spiegelt sich heute vor allem der bisherige Stand der globalen Wirtschaftsbeziehungen, orientieren sich die Kabelbetreiber doch primär an ökonomischen Aspekten. Eine Verbindung zwischen den USA und Europa erscheint schlicht lukrativer als eine zwischen den USA und Afrika.

Weil Kabelverbindungen noch immer aufwändige Projekte darstellen und entsprechend langfristig angelegt sind, entstehen auf diese Weise aber zugleich dauerhafte Pfadabhängigkeiten bis hin zu »self-fulfilling prophecies«. Denn die Frage, zu welchen Kosten und mit welcher Verfügbarkeit ein Staat an die globale Internet-Infrastruktur angeschlossen ist, kann sich durchaus auf dessen wirtschaftliche Entwicklung auswirken. Die unmittelbaren Marktanreize für die Betreiber von Unterseekabeln (#E3) stehen hier in Spannung zu den wirtschaftspolitischen Bedürfnissen von Entwicklungsländern.

Autoritative Regelsetzung als Ausweg?

Die globale Internet Governance kennt bisher kaum Autorität. Den vorherrschenden Modus sozialer Koordination bildet hier vielmehr die nichthierarchische Bereitstellung kollektiver Güter. Analysiert man die Grenzen dieses institutionellen Arrangements, stellt sich indes die Frage, ob nicht doch ein Mehr an globaler Autorität nötig ist, um die genannten Konflikte zu lösen.

Praktische Relevanz, ja Brisanz gewinnt diese Fragestellung in den Auseinandersetzungen um zwei zentrale Institutionen der Internet Governance, nämlich die Internet Corporation for Assigned Names and Numbers sowie die International Telecommunication Union.

ICANN: Politisierung

In der globalen Internet Governance nimmt ICANN eine zentrale Stellung ein, weil der Organisation die autoritative Verwaltung des DNS obliegt (siehe S. 12). Diese Funktion würde es ICANN im Prinzip ermöglichen, einige der Konflikte um die Weiterentwicklung der Internet-Infrastruktur durch verbindliche Vorgaben zu beenden. So könnte ICANN etwa die Vergabe von Domains an die Bedingung knüpfen, dass diese nur in Verbindung mit Sicherheitsmaßnahmen wie DNSSEC genutzt werden. Schon heute verlangt die Organisation von Registries neuer gTLD, dass sie in ihrer Infrastruktur DNSSEC einsetzen. Dieses Erfordernis betrifft aber nur die Registries selbst und nicht die Registrars, die Betreiber einzelner Domains oder lokale ISPs.[51]

Es erscheint allerdings höchst unwahrscheinlich, dass die Autorität von ICANN ausgeweitet wird, auch wenn dies grundsätzlich möglich wäre. Im Gegenteil zeichnet sich eine immer stärkere Politisierung der Organisation ab — selbst in bisher weitgehend unstrittigen Bereichen.

ICANN und die Rolle der USA

Den Hintergrund bildet das besondere Verhältnis zwischen ICANN und der amerikanischen Regierung, wie es bis heute besteht. Für die USA war die globale Ausweitung des Internets immer auch mit dem politischen Projekt verbunden, die eigenen liberalen Ordnungsvorstellungen weltweit zur Geltung zu bringen.[52] Dass die amerikanische Regierung das DNS anfangs direkt kontrollierte, spricht dafür, dass sie sich der Bedeutung der Internet-Infrastruktur schon immer bewusst war.

Ursprünglich lag die Verwaltung der DNS Root Zone bei der Internet Assigned Numbers Authority (IANA), die wiederum dem amerikanischen Wirtschaftsministerium unterstand. In einem mehrjährigen Prozess wurde die IANA jedoch ICANN zugeordnet und schließlich 2016 der Kontrolle des Vorstands von ICANN unterstellt. Die »IANA transition« gilt als Zugeständnis der USA. Die Administration in Washington gab dabei allerdings vor, dass ICANN auch künftig nicht der Kontrolle durch Staaten oder internationale Organisationen unterstellt werden solle.[53] Der Widerspruch, dass die USA als Staat ICANN die Vorgabe machen, sich keiner staatlichen Kontrolle zu unterwerfen, ist dabei augenfällig. Zudem wahrten die USA dadurch eine besondere Form von Einfluss für sich, dass ICANN als privates Unter-

51 Siehe hierzu das »Base Registry Agreement« für neue gTLD, Specification 6, Absatz 1.6, S. 78, <https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf> (eingesehen am 24.4.2019).

52 Jack Goldsmith, *The Failure of Internet Freedom*, New York 2018, <https://knightcolumbia.org/content/failure-internet-freedom> (eingesehen am 14.3.2019).

53 Milton Mueller, »The IANA Transition and the Role of Governments in Internet Governance«, in: *IP Justice*, (2015), S. 1—18.

nehmen nach kalifornischem Recht der Jurisdiktion der Vereinigten Staaten untersteht.

Bis jetzt haben die USA von diesem Einfluss nicht offen Gebrauch gemacht. Welche Bedeutung das institutionelle Arrangement hat, zeigte sich jedoch zuletzt im Sommer 2018, als die National Telecommunications and Information Administration (NTIA) öffentlich die Frage aufbrachte, ob die »IANA transition« im Sinne der nationalen Interessen der USA rückgängig zu machen sei.[54] Derzeit sieht es zwar nicht danach aus, dass es tatsächlich zu einem solchen Schritt kommen könnte; sehr deutlich wurden hier aber noch einmal die tatsächlichen Machtverhältnisse in Bezug auf ICANN.

Für Staaten wie Brasilien, Kuba, Russland oder Saudi-Arabien ist diese Sonderstellung der USA schon für sich genommen ein Grund, immer wieder die Rolle von ICANN in der heutigen Internet Governance zu kritisieren. China ist weniger für offene Kritik an ICANN bekannt. In der »International Strategy of Cooperation on Cyberspace«, die Peking 2017 veröffentlicht hat, wird jedoch sehr deutlich eine gleichberechtigte Beteiligung aller Staaten in der Internet Governance gefordert. Dabei wird unter anderem explizit auf die Verwaltung der DNS Root Zone verwiesen.[55]

WHOIS und der europäische Datenschutz

Zwischen ICANN und der EU schwelt bereits seit einigen Jahren ein Konflikt um die Zukunft des WHOIS-Systems. Vereinfacht gesprochen ist WHOIS ein Protokoll, das es erlaubt, Anfragen zu den Besitzern bzw. Betreibern von Domains zu stellen. Entsprechend der dezentralen Struktur des DNS ist auch WHOIS im Kern dezentral organisiert. Die für eine Domain zuständige Registry (siehe Box 5) betreibt in der Regel auch das jeweilige WHOIS-System, zum Beispiel das Deutsche Network Information Center (DENIC) für die .de-Domain. Die Registries für ccTLD sind in der Regel in dem Land angesiedelt, dessen Domain sie verwalten, und unterstehen somit den entsprechenden gesetzlichen Vorgaben. Umstritten ist jedoch, welche Vorgaben für gTLD gelten sollen.

Box 5: gTLD und ccTLD, Registries und Registrars

Das DNS verknüpft Domain-Namen mit IP-Adressen (siehe Box 2, S. 12). Für ein einheitliches DNS ist dabei entscheidend, dass jeder Domain-Name nur einmal vergeben wird. ICANN delegiert die Vergabe von TLDs an Registries (wie DENIC für .de oder Verisign für .com). Die Registries jedoch vergeben nicht einzelne Domains (wie example.com), sondern delegieren diese Aufgabe wiederum an Registrars.

Heute gibt es im Wesentlichen zwei Typen von Domain-Namen. Für alle offiziell anerkannten Staaten gibt es country-code Top Level Domains (ccTLDs) wie .de oder .fr. Diese werden in der Regel von einer Registry im jeweiligen Land verwaltet. Zudem existiert eine Reihe von generic Top Level Domains (gTLD), wie zum Beispiel .com oder .org. Sie sind nicht geographisch zugeordnet; entsprechend sind auch die jeweiligen Registries global verteilt.

Die EU fordert, dass auch die Daten der Inhaber von gTLD gemäß der europäischen Datenschutz-Grundverordnung (DSGVO) behandelt werden. Deutlich bringt sie damit ihren Anspruch zum Ausdruck, für das »europäische« Internet auch ICANN Vorgaben machen zu können. Die Organisation hingegen ist erkennbar nicht gewillt, sich den Bestimmungen der DSGVO zu fügen. Obwohl seit langem absehbar war, dass das WHOIS-Regime für gTLD unvereinbar mit der DSGVO sein würde, hat ICANN erst kurz vor Ende der Übergangsphase zur Einführung der DSGVO im Mai 2018 reagiert. Für zunächst ein Jahr wurde eine Übergangslösung eingeführt; diese soll möglichst bald durch eine DSGVO-konforme Dauerlösung ersetzt werden.[56]

Wie eine solche Lösung aussehen soll, ist jedoch sowohl innerhalb der Gremien von ICANN als auch im Austausch mit der EU bisher umstritten. Die USA, aber auch viele weitere im GAC vertretene Staaten pochen darauf, dass insbesondere Strafverfolgungsbehörden einen Zugang zu personenbezogenen Daten

54 Kieren McCarthy, »US Govt Mulls Snatching Back Full Control of the Internet's Domain Name and IP Address Admin«, *The Register*, 5.6.2018, <https://www.theregister.co.uk/2018/06/05/us_government_icann_iana/> (eingesehen am 14.3.2019).

55 Ministry of Foreign Affairs of the People's Republic of China, »International Strategy of Cooperation on Cyberspace (2017)«, 1.3.2017, <https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml> (eingesehen am 14.3.2019).

56 Matt Serlin, »The EPDP on Generic Top-Level Domain Registration Data: Phase 1 Down, Phase 2 To Go«, *CircleID*, 28.3.2019, <http://www.circleid.com/posts/20190328_epdp_on_gtld_registration_data_phase_1_down_phase_2_to_go/> (eingesehen am 18.4.2019).

erhalten.[57] Ungeklärt ist jedoch, nach welchen Kriterien und mittels welcher Verfahren den Strafverfolgern dieser Zugriff gewährt werden soll — und ob dies in einer Weise geschehen kann, die den Anforderungen der DSGVO entspricht.[58]

Der Einfluss der Staaten auf die Domain-Vergabe

ICANN verfügt über eine Reihe von Gremien und Verfahren, die im Sinne der Multistakeholder-Governance eine breite Beteiligung der verschiedenen Interessengruppen ermöglichen sollen. Auch die Staaten sind dadurch eingebunden. Sie können eine Mitgliedschaft im Governmental Advisory Committee (GAC) der Organisation erhalten und so beratend an den Entscheidungen von ICANN teilnehmen.[59]

Mittlerweile ist es in der Praxis weithin akzeptiert, dass die Staaten mit Bezug auf »ihre« Domains, also die ccTLD, bei allen Fragen von politischer Bedeutung zu beteiligen sind. Stark umstritten ist jedoch, welchen Einfluss sie bei der Vergabe von gTLD haben sollen. Dies manifestiert sich aktuell in drei Konflikten:[60]

- *2-Character Country/Territory Codes at the Second Level:* Gemeint sind damit nicht ccTLD wie .de. Vielmehr geht es um die zweite Ebene von gTLD wie .edu oder .xxx. Ein »2-character country code« würde dementsprechend zum Beispiel die Form .de.edu annehmen. Vermittelt durch das GAC, pochen nun eine Reihe von Staaten darauf, an der Vergabe dieser Domains beteiligt zu werden bzw. gegebenenfalls kostengünstig die Möglichkeit zu erhalten, die Domains selbst zu verwalten.
- *Neue gTLD:* Immer wieder gibt es strittige Fälle, in denen Staaten beanspruchen, Einfluss auf Entscheidungen über spezifische gTLD zu nehmen. Viel Aufmerksamkeit erfährt derzeit etwa der Streit um die Vergabe der gTLD .amazon. Der US-Konzern Amazon hat schon vor längerer Zeit diese gTLD beantragt, stößt damit aber auf nachhaltigen Widerstand aus den Anrainerstaaten des Amazonas. Alle Vermittlungsversuche des ICANN-Vorstands in der Frage sind bisher gescheitert.[61]
- *Intergovernmental Organizations Identifiers:* Schon seit einigen Jahren drängt das GAC darauf, bei der Domain-Vergabe auch jenseits der Domain .int die Interessen von Internationalen Organisationen wie dem Internationalen Komitee vom Roten Kreuz (IKRK) in besonderer Weise zu berücksichtigen.

Von außen betrachtet scheint es zunächst kaum nachvollziehbar, wie sich an solchen Details jahrelange politische Auseinandersetzungen entzünden können. Tatsächlich jedoch steht für einige Staaten hier Grundsätzliches auf dem Spiel. Sie wollen innerhalb der Strukturen von ICANN rechtliche Mechanismen etablieren, die ihren Autoritätsanspruch auf »ihren« Teil des Internets anerkennen und international absichern.

ITU: Blockade

Die Ursprünge der International Telecommunication Union gehen zurück auf die Gründung des Internationalen Telegraphenvereins 1865. Im Jahr 1932 nahm die Organisation ihren heutigen Namen an, seit 1949 fungiert sie auf Basis eines Übereinkommens mit den Vereinten Nationen als eine von deren Sonderorganisationen. Die ITU besteht im Wesentlichen aus drei organisatorischen Einheiten: ITU-R für den Bereich der Radiokommunikation, ITU-T für den Bereich der Standardsetzung in der Telekommunikation und ITU-D für den Bereich der technischen Unterstützung und Entwicklung (»Development«) in der Telekommunikation.

Schon in diesen Strukturen der ITU zeigt sich, dass für sie das Internet bisher keine zentrale Bedeutung hat. In der Tat besteht seit den späten 1990er Jahren ein anhaltender Streit um die Frage, ob und gegebe-

57 Vgl. etwa »Remarks of Assistant Secretary Redl at IGF-USA 2018«, 27.7.2018, <https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-igf-usa-2018> (eingesehen am 21.8.2018).

58 Farzaneh Badii/Milton Mueller, *Stacking the Deck? The ePDP on the Whois Temp Spec*, 2018, <https://www.internetgovernance.org/2018/07/03/stacking-the-deck-the-epdp-on-the-whois-temp-spec/> (eingesehen am 4.7.2018).

59 Siehe *Bylaws for Internet Corporation for Assigned Names and Numbers (ICANN), as Amended 18 June 2018*, Section 3.6, (a), (III), <https://www.icann.org/resources/pages/governance/bylaws-en> (eingesehen am 14.3.2019).

60 Vgl. ICANN GAC, *GAC Communiqué ICANN 63 – Barcelona, Spain*, 25.10.2018, <https://gac.icann.org/advice/communiques/icann63%20gac%20communique%CC%81.pdf> (eingesehen am 12.11.2018).

61 Monika Ermert, »ICANN setzt Galgenfrist für .amazon«, *heise online*, 14.3.2019, <https://www.heise.de/newsticker/meldung/ICANN-setzt-Galgenfrist-fuer-amazon-4335195.html> (eingesehen am 14.3.2019).

nenfalls in welcher Hinsicht die ITU für Fragen der globalen Internet Governance zuständig sein sollte. 1997 war die Organisation einmal kurz davor, gemeinsam mit weiteren Institutionen wie der Internet Society sieben neue TLDs (vgl. Box 5, S. 23) auszugeben und die direkte Kontrolle über die Domain .int zu übernehmen. Dies allerdings stieß auf erheblichen Widerstand der USA, die nicht zuletzt aus Sorge vor einer solchen Stärkung der ITU 1998 die Gründung von ICANN betrieben.[62]

Seither ist die Konfliktlage stabil. Die westlichen Staaten, angeführt von den USA und Großbritannien, sind strikt dagegen, die Aktivitäten der ITU auf den Bereich der Internet Governance auszuweiten. Staaten wie Russland, China, Brasilien und Saudi-Arabien hingegen versuchen, die Organisation zu einer zentralen Instanz der globalen Internet Governance zu machen.

Die Befürworter einer stärkeren Rolle der ITU berufen sich vor allem auf deren Legitimität. Anders als ICANN könne sie sich darauf stützen, dass ihre Entscheidungen das Ergebnis inklusiver Verhandlungen aller Staaten darstellten.[63] Die westlichen Staaten hingegen betonen, dass das Mandat der ITU auf technische Fragen beschränkt sei und damit eben ungeeignet für genuin politische Entscheidungen. Kaum verhohlen kommt zudem die Sorge zum Ausdruck, eine Stärkung der ITU würde autoritären Staaten wie China, Russland oder Saudi-Arabien zu viel Einfluss auf die künftige Entwicklung des Internets geben.[64]

Der nun schon lange währende Streit um die Rolle der ITU in der Internet Governance ist geprägt durch drei institutionelle Eigenheiten der Organisation.

Box 6: Die Plenipotentiary Conference 2018 in Dubai

Die Verhandlungen um Resolution 102, die im Rahmen der Plenipotentiary Conference 2018 in Dubai geführt wurden, veranschaulichen beispielhaft die festgefahrenen Konfliktlinien in der ITU. Der Titel dieser Resolution, die erstmals 1998 in Minneapolis verabschiedet wurde, ist sperrig, aber doch aussagekräftig: »ITU's role with regard to international public policy issues pertaining to the Internet and the management of Internet resources, including domain names and addresses«. Die Resolution berührt im Kern die Frage, welche Rolle der ITU mit Blick auf das Domain Name System zukommen soll.

Wie zu erwarten, sind die Befürworter des bisherigen Modells der Internet Governance darum bemüht, hier die Rolle von Institutionen wie ICANN zu bekräftigen. Zu diesem Zweck wird die ITU seit 2010 im ersten Absatz des Beschlussteils der Resolution darauf festgelegt, mit relevanten Organisationen der Internet Governance zusammenzuarbeiten. Dabei werden in einer dazugehörigen Fußnote explizit ICANN, die Regional Internet Registries (RIRs), IETF, die Internet Society und W3C genannt.[65]

Seit der Plenipotentiary Conference in Busan 2014 enthält die Resolution aber auch eine Passage, die den Anspruch der Staaten auf »ihre« Domains, also die ccTLD, klar bekräftigt.[66] Im Vorfeld der Konferenz von 2018 legte die Gruppe der arabischen Staaten einen Änderungsantrag vor, der darauf zielte, diesen Anspruch auf die gTLD auszuweiten. In der Präambel der Resolution sollte zugleich kritisiert werden, dass staatliche Interessen bei den Entscheidungen von ICANN zu wenig berücksichtigt würden.[67] Die Gruppe der europäischen Staaten hingegen brachte den Vorschlag ein, die ITU Council Working Group Internet (CWG Internet) im Sinne des Multistakeholder-Ansatzes auch über selektive Konsultationen hinaus für nichtstaatliche Akteure zu öffnen.[68] Letztlich erreichte keiner der beiden Vorschläge in Dubai den notwendigen Konsens.

62 Jill Hills, *Telecommunications and Empire,* Urbana/IL 2007, S. 140ff.

63 Daniel Kennedy, *Deciphering Russia. Russia's Perspectives on Internet Policy and Governance,* November 2013, <https://www.gp-digital.org/wp-content/uploads/pubs/FINAL%20-%20Deciphering%20Russia.pdf> (eingesehen am 14.3.2019); Dave Burstein, »A Closer Look at Why Russia Wants an Independent Internet«, *CircleID*, 15.12.2017, <http://www.circleid.com/posts/20171215_closer_look_at_why_russia_wants_an_independent_internet/> (eingesehen am 19.12.2018).

64 Vgl. beispielhaft Michael O'Rielly, »Reining in UN's Little Known International Telecommunication Union«, *TheHill*, 8.8.2018, <http://thehill.com/opinion/technology/400990-reigning-in-uns-little-known-international-telecommunication-union> (eingesehen am 13.3.2019).

65 International Telecommunication Union (ITU), *Final Acts of the Plenipotentiary Conference, Guadalajara 2010*, 2010, Resolution 102, Resolves 1.

66 ITU, *Final Acts of the Plenipotentiary Conference, Dubai 2018*, 2018, Resolution 102, Resolves 4.

67 ITU, *Coordinated Proposals Received from ITU Member States for the Work of the Conference, 27 October 2018*, 2018, Resolution 102, ARB/72A1/8, noting with concern b).

68 Ebd., Resolution 102, EUR/48A1/8, Resolves 5.

Erstens finden die Treffen des obersten Beschlussgremiums der ITU, der »Plenipotentiary Conference«, nur alle vier Jahre statt. Jedem dieser Treffen kommt damit besondere Bedeutung zu. Zweitens gilt bei der ITU die Regel, dass alle Entscheidungen im Konsens zu treffen sind. Dies gibt den Verfechtern des Status quo, also den westlichen Staaten, einen erkennbaren verhandlungstaktischen Vorteil. Im Wesentlichen können sie sich darauf beschränken, jegliche Ausweitung der ITU-Kompetenzen auf dem Feld der Internet Governance zu verhindern. Drittens sind die Verhandlungen in der ITU dadurch bestimmt, dass die Staaten einerseits im eigenen Namen verhandeln, andererseits aber auch teilweise als Mitglieder regionaler Gruppen auftreten. Letztere überschreiten bisweilen die Grenzen der üblichen politischen Lager, da sie ihren Ausgangspunkt in der technischen Koordinierung regionaler Telekommunikationsnetze haben. So ist Russland hier etwa Teil der Gruppe der europäischen Staaten, die in der European Conference of Postal and Telecommunications Administrations (CEPT) organisiert sind.

Zwei, drei, viele Internets?

Wir haben uns an den Gedanken gewöhnt, dass es *ein* Internet gibt. Seit einiger Zeit jedoch mehren sich die Warnungen, das Internet könnte sich aufspalten. Wahlweise ist dabei von »Fragmentierung« oder »Balkanisierung« die Rede; auch der Begriff des »Splinternet« wird in diesem Kontext gern verwendet.[69] Weit verbreitet ist die Sorge, das Internet werde zwischen den USA und China aufgeteilt. So bemerkte etwa Eric Schmidt, einer der Gründer von Google: »Ich denke, das wahrscheinlichste Szenario heute ist nicht eine Zersplitterung, sondern eine Zweiteilung in ein von China geführtes Internet und ein von Amerika geführtes, nichtchinesisches Internet.«[70]

Eine echte Fragmentierung des Internets wäre dann zu befürchten, wenn es zur Spaltung auf Ebene der Infrastruktur käme.

Mit ähnlicher Stoßrichtung hat der französische Präsident Macron bei der Eröffnung des Internet Governance Forum 2018 zwischen einer kalifornischen und einer chinesischen Variante des Internets unterschieden.[71] Für Macron ergibt sich daraus die Notwendigkeit eines eigenständigen europäischen Weges. Umgekehrt wird aus amerikanischer Sicht gerade der regulatorische Anspruch der europäischen DSGVO bisweilen als Zeichen für eine weitere Spaltung des Internets gedeutet.[72]

So vielfältig die Rhetorik ist, so mannigfaltig sind auch die empirischen Phänomene, um die es in dieser Debatte geht. Die Analyse in den vorherigen Abschnitten legt dabei zwei Differenzierungen nahe. Zunächst gilt es, genauer zu betrachten, auf welcher Ebene eine Fragmentierung des Internets beobachtet oder befürchtet wird. Auf Ebene der Internet-Dienste ist es schon länger praktische Realität, dass eine regulatorische Differenzierung entlang der Grenzen staatlicher Jurisdiktion besteht. Immer mehr Staaten versuchen, »ihren« Teil des Internets zu regulieren. Hier zeigt sich die Beharrungskraft des Ordnungsprinzips territorialer Staatlichkeit.

Es ist jedoch irreführend, diese Bruchlinien auf Ebene der Internet-Dienste als Fragmentierung »des« Internets zu beschreiben. Denn zumindest bislang erfolgt die staatliche Regulierung von Internet-Diensten auf Basis einer global geteilten Internet-Infrastruktur aus gemeinsamen Standards und Protokollen. Eine echte Fragmentierung des Internets wäre erst dann zu befürchten, wenn es zu einer Spaltung auf Ebene der Infrastruktur käme. Besondere Bedeutung kommt dabei dem Domain Name System zu, also dem Adress-System des Internets (siehe Box 2, S. 12), aber auch grundlegenden Protokollen zur Datenübertragung.[73]

Mit Blick auf die logische Infrastruktur gilt es sodann weiter zu unterscheiden, von welchen Akteuren die Gefahr einer Fragmentierung ausgeht. Zum einen sind das die Staaten. Die Frage hier ist, ob sie sich dauerhaft damit »begnügen« werden, die Ebene der Internet-Dienste zu regulieren, oder ob sie ihren Regulierungsanspruch auf die Ebene der Internet-Infrastruktur ausweiten. Insbesondere aus China, aber auch aus Russland kommen immer wieder Hinweise darauf, dass Alternativen zu dem heute von ICANN verwalteten DNS denkbar wären. Die technische Organisation des Internets in China bietet hierfür die Blaupause. Dieses stellt schon heute ein weitgehend geschlossenes *Intra*net dar, das nur über staatlich kontrollierte Zugänge mit dem Rest

69 Vgl. Milton Mueller, *Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace*, Cambridge 2017.

70 Lora Kolodny, »Former Google CEO Predicts the Internet will Split in Two — and One Part Will Be Led by China«, *CNBC*, 20.9.2018, <https://www.cnbc.com/2018/09/20/eric-schmidt-ex-google-ceo-predicts-internet-split-china.html> (eingesehen am 14.3.2019, Übersetzung durch den Autor).

71 Internet Governance Forum, »IGF 2018 Speech by French President Emmanuel Macron« [wie Fn. 18].

72 The Editorial Board, »There May Soon Be Three Internets. America's Won't Necessarily Be the Best«, in: *The New York Times*, 15.10.2018.

73 Vgl. hierzu auch Mirko Hohmann/Thorsten Benner, *Getting »Free and Open« Right. How European Internet Foreign Policy Can Compete in a Fragmented World*, Berlin, Juni 2018, S. 36.

Box 7:
Tor als alternatives Adress-System

Das Tor Onion Service Protocol ist ein Beispiel für ein alternatives Adress-System. Die Entwicklung dieses Protokolls wurde ursprünglich vom Office of Naval Research (ONR) und der Defense Advanced Research Projects Agency (DARPA) gefördert, mithin von zwei Forschungseinrichtungen des US-Militärs. Heute wird das Protokoll aber vor allem deshalb kritisch betrachtet, weil es ein Baustein des sogenannten »Dark Net« ist.[74] Tor dient dazu, über mehrfach gestufte Verschlüsselungsverfahren einen weitgehend anonymen Datenaustausch zu ermöglichen. Dies erlaubt zum einen das anonyme Aufrufen von Websites im »normalen« Internet auf Basis des von ICANN verwalteten DNS. Zum anderen gibt es für die Tor-eigenen »hidden services« aber auch noch ein gesondertes Adressformat, das auf die Domain .onion endet. Diese Domain wird zwar von der IETF als Special-use Domain anerkannt, ist aber nicht über das übliche DNS-System abrufbar.[75] Um Adressen innerhalb der Domain aufrufen zu können, ist ein spezieller Browser erforderlich, der die entsprechenden Adressanfragen innerhalb des Tor-eigenen Netzwerks weiterleiten kann.

des Internets verbunden ist. Denkbar wäre nun, dass China weitere Staaten in dieses System aufnimmt, etwa im Rahmen der noch vagen Ideen einer »digitalen Seidenstraße«.[76] Zudem hat Russland angekündigt, für einen Testzeitraum das russische Internet vom globalen Internet abkoppeln zu wollen.[77] Das im April 2019 von der Duma verabschiedete »Gesetz über das souveräne Internet« bietet dafür die Grundlage; es enthält wiederum Hinweise auf das Ziel, ein eigenes DNS aufzubauen.[78] Nach eigenem Bekunden will Moskau damit sicherstellen, im Falle eines Konflikts nicht von den USA abhängig zu sein. Erkennbar soll aber auch die Basis dafür geschaffen werden, schon auf Ebene der Infrastruktur Kontrolle über das »eigene« Internet zu erlangen — ganz ähnlich, wie dies im Falle Chinas geschieht.

Eine Bedrohung für die gemeinsame globale Internet-Infrastruktur kommt aber auch aus gänzlich anderer Richtung, nämlich von privaten Unternehmen, vor allem solchen in den USA. Wie oben ausgeführt, sind insbesondere Google und Mozilla, mithin die Firmen hinter zweien der wichtigsten Internet-Browser, aktuell darum bemüht, quasi im Alleingang für ihre Nutzer die Sicherheitslücken des heutigen DNS zu beheben (siehe S. 16). Zu diesem Zweck bieten sie in unterschiedlicher Ausprägung an, DNS-Anfragen zu verifizieren und zu verschlüsseln. Noch geschieht das in enger Rückbindung an das von ICANN administrierte globale DNS-System. Verstärkt sich der Trend, so ist jedoch auch denkbar, dass diese Rückbindung immer weiter aufgelöst wird. Gerade für eine so einflussreiche Firma wie Google könnte es verlockend sein, sich gewissermaßen ein eigenes Internet zu schaffen.

Noch sind solche weitergehenden Überlegungen nur spekulativ. Sie geben aber sehr wohl Anlass zur Sorge. Zwar würde es nicht zum Zusammenbruch der globalen Kommunikation führen, sollte das Internet auf Ebene der Infrastruktur aufgespalten werden. Sicherlich ließen sich technische Wege finden, um einen Austausch über die Grenzen verschiedener Netze hinweg zu ermöglichen — so wie es heute auch machbar ist, sich mit dem Internet in China zu verbinden oder mit Diensten innerhalb des Tor-Netzwerks (siehe Box 7). Doch käme es damit zu einer erheblichen Machtverschiebung zugunsten der »gatekeeper«. Schon heute bemühen sich Staaten und Unternehmen, das Geschehen innerhalb »ihrer« Teilnetze zu kontrollieren. Noch geschieht dies aber zum größten

74 Vgl. hierzu Matthias Schulze, *Kriminalitätsbekämpfung im Dark Net. Neue Ermittlungsansätze statt Verbote*, Berlin: Stiftung Wissenschaft und Politik, April 2019 (SWP-Aktuell 28/2019).

75 Jacob Appelbaum, *RFC 7686: The ».onion« Special-Use Domain Name*, 2015, <https://tools.ietf.org/html/rfc7686> (eingesehen am 11.3.2019).

76 Für ein ähnliches Szenario siehe auch Marcel Dickow, »Das EurasiaNet — oder wie das Internet zerbrach«, in: Sabine Fischer u.a. (Hg.), *Denkbare Überraschungen. Elf Entwicklungen, die Russlands Außenpolitik nehmen könnte*, Berlin: Stiftung Wissenschaft und Politik, Juli 2016 (SWP-Studie 15/2016), S. 47—51. Siehe auch Milton Mueller, »Proposed New IETF Standard Would Create a Nationally Partitioned ›Internet‹«, *Internet Governance Project*, 18.6.2012, <https://www. internet governance.org/2012/06/18/proposed-new-ietf-standard-would-create-a-nationally-partitioned-internet/> (eingesehen am 5.2.2019).

77 Markus Ackeret, »Russlands Internet soll von der Welt isoliert werden«, in: *Neue Zürcher Zeitung*, 12.2.2019, <https://www.nzz.ch/international/russlands-politiker-traeumen-von-der-abschottung-des-russischen-internets-ld.1459253> (eingesehen am 14.2.2019).

78 Christina Hebel, »Entscheidung des Parlaments: Wie Russland sich vom Internet abkoppeln will«, *Spiegel Online*, 11.4.2019, <https://www.spiegel.de/netzwelt/netzpolitik/russland-parlament-billigt-gesetz-zum-abkoppeln-des-eigenen-internets-a-1262345.html> (eingesehen am 18.4.2019).

Teil auf der Ebene der Internet-Anwendungen — und auf Basis einer gemeinsam geteilten Infrastruktur. Diese lässt sich von einzelnen Staaten und Unternehmen nicht vollständig kontrollieren. Bürgerinnen und Bürger nutzen die so verbleibenden Freiräume, um sich auf immer neuen Wegen staatlicher Zensur zu entziehen. Selbst mächtige Firmen können nicht verhindern, dass Konkurrenten sie auf Basis der gemeinsamen technischen Infrastruktur herausfordern. Würden Staaten oder Unternehmen hingegen auch die Infrastruktur selbst kontrollieren, so könnten sie auch diese Freiräume schließen.

Mit der Fragmentierung des Internets droht letztlich eine auf den ersten Blick überraschende weitere Machtkonzentration. Während sich die heutige globale Internet-Infrastruktur durch verschiedene »checks and balances« einer Kontrolle durch einzelne Akteure entzieht, würden voneinander getrennte Netze die Macht staatlicher wie privater »gatekeeper« weiter verstärken.

Empfehlungen für die deutsche Politik

Die Konflikte um die Infrastruktur des Internets sind zutiefst politisch, berühren sie doch zentrale Interessen moderner Gesellschaften. Staaten wie die USA, China oder Russland haben dies erkannt und verfolgen sehr strategisch ihre je eigenen Interessen. In Deutschland hingegen steht eine vertiefte Diskussion zu diesem Thema noch aus. Die folgenden Überlegungen sollen einen Beitrag zu der erforderlichen Debatte leisten.

Das strategische Umfeld

Wie ausgeführt, ist die politische Auseinandersetzung um die globale Internet-Infrastruktur von einer verhärteten Lagerbildung geprägt. Die Vertreter des bisherigen, stark von den USA geprägten Modells der Internet Governance sehen sich dabei mit dem zunehmend selbstbewussten und strategischen Auftreten von Staaten wie China, Russland oder Saudi-Arabien konfrontiert. Deutschland zählt traditionell zu dem von den USA angeführten Lager.

Eine politische Strategie muss diese Polarisierung ernst nehmen, auch und gerade um eigene Akzente setzen zu können. Besondere Aufmerksamkeit sollte dabei jenen Staaten gelten, die sich (noch) nicht einem der bestehenden Lager zuordnen lassen. Eine jüngst veröffentlichte Studie des Thinktanks New America identifiziert in ebendiesem Sinne 50 Staaten, die es als potentielle Verbündete der USA besonders in den Blick zu nehmen gilt, darunter etwa Brasilien, Singapur oder Serbien.[79] Aus deutscher Perspektive würde eine solche Liste an einigen Stellen wahrscheinlich anders aussehen. Entscheidend ist aber der generelle Befund, dass es jenseits der bekannten Lagerbildung in der Internet Governance eine große Zahl an Staaten gibt, die noch unentschlossen sind. Durchaus treffend bezeichnet New America sie als »digital deciders«.

Hinzu kommt, dass sich die Verfechter eines »liberalen« Internets auf Dauer nicht darauf werden beschränken können, den Status quo zu wahren. Zwar haben sie hierbei einen gewissen Vorteil. Weil sie die frühe Entwicklung der globalen Internet Governance geprägt haben, konnten sie in dieser ihre politischen Vorstellungen weitgehend verwirklichen. Bisher mussten sie deshalb nicht selbst auf Veränderungen drängen, sondern konnten es dabei belassen, den aktuellen Zustand zu verteidigen. Mehr noch: Die Sonderstellung der USA gegenüber ICANN und das Konsensprinzip in der ITU machten es in der Vergangenheit leicht, unliebsamen Wandel abzublocken.

In Zukunft jedoch wird es nicht ausreichen, sich auf diesen strategischen Vorteil zu verlassen. Die Idee eines »liberalen« Internets muss permanent weiterentwickelt werden. Wie in den vorigen Abschnitten beschrieben, ist es notwendig, die globale technische Infrastruktur in wesentlichen Hinsichten an neue Anforderungen und veränderte Sicherheitsbedrohungen anzupassen. Schon innerhalb des liberalen Lagers entstehen dabei politische Kontroversen. So haben erst im September 2018 die USA und ihre Verbündeten aus der Nachrichtendienst-Allianz »Five Eyes« noch einmal nachdrücklich darauf gedrängt, dass Telekommunikationsfirmen ihnen die Möglichkeit einräumen müssten, die Verschlüsselung der von den Unternehmen angebotenen Dienste zu umgehen (»lawful access«).[80] Und gerade auch in liberalen Staa-

79 Robert Morgus/Jocelyn Woolbright/Justin Sherman, »The Digital Deciders. How a Group of Often Overlooked Countries Could Hold the Keys to the Future of the Global Internet«, *New America*, 2018, <https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/> (eingesehen am 11.12.2018).

80 Carolin Gißibl, »Angriff der ›Five Eyes‹ auf verschlüsselte Chats und Anrufe«, in: *Süddeutsche Zeitung*, 11.9.2018, <https://www.sueddeutsche.de/digital/datensicherheit-verschluesselung-five-eyes-1.4124671> (eingesehen am

ten stellt sich die Frage, wie die Macht großer Digitalunternehmen demokratisch eingehegt werden kann.

Gelingt es dem liberalen Lager nicht, die Probleme der globalen Internet-Infrastruktur in einer Weise zu lösen, die zugleich für andere Staaten zumindest akzeptabel ist, so droht eine Fragmentierung ebendieser Infrastruktur. Mehr noch als heute werden Staaten, Regionen und Unternehmen versuchen, für »ihren« Bereich des Internets eigene Lösungen zu finden. Eine besondere Rolle kommt hier wiederum jenen Staaten zu, die noch nicht klar einem der beiden Lager zuzuordnen sind. Verfestigt sich bei ihnen der Eindruck, dass die liberalen Staaten schon aus Prinzip jegliche Veränderung am Status quo blockieren, so könnte das die Attraktivität alternativer Angebote von Staaten wie China oder Russland erhöhen.

Prioritäten

Die deutsche Politik im Feld der Internet Governance ist bisher von fünf Zielen geprägt (siehe S. 8f): Förderung der digitalen Wirtschaft (#Z1); Stärkung der Sicherheit von IT-Systemen (#Z2); Schutz der Menschenrechte auch im digitalen Raum (#Z3); Stärkung der Multistakeholder-Governance (#Z4); Bewahrung der globalen Interoperabilität (#Z5).

Die Analyse der aktuellen Konfliktlinien legt nahe, hier Prioritäten zu setzen. So zeigen die Auseinandersetzungen sowohl bei ICANN als auch in der ITU, dass auf absehbare Zeit keine Aussicht besteht, sich auf globaler Ebene über politisch aufgeladene Weiterentwicklungen der Internet-Infrastruktur zu einigen. Mit Blick auf wirtschaftliche Fragen, Menschenrechte und Sicherheit (#Z1, #Z2, #Z3) sind die Differenzen zwischen den Staaten schlicht zu groß. Und wie beschrieben, stößt das bisherige Modell der Multistakeholder-Governance (#Z4) gerade bei solch genuin politischen Fragen an seine Grenzen. Das heißt nicht, dass Deutschland nicht weiterhin für diese Ziele einstehen sollte. Doch ist bei der eigenen strategischen Ausrichtung anzuerkennen, dass diese Ziele auf Ebene der globalen Internet-Infrastruktur zeitnah nicht durchsetzbar sein werden.

Tatsächlich scheint es für die globale Ebene notwendig, zunächst einmal die bisherigen Errungenschaften zu verteidigen. In den Fokus rückt damit das Ziel der Interoperabilität (#Z5). Wie dargestellt, kann in Zukunft nicht mehr als selbstverständlich vorausgesetzt werden, dass es weltweit *eine* technisch einheitliche und global anschlussfähige Internet-Infrastruktur gibt. Schaffen Staaten oder Unternehmen technisch voneinander unabhängige Netze, droht eine problematische Machtverschiebung zugunsten der jeweiligen »gatekeeper«. Dies wiederum hätte aller Voraussicht nach negative Effekte sowohl für die wirtschaftliche Entwicklung (#Z1) als auch für den Schutz der Menschenrechte (#Z3). Den bisherigen Konsens, an einem gemeinsamen Fundament des Internets festzuhalten, gilt es daher zu verteidigen.

Das Ziel globaler Interoperabilität steht dabei allerdings für sich genommen in einer gewissen Spannung zur bisher entwickelten Problemdiagnose. Die beschriebenen politischen Probleme der Internet-Infrastruktur werden durch ein Festhalten an technischer Interoperabilität nicht gelöst, sondern müssen im Gegenteil auf der globalen Ebene weitgehend ausgeklammert werden. Ergänzend sollte die deutsche Politik deshalb versuchen, die eigene logische Infrastruktur in einer Weise weiterzuentwickeln, die *nicht* das Ziel globaler Interoperabilität gefährdet. Einen geeigneten Rahmen dafür bildet die EU. Hier ist es im Prinzip möglich, weitergehende Standards etwa zur Privatsphäre im DNS-System gemeinsam und verbindlich zu setzen. Entscheidend ist dabei, dass nicht das gemeinsame Fundament der globalen Internet-Infrastruktur in Frage gestellt wird, sondern diesem speziell für den Bereich der EU Ergänzungen hinzugefügt werden.

Diese doppelte Zielorientierung an globaler Interoperabilität und regionaler Weiterentwicklung der Internet-Infrastruktur lässt sich im nächsten Schritt in drei Handlungsempfehlungen für die deutsche Politik übersetzen.

Beschränkung von ICANN auf technische Kernfunktionen

Ein einheitliches DNS ist eine der wesentlichen Voraussetzungen für globale Interoperabilität. Es bedarf einer Instanz, die in autoritativer Weise »names and numbers« vergibt, also Domain-Namen und IP-Adressen. Im Prinzip wird dies bis heute weithin akzeptiert. Die Legitimation dafür ist funktional:

14.2.2019). Vgl. auch Monika Ermert, »Banken und Geheimdienste wollen die Krypto-Hintertür«, in: *Süddeutsche Zeitung*, 2.6.2019, <https://www.sueddeutsche.de/digital/tls-verschluesselung-1.4317326> (eingesehen am 14.2.2019).

Die Regelsetzung von ICANN wird anerkannt, weil (noch) fast alle beteiligten Akteure die Notwendigkeit einer solchen Institution einsehen.

Diese funktionale Legitimation gerät aber, wie beschrieben, dort an ihre Grenzen, wo ICANN in den Bereich politisch kontroverser Fragen vordringt. Deutlich zeigt sich hier, dass die Organisation trotz aller Bemühungen um Transparenz und Partizipation nicht ausreichend legitimiert ist, genuin politische Vorgaben zu machen. Auf internationaler Ebene gilt die Zustimmung der Staaten weithin als wichtigste Legitimationsquelle. Als privater Institution ist ICANN diese jedoch versperrt; auch sein Governmental Advisory Committee (GAC), in dem Staaten Mitglied werden können, soll explizit nur beratende Funktion haben.

Die Tätigkeit von ICANN sollte soweit wie möglich auf jene technischen Funktionen begrenzt werden, die weithin anerkannt sind.

Wenn sich aber die Legitimationsbasis nicht ausweiten lässt, scheint es ratsam, die Rolle von ICANN in der globalen Internet Governance durch eine bewusste Beschränkung zu verteidigen. Dies würde bedeuten, die Tätigkeit von ICANN soweit wie möglich auf jene Funktionen zu begrenzen, die weithin anerkannt sind. Dazu zählt insbesondere die autoritative Verwaltung der DNS Root Zone, also der hierarchischen Spitze des DNS, als einer wesentlichen Voraussetzung für globale Interoperabilität (siehe Box 2, S. 12).

Diese Position ist nicht unumstritten und müsste proaktiv beworben werden. Einen unmittelbaren Ansatzpunkt hierfür bietet das GAC, in dem Deutschland mit eigener Stimme vertreten ist. Im besten Fall würde man hier eng koordiniert mit den anderen EU-Staaten handeln. Zudem ist nichts Unlauteres daran, auch bei deutschen Unternehmen, die sich in ICANN engagieren, für eine entsprechende Politik zu werben und so den eigenen Wirkungskreis zu erweitern.

Mit Blick auf country-code Top Level Domains (ccTLD) hat sich ganz im Sinne einer solchen Beschränkung von ICANN bereits eine gewisse politische Arbeitsteilung herausgebildet. Die Organisation gesteht bei ccTLD dem GAC eine besondere Rolle zu. Außerdem wird anerkannt, dass die für ccTLD zuständigen Registries (siehe Box 5, S. 23) der Jurisdiktion der jeweiligen Staaten unterstehen, dass also etwa DENIC — die Registry für die Domain .de — dem deutschen Recht untersteht.

Schwieriger ist jedoch, ICANN bei der Vergabe und dem Betrieb von generic Top Level Domains (gTLD) auf technische Kernfunktionen zu beschränken. Das Problem bei der Vergabe einer gTLD wie .amazon besteht darin, dass in solchen Fällen eben umstritten ist, welche Registry eine Domain verwalten darf. Solange ungeklärt ist, welche Registry zuständig ist, bleibt aber auch offen, in welche Jurisdiktion die Domain fällt. Die bei ccTLD übliche Arbeitsteilung zwischen ICANN und den Staaten ist hier also nicht möglich. Auch gibt es keine globale Institution mit der Autorität, Konflikte wie im Fall der Domain .amazon in einer für alle Beteiligen verbindlichen Weise zu lösen. Daher werden solche Auseinandersetzungen auch in Zukunft von ICANN selbst behandelt werden müssen. Mit der Uniform Domain-Name Dispute-Resolution Policy hat ICANN dafür bereits vor längerem ein Verfahren entwickelt, das die Interessen aller Beteiligten berücksichtigen soll. Am Ende jedoch wird es in entsprechenden Fällen auch weiter zu Entscheidungen kommen, deren politische Bedeutung durch die technisch-funktionale Legitimation von ICANN nicht ausreichend gedeckt ist.

Um dieses Problem wenigstens ein Stück weit abzumildern, sollte Deutschland über sein Engagement im GAC die bereits bestehenden Bemühungen unterstützen, Entscheidungsprozesse bei ICANN transparenter zu gestalten. In vielerlei Hinsicht ist die Organisation bereits sehr transparent. Die Vielzahl an Verfahren, Verfahrensregeln und Verfahrensbeteiligten macht es allerdings zu einer ungemein anspruchsvollen Aufgabe, die öffentlich verfügbaren Informationen auszuwerten. Dies ist vor allem ein Problem für die Vertreterinnen und Vertreter der Zivilgesellschaft, aber auch für viele Staaten. Um die Akzeptanz für die Kernfunktionen von ICANN zu erhöhen, sollte Deutschland dementsprechend Initiativen zur Verbesserung der Transparenz von ICANN unterstützen, insbesondere mit Blick auf die Vergabe von gTLD.

Sind gTLD erst einmal vergeben, bietet es sich mit Blick auf den Betrieb dieser Domains wiederum an, eine politische Arbeitsteilung anzustreben, die ICANN davon befreit, unzureichend legitimierte Entscheidungen treffen zu müssen. In diesem Sinne könnte Deutschland im GAC darauf hinwirken, zwei seit längerem schwelende Konflikte zu entschärfen:

- Der erste Fall betrifft die aktuelle Debatte um das WHOIS-System für gTLD (siehe S. 23). Gerade hier scheint es geboten, dass ICANN sich zurückhält.

Anstatt ein universelles WHOIS-System zu schaffen, sollte ICANN die Registries von gTLD darauf verpflichten, transparent aufzuzeigen, welcher Jurisdiktion sie unterstehen, und ein entsprechendes WHOIS-System bereitzustellen. Die gTLD .audi etwa wird von der Audi AG betrieben. ICANN sollte dem Unternehmen dementsprechend abverlangen, ein WHOIS-System zu schaffen, das im Einklang mit deutschem und europäischem Datenschutzrecht steht. Wollen Ermittler aus anderen Staaten darüber hinaus Zugriff auf öffentlich nicht zugängliche Daten erhalten, stehen ihnen die üblichen Wege von Rechtshilfeersuchen zu Gebote. Solche Instrumente erscheinen vielen Strafverfolgungsbehörden im Zeitalter digitaler Kommunikation als zu träge, wie derzeit die Diskussionen um den US Cloud Act und das europäische E-Evidence-Paket verdeutlichen. Gerade hier zeigt sich aber auch, wie hochpolitisch Fragen der digitalen Beweissicherung sind. ICANN verfügt schlicht nicht über die Legitimität, um hier autoritative Antworten zu liefern.

- Auch im Streit um »2nd level two-character country codes« könnte die deutsche Politik im Rahmen des GAC zu deeskalieren versuchen (siehe S. 24). Wie beschrieben, lässt sich diese Kontroverse als Versuch einiger Staaten verstehen, ihre Autorität über ccTLD hinaus auf den Bereich der gTLD auszuweiten. Der Nachweis, dass hier wichtige Interessen der Staaten betroffen sein könnten, steht allerdings noch aus. So ist es seit jeher nicht unüblich, dass Websites auf Deutsch gestaltet sind oder auch eine .de-Domain verwenden, ohne von einem deutschen Anbieter betrieben zu werden. Auch hier steht den Staaten in schwerwiegenden Fällen die Möglichkeit offen, sich über Rechtshilfeersuchen an die jeweils zuständigen Registries zu wenden. Ist der deutschen Politik am Erhalt der Kernfunktion von ICANN gelegen, sollte sie deshalb aktiv dafür eintreten, die Organisation von der Last einer politischen Kontroverse zu befreien, die überwiegend symbolischen Gehalt hat und gerade so dazu dient, die Legitimität von ICANN in Frage zu stellen.

Rückhalt für Multistakeholder-Institutionen in ITU und IGF

Nichtstaatliche Governance stößt bei politischen Konflikten aus systemischen Gründen an ihre Grenzen. Dennoch hat das bisherige Modell der Internet Governance auch seine Stärken. So stellen Multistakeholder-Institutionen wie IETF, IEEE und W3C öffentliche Güter in Form von Protokollen und Standards bereit. Auf diese Weise leisten sie einen wesentlichen Beitrag dazu, die globale Internet-Infrastruktur zu erhalten und weiterzuentwickeln. Und bei aller Kritik im Detail ist es durchaus eine beeindruckende Leistung, dass ICANN zuverlässig ein einheitliches globales DNS zur Verfügung stellt. Im Bewusstsein um die Grenzen nichtstaatlicher Governance sollte die deutsche Politik diesen Institutionen daher überall dort politisch Rückhalt bieten, wo sie ihre Stärken ausspielen können.

Dabei sollte die deutsche Politik die entsprechenden Institutionen der Vereinten Nationen als wichtige Orte der globalen politischen Auseinandersetzung verstehen. Aus unterschiedlichen Gründen sind das Internet Governance Forum (IGF) und die International Telecommunication Union (ITU) selbst nicht geeignet, die Konflikte um die globale Internet-Infrastruktur zu lösen (siehe S. 22ff). Nicht zu unterschätzen ist aber, dass diese Institutionen Foren schaffen, in denen (noch) fast alle Staaten zusammenkommen, um sich über Fragen der globalen Internet Governance auszutauschen. Im Fall des IGF besteht außerdem zumindest von der Grundanlage her ein Rahmen, in dem die Staaten regelmäßig und systematisch in Austausch mit Vertretern aus Wirtschaft und Zivilgesellschaft treten.

Die deutsche Politik sollte diese Foren nutzen, um für die Bedeutung von Multistakeholder-Institutionen wie ICANN, IETF oder W3C zu werben. Die Ausgangslage dafür ist gut. Als drittgrößter Beitragszahler findet die Bundesrepublik in der ITU Gehör, und als Ausrichter des IGF 2019 wird sie auch in diesem Forum prominent wahrgenommen.

Dabei sollte sich Deutschland der beschriebenen Lagerbildung entziehen und konstruktive Kritik an den bestehenden Institutionen der globalen Internet Governance aufgreifen. Dies wäre nicht nur der Sache nach angemessen, sondern zudem ein Signal in Richtung jener Staaten, die ebendiese Art berechtigter Kritik üben. Wie im Fall von ICANN stellt sich auch für Institutionen wie IETF, IEEE oder W3C die Herausforderung, Transparenz in praktisch bedeutsamer Weise herzustellen. Hinzu kommt der Umstand, dass Unternehmen in diesen Institutionen eine dominante Rolle spielen (siehe S. 10). Auch dieses Problem gilt es offen anzuerkennen; um es zumindest auf ein erträgliches Maß zu reduzieren, sollte die Teilnahme von Zivilgesellschaft und Wissenschaft gefördert werden.

Auch sollte sich Deutschland gerade an dieser Stelle um Konsistenz zwischen innerem Wirken und äußerem Auftreten bemühen. Sowohl auf Ebene der Internet-Infrastruktur (z.B. Breitbandausbau, 5G) als auch auf jener der Internet-Dienste (z.B. Netzwerkdurchsetzungsgesetz) bietet sich die Möglichkeit, exemplarisch aufzuzeigen, an welchen Stellen und in welcher Weise die deutsche Politik es für angemessen hält, welche »stakeholder« in welcher Weise zu beteiligen — und wo die Grenzen der Beteiligung nichtstaatlicher Akteure liegen.

Weiterentwicklung der Internet-Infrastruktur auf EU-Ebene

Die bisherigen Überlegungen bilden Vorschläge dazu, wie Deutschland seinen Einfluss in ICANN, ITU und IGF nutzen kann, um das Ziel weltweiter Interoperabilität zu verfolgen. Das politische Bemühen, auf globaler Ebene eine gemeinsame technische Infrastruktur zu erhalten, wird aber noch nicht die Konflikte lösen, die mit der Weiterentwicklung dieser Infrastruktur verbunden sind. Im Gegenteil wird der Preis für das Festhalten an globaler Interoperabilität wahrscheinlich darin bestehen, solche Konflikte zum großen Teil auszuklammern. Wenn aber globale Lösungen dieser Probleme aus politischen Gründen auf absehbare Zeit nicht möglich sind, sollte Deutschland sich dafür einsetzen, Lösungen soweit wie möglich im Rahmen der EU voranzutreiben.[81]

Mit Blick auf die Konfliktlinien der globalen Internet Governance verortet sich die EU selbst im »liberalen« Lager. Sehr deutlich etwa hat sich 2014 die damalige Brüsseler Kommissarin für die Digitale Agenda, Neelie Kroes, für ICANN und das Multistakeholder-Modell der Internet Governance eingesetzt. Zugleich ist jedoch auch innerhalb der EU umstritten, wie die Zukunft des Internets aussehen soll. Mit der DSGVO hat sich die EU zuletzt klar als Verfechter des Datenschutzes positioniert. Die vorgesehene Zuspitzung der DSGVO auf den Bereich digitaler Kommunikation im Rahmen der E-Privacy-Verordnung ist jedoch Gegenstand heftiger Auseinandersetzungen.

81 Zur Rolle der EU siehe auch Matthias Kettemann/Wolfgang Kleinwächter/Max Senges, *The Time Is Right for Europe to Take the Lead in Global Internet Governance*, Frankfurt a.M.: Goethe-Universität, Februar 2018 (Normative Orders Working Paper 2/2018); Hohmann/Benner, *Getting »Free and Open« Right* [wie Fn. 73].

Uneinigkeit herrscht hier sowohl unter den Mitgliedstaaten als auch im Verhältnis zwischen Mitgliedstaaten und europäischen Unternehmen. Und in Europa versuchen Sicherheitsbehörden ebenfalls mit Nachdruck, rechtlich wie operativ Wege zu finden, mit denen sich Verschlüsselungsverfahren für eigene Zwecke umgehen lassen. Um die beschriebenen strukturellen Probleme der Internet-Infrastruktur auf europäischer Ebene anzugehen, bedarf es daher auch hier zunächst intensiver Überzeugungsarbeit.

Weiterentwicklungen in Europa dürfen nur eine Ergänzung der globalen Internet-Infrastruktur sein – keine Alternative zu ihr.

Legt man den Fokus auf die europäische Ebene, entsteht allerdings eine Spannung zwischen dem Ziel globaler Interoperabilität und dem Anliegen, die Internet-Infrastruktur in Europa weiterzuentwickeln. Um diese Spannung nicht in einen Widerspruch münden zu lassen, dürfen alle Weiterentwicklungen in Europa nur eine Ergänzung der globalen Internet-Infrastruktur sein — aber keine Alternative zu ihr. Dieser Leitgedanke soll im Folgenden anhand der zuvor analysierten Konflikte um die globale Internet-Infrastruktur praktisch verdeutlicht werden.

So lassen sich Maßnahmen zur Erhöhung der Sicherheit und des Datenschutzes in Europa durchsetzen, ohne die Kompatibilität mit anderen Konfigurationen zu gefährden. Die EU könnte etwa vorgeben, dass europäische Registrars (siehe Box 5, S. 23) und ISPs DNSSEC einsetzen müssen. Zumindest für alle europäischen ccTLD würde dies die Sicherheit erheblich erhöhen, außerdem auch für alle in Europa registrierten gTLD. Des Weiteren könnte die EU verbindlich vorgeben, dass Internet Service Provider die DNS-Anfragen ihrer Kunden in angemessener Weise verschlüsseln (z.B. durch »DNS-over-TLS«).

Die EU könnte zudem europäische Netzbetreiber darauf verpflichten, Mechanismen in Anlehnung an die bisherigen Varianten von BGPsec (siehe S. 18) zu implementieren, um wenigstens innerhalb der EU die Sicherheit des Routing-Systems zu verbessern. Damit würde das Problem der gezielten Umleitung von Daten im Sinne des »BGP hijacking« zwar nicht in seiner globalen Dimension gelöst, doch gäbe es einen Zugewinn an Sicherheit für europäische Internet-Nutzer. Verstärkt werden könnte der Effekt noch durch die Vorgabe, Verbindungen zwischen Geräten in Europa prioritär über derart abgesicherte Routen

zu leiten. In gewisser Weise knüpft dieser Vorschlag an die Ideen für ein »Schengen-Routing« an, wie sie 2013 in Reaktion auf die Enthüllungen über die Abhörmaßnahmen der NSA aufgekommen sind.[82] Der Gedanke hier war, Verbindungen zwischen zwei Geräten in Europa nicht unnötig über Server außerhalb des Kontinents zu lenken. Anders als bei den Überlegungen für ein »Schengen-Routing« wäre für die Priorisierung beim Routing aber nicht das Territorium an sich entscheidend, sondern die Frage, ob Betreiber von Autonomous Systems ausreichende Maßnahmen zum Schutz vor »BGP hijacking« ergreifen. Im Falle von Verbindungsengpässen innerhalb Europas könnte so weiterhin auf Alternativrouten außerhalb Europas zugegriffen werden — Priorität hätten aber auch hierbei jene Teilnetze, deren Routing-Angaben als hinreichend vertrauenswürdig gelten.

Schließlich könnte Europa seinen wirtschaftlichen Einfluss nutzen, um gezielt die Schwächen des heutigen Netzwerks von Unterseekabeln anzugehen (siehe S. 18f). Besonders verletzbare »chokepoints« zu vermeiden — wie bei den Verbindungen Europas nach Asien durch den Suez-Kanal — liegt im ureigensten europäischen Interesse. Hier gilt es, den Betreibern der Netzwerke entsprechende Anreize zu verschaffen. Darüber hinaus könnte es die EU aber auch als ihre Aufgabe begreifen, im Rahmen der Entwicklungszusammenarbeit die bisher mangelhafte Anbindung vor allem afrikanischer Staaten an das Netz der Unterseekabel zu verbessern. Dies wäre nicht nur im Sinne der eigenen entwicklungspolitischen Ziele Deutschlands sinnvoll, sondern würde zudem der deutschen Politik gerade in dieser Region neue Verbündete in den Auseinandersetzungen um die globale Internet Governance einbringen.

Mit solchen Maßnahmen hat Europa die Chance, sich in den Strukturen der globalen Internet Governance als digitale Gestaltungsmacht zu präsentieren, mithin selbstbewusst und nach eigenen politischen Vorgaben die Weiterentwicklung der globalen Internet-Infrastruktur voranzutreiben. Zu betonen ist dabei noch einmal, dass dies *nicht* im Widerspruch zur Idee globaler Interoperabilität steht. Die vorgeschlagenen Maßnahmen bilden vielmehr Ergänzungen für das gemeinsame globale Fundament des Internets.

82 Jan-Peter Kleinhans, »Schengen-Routing, DE-CIX und die Bedenken der Balkanisierung des Internets«, *netzpolitik.org*, 13.11.2018, <https://netzpolitik.org/2013/schengen-routing-de-cix-und-die-bedenken-der-balkanisierung-des-internets/> (eingesehen am 11.12.2018).

Abkürzungen

BGP	Border Gateway Protocol
BGPsec	Border Gateway Protocol Security
ccTLD	country-code Top Level Domain
DENIC	Deutsches Network Information Center
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DSGVO	Datenschutz-Grundverordnung
GAC	ICANN Governmental Advisory Committee
gTLD	generic Top Level Domain
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IPv4	Internet Protocol Version 4
ISP	Internet Service Provider
ITU	International Telecommunication Union
IXP	Internet Exchange Point
GAC	Governmental Advisory Committee
NGO	Non-Governmental Organization
NSA	National Security Agency
SSL	Secure Socket Layer
TLS	Transport Layer System
W3C	World Wide Web Consortium

Literaturhinweise

Daniel Voelsen
5G, Huawei und die Sicherheit unserer Kommunikationsnetze. Handlungsoptionen für die deutsche Politik
SWP-Aktuell 5/2019, Februar 2019

Matthias Schulze
Kriminalitätsbekämpfung im Dark Net. Neue Ermittlungsansätze statt Verbote
SWP-Aktuell 28/2019, April 2019

Marcel Dickow
Das EurasiaNet – oder wie das Internet zerbrach
in: Sabine Fischer/Margarete Klein (Hg.), Denkbare Überraschungen. Elf Entwicklungen, die Russlands Außenpolitik nehmen könnte
SWP-Studie 15/2016, Juli 2016, S. 47—52