CGS - Discussion Papers
www.cgs-bonn.de

Dominikus Edelbert Leicht

CGS-Spezial-Reihe: Analysen zur globalen Politik des Internets

ZUKUNFT DES CYBERSPACE:

ABGRENZENDE REGULIERUNG ODER WELTWEITER WILDER WESTEN?

CGS - Discussion Paper 16

Dezember 2014

Center for Global Studies bonn

universitätbonn

Liegt die Zukunft des Internets in einem fragmentierten Netzwerk, das sich entlang nationalstaatlicher Grenzen aufspaltet? Ausgangspunkt ist die Feststellung, dass Staaten den neuen Bedrohungen durch und im den Cyberspace nur schwer begegnen können. Im „Wilden Westen“ digitaler Kommunikationsstrukturen sehen viele Regierungen nationalstaatliche Souveränität in Gefahr. In der Tat, gibt es eine wachsende Tendenz, dass Staaten mit Nachdruck versuchen ihre Hoheitsrechte im internationalen Konsens auf das Internet auszubreiten.

1. Einleitung

Die Möglichkeiten, die der Menschheit mit dem Aufkommen des Cyberspace und der breiten Nutzung dessen gegeben worden sind, scheinen endlos. Immer neue Entwicklungen machen uns das Alltagsleben einfacher, ob beim Einkaufen, dem schnellen Abrufen von Informationen oder der Kommunikation. Die ganze Welt ist vernetzt und es ist ein Leichtes, ein in China aufgenommenes Foto über Staatsgrenzen hinweg binnen Sekunden seinen Freunden in Deutschland zugänglich zu machen. Doch neben harmlosen Fotos und Grüßen kann durch den Cyberspace nun auch verschiedenste Malware quer durch die Welt versendet werden. Spätestens mit dem Bekanntwerden des *Stuxnet*-Virus und dessen Ziel – iranische Atomanlagen – stellt sich jedoch die Frage nach der Relevanz von Staatsgrenzen im Cyberspace.

Die vorliegende Arbeit wird das aufkommende Phänomen der Fragmentierung des Internets zum Gegenstand haben. Dabei soll im Besonderen ein Augenmerk auf der Realisierbarkeit von nationalstaatlichen Grenzen im Cyberspace sowie auf Überlegungen, durch staatliche Einrichtungen ihre Souveränität – welche diese durch das Internet in Gefahr sehen – zu erhalten, liegen. Hierbei soll eine Abgrenzung zwischen dem theoretischen Hintergrund und der technischen Realisierbarkeit erfolgen, die zum Teil weit auseinander liegen. Außerdem wird die Rolle nichtstaatlicher Akteure, wie NGOs (nongovernmental organizations) sowie internationaler staatlicher Organisationen in diesem Zusammenhang beleuchtet werden. Ziel der Untersuchung ist es, zu zeigen, dass Staaten in Zukunft Regulierungen schaffen werden, um das Medium Internet politisch und juristisch besser in das theoretische Konzept von Nationalstaaten integrieren zu können.

Die Arbeit wird zu diesem Zweck in drei Teile gegliedert sein. Im ersten Abschnitt sollen theoretische Konzepte zu staatstheoretischen Problemen durch den Cyberspace aufgezeigt werden. Außerdem sollen einige definitorische Grundlagen geschaffen werden, auf welchen die restliche Untersuchung fußt. Im zweiten Abschnitt sollen dann die Theorien zur Fragmentierung des Internets Überlegungen zur technischen Realisierbarkeit gegenüber gestellt werden. Hierbei wird das russische RUNET als empirisches Untersuchungsobjekt herangezogen, um zu zeigen, wie staatliche Grenzziehung im Internet bereits realisiert wird. In einem dritten Teil wird die Rolle von Staaten im Zusammenhang mit NGOs und internationalen staatlichen Organisationen betrachtet. Im Abschluss werden die gewonnenen Erkenntnisse genutzt, um einen Ausblick in die Zukunft nationalstaatlicher Regulierungen des Internets zu wagen.

2. Theoretischer Hintergrund

Mit Stuxnet wurde der Staatengemeinschaft vor Augen geführt, dass die Entwicklung von Malware einen enormen Fortschritt gemacht hat und es nun möglich ist, gezielt – vitale – Infrastrukturen eines Staates anzugreifen, ohne dabei die physischen Staatsgrenzen zu passieren. Dieser Fakt beeinträchtigt in erheblichem Maße das Sicherheitsbedürfnis eines Nationalstaates, der hierdurch seine Souveränität in Gefahr sieht und darum bemüht ist, diesem Problem zu begegnen und staatliche Grenzen auch im Cyberspace zu errichten.
Das Sicherheitsbedürfnis des Nationalstaates ist dabei durch die momentane Struktur des Cyberspace in mehreren Facetten eingeschränkt. Zum einen ist der Staat verantwortlich, für die Unversehrtheit seiner eigenen Bürger Sorge zu tragen. Demchack und Dobrowski weisen darauf hin, dass dem Staat unter anderem diese Fähigkeit zunehmend zu entgleiten droht.[1] Auf der anderen Seite ist es durch den Cyberspace möglich geworden, dass Einzelpersonen oder kleine, kaum zu identifizierende Gruppen bedeutenden wirtschaftlichen Schaden anrichten können.[2] Hiermit wird der Bürger eines Staates zum Objekt, das Schutz benötigt, gleichzeitig aber auch eine mögliche Gefahrenquelle für den Staat.
Die Lokalisierung von Gefahren ist eine weitere Facette, die bei der genauen Definition des Problems wichtig ist. Drezner stellt heraus, dass die niedrigen Transaktionskosten von Kommunikation es einzelnen Individuen und anderen nichtstaatlichen Akteuren erleichtern, sich staatlicher Regulierung zu entziehen.[3] Besonders aus diesem Punkt heraus entsteht ein drängendes Bedürfnis des Staates, sein Gewaltmonopol auch auf den Cyberspace auszubreiten. Dabei ist die Vorstellung naheliegend, nationalstaatliche Grenzen zu errichten. So stellen Demchack und Dobrowski auch klar heraus, dass hier eine Entwicklung – vergleichbar mit der Etablierung von Staatsgrenzen mit dem Westfälischen Frieden 1648 – bereits begonnen hat. Daher treffen sie folgende Prognose: “In the new cyber-Westphalian process, digital regions complete with borders, boundaries and frontiers that are accepted by all states will inevitably emerge“.[4]
Staatsgrenzen, ob physische Ländergrenzen oder ein informationstechnisches Äquivalent, erfüllen dabei mehrere Zwecke. Zum einen sollen sie Gefahren außerhalb des Staatsgebietes und damit abseits der Bevölkerung halten. Zum anderen erfüllen Staatsgrenzen auch den Zweck, Bürger innerhalb eines bestimmten Gebietes zu halten beziehungsweise deren zugängliche Informationen zu begrenzen. Somit haben sie aus rein physischer Sicht eine einschließende und gleichzeitig ausschließende Aufgabe. Welchem Zweck mehr Bedeutung zukommt, unterscheidet sich je nach Staat und Staatsform. Außerdem definieren Staatsgrenzen auch einen rechtlichen Raum, in dem die Jurisdiktion des jeweiligen Staates

[1] Demchack, Chris, Dombrowski Peter, ‘Rise of a Cybered Westphalian Age’, Strategic Studies Quarterly, 5 (1), 2011, S. 33.
[2] Wie hoch die wirtschaftlichen Einbußen durch Cyberattacken tatsächlich sind, ist schwer festzustellen. Schätzungen reichen gar bis Trillionen Dollarbeträgen siehe: Weinberg Allan, Kaplan James, Bailey Tucker , The $3,000bn threat from cyber attacks, Financial Times, 28.01.2014. Allerdings sind hier mögliche wirtschaftliche Interessen, die Kosten höher zu schätzen, um Schutzsoftware zu vertreiben, nicht zu vernachlässigen.
[3] Drezner Daniel, The Global Governeance: Bringing the State Back In, Political Science Quarterly, 119(3), 2002, S. 478.
[4] Demchack/Dombrowski, Westphalian Age, S. 57. Eine ähnliche Position nimmt Paul Fehlinger zuletzt in einem Artikel im April 2014 ein. Siehe: Fehlinger Paul, Cyberspace fragmentation: an internet governance debate beyond infrastructure, Internet Policy Review, 17.04.2014.

gilt. David Johnson und David Post stellten in ihrer Untersuchung dazu fest, dass Staatsgrenzen, die eben die rechtlichen Grenzen und Mächte eines Staates definieren, im Cyberspace nicht vorhanden waren. Dies führten sie unter anderem darauf zurück, dass die Gesetzmäßigkeiten der physischen Welt nicht auf den virtuellen Raum des Cyberspace anwendbar waren. [5] In ihrer Untersuchung kamen sie zu dem Schluss, dass sich Nationalstaaten zunehmend darum bemühen würden, ihre Souveränität auch auf den Cyberspace auszudehnen.

Neben diesem offensichtlichen Zweck können Staatsgrenzen jedoch auch ein Statement darstellen. Diese These geht auf die Untersuchungen von Forrest Hare [6] zurück, der die Errichtung von Grenzen im Cyberspace mit dem Versuch vergleicht, durch die besonderen Maßnahmen der USA, den Drogenhandel über die mexikanisch-US-amerikanische Grenze hinweg zu unterbinden. Beidem schreibt Hare dabei eher einen symbolischen Charakter zu, mit dem Staaten zeigen, dass sie Verbrechen und die Verletzung hoheitlicher Rechte nicht tolerieren und darauf drängen, ihre Souveränität zu erhalten. Der unmittelbare Effekt und Zweck der Grenzen steht dabei dem symbolischen Charakter nach.[7] Dieser Punkt wird im späteren Verlauf der Arbeit bei der Frage nach der Durchführbarkeit einer Grenzziehung eine Rolle spielen.

Eine Abgrenzung kann im Cyberspace jedoch auch ohne ein direktes Zutun des Staates erreicht werden. Im Jahr 2000 griff eine Untersuchung von Alexander Halavais die Ergebnisse Johnsons und Posts über sich entwickelnde nationale Grenzen auf und führte die These an, dass „soziale“ Grenzen im Internet bestehen und den Internetverkehr beeinflussen, sodass die Kommunikation sich weiter an nationalstaatlichen Grenzen orientierte.[8] „Soziale Grenzen“ umfassen hierbei beispielsweise sprachliche Barrieren oder kulturelle Unterschiede, die bedingen, dass die Surfgewohnheiten der Nutzer sich auf einen – im Verhältnis zur Größe des Cyberspace – kleinen Rahmen von Internetseiten beschränken. Das Bemerkenswerte an dieser Feststellung war, dass sich das global vernetzte Internet – zumindest in dieser Zeit – nicht als solches darstellt.[9] Die Gewohnheit, sich im internationalen Cyberspace trotzdem in regionalen Grenzen zu bewegen, kann bei der zukünftigen Errichtung von nationalen Grenzen eine wichtige Rolle zur Realisierbarkeit spielen, da eine Abgrenzung anhand dieser „sozialen“ Grenzen den Bürgern wesentlich einfacher aufzuerlegen wäre.

Das Sicherheitsbedürfnis des Staates ist nicht zuletzt zusätzlich durch die Entwicklung von Technologie in Gefahr. Die technologischen Innovationen in der Informationstechnik schreiten sehr schnell voran. Eine Menge von Daten, die vor wenigen Jahren noch eine ganze Festplatte in der Größe eines Taschenbuchs beanspruchte, lässt sich heute auf einem Speicherchip lagern, der kaum größer als ein Fingernagel ist. Die Geschwindigkeit der

---

[5] So postulieren sie “*The law of a given place must take into account the special charactaristics of the place it regulates and the types of persons, places and things found in there*“ was für den Cyberspace nicht gegeben war. Johnson David, Post David, Law and Broder:The rise of Law in Cyberspace, Stanford Law Review, 48 (5), 1996, S. 1401.

[6] Forrest Hare ist Oberstleutnant (Lt. Colonel) in den amerikanischen Streitkräften und arbeitet für das Department of Defense (DoD).Zuletzt war er für die Entwicklung einer Cyberspace-Strategie der US-Air-Force verantwortlich. http://www.ccdcoe.org/cyberwarfare/156.html (Stand: 28.07.2014).

[7] Hare Forrest, Borders in Cyberspace: Can Sovereignty Adapt to the Challanges of Cyber Security?, 2010, S. 15.

[8] Halavais Alexander, Border on the World Wide Web, in: New Media and Society, Vol 2 (1), 2000, S. 23-24.

[9] Eine Übersicht über die Verteilung der Internet-Kapazität und die Verlinkungen: Global Internet Geography, Executive Summary, http://www.telegeography.com/page_attachments/products/website/research-services/global-internet-geography/0004/1851/GIG_Executive_Summary.pdf (2013).

Entwicklung macht es dabei dem Staat sehr schwer, abzuwägen was heute möglich ist und morgen möglich sein könnte. Damit ist dieser in seinen Möglichkeiten, sich abzusichern, eingeschränkt, da eine Abschätzung zukünftiger Gefahren erschwert wird. Hinzu kommt, dass trotz aller möglichen Sicherheitsmaßnahmen, die Vorteile des Internets für die Wirtschaft nicht geschmälert werden dürfen. Hare merkt dazu an, dass sich Staaten hier in einer Zwickmühle befinden, zwischen dem Drang, den Cyberspace einzugrenzen und der Notwendigkeit, diesen offen genug zu lassen, damit die Kommunikation, speziell zwischen öffentlichem und privatem Sektor, nicht eingeschränkt wird.[10]

3. Technische Realisierbarkeit von staatlicher Grenzziehung

Bei der Realisierung von staatlichen Grenzen im Cyberspace spielt also die schnelle technologische Entwicklung eine wichtige Rolle. Was heute noch unvorstellbar scheint, könnte in sehr naher Zukunft doch realisierbar werden. Es ist daher nicht sinnvoll, an diesem Punkt eine zukünftige Grenzziehung a priori auszuschließen, nur weil heutige Methoden so etwas nicht zulassen. Nichtsdestotrotz ist es zielführend, eine Momentaufnahme der technischen Möglichkeiten zur Regulierung des Internets zu machen, um herauszuarbeiten, inwiefern heute bereits eine Fragmentierung des Internets betrieben wird. Hieraus lassen sich Erkenntnisse darüber ziehen, auf welcher Ebene eine Fragmentierung des Internets in Zukunft am Wahrscheinlichsten ist.

Jonah F. Hill bezieht sich in seiner Untersuchung auf vier verschiedene Ebenen – Layer –, aus denen sich das Internet zusammensetzt: Menschen, Information, sowie eine logische und eine physische Ebene.[11] Hierzu stellt er weiter fest, dass die dezentrale Organisation des Cyberspace – die eben eine Fragmentierung verhindern soll – nur wenige Ansatzpunkte bietet. Eine der wenigen zentralen Stellen auf der logischen Ebene bildet das Domain Name System (DNS), welches die Aufgabe übernimmt, den Namen einer Internetseite mit dessen Internet-Protocol-Adress (IP Adresse) zu verbinden und dem Nutzer die aufgerufenen Information zurückzuliefern. Greift man in diesen Prozess mit Hilfe der Internet Service Provider (ISPs) ein, die hierzu die Möglichkeit haben, kann ein Nutzer auf eine andere Seite geleitet werden, ohne dies zu merken: "If an ISP did so, its users might be sent to an entirely different website than the one they thought they were requesting, or might receive no information back at all. Users would have no way of knowing that they had been sent to the wrong site because the redirection would appear seamless.“[12] Diese Möglichkeit kann ein Staat nutzen, um seinen Bürgern Grenzen zu setzten, indem Anfragen auf Seiten umgeleitet werden und sie sich somit in einem begrenzten Raum des Cyberspace bewegen.

Steven J. Murdoch und Ross Anderson stellen in ihren Untersuchungen aus dem Jahr 2006 einige Mechanismen vor, mit denen Datenfluss im Internet gefiltert werden kann. Dabei stellten sie die Vor- und Nachteile der Methoden einander gegenüber. Einige dieser Möglichkeiten, welche für die Untersuchung besonders relevant sind, sollen an dieser Stelle

[10] Hare, Borders in Cyberspace, 2010, S. 4.
[11] Das Modell geht zurück auf David Clark und bildet ein weit verbreitetes System, das Internet zu unterteilen. Siehe: Hill Jonah F., Internet Fragmentation, Highlighting the Major Technical Governance and Dipmlomatic Challages for U.S. Policy Makers, Belfare Center for Science and International Affairs, 2012, S. 13.
[12] Ebd., S. 15-16.

kurz erläutert werden.[13] Zum einen bietet das IP-Paket, bestehend aus einem Kopfbereich – der Informationen, wie beispielsweise die Ziel-IP-Adresse enthält – und einem Datenbereich – mit dem wirklichen Inhalt der Sendung – zweierlei Möglichkeiten zur Überwachung und Filterung. Zum einen ist dies die Filterung allein nach den im Kopfbereich befindlichen Daten, womit beispielsweise anhand der Zieladresse entschieden werden kann, ob das Paket weitergeleitet wird. Zum anderen besteht aber auch die Möglichkeit, den Inhalt des Pakets zu untersuchen und direkt hiernach zu filtern.[14] Hare sieht in letzterer Methode des sogenannten *deep packet inspection* eine vielversprechende Möglichkeit. Internationale Verbindungen könnten auf ihren Inhalt hin überprüft und dann gegebenenfalls aufgehalten werden. Die Verbindungen im Inland wären hiervon ausgeschlossen. Hare schlägt hierzu die Errichtung von Kontrollen an den physischen Knotenpunkten des Cyberspace vor:

> "For example, a border control point could be established at the terminus between undersea cables and fibre optive lines. At these points, customs, law enforcement, or other agents of the federal government could employ any of several technical solutions such as deep packet inspection devices or Anagran flow management devices".[15]

Eine andere Möglichkeit bietet sich in der Errichtung sogenannter Proxy-Server[16], über die allen Bürgern eines Staates der Zugang zum Internet gewährt wird. Dabei müsste jedoch jegliche Möglichkeit, auf anderem Weg Zugang zum world wide web zu bekommen, verhindert werden.[17] Der Vorteil bei dieser Methode liegt darin, dass Staaten durch diese Proxy-Server den Internetverkehr einfach überwachen und filtern können, gleichzeitig aber auch die Geschwindigkeit der Verbindungen erhöht wird, da einmal aufgerufene Informationen auf dem Proxy-Server „eingelagert" werden und dann schneller wieder abgerufen werden können.[18]
Alle diese Möglichkeiten haben dabei ihrerseits Vor-und Nachteile, die es abzuschätzen gilt. So bietet keine Methode einem Staat absolute Sicherheit, alle Informationen zu blockieren und Vergehen gegen die Gesetze zu verhindern. Sowohl Hare als auch Murdoch und Anderson heben jedoch den Symbolcharakter solcher Maßnahmen hervor. Staaten setzten hierdurch ein Zeichen, dass sie bereit sind, ihre Souveränität zu verteidigen. Die Existenz von nationalstaatlichen Grenzen sehen Letztere dabei bereits heute, wobei sie lediglich anmerken, dass die Effektivität dieser sich unterscheidet und Staaten oft technischen Neuerungen hinterherhinken, was es ihnen schwierig macht, ein hohes Maß an Sicherheit zu erlangen.[19] So ist auch die „Große Firewall" in China durchaus imstande, viele chinesische Staatsbürger davon abzuhalten, freien Zugang zu allen Informationen zu erlangen und somit die rechtlichen Grenzen Chinas auch im Cyberspace zu bestärken. Doch sollte im Kopf behalten werden,

[13] Murdoch und Anderson stellen einige weitere Methoden vor, auf die aber an dieser Stelle nicht weiter eingegangen werden wird. Für mehr Informationen hierzu siehe: Murdoch Steven J., Anderson Ross, Tools and Technology of Internet Filtering, in: Acess Denied, 2006, S. 57-72.
[14] Murdoch,/Anderson, Internet Filtering, 2006, S. 59-60.
[15] Hare, Borders in Cyberspace, 2010, S. 8.
[16] Ein Proxy-Server ist eine Komponente, die es erlaubt, eingehende Verbindungen weiterzuleiten, dabei jedoch den wirklichen Absender zu verschleiern, gleichzeitig aber auch die Weiterleitung selbst zu beeinflussen.
[17] Murdoch,/Anderson, Internet Filterting, 2006, S. 61-63.
[18] Ebd., S. 62.
[19] Ebd., S. 71.

dass auch diese Barriere – wenn auch nur durch einen kleinen Teil von IT-Spezialisten – umgangen werden kann.[20]
Ein gutes Anschauungsobjekt, wie staatliche Grenzziehung bereits heute realisiert wird, bietet der russische Cyberspace RUNET, mit welchem sich Deibert und Rohonzinski im Jahre 2010 in einer Studie näher beschäftigt haben.[21] Sie stellten fest, dass Russland und im allgemeinen Staaten der GUS (Gemeinschaft Unabhängiger Staaten), im Gegensatz zu China, nicht auf eine immer vorhandene physische Grenze setzen, sondern sich darauf konzentrieren, legislative und technische Voraussetzungen zu schaffen, um den Abruf von Informationen „on time“ zu unterbinden sowie Staatskontrolle im nationalen Cyberspace durch gezielte Desinformation zu gewährleisten.[22] So werden in Ländern des RUNET Seitenbetreiber rechtlich dazu bewegt, sich registrieren zu lassen und damit verpflichtet, Regeln für den Inhalt der Seiten einzuhalten. Außerdem wird der Aspekt der Sicherheit des Staates als vordergründige Legitimation angeführt, um kurzzeitig Informationen zu blockieren, z.B. Georgien-Russland Krieg 2008.[23] Des Weiteren versucht u.a. Russland eine Nationalisierung zu erreichen, indem manbeispielsweise Internet an die Schulen bringt, hierbei jedoch darauf achtet, dass lediglich russische Webseiten darüber zu erreichen sind. Dieser Punkt ist besonders interessant, weil sich die räumliche Begrenzung auf in Russland ansässige Seiten für die ISPs als Vorteil herausstellt, da hierdurch weniger Kosten entstehen. Kostentechnisch bildet dies auch einen Vorteil gegenüber der Kontrolle auf physischer Ebene wie in China, bei der durch die massenhafte Zensur ungewollt auch Seiten blockiert werden, die nützlich wären.[24]

4. Staatliche und nichtstaatliche Akteure

Im letzten Abschnitt der Arbeit wird die Frage erörtert, welche Rolle einzelne Staaten bei der Regulierung des Internets und der Errichtung von Grenzen spielen. Diese Frage mag bei der Frage nach der Errichtung von nationalen Grenzen verwundern, doch ist in einer Zeit, in dem Nationalstaaten Teile – wenn auch nur bedingt und in geringem Umfang – ihrer souveränen Rechte an internationale Organisationen wie die EU, NATO oder UN abgeben, wichtig zu untersuchen, inwiefern hiervon Regulierungsmaßnahmen ausgehen und Staaten versuchen, hier ihren Einfluss geltend zu machen. Gerade bei dem Medium Internet, das eben durch seinen internationalen Charakter besticht, gewinnt dieser Punkt an Bedeutung.
Der Aspekt, dass einzelne Staaten ihre eigenen Interessen in überstaatlichen Organisationen zur Regulierung des Internets durchzusetzen suchen, finden seit wenigen Jahren wieder vermehrt Betrachtung. Ross LaJeunesse kritisierte beispielsweise die Sitzungen der International Telecommunication Union (ITU) als absolut undurchsichtig und bemängelt weiter: “You have a number of governments who simply don´t like the way the internet is run

[20] Etwa 1% der 500.000.000 Internetnutzer in China haben die Möglichkeit hierzu. Hill, Internet Fragmentation, 2012, S. 31.
[21] Deibert Ron, Rohonzinski Rafal, Control and Subversion in Russian Cyberspace, 2010, in: Access Controlled, 2008, S. 15-26.
[22] Deibert und Rohonzinski bezeichnen die drei Möglichkeiten der Kontrolle als *First-Generation* (auf physischer Ebene) sowie *Second-* und *Third-Generation-Control.* Deibert/Rohonzinski, Russian Cyberspace, 2010, S. 16-17.
[23] Deibert/Rohonzinski, Russian Cybersoace, 2010, S. 27-28.
[24] Ebd., S. 27-30.

today."[25] Diese Kritik zieht sich fast durch die gesamte Diskussion und gibt bereits einen Hinweis auf die Einflussnahme von Staaten auf den Regulierungsverlauf. Tatsächlich hinterließ die ITU Sitzung 2012 starke Sorgen, nachdem die „westlichen Regierungen" im Verlauf der Konferenz überstimmt worden waren.[26] Grund hierfür ist, dass insbesondere Länder wie China, Russland, Brasilien und Indien sich dadurch benachteiligt sehen, dass die Vergabe von Domain-Namen hauptsächlich durch die Internet Corporation for Assigned Names and Numbers (ICANN) durchgeführt wird, die ihrerseits maßgeblich durch die USA beeinflusst wird.[27]

Doch sind auch die BRICS- Staaten[28], aus deren Reihen ein großer Teil der Kritik kommt, sich nicht einig, welche Alternativen eingeschlagen werden sollen. Ebert und Maurer weisen darauf hin, dass die unterschiedlichen Vorstellungen innerhalb der BRICS auf die verschiedenen politischen Situationen beziehungsweise Regierungsarten der Mitgliedsländer zurückzuführen sind.[29] Dieser Punkt weist auf die große Bedeutung von Nationalstaaten, auf welche die Autoren pochen, hin. Auch Daniel W. Drezner kommt in seinen Untersuchungen zu dem Schluss, dass Nationalstaaten zwar Rechte abgeben, dies teilweise sogar an private Akteure, die Ergebnisse dabei jedoch weiterhin zu ihren Gunsten beeinflussen.[30]

Festzustellen ist allerdings, dass Staaten sich zusehends an supranationale Organisationen wenden, um eine internationale legislative Grundlage und gemeinschaftliche Handlungsweisen abzustimmen, wie im Cyberspace sicherheitspolitisch zu agieren ist. Als Beispiel hierfür ist die Europäische Kommission zur Bekämpfung von Cyberkriminalität oder die Einrichtung eines INTERPOL-Büros für die Verfolgung von Cyberkriminalität zu nennen. Joseph Nye misst diesen Schritten sehr große Bedeutung zu, sagt aber auch voraus, dass Staaten trotzdem eine dominierende Rolle spielen werden.[31] Drezner betont, dass Staaten, insbesondere einflussreiche „Global-Player", sich lediglich an solche Organisationen wenden, wenn sie hierdurch ihren Willen und ihre Ziele einfacher und effektiver realisierbar sehen.[32] Tatsächlich ist Realisierbarkeit von Zielen, besonders im Cyberspace, an eine breite Zustimmung im internationalen Bereich gekoppelt. Nationalstaatliche Regulierungen, die die Gesetze eines Landes im Internet durchzusetzen suchen, können nur schwer realisiert werden, wenn andere Staaten diese Versuche unterwandern, indem sie beispielsweise Server mit im Land A verbotenem Inhalt auf eigenem Territorium dulden.

Um einen wichtigen Vorteil des Internets, nämlich die Konnektivität zum Rest der Welt, zu erhalten und Staaten trotzdem die Möglichkeit zu geben, ihre souveränen Rechte auch auf den Cyberspace auszubreiten, bieten internationale Organisationen, in die bei Bedarf auch private

[25] Chander Anupham, Challenges and Approaches to Effective Cyberspace Governance in a Multipolar World, in: American Society of International Law, Vol. 107, 2013, S. 97.

[26] Auf der Konferenz wurde darüber beraten, inwieweit die ITU als Organisation Einfluss auf die Entwicklung des Internets nehmen sollte. Siehe: Nye Joseph S., The Regime Complex for managing Global Cyber Activities, in: Global Commission on Internet Governance, 1, 2014, S. 5.

[27] Tatsächlich wirkt sich die historische Bedeutung der USA in der frühen Entwicklung des Internets noch heute aus. Siehe: Ebert Hannes, Maurer Tim, Contested Cyberspace and Rising Powers, in: Third World Quarterly, 34 (6), 2013, S. 1057.

[28] BRICS = Brasilien, Russland, Indien, China und Südafrika.

[29] Ebert und Maurer verweisen hierbei auf den Freedom House Index, der China und Russland als „nicht frei" und zudem nicht als „gewählte Demokratie" einstufen, was die anderen drei Staaten Brasilien, Indien und Südafrika hiernach sind. Siehe: Ebert/Maurer, Rising Powers, 2013, S. 1061.

[30] Drezner,, Bringing the State Back In, 2004, S. 498.

[31] Nye, Regime Complex, 2014, S. 6 sowie 12-13.

[32] Drezner, Bringing the State back In, 2004, S. 482-484.

Akteure mit eingebunden werden können, jedoch eine vielversprechende Möglichkeit. Nur wenn staatliche Grenzen im Internet – zumindest aus rechtlicher Sicht – eine breite Zustimmung und damit Akzeptanz im internationalen Bereich erhalten, sind diese sinnvoll und realisierbar.

5. Schlussfolgerungen

Staaten sehen sich und ihr Sicherheitsbedürfnis durch den Cyberspace in Gefahr. Die vielseitigen Möglichkeiten für praktisch jedermann, der ausreichend Hackerkenntnisse besitzt, dem Staat teils empfindliche Schläge zu versetzen, veranlasst jenen, das Konzept nationalstaatlicher Grenzen auf das Medium Internet zu übertragen. Nicht zuletzt durch die Offenlegung der Spionageaktionen der USA gegen ihre Verbündeten, hat hier eine neue Debatte um die Fragmentierung des Cyberspace wieder neue Nahrung bekommen. Besonders der Fakt, dass man sich selbst gegen verbündete Staaten absichern muss, verschärft die Situation zusehends.
Doch stellt eine Fragmentierung den Nationalstaat vor das Problem, wie diese effektiv realisiert werden kann, ohne die Freiheit, besonders der Wirtschaft, zu sehr zu beeinträchtigen. Die Lösung, physisch einen neuen „Sub-Cyberspace“ zu erstellen, der dadurch, dass er keinen beziehungsweise nur wenige gut überwachte Zugänge zum weltweiten Internet besitzt, Sicherheit bringt, halte ich für ausgeschlossen. Die hieraus entstehende wirtschaftliche und kommunikative Abgrenzung zu möglichen Handels- und Vertragspartnern, wäre besonders für kleinere Staaten kaum mit dem sicherheitspolitischen Vorteil aufzuwiegen. Auch bringt diese Möglichkeit keine hundertprozentige Sicherheit vor Angriffen.[33] Staaten befinden sich hier in einer Zwickmühle, da sehr klein abgegrenzte Räume mit weniger Kommunikation besser zu kontrollieren sind, aber auch mehr wirtschaftliche Kosten verursachen, während große – wirtschaftliche – Räume, wie beispielsweise die EU, nur noch schwer zu kontrollieren sein werden.
Eine staatliche Unterteilung des Internets wird sich in Zukunft mehr auf einer sozialen und informellen Ebene bewegen, bei der der Staat sich darauf konzentriert, bestimmte Inhalte „on-time“ nicht zugänglich zu machen, wenn sich eine Gefahr anbahnt. Hierzu werden neue legislative Grundlagen geschaffen werden, die dem Nationalstaat die rechtliche Möglichkeit hierzu geben. Das Statement, dass der Staat etwas gegen Angriffe und für seine Souveränität unternimmt, ist hierbei bereits ein wichtiger Schritt. Auch wird mehr in technologische Entwicklung investiert werden, um mit Angreifern auf Augenhöhe zu sein und so vielleicht eine abschreckende Wirkung aufzubauen. Diese Abschreckung bedarf jedoch, um wirksam zu sein, einer breiteren Zustimmung durch andere Staaten und die Möglichkeit, Verbrechen im Cyberspace weltweit zu verfolgen. Die Einrichtung einer INTEPOL-Einheit ist hier ein erster Schritt.
Um eine breitere Zustimmung auf internationaler Ebene zu erlangen, halte ich es für notwendig, dass sich Staaten in internationalen Organisationen – auch mit privaten Akteuren – zusammenfinden und eine gemeinsame Linie beschließen. Staaten können hierdurch rechtliche Grenzen im Cyberspace um ihr Territorium errichten, welche dann von anderen

[33] Auch die Volksrepublik China, die eine ähnliche Lösung durch die Große Firewall realisieren will, wird Opfer von ausländischen und inländischen Hackerangriffen.

Staaten respektiert und eingehalten werden. Gegen breit angelegte Angriffe von anderen staatlichen Akteuren wird dies jedoch zumindest in naher Zukunft keinen Schutz darstellen. Doch sollte hierbei bedacht werden, dass dies auch in der physischen Welt nicht der Fall ist. So können militärisch stärkere Staaten schwächere noch immer angreifen. Lediglich die Entscheidung, wer hierfür die Schuld trägt und juristisch zur Verantwortung gezogen werden muss, fällt dabei leichter.

Eine solche internationale Übereinstimmung hat es etwa bereits bei dem Schutz von Kindern vor Arbeitsausbeutung gegeben, der auf breite Zustimmung und somit auf breite Unterstützung trifft. Gleiches könnte sich auf andere Bereiche im Cyberspace ausbreiten. Eine Ordnung im Cyberspace – zumindest in manchen Bereichen – ist durchaus notwendig und darf nicht a priori mit dem Argument der Zensur vom Tisch gefegt werden. Nur wenn dem Sicherheitsbedürfnis von Staaten Rechnung getragen wird, wird das Internet global bestehen bleiben können.

Literaturempfehlung

Als weiterführende Literatur zum Thema „Fragmentierung und Zensur des Internets“ sind die drei Bücher „Acess Denied“, „Acess“ Controlled“ und „Acess Contested“ der OpenNet Initiative sehr zu empfehlen. Hierin wird in einzelnen Kapiteln Grundlegendes sowie spezielle Themen angesprochen und erläutert.
Zudem ist die Arbeit „Can Sovereigny Adapt to the Challanges of Cyber Security?“ von Forrest Hare aus dem Jahr 2010 zu empfehlen, in welcher ein sehr guter Überblick zur theoretischen wie praktischen Umsetzung von Staatsgrenzen im Cyberspace gegeben wird. Auch die sehr detaillierte Untersuchung Jonah F. Hills „Internet Fragmentation, Highlighting the Major Technical, Governance and Diplomatic Challanges for U.S. Policy Makers“ ist für eine genauere Untersuchung der technischen Möglichkeiten der Internetfragmentierung sehr lesenswert.

Literaturverzeichnis

[1] Anupham Chander, Challenges and Approaches to Effective Cyberspace Governance in a Multipolar World, in: American Society of International Law, Vol. 107, 2013, S. 95-110.

[2] Ron Deibert, Rafal Rohonzinski, Control and Subversion in Russian Cyberspace, 2010, in: Access Controlled, 2008, S. 15-34.

[3] Chris Demchack, Peter Dombrowski, Rise of a Cybered Westphalian Age, in: Strategic Studies Quarterly 5, No.1, 2011, S. 32-61.

[4] Daniel Drezner, The Global Governeance: Bringing the State Back In, in: Political Science Quarterly, Vol. 119, Issue 3, 2004, S. 477-498.

[5] Hannes Ebert, Tim Maurer, Contested Cyberspace and Rising Powers, in: Third World Quarterly, 34 (6), 2013.

[6] Paul Fehlinger, Cyberspace fragmentation: an internet governance debate beyond infrastructure, Internet Policy Review, 17.04.2014, http://policyreview.info/articles/news/cyberspace-fragmentation-internet-governance-debate-beyond-infrastructure/266 [zuletzt abgerufen: 13.08.2014].

[7] Alexander Halavais, Border on the World Wide Web, in: New Media and Society, Vol. 2 (1), 2000.

[8] Forrest Hare, Can Sovereigny Adapt to the Cahllanges of Cyber Security?, 2010, http://www.ccdcoe.org/publications/virtualbattlefield/06_HARE_Borders%20in%20Cyberspace.pdf [zuletzt abgerufen: 13.08.2014].

[9] Jonah F. Hill, Internet Fargmentation, Highlighting the Major Technical, Governance and Diplomatic Challanges for U.S. Policy Makers, John F. Kennedy School of Government, Harvard University, 2012.

[10] David R.Johnson, David Post, Law and Broder:The rise of Law in Cyberspace, Stanford

Law Review, 48 (5), 1996, S. 1367-1402.

[11] Steven J. Murdoch, Ross Anderson, Tools and Technology of Internet Filtering, in: Acess Denied, 2006, S. 57-72.

[12] Joseph S. Nye, The Regime Complex for managing Global Cyber Activities, in: Global Commission on Internet Governance 1, 2014.

[13] TeleGeography, Global Internet Geography, Executive Summary 2013, http://www.telegeography.com/research-services/global-internet-geography/ [zuletzt abgerufen: 13.08.2014].

[14] Allan Weinberg, James Kaplan, Tucker Bailey , The $3,000bn threat from cyber attacks, Financial Times, 28.01.2014, http://www.ft.com/cms/s/0/1c4115e8-885a-11e3-85a2-00144feab7de.html#axzz3AGpdEYEX [zuletzt abgerufen: 13.08.2014].