

Zur Beziehung von Macht und Technik im Internet

Jeanette Hofmann und Marc Holitscher in: Udo Thiedeke (Hg.): Soziologie des Cyberspace. Medien, Strukturen und Semantiken, Opladen: Westdeutscher Verlag, 2004, S. 411 – 436

Die Absicht dieses Beitrags besteht darin, Thesen zur Konstituierung von Macht im Internet zu entwickeln. Die Beziehung zwischen Macht und Technik im Netz, so unsere Beobachtung, gehört zu den besonders bemerkenswerten Phänomenen des digitalen Kommunikationsraums, denn es sind gerade die machtspezifischen Konstitutionsmerkmale, die das Internet in der allgemeinen Wahrnehmung von anderen Kommunikationsmedien und infrastrukturen unterscheiden.

Das Vorhaben, über Macht im Internet zu schreiben, erweist sich als unerwartet anspruchsvoll. Da das Internet ein technisch konstituierter Kommunikationsraum ist, kommt eine Betrachtung der Macht im Internet schlechterdings nicht umhin, das Verhältnis von Macht und Technik in den Blick zu nehmen. Wie sich zeigt, räumen die "großen" Theorien über Macht technischen Aspekten in der Regel keinen systematischen Stellenwert ein. Gleichzeitig mangelt es der Literatur über das Internet an einer konzeptionellen Auseinandersetzung über struktur und entwicklungsprägende Einflussgrößen. So ist etwa das Verhältnis von technischer und politischer Normsetzungsmacht bislang kaum untersucht. Auffällig ist ferner, dass der Begriff Macht nicht einmal im Index jüngerer Monographien über das Internet zu finden ist.

Unsere Überlegungen zur Beziehung zwischen Macht und Technik im Netz sind daher explorativer Natur. Am Beispiel der Regulierung des Domain Name Systems (DNS) illustrieren wir die These, dass Macht kein genuiner Bestandteil von Technik ist, sondern dieser zugeschrieben wird. Institutionalisierungsprozesse wie die Gründung der Internet Corporation for Assigned Names and Numbers (ICANN) zielen darauf, die Ergebnisse solcher Zuschreibungen abzusichern und zu stabilisieren. Zunächst aber skizzieren wir in knappen Zügen den hier zugrunde gelegten Begriff der Macht, um daran anknüpfend techniksoziologische Überlegungen zum Verhältnis zwischen Macht und Technik vorzustellen.

1. Variationen über Macht im Internet

Ein Blick auf die Literatur zum Internet zeigt, dass das Phänomen der Macht von Beginn an einen besonderen Stellenwert in der Darstellung des Netzes gespielt hat. Die wohl verbreitetste Version handelt von der Abwesenheit von Macht. Exemplarisch dafür ist die 1996 publizierte "Declaration of the Independence of Cyberspace" von John Perry Barlow:

"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. (...) We must declare our virtual selves immune to your sovereignty, even as we continue to consent to your rule over our bodies."
(Barlow, 1996: Online).

In optimistischer Absicht nimmt Barlow eine Unterscheidung zwischen "Meat Space" and "Cyber Space" vor und erklärt die virtuelle Welt als befreit von den traditionellen Formen staatlicher Souveränität. John Walker schreibt rückblickend über den gleichen Zeitraum, dass er den universalen Zugang zum Internet als "a countervailing force against the centralization and concentration in government and the mass media" ansah (Walker, 2003). Die proklamierte Immunität gegenüber der Macht der Regierungen war mehr als eine bloße Willensbekundung, denn "the very design of the Internet seemed technologically proof against attempts to put the genie back in the bottle" (Walker, 2003), so die allgemeine Wahrnehmung.

Das Herz der Netzarchitektur besteht aus einem Satz technischer Standards namens TCP/IP, der regelt, wie im Internet Rechner adressiert und Daten ausgetauscht werden. Die machtpolitischen Implikationen, die TCP/IP zugeschrieben werden, sind so bedeutsam, dass die Funktionsweise dieser Protokolle vielfach beschrieben worden ist:

"The Internet is built on a simple suite of protocols the basic TCP/IP suite (...) These protocols, however, reveal nothing about the user of the Internet, and very little about the data being exchanged. (...) Like a daydreaming postal worker, the network simply moves the data and leaves interpretation of the data to the applications at either end. This minimalism in design is intentional. It reflects both a political decision about disabling control and a technological decision about the optimal network design."
(Lessig, 1999: 32).

Eine Konsequenz des so genannten "endtoend" Prinzips besteht in "the inability to discriminate" (...) The system was coded to be free." (Lessig, 2002: 1789). Mit anderen Worten ist es also die Netzarchitektur selbst, die die Ausübung hierarchisch organisierter Macht verhindert, sei es in der Form von Zensur, Ungleichheit oder kommerzieller Monopolbildung.

Die Netzarchitektur wird jedoch nicht nur als Verhinderungsinstrument beschrieben, sie gilt zugleich als Quelle der Ermächtigung, die die Selbstorganisation auch geographisch weit verstreuter Gruppen fördert und zur Herstellung von Gegenöffentlichkeit befähigt.¹ (Siehe auch Geser in diesem Band).

"Individuals, all over the globe, were empowered to create and exchange information of all kinds, spontaneously form virtual communities, and do so in a totally decentralized manner, free of any kind of restrictions."
(Walker, 2003).

Wiederum ist es die Technik, insbesondere die neuen interaktiven, bidirektionalen Kommunikationsdienste wie Mailinglisten, die als gemeinschaftsstiftend vorgestellt wird.

Eine weitere Version zum Thema Macht im Internet stellt die handlungsnormierende Wirkung der Netzarchitektur in den Vordergrund. Technik, so die Feststellung, bildet eine wesentliche Quelle von Macht im Internet. Einer der prominentesten Vertreter dieser These ist wiederum Larry Lessig, auf den die griffige Formel "code is law" zurückgeht. In Netzwerkumgebungen, so auch Reidenberg, sind:

"law and government regulation [...] not the only source of rulemaking. Technological capabilities and system design choices impose rules on participants (...) the set of rules for information flows imposed by technology and communication networks form a 'lex informatica'."
(Reidenberg, 1998: 553).

Technische Architekturen, so Reidenberg weiter, können wie gesetzliche Regelungen auch Handlungsweisen im Netz ausschließen oder umgekehrt bestimmte Datenflüsse erzwingen.

"Like a legal regime, Lex Informatica offers both customization of rules and inalienable rules. Customization for Lex Informatica occurs through technological configurations" vorausgesetzt die technischen Standards lassen solche Neukonfigurationen zu (Reidenberg 1999: 567/568). Je tiefer die jeweilige Schicht der Netzarchitektur, desto größer die Macht, die von den Informationsregeln ausgeht. Umgekehrt besteht im Bereich der anwendungsnahen Regeln größere Flexibilität für die Nutzer. Resümierend stellt Reidenberg fest, "the power of Lex Informatica to embed nonderogable, publicorder rules in network systems is not benign", und sei es nur, weil die Kosten ihrer Abschaffung oder Ersetzung hoch sind (O.c.: 553).

Von Technik kann mithin eine ähnliche Wirkungsmacht ausgehen wie von Gesetzen auch (Saretzky, 2000: 23). Mit Blick auf das Internet, so auch Fuhrmann, müsse bei der Suche nach angemessenen Regelungsstrategien die "faktische Gestaltungswirkung der Technik berücksichtigt" werden.

"Die Handlungsoptionen im Internet, und damit das Spektrum der regelbaren und zu regelnden Gegenstände, hängen in starkem Maße von der Ausprägung der technischen Infrastrukturen ab." (Fuhrmann, 2002: 118).

Macht im Internet, so kann man daraus schließen, äußert sich sowohl als handlungsermöglichende als auch als handlungsnormierende bzw. reglementierende Kraft. Der Soziologe Michael Mann unterscheidet in diesem Zusammenhang unter Rückgriff auf Talcott Parsons zwischen distributiven und kollektiven Aspekten von Macht. Während distributive Macht ein Nullsummenspiel definiert, in dem "eine feststehende Machtmenge auf verschiedene Beteiligte verteilt werden kann", beruht kollektive Macht auf der Kooperation von Menschen, die "ihre gemeinsame Macht über Dritte oder die Natur ausweiten können" (Mann, 1990: 22). Die beiden (idealtypischen) Formen von Macht, die "Macht zu" und die "Macht über", sind zumeist untrennbar miteinander verwoben, entsprechend zweischneidig erweist sich ihre Ausübung (O.c.: 23). So verdanken wir dem Internet einerseits eine beispiellose Kommunikations- und Innovationsfreiheit, der Preis dafür besteht jedoch andererseits in einer umfassenden Normierung von Interaktionsbeziehungen, deren Folgen in ihrem ganzen Ausmaß wohl erst langfristig sichtbar werden. Michael Manns Konzeption von Macht erlaubt es, die Ambivalenz, die ihr innewohnt, in den Blick zu nehmen.

Eine daran anschlussfähige und wie wir finden überzeugende Definition, die sich ebenfalls partiell auf Parsons beruft, findet sich bei Giddens, der Macht als "transformative Kapazität menschlicher Handlungen" fasst (Giddens, 1998: 145). Handlungen im Verständnis von Giddens stellen ein Eingreifen des Individuums ins Weltgeschehen dar. Im weitesten Sinne ergreifen die Menschen Maßnahmen, um bestimmte Ergebnisse zu erzielen. Macht bildet hier ein "Element des Handelns." Auch Giddens beschäftigt sich nicht mit der Bedeutung von Technik für die Ausübung von Macht, aber er stellt ausdrücklich klar, dass Macht an menschliches Handeln gebunden ist.

2. Die Beziehung zwischen Macht und Technik

In den Darstellungen über Macht im Internet werden der Technik unterschiedliche Wirkungen und Funktionen zugeschrieben. Die Gesetzesmetapher "code is law" etwa legt die Vorstellung nahe, bei Technik handele es sich um eine autonome, von sozialen Bedeutungen und Nutzungen unabhängig wirkende Macht. Standards wie TCP/IP oder das Domain Name System enthielten demzufolge Handlungsvorschriften, die zwar spezifische, von den Entwicklern formulierte Werthaltungen und politische Ziele repräsentieren, die aber nutzerseitig nicht verhandelbar sind. Technik verkörpert in dieser Lesart Zwänge und Freiheiten, die die Nutzer gleichermaßen vorfinden, nicht jedoch koproduzieren. Die Handlungsoptionen im Internet unterliegen mit anderen Worten einer "technischen Vorbestimmung" (Fuhrmann, 2002: 117).

Es gibt jedoch noch weitere, weniger technikdeterministisch angelegte Darstellungen zum Verhältnis zwischen Macht und Technik, die den Menschen einen größeren Einfluss auf die Wirkung von Technik zugestehen. Reidenberg etwa verteilt die Macht der Reglementierung auf die Technikentwickler und die Nutzer:

"For Lex Informatica, however, the primary source of default rulemaking is the technology developer and the social process by which customary uses evolve. Technologists design the basic infrastructure features that create and implement information policy defaults (...) and the users adopt precise interpretations through practices." (Reidenberg 1998: 567).

Die Regelungsmacht residiert Reidenberg zufolge nicht allein in der Netzarchitektur, sondern die Nutzer besitzen eine gewisse Interpretationsmacht, die sich im Zuge der Kommunikationspraxis entfaltet. Auf der Grundlage eines sehr erhellenden Vergleichs der Entwicklung von Uhren und Computern kommt Sawhney zu dem Schluss, dass die Verbreitung neuer Technologien zwar "a sense of empowerment" evoziere, die soziale und kulturelle Integration der Geräte jedoch einen neuen Kontrollapparat hervorbringe:

"The hardware only provides the physical foundations for coordination. It is the regulative power of cultural norms that induces compliance to system cues."
(Sawhney, 2004: 370).²

Die regulative Macht, die wir allgemein verbreiteten Technologien wie der Uhr zuschreiben, ergeben sich Sawhney zufolge erst aus den sozialen Normen, die den Gebrauch solcher Technologien regeln. Es sind mithin die gesellschaftlichen, nicht die technischen Normen, die Macht konstituieren.

In der Techniksoziologie hat es in den 1990er Jahren unter dem Titel "do artifacts have politics" eine intensive Auseinandersetzung über die Frage gegeben, ob technische Artefakte "eigenmächtig" in dem Sinne sind, dass sich "Handlungsprogramme" in diese einbauen lassen, so dass gesellschaftliche Prozesse mit Hilfe technischer Objekte gezielt gesteuert werden können.³ Von den verschiedenen Schlussfolgerungen, die aus der Debatte gezogen worden sind, erscheinen uns vor allem die Befunde unter dem Stichwort "Autorisierung der Dinge" unmittelbar relevant für die Frage nach der Konstituierung von Macht im Internet. Joerges etwa wendet sich gegen "kausalistische" Beschreibungen" von technischen Objekten:

"Bauten müssen und können immer wieder neu gelesen werden. Dabei spielen die Intentionen der Autoren, sprich der Designer, manchmal auch eine Rolle, aber meist eine eigenartig indeterminierte. Welchen Bedeutungen und Nutzungsformen gebauten Räumen eingeschrieben werden, darüber entscheiden andere."
(Joerges, 1997: 23).

Joerges Einwänden gegenüber Winner entsprechend können Bedeutungen und Wirkungen von Technologien nicht aus den Intentionen ihrer Designer und auch nicht aus den intrinsischen Eigenarten der Artefakte abgeleitet werden. Eben aus diesem Grunde scheint es ratsam, zwischen (Macht)Effekten von Technologien und den Intentionen ihrer Entwickler explizit zu unterscheiden. Die Macht befinde sich nämlich nicht in den Dingen selbst, sie sei vielmehr "delegierte Macht", und "ihr konkretes Funktionieren" sei "allenfalls ein Beweis" für die "Delegationsgarantie", mit der sie versehen ist." (Joerges, 1997: 24) Seine Autorität beziehe der gebaute Raum von außen. Es sei die "Kollaboration der Regierten", die technische Artefakte dazu befähige, Autorität zu repräsentieren, symbolisieren und manifestieren (Joerges, 1997: 27).

Die Erzeugung von Macht kann man sich demnach als einen kollektiven Zuschreibungsprozess vorstellen, in dem Entwickler, Produzenten, Nutzer und weitere Akteure technische Objekte mit einem veränderlichen Gefüge von Regeln, Werten, Glaubenssätzen und Bildern versehen.⁴ Die unterstellte Eigenmächtigkeit der Netzarchitektur, die in vielen Darstellungen über Macht im Netz durchscheint, verkennt offensichtlich deren kollaborativen Ursprung. Technisch konstituierte Macht ist ein Produkt menschlichen Handelns und nicht eine vorgefundene, verhaltensdeterminierende Größe. Artefakte führen folglich vorgefertigte politische Pläne nicht einfach aus, sondern sie sind, wie Latour schreibt, voller unerwarteter, weil nicht steuerbarer Konsequenzen:

"They do much more than carrying out power and domination (...) [they] are also offering permissions, possibilities, affordances (...) And yet all artifacts reside inside a corporate body which affirms their

existence or, alas, fail to do so."
(Latour, 2004).

Damit Technologien zu Werkzeugen transformativer Handlungskapazität werden können, müssen sie in stabile institutionelle Kontexte eingebunden sein. Wie wir später zeigen, schafft die Gründung der ICANN einen solchen "corporate body", der eine spezifische Delegation von Macht im Namensraum institutionell befestigt.

Ein möglicher Angelpunkt, um sich der Konstitution von Macht im Internet empirisch zu nähern, besteht in der Untersuchung solcher "permissions" und "possibilities". Gebaute Räume, so stellt Joerges fest, "repräsentieren Verfügungsrechte. Sie gehören jemandem und anderen nicht, sie dürfen von manchen legitimerweise genutzt werden, von anderen nicht. Variable, und das ist eben wichtig; nicht an die bauliche Form geknüpfte, Verfügungsrechte angebauten Räumen legen fest, was in diesen Räumen passiert." Entsprechend müsse man sich Gedanken machen über die "Art und Weise, in der solche Verfügungsrechte eingerichtet und verändert werden." (Joerges, 1997: 23) Eben darin besteht die Absicht der folgenden Abschnitte: Wir wollen den Wandel und die Absicherung von Verfügungsrechten im Namensraum rekonstruieren und uns Gedanken darüber machen, wie dies im Einzelnen geschieht.

2.1 Das Domain Name System: Die Delegation von Verfügungsrechten über Namen im Internet

Der Namensraum des Internets erweist sich als gutes Beispiel für die Variabilität von Macht in digitalen Räumen. Auf der Artefaktebene ist das DNS ein Datenbanksystem, das geschaffen wurde, um digitale Objekte im Internet mit einer zweifachen Identität auszustatten, einer numerischen Adresse und einem Namen. Das Ziel besteht darin, nutzerfreundliche Domain-Namen in maschinenlesbare Nummern und diese wiederum in Domain-Namen zu übersetzen. Das DNS delegiert diese Aufgabe an ein Programm namens "Nameserver". In gewisser Hinsicht erfüllt das DNS damit die Funktion eines Telefonbuchs. Für gesuchte Domain-Namen ermitteln die "Namensdiener" die maschinenlesbare, numerische Anschrift. Die wohl wichtigste Differenz zum Telefonbuch besteht darin, dass die Informationen über Namen und Nummern nicht in einem zentralen Register gespeichert sind, sondern dezentral verwaltet werden. Das DNS ist eine verteilte Datenbank. Die Inhaber von Domain-Namen sind im Prinzip selbst für die "Publikation" ihrer Daten bzw. den Betrieb der Nameserver verantwortlich.

Das DNS wurde Anfang der 1980er Jahre entwickelt. Es löste ein früheres System der Namensverwaltung ab, bei dem alle Hostnamen in einer zentralen Textdatei namens "host.txt" gespeichert wurden. Die Datei wurde vom Network Information Center (NIC)⁶ verwaltet, das jeden neuen Namen auf mögliche Doppelgänger prüfte, bevor er in die Namensliste aufgenommen wurde. Die Aktualisierung der Namensdatei erfolgte nur schleppend, und als die Anzahl der Einträge mehrere Hundert Namen überstieg, deutete sich die Einsicht an, dass die Kapazität des flachen Namensraums auf Dauer nicht ausreichen und auch das bisherige Zuteilungsverfahren bald an seine Grenzen stoßen würde. Um diese Probleme zu umgehen, sollte die Verantwortung für die Organisation des Namensraums an die Inhaber der Domain-Namen selbst delegiert werden: "Put organizations in charge of their names", lautete die Devise (Craig Partridge zitiert nach Salus, 1998: Online). Denn "centralized administration was against the spirit of what we wanted to do. (...) In layman's terms, once I have a domain, I'm free to maintain and change it by myself without calling the NIC." (Mockapetris zitiert nach Salus, 1998: Online).

Die Absicht der Entwickler bestand darin, die Autorität über den Namensraum an die Nutzer, das heißt im Kontext der 1980er Jahre: an die Betreiber lokaler Netze, vor allem Universitäten, Forschungseinrichtungen und wenige Unternehmen, zu delegieren. Autorität im Namensraum wie sie von den Entwicklern des DNS verstanden wurde, beruht in technischer Hinsicht auf den Informationen eines Nameservers über die Erreichbarkeit einer Domain. Der Eintrag in der Datenbank entscheidet darüber, ob eine Domain auffindbar ist und somit im Internet existiert oder nicht. In administrativer Hinsicht stellt sich Autorität im Namensraum als ein Delegationsverhältnis dar. Die Inhaber von Domain-Namen besitzen die

Verfügungsrechte über ihre Domain und können diese partiell weiter delegieren.

Die Nutzer sollten Autonomie über ihre Domain-Namen erhalten, das heißt, diese selbst verwalten und Änderungen vornehmen können, ohne hierfür das NIC um Zustimmung bitten zu müssen. Die Autonomie über die eigene Domain besteht vor allem in der Möglichkeit, Substrukturen zu schaffen. Mit der Registrierung eines Domain-Namens gewinnt der Inhaber das Recht, unterhalb dieses Domain-Namens einen beliebig strukturierten Namensraum einzurichten:

"DNS was organized around the principle that a 'responsible person' would be delegated the authority to assign and resolve names at any level of the hierarchy. (. . .) The designers of DNS had a good idea who they expected to take responsibility for second and third level names. Second level domains were thought of as names for major organizations whose networks contained 50 100 hosts. Third level domains would be administered by divisions of those organizations."

(Klensin zitiert nach Mueller, 2002a: 78f.).

Die Entwickler des DNS gingen davon aus, dass die Inhaber von Domain-Namen ihrerseits hierarchische Namensräume generieren würden, die ihre jeweiligen Organisationsstrukturen, etwa Disziplinen oder Abteilungen, reflektieren. Individuelle oder gar produkt und themenspezifische Domain-Namen, die seit Mitte der 1990er Jahre das Gesicht des DNS bestimmen, spielten in den frühen Überlegungen über die künftige Nutzung keine Rolle.

Das Prinzip der Delegation von Namensrechten konstituiert einen hierarchischen, pyramidenförmig aufgebauten Namensraum. Jede Ebene verwaltet Informationen und besitzt folglich die Autorität über die Erreichbarkeit der darunter liegenden Ebene. Die verteilte, hierarchisch angeordnete Namensautorität lässt sich sowohl als "Macht über" im Sinne einer Kontrolle über alle nachgeordneten Ebenen wie auch als "Macht zu" im Sinne der Ermächtigung beschreiben. So verdankt jede Hierarchiestufe im Namensraum ihre Existenz einer Delegation von Verfügungsrechten durch die nächst höhere Ebene. Andererseits kann das Löschen von Einträgen in der Datenbank des entsprechenden Nameservers dazu führen, dass Segmente des Namensraums schlichtweg verschwinden. Eine Schlüsselfunktion im Hinblick auf die Gestaltung von Verfügungsrechten nehmen die 13 root server an der Spitze der DNS Hierarchie ein. Wer das so ge nannte "master root file"⁷ verwaltet, kann Top-Level-Domains schaffen oder diese eliminieren (ausführlich Hofmann, 2003).

Im Selbstverständnis der Entwickler des DNS stand die kollektive, verteilt ausgelegte Dimension von Verfügungsrechten über den Namensraum im Vordergrund. Aus pragmatischen und wohl auch kulturspezifischen Erwägungen sollten die Inhaber von Domain-Namen befähigt werden, Segmente des Namensraums autonom zu gestalten und zu verwalten. Das Potenzial zur Monopolisierung der Verfügungsrechte über das DNS, welches der hierarchischen Struktur des Namensraums wenige Jahre später zugeschrieben wurde, spielte in den Anfangsjahren schon deshalb keine Rolle, weil der Betrieb des autoritativen root servers "A" als bloße operative Aufgabe wahrgenommen wurde.

2.2 Die Transformation von Macht im Namensraum

Mitte der 90er Jahre setzte ein Funktionswandel des DNS ein, der als "transmutation of domain names" bezeichnet worden ist (WIPO 1999: 12). Konzipiert worden waren Domain-Namen ursprünglich als beliebig wählbare Zeichenfolge, deren Geltungsbereich ausschließlich auf die Netzwelt beschränkt sein sollte. Ihre Vergabe folgte dem "first come, first served" Prinzip. Domain-Namen galten als öffentliches Gut, Besitzansprüche waren ausgeschlossen:

"Domain names provide a convenient addressing mechanism for people and machines to identify resources without having to remember long strings of numbers. Registration [...] confers no ownership or legal rights to the name beyond establishing the relationship for Internet addressing purposes."

(Mitchell et al. 1997: 262).

Zwei für die Entwicklung des Internets einschneidende Ereignisse änderten die Bedeutung und Nutzungsweise des DNS, die Entstehung des World Wide Web und die etwa im gleichen Zeitraum eingeleitete Privatisierung der amerikanischen Netzinfrastruktur, die das Internet für kommerzielle Nutzungen öffnete. Das WWW machte in neuartiger Weise Gebrauch von Domain-Namen, indem es diese als "locator" für Inhalte einsetzte.⁸ Die weder intendierte, noch vorausgesehene Folge dieses Adressierungsverfahrens war, dass Domain-Namen fortan nicht mehr vorrangig zur Identifizierung von Organisationen dienten, sondern als Kennzeichnung beliebiger Ressourcen und Personen entdeckt wurden (vgl. Mueller, 2002a: 107f.). Zugleich zog sich die bisherige Praxis einer hierarchischen "Besiedlung" einzelner Domain-Namen auf die akademische Welt zurück. Unternehmen begannen Domain-Namen für einzelne Produkte und Standorte zu registrieren, um von ihren Kunden besser gefunden zu werden. Der Handel mit Domain-Namen entwickelte sich zu einem einträglichen Geschäft.

1994 kam es zu ersten Rechtsstreitigkeiten um Domain-Namen. Das first come, first served Prinzip bei der Namensvergabe wurde durch Markenschutzansprüche in Frage gestellt. Seither besteht ein Spannungsverhältnis zwischen den verschiedenen Nutzungsansprüchen gegenüber dem DNS:

"It has become apparent to all that a considerable amount of tension has unwittingly been created between, on the one hand, addresses on the Internet in a humanfriendly form which carry the power of connotation and identification and, on the other hand, the recognized rights of identification in the real world, consisting of trademarks and other rights of business identification, the developing field of personality rights, whether attaching to real or fictional characters, and geographical indications."
(WIPO, 1999: 12f.).

Das Eindringen markenrechtlicher Ansprüche in den Namensraum und der steigende wirtschaftliche Wert von DomainNamen veränderte ihren Status und bewirkte zugleich eine Reinterpretation der Namenshierarchie. Konflikte um die künftige Entwicklung des DNS, darunter die Schaffung zusätzlicher TopLevel Domains und die Einführung von Wettbewerb bei der Registrierung von DomainNamen, führten zu einer politischen Aufwertung der root server Verwaltung. Im Zentrum standen hierbei die Verfügungsrechte über das master root file.

Anfang 1998, inmitten der Auseinandersetzung um die Verfügungsrechte über den Namensraum initiierte einer der Väter des DNS, Jon Postel, kurzfristig eine Maßnahme, die später als "Test" deklariert wurde. In einem Schreiben forderte er alle root server Betreiber auf, das master file nicht mehr vom root server A, sondern von seinem name server zu beziehen. Acht von 13 root server Betreibern folgten Postels Aufforderung (Mueller, 2002: 1612). Der kurze Aufstand gegenüber den sich durchsetzenden Machtansprüchen im Namensraum zeigte zumindest eines: Die Autorität des master root files ist auf die Zustimmung der root server Betreiber angewiesen. Auf der obersten Ebene im Namensraum besteht somit eine Delegationsbeziehung, die sich widerrufen lässt. Den 13 Betreibern der root server steht es im Prinzip offen, sich auf eine andere autoritative Quelle für den Bezug der Daten zu einigen. Das Domain Name System selbst bietet folglich keine Garantie für das stabile Funktionieren einer Namensautorität im Internet. Weder das DNS, noch der Verwalter des master files besitzt Sanktionsmacht gegenüber den Betreibern der root server. Stabile Machtverhältnisse im Namensraum lassen sich daher nur durch eine Institutionalisierung und Verregelung des DNS Betriebs erreichen.

3. Institutionalisierungsprozesse: Die Gründung und Entwicklung der ICANN

In den Medien wird die im amerikanischen Bundesstaat Kalifornien beheimatete ICANN gern als die "Regierung des Internets" bezeichnet. Die zitierte Analogie zur Staatenwelt jedoch ist in verschiedener Hinsicht falsch und irreführend: Regierungen besitzen gewöhnlich das uneingeschränkte Gewaltmonopol über ein geographisch definiertes Territorium. Ihre verfassungsmäßige Weisungsmacht gegenüber den

Bürgerinnen und Bürgern wird als legitim anerkannt, zumindest in demokratischen Staaten. Zudem sind die Regierungen gegen Außen hin souverän, also keiner dritten Gewalt gegenüber rechenschaftspflichtig.

Ganz anders präsentiert sich die Sachlage in Bezug auf das Internet. Als oberstes Verwaltungsorgan besitzt die ICANN kein natürliches Gewaltmonopol, ebenso wenig wie ihre Entscheidungsträger basisdemokratisch legitimiert sind. Die weit reichenden Machtressourcen der Behörde ergeben sich hauptsächlich aus der politischen Kontrolle, die sie über die technische Infrastruktur des Internets ausübt, in erster Linie das Domain Name System. Die notwendige Autorität für ihr Wirken leitet die oberste Internetbehörde aus einer Reihe von bilateralen Verträgen mit dem amerikanischen Handelsministerium ab (siehe auch Hutter in diesem Band). Somit ist die ICANN nicht souverän, sondern steht im langen Schatten der US-Regierung, die obwohl die Regelungsentscheide der ICANN globalen Gültigkeitsanspruch haben. In der Praxis ist die Behörde zudem fundamental auf die freiwillige Akzeptanz ihrer Autorität durch die Gemeinschaft der Internetnutzer angewiesen. Letztere sind potenziell jederzeit in der Lage, das von der ICANN kontrollierte Internet zu verlassen und in einen Netzverbund abzuwandern, der einer alternativen Kommunikationsordnung unterliegt.

Die Quelle der globalen Verfügungsgewalt, die die ICANN für sich reklamiert, nährt sich aus dem direkten Zusammenhang zwischen der technischen Architektur und den damit einhergehenden Nutzungschancen des Internets für die Anwender. Es benötigt keine große Vorstellungskraft sich auszumalen, dass die große Definitionsmacht, die sich aus der exklusiven Kontrolle der technischen Kernressourcen ergibt, begehrt und beneidet wird. Entsprechend umstritten war und ist denn auch das institutionelle Arrangement mit der ICANN, das den Umgang mit den technischen Ressourcen des Internets steuert und verbindlich regelt.

Die Gründung und Entwicklung der ICANN als fokale Institution im Bereich der Internetregulierung vermittelt eindrücklich, wie verschiedene Interessengruppen das über die Netztechnik vermittelte Machtpotential entweder zur ihrem Vorteil auszunutzen oder zum Wohle der Allgemeinheit zu disziplinieren suchten (Holitscher, 2004; Leib, 2002). Zur besseren Übersichtlichkeit wird die Entstehungsgeschichte der ICANN in drei verschiedene Phasen aufgeteilt.

Phase 1: Die Entscheidungshoheit der Ingenieure

Solange das Internet in erster Linie ein Experimentierfeld für überwiegend amerikanische Computerspezialisten in ursprünglich akademischem oder militärischem Auftrag war, basierte die Organisationsstruktur der Netzverwaltung weitgehend auf der von unten her (bottomup) gewachsenen Selbstregulierung der Ingenieure. Ihr gemeinsamer Nenner bildete ein kollektiv getragenes Ethos, das sich eng an den egalitären Idealen der Hippie-Bewegung der 1960er Jahre orientierte (Hofmann, 2000). Entsprechend informell und offen gestalteten sich denn auch die Entscheidungsmechanismen der wichtigen Technikergremien wie etwa der IANA oder IETF. Diese Grundhaltung konnte umso besser zum Nährboden des entstehenden Internetregimes werden, als sich die amerikanische Regierung trotz ihrer Finanzierung über öffentliche Gelder praktisch vollständig aus dem Alltagsgeschäft des Internets heraushielt.

Der Aufbau des Domain Name Systems nach dem Muster eines umgekehrten Baums war kein Zufall, sondern orientierte sich seinem Wesen nach unmittelbar an der dezentralisierten Architektur des Internets. Dabei waren sich die Ingenieure der Kontrollmöglichkeiten sehr wohl bewusst, die mit der übertriebenen Konzentration von Autorität auf einer bestimmten Stufe in der Namenhierarchie einhergingen. Auf diese Gefahr hin reagierten sie wiederum mit Dezentralisierung und der konsequenten Delegation von Autorität nach unten, also einer subsidiären Teilung von Verantwortung und Risiko (Mockapetris, 1983). Paradigmatisch verdeutlicht diese handlungsleitende Maxime ein viel zitierter Ausspruch von John Gilmore aus dem Jahre 1994: "The Net interprets censorship as damage and routes around it". Zentrale Schaltstellen sollten tunlichst vermieden und dafür die Verantwortung über die einzelnen Netzbereiche so

breit wie nur möglich auf die einzelnen Nutzer verteilt werden (Postel, 1994). Es war der Anspruch horizontale Netzwerke gleichberechtigter Computer zu schaffen, nicht eine hierarchisch strukturierte Kommunikationsordnung, wie sie aus der traditionellen Telekommunikation oder anderen Informationsinfrastrukturen bekannt war (Shapiro, 1999).

Die frühen Internetingenieure waren sich des engen Wirkungszusammenhangs von Technik und Macht sowie der eventuell schädlichen Konsequenzen sehr wohl bewusst. Übereinstimmend mit ihren freiheitlichen Grundwerten in stellten sie die bindenden Regeln zur gemeinschaftlichen Nutzung und Organisation der technischen Kernressourcen dergestalt, dass diese nicht von Partikularinteressen zur Durchsetzung ihrer spezifischen Ansprüche instrumentalisiert werden konnten. Auf diese Weise nutzten die Computerspezialisten beide vorgängig beschriebenen Dimensionen von Macht zur Erreichung ihrer Ziele: Einerseits sollte das Internet seine Nutzer zur diskriminierungsfreien Kommunikation in globalem Ausmaß ermächtigen, andererseits formten sie die Architektur des Domain Name Systems gezielt in eine Richtung, dass das technikhärente Normierungspotenzial effektiv diszipliniert wurde.

Doch auch die von der Ingenieursgruppe um John Postel gewählte Architekturlösung konnte die Notwendigkeit eines zentralen Koordinationspunktes in der Form des A-Rootservers nicht vermeiden. Dieser sollte aber keinesfalls mehr Aufgaben wahrnehmen als unbedingt notwendig, also die Adressinformationen der verteilten Netzwerke sammeln und für die Vermittlung der angeforderten Querverbindungen sorgen. John Postel nahm die wichtige Aufsichts und Koordinationsfunktion über die A-Root weit gehend in Eigenregie wahr. Er genoss dabei das unbedingte Vertrauen und große Ansehen der restlichen Technikergemeinschaft (Hafner, Lyon, 1996). Einzig auf dieser Grundlage konnte die notwendige Gewissheit herrschen, dass die mit der Kontrolle über die Kernaspekte der Netzinfrastruktur einhergehenden Handlungsressourcen nicht als Verhinderungsinstrument eingesetzt und damit missbraucht würden.

Zusätzliche Legitimation erhielt die IANA und damit Postel von der wachsenden Internetgemeinschaft selbst, also von den vielen verschiedenen Softwareprogrammierern, Inhaltsanbietern und vernetzten Forschungseinrichtungen, die sich zusehends von überall her in das entstehende Netzwerk einklinkten (Cukier, 1999). Sie alle hätten zu jedem Zeitpunkt die Weisungen Postels ignorieren können, was jedoch angesichts der Kompatibilitätsvorteile und erwarteten Netzwerkeffekte einer einzigen Koordinationsstelle niemand tat. Dies aus dem Grund, weil Metcalfe's Gesetz entsprechend der Nutzen für den einzelnen Anwender mit jedem neu an ein Gemeinschaftsnetz angeschlossenen Knotenpunkt (Host) exponentiell ansteigt. Verfügt ein Netzwerk erst einmal über eine kritische Masse von Anwendern, so macht es für die neu hinzukommenden Nutzer keinen Sinn, ein eigenständiges Netz aufzubauen; sie schließen sich aus eigenem Kalkül dem bereits bestehenden Netzverbund an (McKnight, Bailey, 1997). Oder etwas weniger rationalistisch formuliert: Die offene Architektur des Internets ermöglichte dem interessierten Anwender eine Chance der unmittelbar globalen Kommunikation, die ihresgleichen suchte und damit über enorme Anziehungskraft verfügte.

Dieser freiwillig sowie unkoordiniert ablaufende Konzentrationsprozess verdeutlicht in paradigmatischer Weise, dass sich die Macht der Regelsetzung nicht nur in den Techniken selbst findet, sondern ebenso bei den Nutzern liegt. Die A-Root konnte ihre übergeordnete Bedeutung für ein stabil funktionierendes Internet nur erlangen, weil sie von einer kritischen Anwendermasse als autoritative Quelle ihrer Kommunikationsverbindungen ausgewählt wurde. Dadurch begaben sich die Nutzer aber gleichzeitig auch in eine Abhängigkeit vom Zentralserversystem, was wiederum die politische Bedeutung potenzierte, die zu einem späteren Zeitpunkt der A-Root, bzw. der Kontrolle derselben zukommen sollte. Umso mehr setzten die Ingenieure ihre Verfügungsgewalt über die bestandswichtige Technik des Internets dafür ein, keine künstlichen Nutzungseinschränkungen zu installieren und allen interessierten Parteien gleichberechtigten Zugang zum expandierenden Netzverbund zu ermöglichen. Entsprechend offen gestaltete sich das Vergabesystem für Domain-Namen, die nach dem Prinzip des "first come, first served" angeboten wurden. Damit bildete die auf Gleichbehandlung und Offenheit bedachte

Technikergemeinschaft ihre fundamentalen Wertvorstellungen nicht nur auf die dezentrale Architektur des Netzes ab, sondern machten sie bewusst zur Grundlage auch des politischen Umgangs mit den technischen Kernressourcen an sich.

In dem Maße wie vermehrt neue Akteure das Internet als ebenso kostengünstiges wie faszinierendes Kommunikationsinstrument entdeckten, gerieten die "Entscheidungshoheit der Ingenieure" verstärkt unter Druck (Hofmann, 2000). Aufstrebende Internetunternehmen verlangten nach Planungssicherheit und einige entdeckten die Verfügungsgewalt über die Kernressourcen des Internets als willkommenen Hebel zur Sicherung ihrer partikularen Interessen. Entsprechend gewichteten sie das handlungsnormierende Potenzial der Internettechnik stärker als dies die Ingenieure getan hatten. Wie vorgängig skizziert spielten in dieser Beziehung vor allem Interessenten mit Markenansprüchen eine Vorreiterrolle, indem sie in den technischen Voraussetzungen des DNS einen effizienten Mechanismus zum Schutz ihrer eingetragenen Warenzeichen auch auf dem Internet erkannten (Mueller, 2002).

Unter diesen verschärften Bedingungen konnte das "old boys network" (Recke, 1999) der Techniker der zunehmenden kommerziellen Bedeutung des Internets nicht mehr länger gerecht werden. An der Spitze der Internetverwaltung zeichnete sich anfangs der 1990er Jahre ein rasch expandierendes Autoritätsvakuum ab. Diese unbefriedigende Situation konnte nur durch die Schaffung einer neuen institutionellen Ordnung auf globaler Ebene behoben werden, welche die Verfügungsrechte über die Kernressourcen des Internets eindeutig definierte und damit die wachsende Unsicherheit im Bereich der Internetverwaltung beseitigte. In Anlehnung an die Beobachtung Swahney's kann somit in Bezug auf die DNS-Reform argumentiert werden, dass die technologisch induzierte Ermächtigung zur informationellen Selbstbestimmung der Nutzer sehr schnell die Etablierung eines institutionell gebundenen Kontrollapparates durch profitorientierte Interessengruppen provozierte. Dies war ein Paradigmenwechsel den wir vorgängig mit dem Spannungsbogen zwischen der "Macht zu" bis zu einem "Macht über" beschrieben haben.

Phase 2: Kommerzialisierung und Internationalisierung des Internets

Antriebsmotor des institutionellen Wandels im Bereich der Internetverwaltung waren nach dem Zusammenbruch des Technikerregimes die ungeklärten Autoritätsverhältnisse über die bestandswichtigen Netzressourcen, also den Namenraum und das Zentralserversystem. Unterschiedliche private Parteien versuchten, sich diese unbesetzten Autoritätspositionen zu sichern und darauf aufbauend ein ihren jeweiligen Interessen entsprechendes Verfügungsregime einzurichten (Mueller, 2002). Schließlich verdichteten sich die gegensätzlichen Autoritätsambitionen zu einer zähen politischen Auseinandersetzung darüber, welche Interessengruppe wie viel Einfluss auf das neue Netzregime ausüben konnte. Dabei waren sich die Akteure sehr wohl bewusst, dass je nach dem, wie diese institutionelle Neugestaltung konkret ausfiel mit unterschiedlichen Verteilungswirkungen zu rechnen sein würde. Gleichsam als Kristallisationspunkt und Katalysator für die rasante Kommerzialisierung des Internets fungierte das Domain Name System.

Wie vorgängig dargestellt wandelten sich die Domain-Namen in der zweiten Hälfte der 1990er-Jahre in der Praxis der Anwender von hauptsächlich technisch relevanten Verbindungsmerkmalen zu genuin identitätsstiftenden Kategorien der Internetnutzung. Im Laufe dieses kollektiven Zuschreibungsprozesses wurde den Domain-Namen eine neue, von ihrer technischen Funktionalität abgekoppelte Qualität übertragen eine Entwicklung, die von den Erfindern des DNS weder intendiert noch vorausgesehen worden war. Im Sinne unserer einleitenden Überlegungen haben wir es hierbei also mit einer kollektiven Autorisierung des Domain Name Systems durch die Nutzer selbst zu tun.

Als unmittelbare Konsequenz davon änderten sich zusehends auch die Ansprüche, die man an die Regeln und Prozeduren ihrer Verwaltung stellte. Denn nun rückten die fehlenden, aber notwendigen politischen Entscheidungsmechanismen in den Vordergrund, welche die Verteilung der künstlich knappen

Kernressourcen an konkurrierende Interessen verbindlich regeln sollten. Im Laufe dieser Problematisierung mutierte das Domain Name System in der Rhetorik der involvierten Akteure von einer rein technischen Infrastruktur zur primären Trägerin sowohl des individuellen Existenzrechts im Cyberspace als auch der wirtschaftlichen Gewinnchancen, die sich daraus ergaben.

Aus dieser Perspektive verkörperte das Domain Name System in Form der hierarchisch organisierten Namenräume nicht nur eine wichtige technische Infrastruktur der globalen Kommunikation sondern auch ein sehr effektives Sanktionsinstrument. Die Domainvergabe konnte gezielt an gewisse Verpflichtungen seitens der Konsumenten gekoppelt oder einer wie auch immer gearteten Wettbewerbsordnung unterworfen werden. Die wachsende Erkenntnis der Möglichkeit einer direkten Implementierung bestimmter, global gültiger Verhaltensstandards über die Regulierung der zentralen Internettechnik war es denn auch, was die Kernressourcen und die institutionelle Ausbildung ihrer Verwaltung in den Augen profitorientierter Akteure zunehmend wichtig machte. Angesichts der enormen wirtschaftlichen Gewinnerwartungen, bemühten sich diese hartnäckig darum, den Schutz ihrer spezifischen Interessen direkt in das technischorganisatorische Design der Internetverwaltung einzubauen.

Insofern übertrugen die Akteure des politischen Diskurses in zunehmendem Masse verschiedene machtrelevante Wirkungszusammenhänge auf das Domain Name System, die aufgrund der ungeklärten Autoritätsverhältnisse in neue institutionelle Bahnen gelenkt werden mussten. Im Unterschied zur vorgängig skizzierten Phase der "Entscheidungshoheit der Ingenieure" standen im kommerzialisierten Umfeld der 1990er Jahre also nicht mehr die kommunikationsermöglichenden Aspekte der Internetinfrastruktur im Vordergrund, sondern vielmehr deren Macht, distributive Folgewirkungen zu erzeugen: Je nach dem wer die Allokationsmechanismen zur Bewirtschaftung der Namenräume neu installierte und wie diese aussahen, würden sich die einen Akteurgruppen vorteilhaftere Nutzungsrechte und damit ökonomische Gewinnchancen sichern können, andere aber zu den Verlieren gehören (Leib, 2001). Im Endeffekt war gerade diese Wahrnehmung der Reformbestrebungen als unüberwindbares Nullsummenspiel im Parsons'schen Sinne mitverantwortlich dafür, dass die involvierten Akteure zur Sicherung ihrer Interessen von vorneherein auf den Einsatz ihrer Machtressourcen setzten und nicht auf politischen Ausgleich besonnen waren.

In der Folge entbrannte zwischen NSI, dem old boys network der Internetingenieure und den Markeninhabern ein bitterer Streit um die zukünftige Regelung des DNS, wobei jede Gruppierung ihre eigene Agenda zu verwirklichen hoffte. Hierbei bestand das primäre Interesse der alten Technikergemeinschaft vor allem darin, weiterhin die Kontrolle über ihr Internet zu behalten und schädliche Einflüsse möglichst fernzuhalten. Die Ingenieure mussten aber bald realisieren, dass sie die erstarkenden Ansprüche der Markenschützer nicht ignorieren konnten. Letztere waren nicht nur sehr gut organisiert, sondern verfügten sowohl über enorme finanzielle Ressourcen wie auch gut etablierte Kanäle zu den politischen Entscheidungsträgern in Washington. Ihre Exponenten machten denn auch keinen Hehl daraus, dass sie im Domain-Name System das ideale Vehikel zur globalen Bestandeswahrung erkannten. Schließlich drängte eine wachsende Gruppe von privaten Unternehmen auf eine konsequente Öffnung des Marktes für die Registrierung von Domain-Namen und die entsprechende Abschaffung des NSI-Monopols.

Die Heftigkeit und große Emotionalität, mit der die Auseinandersetzung ausgetragen wurde, weckte zusehends auch die Aufmerksamkeit etablierter internationaler Organisationen wie etwa der ITU oder WIPO, aber auch verschiedener Regierungen. So erkannten die Regierungen im Laufe des ICANN-Prozesses nicht nur die politischen Implikationen vermeintlich technischer Koordinationsaufgaben, sondern lernten auch die strategische Bedeutung des Zentralserversystems für ihre nationalen (Sicherheits-)Interessen sowie die ökonomischen Potenziale der Internetinfrastruktur für ihre Volkswirtschaften kennen. Die Konfrontation entwickelte sich dabei zusehends zu einem Konflikt um die Frage, wer die politischen Verfügungsrechte über die Namens- und Nummernräume des Internets für sich beanspruchen konnte und entsprechend die notwendige Autorität innehielt, allfällige Änderungen der Spielregeln

durchzusetzen (Holitscher, 1999). Denn allen Beteiligten war klar: Wer das DNS hat, hat die Macht im Netz.

Diese Einschätzung der Sachlage führte zu einer Fortsetzung des Konflikts auf höherer politischer Ebene. Involviert wurden jetzt die USA und die EU, die ihre je individuellen Prioritäten betreffend die bevorzugte Ausgestaltung der künftigen Internetadministration zur Sicherung ihrer politischen Eigeninteressen und derjenigen der heimischen Industrie durchsetzen wollten. Der Konsens zwischen Washington und Brüssel zerbrach an der zentralen Frage, inwieweit die Internetadministration tatsächlich auf der weitgehend autonomen Selbstregulierung des internationalen Privatsektors basieren oder formal in einen zwischenstaatlich verfassten Ordnungsrahmen eingebunden werden sollte. Je nach dem wie die konkrete Mischung der staatlichen und nichtstaatlichen Einflussnahme auf die neue Internetverwaltung ausfallen würde, fühlten sich entweder die Amerikaner oder die Europäer übervorteilt. Dabei bevorzugten die Amerikaner den ihrer regulativen Tradition entsprechenden Ansatz einer dezidiert marktbasierter Regulierung, während die EU, ebenfalls ihrer regulativen Tradition entsprechend, auf die Etablierung einer eher korporatistisch ausgelegten Verwaltungsstruktur drängte.

Im November 1998 plädierten die USA nicht nur für die weitestgehende Delegation von Regelungsautorität an den internationalen Privatsektor, weil das aus ihrer Sicht eine besonders effiziente Lösung darstellte, sondern weil sie damit auch handfeste Interessen verfolgten: Vordergründig ganz der Steigerung wirtschaftlicher Wohlfahrt verpflichtet, schuf die ClintonAdministration mit ihrer Politik staatlichen Regulierungsverzichts aber vor allem eines: ein freies Spielfeld für die aufstrebende amerikanische Internetindustrie, die dem Rest der Welt technologisch und kommerziell weit überlegen war. Daneben behält sich die US-Regierung bis heute ein Kontrollrecht vor, das es ihr prinzipiell erlaubt, jeden Entscheid der ICANN für nichtig zu erklären. Die Europäer taten sich zunächst mit dem Modell des "hands off the Internet" schwer; mit institutionellen Zugeständnissen brachten die USA aber dann auch die EU ins Boot.

Vor diesem Hintergrund betrachtet muss die Gründung der ICANN im Spätherbst 1998 als komplexes Zusammenspiel verschiedener privater und staatlicher Interessen sowohl im jeweils nationalen, schließlich aber auch im transnationalen und internationalen Kontext interpretiert werden (Leib, 2002). Sie alle konkurrierten um den möglichst direkten Zugriff auf die technischen Kernressourcen des Internets, weil sie über diese vermittelt ihre jeweiligen Interessen optimal zu sichern hofften sei dies nun der Schutz von Markenzeichen, die Erweiterung des Namenraums zur Ermöglichung von mehr Wettbewerb unter den Registraren oder schlicht die Wahrung einer angemessenen Einflussbalance in der globalen Internetpolitik.

Die Frage der Internetregulierung war somit spätestens im Herbst 1998 eine hoch politische und die eigentlich zur Debatte stehenden Koordinationsfunktionen traten immer mehr in den Hintergrund. Die ICANN wurde als Symbol einer zukünftigen Machtverteilung in der globalen Internetpolitik gesehen denn als schlichte technische Verwaltungsinstanz. Diese an sich übersteigerte Sichtweise der ICANN ergab sich dabei nicht aus der tatsächlichen Sachlage selbst, sondern wurde vielmehr von einem expandierenden Akteursfeld an die Organisation herangetragen und auf diese projiziert. In dieser unübersichtlichen Gemengelage der vielen verschiedenen Akteure und ihrer unterschiedlichen Interessenlagen konnte sich jedoch keine Gruppierung vollständig durchsetzen. Vielmehr war eine ganze Reihe von politischen Kompromissen notwendig, die sich schließlich in der konkreten institutionellen Ausgestaltung der ICANN niederschlugen. Diese sollten sicherstellen, dass das große Machtpotenzial, das die verschiedenen beteiligten Akteure dem Domain-Name System und damit der Internetinfrastruktur zuschrieben wieder gleichmäßig auf diese (rück)verteilt wurde und damit kontrollierbar war.

Phase 3: Konsolidierung und Existenzsicherung

Seit ihrer Gründung im Herbst 1998 verfügt die ICANN nicht über die notwendige und genügend breite

Legitimität, so dass sich alle betroffenen Akteure freiwillig ihrem Vertragssystem mit globaler Ausdehnung unterordnen. Die Gründe hierfür sind vielfältig, in erster Linie werden der Internetbehörde aber Intransparenz und die regulative Vereinnahmung durch Wirtschaftsinteressen auf Kosten zivilgesellschaftlicher Kräfte vorgebracht. Diese anhaltende Kritik hat zu zwei Reaktionen seitens der ICANN geführt: Einerseits suchte das Direktorium immer offener die Nähe zu den Regierungen in der Hoffnung, dass diese die Regierten ruhigstellen und in die Arme der ICANN treiben würden. Andererseits verfolgte die ICANN selbst immer offener einen recht autokratischen, um nicht zu sagen aggressiven Politikstil.

Vor diesem an sich schon angespannten Hintergrund löste im Mai 2002 der Bankrott des mit 1,8 Milliarden Euro verschuldeten amerikanisch-niederländischen Backboneproviders KPN-Qwest eine ernsthafte Krise zwischen der ICANN und den ccTLDs aus (Heise Online, 2002). Das Problem bestand darin, dass KPNQwest für rund 60 Verwaltungen von LänderDomains den so genannten Secondary Name Server betrieb (Centr, 2002). Aufgrund der exemplarischen Implikationen dieses Konflikts für die gegenwärtige und auch künftige Stellung der ICANN soll nachfolgend ausführlicher auf die Details der Auseinandersetzung eingegangen werden.

Die Secondary Name Server beinhalten für die jeweiligen Namenräume beispielsweise für *.ch* alle notwendigen Informationen, unter welchen IP-Adressen sich sämtliche in diesen Namenräumen registrierten Domänen finden lassen. Ein Secondary Name Server weiss also, wohin er etwa die Anfrage nach der Domain *unizh.ch* weiterleiten muss, damit die Verbindung zustande kommt. Diese Name Server wiederum füttern die A-Root mit solchen Verbindungsdaten. Oder anders herum formuliert: Ist die Verbindung zwischen dem A-Rootserver und den jeweiligen für eine länderspezifische Domäne zuständigen Secondary Name Server gestört, kann es zu Unstabilitäten in der Auffindbarkeit dieser Länderdomänen und im Extremfall sogar zu deren Ausfall kommen.

Mit dem Zusammenbruch von KPN-Qwest war plötzlich auch der Betrieb des Secondary Name Servers für viele europäische Länderregistrare (ccTLDs) nicht mehr gewährleistet und ihre Domain-Namen waren nicht mehr fehlerfrei auffindbar, wenn entsprechende Anfragen über den festgefahrenen Name Server geleitet wurden. Entsprechend beeilten sich die betroffenen ccTLD sehr, einen Ersatz bereitzustellen. Sie baten die ICANN darum, die Einträge in der A-Root so zu verändern, dass künftige Anfragen nicht mehr über den fehlbaren Server bei KPN-Qwest, sondern über die neuen Secondary Name Server geleitet würden und damit die durchgehende Verbindung wieder sichergestellt sei.

Zur Verwunderung vieler Länderverwaltungen weigerte sich die ICANN jedoch, diese simple Änderung in gebührender Frist vorzunehmen. Vorab sollten die ccTLDs eine Kopie von sämtlichen Registrierungseinträgen unter ihrer jeweiligen Domain nach Marina del Rey zur "Überprüfung" durch die ICANN-Techniker schicken. Erst dann würde man das Update der A-Root vornehmen. Nicht von ungefähr weigerten sich die schon genügend um ihre Autonomie bangenden ccTLDs, allen voran die Deutsche DENIC, dieser Aufforderung nachzukommen:

"ICANN's demand on providing them unqualified access to the zone file, without any contract, and without open, established and publicly agreed policies on exactly how that data may be used, would represent a clear failure by ccTLDs in their fiduciary duty."
(Centr, 2002: 3).

Abgesehen von den riskanten Unsicherheiten, welche diese Blockade für das Internet mit sich brachte, trug besonders ein anderer Umstand zur Empörung der ccTLDs bei. Indem die ICANN Serviceleistungen an bestimmte Zugeständnisse der RegistryBetreiber knüpfte, machte die Organisation zum ersten Male ihre exklusive Kontrolle über die A-Root zur Erreichung regulativer Ziele nutzbar. Abgesehen vom rein technischen Schaden, der damit angerichtet wurde, war das hiermit ausgesendete Signal alarmierend: Die ICANN war also offensichtlich bereit, ihre Spitzenstellung an der DomainHierarchie als Hebel für die

globale Durchsetzung von bestimmten Verhaltensmaßnahmen zu gebrauchen.

In Verkennung der tatsächlichen Umstände versuchte die ICANN im Sommer 2002 die fehlbaren ccTLDs nicht etwa durch gezielte Anreize einzubinden, sondern setzte wie im Zusammenhang mit dem KPNQwestKonkurs geschehen ihre Kontrolle über die A-Root als Zwangsmittel ein. Damit forcierte die ICANN in einem dezentralen Netzwerk die Konzentration von weitreichenden und traditionell an die einzelnen Netzteilnehmer delegierten Autoritäten in ihrer Hand. Mit ihrem Zentralisierungsstreben forderte das Unternehmen nicht nur das fundamentale Design und Ideenprinzip des Internets heraus, dass Zentralisierung konsequent vermieden und notwendige Managementaufgaben möglichst dezentralisiert und weiterdelegiert werden sollen; sie lieferte ihrer wachsenden Kritikerschar gleich noch das Totschlägerargument, mit ihrem auf Konfrontation angelegten Vorgehen, die Stabilität des Internets an sich gefährdet zu haben:

"This exercise, however, demonstrated to the Internet technical community that ICANN would risk the stability of the Internet its entire reason for existence from the technical community's perspective to achieve its policy objectives."

(Feld, 2003: 352).

Obwohl sich die ICANN nach einigem Hin und Her dennoch überreden ließ, die notwendigen Änderungen auch ohne die Aushändigung der länderspezifischen Zonefiles durchzuführen, war in diesem Machtkampf genügend Porzellan zerschlagen, so dass eine vertragliche Einigung beider Parteien wieder in die Ferne gerückt ist. Die ccTLDs bestehen dementsprechend weiterhin darauf, dass die ICANN für sie eine technische Serviceorganisation ist, die für das reibungslose Funktionieren des Domain Name Systems zu sorgen hat. Die ICANN selbst sieht sich in diesem Bereich offenbar aber stärker als Institution mit einem globalen, politischen Auftrag.

Zusammenfassend zeigt diese Episode eindrücklich, dass eine Zentralisierung von Autoritäten gegen den Willen der Nutzerschaft auf dem Internet nicht oder nur bis zu einem gewissen Grade möglich ist. Die dezentrale Architektur des weltumspannenden Kommunikationsmediums schränkt die Möglichkeiten zur Machtausübung selbst ein, die sich aus der exklusiven Kontrolle gerade eben der Internetinfrastruktur ergeben. Damit verfügt das Internet über einen einzigartigen Selbstregelungsmechanismus, der das Entstehen von hierarchischen politischen Strukturen ohne ausreichende Legitimation effektiv und nachhaltig verhindert.

4. Fazit: Macht im Internet

Auch in technisch konstituierten Umgebungen wie dem Internet wird Macht durch soziales Handeln, nicht durch Code konstituiert. Gleichgültig, ob es um distributive oder kollektive Formen von Macht geht, sie ist ultimativ auf die Anerkennung durch die Unterworfenen angewiesen. Das root master file konnte seine überragende Bedeutung als Herzstück der expandierenden Internetinfrastruktur nur erlangen, weil die Nutzer ihre Computer mit den autoritativen Verbindungsdaten fütterten. Erst dieser kollektive, unkoordiniert ablaufende Zu schreibungsprozess bewirkt, dass der physischen Kontrolle über das master file unmittelbar politische Bedeutung zukommt. Gleichzeitig diszipliniert jedoch gerade die Notwendigkeit der Anerkennung von Macht deren willkürliche Ausübung. Weil die Autorität des root master files auf einer reversiblen Delegationsentscheidung beruht, sind der Ausübung von Macht im Namensraum vergleichsweise enge Grenzen gesetzt, wie das Beispiel der glücklosen Einbindung der ccTLDs in das von der ICANN kontrollierte Vertragssystem gezeigt hat.

Als Ergebnis eines grundlegenden Perzeptionswandels stehen heute nicht mehr die operativen Funktionen der Rootserver im Vordergrund, sondern die machtpolitischen Effekte, die sich aus ihrer Kontrolle ergeben: das einmalige Potenzial zur Durchsetzung netzweit gültiger Verhaltensstandards. In der zweiten Hälfte der 1990er Jahre konkurrierten verschiedene Akteursgruppen um die Macht, diese Regeln zu ihren

Gunsten definieren zu können. Das Beispiel Do main Name System unterstreicht die These, dass sich Macht im Internet in Form der Verteilung von Verfügungsrechten äußert. Stand zunächst die Delegation von Verfügungsrechten und somit die kollektive Dimension von Macht im Vordergrund, gewinnen seit der zweiten Hälfte der 1990er Jahre Strategien zur Konzentration und Instrumentalisierung von Verfügungsrechten an Bedeutung.

In diesem Sinne lässt sich mit Verweis auf Joerges feststellen, dass technisch konstituierte Verfügungsrechte und die verschiedenen Formen von Macht, die sie ermöglichen, tatsächlich variabel, also nicht technisch determiniert sind. Die Architektur des Namensraums gibt Machtstrukturen nicht vor, die Verteilung von Verfügungsrechten wird vielmehr auf der Grundlage politischer und rechtlicher Normen wie dem Markenrecht ausgehandelt. Es sind also gerade nicht die ursprünglichen Vorstellungen und Gebote der Ingenieure, der Architekten des DNS, die den heutigen Gebrauch von Domain-Namen bestimmen, sondern eher technikferne Akteure. Macht, so Giddens, ist gleichbedeutend mit dem transformativen, intervenierenden Element menschlichen Handelns. Im Kommunikationsraum Internet wird sie daher vielleicht besonders an den Orten greifbar, wo die Bedeutung von Normen, technische wie kulturelle, neu ausgehandelt und möglicherweise umgeschrieben wird.

Fußnoten

1 Eine der jüngeren Erscheinungsformen dieser Art stellen "blogs" dar, deren Vernetzung einen neuen Typ der Öffentlichkeit hervorbringt (Sullivan 2002).

2 Sawhneys vielleicht anschaulichstes Beispiel ist das Prinzip der Pünktlichkeit, das der Uhr zu ihrer disziplinierenden Macht verhilft.

3 Anlass für diese Auseinandersetzung war ein berühmt gewordener Artikel von Langdon Winner, der unter anderem am Beispiel der Brücken von Bob Moses zu zeigen versucht hat, dass "power relations can literally be built into and perpetuated through stone" (Winner zitiert nach Joerges, 1999). Ein Teil der Beiträge zur "Steuerungsdebatte" in der Techniksoziologie findet sich bei Joerges 1999 zitiert.

4 Law spricht in diesem Zusammenhang von soziotechnischen Ordnungen oder Netzwerken heterogener Materialität: "wherever we scrape the social surface we will find that it is composed of networks of heterogeneous materials" (Law, 1991: 10). Physische und immaterielle Elemente gehen Verbindungen ein, die ihrerseits soziale Ordnung generieren.

5 Praktisch wird diese Aufgabe zumeist von Providern bzw. Webhostern wahrgenommen.

6 Das NIC operierte unter dem Dach des SRI International (Stanford Research Institute).

7 Das Master Root File, auch als primary server bezeichnet, ist gewissermaßen die Ahnin aller Top Level Domains. Von den übrigen Rootservern unterscheidet es sich dadurch, dass es seine Daten nicht von einer übergeordneten Instanz bezieht, sondern selbst die autoritative Quelle bildet, von der Informationen über TLDs bezogen werden. Die politische Kontrolle über das Master Root File liegt beim US-Wirtschaftsministerium, das die operative Aufsicht an das amerikanische Unternehmen Verisign delegiert hat. Änderungen an den Root Zone-Einträgen werden allerdings nur nach Zustimmung der US-Regierung vorgenommen. Die Rootserver beziehen alle 30 Minuten eine aktuelle Kopie des Masterfiles.

8 Der Adressierungsstandard des WWW, der Universal Resource Locator (URL), beruht auf Domain-Namen: www.domain.de.

Literatur

John Perry Barlow, 1996: A Declaration of the Independence of Cyberspace Online:

<http://www.eff.org/~barlow/DeclarationFinal.html>

Centr, Council of European National TopLevel Domain Registries, 2002: Comments on ICANN Zone Access Policy. Online: <http://www.centr.org/docs/statements/ICANNZoneAccessComments.html>

Kenneth Neil Cukier, 1999: Internet Governance and the Ancien Regime, in: Swiss Political Science Review, 5, 1. S. 127-134.

Harold Feld, 2003: Structured to Fail: ICANN and the 'Privatization' Experiment, in: Adam Thierer, Clyde Wayne Crews Jr. (Hrsg.): Who rules the Net? Internet Governance and Jurisdiction. Cato Institute, Washington, D.C. S. 333-363.

Heiner Fuhrmann, 2002: Technikgestaltung als Mittel zur rechtlichen Steuerung im Internet, in: Zeitschrift für Rechtssoziologie, 23, 1. S. 115-130.

Anthony Giddens, 1998: Macht in den Schriften von Talcott Parsons, in: Peter Imbusch (Hrsg.): Macht und Herrschaft. Sozialwissenschaftliche Konzeptionen und Theorien. Opladen. S. 131-147.

Katie Hafner, Matthew Lyon, 1996: Where Wizards Stay Up Late: The Origins of the Internet. New York.

Heise Online, 2002: News. KPNQwest beantragt Gläubigerschutz. Online:
<http://www.heise.de/newsticker/data/jk23.05.02008/>

Jeanette Hofmann, 2000: Und wer regiert das Internet? Regimewechsel im Cyberspace, in: Herbert Kubicek, et al. (Hrsg.): Jahrbuch Telekommunikation und Gesellschaft. Heidelberg

Jeanette Hofmann, 2003: Die Regulierung des DomainNamensystems Entscheidungsprozess und gesellschaftliche Auswirkungen der Einrichtung neuer Top Level Domains im Internet. WZB discussion paper, SP III 2003-104.

Marc Holitscher, 1999: Global Internet Governance and the Rise of the Private Sector, in: Swiss Political Science Review, 5, 2. S. 134-142.

Marc Holitscher, 2004: Die Regulierung des Internets zwischen technischer Koordination und politischer Steuerung: Eine explorative Einzelfallstudie am Beispiel der Internet Corporation for Assigned Names and Numbers zur Rolle privater Akteure in den internationalen Beziehungen. Zürich: Universität Zürich.

Bernward Joerges, 1997: Die Brücken des Robert Moses oder: Do Politics Have Artifacts? Zur Konstruktion von Stadtraum und Stadtgesellschaft in technik und planungssoziologischen Diskursen. WZB discussion paper, FS II 97-502.

Bruno Latour, 2004: Which politics for which artifacts, in: Domus. Online:
http://www.ensmp.fr/~latour/presse/presse_art/GB06%20DOMUS%200604.html

John Law, 1991: monsters, machines and sociotechnical relations, in: ders. (Hrsg.): A Sociology of Monsters. Essays on Power, Technology and Domination, Routledge, London. S. 123.

Volker Leib, 2001: Das Doppelgesicht von Ican: Koordination und Regulierung des Internet, 2001. Online: <http://www.politikdigital.de/netzpolitik/icann/doppel.shtml>

Volker Leib, 2002: ICANN und der Konflikt um die InternetRessourcen: Institutionenbildung im Problemfeld Internet Governance zwischen multinationaler Staatstätigkeit und globaler Selbstregulierung, 2002. Dissertation. Online: <http://www.ub.unikonstanz.de/kops>

Lawrence Lessig, 2002: The Architecture of Innovation, in: Duke Law Journal, 51, 6. S. 1783-1801.

Lawrence Lessig, 1999: Code and other laws of cyberspace. New York.

Michael Mann, 1990: Geschichte der Macht, Bd. 1. Frankfurt/M.

Lee W. McKnight, Joseph P. Bailey, 1997: Internet Economics. Cambridge, Mass.

Don Mitchell, Scott Bradner, K. Claffy, 1997: In Whose Domain?: Name Service in Adolescence, in: Brian Kahin, James H. Keller (Hrsg.): Coordinating the Internet. Cambridge, Mass. S. 258-270.

Paul Mockapetris, 1983: Domain Names: Concepts and Facilities. Online:
<http://rfc.sunsite.dk/rfc/rfc882.html>.

Milton Mueller, 2002: Ruling the Root: Internet Governance and the Taming of Cyberspace. Cambridge, Mass.

Jon Postel, 1994: Domain Name System Structure and Delegation. Online: <http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc1591.html>.

Martin Recke, 1999: Das Internet im Zugriff der Politik: Das Beispiel der DomainNamenDebatte, in: Eike Hebecker, Frank Kleemann, Harald Neymanns (Hrsg.): Neue Medioumwelten. Zwischen Regulierungsprozessen und alltäglicher Aneignung. Frankfurt/M. S. 195-200.

Joel R. Reidenberg, 1998: Lex Informatica: The Formulation of Information Policy Rules Through Technology, in: Texas Law Review, 76, 3. S. 553-584.

Peter H. Salus, 1998: Domain Name System, in: Matrix News, 8, 10. Online:
<http://www.mids.org/pay/mn/810/domain.html>

Thomas Saretzki, 2000: Technologische Bürgerschaft? Anmerkungen zur Konstruktion von "citizenship" in einer technologischen "polity", in: Renate Martinsen, Georg Simonis (Hrsg.): Demokratie und Technik (k)eine Wahlverwandtschaft? Opladen. S. 17-51.

Harmeet Sawhney, 2004: The slide towards decentralization: clock and computer, in: Media, Culture &

Society, 26, 3. S. 359-374.

Andrew L. Shapiro, 1999: The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know. Edited by A Century Foundation Book. New York.

Andrew Sullivan, 2002: A Blogger Manifesto Why online weblogs are one future for journalism. Online: <http://www.andrewsullivan.com/culture.php>

John Walker, 2003: The Digital Imprimatur How big brother and big media can put the Internet genie back in the bottle. Online: <http://www.fourmilab.ch/documents/digitalimprimatur/>

WIPO (World Intellectual Property Organization), 1999: The Management of Internet Names and Numbers Report of the WIPO Internet Domain Name Process, Genf. Online: <http://wipo2.wipo.int/process1/report/index.html>