

Internet Governance – die Kontroverse des WSIS

Eine globale Ressource im Spannungsfeld nationaler Interessen

Wolfgang Kleinwächter

Beinahe wäre der Weltgipfel zur Informationsgesellschaft 2003 an der Kontroverse gescheitert, wer in Zukunft die Kernressourcen des Internets verwalten soll: weiterhin die unter amerikanischem Recht stehende private ICANN oder eine neue, von der UNO beauftragte Organisation wie die ITU? Vor allem stellte sich dabei die Frage, welche Aspekte der Internetkommunikation rein technischer Art sind und welche politische Kernbereiche betreffen. Zur Klärung wurde von UNO-Generalsekretär Kofi Annan eine Arbeitsgruppe ins Leben gerufen, die den Begriff "Internet Governance" definieren und Modelle für die künftige Administration des Internets ausarbeiten soll. Zum Bericht der "Working Group on Internet Governance" (WGIG).

Der erste Weltgipfel zur Informationsgesellschaft (WSIS I) wäre im Dezember 2003 in Genf um Haaresbreite an dem konflikträchtigen Thema "Internet Governance" gescheitert. Während auf der einen Seite die US-Regierung, weitgehend unterstützt durch die Europäische Union, Kanada, Australien und Japan, davon ausging, dass sich für das Management des Internets das Prinzip der "Private Sector Leadership" bewährt habe und die Kernressourcen des Internets auch zukünftig von der in Kalifornien angesiedelten privaten "Internet Corporation for Assigned Names and Numbers" (ICANN) verwaltet werden sollten, forderten China, Indien, Brasilien und Südafrika, unterstützt von der Mehrheit der Entwicklungsländer, dass die Regierungen eine führende Rolle spielen müssten und das Internet zukünftig von einer UN-Organisation, vorrangig von der in Genf angesiedelten "International Telecommunication Union" (ITU), beaufsichtigt werden sollte (vgl. Kleinwächter 2004).

Ein Kompromiss schien nicht möglich, noch zumal die streitenden Parteien weitgehend aneinander vorbeiredeten, da sie unter dem Thema "Internet Governance" Unterschiedliches verstanden. Während die einen damit vorrangig das technische Management der Internet-Kernressourcen – Root-Server, IP-Adressen und Domain-Namen – meinten, verbanden die anderen mit dem Thema auch alle Internet-Anwendungen und damit verbundenen Probleme – von eCommerce bis zu eGovernment, von Spam bis zu Cybercrime. Die Unklarheiten vergrößerten sich noch dadurch, dass es in der Tat schwierig ist, eine eindeutige Grenzlinie zwischen technischen und politischen Aspekten im Zusammenhang mit dem Internet zu ziehen.

Im Cyberspace ist "Code the Law"

Das problemlose Funktionieren der technischen Internet-Infrastruktur ist eine Voraussetzung für dessen wirtschaftliche Nutzung. Das technische Management von Internet "Root Zone Files" und Servern, von Protokollen, IP-Adressen und Domain-Namen hat wirtschaftliche und politische Implikationen. Die "Root Zone Files" von nationalen Länderkennungen (ccTLDs) werden in einer globalen Datenbank von ICANN verwaltet, einer privaten Gesellschaft unter kalifornischem Recht, über die die US-Regierung die Oberhoheit hat. Der Kampf gegen die wachsende globale Kriminalität im Cyberspace ist ohne Zugang zu Servern und IP-Adressen wirkungslos. Die Musik-, Film- und Spiele-Industrie setzt bei ihren Anstrengungen, illegales Downloaden von geistigem Eigentum

zu verhindern, wesentlich auf technische Mittel bzw. auf die Kontrolle von IP-Adressen und Servern. Das "Domain Name System" (DNS) gilt als das "Territorium des Cyberspace". Was in der realen Welt ein Stück Land ist, ist in der virtuellen Welt eine Domain. Ohne Grund und Boden kann man in der realen Welt keine Fabrik aufbauen, ohne einen Domain-Namen gibt es kein eBusiness. Google, Yahoo, Amazon und eBay haben ihre Imperien zunächst auf nichts anderem als einem Domain-Namen aufgebaut.

Insofern ist es nicht verwunderlich, dass technische Protokolle, Standards und Verfahren zunehmend ins Blickfeld der Politik geraten, schaffen und definieren diese Parameter doch häufig diejenigen neuen virtuellen Räume, in denen sich die Internet Nutzer bewegen. Diese Räume kennen die Grenzen von Zeit und Raum nicht. Dies ist zwangsläufig eine Herausforderung für die allgemeine nationale Rechtsordnung, die sich jeweils auf ein konkret definiertes reales Territorium bezieht. Zwar gilt grundsätzlich, dass der Cyberspace kein rechtsfreier Raum ist, dass der Staatsbürger (citizen), wenn er im Cyberspace zum Netzbürger (netizen) wird, nicht der nationalen Rechtsordnung entflieht und dass das, was offline illegal ist, auch online als rechtswidrig gilt. Aber bereits bei unterschiedlichen nationalen Regelungen für einzelne Sachbereiche – z.B. bei der Definition von strafbaren Informationsinhalten – wird das objektive Dilemma sichtbar. "In real space we recognize how laws regulate – through constitutions, statutes and other legal codes. In cyberspace we must understand how code regulates – how the software and hardware that make cyberspace what it is regulate cyberspace as it is", schrieb Lawrence Lessig bereits 1999 in "Code and other Laws of Cyberspace" (S. 6).

Working Group on Internet Governance (WGIG)

Der Kompromiss, der im Dezember 2003 letztendlich doch noch gefunden wurde, bestand darin, UN-Generalsekretär Kofi Annan zu bitten, eine Arbeitsgruppe zu bilden, die bis zum 2. Weltgipfel zur Informationsgesellschaft im November 2005 in Tunis mehr Klarheit in das kontroverse Thema bringen sollte. Die "Working Group on Internet Governance" (WGIG) erhielt das Mandat: a) eine Arbeitsdefinition für "Internet Governance" vorzulegen, b) jene Themen zu identifizieren, die im Zusammenhang mit dem Management des Internets eine politische Komponente haben und c) die Rolle und Verantwortlichkeiten der an "Internet Governance" beteiligten "Stakeholder", also der Regierungen, der Privatwirtschaft und der Zivilgesellschaft, zu klären. Zusätzlich sollte die WGIG dort, wo es ihr sinnvoll erschien, Vorschläge erarbeiten, wie aktuelle oder potentielle Probleme gelöst werden könnten. Nach Artikel 48 der "WSIS Declaration of Principles" sollte die WGIG unter voller Einbeziehung aller Stakeholder arbeiten.

Als Kofi Annan im November 2004 die 40 Mitglieder der WGIG berief, hielt er sich strikt an diese Vorgabe: Je ein Drittel der Experten kam von Regierungen, von der Privatwirtschaft und der Zivilgesellschaft. Den Vorsitz dieser Multistakeholder-Gruppe übernahm Kofi Annans Special Adviser, der Inder Nitin Desai. Nach neun Monaten, in denen die Mitglieder der WGIG rund 10'000 E-Mails austauschten und sich viermal zu offenen und geschlossenen Sitzungen trafen, legte die WGIG am 18. Juli 2005 in Genf ihren Abschlussbericht vor. Dieser 16-seitige Bericht, der durch einen umfangreichen "Background Report" ergänzt wird, folgt in seiner Struktur dem erteilten Mandat.

Die von der WGIG vorgelegte Arbeitsdefinition für "Internet Governance" basiert auf einem breiten Ansatz:

"Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."
(WGIG Final Report 2005)

Mit dieser Definition macht die WGIG klar, dass Internet Governance mehr ist als das Management der Internet-Kernressourcen und nicht in die alleinige Zuständigkeit von Regierungen fällt. Diese breite Definition wird differenziert und strukturiert durch vier Cluster, in die sich die einzelnen Sachthemen einordnen lassen:

a) Issues relating to infrastructure and the management of critical Internet resources, including administration of the domain name system and Internet protocol addresses (IP addresses), administration of the root server system, technical standards, peering and interconnection, telecommunications infrastructure, including innovative and convergent technologies, as well as multilingualization. These issues are matters of direct relevance to Internet governance and fall within the ambit of existing organizations with responsibility for these matters;

b) Issues relating to the use of the Internet, including spam, network security and cybercrime. While these issues are directly related to Internet governance, the nature of global cooperation required is not well defined;

c) Issues that are relevant to the Internet but have an impact much wider than the Internet and for which existing organizations are responsible, such as intellectual property rights (IPRs) or international trade. The WGIG started examining the extent to which these matters are being handled consistent with the Declaration of Principles;

d) Issues relating to the developmental aspects of Internet governance, in particular capacity-building in developing countries.

(WGIG Final Report 2005)

Basierend auf dieser Clusterbildung hat die WGIG folgende sechzehn prioritären Themen identifiziert:

1. Administration of the root zone files and system
2. Interconnection costs
3. Internet stability, security and cybercrime
4. Spam
5. Meaningful participation in global policy development
6. Capacity-building
7. Allocation of domain names
8. IP addressing
9. Intellectual property rights (IPR)
10. Freedom of expression
11. Data protection and privacy rights
12. Consumer rights
13. Multilingualism
14. Convergence
15. Next Generation Networks
16. eCommerce

Schliesslich präzisiert die WGIG die spezifische Rolle und die Verantwortlichkeiten der beteiligten Stakeholder. Dabei sind die Mitglieder der WGIG einheitlich zu der Erkenntnis gelangt, dass das Internet nicht durch eine einzige Organisation oder eine einzige Gruppe von "Stakeholdern" gemanagt werden kann, sondern ein konstruktives Zusammenwirken von unterschiedlichen Akteuren auf unterschiedlichen Ebenen erfordert. Nur durch ein solches Miteinander sei Funktionsfähigkeit, Stabilität und Sicherheit des

Internets zu gewährleisten und nur so könne eine Weiterentwicklung des Internets garantiert werden.

In einem solchen "Multilayer Multiplayer Mechanismus" ist Platz sowohl für zwischenstaatliche Organisationen wie ITU, WTO, WIPO und OECD als auch für private und zivilgesellschaftliche Organisationen wie ICANN, IETF, ISOC, IAB, W3C, RIRs, CPSR, CDT, EFF, APC, Article 19, WPCF, etc. Was notwendig ist, ist eine verbesserte Kommunikation, Koordination und Kooperation zwischen allen Betroffenen und Beteiligten. Wenn das Internet ein "Netz von Netzwerken" ist, dann ist Internet Governance ein "Mechanismus von Mechanismen". Was die WGIG vorschlägt, ist mithin ein Internet-Governance-Modell, dessen Struktur weitgehend die Netzwerkstruktur des Internets widerspiegelt.

WGIG plädiert daher für ein neues, innovatives und kreatives Miteinander von Regierungen, Privatwirtschaft und Zivilgesellschaft, wobei die Frage der "führenden Rolle" aus der Sicht der WGIG eher sekundär ist und nicht per se entschieden werden kann, sondern sich aus dem jeweiligen konkreten Sachverhalt ergeben sollte. So ist es z.B. nahe liegend, dass beim technischen Management der Internet-Kernressourcen der private Sektor – von den Technikern und Entwicklern bis zu den Dienste-Anbietern und Nutzern – eine führende Rolle behalten sollte, wobei Regierungen – z.B. über ICANN's "Governmental Advisory Committee" (GAC) – einen Mitsprachekanal haben, um auf die politischen Aspekte technischer Entscheidungen aufmerksam machen zu können. Auf der anderen Seite scheint klar, dass bei der Strafverfolgung im Internet die Regierungen zuerst gefragt sind. Aber auch hier erweist sich ein Zusammenwirken mit der Privatwirtschaft und der Zivilgesellschaft nicht nur als nützlich, sondern in einzelnen Fällen auch als unabdingbar.

Jedes einzelne Thema der "Top 16 Liste" der WGIG benötigt also einen spezifischen, dem Sachverhalt angepassten, triangularen Governance Mechanismus, wobei die konkrete Ausgestaltung des jeweiligen Dreiecks eben von den spezifischen Anforderungen und den vorhandenen Kompetenzen abhängig ist. Wesentlich ist bei diesem multiplen Trilateralismus, dass Politikentwicklung "von unten" (bottom up) erfolgt unter Einbeziehung aller Betroffenen und Beteiligten und dass dies in einer offenen Umgebung und auf der Basis transparenter Prozeduren stattfindet.

Indem der WGIG-Report die spezifischen Rollen und Verantwortlichkeiten der einzelnen Stakeholder präzisiert, eröffnet er die Möglichkeit, neue Formen des Zusammenwirkens zwischen gouvernementalen und nicht-gouvernementalen Akteuren zu erkunden und zu praktizieren. Der Bericht macht jedoch auch klar, dass es, zumindest auf globaler Ebene, kein Zurück mehr gibt zur alleinigen Regierungszuständigkeit für das Internet. Die Option der Gründung einer "Internet-UNO" wird von der WGIG als nicht den neuen globalen Realitäten entsprechend verworfen. Zu dem in Artikel 1 der WSIS-Deklaration vom 13. Dezember 2003 verankerten Prinzip des "Multistakeholderismus" gäbe es keine funktionsfähige Alternative. Regierungen müssten ihrer Verantwortung dergestalt gerecht werden, dass sie lernen, enger mit Stakeholdern aus der Privatwirtschaft und der Zivilgesellschaft zusammenzuarbeiten und Verantwortung und Souveränitätsrechte zu teilen. In der letzten Konsequenz bedeutet der WGIG-Vorschlag, die intergouvernementale Diplomatie des 19. und 20. Jahrhunderts, die nicht selten auch eine Art von Geheimdiplomatie war, zu ergänzen durch eine neue, offene Multistakeholder-Diplomatie für jene globalen Probleme des 21. Jahrhunderts, die mit dem Internet und der Informationsgesellschaft heraufziehen.

Souveränitätsteilung im Cyberspace?

Nicht unwesentlich wird diese Herausforderung an das gegenwärtig noch dominierende System der zwischenstaatlichen Beziehungen dadurch bedingt, dass der Cyberspace die Grenzen von Zeit und Raum nicht mehr kennt, kein physisches Territorium repräsentiert und die virtuellen Ressourcen des Informationszeitalters, also primär IP-Adressen und Domain-Namen, eine andere Qualität aufweisen als die natürlichen Ressourcen des Industriezeitalters wie Öl oder Gold.

Das seit dem Westfälischen Frieden von 1648 funktionierende System der internationalen Beziehungen basiert auf dem Nationalstaatsgedanken. Die Regierung, die für das in den Grenzen eines Landes lebende Volk agiert, besitzt die volle Souveränität, die sich primär aus der Territorial- und Personalhoheit zusammensetzt. Gesetze gelten jeweils für das entsprechende Land und dessen Staatsbürger. Ihre Gültigkeit endet an den Landesgrenzen. Grenzüberschreitende Probleme werden in Form von bilateralen Verträgen mit anderen Regierungen geregelt, die dann durch die jeweiligen Parlamente zu ratifizieren sind. Der grenzüberschreitende Verkehr von Personen, Waren und Dienstleistungen unterliegt der Kontrolle der jeweiligen Regierung.

Die Informationsrevolution hat dieses in der UN-Charta verankerte Souveränitätsprinzip nicht aufgehoben, es aber in einen anderen Kontext gestellt. Das Internet kennt keine nationalen Grenzen. Die Kontrolle grenzüberschreitender Kommunikation über das Internet – und das betrifft nicht nur die individuelle Kommunikation von einzelnen Nutzern, sondern auch den kommerziellen Austausch von digitalisierten Produkten und Dienstleistungen, – wird immer komplizierter. Im Internet ist praktisch jedermann "just one click away". Der Cyberspace ist keine "law free zone". Aber die Durchsetzung von Rechtsansprüchen in konkreten Einzelfällen wird immer schwieriger, zumal wenn es sich um Transaktionen mit Beteiligten aus verschiedenen Jurisdiktionen mit möglicherweise differierenden Gesetzen handelt.

Der Zwang, nationale Regulierungsansätze durch globale Strategien und weltweit einheitliches Handeln auf der Basis einer internationalen Rechtsordnung zu ersetzen, führt in der Konsequenz zu der Notwendigkeit, dass Regierungen stärker anfangen müssen, in den Kategorien einer gemeinsamen globalen Verantwortung und einer geteilten Souveränität zu denken. Dies wird nicht unwesentlich mitbedingt durch den oben bereits erwähnten Qualitätsunterschied zwischen den Ressourcen des Industrie- und des Informationszeitalters.

Die Schlüsselressourcen des Industriezeitalters – Rohstoffe, Energie, aber auch Satellitenpositionen auf dem geostationären Orbit oder das Frequenzspektrum – sind durchweg so genannte begrenzte Ressourcen. Um einen gleichberechtigten Zugang und eine faire Verteilung dieser Ressourcen zu gewährleisten, ist ein vorrangig staatlich reguliertes Ressourcenmanagement, auch auf internationaler Ebene, notwendig.

Die Kernressourcen des Internets sind jedoch im Prinzip unbegrenzt. Selbst wenn es richtig ist, dass es im mathematischen Sinne eine endliche Zahl von IP-Adressen gibt, so ist das eine mehr theoretische denn praktische Begrenzung. Zwar gibt es in der Tat nur etwa vier Milliarden IPv4-Adressen, aber das bereits Mitte der 90er-Jahre entwickelte IPv6-Protokoll ermöglicht die Zuordnung von mehreren Millionen IP-Adressen an jeden der sechs Milliarden Bewohner unseres Planeten. Das gleiche gilt für die unbegrenzt verfügbaren Domain-Namen. Selbst die Zahl der "Top Level Domains" (TLDs)

– im Moment gibt es 243 "country code TLDs" (ccTLDs) und knapp 20 "generic TLDs" (gTLDs) – kann endlos erhöht werden. Wenn die Server von DENIC mehr als neun Millionen Dateien von .de Namen verwalten können, die VeriSign-Server sogar mehr als 30 Millionen in der .com Domain, dann können die Root-Server, die die "TLD Zone Files" verwalten, mindestens einige zehntausend TLDs problemlos managen. Wenn es einen Namens-Engpass geben sollte, schafft man einfach eine neue Domain, wobei Sinnhaftigkeit und Wirtschaftlichkeit solcher neuen TLDs auf einem anderen Blatt stehen.

Genau diese problemlose Möglichkeit der Ressourcenvermehrung macht den wesentlichen Unterschied zwischen den Ressourcen des Industrie- und des Informationszeitalters aus. Man kann zwar die Hälfte der Weltreserven an Erdöl kontrollieren, aber nicht die Hälfte der Domain-Namen. Dies hat weit reichende Konsequenzen für das Ressourcenmanagement. Während es bei den begrenzten Ressourcen darum geht, eine gerechte Verteilung zu gewährleisten, und die Kontrolle über diese Ressourcen Machtpositionen konstituiert, geht es bei den unbegrenzten Ressourcen vorrangig darum, den ungehinderten Zugang zu ihnen zu gewährleisten. Und die Kontrolle über diese unbegrenzten Ressourcen (die ohnehin kaum möglich ist) konstituiert keine Machtposition im traditionellen Sinn.

Insofern ist Ressourcenmanagement und Kontrolle im Cyberspace weit weniger mit realer Machtausübung verbunden als z.B. die Kontrolle über Erdölreserven. Dazu kommt der Fakt, dass die natürlichen Ressourcen geographisch lokalisierbar sind. Erdöl liegt nun mal im Persischen Golf, in der Nordsee oder in Sibirien. Eine solche lokale Verortung aber ist für die virtuellen Ressourcen des Cyberspace nicht möglich. Die TLD von Tuvalu (.tv) wird von den USA aus gemanagt, und die Registranten sind mehrheitlich nicht Bewohner dieser kleinen pazifischen Insel. Damit verändert sich zwangsläufig die Exekutionsfähigkeit traditioneller Souveränitätsrechte durch nationale Regierungen.

Es verändert sich aber auch das bisherige landläufige Verständnis, dass Ressourcenkontrolle politische und wirtschaftliche Macht konstituiert. Man kann vielleicht Eigentumsrechte an einem einzelnen Domain-Namen reklamieren, man kann auch lukrative und wirtschaftliche Domain-Namen horten und mit ihnen spekulieren, aber man kann die virtuellen Ressourcen nicht als solche im klassischen Sinne besitzen. Insofern sind die Internet-Kernressourcen eher mit der uns umgebenden Luft vergleichbar. Sie muss sauber und verfügbar sein, damit das Leben funktioniert. IP-Adressen und Domain-Namen müssen problemlos zugänglich sein, damit das virtuelle Leben im Internet, von E-Mail über eGovernment bis eCommerce, funktioniert.

Streitpunkt "Oversight"

Die potentielle Ubiquität der Internet-Kernressourcen bedarf dennoch eines professionellen Managements. Dieses globale Management hat sich, wie oben bereits angedeutet, über die Jahre hinweg von unten entwickelt. Triebkraft dieser Entwicklung war primär die Vision, Kommunikation zwischen jedermann zu jeder Zeit und überall möglich zu machen. In diesem Prozess hat sich ein Managementsystem herausgebildet, in dem der US-Regierung eine spezifische und unilaterale Rolle zugewachsen ist.

Die von der US-Regierung ausgeübte Funktion der Autorisierung der Publikation von "TLD Zone Files" im Root ist dabei tatsächlich von zentraler und strategischer Bedeutung. Die politische Dimension dieser Funktion wird aber in der allgemeinen Öffentlich-

keit weitgehend überschätzt. Die Kontrolle über den Root ist nicht vergleichbar mit dem "roten Knopf der Atombombe". Selbst wenn die US-Regierung es wollte, sie kann alleine kein Land vom Internet abklemmen. Nichtsdestotrotz stand das Thema "Oversight" im Zentrum der Diskussion innerhalb der WGIG.

Das historisch gewachsene Aufsichtssystem über den Root hat bis heute problemlos funktioniert. Es basiert aber weitgehend darauf, dass jeder jedem vertraut. Wenn SWITCH einen neuen Name-Server in Betrieb nehmen will, dann vertraut es darauf, dass ICANN und IANA die entsprechenden Änderungen der "Zone Files" sorgsam behandeln, an das US-Handelsministerium weiterleiten und dass die Daten von dort aus ohne Änderungen an VeriSign (den Manager des "Hidden Master") gehen und so in den Root gelangen. SWITCH hat aber weder einen Vertrag mit IANA noch mit dem US-Handelsministerium oder mit VeriSign.

Eine solche Konstellation, so argumentierten einige Mitglieder der WGIG, mache ganze Länder abhängig von einer Einzelentscheidung der US-Regierung. Was würde passieren, wenn die US-Regierung diese Funktion missbrauchen würde? Man habe keine Verträge in der Hand, sondern müsse darauf vertrauen, dass "alles seinen Gang geht". In guten Zeiten mag das funktionieren, aber was passiert, wenn es nicht funktioniert?

In den "Worst Case Szenarien" einiger Mitglieder der WGIG wurde der hypothetische Fall durchgespielt, dass ein US-Präsident, der politisches Fehlverhalten eines Landes bestrafen will, lediglich seinem Handelsminister im "Department of Commerce" (DOC) befehlen muss, VeriSign anzuweisen, den entsprechenden Ländercode aus dem Root zu nehmen, um damit die Internet-Kommunikation des betroffenen Landes zu verhindern. Sorge wurde auch geäußert, dass "unfolgsamen" Ländern der Zugang zum Root-Server – 10 von den 13 Servern des "authoritative root" befinden sich in den USA – verweigert werden könnte. Daraus wurde die Forderung abgeleitet, Vertrauen durch Verträge zu ersetzen, also anstelle des "Trust Systems" ein "Treaty System" zu etablieren.

Die zwingende Logik einer solchen Argumentation steht jedoch auf tönernen Füßen. Abgesehen von dem weltweiten öffentlichen Protest, den ein solch unilateraler Missbrauch der Ausübung einer auf Vertrauen basierenden Funktion auslösen würde, gäbe eine solche Aktion auch sachlich keinen Sinn. Es würde ausreichen, dass der in Schweden situierte I-Root-Server die vom A-Root-Server kommende modifizierte "Zone File"-Spiegelung in diesem Fall verweigern würde und die Kommunikation der inkriminierten ccTLD könnte weitergehen wie zuvor, möglicherweise mit einigen Milli-Sekunden Verzögerung bei einer temporären Überlastung. In diesem Fall wäre es sogar vorteilhaft, dass der schwedische Root-Server keinen Vertrag mit VeriSign hat und damit nicht vertragsbrüchig würde, wenn er einen solchen Vertrauensmissbrauch nicht mitmacht.

Insofern ist die freiwillige Vereinbarung zwischen den "Root Server Operators" nicht eigentlich eine Schwäche des Systems, wie gelegentlich behauptet wird, sondern eher eine Stärke, die dem System eine gewisse Robustheit und Stabilität gibt und zusätzlich absichert. Auch ist mittlerweile der "authoritative root" mittels des "Anycast Systems" um mehr als 100 Root-Server weltweit erweitert worden. Bei Anycast spiegeln die neuen Root-Server jeweils einen Root-Server der 13er-Kette. An dem schwedischen I-Root-Server hängen jetzt bereits mehr als 30 Root-Server in Afrika, Asien und Europa.

Die Vorstellung, die unilaterale Autorisierungsfunktion konstituiere eine Kontrolle über das Internet, ist ein Mythos. Hinter der Idee des Internets steckte ja von Anfang an auch

die strategische Absicht, ein dezentrales Kommunikationssystem aufzubauen, das durch keinen militärischen Angriff zerstörbar oder einseitig kontrollierbar ist. Der Geist ist längst aus der Flasche und dieses strategische Ziel ist schon längst erreicht. Keine Regierung, auch nicht die der Vereinigten Staaten von Amerika, kann das Internet einseitig kontrollieren.

Konsens gab es innerhalb der WGIG jedoch über drei Grundprinzipien, auf denen ein weiterentwickeltes Aufsichtssystem basieren sollte. In Paragraph 48 des WGIG-Reports heisst es dazu:

1. No single Government should have a pre-eminent role in relation to international Internet governance.
2. The organizational form for the governance function will be multilateral, transparent and democratic, with the full involvement of Governments, the private sector, civil society and international organizations.
3. The organizational form for the governance function will involve all stakeholders and relevant intergovernmental and international organizations within their respective roles.

(WGIG Final Report 2005)

Vier Modelle der WGIG

Wiewohl sich also die WGIG-Mitglieder darauf einigen konnten zu empfehlen, das unilaterale Aufsichtssystem durch die US-Regierung aufzuheben, führte das schlussendlich nicht dazu, ein neues Modell vorzuschlagen. Zu unterschiedlich waren die Vorstellungen auch innerhalb der Gruppe. Am Schluss vereinbarte man, vier verschiedene Modelle zur Diskussion zu stellen und es den Verhandlern im Rahmen des WSIS-Prozesses zu überlassen, eine diplomatische Lösung zu finden. Die vier Modelle reichen von einer etwas präzisierten Rolle von ICANN's "Governmental Advisory Committee" (GAC) über die Schaffung eines neuen "Governmental Internet Council" (GIC) bis zur Gründung einer neuen "World Internet Corporation for Assigned Names and Numbers" (WICANN) mit einem "Governmental Internet Council" (GIC) als Entscheidungsorgan und einem "Global Internet Forum" (GIF) als Beratungsgremium.

Aus der Sicht der Internet-Nutzer macht es jedoch wenig Sinn, unter dem Stichwort der "Internationalisierung des Internets" ein System einzuführen, wonach anstelle einer Regierung ein ganzer Regierungsrat mit vielleicht 15 oder 50 Mitgliedern die Autorisierungsfunktion übernimmt. Ein Blick in die Debatten des UN-Sicherheitsrates verdeutlicht, dass das wahrscheinliche Resultat einer solchen Multilateralisierung der Internet-Aufsicht eine Blockade der Internet-Entwicklung wäre. Wenn die Einführung neuer TLDs einen Konsens aller UN-Mitglieder bedarf oder wenn eine Veränderung des Name-Servers von Pakistan die Zustimmung der indischen Regierung erfordert, dann kann man sich ausmalen, wohin eine solche Reise gehen würde. Bei einer solchen Entwicklung wäre über kurz oder lang auch vorstellbar, dass Regierungen ein wirtschaftliches Interesse daran entwickeln könnten, die unbegrenzten Kernressourcen des Internets künstlich zu verknappen, um für deren Nutzung "IP-Lizenzgebühren" oder "Domain-Steuern" zu kassieren.

Ein solcher Weg führte in eine Sackgasse. Eine Lösung des Problems kann daher nur in einer anderen Richtung liegen. Wenn es unakzeptabel ist, dass eine einzige Regierung eine solche zentrale Funktion ausübt, die bei Lichte gesehen einen vorrangig techni-

schen Charakter hat und nicht in politische und wirtschaftliche Aktionen umsetzbar ist, stellt sich doch die Frage, ob man überhaupt eine Regierungsaufsicht über den Root in der bisher praktizierten Art benötigt. Wäre es nicht viel einfacher, wenn der "Hidden Server" gleich von ICANN verwaltet würde und Modifikationen, Zufügungen oder Streichungen von "Root Zone Files" für TLDs von ICANN direkt vorgenommen würden?

Es besteht keine sachliche Notwendigkeit, dass die "Root Zone Files" über den Schreibtisch eines US-Beamten im DOC gehen. Wenn ICANN in ein vertragliches System mit allen TLD-Managern und dem Operator des A-Root-Servers eingebunden ist, ist ein Missbrauch dieser Funktion kaum möglich. Die sachliche und technische Korrektheit eines dokumentierten "Zone File Managements" könnte von einer Wirtschaftsprüfungsgesellschaft regelmässig überprüft werden. Für die wohl mehr hypothetischen Fälle, dass damit politischer oder wirtschaftlicher Missbrauch betrieben würde, hätten die Regierungen durch ICANN's "Governmental Advisory Committee" (GAC) bereits jetzt genügend Instrumente in der Hand, um ICANN zur Ordnung zu rufen.

Notwendig ist mithin eine De-Mystifizierung des "Internet Root Managements" und eine Ent-Politisierung der Diskussion über die Kontrolle der Internet-Kernressourcen. Ob sich diese, dem Modell II des WGIG-Reports annähernde Variante jedoch durchsetzen wird, ist offen. Eine solche Lösung würde dreierlei erfordern: die Entlassung ICANNs in die Unabhängigkeit, eine weitere Entwicklung und Demokratisierung der inneren Strukturen von ICANN sowie die Einbettung von ICANN in ein vielschichtiges System von bilateralen Verträgen mit "TLD Registries" und "Root Server Operators" erfordern.

Die angekündigte Beendigung des aus dem Jahre 1998 stammenden "Memorandums of Understanding" (MoU) zwischen ICANN und dem DOC für den Oktober 2006 lässt jedoch zunächst offen, ob sie auch die Übergabe der Autorisierungsfunktion für "Root Zone Files" einschliesst. Noch vor der Veröffentlichung des WGIG-Reports hat die US-Regierung am 30. Juni 2005 angekündigt, dass sie zum jetzigen Zeitpunkt keinerlei Veranlassung sieht, an dem eingespielten System etwas zu verändern:

"The United States Government intends to preserve the security and stability of the Internet's Domain Name and Addressing System (DNS) and will therefore maintain its historic role in authorizing changes or modifications to the authoritative root zone file."
(US Department of Commerce 2005)

An der dritten Vorbereitungs-konferenz (PrepCom3) für den WSIS in Tunis kam es dabei zu einem nicht unerheblichen Konflikt zwischen den USA und der Europäischen Union. Als die EU die Schaffung eines neuen Kooperationsmodells vorschlug, das auf einer "Public Private Partnership" basieren sollte, wobei die Regierungen für die grundsätzlichen Fragen (on the level of principle) und der Private Sektor für das Tagesgeschäft (day to day operations) zuständig gewesen wären, stiess sie auf krasse Ablehnung seitens der US-Delegation (vgl. Wright 2005).

Sollte die US-Regierung jedoch an einer Position festhalten, die jedwede Veränderung des momentan praktizierten Systems ablehnt, könnte ein anderes "Schreckensszenario" drohen. Grosse Internet-Märkte mit Sprachen, die nicht auf dem lateinischen Alphabet basieren, könnten alternative Roots aufbauen und ein "eigenes Internet" schaffen, das man nur noch mit einem von der Regierung ausgegebenen "Passwort" in Richtung des heutigen globalen Internets verlassen darf – so wie man eben zur Ausreise aus einem Land einen "Passport" benötigt. Die separate Speicherung von "TLD Zone Files" für internationalisierte Domains (IDNs) – d.h. TLDs, die nicht auf ASCII basieren, sondern

chinesische, koreanische, japanische, arabische, kyrillische und andere Schriftzeichen verwenden, – in einem alternativen Root, ist rein technisch gesehen kein Problem. Die Konsequenz wäre eine Fragmentierung des Internets. Bei diesem Szenario, das einige Beobachter auch als eine mögliche "Balkanisierung des Internets" beschreiben, würden E-Mails im Cyberspace herumirren, weil sie nicht mehr ihren Adressaten finden oder weil es ein und dieselbe Adresse in mehreren Roots gibt. Der Turmbau zu Babel lässt grüssen.

Vor diesem Hintergrund einer drohenden babylonischen Verwirrung könnte der WGIG-Vorschlag, ein globales Internet-Forum zu schaffen, das den Dialog zwischen Regierungen, Privatwirtschaft und Zivilgesellschaft befördert, um durch verbesserte Kommunikation allseits akzeptable Lösungen zu entwickeln, einen zusätzlichen Sinn bekommen. In Paragraph 40 des WGIG-Reports heisst es dazu:

"The WGIG identified a vacuum within the context of existing structures, since there is no global multi-stakeholder forum to address Internet-related public policy issues. It came to the conclusion that there would be merit in creating such a space for dialogue among all stakeholders. This space could address these issues, as well as emerging issues, that are cross-cutting and multi-dimensional and that either affect more than one institution, are not dealt with by any institution or are not addressed in a coordinated manner."

(WGIG Final Report 2005)

Die WGIG hat den Weg von einem unstrukturierten und diversifizierten zu einem mehr qualifizierten und konzentrierten globalen Dialog geebnet. Die WGIG hat keine Lösungen erarbeitet. Wie sollte sie auch. Das hoch politisierte Thema "Internet Governance" wird noch lange auf der Tagesordnung der internationalen Diplomatie bleiben. Es wäre insofern schon ein Erfolg, wenn der 2. Weltgipfel zur Informationsgesellschaft (WSIS II) beschliessen würde, die globale Diskussion in einem mehr strukturierten Dialog unter Einbeziehung aller Beteiligten und Betroffenen fortzusetzen. Das Internet ist primär ein Kommunikationsmedium, sein Management aber bedarf selbst der Kommunikation. Nur wenn das Internet stabil und sicher funktioniert und ein für jedermann öffentlich zugänglicher Raum bleibt, werden sich die grenzenlosen Möglichkeiten der Informationsgesellschaft auch für jedermann erschliessen lassen.

Wolfgang Kleinwächter ist Professor für internationale Kommunikationspolitik an der Universität Aarhus, Dänemark, und Mitglied der "Working Group on Internet Governance" (WGIG).

Literatur:

Kleinwächter, Wolfgang (2004): Macht und Geld im Cyberspace: Wie der Weltgipfel zur Informationsgesellschaft die Weichen für die Zukunft stellt. Hannover.

Lessig, Lawrence (1999): Code and other Laws of Cyberspace. New York.

US Department of Commerce (2005): US Principles on the Internet's Domain Name and Addressing System. Washington, 30. Juni 2005:
http://www.ntia.doc.gov/ntiahome/domainname/USDNSprinciples_06302005.htm

WGIG (2005): WGIG Final Report. Genf, 12. Juli 2005:
<http://www.wgig.org>.

Wright, Tom (2005): EU and US Clash over Control of Net. In: International Herald Tribune, 30. September 2005.

Abkürzungen:

Offizielle Webseiten zum UN-Weltgipfel der Informationsgesellschaft

ITU	International Telecommunication Union (www.itu.org)
UNO	United Nations Organization (www.un.org)
WGIG	Working Group on Internet Governance (www.wgig.org)
WSIS	World Summit on the Information Society (www.itu.int/wsis/)

Management der Internet-Ressourcen

IANA	Internet Assigned Numbers Authority (www.iana.org)
ICANN	Internet Corporation for Assigned Names and Numbers (www.icann.org)
MoU	Memorandums of Understanding, US-Department of Commerce (DOC)
GAC	Governmental Advisory Committee (www.gac.icann.org)
GIC	Governmental Internet Council (in Diskussion)
GIF	Global Internet Forum (in Diskussion)
WICANN	World Internet Corporation for Assigned Names and Numbers (in Diskussion)

Registrierungsstellen für Domain-Namen

DENIC	Registrierungsstelle für Domains mit .de (www.denic.de)
RIRs	Regional Internet Registries (vgl. www.aso.icann.org/rirs/)
SWITCH	Registrierungsstelle für Domains mit .ch und .li (www.switch.ch)
VeriSign	Registrierungsstelle für Domains mit .com, .net, .cc, und .tv (www.verisign.com)

Private und zivilgesellschaftliche Akteure

APC	Association for Progressive Communications (www.apc.org)
ARTICLE 19	ARTICLE 19 – Global Campaign for Free Expression (www.article19.org)
CDT	Center for Democracy Technology (www.cdt.org)
CPSR	Computer Professionals for Social Responsibility (www.cpsr.org)
EFF	Electronic Frontier Foundation (www.eff.org)
IAB	Internet Architecture Board (www.iab.org)
IETF	Internet Engineering Task Force (www.ietf.org)
ISOC	Internet Society (www.isoc.org)
OECD	Organization for Economic Co-operation and Development (www.oecd.org)
W3C	World Wide Web Consortium (www.w3.org)
WIPO	World Intellectual Property Organization (www.wipo.int)
WPFC	World Press Freedom Committee (www.wpfc.org)
WTO	World Trade Organization (www.wto.org)

Technische Abkürzungen

ASCII	American Standard Code for Information Interchange
DNS	Domain Name System
IDNs	Internationalized Domain Names
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
TLDs	Top Level Domains
ccTLDs	country code Top Level Domains
gTLD	generic Top Level Domains

Der Text befindet sich im Internet unter:

http://www.medienheft.ch/dossier/bibliothek/d24_KleinwaechterWolfgang.html