

# **Die Selbstregulierung im Internet**

**Unter besonderer Betrachtung der  
Standardsetzung und des  
Domain Name Systems**

**Dissertation**

**zur Erlangung des akademischen Grades**

**doctor iuris (Dr. iur)**

vorgelegt dem Fakultätsrat der Rechtswissenschaftlichen Fakultät  
der Friedrich-Schiller-Universität Jena

von Hans Reip  
geb. am 1. April 1974, in Meerane

---

Gutachter

1.:

2.:

Disputation:

## I. Inhaltsverzeichnis

I.	Inhaltsverzeichnis.....	III
II.	Literaturverzeichnis .....	VII
•	Kommentare – Bücher – Festschriften .....	VII
•	Aufsätze – Essays.....	IX
•	Zeitungsaartikel – Online-News .....	XXIX
•	Internetstandards .....	XXXV
III.	Abkürzungsverzeichnis .....	XXXIX
1.	Einleitung.....	1
2.	Das Internet als System .....	6
2.1.	Geschichtlicher Hintergrund.....	6
2.2.	Technischer Einblick .....	8
2.2.1.	Aufbau in einzelnen Schichten .....	8
2.2.2.	Adressierung von Computern im Internet.....	13
2.2.2.1.	IP-Nummern als Internetadressen .....	13
2.2.2.2.	Domainnamen als Internetadressen.....	14
2.2.2.2.1.	Nutzung der Domainnamen .....	15
2.2.2.2.2.	Aufbau und Einteilung der Domainnamen .....	15
2.2.2.3.	Feststellung der IP-Nummern durch Domain Name Server.....	18
2.3.	Staatlicher Eingriff vs. Selbstregulierung.....	20
2.3.1.	Selbstregulierung im Deutschen Staatssystem.....	20
2.3.2.	Regulierung des Internets.....	25
2.3.3.	Staatliche Regulierung .....	30
2.3.3.1.	Vor- und Nachteile staatlicher Regulierung .....	31
2.3.3.2.	Umsetzung .....	36
2.3.4.	Selbstregulierung .....	37
2.3.4.1.	Cyberspace als eigenes Rechtsterritorium.....	37
2.3.4.2.	Berechtigung einer Selbstregulierung .....	42
2.3.4.3.	Transnationale Regulierung durch Organisationen und Regeln .....	45
2.3.4.4.	Nachteile der Selbstregulierung .....	45
2.3.4.5.	Formen der Selbstregulierung .....	46
2.3.4.6.	Regulierung durch Privatrecht.....	48
2.3.4.7.	Erfordernis einer eigenen Jurisdiktion .....	52
2.3.5.	Regulatorische Mix .....	54
2.4.	Verwaltung des Internet.....	54
2.4.1.	Standards im Internet .....	55
2.4.1.1.	Standardsetzung im Allgemeinen.....	55
2.4.1.1.1.	Wirkungsweise von Standards.....	56
2.4.1.1.2.	Vorteile für den Verbraucher.....	57

---

2.4.1.1.3. Potentielle Risiken für den Verbraucher .....	58
2.4.1.1.4. Weg zur Standardisierung.....	60
2.4.1.2. Standardsetzende Organisationen im Internet.....	67
2.4.1.2.1. Traditionelle Organisationen .....	67
• ISO – <i>International Organization for Standardization</i> .....	67
• ITU – <i>International Telecommunications Union</i> .....	69
• ANSI – <i>American National Standards Institute</i> .....	70
• ETSI – <i>European Telecommunications Standards Institute</i> .....	71
2.4.1.2.2. Moderne Organisationen .....	71
• IETF – <i>Internet Engineering Task Force</i> .....	72
• IESG – <i>Internet Engineering Steering Group</i> .....	74
• IRTF – <i>Internet Research Task Force</i> .....	75
• IRSG – <i>Internet Research Steering Group</i> .....	77
• IANA – <i>Internet Assigned Numbers Authority</i> .....	77
• RFC-Editor .....	79
• IAB – <i>Internet Architecture Board</i> .....	79
• ISOC – <i>Internet Society</i> .....	81
• ICANN – <i>Internet Corporation for Assigned Names and Numbers</i> .....	88
• W3C – <i>World Wide Web Consortium</i> .....	88
2.4.1.3. Standardsetzung im Internet.....	92
2.4.1.3.1. RFCs, BCPs und STDs als Grundlage.....	95
2.4.1.3.2. Verfahrensgang der Standardsetzung .....	97
2.4.1.3.3. Wettbewerbsbeschränkungen durch öffentliche Standards .....	101
2.4.1.3.4. Überblick über Vorteile des offenen Standardisierungsprozesses .....	102
2.4.2. Vergabe der IP-Nummern durch ARIN, RIPE-NCC und APNIC .....	103
2.4.3. Vergabe und Verwaltung der Domainnamen.....	106
2.4.3.1. Verwaltung und Vergabe von Domains unter gTLDs.....	106
2.4.3.2. Delegation neuer ccTLDs.....	108
2.4.3.3. Die deutsche TLD .de.....	109
3. ICANN als neue Verwaltungsstruktur.....	111
3.1. Geschichtlicher Hintergrund der ICANN .....	111
3.1.1. Notwendigkeit einer Strukturreform .....	114
3.1.2. Von der IANA zur ICANN .....	115
3.1.2.1. 1994 – Versuch der Übertragung der IANA Aufgaben an die ISOC .....	116
3.1.2.2. Dr. Jon Postels Vorschlag von 150 neuen TLDs.....	116
3.1.2.3. <i>International Ad Hoc Committee</i> – IAHC .....	118
3.1.2.3.1. Zeitplan .....	119
3.1.2.3.2. gTLD-MoU .....	120
3.1.2.3.3. Kritikpunkte .....	124
3.1.2.4. Intervention der US-Regierung – <i>Green Paper</i> .....	126
3.1.2.5. <i>White Paper</i> der US-Regierung.....	129
3.1.2.6. IFWP gegen Dr. Jon Postels ICANN-Plan.....	132

---

3.1.3. Vertragliche Grundlagen der Autorität der ICANN .....	134
3.1.3.1. NSI/DoC-Amendment Nr. 11 und ICANN/US-DoC-MoU .....	134
3.1.3.2. Verhältnis zwischen NSI, ICANN und US-DoC .....	138
3.2. Arbeit der ICANN .....	141
3.2.1. Funktionen der ICANN.....	142
3.2.2. Struktur der ICANN .....	145
3.2.2.1. <i>Board of Directors</i> und der Präsident der ICANN.....	146
3.2.2.2. <i>Supporting Organizations</i> .....	148
3.2.2.3. <i>Advisory Committees</i> .....	150
3.2.2.4. <i>At-Large Membership</i> – ALM-Direktoren .....	153
3.2.3. Probleme rund um die ICANN .....	161
3.2.3.1. Legitimation durch Mehrheitsentscheidungen oder Konsens .....	162
3.2.3.2. Verhältnis der ICANN zur NSI.....	166
3.2.3.3. Verhältnis der ICANN zu den ccTLDs .....	167
3.2.3.4. Autorität über den A Root Server.....	170
3.2.3.5. Finanzierung der ICANN .....	171
3.2.4. ICANN in der Zukunft.....	172
3.3. Reform des DNS durch die ICANN .....	174
3.3.1. <i>Uniform Domain Name Dispute Resolution Policy</i> .....	174
3.3.1.1. Lösungen durch die NSI und das gTLD-MoU.....	175
3.3.1.2. Streitschlichtung unter Führung der WIPO.....	177
3.3.2. Einführung neuer TLDs .....	184
3.3.2.1. Neue ccTLDs.....	184
3.3.2.2. Neue gTLDs .....	185
3.3.2.3. Eine TLD für Europa.....	190
3.3.3. Multilinguale Domainnamen .....	192
4. Die Domainnamen .....	193
4.1. Bedeutung von Namensbezeichnungen .....	194
4.2. Bisher verwendete Kurzbezeichnungen.....	194
4.2.1. Aktiensymbole an den Börsen .....	195
4.2.2. Alphanumerische Telegrammadressen und Fernschreiberkennungen.....	195
4.2.3. ISO-Nummern für Publikationen.....	196
4.2.3.1. <i>International Standard Book Number</i> .....	196
4.2.3.2. <i>International Standard Serial Number</i> .....	197
4.2.4. Alphanumerische Telefonnummern – Vanity-Nummern .....	198
4.3. Rechtsnatur der Domainnamen.....	200
4.3.1. Domainnamen als technische Angaben oder klassische Namen.....	201
4.3.2. Namenschutz nach § 12 BGB.....	203
4.3.3. Markenrechtliche Implikationen .....	204
4.3.3.1. Domainnamen als Marken im Sinne § 4 MarkenG .....	204
4.3.3.2. Ansprüche nach §§ 14 und 15 MarkenG.....	205
4.3.4. Verstoß gegen das Wettbewerbsrecht .....	208
4.3.4.1. Sittenwidrige Wettbewerbshandlung, § 1 UWG .....	208

---

4.3.4.2. Irreführende Angaben, § 3 UWG .....	209
4.3.5. Verstoß gegen das Deliktsrecht.....	210
4.4. Rechtliche Verantwortung der DENIC eG .....	211
4.4.1. Exkurs 1: Vergabe von Domainnamen durch die DENIC eG .....	212
4.4.2. Exkurs 2: Hoheitlicher Belang oder Privatsache .....	215
4.4.3. Unterlassungs- und Freigabeansprüche .....	220
5. Alternativen zum jetzigen DNS.....	223
5.1. Alternativen innerhalb des DNS .....	224
5.2. Ausdehnung des DNS auf andere Systeme – ENUM.....	230
5.3. Parallel zum DNS .....	233
6. Ausblick.....	237

## II. Literaturverzeichnis

### • Kommentare – Bücher – Festschriften

- Brams, Stevens J.* Alternative Voting Systems  
*Fishburne, Peter C.* in Maisel, L. Sandy (Hrsg.)  
Political Parties and Elections in the United States:  
An Encyclopedia, Vol. 1., S. 23-31  
New York, 1991  
<http://bcn.boulder.co.us/government/approvalvote/altvote.html>.  
(zit.: *Brams/Fishburne*, Alternative Voting Systems, S.)
- Bücking, Jens* Namens- und Kennzeichenrecht im Internet (Domainrecht)  
Stuttgart, 1999  
(zit.: *Bücking*, Domainrecht, Rdnr.)
- Deutsches Institut für  
Normung e.V.* DIN-Normenheft 10  
Grundlagen der Normungsarbeit des DIN  
Berlin, 6. Auflage, 1995  
(zit.: *DIN*, DIN-Normenheft 10, DIN-Nr.)
- Gibson, William* The Difference Engine  
*Sterling, Bruce* London, 1990  
(zit.: *Gibson/Sterling*, The Difference Engine)
- Gibson, William* Neuromancer  
München, 7. Auflage, 1997  
(zit.: *Gibson*, Neuromancer)
- Harbecke, Ulrich* 50 Jahre UNO  
Bergisch Gladbach, 1995  
(zit.: *Harbecke*, 50 Jahre UNO, S.)
- Hoeren, Thomas* Rechtsfragen des Internet  
Köln, 1998  
(zit.: *Hoeren*, Rechtsfragen des Internet, S.)
- Hufen, Friedhelm* Die Grundrechte und der Vorbehalt des Gesetzes  
Wachsende Staatsaufgaben  
– sinkende Steuerungsfähigkeit des Rechts, S. 273ff.  
Baden-Baden, 1990  
(zit.: *Hufen*, Staatsaufgaben, S.)
- Koch, Frank A.* Internet-Recht  
München, 1998  
(zit.: *Koch*, Internet-Recht, S.)

---

<i>Rebmann, Kurt</i>	Münchener Kommentar
<i>Sächer, Franz Jürgen</i>	Band 5, Schuldrecht: Besonderer Teil, Teil III
<i>(Hrsg.)</i>	München 1997
	(zit.: <i>MüKo-Bearbeiter</i> , § Rdnr.)
<i>Rony, Ellen</i>	The Domain Name Handbook
<i>Rony, Peter</i>	High Stakes and Strategies in Cyberspace
	Lawrence, 1998
	(zit.: <i>Rony/Rony</i> , Domain Name Handbook, S.)
<i>Schneider, Jochen</i>	Handbuch des EDV-Rechts
	Köln, 2. Auflage, 1997
	(zit.: <i>Schneider</i> , EDV-Recht, S.)
<i>Waltermann, Jens</i>	Verantwortung im Internet
<i>Machill, Marcel</i>	Selbstregulierung und Jugendschutz
<i>(Hrsg.)</i>	Gütersloh, 2000
	(zit.: <i>Waltermann/Machill</i> , Verantwortung im Internet, S.)
<i>Wendel, Dominik</i>	Wer hat Recht im Internet
	Aachen, 1997
	(zit.: <i>Wendel</i> , Recht im Internet, S.)

- **Aufsätze – Essays**

- Ahlert, Christian* Babylon 3.0.: Die Dialektik digitaler Demokratie  
Telepolis Nr. 4344, 27. November 2000  
<http://www.heise.de/tp/deutsch/inhalt/te/4344/1.html>
- Albert, Peter G.* Eminent Domain Names  
The Struggle to Gain Control of the Internet  
16 John Marshall Journal of Computer and Information Law 781  
(1998)  
(zit.: *Albert*, 16 J. Marshall J. Computer & Info. L. 781, S.)
- Aragón, Aurora Rodríguez* Competing Telecommunications and Cyber Regulation:  
Is There a Need for Transatlantic Regulatory Framework?  
3 International Journal of Communications Law and Policy, Web-Doc 8 (1999)  
[http://www.digital-law.net/IJCLP/3\\_1999/pdf/ijclp\\_webdoc\\_8\\_3\\_1999.pdf](http://www.digital-law.net/IJCLP/3_1999/pdf/ijclp_webdoc_8_3_1999.pdf)  
(zit.: *Aragón*, 3 Int. J. Com. L. & Pol'y, Web-Doc 8, S.)
- Badura, Peter* Der Sozialstaat  
Die öffentliche Verwaltung 1989, S. 491ff.  
(zit.: *Badura*, DöV 1989, 491, S.)
- Bager, Jo* Selbstkontrolle, aber wie?  
Magazin für Computertechnik 1999, Heft 20, S. 40  
(zit.: *Bager*, c't 1999, Heft 20, S. 40)
- Bar, Francois* Interoperability and the NII: Mapping the Debate  
4 Information Infrastructure & Policy 235 (1995)  
(zit.: *Bar*, 4 Info. Inf. & Pol. 235, S.)
- Beck, Hanno* Die wettbewerbspolitische Relevanz des Internet  
Wirtschaft und Wettbewerb 1999, S. 460ff.  
(zit.: *Beck*, WuW, 1999, 460, S.)
- Benkler, Yochai* Net Regulation: Taking Stock and Looking Forward  
71 University of Colorado Law Review 1203 (2000)  
(zit.: *Benkler* 71 U. Colo. L. Rev. 1203, S.)
- Bettinger, Torsten* Der Abschlußbericht der WIPO zum  
Internet Domain Name Process  
Computer und Recht 1999, S. 445ff.  
(zit.: *Bettinger*, CR 1999, 445, S.)

---

<i>Bettinger, Torsten</i>	Kennzeichenrecht im Cyberspace: Der Kampf um die Domain-Namen Gewerblicher Rechtsschutz und Urheberrecht Int. 1997, S. 402ff. (zit.: <i>Bettinger</i> , GRUR Int. 1997, 402, S.)
<i>Bettinger, Torsten</i> <i>Freytag, Stefan</i>	Verantwortlichkeit der DENIC e.G. für rechtswidrige Domains Computer und Recht 1999, S. 28ff. (zit.: <i>Bettinger/Freytag</i> , CR 1999, 28, S.)
<i>Birkenbihl, Klaus</i>	ISOC.DE Backgrounder – Zur Rolle der Internet Society August 1998 <a href="http://www.isoc.de/presse/pre21.html">http://www.isoc.de/presse/pre21.html</a> (zit.: <i>Birkenbihl</i> , ISOC.DE Backgrounder)
<i>Bleich, Holger</i>	Digitale Distanzen Verschiedene Perspektiven auf den Raum der Räume Magazin für Computertechnik 2000, Heft 9, S. 212ff. (zit.: <i>Bleich</i> , c't 2000, Heft 9, 212, S.)
<i>Bottenschein, Florian</i>	Namensschutz bei Streitigkeiten um Internet-Domains Multimedia und Recht 2001, S. 286ff. (zit.: <i>Bottenschein</i> , MMR 2001, 286, S.)
<i>Breuer, Rüdiger</i>	Direkte und indirekte Rezeption technischer Regeln durch die Rechtsordnung Archiv des öffentlichen Rechts 101 (1976), S. 46ff. (zit.: <i>Breuer</i> , AöR 101 (1976), 46, S.)
<i>Bröhl, Georg M.</i>	Rechtliche Rahmenbedingungen für neue Informations- und Kommunikationsdienste Computer und Recht 1997, S. 73ff. (zit.: <i>Bröhl</i> , CR 1997, 73, S.)
<i>Bücking, Jens</i>	Internet-Domains Neue Wege und Grenzen des bürgerlich-rechtlichen Namensschutzes Neue Juristische Wochenschrift 1997, S. 1886ff. (zit.: <i>Bücking</i> , NJW 1997, 1886, S.)
<i>Byfield, Ted</i>	Die Einführung der Banalität Telepolis Nr. 4402, 6. Dezember 2000 <a href="http://www.heise.de/tp/deutsch/inhalt/te/4402/1.html">http://www.heise.de/tp/deutsch/inhalt/te/4402/1.html</a>
<i>Cerf, Vinton</i>	IETF and ISOC 18. Juli 1995 <a href="http://www.isoc.org/isoc/related/ietf/">http://www.isoc.org/isoc/related/ietf/</a> (zit.: <i>Cerf</i> , IETF and ISOC)

---

- Christiansen, Per* Selbstregulierung, regulatorischer Wettbewerb und staatliche Eingriffe im Internet  
Multimedia und Recht 2000, S. 123ff.  
(zit.: *Christiansen*, MMR 2000, 123, S.)
- Cook Report* ISOC's ICANN Coalition Widens Its Control  
9. September 1999  
<http://www.cookreport.com/isoccontrol.shtml>  
(zit.: *Cook Report*, ISOC's ICANN Coalition Widens Its Control, Kap.)
- Cooter, Robert D.* Decentralized Law for a Complex Economy  
23 Southwestern University Law Review 443 (1994)  
(zit.: *Cooter*, 23 SW. U.L. Rev. 443, S.)
- Crago, Patrick G.* Fundamental Rights on the Infobahn: Regulating the Delivery of Internet Related Services within the European Union  
20 Hastings International and Comparative Law Review 467 (1997)  
(zit.: *Crago*, 20 Hastings Int'l & Comp. L. Rev. 467, S.)
- Crispin, Kent* Alt-Roots, Alt-TLDs, Internet-Draft  
Mai 2001  
<http://www.icann.org/stockholm/draft-crispin-alt-roots-tlds-00.txt>  
(zit.: *Crispin*, Alt-Roots)
- Crocker, David H.* Making Standards the IETF Way  
<http://info.isoc.org/papers/standards/crocker-on-standards.html>  
1 StandardView 46 (1993)  
(zit.: *Crocker*, Standards, Kap.)
- Dane, Perry* The Maps of Sovereignty: A Meditation  
12 Cardozo Law Review 959 (1991)  
(zit.: *Dane*, 12 Cardozo L. Rev. 959, S.)
- Demmel, Annette* Vergabe und Nutzung von Vanity-Nummern  
*Skröbotz, Jan* Multimedia und Recht 1999, S. 74ff.  
(zit.: *Demmel/Skröbotz*, MMR 1999, 74, S.)
- Di Fabio, Udo* Verwaltung und Verwaltungsrecht zwischen gesellschaftlicher Selbstregulierung und staatlicher Steuerung  
Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer 56 (1997), S. 235ff.  
(zit.: *Di Fabio*, VVDSStRL 56 (1997), 235, S.)
- DiFabio, Udo* Selbstverpflichtungen der Wirtschaft  
Grenzgänger zwischen Freiheit und Zwang  
Juristen-Zeitung 1997, S. 969ff.  
(zit.: *Di Fabio*, JZ 1997, 969, S.)

- 
- Dunne, Robert L.* Deterring Unauthorized Access to Computers: Controlling Behavior in Cyberspace Through a Contract Law Paradigm  
35 Jurimetrics Journal 1 (1995)  
(zit.: *Dunne*, 35 Jurimetrics Journal 1, S.)
- Ermert, Monika* Ein Königreich für einen (Internet-)Namen  
Magazin für Computertechnik 2000, Heft 25, S. 66ff.  
(zit.: *Ermert*, c't 2000, Heft 25, 66, S.)
- Ermert, Monika* Interim-Finanzierung für Interim-Verwalter  
Telepolis Nr. 5107, 24. Juli 1999  
<http://www.heise.de/tp/deutsch/inhalt/te/5107/1.html>
- Ermert, Monika* IPv6 auf allen Kanälen  
Die Einführung des neuen IP-Standards drängt  
Magazin für Computertechnik 2000, Heft 1, S. 32f.  
(zit.: *Ermert*, c't 2000, Heft 1, 32, S.)
- Ermert, Monika* Vor ICANN sind nicht alle gleich  
Telepolis Nr. 7812, 5. Juni 2001  
<http://www.heise.de/tp/deutsch/inhalt/te/7812/1.html>
- Ernst, Steffan* Internetadressen – Der Stand der Rechtsprechung  
Multimedia und Recht 2001, S. 368ff.  
(zit.: *Ernst*, MMR 2001, 368, S.)
- Europäische Kommission* Internet Governance – Reply of the European Community and its Member States to the US Green Paper  
<http://europa.eu.int/ISPO/eif/InternetPoliciesSite/InternetGovernance/MainDocuments/ReplytoUSGreenPaper.html>  
(zit.: *Europäische Kommission*, Reply to US Green Paper)
- European Union Ministers* Ministerial declaration:  
Global Information Networks – Realising the Potential  
1997  
<http://www.echo.lu/bonn/final.html>  
(zit.: *EU*, Ministerial declaration: Global Information Networks, Rdnr.)
- Fausett, Bret A.* Want to Create a Secret Committee?  
It's Easy. Violate Your Bylaws.  
10. Mai 2000  
<http://www.lextext.com/21days.html>  
(zit.: *Fausett*, Secret Committee)

- Friedman, George H.* Alternative Dispute Resolution and Emerging Online Technologies: Challenges and Opportunities  
19 Hastings Communications and Entertainment Law Journal 695 (1997)  
(zit.: *Friedman*, 19 Hastings Comm/Ent L.J. 695, S.)
- Froomkin, A. Michael* Wrong Turn in Cyberspace:  
Using ICANN to Route around the APA and the Constitution  
50 Duke Law Journal 17 (2000)  
(zit.: *Froomkin*, 50 Duke L.J. 17, S.)
- Froomkin, Michael A.* Beware the ICANN Board Squatters  
27. Oktober 2000  
<http://personal.law.miami.edu/~froomkin/boardsquat.htm>  
(zit.: *Froomkin*, Beware the ICANN Board Squatters)
- Froomkin, Michael A.* Is ICANN's New Generation of Internet Domain Name Selection Process Thwarting Competition?  
8. Februar 2001  
<http://personal.law.miami.edu/~froomkin/articles/commerce8Jan2001.htm>  
(zit.: *Froomkin*, Thwarting Competition, Kap.)
- Froomkin, Michael A.* Replacing the ICANN Board Squatters  
9. November 2000  
<http://personal.law.miami.edu/~froomkin/boardsquat2.htm>  
(zit.: *Froomkin*, Replacing the ICANN Board Squatters)
- Gallwas, Hans-Ullrich* Die Erfüllung von Verwaltungsaufgaben durch Private Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer 29 (1971), S. 211ff.  
(zit.: *Gallwas*, VVDStRL 29 (1971), 211, S.)
- Gibbons, Llewellyn Joseph* No Regulation, Government Regulation, or Self-Regulation:  
Social Enforcement or Social Contracting for Governance in Cyberspace  
6 Cornell Journal of Law and Policy 475 (1997)  
(zit.: *Gibbons*, 6 Cornell J.L. & Pub. Pol'y 475, S.)
- Gigante, Alexander* Blackhole in Cyberspace: The Legal Void in the Internet  
15 John Marshall Journal of Computer and Information Law 413 (1997)  
(zit.: *Gigante*, J. Marshall J. Computer & Info. L. 413, S.)
- Gigante, Alexander* Ice Patch on the Information Superhighway:  
Foreign Liability for Domestically Created Content  
14 Cardozo Arts and Entertainment Law Journal 523 (1996)  
(zit.: *Gigante*, 14 Cardozo Arts & Ent. L.J. 523, S.)

- 
- Gneiting, Stefan* Strahleninferno oder Öko-funk?  
*Demmelhuber, Simon* UMTS und die Strahlendebatte  
Magazin für Computertechnik 2002, Heft 3, S. 82ff.  
(zit.: *Gneiting/Demmelhuber*, c't 2002, Heft 3, 82, S.)
- Goldfoot, Josh A.* Antitrust Implications of Internet Administration  
84 Virginia Law Review 909 (1998)  
(zit.: *Goldfoot*, 84 Va. L. Rev. 909, S.)
- Gole, Rebecca W.* Playing the Name Game  
A Glimpse at the Future of the Internet Domain Name System  
51 Federal Communications Law Journal 403 (1999)  
(zit.: *Gole*, 51 Fed. Comm. L.J. 403, S.)
- Goltzsch* Nationales Internet  
Telepolis Nr. 5833, 24. Februar 2000  
<http://www.heise.de/tp/deutsch/inhalt/te/5833/1.html>
- Goodman, Marc D.* Why the Police don't care about Computer Crime  
10 Harvard Journal of Law and Technology 465 (1997)  
(zit.: *Goodman*, 10 Harv. J.L. & Tech. 465, S.)
- Gordon, Irlam* Controlling the Internet:  
Legal and Technical Aspects of the Domain Name System  
5. Mai 1999  
<http://www.base.com/gordoni/thoughts/dns-control.html>  
(zit.: *Gordon*, Controlling the Internet, Kap.)
- Gordon, Mark L.* A Lawyer's Roadmap of the Information Superhighway  
13 John Marshall Journal of Computer & Information Law 177  
(1995)  
(zit.: *Gordon*, 13 J. Marshall J. Computer & Info. L. 177, S.)
- Graefe, Thomas* Marken und Internet  
Markenartikel 1996, S. 100ff.  
(zit.: *Graefe*, Markenartikel 1996, 100, S.)
- Graf von Bernstorff, Christoph* Ausgewählte Rechtsprobleme im Electronic Commerce  
Recht der internationalen Wirtschaft 2000, S. 14ff.  
(zit.: *Bernstorff*, RIW 2000, 14, S.)
- Grindley, Peter* Standard Wars  
*Salant, David J.* The Use of Standard Setting as a Mean of Facilitating Cartels  
*Wavermann Leonard* 3 International Journal of Communications Law and Policy, Web-Doc 2, (1999)  
[http://www.digital-law.net/IJCLP/3\\_1999/pdf/ijclp\\_webdoc\\_2\\_3\\_1999.pdf](http://www.digital-law.net/IJCLP/3_1999/pdf/ijclp_webdoc_2_3_1999.pdf)  
(zit.: *Grindley/Salant/Wavermann*, 3 Int. J. Com. L. & Pol'y, Web-Doc 2, Kap.)

- Hack, Günter* Andy Müller-Maguhn ist Sieger bei ICANN  
Telepolis Nr. 8892, 11. Oktober 2000  
<http://www.heise.de/tp/deutsch/inhalt/te/8892/1.html>
- Hanloser, Stephan* Die Internet Corporation for Assigned Names and Numbers  
(ICANN)  
Legislative, exekutive und judikative Selbstverwaltung im  
Internet  
JurPC Web-Doc 158/2000  
<http://www.jurpc.de/aufsatz/20000158.htm>  
(zit.: *Hanloser*, JurPC Web-Doc 158/2000, Abs.)
- Hardy, Trotter* The Proper Legal Regime for Cyberspace  
55 University of Pittsburgh Law Review. 993 (1994)  
(zit.: *Trotter*, 55 U. Pitt. L. Rev. 993, S.)
- Harvard Law Review Association* Developments in the Law--The Law of Cyberspace  
IV. Internet Regulation Through Architectural Modification  
The Property Rule Structure of Code Solutions  
112 Harvard Law Review 1634 (1999)  
(zit.: *HLRA*, 112 Harv. L. Rev. 1634, S.)
- Harvard Law Review Association* Developments in the Law--The Law of Cyberspace  
II. Communities Virtual and Real  
Social and Political Dynamics of Law in Cyberspace  
112 Harvard Law Review 1586 (1999)  
(zit.: *HLRA*, 112 Harv. L. Rev. 1586, S.)
- Harvard Law Review Association* Developments in the Law--The Law of Cyberspace  
V. The Domain Name System  
A Case Study of the Significance of Norms to Internet  
Governance  
112 Harvard Law Review 1657 (1999)  
(zit.: *HLRA*, 112 Harv. L. Rev. 1657, S.)
- Higgs, Simon* Alternative Roots and the Virtual Inclusive Root, Internet-Draft  
Mai 2001  
<http://www.ietf.org/internet-drafts/draft-higgs-virtual-root-00.txt>  
(zit.: *Higgs*, Alternative Roots)
- Higgs, Simon* Root Zone Definitions, Internet-Draft  
Mai 2001  
<http://www.ietf.org/internet-drafts/draft-higgs-root-defs-01.txt>  
(zit.: Higgs, Root Zone Definitions)

---

<i>Higgs, Simon</i>	Why Care About The Namespace? 17. Mai 1997 <a href="http://www.simon.higgs.com/net/why-care.html">http://www.simon.higgs.com/net/why-care.html</a> (zit.: <i>Higgs</i> , Why Care About The Namespace?)
<i>Hoeren, Thomas</i>	Vorschlag für eine EU-Richtlinie über E-Commerce Multimedia und Recht 1999, S. 192ff. (zit.: <i>Hoeren</i> , MMR 1999, 192, S.)
<i>Industry Canada</i>	Preparing Canada for a Digital World 1997 <a href="http://strategis.ic.gc.ca/SSG/ih01650e.html">http://strategis.ic.gc.ca/SSG/ih01650e.html</a> (zit.: <i>Industry Canada</i> , Digital World)
<i>Information Industries Taskforce (Australia)</i>	The Global Information Economy 1997 – Executive Summary 1997 <a href="http://www.dist.gov.au/itt/golds/html/execsumm.html">http://www.dist.gov.au/itt/golds/html/execsumm.html</a> (zit.: <i>IIT, Australia</i> , Global Information Economy, Kap.)
<i>ISO</i>	How are ISO Standards Developed? <a href="http://www.iso.ch/iso/en/aboutiso/introduction/howstdsdev.html">http://www.iso.ch/iso/en/aboutiso/introduction/howstdsdev.html</a> (zit.: <i>ISO</i> , How are ISO Standards Developed?)
<i>ISO</i>	Why is International Standardization Needed? <a href="http://www.iso.ch/iso/en/aboutiso/introduction/whyneeded.html">http://www.iso.ch/iso/en/aboutiso/introduction/whyneeded.html</a> (zit.: <i>ISO</i> , Why is International Standardization Needed?)
<i>Japan Ministry of International Trade and Industry</i>	Towards the Age of the Digital Economy Mai 1997 <a href="http://www.miti.go.jp/intro-e/a228100e.html">http://www.miti.go.jp/intro-e/a228100e.html</a> (zit.: <i>Japan</i> , Digital Economy)
<i>Johnson, David R. Post, David G.</i>	Law and Borders: The Rise of Law in Cyberspace 48 Stanford Law Review 1367 (1996) <a href="http://www.cli.org/X0025_LBFIN.html">http://www.cli.org/X0025_LBFIN.html</a> (zit.: <i>Johnson/Post</i> , 48 Stan. L. Rev. 1367, S.)
<i>Johnson, David R. Marks, Kevin A.</i>	Mapping Electronic Data Communications onto Existing Legal Metaphors: Should We Let Our Conscience (and Our Contracts) be Our Guide? 38 Villanova Law Review 487 (1993) (zit.: <i>Johnson/Marks</i> , 38 Vill. L. Rev. 487, S.)
<i>Johnson, David R. Crawford, Susan P.</i>	The Idea of ICANN <a href="http://www.icannwatch.org/archive/the_idea_of_icann.htm">http://www.icannwatch.org/archive/the_idea_of_icann.htm</a> (zit.: <i>Johnson/Crawford</i> , The Idea of ICANN)

- Johnson, David R.* What an ICANN Consensus Report Should Look Like  
*Crawford, Susan P.* [http://www.icannwatch.org/archive/what\\_icann\\_consensus\\_should\\_look\\_like.htm](http://www.icannwatch.org/archive/what_icann_consensus_should_look_like.htm)  
(zit.: *Johnson/Crawford*, ICANN Consensus Report)
- Johnson, David R.* Why Consensus Matters:  
*Crawford, Susan P.* The Theory Underlying ICANN's Mandate to Set Policy Standards for the Domain Name System  
23. August 2000  
[http://www.icannwatch.org/archive/why\\_consensus\\_matters.htm](http://www.icannwatch.org/archive/why_consensus_matters.htm)  
(zit.: *Johnson/Crawford*, Why Consensus Matters)
- Jonas, Kay-Uwe* Neue Möglichkeiten für den Kennzeichenmißbrauch?  
*Schmitz, Nicolás* Zur Einordnung von sogenannten Vanity-Rufnummern  
Gewerblicher Rechtsschutz und Urheberrecht 2000, S. 183ff.  
(zit.: *Jonas/Schmitz*, GRUR 2000, 183, S.)
- Katz, Michael L.* Network Externalities, Competition, and Compatibility  
*Shapiro, Carl* 75 American Economy Review 424 (1985)  
(zit.: *Katz/Shapiro*, 75 Am. Econ. Rev. 424, S.)
- Kilian, Matthias* Die Adresse im Internet – Domains und ihr rechtlicher Schutz  
Deutsche Zeitschrift für Wirtschaftsrecht 1997, S. 381ff.  
(zit.: *Kilian*, DZWIR 1997, 381, S.)
- King, James J.* Hütet Euch vor der UDRP  
Telepolis Nr. 8694, 9. September 2000  
<http://www.heise.de/tp/deutsch/inhalt/te/8694/1.html>
- Kleinwächter, Wolfgang* Internet Governance: ICANN „Out of Control“?  
Multimedia und Recht 1999, S. 10  
(zit.: Kleinwächter, MMR 1999, S. 10)
- Kloepfer, Michael* Selbstregulierung im Umwelt- und Technikrecht  
*Elsner, Thomas* Perspektiven einer kooperativen Normsetzung  
Deutsches Verwaltungsblatt 1996, S. 964ff.  
(zit.: *Kloepfer/Elsner*, DVBl. 1996, 964, S.)
- Koch, Hans-Joachim* Die neue Verpackungsordnung  
Neue Zeitschrift für Verwaltungsrecht 1998, S. 1155ff.  
(zit.: *Koch*, NvWZ 1998, 1155, S.)
- Koenig, Christian* Internet-Protokoll-Adressen  
*Neumann, Andreas* als Nummern im Sinne des Telekommunikationsrechts?  
Kommunikation & Recht 1999, S. 145ff.  
(zit.: *Koenig/Neumann*, K&R 1999, 145, S.)

---

<i>Köhntopp, Kristian</i>	Einheitliche Sicht – Netzwerkprotokolle im Internet Magazin für Computertechnik 1993, Heft 3, S. 232ff. (zit.: <i>Köhntopp</i> , c't 1993, Heft 3, 232, S.)
<i>Krempl, Stefan</i>	Fette Bugs im Cybercrime-Abkommen Telepolis Nr. 7239, 28. März 2001 <a href="http://www.heise.de/tp/deutsch/inhalt/te/7239/1.html">http://www.heise.de/tp/deutsch/inhalt/te/7239/1.html</a>
<i>Krempl, Stefan</i>	Filterinitiative ICRA: Wir sind die Guten Telepolis Nr. 7344, 14. April 2001 <a href="http://www.heise.de/tp/deutsch/inhalt/te/7344/1.html">http://www.heise.de/tp/deutsch/inhalt/te/7344/1.html</a>
<i>Krempl, Stephan</i>	Generalüberholung für das Internet Magazin für Computertechnik 1999, Heft 20, S. 212ff. (zit.: <i>Krempl</i> , c't Heft 20, 212, S.)
<i>Krist, Georg</i>	Die Bedeutung technischer Regelwerke des Immissionsschutzrechtes im Verwaltungsprozeß Umweltpolitik und Recht 1993, S. 178ff. (zit.: <i>Krist</i> , UPR 1993, 178, S.)
<i>Kubicek, Herbert</i>	Universaldienstleistungen in den USA und in Deutschland Computer und Recht 1997, S. 1ff. (zit.: <i>Kubicek</i> , CR 1997, 1, S.)
<i>Kuri, Jürgen</i>	Da geht's lang! Routing, oder: wie die Daten im Internet ihren Weg finden Magazin für Computertechnik 1997, Heft 6, S. 380ff. (zit.: <i>Kuri</i> , c't 1997, Heft 6, 380, S.)
<i>Kuri, Jürgen</i>	Das vernetzte Haus Von der automatischen Lichtregelung bis zum intelligenten Haus Magazin für Computertechnik 1999, Heft 22, S. 178ff. (zit.: <i>Kuri</i> , c't 1999, Heft 22, 178, S.)
<i>Kuri, Jürgen</i>	Wenn der Postmann zweimal klingelt Namen und Adressen im TCP/IP-Netzwerk und im Internet Magazin für Computertechnik 1996, Heft 12, S. 334ff. (zit.: <i>Kuri</i> , c't 1996, Heft 12, 334, S.)
<i>Ladeur, Karl-Heinz</i>	Rechtliche Regulierung von Informationstechnologien und Standardsetzung Computer und Recht 1999, S. 395ff. (zit.: <i>Ladeur</i> , CR 1999, 395, S.)
<i>Leaffer, Marshall</i>	Domain Names, Globalization and Internet Governance 6 Indiana Journal of Global Legal Studies 139 (1998) (zit.: <i>Leaffer</i> , 6 Ind. J. Global Legal Stud. 139, S.)

- Lee, Christopher S.* The Development of Arbitration in the Resolution of Internet Domain Name Disputes  
7 Richmond Journal of Law and Technology, 2 (2000)  
(zit.: *Lee*, 7 Rich. J.L. & Tech. 2, S.)
- Leiner, Barry M. u.a.* A Brief History of the Internet  
4. August 2000  
<http://www.isoc.org/internet-history/brief.html>  
(zit.: *Leiner*, u.a., A Brief History, Kap.)
- Lemley, Mark A.* Antitrust and the Internet Standardization Problem  
28 Connecticut Law Review 1041 (1996)  
(zit.: *Lemley*, 28 Conn. L. Rev. 1041, S.)
- Lemley, Mark A.* Standardizing Government  
Standard-Setting Policy for Electronic Commerce  
14 Berkeley Technology Law Journal 745 (1999)  
(zit.: *Lemley*, 14 Berkeley Tech. L.J. 745, S.)
- Lessing, Lawrence* Constitution and Code  
27 Cumberland Law Review 1 (1996-1997)  
(zit.: *Lessing*, 27 Cumb. L. Rev. 1, S.)
- Lessing, Lawrence* The Constitution of Code  
Limitations on Choice-Based Critiques of Cyberspace Regulation  
5 Common Law Conspectus 181 (1997)  
(zit.: *Lessing*, 5 CommLaw Conspectus 181, S.)
- Lessing, Lawrence* The Zones of Cyberspace  
48 Stanford Law Review 1403 (1996)  
(zit.: *Lessing*, 48 Stan. L. Rev. 1403, S.)
- Liu, Joseph P.* Legitimacy and Authority in Internet Coordination:  
A Domain Name Case Study  
74 Indiana Law Journal 587 (1999)  
(zit.: *Liu*, 74 Ind. L.J. 587, S.)
- Love, James* What You Should Know about the Hague Convention  
2. Juni 2001  
<http://www.cptech.org/ecom/jurisdiction/whatyoushouldknow.html>  
(zit.: *Love*, Hague Convention)
- Lynn, M. Stuart* Discussion Draft: A Unique, Authoritative Root for the DNS  
28. Mai 2001  
<http://www.icann.org/stockholm/unique-root-draft.htm>  
(zit.: *Lynn*, Authoritative Root)

- 
- Maennel, Frithjof A.* Elektronischer Geschäftsverkehr ohne Grenzen  
Der Richtlinienvorschlag der Europäischen Kommission  
Multimedia und Recht 1999, S. 187ff.  
(zit.: *Maennel*, MMR 1999, 187, S.)
- Maher, Marcus* An Analysis of Internet Standardization  
3 Virginia Journal of Law and Technology 5, Art. 5 (1998)  
[http://vjolt.student.virginia.edu/graphics/vol3/home\\_art5.html](http://vjolt.student.virginia.edu/graphics/vol3/home_art5.html)  
(zit.: *Maher*, 3 Va. J.L. & Tech. 5, Art. 5 Rdnr.)
- Mankowski, Peter* Wider ein transnationales Cyberlaw  
Archiv für Presserecht 1999, S. 138ff.  
(zit.: *Mankowski*, AfP 1999, 138, S.)
- Matsuura, Jeffrey H.* The Case Against Internet Law  
*Auffret, Jean-Pierre* 1998  
[http://fc.vdu.lt/Conferences/INET98/2a/2a\\_2.htm](http://fc.vdu.lt/Conferences/INET98/2a/2a_2.htm)  
(zit.: *Matsuura/Auffret*, Internet Law, Kap.)
- Mayer, Patrick* Selbstregulierung im Internet: Institutionen und Verfahren zur  
Setzung technischer Standards  
Kommunikation & Recht 2000, S. 13ff.  
(zit.: *Mayer*, K&R 2000, 13, S.)
- McGowan, David* Regulating Competition in the Information Age  
Computer Software as an Essential Facility Under the  
Sherman Act  
18 Hastings Communications and Entertainment Law Journal 771  
(1996)  
(zit.: *McGowan*, 18 Hastings Comm. & Ent. L.J. 771, S.)
- Mecklenburg, Wilhelm* Internetfreiheit  
Zeitschrift für Urheber- und Medienrecht 1997, S. 525ff.  
(zit.: *Mecklenburg*, ZUM 1997, 525, S.)
- Mestmäcker,  
Ernst-Joachim* Staat und Unternehmen im europäischen Gemeinschaftsrecht  
Zeitschrift für ausländisches und internationales Privatrecht 52  
(1988), S. 526ff.  
(zit.: *Mestmäcker*, RabelZ 52 (1988), 526, S.)
- Mewes, Heather N.* Memorandum of Understanding on the Generic Top-Level  
Domain Name Space of the Internet Domain Name System  
13 Berkeley Technology Law Journal 235 (1998)  
(zit.: *Mewes*, 13 Berkeley Tech. L.J. 235, S.)

- Meyer-Hauser, Bernhard* Preiswert, schnell und effizient:  
Domain Name-Streitigkeiten on Line regeln?
- Zuberbühler, Tobias H.* 30./31. März 2000  
<http://www.icann-studienkreis.net/zuberb.htm>  
(zit.: *Meyer-Hauser/Zuberbühler*, Domain Name-Streitigkeiten)
- Meyerson, Michael I.* Virtual Constitutions:  
The Creation of Rules for Governing Private Networks  
8 Harvard Journal of Law & Technology 129 (1994)  
(zit.: *Meyerson*, 8 Harv. J.L. & Tech. 129, S.)
- Mueller, Milton* ICANN and the Internet Governance  
Sorting through the debris of 'Self Regulation'  
1 info 6, S. 497 (1999)  
(zit.: *Mueller*, 1 info 6, 497, S.)
- Mueller, Milton* Rough Justice  
An Analysis of ICANN's Uniform Dispute Resolution Policy  
<http://dcc.syr.edu/roughjustice.htm>  
(zit.: *Mueller*, Rough Justice, Kap.)
- Mueller, Milton* Technology and Institutional Innovation: Internet Domain Names  
5 International Journal of Communications Law and Policy,  
Web-Doc 1, (2000)  
[http://www.digital-  
law.net/IJCLP/5\\_2000/pdf/ijclp\\_webdoc\\_1\\_5\\_2000.pdf](http://www.digital-law.net/IJCLP/5_2000/pdf/ijclp_webdoc_1_5_2000.pdf)  
(zit.: *Mueller*, 5 Int. J. Com. L. & Pol'y, Web-Doc 1, S.)
- Mühlbauer, Peter* Muss Deutschland bald amerikanische Copyrightstandards  
durchsetzen?  
Telepolis Nr. 7344, 19. Mai 2001  
<http://www.heise.de/tp/deutsch/inhalt/te/7676/1.html>
- Netanel, Neil Weinstock* Cyberspace Self-Governance:  
A Skeptical View from Liberal Democratic  
88 California Law Review 395 (2000)  
(zit.: *Netanel*, 88 Calif. L. Rev. 395, S.)
- Network Solutions Inc.* Enhancing Internet commerce through secure administration and  
competitive Domain Naming Service  
26. Juni 1998  
<http://netsol.com/policy/internet.pdf>  
(zit.: *NSI*, Enhancing Internet, Kap.)
- Nicklisch, Fritz* Technische Regelwerke – Sachverständigengutachten im  
Rechtssinne Neue Juristische Wochenschrift 1983, S. 841ff.  
(zit.: *Nicklisch*, NJW 1983, 841, S.)

---

<i>Nietzold</i>	Prioritätsstreit zwischen Warenzeichen und nicht registrierten Rechten Gewerblicher Rechtsschutz und Urheberrecht 1925, S. 1ff. (zit.: <i>Nietzold</i> , GRUR 1925, 1, S.)
<i>Noll, Alfons A. E.</i>	The International Telecommunication Union (ITU) Its Inception, Evolution and Innate, Constant Reform Process Multimedia und Recht 1999, S. 465ff. (zit.: <i>Noll</i> , MMR 1999, 465, S.)
<i>Nordemann, Axel</i>	Internet-Domains und zeichenrechtliche Kollisionen Neue Juristische Wochenschrift 1997, S. 1891ff. (zit.: <i>Nordemann</i> , NJW 1997, 1891, S.)
<i>Omsels, Hermann-Josef</i>	Die Kennzeichenrechte im Internet Gewerblicher Rechtsschutz und Urheberrecht 1997, S. 328ff. (zit.: <i>Omsels</i> , GRUR 1997, 328, S.)
<i>Ossenbühl, Fritz</i>	Die Freiheit des Unternehmers nach dem Grundgesetz Archiv des öffentlichen Rechts 115 (1990), S. 1ff. (zit.: <i>Ossenbühl</i> , AÖR 115 (1990), 1, S.)
<i>Osthause, Wolf</i>	Die Renaissance des Privatrechts im Cyberspace Archiv für Presserecht 2001, S. 13ff. (zit.: <i>Osthause</i> , AfP 2001, 13, S.)
<i>Paloubis, Christos</i>	IuKDG und Mediendienste-Staatsvertrag 1997 <a href="http://www.internetrecht-info.de/archiv/multime.htm">http://www.internetrecht-info.de/archiv/multime.htm</a> (zit.: <i>Paloubis</i> , IuKDG u. MDStV)
<i>Perritt Jr., Henry H.</i>	Dispute Resolution in electronic network communities 38 Villanova Law Review 349 (1993) (zit.: <i>Perritt</i> , 38 Vill. L. Rev. 349, S.)
<i>Perritt Jr., Henry H.</i>	Jurisdiction in Cyberspace 41 Villanova Law Review 1 (1996) (zit.: <i>Perritt</i> , 41 Vill. L. Rev. 1, S.)
<i>Perritt, Henry H. Jr.</i>	Cyberspace Self-Government: Town Hall Democracy or Rediscovered Royalism? 12 Berkeley Technology Law Journal 413 (1997) (zit.: <i>Perritt</i> , Berkeley Tech. L.J. 413, S.)
<i>Post, David</i>	Anarchy, State and Internet 1995 Journal of Online Law, Artikel 3 <a href="http://www.wm.edu/law/publications/jol/articles/post.shtml">http://www.wm.edu/law/publications/jol/articles/post.shtml</a> (zit.: <i>Post</i> , 1995 J. Online L., Artikel 3, Nr.)

- Post, David G.* Governing Cyberspace  
6. Juni 1999  
[http://www.icannwatch.org/archive/governing\\_cyberspace.htm](http://www.icannwatch.org/archive/governing_cyberspace.htm)  
(zit.: *Post*, Governing Cyberspace)
- Post, David G.* ICANN and Independent Review  
August 1999  
[http://www.icannwatch.org/archive/icann\\_and\\_independent\\_review.htm](http://www.icannwatch.org/archive/icann_and_independent_review.htm)  
(zit.: *Post*, ICANN and Independent Review)
- Post, David G.* ICANN and the Consensus of the Internet Community  
20. August 1999  
[http://www.icannwatch.org/archive/icann\\_and\\_the\\_consensus\\_of\\_the\\_community.htm](http://www.icannwatch.org/archive/icann_and_the_consensus_of_the_community.htm)  
(zit.: *Post*, ICANN and the Consensus)
- Recke, Martin* Identität zu verkaufen  
Probleme und Entwicklungsoptionen des Internet Domain Name Service  
<http://duploxx.wz-berlin.de/texte/dns/index.html>  
(zit.: *Recke*, DNS, Kap.)
- Reidenberg, Joel R.* Governing Networks and Rule-Making in Cyberspace  
45 Emory Law Journal 911 (1996)  
(zit.: *Reidenberg*, Emory L.J. 911, S.)
- Reidenberg, Joel R.* Lex Informatica:  
The Formulation of Information Policy Rules through Technology  
76 Texas Law Review 553 (1998)  
(zit.: *Reidenberg*, 76 Tex. L. Rev. 553, S.)
- Resnick, Paul* Filtering Information on the Internet  
1997  
<http://www.sciam.com/0397/0397resnick.html>  
(zit.: *Resnick*, Filtering Information, Kap.)
- Röger, Ralf* Internet und Verfassungsrecht  
Zeitschrift für Rechtspolitik 1997, S. 203ff.  
(zit.: *Röger*, ZRP 1997, 203, S.)
- Roßnagel, Alexander* Globale Datennetze  
Ohnmacht des Staates – Selbstschutz der Bürger  
Zeitschrift für Rechtspolitik 1997, S. 26ff.  
(zit.: *Roßnagel*, ZRP 1997, 26, S.)

- 
- Roth, Wulf-Henning* Eingetragene Genossenschaft  
Zeitschrift für Genossenschaftsrecht 1992, S. 367ff.  
(zit.: *Roth*, ZfG 1992, 367, S.)
- Rötzer, Florian* Das Internetvolk hat gewählt: in Europa haben zwei Deutsche gewonnen  
Telepolis Nr. 8696, 9. September 2000  
<http://www.heise.de/tp/deutsch/inhalt/te/8696/1.html>
- Rötzer, Florian* Taliban bauen weiter an der Abschließung des Landes  
Telepolis, Nr. 9082, 13. Juli 2001  
<http://www.heise.de/tp/deutsch/inhalt/te/9082/1.html>
- Rowland, Diane* Cyberspace – A Contemporary Utopia?  
The Journal of Information, Law and Technology 1998, Issue 3  
<http://elj.warwick.ac.uk/jilt/98-3/rowland.html>  
(zit.: *Rowland*, IJLT 1998 (3), Kap.)
- Rutkowski, Anthony M.* Testimony Before the Committee on Commerce  
U.S. House of Representatives  
10. Juni 1998  
<http://www.ngi.org/pub/amr-testimony.htm>  
(zit.: *Rutkowski*, Testimony Before the Committee on Commerce)
- Rutkowski, Anthony M.* Today's Cooperative Competitive Standards Environment For  
Open Information and Telecommunication Networks and the  
Internet Standards-Making Model  
<http://info.isoc.org/papers/standards/amr-on-standards.html>  
(zit.: *Rutkowski*, Standards, Kap.)
- Scheuner, Ulrich* Die staatliche Intervention im Bereich der Wirtschaft  
Veröffentlichungen der Vereinigung der Deutschen  
Staatsrechtslehrer 11 (1954), S. 1ff.  
(zit.: *Scheuner*, VVDStRL 11 (1954), 1, S.)
- Schmidt-Preuß, Matthias* Soziale Marktwirtschaft und Grundgesetz vor dem Hintergrund  
des Staatsvertrags zur Währungs-, Wirtschafts- und  
Sozialunion  
Deutsches Verwaltungsblatt 1993, S. 236ff.  
(zit.: *Schmidt-Preuß*, DVBl. 1993, 236, S.)
- Schmidt-Preuß, Matthias* Verwaltung und Verwaltungsrecht zwischen gesellschaftlicher  
Selbstregulierung und staatlicher Steuerung  
Veröffentlichungen der Vereinigung der Deutschen  
Staatsrechtslehrer 56 (1997), S. 160ff.  
(zit.: *Schmidt-Preuß*, VVDStRL 56 (1997), 160, S.)

- Schneider, Michael* Domain- und Namensrecht  
6. November 1996  
<http://www.anwalt.de/publicat/seyb9611.htm>  
(zit.: *Schneider*, Domain- und Namensrecht)
- Sietmann, Richard* Nummernspiele  
Ressourcenkonflikte um Namen und Adressen bleiben ein Politikum  
Magazin für Computertechnik 1999, Heft 9, S. 180ff.  
(zit.: *Sietmann*, c't 1999, Heft 9, 180, S.)
- Simon, Michaela* Schön schimpfen  
Telepolis Nr. 8447, 27. Juli 2000  
<http://www.heise.de/tp/deutsch/inhalt/te/8447/1.html>
- Steigleder, Thomas* Möglichkeiten der Selbstregulierung im Bereich naturwissenschaftlich-technischer Forschung  
Wissenschaftsrecht 33 (2000), S. 111ff.  
(zit.: *Steigleder*, WissR 33 (2000), 111, S.)
- Stein, Allen R.* The Unexceptional Problem of Jurisdiction in Cyberspace  
32 International Lawyer 1167 (1998)  
(zit.: *Stein*, 32 Int'l Law. 1167, S.)
- Strömer, Tobias* Anmerkung zu LG Lüneburg vom 29.1.1997  
Computer und Recht 1997, S. 290  
(zit.: *Strömer*, CR 1997, 290)
- Strömer, Tobias H.* Das ICANN-Schiedsverfahren – Königsweg bei Domainstreitigkeiten  
Mai/Juni 2001  
<http://www.netlaw.de/newsletter/news0103/icann.htm>  
(zit.: *Strömer*, ICANN-Schiedsverfahren)
- Tetley, William* The General Maritime Law -- The Lex Maritima  
20 Syracuse Journal of International Law and Commerce S. 105 (1994)  
(zit.: *Tetley*, 20 Syracuse J. Int'l L. & Com. 105, S.)
- Thatch, David* Personal jurisdiction and the World-Wide Web  
23 Rutgers Computer and Technology Law Journal 143 (1997)  
(zit.: *Thatch*, 23 Rutgers Computer & Tech. L.J. 143, S.)
- US Department of Commerce* Improvement of Technical Management of Internet Names and Addresses
- National Telecommunications and Information Administration* 63 Federal Register 8826 (1998)  
<http://www.ntia.doc.gov/ntiahome/domainname/022098fedreg.htm>  
(zit.: *US-DoC, NTIA*, Green Paper, 63 Fed. Reg. 8826, S.)

---

<i>US Department of Commerce</i>	Management of Internet Names and Addresses White Paper
<i>National Telecommunications and Information Administration</i>	63 Federal Register 31741 (1998) <a href="http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm">http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm</a> (zit.: <i>US-DoC, NTIA</i> , White Paper, 63 Fed. Reg. 31741, S.)
<i>US Department of Commerce</i>	Notice of a Cooperative Agreement with EDUCAUSE for Management of .edu Domain Name Space
<i>National Telecommunications and Information Administration</i>	6. April 2001 <a href="http://www.ntia.doc.gov/ntiahome/frnotices/edunoi41101.htm">http://www.ntia.doc.gov/ntiahome/frnotices/edunoi41101.htm</a> (zit.: <i>US-DoC, NTIA</i> , Cooperative Agreement with EDUCAUSE)
<i>US Department of Commerce</i>	Request for Comments on the Registration and Administration of Internet Domain Names
<i>National Telecommunications and Information Administration</i>	62 Federal Register 35896 (1997) <a href="http://www.ntia.doc.gov/ntiahome/domainname/DN5NOTIC.htm">http://www.ntia.doc.gov/ntiahome/domainname/DN5NOTIC.htm</a> (zit.: <i>US-DoC, NTIA</i> , RFC, 62 Fed. Reg. 35896, S. )
<i>US General Accounting Office</i>	Department of Commerce: Relationship with the Internet Corporation for Assigned Names and Numbers 7. Juli 2000 <a href="http://www.gao.gov/new.items/og00033r.pdf">http://www.gao.gov/new.items/og00033r.pdf</a> (zit.: <i>US GAO</i> , Report, S.)
<i>US White House</i>	A Framework for Global Electronic Commerce 1. Juli 1997 <a href="http://www.doc.gov/ecommerce/framewrk.htm">http://www.doc.gov/ecommerce/framewrk.htm</a> (zit.: <i>US-White House</i> , Framework, Kap.)
<i>Vetter, Tobias</i>	Die Geschichte des Internets 25. August 2000 <a href="http://www.phil-fak.uni-duesseldorf.de/mmedia/web/index2.html">http://www.phil-fak.uni-duesseldorf.de/mmedia/web/index2.html</a> (zit.: <i>Vetter</i> , Geschichte des Internets)
<i>Völker, Stefan</i> <i>Weidert, Stefan</i>	Domain-Namen im Internet Wettbewerb in Recht und Praxis 1997, S. 652ff. (zit.: <i>Völker/Weidert</i> , WRP 1997, 652, S.)
<i>Voßkuhle, Andreas</i>	„Schlüsselbegriffe“ der Verwaltungsrechtsreform Verwaltungsarchiv 92 (2001), S. 184ff. (zit.: <i>Voßkuhle</i> , VerwArch 92 (2001), 184, S.)

- W3C* World Wide Web Consortium Process Document  
1999  
[http://www.w3.org/Consortium/Process/Process-19991111/  
process.html](http://www.w3.org/Consortium/Process/Process-19991111/process.html)  
(zit.: *W3C*, WWW Consortium Process Document, Kap.)
- Wegner, Ralf* Der rechtliche Schutz von Internetdomains  
Computer und Recht 1999, S. 250ff.  
(zit.: *Wegner* CR 1999, 250, S.)
- Weihrich, Thomas* Filofax fürs Internet – Der Domain Name Service von TCP/IP  
Magazin für Computertechnik 1997, Heft 10, S. 346ff.  
(zit.: *Weihrich*, c't 1997, Heft 10, S. 346, S.)
- Weinberg, Jonathan* ICANN and the Problem of Legitimacy  
50 Duke Law Journal 187 (2000)  
(zit.: *Weinberg*, 50 Duke L.J. 187, S.)
- Weinberg, Jonathan* Review of the Domain Name Supporting Organization  
2000  
[http://www.law.wayne.edu/weinberg/dns\\_review.htm](http://www.law.wayne.edu/weinberg/dns_review.htm)  
(zit.: *Weinberg*, Review of DNSO, Kap.)
- Wenning, Rigo* Der große Streit um Internet-Domain-Namen  
JurPC Web-Doc 31/1998  
<http://www.jurpc.de/aufsatz/19980031.htm>  
(zit.: *Wenning*, JurPC Web-Doc 31/1998, Abs.)
- Werle, Raymund* The Internet Society and its Struggle for Recognition and  
*Leib, Volker* Influence  
Oktober 1999  
[www.mpi-fg-koeln.mpg.de/projekt\\_dir/wevl\\_internet/ISOC.pdf](http://www.mpi-fg-koeln.mpg.de/projekt_dir/wevl_internet/ISOC.pdf)  
(zit.: *Werle/Leib*, The Internet Society, S.)
- Wertheimer, Ludwig* Der Schutz der Telegramm-Adresse  
Gewerblicher Rechtsschutz und Urheberrecht 1907, S. 348ff.  
(zit.: *Wertheimer*, GRUR 1907, 348, S.)
- White, Harold M.* The Impact of New Communication Technologies on  
*Lauria, Rita* International Telecommunication Law and Policy:  
Cyberspace and the Restructuring of the International  
Telecommunication Union  
32 California Western Law Review 1 (1995)  
(zit.: *White/Lauria*, 32 Cal. W. L. Rev. 1, S.)
- WIPO* Final Report of the WIPO Internet Domain Name Process  
30. April, 1999  
<http://wipo2.wipo.int/process1/report/index.html>  
(zit. : *WIPO*, Final Report)

Interim Report of the Second WIPO Internet Domain Name  
Process

12. April 2001

<http://wipo2.wipo.int/process2/rfc/rfc3/index.html>

(zit.: *WIPO*, Interim Report – Second Process)

Jurisdiction and the Internet: Fundamental Fairness in the  
Networked World of Cyberspace

6 Albany Law Journal of Science and Technology 339 (1996)

(zit.: *Zembek*, 6 Alb. L.J. Sci. & Tech. 339, S.)

- **Zeitungsa**rtikel – Online-News

Zitierweise: *Herausgeber*, Titel, Datum

- |                                       |  |
|---------------------------------------|--|
| Afilias                               | Afilias Announces Opening Day<br>1. Oktober 2001<br><a href="http://www.afilias.info/news/press_releases/pr_articles/2001-10-01-01">http://www.afilias.info/news/press_releases/pr_articles/2001-10-01-01</a>  |
| Afilias                               | Afilias Opens .info Registrations to General Public<br>12. September 2001<br><a href="http://www.afilias.info/news/press_releases/pr_articles/2001-09-12-01">http://www.afilias.info/news/press_releases/pr_articles/2001-09-12-01</a>   |
| Afilias                               | Afilias Announces Sunrise Period<br>25. Juli 2001<br><a href="http://www.afilias.info/news/press_releases/pr_articles/2001-07-25-01">http://www.afilias.info/news/press_releases/pr_articles/2001-07-25-01</a>   |
| Buigues/Urrutia                       | Les enjeux pour la concurrence des marchés liés à Internet et au commerce électronique<br>Gazette Européenne Nr. 24, Juni 2000, S. 6   |
| CENTR                                 | European ccTLD Registries Respond to ICANN Invoices<br>5. Juni 2000<br><a href="http://www.centr.org/docs/press/20000605-icann.html">http://www.centr.org/docs/press/20000605-icann.html</a>   |
| Cnet                                  | Magaziner : Domain consensus possible  |
| Kornblum, Janet                       | 5. Juni 1998<br><a href="http://news.cnet.com/news/0,10000,0-1005-200-330007,00.html">http://news.cnet.com/news/0,10000,0-1005-200-330007,00.html</a>  |
| Cook Report                           | ISOC's ICANN Coalition Widens Its Control<br>9. September 1999<br><a href="http://www.cookreport.com/isoccontrol.shtml">http://www.cookreport.com/isoccontrol.shtml</a>  |
| Handelsblatt-Online<br>Kupilas, Bernd | Netzdemokraten kämpfen um ihren Einfluss bei ICANN<br>4. Februar 2001<br><a href="http://www.handelsblatt.com/hbiwwwangebot/fn/relhbi/sfn/buildhbi/cn/bp_artikel/STRUCID/PAGE_200013/PAGEID/PAGE_200052/docid/379509/SH/0/depot/0/">http://www.handelsblatt.com/hbiwwwangebot/fn/relhbi/sfn/buildhbi/cn/bp_artikel/STRUCID/PAGE_200013/PAGEID/PAGE_200052/docid/379509/SH/0/depot/0/</a> |
| Heise-Newsticker                      | Neue Domain .name im Netz<br>16. Januar 2002<br><a href="http://www.heise.de/newsticker/data/wst-16.01.02-005/">http://www.heise.de/newsticker/data/wst-16.01.02-005/</a>  |

---

Heise-Newsticker	.eu kommt – sicher, aber langsam ... 28. Juni 2001 <a href="http://www.heise.de/newsticker/data/hob-28.06.01-000/">http://www.heise.de/newsticker/data/hob-28.06.01-000/</a>
Heise-Newsticker	AOL Time Warner gegen Harry Porter Fanseiten, Warner lenkt im Streit um Harry-Potter-Sites ein 19. März 2001 <a href="http://www.heise.de/newsticker/data/hag-19.03.01-000/">http://www.heise.de/newsticker/data/hag-19.03.01-000/</a>
Heise-Newsticker	China: Nur offizielle Nachrichten im Web 7. November 2000 <a href="http://www.heise.de/newsticker/data/cp-07.11.00-002/">http://www.heise.de/newsticker/data/cp-07.11.00-002/</a>
Heise-Newsticker	Der ICANN-Wahlkampf läuft an 21. September 2000 <a href="http://www.heise.de/newsticker/data/chr-21.09.00-004/">http://www.heise.de/newsticker/data/chr-21.09.00-004/</a>
Heise-Newsticker	Die ICANN hat einen neuen Präsidenten 24. Januar 2001 <a href="http://www.heise.de/newsticker/data/jk-24.01.01-003/">http://www.heise.de/newsticker/data/jk-24.01.01-003/</a>
Heise-Newsticker	Domain-Namen auf Chinesisch 10. November 2000 <a href="http://www.heise.de/newsticker/data/jk-10.11.00-004/">http://www.heise.de/newsticker/data/jk-10.11.00-004/</a>
Heise-Newsticker	eBook-Hacker nach Vortrag festgenommen 17. Juli 2001 <a href="http://www.heise.de/newsticker/data/daa-17.07.01-003/">http://www.heise.de/newsticker/data/daa-17.07.01-003/</a>
Heise-Newsticker	EU-Kommission warnt vor Alleingang bei .eu-Domains 5. Juni 2001 <a href="http://www.heise.de/newsticker/data/em-05.06.01-000/">http://www.heise.de/newsticker/data/em-05.06.01-000/</a>
Heise-Newsticker	Gewählte ICANN-Direktoren stehen zur Disposition 9. November 2000 <a href="http://www.heise.de/newsticker/data/jk-09.11.00-002/">http://www.heise.de/newsticker/data/jk-09.11.00-002/</a>
Heise-Newsticker	Hintergrund: Der Ärger mit den Domain-Namen 19. November 2000 <a href="http://www.heise.de/newsticker/data/jk-19.11.00-003/">http://www.heise.de/newsticker/data/jk-19.11.00-003/</a>
Heise-Newsticker	Hyperlink-Patent: British Telecom macht ernst 17. Dezember 2000 <a href="http://www.heise.de/newsticker/data/jk-17.12.00-001/">http://www.heise.de/newsticker/data/jk-17.12.00-001/</a>
Heise-Newsticker	ICANN startet Studie zur Mitbestimmung durch Internet-Nutzer 28. Januar 2001 <a href="http://www.heise.de/newsticker/data/jk-28.01.01-006/">http://www.heise.de/newsticker/data/jk-28.01.01-006/</a>

- Heise-Newsticker ICANN: Hitzige Diskussionen über neue Domain-Namen  
16. November 2000  
<http://www.heise.de/newsticker/data/jk-16.11.00-006/>
- Heise-Newsticker ICANN-Bericht: Keine Chance für Sex- und Kids-Domain  
10. November 2000  
<http://www.heise.de/newsticker/data/jk-10.11.00-008/>
- Heise-Newsticker ICANN-Fachgruppe gegen neue Verträge zu .com-Domain  
29. März 2001  
<http://www.heise.de/newsticker/data/jk-29.03.01-001/>
- Heise-Newsticker ICANNs Mann in Europa  
22. Januar 2001  
<http://www.heise.de/newsticker/data/jk-22.01.01-004/>
- Heise-Newsticker ICANNs Verhältnis zu Länder-Domains ungeklärt  
16. Juni 2000  
<http://www.heise.de/newsticker/data/jk-16.06.00-000/>
- Heise-Newsticker Internet-Explorer-Beta mit Smart Tags  
26. Juni 2001  
<http://www.heise.de/newsticker/data/jo-26.06.01-001/>
- Heise-Newsticker Komitee für die Organisierung der ICANN-Mitglieder gegründet  
13. November 2000  
<http://www.heise.de/newsticker/data/jk-13.11.00-003/>
- Heise-Newsticker Länder-Domain .tv kostete 50 Millionen US-Dollar  
9. April 2000  
<http://www.heise.de/newsticker/data/jk-09.04.00-002/>
- Heise-Newsticker Neue Top Level Domains – die EU will genau wissen  
3. Dezember 2000  
<http://www.heise.de/newsticker/data/jk-03.12.00-001/>
- Heise-Newsticker new.net forciert unautorisierte Top-Level-Domains  
9. April 2001  
<http://www.heise.de/newsticker/data/wst-09.04.01-003/>
- Heise-Newsticker Niederlage für Ferrero im Streit um "Kinder.at"  
18. Dezember 2001  
<http://www.heise.de/newsticker/data/psz-18.12.01-000/>
- Heise-Newsticker Rückschlag für Ferrero im „kinder.at“-Markenstreit  
15. Januar 2001  
<http://www.heise.de/newsticker/data/psz-15.01.01-000/>
- Heise-Newsticker Sieben neue Top Level Domains beschlossen  
17. November 2000  
<http://www.heise.de/newsticker/data/jk-17.11.00-000/>

---

Heise-Newsticker	Vereinigung europäische Registrare will .eu-Registry 13. Januar 2001 <a href="http://www.heise.de/newsticker/data/jk-13.01.01-004/">http://www.heise.de/newsticker/data/jk-13.01.01-004/</a>
Heise-Newsticker	Verfahren gegen eBook-Hacker eröffnet 29. August 2001 <a href="http://www.heise.de/newsticker/data/daa-29.08.01-000/">http://www.heise.de/newsticker/data/daa-29.08.01-000/</a>
Heise-Newsticker	Wer kontrolliert die Länder-Domains? 14. März 2001 <a href="http://www.heise.de/newsticker/data/jk-14.03.01-004/">http://www.heise.de/newsticker/data/jk-14.03.01-004/</a>
Heise-Newsticker	WIPO rügt Deutsche Welle wegen Reverse Domain Hijacking 20. Januar 2001 <a href="http://www.heise.de/newsticker/data/fr-20.01.01-001/">http://www.heise.de/newsticker/data/fr-20.01.01-001/</a>
Heise-Newsticker	WIPO schlägt Schlichtungsstellen für Länder-Domains vor 4. März 2001 <a href="http://www.heise.de/newsticker/data/jk-04.03.01-005/">http://www.heise.de/newsticker/data/jk-04.03.01-005/</a>
Heise-Newsticker	WIPO will strikteren Namensschutz im Web 18. April 2001 <a href="http://www.heise.de/newsticker/data/jk-18.04.01-009/">http://www.heise.de/newsticker/data/jk-18.04.01-009/</a>
ICANN Channel	NAIS-Gruppe plant At-Large-Studie 5. Februar 2001 <a href="http://www.icannchannel.de/2001_02_04_news.htm#2247271">http://www.icannchannel.de/2001_02_04_news.htm#2247271</a>
ICANN-Announcement	ICANN Accredits New Top-Level Domains .biz and .info Registration Process to Begin this Summer 15. Mai 2001 <a href="http://www.icann.org/announcements/icann-pr15may01.htm">http://www.icann.org/announcements/icann-pr15may01.htm</a>
ICANN-Announcement	ICANN and U.S. Government Agree to Extend Agreements 4. September 2000 <a href="http://www.icann.org/announcements/icann-pr04sep00.htm">http://www.icann.org/announcements/icann-pr04sep00.htm</a>
ICANN-Announcement	ICANN Announces Decision on Registry Agreement for .com/.net/.org Domains 2. April 2001 <a href="http://www.icann.org/announcements/icann-pr02apr01.htm">http://www.icann.org/announcements/icann-pr02apr01.htm</a>
ICANN-Announcement	ICANN Names Competitive Domain-Name Registrars 21. April 1999 <a href="http://www.icann.org/announcements/icann-pr21apr99.htm">http://www.icann.org/announcements/icann-pr21apr99.htm</a>
ICANN-Announcement	Two New Top-Level Domains for the Internet: .biz and.info to be Activated Tomorrow 26. Juni 2001 <a href="http://www.icann.org/announcements/icann-pr26jun01.htm">http://www.icann.org/announcements/icann-pr26jun01.htm</a>

---

- ICANN-Announcement ICANN and VeriSign Sign on the Dotted Line  
25. Mai 2001  
<http://www.icann.org/announcements/icann-pr25may01.htm>
- ICANNWatch .ph Dispute Escalates: Government, ICANN to be Involved  
20. April 2001  
<http://www.icannwatch.org/article.php?sid=116>
- ICB Toll Free Internet and Public Domain at Risk  
Love, James 20. Juni 2001  
<http://www.icbtollfree.com/article.cfm?articleId=5353>
- Internet Intern NSI unter Beschuß  
Intern 17. November 1999  
<http://www.intern.de/99/29/53.shtml>
- ITU 80 Organizations Sign MoU to Restructure the Internet  
1. Mai 1997  
<http://www.itu.int/newsarchive/press/releases/1997/itu-08.html>
- ITU Changes to Internet Domain Names will Encourage Competition,  
Foster Growth and Stability  
29. April 1997  
<http://www.itu.int/newsarchive/press/releases/1997/itu-07.html>
- Nettime Maverick Registries Threaten an Internet Monopoly  
Crysler, Julie 14. Januar 1997  
<http://www.nettime.org/nettime.w3archive/199701/msg00021.html>
- Network World IETF Spec Could Propel Internet Telephony  
Marsan, Carolyn Duffy 2. Oktober 2000  
<http://www.nwfusion.com/news/2000/1002enum.html>
- Neulevel Press Release .bis goes live  
Neulevel Press Release 7. November 2001  
[http://www.neulevel.biz/press/press\\_release/pr\\_archive\\_2000\\_2001/2001.11.07.html](http://www.neulevel.biz/press/press_release/pr_archive_2000_2001/2001.11.07.html)
- TBTF ICANN Journal 1  
the roving\_reporter 10. September 2000  
[http://www.tbtf.com/roving\\_reporter/icann1.html](http://www.tbtf.com/roving_reporter/icann1.html)
- TBTF TBTF for 1998-02-02: Lie down with trains  
Dawson, Keith US Government green paper on domain names  
2. Februar 1998  
<http://www.tbtf.com/archive/0138.html#s01>

---

TechWeb Maclachlan, Malcolm	Analysts Cautious But Positive On Green Paper 2. Februar 1998 <a href="http://content.techweb.com/wire/story/domnam/TWB19980202S0014">http://content.techweb.com/wire/story/domnam/ TWB19980202S0014</a>
TechWeb Craig, Andrew	European Commission OKs Domain Proposal 30. Juli 1998 <a href="http://content.techweb.com/wire/story/TWB19980729S0013">http://content.techweb.com/wire/story/TWB19980729S0013</a>
TechWeb Mosquera, Mary	Groups Build Unity, Lay Down Swords 3. Juli 1998 <a href="http://content.techweb.com/wire/story/TWB19980703S0003">http://content.techweb.com/wire/story/TWB19980703S0003</a>
TechWeb Krochmal, Mo	Magaziner, Lessig Spar Over Domain Name Plan 11. Juni 1998 <a href="http://content.techweb.com/wire/story/TWB19980611S0009">http://content.techweb.com/wire/story/TWB19980611S0009</a>
TechWeb Borland, John	Registrars Applaud New Domain Name Policy 5. Juni 1998 <a href="http://content.techweb.com/wire/story/TWB19980605S0013">http://content.techweb.com/wire/story/TWB19980605S0013</a>
The Wall Street Journal Mossberg, Walter S.	New Windows XP Feature Can Re-Edit Others' Sites 7. Juni 2001 <a href="http://public.wsj.com/sn/y/SB991862595554629527.html">http://public.wsj.com/sn/y/SB991862595554629527.html</a>
UnixInsider Lawton, George	New Top-level Domains Promise Descriptive Names September 1996 <a href="http://www.unixinsider.com/swol-09-1996/swol-09-domain.html">http://www.unixinsider.com/swol-09-1996/swol-09-domain.html</a>
UnixInsider Mills, Elinor	Proposal for new Internet Organization goes Public September 1998 <a href="http://sw.itworld.com/swol-09-1998/swol-09-if.html">http://sw.itworld.com/swol-09-1998/swol-09-if.html</a>
UnixInsider Essick, Kristi	Steps Made in Formation of new Domain Name Organization August 1998 <a href="http://www.unixinsider.com/swol-08-1998/swol-08-if.html">http://www.unixinsider.com/swol-08-1998/swol-08-if.html</a>
VNUNet, Geralds, John	Wap Patent 'Owner' Extends Licence Deadline 7. Juni 2000 <a href="http://www.vnunet.com/News/1105878">http://www.vnunet.com/News/1105878</a>
Wired McKay, Niall	New Internet Government Forged 17. September 1998 <a href="http://www.wired.com/news/print/0,1294,14795,00.html">http://www.wired.com/news/print/0,1294,14795,00.html</a>
ZDNet Broersma, Matthew	Domain Plan Draws Industry Reaction 5. Juni 1998 <a href="http://www.zdnet.com/zdnn/stories/zdnn_display/0,3440,2110359,00.html">http://www.zdnet.com/zdnn/stories/zdnn_display/ 0,3440,2110359,00.html</a>

- **Internetstandards**

Zitierweise: *RFC Nr.*, Autor, Kapitel

- RFC 204 Postel, Jon  
Sockets in use  
<http://www.rfc-editor.org/rfc/rfc204.txt>, August 1971
- RFC 349 Postel, Jon  
Proposed Standard Socket Numbers  
<http://www.rfc-editor.org/rfc/rfc349.txt>, Mai 1972
- RFC 768 Postel, Jon  
User Datagram Protocol  
<http://www.rfc-editor.org/rfc/rfc768.txt>, August 1980
- RFC 791 Postel, Jon  
Internet Protocol  
<http://www.rfc-editor.org/rfc/rfc791.txt>, September 1981
- RFC 792 Postel, Jon  
Internet Control Message Protocol  
<http://www.rfc-editor.org/rfc/rfc792.txt>, September 1981
- RFC 793 Postel, Jon  
Transmission Control Protocol.  
<http://www.rfc-editor.org/rfc/rfc793.txt>, September 1981
- RFC 821 Postel, Jon  
Simple Mail Transfer Protocol  
<http://www.rfc-editor.org/rfc/rfc821.txt>, August 1982
- RFC 854 Postel, Jon / Reynolds, Joyce K.  
Telnet Protocol Specification  
<http://www.rfc-editor.org/rfc/rfc854.txt>, Mai 1983
- RFC 959 Postel, Jon / Reynolds, Joyce K.  
File Transfer Protocol (FTP)  
<http://www.rfc-editor.org/rfc/rfc959.txt>, Oktober 1995
- RFC 1034 P. Mockapetris  
Domain Names – Concepts and Facilities  
<http://www.rfc-editor.org/rfc/rfc1034.txt>, November 1987
- RFC 1055 Romkey, J.  
A Nonstandard for Transmission of IP Datagrams over Serial Lines: SLIP  
<http://www.rfc-editor.org/rfc/rfc1055.txt>, Juni 1988

- 
- RFC 1134 Perkins, D.  
The Point-to-Point Protocol  
<http://www.rfc-editor.org/rfc/rfc1134.txt>, November 1989
- RFC 1144 Van Jacobson  
Compressing TCP/IP Headers for Low-Speed Serial Links  
<http://www.rfc-editor.org/rfc/rfc1144.txt>, Februar 1990
- RFC 1150 Malkin, Gary Scott / Reynolds, Joyce K.  
F.Y.I. on F.Y.I.  
<http://www.rfc-editor.org/rfc/rfc1150.txt>, März 1990
- RFC 1160 Cerf, Vinton G.  
The Internet Activities Board  
<http://www.rfc-editor.org/rfc/rfc1160.txt>, Mai 1990
- RFC 1331 Simpson, William Allen  
The Point-to-Point Protocol (PPP)  
<http://www.rfc-editor.org/rfc/rfc1331.txt>, Mai 1992
- RFC 1535 Gavron, Ehud  
A Security Problem and Proposed Correction With Widely Deployed DNS  
Software  
<http://www.rfc-editor.org/rfc/rfc1535.txt>, Oktober 1993
- RFC 1591 Postel, Jon  
Domain Name System Structure and Delegation  
<http://www.rfc-editor.org/rfc/rfc1591.txt>, März 1994
- RFC 1601 Huitema, C.  
Charter of the Internet Architecture Board  
<http://www.rfc-editor.org/rfc/rfc1601.txt>, März 1994
- RFC 1855 Hambridge, Sally  
Netiquette Guidelines  
<http://www.rfc-editor.org/rfc/rfc1855.txt>, Oktober 1995
- RFC 1956 Engebretson, D.W. / Plzak, Raymond  
Registration in the MIL Domain  
<http://www.rfc-editor.org/rfc/rfc1956.txt>, Juni 1996
- RFC 2014 Weinrib, A.  
IRTF Research Group Guidelines & Procedures  
<http://www.rfc-editor.org/rfc/rfc2014.txt>, Oktober 1996
- RFC 2026 Bradner, S.  
The Internet Standards Process -- Revision 3  
<http://www.rfc-editor.org/rfc/rfc2026.txt>, Oktober 1996

- RFC 2027 Galvin, James M.  
IAB and IESG Selection, Confirmation, and Recall Process  
<http://www.rfc-editor.org/rfc/rfc2027.txt>, Oktober 1996
- RFC 2028 Hovey, R.  
The Organisations Involved in the IETF Standards Process  
<http://www.rfc-editor.org/rfc/rfc2028.txt>, Oktober 1996
- RFC 2031 Huizer, Erik  
IETF-ISOC relationship  
<http://www.rfc-editor.org/rfc/rfc2031.txt>, Oktober 1996
- RFC 2050 Hubbard, Kim u.a.  
Internet Registry IP Allocation Guidelines  
<http://www.rfc-editor.org/rfc/rfc2050.txt>, November 1996
- RFC 2068 Fielding, Roy T.  
Hypertext Transfer Protocol -- HTTP/1.1  
<http://www.rfc-editor.org/rfc/rfc2068.txt>, Januar 1997
- RFC 2134 ISOC Board of Trustees  
Articles of Incorporation of Internet Society  
<http://www.rfc-editor.org/rfc/rfc2134.txt>, April 1997
- RFC 2135 ISOC Board of Trustees  
Internet Society By-Laws  
<http://www.rfc-editor.org/rfc/rfc2135.txt>, April 1997
- RFC 2360 Scott, Gregor D.  
Guide for Internet Standards Writers  
<http://www.rfc-editor.org/rfc/rfc2360.txt>, Juni 1998
- RFC 2418 Bradner, Scott O.  
IETF Working Group – Guidelines and Procedures  
<http://www.rfc-editor.org/rfc/rfc418.txt>, September 1998
- RFC 2436 Brett, R. F./ Bradner, Scott O. / Parsons, Glenn W.  
Collaboration between ISOC/IETF and ITU-T  
<http://www.rfc-editor.org/rfc/rfc2436.txt>, Oktober 1998
- RFC 2460 Deering, S. / Hinden, R.  
Internet Protocol, Version 6 (IPv6)  
<http://www.rfc-editor.org/rfc/rfc2460.txt>, Dezember 1998
- RFC 2555 RFC Editor, u. a.  
30 Years of RFCs  
<http://www.rfc-editor.org/rfc/rfc2555.txt>, April 1999

- 
- RFC 2691 Bradner, Scott  
A Memorandum of Understanding for an ICANN  
Protocol Support Organization  
<http://www.rfc-editor.org/rfc/rfc2691.txt>, September 1999
- RFC 2727 Galvin, James M.  
IAB and IESG Selection, Confirmation, and Recall Process  
<http://www.rfc-editor.org/rfc/rfc2727.txt>, Februar 2000
- RFC 2826 Internet Architecture Board  
IAB Technical Comment on the Unique DNS Root,  
<http://www.rfc-editor.org/rfc/rfc2826.txt>, Mai 2000
- RFC 2850 Internet Architecture Board  
Charter of the Internet Architecture Board (IAB)  
<http://www.rfc-editor.org/rfc/rfc2850.txt>, Mai 2000
- RFC 2860 Carpenter, Brian E. / Baker, Fred / Roberts, Michael M.  
Memorandum of Understandig Concerning the Technical Work of the  
Internet Assigned Numbers Authority  
<http://www.rfc-editor.org/rfc/rfc2860.txt>, Juni 2000
- RFC 2915 Mealling, Michael / Daniel, Ron  
The Naming Authority Pointer (NAPTR) DNS Resource Record  
<http://www.rfc-editor.org/rfc/rfc2915.txt>, September 2000
- RFC 2916 Faltstrom, Patrik  
E.164 number and DNS  
<http://www.rfc-editor.org/rfc/rfc2916.txt>, September 2000
- RFC 2972 Masinter, Larry, u. a.  
Context and Goals for Common Name Resolution  
<http://www.rfc-editor.org/rfc/rfc2972.txt>, Oktober 2000
- RFC 3026 Blane, Roy  
ITU, Liaison to IETF/ISOC on ENUM  
<http://www.rfc-editor.org/rfc/rfc3026.txt>, Januar 2001
- RFC 3160 Harris, Susan  
The Tao of IETF  
<http://www.rfc-editor.org/rfc/rfc3160.txt>, August 2001

### III. Abkürzungsverzeichnis

Abl.	Amtsblatt
Abs.	Absatz
ACPs	Administrative Domain Name Challenge Panels
AfriNIC	African Network Information Center
AmtsG	Amtsgericht
ANSI	American National Standards Institute
APNIC	Asia Pacific Network Information Center
ARIN	American Registry for Internet Numbers
ARPAnet	Advanced Research Projects Agency Network
Art.	Artikel
ASO	Address Supporting Organization
BGH	Bundesgerichtshof
BGHZ	Bundesgerichtshof, Entscheidungssammlung in Zivilsachen
BOF	Birds Of a Feather Session der IETF
BoT	Board of Trustees der ISOC
Buchst.	Buchstabe
bzw.	beziehungsweise
ca.	circa
ccTLD	Country Code Top Level Domain
CENTR	Council of European National Top-Level Domain Registries
CERT	Computer Emergency Response Team
CREN	The Corporation for Research and Educational Networking
DARPA	Defense Advanced Research Projects Agency (USA)
DDN	Defense Data Network (USA)
DENIC	Deutsches Network Information Center
DIGI e.V.	Deutsche Interessengemeinschaft Internet e.V.
DIN	Deutsches Institut für Normung
DISA	Defense Information Systems Agency (USA)
DNDP	NSI Domain Name Dispute Policy
DNDP	Domain Name Dispute Policy
DNS	Domain Name System
ECMA	European Computer Manufacturers Association
ENUM	Electronic Number and Telephone Number URI Mapping
ETSI	European Telecommunication Standards Institute
FAQ	Frequently Asked Questions
FCC	Federal Communications Commission (USA)
FNC	Federal Network Council (USA)
ftp	File Transfer Protocol
FYI	For Your Information (RFC)
GSI	Government Systems Inc.

---

gTLD	generic Top Level Domain
gTLD-MoU	Generic Top Level Domains – Memorandum of Understanding
Hrsg.	Herausgeber
HTML	Hypertext Mark Up Language
HTTP	Hyper Text Transport Protocol
i.V.m.	in Verbindung mit
IAB	Internet Architecture Board
IAHC	Internet Ad Hoc Committee
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICC	International Chamber of Commerce
IEC	International Electrotechnical Commission
IEEE	Institute for Electrical and Electronics Engineers
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
INTA	International Trademark Association
InterNIC	Internet Network Information Center
IP	Internet Protocol
IR	Internet Registry
IRSG	Internet Research Steering Group
IRTF	Internet Research Task Force
ISBN	International Standard Book Number
ISO	International Organization for Standardization
ISOC	Internet Society
ISOC.DE	Deutsches Chapter der ISOC
ISSN	International Standard Serial Number
iTLD	international Top Level Domain – entspricht gTLD
ITU	International Telecommunications Union
ITU-T	ITU Telecommunication Standardization Sector
IuKDG	Informations- und Kommunikationsdienstgesetz
JTC1	ISO/IEC Joint Technical Committee 1
Kap.	Kapitel
LACNIC	Registro Regional de Direcciones IP Latinoamericano y Caribeño
LG	Landgericht
MUD	Multi User Dungeons
MUSH	Multi User Shared Hallucination
NASDAQ	National Association of Securities Dealers Automated Quotation System
NIC	Network Information Center
NIST	National Institute of Standards and Technology (USA)
NREN	National Research and Education Network
NSF	National Science Foundation (USA)
NSI	Network Solutions Inc.
NYSE	New York Stock Exchange

---

OLG	Oberlandesgericht
OMG	Object Management Group
OSI	Open Systems Interconnection
RegTP	Regulierungsbehörde für Telekommunikation und Post
RFC	Request For Comments
RG	Reichsgericht
RGZ	Reichsgericht, Entscheidungssammlung in Zivilsachen
RIPE NCC	Réseaux IP Européenne Network Coordination Center
S.	Seite
SAIC	(Muttergesellschaft von NSI)
SigG	Signaturgesetz
SLD	Second Level Domain
SMTP	Simply Mail Transport Protocol
SRI	Stanford Research Institute
STD	Standard (RFC)
TCP	Transmission Control Protocol
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TLD	Top Level Domain
UCC	Uniform Commercial Code
UMTS	Universal Mobile Telecommunications Systems
UNCITRAL	United Nations Commission on International Trade Law
u.a.	und andere
u.a.	unter anderem
URI	Universal Resource Indicator
USC	University of Southern California
USC-ISI	Information Sciences Institute of the University of Southern California
US-DoC	United States Department of Commerce (USA)
US-DoD	United States Department of Defense
US-FNC	United States Federal Network Counsel
USNC	U.S. National Committee
VDE	Verband Deutscher Elektrotechniker
VDI	Verein Deutscher Ingenieure
vgl.	vergleiche
VO	Verordnung
W3C	World Wide Web Consortium
WAP	Wireless Application Protocol
WG	Working Group
WIPO	World Intellectual Property Organization
WWW	World Wide Web
z.B.	zum Beispiel
zit.	zitiert



*Not that there is no control. Cyberspace is not anarchy. But that control is exercised through the ordinary tools of human regulation – through social norms, and social stigma; through peer pressure, and reward.*

– Lawrence Lessing – *The Zones of Cyberspace* –

*Das Internet ist kein anarchistisches Netz. Die Vorstellung, ein weltweites Netz könne ohne Hierarchie, Kommunikationsstrukturen und einheitliche, definierte Standards und Regeln kommunizieren, ist von Unkenntnis der komplexen Wirkungszusammenhänge und massiver Naivität geprägt.*

– Patrick G. Mayer – *Das Internet im öffentlichen Recht* –

## 1. Einleitung

Das heute kaum mehr wegzudenkende Internet ist ein Verbund aus vielen einzelnen Computernetzwerken. Es ist das inzwischen wichtigste elektronische System neben verschiedenen anderen älteren Netzwerken, wie zum Beispiel das Fidonet<sup>1</sup> oder das frühere Deutsche Forschungsnetz (DFN)<sup>2</sup>. Mit dem Internet selbst dürfen nicht die kommerziellen Onlinedienste wie T-Online oder AOL verwechselt werden<sup>3</sup>.

Das Internet erlangte in den letzten Jahren eine immer umfangreichere Bedeutung und Beliebtheit. Ursprünglich nur als militärisches Computernetzwerk und Kommunikationsmedium für amerikanische Wissenschaftler gedacht, hat es sich inzwischen über den ganzen Erdball ausgebreitet. Dabei zieht es immer mehr Nutzer aus dem privaten oder dem kommerziellen Bereich an. 1971 bestand es aus 23 Militärcomputern, heute dagegen sind es schon über 150 Mio. Rechner. Die zunächst einfachen Anwendungen des Internets, wie textbasiertes Senden und Empfangen von Briefen (Email) und die simplen Mechanismen zur Übertragung von Daten (ftp – *file transfer protocol*), wurden inzwischen durch multimediale Anwendungen erweitert.

---

<sup>1</sup> Das Fidonet ist ein Zusammenschluß privat betriebener Mailboxen.

<sup>2</sup> Heute nehmen die deutschen wissenschaftlichen Institutionen mittels des DFN am Internet teil.

<sup>3</sup> Diese bieten über ihr Onlineangebot hinausgehend einen Zugriff auf das Internet an.

---

Den größten Bedeutungszuwachs erlangte das Internet vorrangig durch die Einführung und Weiterentwicklung des *World Wide Web* (WWW). Mit dessen Hilfe lassen sich Texte, Grafiken und Tondateien zu einheitlichen Präsentationen (Homepages) zusammenstellen und es kann auf einfache Weise auf große Datenbanken zugegriffen werden. Die einzelnen Seiten lassen sich durch einen uniformen Rahmen einfach miteinander verbinden und indizieren. Diese Querverbindungen und Indizierungen machen es möglich, weitere Dokumente zu finden und schnell von einem Dokument zu einem anderen zu wechseln. Es wurden damit völlig neue kommerzielle Anwendungsbereiche wie der virtuelle Einkauf oder die Erledigung von Bankgeschäften über den Computer ermöglicht.

Ebenso erlangte die Internetanwendung Email eine beachtliche wirtschaftliche Bedeutung, da es möglich wurde, einen elektronischen Brief jedem zu senden, der Zugang zum Internet hat, egal, wo er sich gerade befindet. Außerdem sind die Kosten im Vergleich zum herkömmlichen Briefverkehr bedeutend geringer.

Die Vielfältigkeit der Nutzungsmöglichkeiten und der grenzüberschreitende Datenverkehr des Internets führten verständlicherweise zu juristische Streitigkeiten. Zuerst wurden vor allem strafrechtliche Aspekte von diversen Angeboten im WWW wie die Verbreitung von Kinderpornographie, die Anleitung zum Bombenbau oder Aufstachelung zum Rassenhaß diskutiert und gleichzeitig die Reichweite der Meinungsfreiheit erörtert. Bald folgten auch zivilrechtliche Streitigkeiten, zum Beispiel darüber, wie die Vertragsanbahnung über das Internet erfolgt oder wie AGBs in einen über das Internet geschlossenen Vertrag mit einbezogen werden können. Weitere Problemfelder sind zum einen der Datenschutz durch das massive Sammeln von Nutzerdaten und zum anderen der Urheberrechtsschutz durch das rigorose Kopieren von Software, das Einscannen von Büchern und dem weltweiten Austausch von Musikdateien.

Die meisten Computer im Internet sind über einen bestimmten Namen (Domainname) erreichbar. Der Hauptrechner unserer Universität trägt zum Beispiel den Namen „uni-jena.de“. Der Hauptrechner der rechtswissenschaftlichen Fakultät selbst hat den Namen „recht.uni-jena.de“. Ohne eine solche Adresse kann man weder elektronische Post erhalten, noch kann man selber Informationen im WWW anbieten. Die Internetadressen müssen, wie eine normale Postanschrift, einmalig sein, das heißt, sie dürfen nur jeweils einmal vergeben werden. Entsprechend stark ist der Wettlauf um die Registrierung verschiedener Adressen.

Ein einheitliches Adresssystem ist für das WWW und andere Anwendungsmoduln des Internets unerlässlich. Diese einheitlich verwendeten Adressen basieren auf dem *Domain Name System* (DNS), welches durch seine einfache Form der Namensgebung die Verbreitung des Internets beschleunigt und dessen ökonomischen Wert um ein Vielfaches erhöht hat<sup>4</sup>.

---

<sup>4</sup> Gordon, Controlling the Internet, Kap. 2.1.

In letzter Zeit wurde die Frage oft diskutiert, ob bei der Vergabe und Verwendung von Domainnamen Namens- und Markenrechte anderer Personen verletzt werden können, wobei es nicht darauf ankommt, ob diese anderen Personen selbst im Internet vertreten sind. Entsprechend gibt es zu diesem Thema in Deutschland eine Serie von Gerichtsentscheidungen und viele wissenschaftliche Abhandlungen. Auf welchen wirtschaftlichen, technischen und vor allen juristischen Grundlagen das DNS basiert, wurde bislang jedoch nur selten in der deutschen juristischen Literatur diskutiert. Die genaue Bestimmung dieser Grundlagen, in welche nicht nur technische, sondern auch rechtliche Aspekte verwoben sind, bildet jedoch eine Voraussetzung für den weiteren wirtschaftlichen Erfolg des Internets.

Es ist deshalb wichtig, die Grundstrukturen zu beleuchten und näher auf die Organisationen einzugehen, die das DNS verwalten und die Domainnamen vergeben. Dabei wird erörtert, inwieweit das Internet auf soliden Mechanismen der Selbstregulierung basiert. Beim Konzept der Selbstregulierung<sup>5</sup> handelt es sich um eine Fülle besonders in letzter Zeit intensiv diskutierter Rechtssetzungs- und Verwaltungsverfahren unterschiedlicher Struktur und Ausprägung. Bei der Anwendung von Selbstregulierungsstrategien wird hauptsächlich auf eine direkte staatliche Einwirkung verzichtet und eine dezentrale Steuerung von komplexen Systemen vorgezogen. Ziel dieser außerhalb staatlicher Verwaltung anzusiedelnder Regulierung ist zum einen eine Entlastung des öffentlichen Sektors und der politischen Entscheidungsträger und zum anderen eine Mobilisierung des Wissens und der Fähigkeiten der Gesellschaft<sup>6</sup>. Es sollen Alternativen zum einseitigen hoheitlichen Verwaltungshandeln, welches auf Grund komplexer Regelungsmaterien und kaum noch überschaubarer Wirkungszusammenhänge immer weniger geeignet scheint, durchgängig effektive und vollziehbare Regelungen zu schaffen, angeboten werden. Soweit wie möglich tritt dabei an die Stelle staatlicher Normierung und Überwachung die eigenverantwortliche Selbstregulierung und -kontrolle der privatrechtlich organisierten Gesellschaft<sup>7</sup>.

Ungeachtet von deutscher Seite bestehenden rechtlichen Rahmenbedingungen hat sich auf internationaler Basis ein kaum durchschaubares System aus wissenschaftlichen Institutionen, gemeinnützigen Organisationen und Unternehmen herausgebildet, die regulierend und verwaltend auf das Internet einwirken. Die Hauptakteure sind hierbei dem privatrechtlich organisierten Bereich zuzuordnen, während staatliche Behörden nur marginal an der Administration des Internets beteiligt sind. Diese Arbeit beschäftigt sich mit der Regulierung der Adresssysteme und der Standardisierung des Internets. Es soll aufgezeigt werden, daß es zwei wichtige Möglichkeiten der Adressierung von Computern im Internet gibt, zum einen das System der sogenannten IP-Adressen und zum anderen das DNS (Kapitel 2.2). Die jeweiligen Verwaltungen dieser Adressierungssysteme stellen zwei Säulen der Internetregulierung dar. Über

---

<sup>5</sup> Zum Begriff siehe *Voßkuhle*, VerwArch 92 (2001), 184, 213ff.; *Schmidt-Preuß*, VVDStRL 56 (1997), 160, 162ff.; *Di Fabio*, VVDStRL 56 (1997), 235, 237ff. ;Einführend zur Selbstregulierung im Internet siehe auch *Christiansen*, MMR 2000, 123ff.

<sup>6</sup> Vgl. *Voßkuhle*, VerwArch 92 (2001), 184, 214

<sup>7</sup> Vgl. *Kloepfer/Elsner*, DVBl. 1996, 964, 965.

---

die Problematik der Adressierung von Computern im Internet hinaus soll festgestellt werden, daß die dritte und am weitesten ausgebildete Säule der Internetregulierung die Entwicklung und Gestaltung der Internetstandards darstellt (Kapitel 2.4), ohne die das Internet nicht als einheitliches Netzwerk bestehen könnte. Da die Entwicklung der beteiligten Organisationen frei von jeglichen staatlichen Einflüssen war und somit ein glänzendes Beispiel privatrechtlicher Regelungsmechanismen ist, soll in dieser Arbeit auf das Verhältnis zwischen privater staatsfreier Regulierung und dem Erfordernis staatlichen Eingreifens in die Verwaltung des Internets eingegangen werden.

Es wird zu zeigen sein, daß sich die drei fundamentalen Aufgaben der Internetregulierung in der Organisation *Internet Corporation for Assigned Names and Numbers* (ICANN) vereinigen (Kapitel 3). Dabei soll besonders der geschichtliche Hintergrund hervorgehoben werden, der zur Entstehung dieses bedeutenden Organs geführt hat. Trotz der inzwischen erfolgten internationalen Anerkennung der ICANN, ist festzustellen, daß eine demokratische Legitimation der ICANN nicht gesichert ist, daß das rechtliche Verhältnis der ICANN zu landesspezifischen Organisationen noch nicht geklärt ist und das die USA mit ihrer Autorität über den sogenannten *A Root Server* noch eine enorme Machtposition über das Schicksal des Internets innehaben. Auch wird zu zeigen sein, daß die ICANN bei der Reform des DNS noch einige Stolpersteine zu überwinden hat. Insbesondere soll dargelegt werden, daß die ICANN die Fairneß schiedsgerichtlicher Streitschlichtung zu erhöhen und klare Regeln zur Einführung neuer Domains zu erlassen hat.

Die Öffentlichkeit richtet ihr Hauptaugenmerk bei Betrachtung der Arbeit der ICANN auf die Vergabe der Domainnamen. Dabei spielt nicht nur die Praxis der schiedsgerichtlichen Streitschlichtung um Domainnamen eine Rolle, sondern auch die vielen vor staatlichen Gerichten stattfindenden Verfahren. Es wird festzustellen sein, daß sich insbesondere im Deutschen Recht eine feste Rechtsprechung bezüglich der Lösung dieser rechtlichen Streitigkeiten herausgebildet hat (Kapitel 4). Im Rahmen dieser Erörterungen soll im Rahmen eines Exkurses auch näher auf das Vergabeverfahren für deutsche Domainnamen eingegangen werden.

Abschließend ist festzustellen, daß weitere Alternativen zum heute bestehenden DNS existieren, mögen dies Alternativen innerhalb des DNS oder parallel zu diesem sein (Kapitel 5).

In dieser Arbeit soll folgende Hauptthese dargelegt und erörtert werden, daß das Internet weder chaotisch noch anarchistisch aufgebaut ist, sondern auf komplizierten Mechanismen der Selbstregulierung basiert. Die Selbstregulierung des Internets basiert auf drei Säulen: der Standardsetzung, der Verwaltung des IP-Adressraumes und des *Domain Name Systems*. Dabei stellt die wichtigste und älteste Säule die Standardsetzung dar. Es soll der These nachgegangen werden, daß die ICANN ein Dach über die drei Säulen der Internet-Selbstregulierung bildet und für die Wahrnehmung ihrer Aufgaben, eine demokratische Legitimierung benötigt. Schließlich soll die These belegt werden, daß es eine Reihe von Alternativen zu dem von ICANN verwalteten System der Internetressourcen gibt.

In die Dissertation wurde, soweit dem Autor bekannt, der Meinungsstand aus Schrifttum und Rechtsprechung bis Ende Dezember 2001 eingearbeitet. Die eingefügten Tabellen und Abbildungen basieren, soweit nicht anderweitig gekennzeichnet, auf eigenen Entwürfen des Verfassers.

In Anbetracht der Tatsache, daß viele wertvolle Informationen im Internet nur eine zeitlang veröffentlicht werden ist es möglich, daß einige Verweise auf WWW-Seiten nicht mehr erreichbar sind. Um dem Leser dennoch einen Zugriff auf die zitierten Aufsätze und Artikel zu ermöglichen, ist der Arbeit eine CD mit einer Kopie der angeführten Webseiten beigelegt. Dazu wurde nur der jeweils zitierte Aufsatz oder Artikel beziehungsweise die jeweilige Startseite übernommen. Hinzuweisen ist, daß unter der WWW-Adresse <http://www.archive.org> ein Internetarchiv geführt wird, welches aller zwei Monate die dem Archiv bekannten Veröffentlichungen archiviert und damit einen Rückgriff auf bereits gelöschte WWW-Seiten ermöglicht.

*Without an agreement on a single data transmission and routing protocol suite, the Internet would be a worthless set of cables unable to transmit data reliably.*

*– Josh A. Goldfoot – Antitrust Implications of Internet Administration –*

*We reject Kings, Presidents, and Voting: We believe in rough consensus and a running code.*

## 2. Das Internet als System

Nur wenige Internetnutzer werden sich damit auseinandersetzen, wie eine Email um die Welt gesendet wird oder wie man durch Klicken auf einen Hyperlink zu einer weiteren WWW-Seite gelangt. Bei der Benutzung müssen sich die wenigsten Nutzer Gedanken über die Herkunft des Internets machen. Dennoch ist eine Kenntnis der Geschichte des Internets und deren zugrundeliegender Technologie von beträchtlichem Wert für diejenigen, welche regulierend in das Internet eingreifen wollen, da sich das Internet in Folge der rasanten Entwicklung stark von anderen vorhandenen Medien unterscheidet. So setzten sich die älteren Medien wie Radio, Fernsehen oder Fax in der Bevölkerung nur langsam durch und die existierenden Gesetzeswerke konnten zeitgleich angepaßt werden. Das explosionsartige Wachstum des Internets hingegen mit seinen vielen technischen Neuerungen und der internationalem Reichweite ließ kaum eine parallele Anpassung der verschiedenen staatlichen Regeln zu. In diesem Kapitel soll deshalb ein Überblick über die Entwicklung die zugrundeliegende Technik des Internets gegeben werden. Neben geschichtlichen Daten richtet sich meine Aufmerksamkeit auf technische Erläuterungen, die wichtig für das Verständnis der nachfolgenden Kapitel sind. Die Entwicklung des Internets ging einher mit einem bislang unvergleichlichen Standardisierungsprozeß. Deshalb werde ich im Folgenden auch auf die Standardsetzung eingehen und die Probleme diskutieren, die mit diesem Prozeß verbunden sind.

### 2.1. Geschichtlicher Hintergrund

Dem sogenannten Netz der Netze, welches seinen Ursprung im Verteidigungsministerium der USA hatte, lagen zwei Interessen zugrunde. Zum einen wollte man in den USA durch eine Vernetzung von Computern die hohen Rechnerkosten der sechziger Jahre minimieren. Zum anderen hatte man in Zeiten des kalten Krieges die Befürchtung, nicht auf einen atomaren Erstschlag reagieren zu können, falls hierdurch die Kommunikation im nationalen Rechnernetzwerk verhindert würde. Das Design des nunmehr entwickelten Ausgangsgangsnetworks

kes, das sogenannte ARPAnet (benannt nach der zuständigen Dienststelle des Verteidigungsministeriums, der *Advanced Research Projects Agency*), spiegelte diese Interessen wieder und hilft, die Struktur und Beschränkungen des heutigen Internets zu erklären<sup>8</sup>. Ein Hauptmerkmal des ARPAnet war die Verwendung eines verteilten Netzwerkes. Dieses vermied eine zentrale Einheit, damit bei einem atomaren Angriff die Kommunikation aufrecht erhalten werden konnte<sup>9</sup>. Das Netz bestand aus Einzelcomputern, die untereinander mittels einer Vielzahl von Knotenpunkten verbunden waren. Das dezentralisierte Modell stellte sicher, daß eine einzelne Nachricht unterschiedliche Wege im Rechennetzwerk nehmen konnte, um von einem Rechner zu einem anderen zu gelangen. Sollte ein Teil des Netzes ausfallen, war eine Umleitung über einen anderen Weg möglich. Ein weiteres Hauptmerkmal war das Zerteilen einer Nachricht in eine Vielzahl von Bruchstücken (Datenpakete) durch den Ausgangscomputer, welche getrennt über das Netzwerk versendet und beim Zielcomputer wieder zusammenge setzt wurden. Dadurch konnten zwei nachrichtentechnische Probleme gelöst werden. Erstens war es nur bedingt möglich, daß von einem unbefugten Dritten die gesamte Nachricht abgefangen werden konnte und zweitens wurde eine Überlastung eines Streckenabschnittes vermieden.

Mit der Verbindung von vier verschiedenen US-amerikanischen Universitätsrechenzentren ist das geplante ARPAnet 1970 Realität geworden. Zunächst wurde es durch den Anschluß weiterer amerikanischer Universitätsnetzwerke erweitert. Es wuchs in den frühen siebziger Jahren allmählich mit circa einem neuen Knotenpunkt je Monat. Anfang der achtziger Jahre wurde es fast ausschließlich von Universitäten und Militäreinrichtungen genutzt. Erst 1990 wurde der kommerzielle Gebrauch durch die Allgemeinheit erlaubt<sup>10</sup>.

Die Transformation des ARPAnet in das heutige Internet begann mit der Entwicklung der noch zu erläuternden Netzwerkspezifikation des sogenannten *Transmission Control Protocol/Internet Protocol* (TCP/IP) im Jahre 1974 durch die Wissenschaftler Vinton Cerf und Bob Kahn<sup>11</sup>. Mittels des TCP/IP, welches erst zehn Jahre später umfassend umgesetzt war, konnten die unterschiedlichen Netzwerke Daten untereinander austauschen, ohne daß intern Änderungen am jeweiligen Netzwerk erforderlich waren. Die zugrundeliegende Netzwerkspezifikation verwendete eine globale Adressierungsmethode, durch welche sich Computer ohne Rücksicht auf deren geographische Position erreichen ließen.

Das ARPAnet wurde zunächst vorrangig zur Kommunikation zwischen den Wissenschaftlern verwendet. So verursachten schon 1973 Emails 3/4 des Netzverkehrs. Auch fingen die ersten Benutzer des Netzes an, Nachrichten online zu suchen und nutzten dabei das auch heute noch weit verbreitete News-System. Doch das Internet wäre ein Medium für die Wissenschaftler

---

<sup>8</sup> Ausführlich zur Entstehung des ARPAnet: *Leiner, u.a.*, A Brief History, Kap. Origins of the Internet; *Vetter*, Geschichte des Internets.

<sup>9</sup> Siehe *Völker/Weidert*, WRP 1997, 652, 652.

<sup>10</sup> Siehe *Völker/Weidert*, WRP 1997, 652, 652.

<sup>11</sup> Siehe *Vetter*, Die Geschichte des Internets.

und die akademische Gemeinschaft geblieben, wäre nicht am CERN Atomforschungszentrum in der Schweiz 1989 ein System entwickelt worden, das ein leichtes Auffinden von Informationen im Internet ermöglicht. Tim Berners-Lee schlug hierzu eine Reihe von Spezifikationen und Protokollen vor, welche das Ansteuern von Dokumenten ermöglichte, die durch Hyperlinks untereinander verbunden waren. Durch einen Mausklick auf die Hyperlinks sollte ein Springen zwischen den einzelnen Dokumenten möglich werden. Dieses Verfahren wurde weltweit als *World Wide Web* bekannt. Die das WWW vervollständigende Software, welche bislang primitiv und kaum öffentlich zugänglich war, sollte 1993 entwickelt werden. Marc Andreessen, ein amerikanischer Student der *University of Illinois* schuf einen WWW-Browser namens Mosaic. Dieser war entwickelter und stabiler als seine Vorgänger und erlaubte Bilder in das WWW zu integrieren. Das Programm Mosaic benutzte eine grafische Bildschirmoberfläche, welche den Benutzer ein einfaches, heute weit verbreitetes und selbstverständliches, Rollen des Bildschirminhaltes ermöglichte und für die gängigsten Betriebssysteme wie UNIX, Windows oder Macintosh innerhalb eines Jahres verfügbar war<sup>12</sup>. Dieses Programm für das WWW bildete die Initialzündung für das stetig wachsende Interesse der Bevölkerung an dem neuen Medium mit einer jährlichen Wachstumsrate von 50%.

Das Internet ist inzwischen von einem nur vier Computer umfassenden Netzwerk zu einem Netz der Netze von Millionen Computern herangewachsen. Obgleich das Internet, insbesondere das WWW, inzwischen Audio, Video und flexible Softwareerweiterungen wie Java beherrscht, ist die zugrundeliegende Struktur relativ unverändert geblieben. Dieses ursprüngliche Design, das sich im offenen und verteilten Netzwerk sowie dem universellen Kommunikationsprotokoll TCP/IP wiederspiegelt, ist verantwortlich für die Macht und die Beschränkungen des Internets.

### 2.2. Technischer Einblick

Um das Zusammenspiel der einzelnen Anwendungen des Internets zu verstehen, muß man einen Blick auf die technischen Grundbedingungen des Internets werfen. Im folgenden soll deshalb zunächst auf den technischen Aufbau des Internets und das sogenannte Routing durch IP-Adressen eingegangen werden. Um die Ausführungen für einen technischen Laien verständlich zu halten, stellen die folgenden Ausführungen nur einen Überblick dar, welcher keinen Anspruch auf Vollständigkeit erhebt.

#### 2.2.1. Aufbau in einzelnen Schichten

Ebenso wie Menschen müssen Computer eine gemeinsame Sprache sprechen, um miteinander kommunizieren zu können. In der Computertechnologie werden diese Sprachen *Common Network Protocols* genannt, die jeder verbundene Computer zu beachten hat. Ein Netzwerkprotokoll ist aus einem Set von Vorschriften zusammengesetzt, denen zwei Rechner folgen

---

<sup>12</sup> Zu den historischen Hintergründen des WWW und des Programmes Mosaic, siehe *Klaasen, Gerd*, Das World Wide Web Museum, <http://spot.fho-emden.de/alge/museum/index.htm>. Siehe auch *Hoeren, Rechtsfragen des Internet*, Rdnr. 24.

müssen, um Nachrichten austauschen zu können. Protokolle beschreiben einerseits das Format einer Nachricht, welche gesendet werden kann, andererseits die Antwort des Gegencomputers auf eine solche Nachricht. Sie dienen damit als Koordinationswerkzeuge in der Computerkommunikation. Alle Computer, die mit dem Internet verbunden sind, folgen der später noch öfters zu erwähnenden Vereinigung des *Transmission Control Protocols* (TCP) und des *Internet Protocols* (IP). Diese Protokolle sind für die grundlegende Kommunikation über das Internet unabdingbar. Gerade das TCP/IP und das Einverständnis der Netzbetreiber es zu benutzen, schweißt die verschiedenen Netze des Internets zusammen, als wäre es eine zusammenhängende Einheit<sup>13</sup>.

Der Aufbau des Internets lässt sich am besten mit Hilfe des Schichtenmodells erklären, welches besagt, daß die Kommunikation im Internet durch verschiedene aufeinander aufbauende Ebenen erfolgt<sup>14</sup>. Der Prozeß der Datenkommunikation über ein Rechnernetz wird durch dieses Modell in sieben aufeinanderfolgende Schichten eingeteilt, die einander zuarbeiten und jede für sich eine bestimmte Abstraktionsebene kennzeichnet. Bei abstrakter Betrachtung scheinen die jeweils gleichen Schichten verschiedener Rechner miteinander zu kommunizieren. Die Details der darunterliegenden Abstraktionsebenen werden von den darüberliegenden Schichten verborgen (vgl. zum Schichtenmodell Tabelle 1 unten).

Die unterste Ebene ist die Hardware. Dazu zählen die Computer mit ihren Netzwerkgeräten sowie alle erdenklichen Datenübertragungsstrecken (Telefonleitungen, Glasfaserkabel oder Satellitenfunkstrecken). Diese werden durch die zweite Ebene genutzt, welche zunächst die Verbindungen für den Datentransfer zwischen den zwei Endcomputern einer Datenübertragungsstrecke mittels eines Netzkettenprotokolls, wie Ethernet oder X.25, herstellt. Diese beiden Ebenen sind zunächst noch nicht direkt dem Internet zuzuordnen, sondern sind Grundvoraussetzung für jedes Computernetzwerk.

Auf der zweiten Ebene lagert die sogenannte Internetnetzwerkschicht (dritte Ebene). In ihr erfolgt die Kontaktaufnahme mit dem gewünschten Internetcomputer. Dazu ist die Kenntnis der sogenannten IP-Nummer des anzusprechenden Rechners im Internet erforderlich. Jeder Computer im Internet muß eine eigene IP-Nummer haben, um überhaupt Daten senden oder empfangen zu können. Diese IP-Nummer ist dabei mit unserer Postadresse vergleichbar. Um eine Nachricht zu versenden, wird diese in eine Art „Umschlag“ verpackt und mit der IP-Adresse versehen. Die Zustellinformation ist somit in der Nachricht selbst enthalten. Wenn die Nachricht durch die Internetcomputer geleitet wird, so wird an jedem Knotenpunkt an Hand der Adresse auf dem „Umschlag“ über die richtige Weiterleitung entschieden. Bei einer fehlerhaften Übertragung wird gegebenenfalls eine neue Weiterleitung über eine andere Strecke gewählt (*dynamic routing*)<sup>15</sup>. Diese Flexibilität ist die größte Stärke des Internets. Der Ausfall eines Teils des Internets kann durch das Wählen anderer Übertragungswege umgangen wer-

---

<sup>13</sup> Siehe *Goldfoot*, 84 Va. L. Rev. 909, 911.

<sup>14</sup> Näheres zur Strukturierung des Internets in einzelne Schichten: *Köhntopp*, c't 1993, Heft 3, 232ff.

<sup>15</sup> Zur Technik des Dynamic Routing siehe ausführlich *Kuri*, c't 1997, Heft 6, 380ff.

den. Dabei überwacht ein Computer an jedem Knotenpunkt die Stärke des Datenverkehrs und entscheidet sich für die am wenigsten frequentierte Strecke zum nächsten Knotenpunkt, an welchem der Prozeß wiederholt wird. Eine Verbindung zu einem anderen Internetteilnehmer läßt sich somit auch bei starker Beschädigung des Netzwerkes herstellen.

Problematisch für einen Sender einer Nachricht ist hierbei, daß er nicht vorhersehen kann, welchen Weg seine Nachricht nehmen wird, da an jedem Knotenpunkt die Daten Manipulationen ausgesetzt sein könnten. Ebenso ist für die einzelnen Knotenpunkte des Internets unklar, von wem sie Nachrichten weiterreichen<sup>16</sup>. Damit haben sie keinen Einfluß darüber, ob die Daten aus seriöser Quelle oder von Anbietern rechtswidrigen Inhaltes entspringen.

Die IP-Nummern (auch IP-Adressen) sind nur einmal vorkommende 32-Bit Zahlen (siehe Kapitel 2.2.2.1 unten). Damit das Internet funktioniert, darf jede IP-Adresse nur durch einen einzigen Computer verwendet werden. Nur so können die Netzwerkrouter wissen, an welchen Rechner sie die ankommenden Datenpakete weitersenden müssen. Das Ansprechen des Empfangscomputers erfolgt hierbei nach den international anerkannten Regeln des *Internet Protocols*<sup>17</sup> (IP). Dieses Protokoll definiert das Internet. Die Computer, welche miteinander kommunizieren und das IP verwenden, bilden das Internet.

Eine wichtige technische Neuerung, die stark zum Erfolg des Internets beitrug, ist das sogenannte *Packet Switching*<sup>18</sup>. Um die Sicherheit der Datenübertragung zu gewährleisten, werden die zu sendenden Daten in einzelne schmale Pakete zerteilt, getrennt gesendet und beim Empfänger wieder zusammengefügt. Durch das Aufteilen der Daten in kleine Portionen ist eine effektivere Nutzung der Datenleitungen möglich. *Packet Switching* ermöglicht auch das Überbrücken von gestörten Leitungen, da dann die einzelnen Pakete auf einen anderen Übertragungsweg umgeleitet werden. Da nicht alle Computer mit der gleichen Geschwindigkeit miteinander kommunizieren, ermöglicht das *Packet Switching*, daß Internetrouter die ankommenden Datenpakete in Warteschlangen stellen, so daß neuere Datenpakete erst dann gesendet werden, wenn ältere übertragen wurden. Entsprechend hängt die Zeit, welche ein Datenpaket für die Übertragung über das Internet benötigt, von der Netzbela stung und der Anzahl der Router, über die es übertragen wird, ab<sup>19</sup>. Diese Arbeit des Teilens und späteren Zusammenfügens übernimmt die vierte Ebene, die Transportschicht. Das dazu notwendige Verfahren regelt das *Transmission Control Protocol*<sup>20</sup> (TCP), wiederum ein allgemeingültiger Standard der Computerkommunikation und zweiter Bestandteil des TCP/IP. Die einzelnen Pakete werden von Computer zu Computer übertragen, bis sie ihr Ziel erreicht haben. Jedes einzelne Datenpaket enthält die spezielle IP-Nummer des Empfangscomputers<sup>21</sup> und eine laufen-

---

<sup>16</sup> Gibbons, Cornell J.L. & Pol'y 475, 486.

<sup>17</sup> Das Internet Protocol wird durch *RFC 791*, Postel und *RFC 792*, Postel definiert.

<sup>18</sup> Zu den technischen Details siehe *RFC 791*, Postel und *RFC 793*, Postel.

<sup>19</sup> Vgl. *Goldfoot*, 84 Va. L. Rev. 909, 911.

<sup>20</sup> Das Transmission Control Protocol wird durch *RFC 793*, Postel definiert.

<sup>21</sup> Dazu auch *Gordon*, Controlling the Internet, Kap. 1.1.

de Nummer, nach welcher die Daten beim Empfangsrechner wieder sortiert werden. Sollte ein Paket während des Transportes verloren gehen, wird es noch einmal gesendet.

Die fünfte Ebene beinhaltet die eigentlichen Anwendungen des Internets. Dazu zählt zum Beispiel die bekannte Möglichkeit des Versendens von Emails oder die Nutzung des *World Wide Web's*, aber ebenso weniger häufig genutzte Dienste (zum Beispiel *FTP*, *Telnet* oder *USENET*<sup>22</sup>).

Um über diese Dienste einen Datenaustausch zu ermöglichen, wurden auch hier verschiedene Übertragungsstandards in Form von Protokollen festgelegt. Zum Beispiel liegt dem Emailsystem das *Simply Mail Transport Protocol* (SMTP) und dem WWW das *Hyper Text Transport Protocol* (HTTP) zugrunde. Es gibt jedoch noch eine Vielzahl weiterer Anwendungen, die weniger gebräuchlich, in der Informatik jedoch sehr wichtig sind (zum Beispiel *Telnet* und *File Transfer*). Hieraus ist auch ersichtlich, daß das *World Wide Web* nicht, wie weitläufig angenommen wird, das Internet darstellt, sondern nur eine der wichtige Anwendungen des Internets ist. Ständig werden neue Anwendungen für das Internet entwickelt, um den modernen Anforderungen an eine immer schnellere, einfachere und effektivere Informationsübertragung gerecht zu werden. Hierzu zählen die zum Teil umstrittenen Anwendungen *Napster*<sup>23</sup>, *Gnutella*<sup>24</sup> oder *Freenet*<sup>25</sup>, welche einen anonymen und effektiveren Dateiaustausch als über *FTP* oder *WWW* ermöglichen.

Zur Nutzung der Internetanwendungen benötigt man Computerprogramme, die bei entsprechender Anwendung der standardisierten Protokolle Daten senden und empfangen können. Das WWW kann zum Beispiel mit Hilfe des *Netscape Navigator* oder des *Microsoft Internet Explorer* gelesen werden. An der *Friedrich-Schiller-Universität Jena* wird das Programm *Pegasus Mail* zum Senden und Empfangen von Emails verwendet, obwohl man ebenso ein anderes Emailprogramm benutzen könnte (zum Beispiel *Microsoft Mail*). Zu betonen ist deshalb, daß die einzelnen Anwendungen des Internets völlig unabhängig von den Programmen sind, mit denen sie genutzt werden.

---

<sup>22</sup> Erläuterungen der einzelnen Möglichkeiten des Internets siehe: *Wendel*, Recht im Internet, S. 5ff. sowie *Schneider*, EDV-Recht, S. 1685ff.

<sup>23</sup> Siehe <http://www.napster.com>.

<sup>24</sup> Siehe <http://www.gnutellums.com/>.

<sup>25</sup> Siehe <http://freenetproject.org/>.

Tabelle 1 – Das Schichtenmodell des Internets – Eine Auswahl an Diensten, Anwendungen und Protokollen.

5. Anwendungsprogramme	FTP, XFTP, diverse WWW-Browser	Elm, Pegasus Mail, Outlook Express	Standard Telnet-Programme	WWW-Browser, z.B.: Netscape Navigator Microsoft Internet Explorer	Domain Name Server Von allen Anwendungen benutzt
Anwendungsprotokolle	File Transfer Protocol (FTP) RFC 959	Simple Mail Transfer Protocol (SMTP) RFC 821	Telnet Protocol RFC 854	Hyper Text Transfer Protocol (HTTP) RFC 2068	Domain Name System RFC 1034
4. Transmission Control Protocol			Transmission Control Protocol (TCP) RFC 793		User Datagram Protocol (UDP) RFC 768
3. Internet Protocol		Internet Control Message Protocol (ICMP) RFC 792	Internet Protocol (IP) RFC 791		Internet Control Message Protocol (ICMP) RFC 792
2. Datenverbindung	SLIP RFC 1055	CSLIP RFC 1144	PPP RFC 1331		Entsprechende Verbindungsprotokolle für Netzwerksystem
1. Hardware	Modem oder ISDN-Karte		Ethernet	Token Ring	ISDN-CAPI
			Computer, Router, Telefonleitungen, Glasfaserstrecken ...		

## 2.2.2. Adressierung von Computern im Internet

Um auf Informationen über das Internet zugreifen und miteinander kommunizieren zu können, müssen die beteiligten Computer, jeweils eine spezielle Adresse aufweisen. Mittels dieser Adresse kann zum einen durch den nachfragenden Computer der Quellcomputer bestimmt werden, auf welchen sich die gesuchten Informationen befinden, um dann dort die speziellen Daten abzurufen. Zum anderen muß der Quellcomputer die Adresse des nachfragenden Computers wissen, um an diesen die gewünschten Informationen zu senden. Diese notwendige und dem Internet zugrundeliegende Adressierung erfolgt durch die sogenannten IP-Adressen (auch IP-Nummern genannt). Zur Vereinfachung des Umgangs mit den IP-Adressen werden diese in Domainnamen umgesetzt und bleiben für die meisten Endnutzer verborgen.

### 2.2.2.1. IP-Nummern als Internetadressen

Wie eben erläutert, braucht jeder Computer im Internet eine eindeutige IP-Adresse, um am Internet teilnehmen zu können. Vergleichen kann man diese Adresse mit einer Telefonnummer, die auch einmalig und eindeutig ist. Diese IP-Adresse besteht gemäß dem *Internet Protokoll* aus 32 Bit (Ein Bit ist eine Ziffer, die den Wert 0 oder 1 annehmen kann). Diese Adresse in der einfacheren dezimalen Schreibweise geschrieben, ergibt vier einzelne Zahlen (vier einzelne Byte), die durch einen Punkt getrennt werden. Die IP-Nummer spezifiziert dann das spezielle Computernetz und den einzelnen Computer. Z.B. beschreibt die IP-Nummer 141.35.1.2 den Hauptrechner des Jenenser universitären Rechnernetzwerkes. Diese IP-Nummern sind mit anderen Worten die „Hausnummern“ der Rechner<sup>26</sup>.

Die Version des Internetprotokolls IPv4, auf welchem momentan das Internet basiert, ist trotz aller Vorteile nicht mehr auf dem aktuellen technischen Niveau. Obgleich es kontinuierlich weiter entwickelt und durch technische Zusätze an aktuelle Umstände angepaßt wurde, droht ein Zusammenbruch des Internets durch die Verknappung der Adressen<sup>27</sup>. Theoretisch ermöglicht das IPv4 vier Milliarden eindeutige IP-Adressen. In den Anfangszeiten des Internets wurde jedoch sehr großzügig mit der Zuweisung von Adressen verfahren, so daß einige Institutionen, auf Kosten der heutigen Nutzer, völlig überdimensionierte Blöcke von Adressen erhalten hatten. In Zukunft soll jedem technischen Gerät eine eigene IP-Adresse zugewiesen werden, um eine Fernsteuerung zu ermöglichen und um theoretisch jeder Person auf der Erde eine persönliche Adresse zuzuteilen. Dadurch ist eine Erweiterung des aktuellen Systems unausweichlich geworden.

Zu diesem Zweck wurde die Version des Internetprotokolls IPv6 von der *Internet Engineering Task Force* (IETF) entworfen, welches auf einem 128 Bit Adresssystem basiert. Seit dem 14. Juli 1999 werden von der *Internet Assigned Numbers Authority* (IANA) auch offiziell entsprechende Adressen an die Anwender des neuen Protokolls ausgegeben. Mit dieser neuen

---

<sup>26</sup> Bettinger, GRUR Int. 1997, 402. Zu der Problematik der Adressierungstechnik im Internet siehe Kuri, c't 1996, Heft 12, 334ff.

<sup>27</sup> Krempl, c't 1999, Heft 20, 212; Ermert, c't 2000, Heft 1, 32f. Zur neuen Protokollspezifikation siehe RFC 2460, Deering/Hinden.

## 2.2. Technischer Einblick

---

Version wurde nicht nur der Adreßraum enorm erweitert, sondern auch bekannte Sicherheitsprobleme entfernt, verschlüsselte Kommunikation auf der Basisebene des Internets ermöglicht und die automatische Konfiguration neuer in ein Netzwerk eingebrachter Geräte eingeführt<sup>28</sup>.

Dabei wurde auf eine Kompatibilität zu IPv4 geachtet und dessen Adreßraum in IPv6 integriert. Damit ist die Einführung des neuen Internetprotokolls kein Bruch im Betrieb des Internets. Vielmehr wird ein allmählicher Übergang der Verwendung zum neuen IPv6 erfolgen.

### 2.2.2.2. Domainnamen als Internetadressen

Für die Kommunikation von Computer zu Computer mag eine numerische Adressierung ideal sein. Für den Menschen selbst sind diese Nummern weder leicht zu merken noch leicht anzuwenden<sup>29</sup>. Es existiert deshalb seit 1986 ein zweites Namenssystem, das *Domain Name System* (DNS). Dieses basiert auf besser einprägsamen alphanumerischen Namen. So ist fast jeder Internetadresse mindestens ein Name zugeordnet. Zum Beispiel entspricht die oben genannte IP-Nummer 141.35.1.2. dem Domainnamen „fsuj02.rz.uni-jena.de“. Das DNS bildet damit die Komponente der Infrastruktur des Internets, welche für die Übersetzung der alphanumerischen Computernamen in IP-Adressen verantwortlich ist. Jeder Domainname besitzt eine korrespondierende IP-Adresse, obgleich nicht jede IP-Adresse einen Domainnamen besitzt. Auch können mehrere Domainnamen auf eine IP-Adresse verweisen<sup>30</sup>.

Die Übersetzung der Domainnamen in IP-Adressen ist nicht statisch. Die IP-Adresse, welche das DNS für einen Domainnamen zurückgibt, kann sich von Zeit zu Zeit ändern, je nachdem, auf welchen aktuellen Computer der Domainname verweisen soll. Dadurch wird die Flexibilität erhöht, ältere Computer durch neuere auszuwechseln oder die Anbindung des Rechners im Netzwerk zu ändern, ohne daß es zu einem Ausfall des Systems kommt<sup>31</sup>.

Die dem DNS zugrundeliegende Rootdatenbank wird derzeit von der Firma *Network Solution, Inc.* (NSI) im Auftrag der *Internet Corporation for Assigned Names and Numbers* (ICANN) verwaltet. Schon 1993 hatte die NSI den Auftrag zur Verwaltung des DNS schon von der US-amerikanischen *National Science Foundation* (NSF) erhalten<sup>32</sup>. In dieser, von der NSI erstellten Rootdatenbank sind Verweise auf alle untergeordneten Domaindatenbanken mit den darin eingetragenen Domainnamen enthalten, um eine IP-Adresse von jedem Computer zu erhalten, für den eine eigene Domain existiert (vgl. Kapitel 2.2.2.3 unten).

---

<sup>28</sup> Siehe *Krempel*, c't 1999, Heft 20, 212, 213.

<sup>29</sup> Siehe auch *Bettinger*, GRUR Int. 1997, 402f.

<sup>30</sup> Zum Beispiel verweisen die Domainnamen [www.uni-jena.de](http://www.uni-jena.de) und susi.rz.uni-jena.de auf den gleichen Rechner mit der IP-Adresse 141.35.4.20.

<sup>31</sup> *Gordon*, Controlling the Internet, Kap. 1.2.

<sup>32</sup> Ein Verzeichnis des NSF Cooperative Agreement zuzüglich aller Erweiterungen kann unter [http://www.networksolutions.com/en\\_US/legal/internic/cooperative-agreement](http://www.networksolutions.com/en_US/legal/internic/cooperative-agreement) gefunden werden. Vgl. auch *US-DoC, NTIA*, White Paper, 63 Fed. Reg. 31741, 31741.

### 2.2.2.2.1. Nutzung der Domainnamen

Domainnamen werden durch die verschiedenen Anwendungen des Internets genutzt. Zum Beispiel bestehen Emailadressen aus zwei Bestandteilen: der Benutzerkennung (meist ein Kürzel des Empfängernamens) und, getrennt durch das Zeichen @, dem Domainnamen des benutzten Internetrechners<sup>33</sup>. Zum Auffinden von Informationen im WWW reicht der Domainname allein nicht aus. Da in der Regel ein WWW-Server viele verschiedene Informationen in Form von Dateien anbietet, muß jede Datei eindeutig bestimmt werden können. Dazu erhält der Domainname einen Anhang, mit einem festgelegten Adressierungsschema<sup>34</sup>. Dieses bezeichnet das Format der abgerufenen Information und das Verzeichnis, in welchem es sich befindet.

Meistens ist es einfach, den Domainname einer Einrichtung oder eines Unternehmens herauszufinden. Deutsche Universitäten haben gewöhnlich einen Domainname entsprechend „uni-jena.de“. Die großen Firmen sind unter „firmenname.de“ zu erreichen (zum Beispiel „bmw.de“ oder „microsoft.de“). Wenn es einem Unternehmen gelungen ist, einen Domainnamen entsprechend der eigenen Marke oder eines sonstigen Unternehmenskennzeichens zu registrieren, dann können Interessenten die Homepage sehr schnell finden<sup>35</sup>. Sollte die Adresse einer Einrichtung nicht erraten werden können, hat ein Nutzer die Möglichkeit diese durch Suchmaschinen oder manuell erstellte Internetkataloge zu ermitteln.

### 2.2.2.2.2. Aufbau und Einteilung der Domainnamen

Wie die IP-Nummern werden die Domainnamen in einzelne Bestandteile durch Punkte getrennt. Somit lassen sie sich in mehrere Unterabschnitte, sogenannte *Sub Domains*, einteilen. Die Anzahl der Untereinheiten ist nicht festgelegt, übersteigt regelmäßig jedoch nicht fünf, meistens werden nur drei verwendet. Geht man von dem obigen Beispiel „fsuj02.rz.uni-jena.de“ aus, so bildet die letzte Einheit, in unserem Falle „.de“, immer die *Top Level Domain* (TLD). Als vorletzte Einheit steht die *Second Level Domain* (SLD), hier „uni-jena“. Dieser Unterabschnitt kennzeichnet die Institution oder das Unternehmen. Fast alle rechtlichen Streitigkeiten haben diese *Second Level Domain* als Gegenstand. Es folgen die *Sub Level Domains* „.rz“ und „.fsuj02“, die das universitätsinterne Computernetzwerk des Rechenzentrums und einen spezifischen Rechner kennzeichnen.

Die Anzahl und die Bezeichnung aller TLDs ist vorgegeben<sup>36</sup>. Ein Nutzer, der sich eine Internetadresse zulegen möchte, muß dabei zunächst eine TLD auswählen, unter welcher er sich registrieren lassen will. Die *Top Level Domains* sind in zwei Gruppen unterteilt<sup>37</sup>, internatio-

---

<sup>33</sup> Die Email des Verfassers setzt sich z.B. aus der Kennung mail für den Posteingang und dem von ihm registrierten Domainnamen hansreip zusammen: mail@hansreip.de.

<sup>34</sup> Dieses Schema wird Unified Resource Locator (URL) genannt, z.B.: „<http://www.recht.uni-jena.de/index.html>“. „http://“ gibt den Internet-Service an, hier das WWW. „www.recht.uni-jena.de“ ist Domainname. „index.html“ bezeichnet die zu ladende Datei.

<sup>35</sup> Siehe auch *Bettinger*, GRUR Int. 1997, 402, 403f.

<sup>36</sup> Eine Festlegung der TLDs erfolgte im *RFC 1591*, Postel.

<sup>37</sup> Vgl. *RFC 1591*, Postel, Kap. 2. The Top Level Structure of the Domain Names.

## 2.2. Technischer Einblick

---

nale (generische) und nationale. Die internationalen *Top Level Domains* bezeichnen, zu welcher Gruppe von Internetnutzern die entsprechende Institution, dessen Netzwerk unter einer solchen TLD angemeldet ist, angehört. Die nationalen TLDs wiederum fassen Nutzer eines bestimmten Landes zusammen. Jede *Top Level Domain* wird von einer Organisation verwaltet, welche entweder die Vergabe der *Second Level Domains* auf Antrag selbst vornimmt, oder die Aufgabe der Registrierung an andere Unternehmen delegiert hat.

Die erste Gruppe der internationalen *Top Level Domains* (*generic Top Level Domains* – gTLD) sind im Prinzip länderunabhängig. Zu ihnen zählen .com, .net, .org und .int als international zugängliche TLDs, sowie .gov, .mil und .edu, welche speziell US-amerikanischen Einrichtungen vorbehalten sind (siehe Tabelle 2 unten). Ab Mitte 2001 sind dem System der gTLDs sieben weitere hinzugefügt worden (siehe Kapitel 3.3.2 unten). Die TLD .com ist im aktuellen Internetverkehr die Wichtigste. Ursprünglich registrierten sich nur kommerzielle Unternehmen der USA unter ihr. Inzwischen versuchen die verschiedenen Unternehmen und Institutionen weltweit einen Domainnamen unter .com zu erlangen. Dies hat zur völligen Überfüllung dieser *Top Level Domain* geführt. Kaum ein geläufiger Name ist noch frei. Als Resultat findet ein reger Handel mit .com-Adressen statt. Darüber hinaus versuchen viele Interessenten auf die TLDs .net und .org auszuweichen.

Die nationalen *Top Level Domains* entsprechen den Länderkodes der ISO Norm 3166<sup>38</sup>. Deutschland hat somit die *Top Level Domain* .de, Frankreich .fr und die USA .us (siehe Tabelle 2 unten). Es existieren über 200 nationale *Top Level Domains*, die jedoch nicht alle genutzt werden. Anders, als die Bezeichnung es vermuten lässt, ist es nicht zwingend, daß sich ein Verwender einer bestimmten TLD im Land befindet, welches die TLD bezeichnet. Vielmehr sollen durch die TLDs die einzelnen Staaten für sich die Möglichkeit haben, eine länderspezifische Domainvergabe eigenverantwortlich zu organisieren. Dementsprechend erfolgt die Registrierung der Domainnamen durch nationale Vergabestellen.

Es steht den Vergabestellen dabei frei, die einzelnen Domains direkt unter der TLD zu registrieren oder die TLD erneut in einzelne Bereiche zu untergliedern. Entsprechend variiert die Struktur unter den einzelnen TLDs sehr stark<sup>39</sup>. In einigen können Organisationen direkt unter der TLD gelistet werden, in anderen besteht die zweite Ebene wiederum aus generischen Kategorien oder ist nach geographischen Gebieten unterteilt. Eine solche Untergliederung erfolgt zum Beispiel in Frankreich. Nichtkommerzielle Vereinigungen werden unter asso.fr (Associations) registriert, Rechtsanwälte unter barreau.fr oder

---

<sup>38</sup> Vgl. *RFC 1591*, Postel, Kap. 2. The Top Level Structure of the Domain Names. Die Länderkodes werden von der ISO 3166 Maintenance Agency (ISO 3166/MA) (<http://www.din.de/gremien/nas/nabd/iso3166ma>) unabhängig von den verschiedenen Internetorganisationen verwaltet. Die Länderkodes können unter <http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/index.html> eingesehen werden.

<sup>39</sup> In Deutschland werden die Domains direkt unter .de registriert. In Großbritannien dürfen kommerzielle Institutionen sich nur unter co.uk anmelden, siehe *Nominet UK*, Rules for the .uk Top Level Domains, <http://www.nic.uk/rules.html>.

(Associations) registriert, Rechtsanwälte unter barreau.fr oder Presseunternehmen unter presse.fr.<sup>40</sup>.

Tabelle 2 – Die verschiedenen *Top Level Domains*.

Top Level Domain	Zielnutzergruppe
.com	Kommerzielle Nutzer
.org	Organisationen
.net	Internet-Service-Provider
.mil	Militär der USA
.edu	Hochschulen der USA
.gov	Regierung der USA
.int	Internationale Organisationen
Neue gTLDs: .biz, .name, .info ...	Diverse
Ländercodes: z.B. .de, .uk, .us, .mx ...	Bestimmung erfolgt durch nationale Registrierungsorganisationen

Die *Second Level Domains* können frei gewählt werden. Zur Registrierung stellt ein Interessent bei einer Vergabeorganisation einen Antrag auf einen bestimmten Namen. Die Vergabeorganisation prüft, ob dieser schon vergeben ist und wenn der Name noch frei ist, registriert die Vergabeorganisation den Namen als dem Antragsteller zugehörend. Der Antragsteller kann dann unter der beantragten *Top Level Domain* mit seiner registrierten *Second Level Domain* in das Internet gehen. Da auch die Domainadresse (wie die IP-Adresse) einen bestimmten Internetcomputer kennzeichnen soll, darf eine *Second Level Domain* nur einmal unter einer *Top Level Domain* vergeben werden. Unter einer anderen TLD kann dieser Name jedoch erneut registriert werden<sup>41</sup>. Jeder Domainname ist somit eindeutig und einmalig.

Vor den *Second Level Domains* können noch eine Anzahl weiterer Unterdomainnamen stehen (zum Beispiel: fsuj50.rz.uni-jena.de). Am häufigsten tritt das Kürzel www (zum Beispiel [www.uni-jena.de](http://www.uni-jena.de)) auf, welches einen WWW-Server kennzeichnet. Eine Begrenzung der Anzahl dieser sogenannten *Sub Level Domains* ist nicht vorgesehen. Wegen der praktischen Handhabbarkeit, liegt die maximale Anzahl jedoch bei fünf bis sechs Domainangaben. Die einzelnen *Sub Level Domains* werden von dem Betreiber der jeweils höherangigen *Sub Level Domain* vergeben und verwaltet. Die Universität Jena hat somit die Möglichkeit, alle Namen, welche vor „uni-jena“ erscheinen, zu vergeben<sup>42</sup>. Sie ist dafür zuständig, daß die entsprechenden IP-Adressen über das DNS (siehe Kapitel 2.2.2.3 unten) dem gesamten Domainnamen zugewiesen werden können.

<sup>40</sup> Siehe AFNIC, Charte de nommage de la zone .fr, 12. Juli 2001, <http://www.nic.fr/enregistrement/nommage-fr.html>.

<sup>41</sup> So können microsoft.com, microsoft.de und microsoft.fr nebeneinander existieren.

<sup>42</sup> An der FSU-Jena sind dies z.B. „recht“ für die rechtswissenschaftliche Fakultät oder „rz“ für das Rechenzentrum.

Einzelne Pfad- und Dateiangaben stehen häufig direkt hinter dem Domainnamen und werden durch einen Schrägstrich voneinander getrennt. Diese Angaben ermöglichen dem Betreiber einer Webseite eine durchdachte Struktur für seine einzelnen Unterseiten anzulegen. Über die Pfad- und Dateiangabe kann jedes im Webbrower darzustellende Objekt angesprochen werden. Ein Interessent einer Seite kann häufig aus den Zusätzen nähere Informationen über den Inhalt erfahren (zum Beispiel [www.verwaltung.uni-jena.de/hochschulsport/](http://www.verwaltung.uni-jena.de/hochschulsport/)).

### 2.2.2.3. Feststellung der IP-Nummern durch Domain Name Server

Die Verbindung zwischen Internetcomputern erfolgt, wie oben festgestellt (siehe Kapitel 2.2.1 oben), über das IP-System. Wenn ein Computer einen Datenaustausch mit einem anderen Computer durchführen will, benötigt er somit dessen IP-Nummer. Da der Ausgangscomputer zunächst nur den Domainnamen des anzusprechenden Computers wissen wird, fragt er automatisch in der Datenbank<sup>43</sup> einer *Registry* die zugehörige IP-Nummer ab. Das technische Management für die Abfragen übernimmt das *Domain Name System*. Dieses besteht aus einem weltweit verbreiteten Netz von sogenannten *Name Servern* und Datenbanken<sup>44</sup>.

Die dem DNS zugrundeliegenden Datenbanken sind hierarchisch organisiert (vgl. Abbildung 1 unten). Die Spitze bildet der sogenannte *A Root Server*, der die Verweise auf alle TLDs enthält. Soll eine neue TLD eingeführt werden, so muß diese in die Datenbank des *A Root Servers* eingetragen werden. Dieser Server wird derzeit von der NSI verwaltet. Von der Datenbank des *A Root Servers* existieren zwölf Kopien<sup>45</sup>, welche von unabhängigen dritten Institutionen betrieben werden<sup>46</sup>. Dadurch soll die zentrale Datenbank bei der NSI entlastet werden. Sollte ein Server ausfallen, kann problemlos auf eine andere Kopie zugegriffen werden, ohne daß es zu Unterbrechungen des DNS-Betriebes kommt. Die Einträge im *A Root Server* verweisen auf die sogenannten *TLD-Registries*. Die *Registries* betreiben die Datenbanken für die jeweiligen TLDs, in die alle SLDs eingetragen werden müssen. Jeder in einer TLD-Datenbank eingetragenen SLD ist die zugehörige IP-Adresse des jeweiligen Nutzers der SLD zugewiesen. Die Nutzer können schließlich ihren SLDs mittels einer eigenen Datenbank *Sub Level Domains* (zum Beispiel [www.jura.rz](http://www.jura.rz)) und die IP-Adressen der korrespondierenden Computer zuweisen. Entsprechend enthalten alle untergeordneten Datenbanken Ausschnitte aus dem verteilten Datenbanksystem des DNS.

---

<sup>43</sup> Vgl. zum Inhalt der Datenbank über Domainnamen: *Kuri*, c't 1996, Heft 12, 334ff. sowie *Gordon*, Controlling the Internet, Kap. 4.1 Registration Database Contents.

<sup>44</sup> Ausführlich zum Domain Name System vgl.: *Weihrich*, c't 1997, Heft 10, 346ff.

<sup>45</sup> Aktuelle Informationen über den Bestand der Rootserver können unter *ICANN*, Root Nameserver Year 2000 Status, 15. Juli 1999, <http://www.icann.org/committees/dns-root/y2k-statement.htm> abgerufen werden.

<sup>46</sup> *Gordon*, Controlling the Internet, Kap. 1.2. und 4.4.

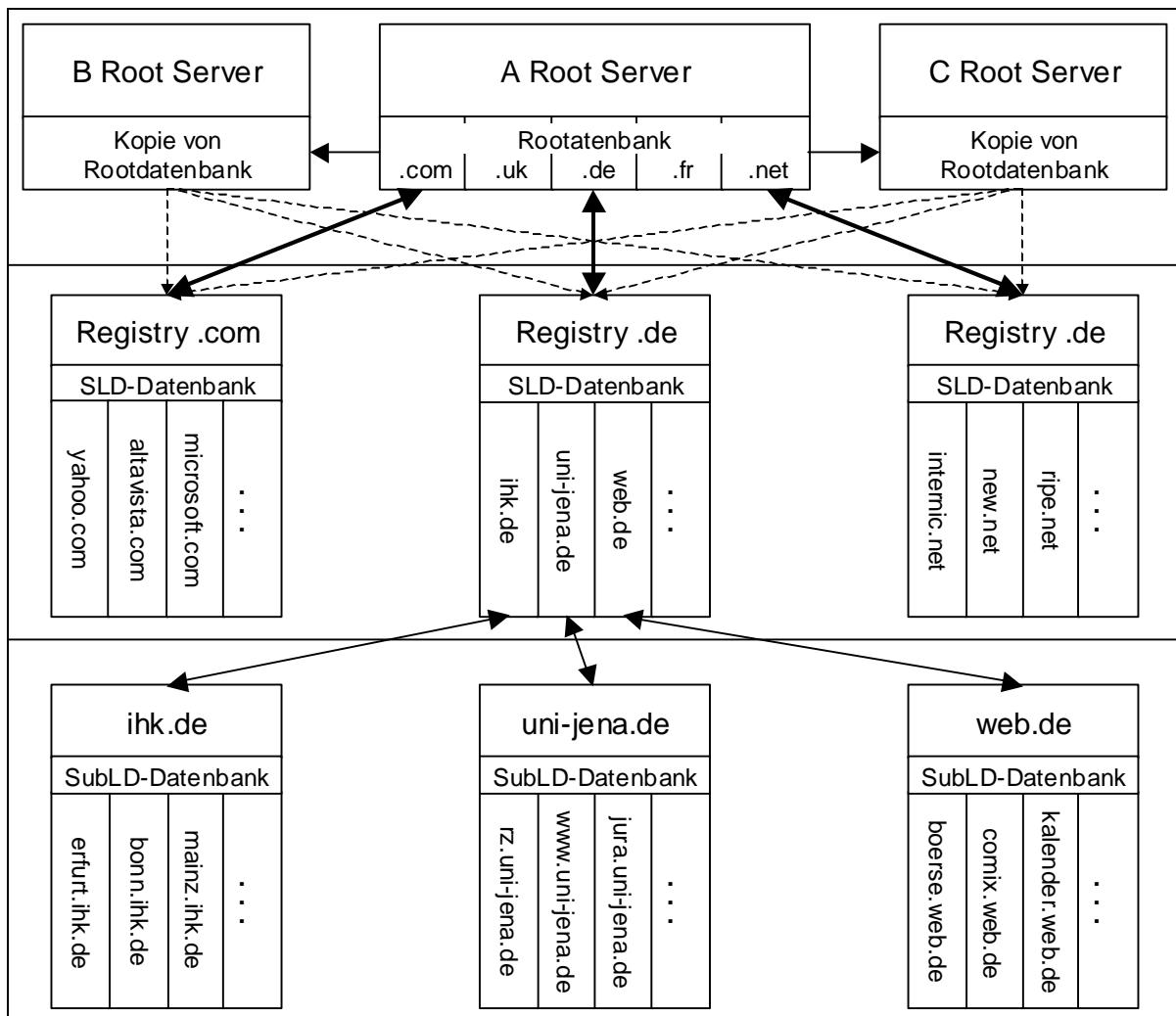


Abbildung 1 – Struktur des Domain Name Systems.

Auf die in den DNS-Datenbanken gespeicherten Informationen kann mittels der DNS-Server zugegriffen werden. Dazu sendet ein Computer, der eine IP-Adresse für einen Domainnamen wissen möchte, eine Anfrage an einen DNS-Server. Dieser sendet dann die zugehörige IP-Adresse zurück (sogenanntes *IP-Resolving*). Sollte ein *Name Server* die Domainadresse nicht kennen, leitet er die Anfrage an einen höherrangigen *Name Server* weiter, welcher selbst die IP-Adresse zurückliefert<sup>47</sup>.

Die Kontrolle über die *Root Name Server* ist bedeutsam für eine Überwachung des gesamten DNS. Dadurch, daß unabhängige Institutionen auf freiwilliger Basis die einzelnen Server betreiben, ist ein möglichst reibungsloser Betrieb gewährleistet. Einzelne Serverbetreiber können somit nur geringen Einfluß auf das *IP-Resolving* nehmen. Alle Rootserver orientieren sich an dem Datenbestand des *A Root Server*, welcher täglich aktualisiert wird<sup>48</sup>. Würde ein

<sup>47</sup> Vgl. zu den technischen Aspekten des IP-Resolving: *Kuri, c't* 1996, Heft 12, 334ff.

<sup>48</sup> Näheres zum Aufbau der Rootserver siehe *RFC 1034*, Mockapetris, Kap. 2.4.

## 2.3. Staatlicher Eingriff vs. Selbstregulierung

---

Rootserver andere Daten als die vom NSI bereitgestellten anbieten, würde dies unweigerlich zu einer Fragmentierung des Internets führen<sup>49</sup>.

Die Stabilität des DNS basiert nicht auf rechtlichen Grundlagen, denn das System des Daten-austausches wird gerade nicht durch Verträge oder Gesetze manifestiert. Im wesentlichen beruht es auf einem gegenseitigen Entgegenkommen<sup>50</sup> der Betreiber der einzelnen *Root Name Server* und der Akzeptanz der Struktur des DNS, welche aus der Frühgeschichte des Internets herrührt. Insgesamt ist damit das DNS potentiell instabil.

### 2.3. Staatlicher Eingriff vs. Selbstregulierung

Wie im Kapitel 2.2.2 oben festgestellt, besteht das Internet aus vielen einzelnen Computern, welche über Router und Knotenpunkte miteinander verbunden sind. Dabei ist jeder Knotenpunkt unabhängig und nicht einer zentralen Organisation untergeordnet. Auch muß sich ein Internetnutzer nicht einer solchen Organisation anschließen, um an der Kommunikation teilnehmen zu dürfen. Es existiert somit keine zentrale Organisation, welche die Internetnutzung reguliert, welche eine Erlaubnis zum Anschluß an das Netz erteilt und bei der man sich beschweren kann, wenn eigene Rechte verletzt wurden. Nach einem Exkurs auf verschiedene Beispiele von Selbstregulierung innerhalb des deutschen Staatssystems und allgemeinen verfassungsrechtlichen Vorgaben, soll deshalb erklärt werden, wer das Internet steuern darf und Regeln für die Nutzung entwerfen soll.

#### 2.3.1. Selbstregulierung im Deutschen Staatssystem

Eine Selbstregulierung ist dem deutschen Staats- und Wirtschaftssystem nicht fremd. Eine ursprüngliche und inzwischen weit entwickelte Form gesellschaftlicher Selbstregulierung ist im kollektiven Arbeitsrecht zu finden. Ausgehend von der Gewähr der Koalitionsfreiheit im Rahmen des Art. 9 Abs. 3 GG wird Arbeitnehmern und Arbeitgebern ein von staatlicher Regulierung freier Raum gelassen, in dem sie eigenverantwortlich ihre arbeitsvertraglichen Beziehungen bestimmen können<sup>51</sup>. Insbesondere das Tarifvertragsgesetz gibt diesen verfassungsrechtlichen Schutz der kollektiven Selbstregulierung wieder und ermöglicht eine staatliche Anerkennung der im privaten Verfahren ausgehandelten Tarifverträge, § 5 Abs. 1 TVG. Die Tarifverträge sind damit privat gesetztes Recht, welches von den nicht in die staatliche Organisation eingebundenen, privatrechtlich organisierten Gewerkschaften und Arbeitsgeberverbänden gestaltet wird. Im Wege der Allgemeinverbindlichkeitserklärung durch den Bundesminister für Arbeit und Sozialordnung erlangen diese zunächst nur zwischen den Tarifparteien verbindlichen Verträge eine Außenwirkung für nichttarifgebundene Arbeitgeber und Arbeitnehmer.

Eine besonders in der Technik aber vor allem auch im Umweltbereich wichtige Form der Selbstregulierung stellt die Erarbeitung technischer Regeln durch die verschiedenen privat-

---

<sup>49</sup> Gordon, Controlling the Internet, Kap. 1.2. und 4.4.

<sup>50</sup> Nordemann, NJW 1997, 1897, 1899

<sup>51</sup> BVerfG vom 1. März 1979, BVerfGE 50, 290, 371.

rechtlich organisierten Normungsverbände dar<sup>52</sup>. Die gesellschaftliche Bedeutung der Normungsinstitute ist heutzutage außerordentlich. Als eine der wichtigsten Verbände gelten das *Deutsche Institut für Normung* (DIN), der *Verein Deutscher Ingenieure e.V.* (VDI) und der *Verband Deutscher Elektrotechniker* (VDE). Die verabschiedeten Normen und Regeln sollen der technischen Sicherheit dienen, die Produktqualität gewährleisten sowie Standardisierung und damit stärkere Chancengleichheit im Wettbewerb ermöglichen<sup>53</sup>. Obgleich die privaten Normen dieser Verbände keine Rechtsqualität entfalten<sup>54</sup>, ist ihre faktische Bindungswirkung kaum zu unterschätzen. Darüber hinaus wird das Umweltrecht unter Verwendung diverser Generalklauseln häufig mit den technischen Regeln verknüpft<sup>55</sup>. Nach allgemeiner Auffassung werden die Regelwerke als antizipierte Sachverständigengutachten eingeordnet<sup>56</sup> und können im beschränkten Maße behördlichen und gerichtlichen Entscheidungen ohne weiteres zugrundegelegt werden<sup>57</sup>. Eine intensivere Bindungswirkung können technische Normen durch die Bezugnahme von Rechtsnormen im Wege der Verweisung erhalten<sup>58</sup>. So finden sich zum einen starre gesetzliche Verweise auf bestimmte technische Normen (zum Beispiel §§ 2, 3, 4 und 6 der 10. BImSchV<sup>59</sup> mit Verweisen auf bezeichnete DIN-Normen) oder entsprechende Verordnungsermächtigungen (zum Beispiel § 7 Abs. 5 BImSchG oder § 19 Abs. 4 ChemG<sup>60</sup>) und zum anderen dynamische Verweise auf aktuelle und zukünftige Bestimmungen von Normungsinstituten (zum Beispiel § 1 der 2. DVO zum Energiegesetz<sup>61</sup> mit Verweis auf die Bestimmungen des VDE).

In der letzten Zeit wurden vor allem im Umweltbereich sogenannte Selbstverpflichtungsvereinbarungen abgeschlossen. Industrieverbände verpflichteten sich mit diesen, bestimmte Verfahren einzusetzen, die Umweltbelastungen herabsetzen oder vermeiden helfen sollen. Zum einen soll durch normvollziehende Absprachen die Umsetzung von bestehenden Gesetzesre-

---

<sup>52</sup> Aus DIN, DIN-Normenheft 10, DIN 820 Teil 1 Nr. 2 Satz 1 ergibt sich der Begriff Norm: „Normung ist die planmäßige, durch die interessierten Kreise gemeinschaftlich durchgeführte Vereinheitlichung von materiellen und immateriellen Gegenständen zum Nutzen der Allgemeinheit.“

<sup>53</sup> Schmidt-Preuß, VVDStRL 56 (1997), 160, 203.

<sup>54</sup> Vgl. BVerfG vom 29. August 1961, NJW 1962, 506.

<sup>55</sup> Vgl. zum Beispiel die Klauseln: „allgemein anerkannte Regeln der Technik“ (§ 7a Abs. 1 Satz 1 WHG), „Stand der Technik“ (§ 5 Abs. 1 Nr. 2 BImSchG) oder „Stand von Wissenschaft und Technik“ (§ 7 Abs. 2 Nr. 3 AtomG).

<sup>56</sup> Vgl. Breuer, AöR 101 (1976), 46, 79ff. und Nicklisch, NJW 1983, 841ff. Das BVerwG (vom 17. Februar 1978, BVerwGE 55, 250, 255ff.) ordnet den Begriff „antizipiertes Sachverständigengutachten“ zu den technischen Verwaltungsvorschriften ein, welche in Zusammenarbeit zwischen Staat und Normungsverbänden entwickelt werden. Hierzu gehören z.B. die nach § 48 BImSchG ergangenen Technische Anleitung zur Reinhaltung der Luft (TA Luft) vom 27. Februar 1986, GMBI. 1986, 95, ber. S. 202 und die Technische Anleitung zum Schutz gegen Lärm (TA Lärm) vom 26. August 1998, GMBI. 1998, 503.

<sup>57</sup> Nach dem BVerwG (vom 29. April 1988, BVerwGE 79, 254, 264) kommt privaten technischen Regelwerken eine widerlegbare Indizwirkung zu. Vgl. auch Krist, UPR 1993, 178ff.

<sup>58</sup> Vgl. Kloepfer/Elsner, DVBl. 1996, 964, 967.

<sup>59</sup> Verordnung über die Beschaffenheit und die Auszeichnung der Qualitäten von Kraftstoffen, vom 13. Dezember 1993, BGBl. I 1993, 2036; BGBl. I 1997, 2858; BGBl. I 1999, 2845

<sup>60</sup> Gesetz zum Schutz vor gefährlichen Stoffen vom 16. September 1980, BGBl. I 1980, 1718.

<sup>61</sup> Fassung vom 14. Januar 1987, BGBl. I 1997, 146.

## 2.3. Staatlicher Eingriff vs. Selbstregulierung

---

geln oder Verwaltungsmaßnahmen vermieden werden<sup>62</sup>. Zum anderen sollen normvertretende Absprachen konkrete Gesetzes- oder Verordnungsvorhaben verhindern<sup>63</sup>. Gegenüber klassischen Ge- und Verbotsnormen des Verwaltungsrechts wird der Vorteil von Selbstverpflichtungsabkommen darin gesehen, daß durch sie unnötiger Zwang vermieden wird und die betroffenen Unternehmen eine größere Handlungsfreiheit bei der Umsetzung der gemeinsam mit staatlichen Vertretern ausgehandelten Ziele gewährt wird. Individuelle Strukturen werden dadurch deutlich besser berücksichtigt und damit Anreize geschaffen, über das gesetzlich vorgesehene Maß hinausgehende Regelungen zu treffen<sup>64</sup>.

Als letztes Beispiel aus einer Vielzahl weiterer verschiedenartiger Möglichkeiten zur Selbstregulierung sollen die dem öffentlichrechtlichen Sektor zuordenbaren Selbstverwaltungskörperschaften im Bereich des deutschen Gewässer- und Bodenschutzes erwähnt werden<sup>65</sup>. Das Prinzip der gemeinsamen Verwaltung von Gewässern und Böden lässt sich auf die Deich- und Sielverbände der letzten Jahrhunderte zurückführen. Diese Verbände haben ihre rechtliche Grundlage besonders im Wasserverbandsgesetz<sup>66</sup> des Bundes gefunden. Die Verbände übernehmen die Aufgabe, bauliche Anlagen zu errichten und zu betreiben sowie Arbeiten an Grundstücken oder Maßnahmen, die der Gewässerbewirtschaftung und dem Bodenschutz dienen, vorzunehmen.

Der Verfassung der BRD können zunächst keine konkreten Bestimmungen zur Selbstregulierung der komplex strukturierten Problemlagen entnommen werden. Dennoch ist es zur Einführung notwendig, die verfassungsrechtlichen Vorgaben und Grenzen gesellschaftlicher Selbstregulierung zu bestimmen, bevor intensiver auf den speziellen Anwendungsbereich der Internetregulierung eingegangen werden kann. Zunächst generieren die allgemeine Handlungsfreiheit des Art. 2 Abs. 1 GG, die Wissenschaftsfreiheit des Art. 5 Abs. 3 GG und die wirtschaftsspezifischen Freiheitsrechte der Art. 9, 12 und 14 GG eine staatliche Verpflichtung.

---

<sup>62</sup> Hierzu zählt zum Beispiel die Umsetzung der Verordnung über die Vermeidung und Verwertung von Verpackungsabfällen, Verpackungsverordnung in der Fassung vom 21. August 1998, BGBI. I 1998, 2379, zuletzt geändert durch VO vom 28. August 2000, BGBI. I 2000, 1344 durch das Duale System. Dazu siehe Koch, NVwZ 1998, 1155ff.

<sup>63</sup> Gestützt auf die freiwillige Selbstverpflichtung der Mobilfunkbetreiber setzte das Bundesumweltministerium die bereits in Angriff genommene Novellierung der 26. BImSchV vom 16. Dezember 1996, BGBI. I 1996, 1966 zunächst aus. Vgl. Gneiting/Demmelhuber, c't 2002, Heft 3, 82, 85 und Bundesregierung Deutschland, Die Vorsorgemaßnahmen der Bundesregierung im Bereich Mobilfunk, 7. Dezember 2001,

[http://www.bundesregierung.de/top/dokumente/Artikel/ix\\_65285.htm](http://www.bundesregierung.de/top/dokumente/Artikel/ix_65285.htm). Ein weiteres aktuelles Beispiel stellen die Konsensgespräche um den Ausstieg aus der Kernenergie dar, die am 14. Juni 2000 zwischen der Bundesregierung und vier Energieversorgungsunternehmen zu einer Verständigung geführt haben, siehe Vereinbarung zwischen der Bundesregierung und den Energieversorungsunternehmen, umwelt 2000, Heft 7/8, Sonderteil, im WWW unter UWG Ahaus, [http://www.uwg-ahaus.de/aktuelljuni\\_nondoku.htm](http://www.uwg-ahaus.de/aktuelljuni_nondoku.htm) zu finden. Zur Selbstverpflichtung im Ganzen siehe auch Di Fabio, JZ 1997, 969ff.

<sup>64</sup> Vgl. Steigleder, WissR 33 (2000), 111, 115 und Kloepfer/Elsner, DVBl. 1996, 964, 967.

<sup>65</sup> Eingehend hierzu Kloepfer/Elsner, DVBl. 1996, 964, 967f.

<sup>66</sup> Gesetz über Wasser- und Bodenverbände vom 12. Februar 1991, BGBI. I 1991, 405.

tung, Aufgabenbereiche der Wirtschaft und Gesellschaft selbstregulierend zu überlassen<sup>67</sup>. Art. 20 Abs. 3 GG gebietet die Anerkennung des sich in der Gesellschaft entwickelten Gewohnheitsrechts. Tarifverträge, Vereins- und Parteisatzungen sind nach dem Art. 9 Abs. 1 und 3 sowie dem Art. 21 Abs. GG verfassungsrechtlich veranlaßt und gewährleistet<sup>68</sup>. Auch das der Bundesrepublik Deutschland zugrundeliegende Ordnungsprinzip der sozialen Marktwirtschaft stützt das Gebot der Selbstregulierung<sup>69</sup>. Aus der Sicht der Europäischen Gemeinschaft gewährleisten dies ansatzweise die Gemeinschaftsgrundrechte<sup>70</sup> und die primär an die Mitgliedstaaten gerichteten Prinzipien der Subsidiarität und der Verhältnismäßigkeit nach Art. 3b EGV. Diese Regeln gewähren Unternehmen, wie auch der Wissenschaft einen Kernbestand an Autonomie, ohne dessen eine Marktwirtschaft nicht vorstellbar ist. Besonders in den Bereichen ist eine Eigenverwaltung notwendig, in denen die staatlichen Eingriffsmöglichkeiten schon wegen der Komplexität und Eigengesetzlichkeit der Materie an ihre Schranken stoßen. So weist besonders der wissenschaftlich-technische Bereich kaum mit staatlicher Gesetzgebung und Verwaltung faßbare Strukturen auf, welche die Notwendigkeit einer Selbstregulierung direkt indizieren<sup>71</sup>. Autonome Verwaltung verlangt jedoch Eigenverantwortung und die Befähigung zu freier und selbstbestimmter Gestaltung der eigenen Organisation und der Beziehungen zur Umwelt. Der Staat ist folglich gehalten, nur dort regelnd einzutreten, wo die Fähigkeiten der Gesellschaft überfordert sind oder eine Selbstregulierung sich schädlich auf die Gemeinschaft auswirkt.

Die Grundrechte stellen gleichzeitig auch eine Grenze gesellschaftlicher Freiheit dar<sup>72</sup>. Auch Staatszielbestimmungen wie Art. 20a GG oder das Demokratieprinzip, nach welchem alle Staatsgewalt vom Volke auszugehen hat, verpflichten den Staat, selbst die verschiedenen gesellschaftlich notwendigen Aufgaben auszuführen. Die Regeln der Verfassung stehen damit in einer Wechselwirkung mit den Regulierungstätigkeiten von Staat und Gesellschaft<sup>73</sup>. Soweit staatliche Verwaltungstätigkeit auf privatrechtlich organisierte Verbände übertragen wird, kann dies positiv die Freiheitsrechte des einzelnen erweitern, da er neue Mitwirkungsmöglichkeiten an der Gestaltung seines Umfeldes erlangt. Andererseits kann dies eine freiheits einschränkende Wirkung entfalten, soweit Individuen diesen Organisationen und deren aufgestellten Regeln ausgeliefert sind und nunmehr keinen rechtlichen Rückgriff auf den Staat nehmen können. Betroffene Personen sind heute selbst aufgerufen, sich zu organisieren, um ihre Interessen zu vertreten und können folglich nicht mehr darauf vertrauen, daß der Staat in ge-

<sup>67</sup> Zur Selbstregulierung im Bereich naturwissenschaftlich-technischer Forschung siehe *Steigleder*, WissR 33 (2000), 111ff. Zu wirtschaftsspezifischen Freiheitsrechten vgl. *Ossenbühl*, AöR 115 (1990), 1, 12ff. Zusammenfassend siehe auch *Hufen*, Staatsaufgaben, S. 284ff.

<sup>68</sup> *Kloepfer/Elsner*, DVBl. 1996, 964, 968.

<sup>69</sup> Siehe dazu *Schmidt-Preuß*, DVBl. 1993, 236ff. und *Badura*, DÖV 1989, 491ff.

<sup>70</sup> Zum Eigentumsrecht und zum Recht der freien Berufsausübung vlg. *EuGH* vom 17. Oktober 1995, „Fisher- men's Organisations u.a.“, Slg. 1995 I, 3115, 3152ff.; *EuGH* vom 5. Oktober 1994, „Bananenmarktordnung“, Slg. 1994 I, 4973, 5065ff.; *EuGH* vom 13. Dezember 1979, „Hauser“, Slg. 1979, 3727, 3745/3750.

<sup>71</sup> Vgl. *Hufen*, Staatsaufgaben, S. 286.

<sup>72</sup> Ausführlich hierzu *Di Fabio*, VVDStRL 56 (1997), 235, 252ff., *Schmidt-Preuß*, VVDStRL 56 (1997), 160, 172ff. sowie *Hufen*, Staatsaufgaben, S. 285ff.

<sup>73</sup> Ähnlich *Di Fabio*, VVDStRL 56 (1997), 235, 252.

## 2.3. Staatlicher Eingriff vs. Selbstregulierung

---

rechter Weise ihre Anliegen vertritt. Selbstregulierung ist vor allem durch die Bildung von Organisationen und Verbänden charakterisiert, welche häufig erst durch die Bündelung der einzelnen Kräfte ein deutliches Auftreten nach Außen ermöglichen. Organisationen sind das Fundament erfolgreicher Selbstregulierung, denen sich der Bürger kaum entziehen kann<sup>74</sup>.

Ein Problem stellt die Verschiebung der Grundrechtspositionen dar. Im Verhältnis Bürger zum Staat besteht nur eine eindimensionale einseitige Beziehung, in welcher der Staat die Grundrechte des Bürgers zu beachten hat, aber sich nicht selbst auf diese berufen kann. Selbstverwaltungsorganisationen sind jedoch im Gegensatz zum Staat nicht grundrechtsgebunden, sondern ihnen fällt ein eigener Grundrechtsschutz zu. Die Durchsetzung grundrechtlicher Abwehr- oder Leistungsansprüche durch betroffene Dritte gestaltet sich in diesem Dreiecksverhältnis somit schwieriger als im herkömmlichen staatlichen Über-Unterordnungsverhältnis<sup>75</sup>.

Schließlich stellt sich die Frage, inwieweit durch die Verlagerung staatlicher Aufgaben auf den privaten Sektor das Demokratieprinzip verletzt wird. Das Handeln durch Staatsorgane lässt sich in jeglicher Erscheinungsform gemäß Art. 20 Abs. 2 Satz 1 GG auf das Volk zurückführen. Durch die Wahlen von Abgeordneten des Bundestages, der Landtage, der Gemeinderäte oder sonstigen Plenarversammlungen lässt sich eine ununterbrochene Legitimationskette bis zum einfachen Beamten konstruieren<sup>76</sup>. Folglich ist der Staat gehalten, gesellschaftlich wahrgenommene Freiheit von demokratisch bedingter öffentlicher Gewalt zu trennen<sup>77</sup>. Dies wird jedoch nur in den seltensten Fällen gelingen, da es kaum eine klar bestimmbare Grenzlinie zwischen diesen beiden Regelungsbereichen gibt. Vielmehr ist in allen zu verwaltenden Materien ein fließender Übergang feststellbar, welcher nur eine Grenzziehung abhängig von politischer und gesellschaftlicher Einstellung ermöglicht.

Im Rahmen dieser unklaren Gemengelage der Wirkungen von Grundrechten und Demokratieprinzip muß verlangt werden, daß auch die selbstregulierenden Organisationen bei der Wahrnehmung halbstaatlicher Aufgaben verfassungsrechtlich gewährte Prinzipien beachten. Dazu zählen aus rechtsstaatlicher Sicht das Einhalten des Gleichheits-, Mehrheits- und Transparentsgebots, der Schutz von Minderheiten oder der Ausgleich von individuellen Defiziten. Auf der Grundlage dieser demokratisch-rechtsstaatlichen Mindeststandards<sup>78</sup> kann zum Beispiel verlangt werden, daß Entscheidungen begründet und der Allgemeinheit zugänglich gemacht werden, daß interessierte Kreise sich in ausgewogener Weise am Entscheidungsprozeß beteiligen können<sup>79</sup> sowie, daß gegen die Entscheidungen Einwendungsmöglichkeiten beste-

---

<sup>74</sup> Vgl. *Di Fabio*, VVDStRL 56 (1997), 235, 254f.

<sup>75</sup> Siehe schon *Scheuner*, VVDStRL 11 (1954), 1, 38 und *Gallwas*, VVDStRL 29 (1971), 211, 216f.

<sup>76</sup> Vgl. *BVerfG* vom 24. Mai 1995, BVerfGE 93, 37, 68: „Demokratischer Legitimation bedarf die Ausübung der Staatsgewalt in ihrer jeweiligen Funktion.“

<sup>77</sup> Vgl. *Di Fabio*, VVDStRL 56 (1997), 235, 264.

<sup>78</sup> Siehe *Schmidt-Preuß*, VVDStRL 56 (1997), 160, 205.

<sup>79</sup> So ist in der DIN vorgesehen, „daß die interessierten Kreise in einem angemessenen Verhältnis vertreten sind“, siehe *DIN*, DIN-Normenheft 10, DIN 820 Teil 1 Nr. 3.4 Abs. 2 und 3 Satz 1. Auch ist vorgesehen, daß

hen oder Schiedsverfahren zur Verfügung gestellt werden. Darüber hinaus hat der Bundesgesetzesgeber im Rahmen seiner Gesetzgebungskompetenz nach Art. 74 Abs. 1 Nr. 11 GG (Recht der Wirtschaft) sowie nach Art. 74 Abs. 1 Nr. 11a, 12 und 21ff. GG (Kernenergie, Arbeitsrecht, Schiffahrt, Straßenbau, Abfallbeseitigung) selbst notfalls regulierend einzutreten, um die erforderlichen Bedingungen für einen ausreichenden Grundrechtsschutz der Betroffenen zu sichern.

### 2.3.2. Regulierung des Internets

Obgleich gezeigt werden konnte, daß die Selbstregulierung ein notwendiges Element eines demokratischen Staatssystems ist, bleibt offen, inwieweit der Staat regulierend in die Entwicklung des Internets und des DNS-Systems eingreifen sollte. Entstanden aus einem schnellen und kostengünstigen Kommunikationsmedium zwischen Wissenschaftlern, konnten weder Staat noch Gesellschaft das explosionsartige Wachstum des Internets erahnen. Inzwischen sind unter verschiedenen Internetadressen Firmen, wie *Yahoo, Inc.*, *AOL, Inc.* oder *Amazon, Inc.* zu finden, welche Milliarden Dollar im Internet umsetzen. Nicht für einen solch expandierenden Markt entworfen, ist das aktuelle rechtliche Rahmengerüst für die kommerzielle Nutzung des Internets stets veraltet<sup>80</sup>. Der Spalt zwischen der sich ständig weiter entwickelnden Technik und den Rechtsregeln ist zumeist nützlich und notwendig, damit die Entwicklung nicht unnötig gebremst wird. Um eine völlige Entfaltung des elektronischen Marktplatzes zu gewähren, ist bei der Regulierung ein technologienutraler Ansatz zu wählen, der auf die Änderungen der Technologie reagiert, anstatt die Entwicklung der Technologie zu forcieren.

Ein Regulierungsansatz für das Internet muß flexibel und stark genug sein, um auch den Herausforderungen des nächsten Jahrhunderts gewachsen zu sein. Es muß eine Möglichkeit der Schlichtung von Rechtsstreitigkeiten bestehen und die Netznutzer müssen das „Recht des Cyberspace“ akzeptieren und als gerecht empfinden<sup>81</sup>. Verletzungen der Regeln müssen durch die zugrundeliegende Technologie, soziale Kräfte oder den Systemadministrator bestraft werden können. Nicht nur im Internet selbst, auch in der realen Welt muß eine solche Rechtsetzung, -sprechung und -vollziehung anerkannt werden.

Um die Regulierung des Internets zu ermöglichen, existieren verschiedene Ansätze. Einerseits kann man das Internet voll unter die staatliche Kontrolle stellen<sup>82</sup>. Andererseits wäre die Bil-

---

bei Normungsanträgen und Normentwürfen die Öffentlichkeit Gelegenheit zur Information und zum Einspruch erhält (DIN, DIN-Normenheft 10, DIN 820 Teil 1 Nr. 5.3) und gegebenenfalls ein Schlichtungs- und Schiedsverfahren eingeleitet werden kann, (DIN, DIN-Normenheft 10, DIN 820 Teil 4 Nr. 2.4.7.)

<sup>80</sup> Vgl. *Geist*, Wash. L. Rev. 521, 523.

<sup>81</sup> *Gibbons*, 6 Cornell J.L. & Pub. Pol'y 475, 481.

<sup>82</sup> Diesen Weg versuchen autoritäre Staaten zu begehen, welche im großen Umfang unerwünschte Informationen aus dem Internet herausfiltern, vgl. u.a. *Heise-Newsticker*, China: Nur offizielle Nachrichten im Web, 7. November 2000. Die Vereinigung *Reporters Sans Frontières* analysiert in ihrer umfangreichen Studie, The Enemies of the Internet, 59 Staaten, welche auf verschiedene Weise den Zugang zum Internet oder zu bestimmten Informationen im Netz sperren, im Internet unter <http://www.rsf.fr/uk/homenemis.html> zu finden. Als wahre Feinde des Internets werden neben vielen anderen besonders Weißrussland, China, Kuba oder der Irak darge-

## 2.3. Staatlicher Eingriff vs. Selbstregulierung

---

dung eines eigenen Rechtssystems für das Internet als „Cyberspace“ möglich, das neben Rechtssetzung und -kontrolle auch eine eigene Jurisdiktion und Durchsetzung der rechtlichen Regelungen ermöglicht. Als dritter Ansatz wäre eine Regulierung auf Vertragsbasis unter Anwendung des Privatrechtes erwägenswert. Alle drei Regulierungsvarianten müßten dabei auf die aktuelle Struktur des Internets, als größtenteils geographisch unabhängiges Gebilde, Rücksicht nehmen. Sicherlich wird sich keine der drei Varianten als allgemeingültiges Prinzip durchsetzen können. Die meisten Staaten werden es kaum zulassen, daß ihnen die Kontrolle über das Internet voll entzogen und auf eine quasi-staatliche selbständige Körperschaft übertragen wird, sondern werden durch eigene Gesetze in die Struktur des Internets eingreifen wollen. Auch wird sich die Lösung kleinerer und thematisch begrenzter Problemkreise, wie zum Beispiel der Zugang zu verschiedenen Angeboten im Internet, wohl auf das Privatrecht beschränken lassen.

Obwohl in den Anfangsjahren des Internets (bis 1996) verschiedentlich versucht wurde, das Internet analog anderen Rechtssystemen zu behandeln, änderte sich diese Ansicht Anfang 1997. Allmählich begann man, um die Besonderheiten herauszuarbeiten, die einzelnen Aktivitäten im Internet nach Art und Weise zu qualifizieren und zu analysieren<sup>83</sup>. Entsprechend dem Ursprung des Internets erfolgte die Diskussion fast ausschließlich in den USA. In Deutschland zeigte die Rechtswissenschaft nur geringes Interesse an grundlegenden Problemen der Regulierung des Internets. Bis 1996 erschienen zahlreiche Arbeiten im englischsprachigen Raum, welche unterschiedliche Analogien anboten, zum Beispiel<sup>84</sup>:

- zu den 0800 Telefonnummern, da auch im Internet von verschiedenen Stellen Informationen abgerufen, oder Waren bestellt werden können<sup>85</sup>,
- zum Umweltrecht, da die Daten im Internet Wege nehmen können, die genauso unvorhersehbar sind, wie der Schadensverlauf von Umweltverschmutzungen<sup>86</sup>,
- zum Seerecht<sup>87</sup>, zum Weltraumrecht<sup>88</sup> oder zum Recht der Antarktis<sup>89</sup>, da, wie in diesen Räumen, niemand Souveränität über das Internet beanspruchen kann.

---

stellt. Den extremsten Weg gingen die Taliban in Afghanistan, welche die Nutzung des Internets völlig verboten hatten, Rötzer, *Telepolis* 9082.

<sup>83</sup> Vgl. in einer Zusammenfassung: *Geist*, Wash. L. Rev. 521, 525.

<sup>84</sup> Vgl. *Geist*, Wash. L. Rev. 521, 546ff.

<sup>85</sup> *Zembek*, 6 Alb. L.J. Sci. & Tech. 339, 370-376.

<sup>86</sup> *Zembek*, 6 Alb. L.J. Sci. & Tech. 339, 376-380.

<sup>87</sup> *Burnstein*, 29 Vand. J. Transnat'l L. 75, 103-108.

<sup>88</sup> *Burnstein*, 29 Vand. J. Transnat'l L. 75, 110f.; zwei wichtige von fünf internationalen Übereinkommen sind das Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, in Kraft seit 10. Oktober 1967,

<http://www.oosa.unvienna.org/SpaceLaw/outerspt.htm> und das Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, in Kraft seit 11. Juli 1984,

<http://www.oosa.unvienna.org/SpaceLaw/moon.htm>.

<sup>89</sup> *Burnstein*, 29 Vand. J. Transnat'l L. 75, 111f.

Ein wahrhaftig internationaler Raum ist die hohe See, in dem sich das Seerecht über viele hundert Jahre entwickelt hat und zum Teil aus dem Seehandelsrecht der Rôles d'Oléron<sup>90</sup> und der Lex Rhodia<sup>91</sup> stammt<sup>92</sup>. Viele Handlungen auf hoher See drohten nicht reguliert werden zu können, da sie nicht an ein festes Land gebunden waren<sup>93</sup>. Andererseits konnte es einem Schiff nicht zugemutet werden, daß sich bei jedem Wechsel in ein neues nationales Gewässer das anzuwendende Recht ändern würde. Ebenso scheinen Transaktionen im Internet kaum rechtlich faßbar zu sein, da sie genauso wenig an einen Ort gebunden sind. Auch das Internet läßt sich nicht durch den Alleingang eines Landes regulieren, sondern erfordert gleichfalls eine internationale Regelung<sup>94</sup>. Ein eigenständiges Seerecht existiert jedoch auf internationaler Ebene nicht<sup>95</sup>, sondern im Seerecht folgt das anzuwendende Recht der Flagge, unter welcher ein Schiff registriert ist<sup>96</sup>. Analog würde es sich anbieten, im Internet das anwendbare Recht nach dem Sitz des jeweiligen ISP zu richten, über welchen ein Nutzer auf das Internet zugreift oder Inhalte anbietet<sup>97</sup>.

Nachteilig bei dieser Lösung ist, daß Nutzer bevorzugt über einen ISP das Netz benutzen würden, welcher sich in einem Land mit sehr geringen Rechtsstandards, zum Beispiel gerinem Datenschutz oder fehlendem Recht zum Schutz von geistigem Eigentum, befindet<sup>98</sup>. Geschickte Anwender könnten dies ausnutzen und über solche Länder Softwarepiraterie oder Markenrechtsverletzungen begehen, ohne bestraft werden zu können<sup>99</sup>.

Andererseits entstanden ausgehend von Post und Johnson Bestrebungen, das Internet (Cyberspace) als eigenen Rechtsraum zu betrachten, in welchem Analogien zum herkömmlichen Recht nicht funktionieren<sup>100</sup> (vgl. Kapitel 2.3.4.1 unten). Es sollte von einem eigenen Rechtswerk regiert werden. Mit Überschreiten der Grenze von der physischen zur virtuellen

<sup>90</sup> Eine Sammlung von Entscheidungen, benannt nach der französischen Insel Oléron, welche im 14. Jahrhunder in verschiedenen Übersetzungen in Westeuropa verbreitet war.

<sup>91</sup> Lex Rhodia de iactu: Seerecht der griechischen Insel Rhodos, welche im 2. Jahrhundert v. Chr. die Ägäis beherrschte.

<sup>92</sup> *Tetley*, 20 *Syracuse J. Int'l L. & Com.* 105, 109ff.

<sup>93</sup> Vgl. *Perritt*, *Berkeley Tech. L.J.* 413, 461ff.; generell: ders., 38 *Vill. L. Rev.* 349, 352.

<sup>94</sup> *Burnstein*, 29 *Vand. J. Transnat'l L.* 75, 104; *Gibbons*, 6 *Cornell J.L. & Pub. Pol'y* 475, 506

<sup>95</sup> Nur in den Staaten USA und Kanada gibt es die Vorstellung eines General Maritime Law, welches anderes Recht verdrängt; vgl. zum Ganzen: *Tetley*, 20 *Syracuse J. Int'l L. & Com.* 105, 117ff.

<sup>96</sup> Z.B. bestimmt die United Nations Convention on the Law of the Sea, 10. Dezember 1982,

[http://www.un.org/Depts/los/convention\\_agreements/texts/unclos/closindx.htm](http://www.un.org/Depts/los/convention_agreements/texts/unclos/closindx.htm), die Abgrenzung und die Rechtsfolgen zwischen nationaler und internationaler See, die Nutzung von Meeresprodukten oder die Schiedsgerichtsbarkeit des International Tribunal for the Law of the Sea. Die Art. 27 und 28 ordnen hingegen an, welches Straf- und Zivilrecht auf Handelsschiffen anzuwenden ist. Vgl. auch die Convention on the High Seas vom 29. April, 1958 (13 U.S.T. 2312, T.I.A.S. No. 5200, 450 U.N.T.S. 82), <http://www.un.org/law/ilc/texts/hseafra.htm>. *Mankowski*, AfP 1999, 138, 141, Fn. 59 gibt einen ausführlichen Überblick zum Schrifttum über das Flaggenrecht.

<sup>97</sup> Vgl. z.B.: *US-White House*, Framework, Kap. Issues, III. 8. („The rules of the ‘country of origin’ should serve as the basis for controlling Internet advertising“); für eine Abwägung: *Burnstein*, 29 *Vand. J. Transnat'l L.* 75, 104.

<sup>98</sup> In einigen Ländern, wie z.B. Slovenien fehlt ein Patentrecht.

<sup>99</sup> *Gibbons*, 6 *Cornell J.L. & Pub. Pol'y* 475, 507

<sup>100</sup> *Johnson/Post* 48 *Stan. L. Rev.* 1367, 1378ff.

## 2.3. Staatlicher Eingriff vs. Selbstregulierung

---

werk regiert werden. Mit Überschreiten der Grenze von der physischen zur virtuellen Welt sollte der Cyberspace betreten werden, als würde eine Person eine Landesgrenze überschritten<sup>101</sup>.

Weniger radikal waren die Stimmen, die einen internationalen Vertrag forderten, um die verschiedenen Rechtsdispute zu lösen, welche von nicht zu vereinbarenden nationalen Regelungen herstammen<sup>102</sup>. Weiterhin wurde vorgeschlagen, Prinzipien des Vertragsrechtes anzuwenden, um das Internet zu regulieren. Die Vorschläge reichten von der Entwicklung von AGBs, welche an die Verträge zwischen Internetnutzern und Internetserviceprovidern angehängt werden sollten<sup>103</sup>, bis zur Anwendung des Vertragsrechtes in schiedsrichterlicher Rolle und durch private Schiedsgerichte<sup>104</sup>. Die Länder könnten versuchen, die Streitigkeiten mit dem herkömmlichen internationalen Privatrecht zu lösen. Handlungen im Internet würden dann als gewöhnliche zwischenstaatliche Transaktionen betrachtet. Es würde dann entweder das Recht des Landes anzuwenden sein, in dem die Fehlhandlung begangen wurde, oder in welchen die intensivste Verbindung zur Handlung bestand<sup>105</sup>.

Man erkannte, daß sich das Internet durch Computerprogramme selbst stark kontrollieren und regulieren läßt<sup>106</sup>. Dabei lenkt die Technologie den Daten- und Informationsstrom und damit den Zugang zu den Informationen im Internet<sup>107</sup>. Dies kann durch die Verwendung von Paßwörtern, Filtersoftware (zum Beispiel NetNanny<sup>108</sup>, We-Blocker<sup>109</sup>), Net-Ratingsysteme<sup>110</sup> oder Verschlüsselungsprogrammen erfolgen.

Erst ab 1997 begann man die Art und Weise der Internetaktivitäten mit in die rechtlichen Be trachtungen einzubeziehen. Um faire und gerechte Entscheidungen durch Gerichte zu ermöglichen, wurde eine intensive Betrachtung aller Fakten bezüglich des Kontaktes über das Internet zwischen Kläger und Beklagten gefordert, ohne das Internet pauschal in eine einzige Kategorie einzuordnen<sup>111</sup>. Der Umfang der Internetaktivitäten läßt sich am besten verstehen, wenn man die Effekte und Wirkungen des Internets auf die Gesellschaft in vier verschiedene Gruppen kategorisiert<sup>112</sup>.

---

<sup>101</sup> *Johnson/Post* 48 Stan. L. Rev. 1367, 1379f.

<sup>102</sup> Z.B. *Gigante*, 14 Cardozo Arts & Ent. L.J. 523, 548; *Crago*, 20 Hastings Int'l & Comp. L. Rev. 467, 491.

<sup>103</sup> *Dunne*, 35 Jurimetrics Journal 1, 11-14; *Trotter*, 55 U. Pitt. L. Rev. 993, 1028ff.; vgl. auch *Gibbons*, 6 Cornell J.L. & Pub. Pol'y 475, 518ff.

<sup>104</sup> Vgl. auch *Gibbons*, 6 Cornell J.L. & Pub. Pol'y 475, 532ff.; näheres zur Schiedsgerichtsbarkeit siehe auch: *Friedman*, 19 Hastings Comm/Ent L.J. und *Perritt*, 41 Vill. L. Rev. 1, 94-100.

<sup>105</sup> *Gibbons*, 6 Cornell J.L. & Pub. Pol'y 475, 505.

<sup>106</sup> *Lessing*, 5 CommLaw Conspectus 181, 183; ders. 48 Stan. L. Rev. 1403, 1408 sowie *HLRA*, 112 Harv. L. Rev. 1634ff.

<sup>107</sup> *Reidenberg*, 76 Tex. L. Rev. 553, 554f.

<sup>108</sup> Siehe <http://www.netnanny.com>.

<sup>109</sup> Siehe <http://www.we-blocker.com>.

<sup>110</sup> Entsprechend dem Ratingsystem der TV-Programme in den USA.

<sup>111</sup> Vgl.: *Thatch*, 23 Rutgers Computer & Tech. L.J. 143, 177; *Geist*, Wash. L. Rev. 521, 554ff.

<sup>112</sup> Ausführlich dazu siehe: *Geist*, Wash. L. Rev. 521, 554-569.

Die erste Kategorie, das Internet als ein Medium, beinhaltet die Nutzung des Internets für die Übertragung von Informationen, ohne die Beeinflussung der zugrundeliegenden Aktivitäten. In der zweiten Kategorie kann das Internet als Katalysator fungieren, wenn es die Quantität der Aktivitäten erhöht, ohne in das basierende Rechtsgerüst einzugreifen. Drittens ist es weiterhin möglich, daß das Internet als ein Auslöser für Veränderungen auftritt, wenn es zusätzlich zur Erhöhung der Quantität der Aktivitäten auch die rechtlichen Ansichten abändert. Im Bereich dieser drei Kategorien kann das Internet nicht als Grundlage einer neuen Jurisdiktion oder gar einer neuen Gesellschaftsstruktur herangezogen werden. Vielmehr stellt es ein neues Mittel dar, um die traditionellen sozialen Beziehungen weiterzuführen<sup>113</sup>. Die genannten Kategorien haben gemeinsam, daß rechtsprechende Institutionen diesen neuen Situationen, die sich innerhalb dieser Kategorien entwickeln, auf die gleiche Art und Weise, wie sie es immer bei neuen Rechtssituationen getan haben, begegnen werden<sup>114</sup>. Gerichte werden bestehendes Recht und Präzedenzfälle durch Auslegung auf den spezifischen, im Internet entstandenen Fall anwenden. Jede zusätzliche Regulierung würde zu einer unnötigen Restriktion der Entwicklung des Internets führen.

Die vierte Kategorie beinhaltet die Auswirkungen des Internets auf die Gesellschaft, die aus der Administration desselben herrühren. Hier erfordert die Verwaltung des Netzwerkes Betätigungen in einem unbekannten Umfeld und damit auch ein neues rechtliches Rahmengerüst. Diese Kategorie spiegelt den hauptsächlichen Anwendungspunkt eines speziellen Internetrechtes wieder. Da die technologische Struktur des Internets alle Nutzer unbedeutlich deren geographischer Lokalisation betrifft, greift die Internetverwaltung häufig in internationale Belänge ein. Diese Form der Regulierung ist durch ihre Natur neu und ohne direkten Vorgänger. Als regulierende Institutionen sind gleichzeitig nationale Regierungsinstitutionen sowie internetspezifische Gruppierungen (wie zum Beispiel die ICANN, das IAB, die IETF, etc.) beteiligt. Die Verwaltung der Domainnamen zählt zu den bekanntesten Beispielen der Internetregulierung, da die Vergabe der Domainnamen immer wieder Anstoß zu Rechtsstreitigkeiten gab<sup>115</sup>. Deshalb versucht man auf internationaler Ebene Standards für Vergabe und Streitlösung zu finden<sup>116</sup>.

Mit dem steten Wachstum des Internets erhält dessen Verwaltung immer größere Aufmerksamkeit, denn diese wirkt sich auf alle Onlineaktivitäten aus. So müssen unter anderem noch internationale Standards in Fragen von elektronischen Signaturen, von Verschlüsselungstechniken und über die Nutzung der Bandbreite des Netzes entwickelt werden, wobei in den einzelnen Staaten die Ansichten darüber stark divergieren.

---

<sup>113</sup> Siehe *Matsuura/Auffret*, Internet Law, Kap. The optimal relationship.

<sup>114</sup> *Matsuura/Auffret*, Internet Law, Kap. Internet law: the consequences.

<sup>115</sup> Beispiele zu deutschen Rechtsstreitigkeiten lassen sich unter *Netlaw*, Entscheidungssammlung Online-Recht, <http://www.netlaw.de/urteile/index.html> finden.

<sup>116</sup> Z.B. die Uniform Domain Name Dispute Resolution Policy der ICANN in Zusammenarbeit mit der WIPO, vgl. Kap. 3.3.1.2.

### 2.3.3. Staatliche Regulierung

Im Gegensatz zu den verschiedenen Rechtsstreitigkeiten vor nationalen Gerichten und der größeren Anzahl von Erörterungen durch die Rechtslehre begann sich das Interesse der staatlichen Regierungen an einer aktiven Regulierung des Internets erst spät zu entwickeln. Erst im Sommer 1997 wurden vermehrt Positionspapiere der verschiedenen Regierungen zu der Regulierung des Internets veröffentlicht. Dazu zählen Erklärungen von Japan<sup>117</sup>, den USA<sup>118</sup>, der Europäischen Union<sup>119</sup>, von Australien<sup>120</sup> und Kanada<sup>121</sup>. Hauptsächlich wurden diese Veröffentlichungen dem Ecommerce, dem am stärksten wachsenden Wirtschaftszweig, gewidmet. In den dargestellten fundamentalen Prinzipien aller fünf Positionspapieren treten dabei kaum große Differenzen auf. Das „*Framework for Global Electronic Commerce*“ der USA, zum Beispiel, zählt folgende Hauptprinzipien auf:

- Führung durch die Privatwirtschaft,
- Vermeidung von unnötigen Restriktionen,
- Erstellen eines vorhersehbaren, minimalen und dauerhaften Rechtsumfeldes und
- Beachtung der Einzigartigkeit des Internets auf globaler Basis.

Ebenso wird in einer Woche später veröffentlichten Erklärung der Europäischen Union eine Schlüsselrolle des privaten Sektors, die Entwicklung einer klaren und vorhersehbaren Regulierung und die Beachtung des speziellen Charakters und der transnationalen Natur des Internets gefordert. Die Ansichten, welche regulierende Rolle die Regierungen übernehmen sollten, waren jedoch nicht uniform. Während die USA und Australien sich für einen unregulierten, marktorientierten Ansatz einsetzten, ging die Europäische Union von einer aktiven Teilnahme des öffentlichen Sektors aus, um das volle Potential des Internets auszuschöpfen.

Es wurden allerdings keine speziellen Angaben gemacht, welche direkten Veränderungen und Eingriffe nötig wären, um den Ecommerce im Internet zu fördern. Diese ersten staatlichen Bemühungen waren zunächst in ihrem Inhalt zu generell und benötigten weiterer Betrachtung und Ergänzung<sup>122</sup>.

Ab diesem Zeitpunkt wurden verschiedene Gesetze und Regelungen erlassen, um in das Internet einzutreten<sup>123</sup>. Zwei Möglichkeiten stehen zur Regulierung offen. Erstens können bis-

---

<sup>117</sup> Japan, Digital Economy.

<sup>118</sup> Siehe *US-White House*, Framework.

<sup>119</sup> EU, Ministerial declaration: Global Information Networks.

<sup>120</sup> IIT, Australia, Global Information Economy.

<sup>121</sup> Industry Canada, Digital World.

<sup>122</sup> Siehe auch *Geist*, Wash. L. Rev. 521, 552.

<sup>123</sup> Z.B. die Datenschutzrichtlinie der EU vom 24. Oktober 1995, Abl.-EG 1995 L 281, 31ff.,

[http://europa.eu.int/eur-lex/de/lif/dat/1995/de\\_395L0046.html](http://europa.eu.int/eur-lex/de/lif/dat/1995/de_395L0046.html) oder die Richtlinie über den elektronischen Geschäftsvorkehr der EU vom 17. Juli 2000, Abl.-EG 2000 L 178, 1ff., [http://europa.eu.int/eur-lex/de/lif/dat/2000/de\\_300L0031.html](http://europa.eu.int/eur-lex/de/lif/dat/2000/de_300L0031.html).

*Benkler* gibt in 71 U. Colo. L. Rev. 1203ff. einen ausführlichen Überblick über die Regulierung des Internets in den USA.

lang bestehende Gesetze entsprechend auf die neue technische Materie angewendet werden. In der zweiten Variante, die öffentlich intensiver diskutiert wurde, hat der Gesetzgeber die Möglichkeit ein Recht sui generis für das Internet zu entwerfen. Einen gemischten Weg ging der deutsche Gesetzgeber durch das Mantelgesetz Informations- und Kommunikationsdienstgesetz<sup>124</sup> (IuKDG, in Kraft getreten am vom 1. August 1997), mit welchem durch insgesamt elf Artikel ganz unterschiedliche Rechtsmaterien geregelt wurden, ohne jedoch tief in das Internet einzudringen<sup>125</sup>. Mit Art. 1 IuKDG wurde das Teledienstgesetz (TDG<sup>126</sup>) eingeführt, welches unter anderem die Zugangsfreiheit, § 4 TDG und die Verantwortlichkeit der Provider, § 5 TDG regelt. Weiterhin wurde das Teledienstdatenschutzgesetz (TDDSG<sup>127</sup>) und das Signaturgesetz (SigG<sup>128</sup>) durch die Art. 2 und 3 IuKDG verabschiedet. Durch die restlichen Artikel wurden Änderungen an bestehenden Gesetzen, wie dem StGB, dem O-WiG<sup>129</sup> oder dem UrhG<sup>130</sup> vorgenommen.

Einen Prototyp eines staatlichen Instrumentes, um die im Internet zur Verfügung stehenden Informationen zu zensieren, könnte die schon jetzt zur Verfügung stehende Software bilden, welche Eltern erlaubt, den Internetzugriff ihrer Kinder zu kontrollieren. Wenn Blockierungssoftware mehr verbreitet und anerkannt wird und Ratingsysteme Standard werden, könnten Regierungen bestimmen, daß alle ISPs des Landes Blockierungssoftware installieren müssen, um für die Regierung unangenehme Inhalte herauszufiltern<sup>131</sup>.

### 2.3.3.1. Vor- und Nachteile staatlicher Regulierung

Regierungen haben heutzutage die Möglichkeit, das Internet zu regeln, welches in ihren geographischen Grenzen liegt. Es ist jedoch nicht klar, ob sie diesen Ausschnitt des Internets kontrollieren können, ohne den Nutzen und die Vorteile eines internationalen Datennetzes zu schmälern.

---

<sup>124</sup> Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste vom 22. Juli 1997, BGBI. I 1997, 1870.

<sup>125</sup> Ausführliche Beschreibungen des IuKDG werden z.B. von *Bröhl*, CR 1997, 73ff. und *Paloubis*, IuKDG und MDStV gegeben.

<sup>126</sup> Gesetz über die Nutzung von Telediensten, 22. Juli 1997, in der Fassung vom 14. Dezember 2001, BGBI. I 1997, 1870 (2001, 3721).

<sup>127</sup> Gesetz über den Datenschutz bei Telediensten, 22. Juli 1997, in der Fassung vom 14. Dezember 2001, BGBI. I 1997, 1870, 1871 (2001, 3721).

<sup>128</sup> Gesetz über Rahmenbedingungen für elektronische Signaturen, 16. Mai 2001, BGBI. I 2001, 876.

<sup>129</sup> Gesetz über Ordnungswidrigkeiten, 24. Mai 1968, in der Fassung vom 13. Dezember 2001, BGBI. I 1968, 481 (2001, 3574).

<sup>130</sup> Gesetz über Urheberrecht und verwandte Schutzrechte, 9. September 1965, in der Fassung vom 13. Dezember 2001, BGBI. I 1965, 1273 (2001, 3656).

<sup>131</sup> Z.B. verwenden China und Singapore nationale Firewalle um ihren Bürgern den Zugang zu bestimmten Webseiten und Newsgroups zu verweigern, vgl. *Resnick*, Filtering Information, Kap. Establishing Trust. Siehe auch Fn. 82. Der Bundesverband der Phonographischen Wirtschaft versucht für Deutschland ein Filtersystem aufzubauen, welches den Zugriff auf verschiedene Webangebote, welche gegen das Urheberrecht verstößen, zu unterbinden, vgl. der Bericht von *Goltzsch*, Telepolis 5833.

## 2.3. Staatlicher Eingriff vs. Selbstregulierung

---

Geographische Grenzen haben nicht nur im Internet eine immer geringere Bedeutung. Staatsgrenzen werden immer durchlässiger und ausländische Rechtssysteme erlangen lokale Bedeutung. Durch Aktivitäten im Internet setzen sich die Teilnehmer den Regeln fremder Rechtssysteme aus. Die auf geographischer Nähe und physikalischem Kontakt beruhenden politischen und wirtschaftlichen Gemeinschaften verlieren ihre Relevanz im Internet, da hier die physikalische Nähe irrelevant wird.

Räumliche Entfernungen spielen im Internet nur eine geringe Rolle. Zeitliche Entfernungen werden über die Kapazitäten der Leitungen und der passierten Knotenpunkte bestimmt. Welche staatlichen Grenzen ein Datenpaket im Internet überschreitet, spielt auf Grund des ungewissen Weges über welchen es geroutet wird (*dynamic routing*, siehe Kapitel 2.2.1 oben) nur eine geringe Rolle. Beim Abruf von Informationen sind häufig Personen verschiedener Nationen betroffen, ohne daß es den Beteiligten bewußt wird. Entsprechend wird es sich bei Streitigkeiten häufig um internationale, anstatt um nationale handeln. WWW, FTP oder Telnet ermöglichen es Nutzern, in anderen Staaten rechtswirksame Handlungen vorzunehmen, ohne daß den nationalen Autoritäten der Grenzübertritt überhaupt bewußt wird<sup>132</sup>. Gewöhnlich wissen die Nutzer nicht, noch interessiert es sie, welcher nationalen Quelle eine Internetressource entspringt. Die Internetprotokolle sind so aufgebaut, daß geographische Positionen irrelevant sind. Deshalb wird wegen der dem Internet zugrundeliegenden Technik jeder rein nationale Regulierungsversuch ineffizient sein, wenn nicht gar scheitern<sup>133</sup>. Nur ein weltweit einheitliches Vorgehen kann ausreichend gute Erfolge bringen. Als wichtigste Akteure in der Internetregulierung sind die USA und die EU somit aufgerufen, sich auf eine globale Regulierung zu einigen. Sollte es nicht zu einer solchen Einigung kommen, werden die einzelnen Staaten ihre eigenen Regulierungsideen regional noch stärker durchsetzen. Eine undurchschaubare Überregulierung wäre die Folge. Hier setzen die derzeitigen Versuche an, die Streitigkeiten um die verschiedenen Domainnamen wegen Markenrechtsverletzungen über die internationalen Organisationen WIPO und ICANN zu lösen (siehe Kapitel 4.4.1 unten).

Gibbons schlägt zur Lösung des Problems einer begrenzten Reichweite nationaler Alleingänge die Verabschiedung eines internationalen Vertrages über ein Privatrecht des Cyberspace vor<sup>134</sup>. Bislang existieren schon mehrere Möglichkeiten, private internationale Transaktionen zu regulieren. Zum Beispiel erlaubt die *Convention on the International Sales of Goods*<sup>135</sup> (CISG) Käufe von Waren auf internationaler Basis zu tätigen<sup>136</sup>. Die *UN Convention on the*

---

<sup>132</sup> *Burnstein*, 29 Vand. J. Transnat'l L. 75, 81f.

<sup>133</sup> *Roßnagel*, ZRP 1997, 26, 27f.; *Gibbons*, 6 Cornell J.L. & Pub. Pol'y 475, 502; *Lessing*, 48 Stan. L. Rev. 1403, 1406.

<sup>134</sup> *Gibbons*, 6 Cornell J.L. & Pub. Pol'y 475, 508.

<sup>135</sup> U.N. Convention on Contracts for the International Sale of Goods, Final Act, (U.N. Doc. A/CONF.97/18 (1980)), <http://www.uncitral.org/english/texts/sales/CISG.htm>.

<sup>136</sup> Vgl. hierzu *Bernstorff*, RIW 2000, 14, 18.

*Recognition and Enforcement of Foreign Arbitral Awards*<sup>137</sup> gewährt die Durchsetzbarkeit von Urteilen privater Schiedsgerichte.

Durch einen entsprechenden internationalen Vertrag könnten die einzelnen Nationen die rechtlichen Beziehungen privater Personen unterschiedlicher staatlicher Herkunft regeln und Gerichtsinstanzen zur Lösung von Streitfällen einsetzen. Als Modell könnte der Vorschlag der *United Nations Commission on International Trade Law* (UNCITRAL) zum Elektronischen Geschäftsverkehr dienen<sup>138</sup>. Dieses Modellgesetz<sup>139</sup> enthält im ersten Teil Regelungen zur Rechtsverbindlichkeit von elektronischen Informationen (Art. 6 und 7), zum Unterschriftserfordernis (Art. 8 bis 10) und Vorgaben für den Vertragsschluß und elektronischen Willenserklärungen (Art. 11 und 12). Im zweiten Teil werden Sonderbestimmungen zum Warentransport getroffen (Art. 16 und 17). Entsprechend setzen sich die USA in der UNCITRAL für ein Modell ein, welches die geschäftliche Nutzung von internationalen Verträgen im Electronic Commerce unterstützt und ziehen zusätzlich die *International Chamber of Commerce* (ICC) für die Entwicklung eines rechtlichen Rahmengerüstes hinzu<sup>140</sup>. Im Dokument „Framework for Global Electronic Commerce“ schlagen die USA vor, daß Prinzipien, wie die von UNCITRAL entwickelten, von allen Nationen übernommen werden sollten, um ein internationales Set von gleichen gewerblichen Prinzipien für den elektronischen Geschäftsverkehr zu entwerfen<sup>141</sup>.

Den gleichen Zweck erfüllt zumindest auf europäischer Ebene die Richtlinie über den elektronischen Geschäftsverkehr<sup>142</sup> der *Europäischen Union*, welche am 4. Mai 2000 vom *Europäischen Parlament* angenommen wurde. Mit ihr wird nicht nur eine Harmonisierung der Regeln zum Onlinemarketing bezweckt, vielmehr enthält sie Regelungen zum elektronischen Vertragsschluß und zur Haftung von Internetserviceprovidern<sup>143</sup>. Sie soll Rechtssicherheit für Angebote und Nutzung von Internetdiensten gewährleisten. Es wird mit dieser Regelung eine Verbesserung der Stellung der Diensteanbieter angestrebt, mit dem Hintergedanken, ein möglichst breites Angebot europäischer Dienste zu fördern. Zur Förderung von Dienstleistungs- und Warenverkehr sollen dabei die in den Mitgliedstaaten der *Europäischen Union* unterschiedlichen rechtlichen Hindernisse beseitigt werden.

---

<sup>137</sup> U.N. Convention on the Recognition and Enforcement of Foreign Arbitral Awards vom 10. Juni 1958, (21 U.S.T. 2517, T.I.A.S. No. 6997, 330 U.N.T.S. 3), <http://www.uncitral.org/english/texts/arbitration/NY-conv.htm>.

<sup>138</sup> UNCITRAL Model Law on Electronic Commerce (1996) und Guide to Enactment, 16. Dezember 1996, (U.N. Doc. A/51/628 (1996)), <http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm>.

<sup>139</sup> Bernstorff, RIW 2000, 14, 18ff. einen ausführlichen Überblick über das UNCITRAL Model Law on Electronic Commerce.

<sup>140</sup> Siehe der Vorschlag der USA: *US-White House*, Framework, Kap. Principles 5.

<sup>141</sup> *US-White House*, Framework.

<sup>142</sup> Siehe Fn. 123.

<sup>143</sup> Vertiefende Informationen zur Richtlinie über den elektronischen Geschäftsverkehr können z.B. in Maennel, MMR 1999, 187ff.; Hoeren, MMR 1999, 192ff. und Bernstorff, RIW 2000, 14ff. gefunden werden.

## 2.3. Staatlicher Eingriff vs. Selbstregulierung

---

Um einen weiteren internationalen Vertrag handelt es sich bei der Cybercrime-Konvention, welche unter der Federführung des Europarates<sup>144</sup> und unter der Teilnahme der USA, Kanada, Japan und Südafrika seit 1997 erarbeitet und am 8. November 2001 in Budapest durch den Europarat beschlossen und zum 23. November 2001 das Ratifizierungsverfahren eröffnet wurde<sup>145</sup>. Diese Konvention soll die erste international verbindliche Vereinbarung zu Bekämpfung von Computerkriminalität werden. Die teilnehmenden Staaten sollen sich verpflichten, einen einheitlichen rechtlichen Rahmen zur Definition, Verfolgung und Sanktionierung von Straftaten zu schaffen, die mit oder in Bezug auf Computer begangen werden<sup>146</sup>.

Von der Öffentlichkeit ebenfalls kaum bemerkt, wird auf der *Hague Conference on Private International Law* an einem weitreichenden internationalen Vertrag zur globalen Durchsetzung von zivilrechtlichen Urteilen und einstweiligen Verfügungen in kommerziellen Streitigkeiten gearbeitet. Die *Hague Conference on Private International Law* ist eine zwischenstaatliche Organisation deren Absicht die Vereinheitlichung der Regeln des internationalen Privatrechts ist<sup>147</sup>. Sie besteht derzeit aus 53 Mitgliedstaaten, wobei neben den europäischen und amerikanischen Industrienationen auch einige totalitäre Staaten (zum Beispiel China) beteiligt sind. Bei der geplanten *Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters* geht es um die Anerkennung ausländischer Urteile, unter anderem bei Vertragsverletzungen, beim Wettbewerbsrecht sowie bei Industrie- und Handelsgeheimnissen<sup>148</sup>. Die Staaten, welche die Konvention unterzeichnen, verpflichten sich, eine Anzahl von Regeln betreffend ihrer Zuständigkeit in grenzüberschreitenden Streitigkeiten zu beachten. Soweit diese Regeln eingehalten werden, sind die Unterzeichnerstaaten verpflichtet, alle Urteile und einstweiligen Verfügungen anderer Konventionsstaaten, abgesehen von Entscheidungen, die in einem engen Rahmen mit der öffentlichen Politik unvereinbar sind, umzusetzen. Es besteht nach der Konvention keine Verpflichtung zur Harmonisierung des nationalen Rechts mit Ausnahme der Zuständigkeitsregel.

---

<sup>144</sup> Eine nicht mit dem Europäischen Rat oder dem Rat der Europäischen Union zu verwechselnde, von der EU unabhängige Institution.

<sup>145</sup> Vgl. die endgültige vom European Committee on Crime Problems verabschiedete 28. Fassung: European Committee on Crime Problems, Draft Convention on Cyber-crime, 18.-22. Juni 2001, <http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm>.

<sup>146</sup> Diese Konvention ist jedoch unter Menschenrechtsorganisationen sehr umstritten. So kritisieren 30 wichtige Bürgerrechtsorganisationen aus Europa, den USA, Australien, Kanada und Südafrika in einem offenen Brief vom 10. Oktober 2000, daß die Konvention den „etablierten Normen zum Schutz des Einzelnen“ widerspricht, die „Befugnis der Polizei der nationalen Regierungen unangemessen“ erweitert, die „Entwicklung von Sicherheitstechniken für Netzwerke“ behindert und die „Verantwortung der Regierung bei künftiger Strafverfolgung“ herabsetzt; 18. Oktober 2000, <http://www.cluebot.com/articles/00/10/17/1622228.shtml>. Vgl. auch *Krempl, Telepolis* 7239.

<sup>147</sup> Näheres zur Hague Conference on Private International Law siehe Infosheet, 22. Mai 2001, <http://www.hcch.net/e/infosheet.html>.

<sup>148</sup> Näheres zur Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters siehe <http://www.hcch.net/e/workprog/jdgm.html>. Die deutsche Fassung vom 30. Oktober 1999 ist in der *Telepolis* veröffentlicht worden: *Mühlbauer, Telepolis 7676*.

Obgleich die Konvention damit klare Vorteile für eine internationale Umsetzung von zivilrechtlichen Urteilen bildet, unterminiert sie im großen Umfang die nationale Rechtssetzungsbefugnis. Die Diskussion um eine einheitliche Durchsetzung von Zivilrechtsurteilen begann schon 1992. Zu diesem Zeitpunkt spielte das Internet noch eine marginale Rolle und wurde in die anfänglichen Überlegungen nicht mit einbezogen. Da die Informationen des Internets weltweit abrufbar sind, spielt dieses Computernetzwerk, wie schon dargelegt, eine Sonderrolle. Die diskutierte Konvention würde jedem Mitgliedsstaat eine Zuständigkeit über alles, was im Internet publiziert oder vertrieben wird, geben. Da die Hager Konvention nicht zur Harmonisierung des materiellen Rechts beitragen will, würde dies zu einer Umsetzung von unterschiedlichen Rechtsordnungen über Staatsgrenzen hinweg führen. Würde ohne eine solche Konvention sich im Internet die jeweilige nationalstaatliche Rechtsposition mit den geringsten Einschränkungen durchsetzen, so wären alle gewerblichen Nutzer im Internet nunmehr den Rechtsregeln eines bestimmten Anwendungsbereiches ausgesetzt, welche die stärksten Schutz- und Regelungsmechanismen enthalten. Folglich müßten Nutzer feststellen, daß Aktivitäten, welche an ihrem Wohnort legal sind, in anderen Staaten verboten sind. Die Unterschiede in den einzelnen Rechtsordnungen würden dazu führen, daß sich die Kläger das Land mit der für sie jeweils günstigsten Regelung aussuchen würden. Die besondere Brisanz einer solchen Konvention zeigt sich vor allem bei den immateriellen Rechtsgütern<sup>149</sup>. So müßten die europäische Softwareproduzenten befürchten, vor amerikanischen Gerichten wegen Patentverletzungen verklagt zu werden, obgleich das europäische Recht nur einen geringen Patentschutz auf Software vorsieht. Andererseits müßten US-Amerikaner befürchten, durch europäische Urheberrechte in ihrer Redefreiheit eingeschränkt zu werden. Gänzlich unbekannt sind die Risiken für die europäische und amerikanische Rechtsordnung, welche sich ergeben, wenn autoritäre Staaten wie China oder islamische Staaten wie Ägypten der Konvention beitreten würden. Auf der letzten Konferenz vom 20. Juni 2001 konnte man sich noch nicht auf einen gemeinsamen Nenner einigen, wie mit immateriellen Rechtsgütern zu verfahren sei. Amerikanische Unternehmen und Bürgerrechtsbewegungen übten weiterhin Druck aus, damit einschneidende Änderungen noch vorgenommen werden<sup>150</sup>. Auf europäischer, insbesondere deutscher Seite verzichtete man jedoch bislang auf eine direkte Beteiligung der betroffenen Bürger. Um zu einer fairen Lösung zu gelangen werden schließlich einige weitere Diskussionsrunden nötig sein und auch Harmonisierungen des materiellen Rechts nicht unbedacht bleiben.

Auf Grund der schnellen Entwicklung des Internets und dem ständigen Aufkommen neuer Rechtsprobleme, ist eine schnelle Reaktion des Gesetzgebers notwendig. Dazu ist eine Voraussicht der weiteren Entwicklung der Technik unumgänglich. Staatliche Regelungsmechanismen müssen somit eine kurze Reaktionszeit auf aktuelle Probleme bieten.

---

<sup>149</sup> Ausführlich zu den Risiken der Hager Konvention: *Mühlbauer, Telepolis 7676 und Love, Hague Convention*.

<sup>150</sup> Zur Diplomatic Conference vom Juni 2001 und dem aktuellen Diskussionsstand siehe *ICB Toll Free, Love, Internet and Public Domain at Risk*, 20. Juni 2001.

## 2.3. Staatlicher Eingriff vs. Selbstregulierung

---

Damit zeigt sich jedoch der große Nachteil einer staatlichen Regulierung. Um Regeln rechtsstaatlich zu legitimieren, müssen diese in einem demokratischen Verfahren zustande kommen. Entscheidungen durch Einzelpersonen sind damit nicht vereinbar. Es ist das vorgeschriebene Verwaltungsverfahren einzuhalten oder die Diskussion in einem staatlichen Plenum zu gewährleisten, bevor Verordnungen oder Gesetze erlassen werden können. Entsprechend träge ist folglich der Gesetzgeber bei der Regelung anstehender Rechtsprobleme.

Zum Beispiel wurde der erste Entwurf der Datenschutzrichtlinie der EU 1990 veröffentlicht<sup>151</sup>. Die Verabschiedung der Endfassung erfolgte 1995, mit einer Frist zur Implementierung in das nationale Recht der Mitgliedsstaaten bis 1998. Bis die Standards der Datenschutzrichtlinie voll in das nationale Recht integriert und die ersten Gerichtsentscheidungen gefällt werden, wird noch ein langer Zeitraum vergehen. Es besteht das Risiko, daß einige Normen innerhalb des Zeitraums der Implementierung obsolet oder die Rechtsvorschriften zu spät angewendet werden.

Weiterhin ist es für den staatlichen Gesetzgeber schwierig zu entscheiden, wie weit er mit seinen Planungen voraus denken soll. Gewöhnlich versucht die EU in ihren Gesetzesentwürfen langfristige Entwicklungen des entsprechenden zu regelnden Rechtsgebietes einzuplanen und darauf gezielt einzuwirken. Es besteht dabei das Risiko, daß sie kurzfristig die Kontrolle über das Rechtsgebiet verliert, falls sich die Entwicklung in eine andere Richtung als die geplante bewegt. Im Gegensatz dazu versuchen die USA häufig sich durch kurzfristige Aktionen in das aktuelle Geschehen einzumischen und verlieren somit die Möglichkeit einer langfristigen Steuerung<sup>152</sup>.

### 2.3.3.2. Umsetzung

Die Nutzer des Internets sind neben einem „Internetrecht“ vorrangig dem Recht ihrer physikalischen Welt unterworfen. Nationale Gerichte können problemlos zu Strafen und Schadensersatzzahlungen verurteilen, wenn zum Beispiel Verletzungen des Computerstrafrechtes oder des Vertragsrechtes vorliegen. Bei der aktiven Kommunikation über das Internet ist man zusätzlich gezwungen, die ungeschriebenen sozialen Normen zu beachten und sich an die Zugangsregeln seines ISPs zu halten.

Wenn die derzeitigen Regeln, wenn auch ursprünglich nicht vorgesehen, die Nutzung des Internets regulieren, so stellt sich die Frage, ob überhaupt ein eigenes Rechtsgebiet, welches speziell auf den sozialen, ökonomischen, politischen und technischen Rahmen des Internets zugeschnitten ist, nötig wäre<sup>153</sup>. Viele Staaten, welche traditionell zu einer starken Regulierung und Kontrolle neigen, mögen das Internet als eigenen Rechtskörper sehen und als Objekt direkter Regulierung betrachten<sup>154</sup>. Obwohl bei oberflächlicher Betrachtung ein *sui generis*

---

<sup>151</sup> Siehe die endgültige Fassung der Datenschutzrichtlinie, Fn. 123.

<sup>152</sup> Vgl. *Reidenberg*, 45 Emory L.J. 911, 921.

<sup>153</sup> *Trotter*, 55 U. Pitt. L. Rev. 993, 995; *Gibbons*, Cornell J.L. & Pub. Pol'y 475, 499.

<sup>154</sup> *Matsuura/Auffret*, Internet Law, Kap. Internet law: the causes.

Recht für das Internet notwendig erscheint, besteht eine Bindung an internationales, nationales und lokales Recht. Das Internet ist, obgleich sehr mächtig und ausgedehnt, nur ein weiteres Kommunikationssystem, wie das Telefonnetz oder der Rundfunk. Ein spezielles Cyberrecht würde nur eine weitere Ebene hinzukreieren, somit die Komplexität des Rechts weiter erhöhen und die praktische Anwendbarkeit noch schwieriger gestalten, als dies bisher schon der Fall ist<sup>155</sup>.

Bevor eigene Rechtsregeln geschaffen werden, muß zuerst geklärt werden, ob schon vorhandene Regeln für die Anforderungen des Internets geeignet sind und ob die gleichen Ziele erreicht werden können, wie in der realen Welt<sup>156</sup>. Allein aus der Neuheit und Verschiedenheit von bestehenden Kommunikationsmedien kann nicht geschlossen werden, daß ein eigenes Recht benötigt würde. Weiterhin sind die Kosten mit dem Nutzen abzuwegen, welche die Einführung von neuen Regeln in das Internet mit sich bringt<sup>157</sup>. Nur wenn ein existierendes und anwendbares Recht hohe Kosten für die Nutzung des Internets zur Folge hat, ist ein eigenes Internetrecht gerechtfertigt. Andererseits, wenn ein solches Recht die Entwicklung des Internets zu stark bremst, wäre ein *sui generis* Recht notwendig. Durch die weite Auslegungsfähigkeit des Rechts, der Analogiebildung und der Anwendung von allgemeinen Rechtsgrundsätzen wird ein eigenes Internetrecht jedoch nur in den seltensten Fällen gerechtfertigt sein<sup>158</sup>. So wurde mit Entwicklung der Sprachtelefonie kein eigenes „Telefongesetz“ entwickelt, sondern bestehende Rechtsgrundsätze auf die neue Situation angewendet. Jede über die Schließung von Rechtslücken hinausgehende Regulierung wird eine unnötige Behinderung der Entwicklung des Internets darstellen<sup>159</sup>.

### 2.3.4. Selbstregulierung

Selbstregulierung kann in verschiedenen Formen auftreten, von sozialer Eigenkontrolle über eine eigene Regierung bis zu einer Regulierung über allgemein gültige Verträge. Dabei erfolgt ein Großteil der Regulierung durch soziale Normen der einzelnen Nutzer selbst. Der Umfang einer Selbstregulierung ist auf Grund seiner Vielschichtigkeit jedoch unklar und umstritten.

#### 2.3.4.1. Cyberspace als eigenes Rechtsterritorium

Der Wirkungskreis einer Rechtsgemeinschaft muß nicht zwingend durch geographische Grenzen bestimmt werden. Religionsgemeinschaften zum Beispiel sind nicht an Staatsgrenzen oder sonstige geographische Abgrenzungen gebunden. Geographisch betrachtet würde sich deren Rechtswirkung sogar überschneiden, da in einem Land oft viele Religionsgemeinschaften beheimatet sind. Es wäre somit eine Welt vorstellbar, in der sich Recht und Gesetz

---

<sup>155</sup> *Gibbons*, Cornell J.L. & Pub.Pol'y 475, 499.

<sup>156</sup> Vgl. *Trotter*, 55 U. Pitt. L. Rev. 993, 996ff. und *Johnson/Marks*, 38 Vill. L. Rev. 487, 515; *Matsuura/Auffret*, Internet Law, Kap. The optimal relationship.

<sup>157</sup> *Gibbons*, Cornell J.L. & Pub.Pol'y 475, 500 und *Trotter*, 55 U. Pitt. L. Rev. 993, 998.

<sup>158</sup> *Gibbons*, Cornell J.L. & Pub.Pol'y 475, 500.

<sup>159</sup> Vgl. auch die ausführliche Darlegung von *Matsuura/Auffret*, Internet Law, Kap. Internet law: the consequences.

## 2.3. Staatlicher Eingriff vs. Selbstregulierung

---

nicht nach Staatsgrenzen richtet, sondern territorial unspezifisch definiert wird<sup>160</sup>. Ebenso könnte man ungeographischen Räumen ein eigenes Recht zuweisen. Für viele präsentierte der Cyberspace die Gelegenheit einen neuen Standort zu schaffen, in welchem das staatliche Recht der Selbstregulierung damit und eigenem Recht Raum geben würde.

Der Begriff Cyberspace wurde durch den Science Fiction Autor William Gibson in seinen Kurzgeschichten geprägt. Er verwendete ihn, um eine sich verändernde Realität zu beschreiben, in die seine Charaktere eintraten, indem sie ihren Verstand mit einem Computernetzwerk verbanden<sup>161</sup>. Das Wort Cyberspace und weitere Beschreibungen wie Chat Room, Web Space oder Web Site führten zu einem Vergleich des Internets mit der geographischen Welt<sup>162</sup>. Im Rechtsfall *Reno v. ACLU* wird zum Beispiel festgestellt, daß der Cyberspace eine gewisse Form von Geographie wiederspiegelt<sup>163</sup>. Chat Rooms und Webseiten existieren an festen Stellen im Internet und erlaubten es, Barrieren aufzubauen und Identitäten zu prüfen. Es bestände somit große Ähnlichkeit zur physikalischen Welt.

Diese Ähnlichkeit zu einem räumlichen Gebilde scheint so groß zu sein, daß einige Internetnutzer sich selbst als Cyberians oder Cybernauten bezeichnen und die elektronische Welt als Cyberia. Der Cyberspace ist die virtuelle Entsprechung von Marktplätzen und Wohngebieten, in welchen die Aktivitäten der Computernutzer stattfinden.

Grundlegend für diese Ansicht plädierten David Post und David Johnson, welche 1996 argumentierten, der Cyberspace sei von den hergebrachten rechtsetzenden Organisationen der physischen Welt abgeschnitten<sup>164</sup>. Dieser sei ein separater Raum, durch ein eigenes Recht zu regulieren<sup>165</sup>. Der Begriff „Cyberspace“ impliziert dabei eine Verdrängung der molekularen Welt. Die realen Aktivitäten würden nicht mehr im physikalischen Raum stattfinden, sondern in einer neuen Dimension. Die Beziehungen, welche durch die Kommunikation im Internet entstehen, sind gewöhnlich geographisch unspezifisch. Die Kommunikation erfolgt gewöhnlich zwischen Personen mit unbekanntem Standort und nicht sicherer Identität. Eine Email kann von jedem Rechner des Internets gesendet und aus einer Mailbox unbestimmten Ortes abgerufen werden. Ein Webbrower kann nicht die geographische Lage einer Webseite bestimmen. Ebenso kann der Hostcomputer einer Webseite nicht feststellen, von welchem physikalischen Punkt die Webseite abgerufen wurde. Eine Webseite kann dabei nicht als spezifischer geographischer Platz betrachtet werden. Sie besteht vielmehr nur aus Text, Multimedia-Dateien (Bilder, Videos oder Tondateien) und Programmcode, der auf Anfrage an einen anderen Rechner versendet wird. Auch die einzelnen Bestandteile einer Webseite müssen sich nicht alle auf einem Rechner befinden, sondern können verstreut im Internet liegen. Die In-

---

<sup>160</sup> Stein, 32 Int'l Law. 1167, 1168f.

<sup>161</sup> Siehe zum Beispiel die Geschichten: *Burning Chrome* von 1982 (z.B. veröffentlicht in *Gibson/Sterling, The Difference Engine*) und *Neuromancer* von 1984 (*Gibson, Neuromancer*)

<sup>162</sup> Rowland, IJLT 1998 (3), Kap. 3.

<sup>163</sup> U.S. Supreme Court vom 26. Juni 1997, „*Reno v. ACLU*“, 117 S. Ct. 2329, 2353.

<sup>164</sup> Vgl. *Johnson/Post* 48 Stan. L. Rev. 1367, 78ff.

ternetkommunikation geht somit von, zu und über Plätze, welche für den Nutzer größtenteils unbekannt sind und deren Standort für ihn auch völlig irrelevant ist.

Würde man bei der Analyse des Rechts und der rechtlich relevante Grenzen zwischen Cyberspace und realer Welt, den Cyberspaces als einen bestimmten Platz betrachten, könnte dies viele juristische Probleme, die durch das globale Computernetzwerk entstanden sind, lösen<sup>166</sup>. Zum Beispiel würden dann Gerichte, wenn sie mit einem Fall aus der Internetnutzung konfrontiert werden, einfach auf das Recht des Cyberspace verweisen, wie mittelalterliche Gerichte in Fällen mit internationalem Bezug auf das damals geltende Handelsrecht verwiesen hatten<sup>167</sup>.

Ein Vergleich zu anderen souveränen Rechtsordnungen liegt nahe. So besitzen die verschiedenen Religionsgemeinschaften eigene Rechtsregeln, die auch vor staatlichen Gerichten zum Teil anerkannt werden. Ebenso haben ethnische Minderheiten, wie zum Beispiel die Sorben<sup>168</sup> in Deutschland oder die verschiedenen Indianerstämme<sup>169</sup> in den USA einige Sonderrechte oder gar ein eigenes unabhängiges Rechtssystem.

Obwohl es faszinierend erscheint, das Internet als eigenes neues Rechtsterritorium zu betrachten, sollte man jedoch nicht der Versuchung erliegen, umgangssprachlichen Begriffen (wie Cyberspace oder Chat Room) eine tiefergehende Bedeutung beizumessen. Argumentationen, ausgehend von unwissenschaftlichen Ausdrücken, können leicht zu unbegründeten Schlußfolgerungen führen. Cyberspace ist nur ein geeigneter Begriff, um die verschiedenen Kommunikationsmöglichkeiten des Internets zusammenzufassen<sup>170</sup>. Verschiedene Kabel übertragen die Nachrichten im Cyberspace. Diese Leitungen führen jedoch durch den realen Raum und unterliegen der herkömmlichen Rechtssetzung und Rechtsprechung. Ebenso können sich weder die Betreiber der Hardware noch deren Computer der physikalischen Welt entziehen. Das Recht der realen Welt regelt folglich das Eigentumsrecht an den Gegenständen „in“ denen sich der Cyberspace erstreckt. Auch die Nutzer des Internets, welche am Beginn und am Ende des Kommunikationsprozesses stehen, sind nicht virtuelle Gebilde, sondern bewegen

---

<sup>165</sup> Beispiele dazu: *Johnson/Post* 48 Stan. L. Rev. 1367, 1370ff. und 1381ff.

<sup>166</sup> *Johnson/Post* 48 Stan. L. Rev. 1367, 78: „Many of the jurisdictional and substantive quandaries raised by border-crossing electronic communications could be resolved by one simple principle: conceiving of cyberspace as a distinct ‘place’ for purposes of legal analysis and recognizing a legally significant border between cyberspace and the ‘real world.’“; vgl. auch *Lessing*, 48 Stan. L. Rev. 1403, 1403: „Cyberspace is a place. People live there.“

<sup>167</sup> Vgl.: *Johnson/Post* 48 Stan. L. Rev. 1367.

<sup>168</sup> In den Landesverfassungen der Länder Sachsen und Brandenburg wird ausdrücklich auf eine Gleichberechtigung der Sorben hingewiesen. Art. 25 Abs. 1 Satz 1 BbgVerf: „Das Recht des sorbischen Volkes auf Schutz, Erhaltung und Pflege seiner nationalen Identität und seines angestammten Siedlungsgebietes wird gewährleistet.“ Art. 5 Abs. 1 Satz 1 SächsVerf: „Dem Volk des Freistaates Sachsen gehören Bürger deutscher, sorbischer und anderer Volkszugehörigkeit an.“; Art. 6 Abs. 1 Satz 1 SächsVerf: „Die im Land lebenden Bürger sorbischer Volkszugehörigkeit sind gleichberechtigter Teil des Staatsvolkes.“

<sup>169</sup> *Dane*, 12 Cardozo L. Rev. 959, 959ff.

<sup>170</sup> *Goldfoot*, 84 Va. L. Rev. 909, 920.

## 2.3. Staatlicher Eingriff vs. Selbstregulierung

---

sich im realen Raum, wie auch alle internetbezogenen Aktivitäten ihren Ursprung in der körperlichen Welt haben<sup>171</sup>.

Es mag zwar möglich sein, die Internetnutzer als eine Art Gemeinschaft zu betrachten. Es fällt aber schwer, außer der Nutzung der gleichen Technologie, bei diesen Personen eine durchgehende Gemeinsamkeit zu finden. In der Gesamtheit betrachtet, haben sie weder eine gemeinsame Autorität, Geschichte oder Kultur<sup>172</sup>. Man könnte die Internetnutzer eher mit den Nutzern des Post- oder Telefonwesens betrachten, als mit einer Religionsgemeinschaft. Das Internet stellt nur das Medium für die Kommunikation dar, jedoch kein eigenes Rechtsterritorium.

Durch seine Entstehung im wissenschaftlichen Bereich, wurde das Internet ursprünglich ausschließlich von Wissenschaftlern und Studenten genutzt. Aus deren kostenlosen Zugang zum Netz wurde geschlossen, daß das Internet ein freier Raum und damit nur den eigenen Regeln unterworfen sei<sup>173</sup>. Obgleich niemand für den Cyberspace selbst zahlt, bezahlt jeder für seinen eigenen Netzanschluß. So zahlen die Universitäten für ihre wissenschaftlichen Mitarbeiter und Studenten einen Anschlußbeitrag an die regionalen Netzwerke, welche wiederum an die nationalen ISPs bezahlen. Jeder der in das Internet will, kann dies nur über einen ISP und muß deshalb schon beim Zugang seinen Beitrag bezahlen. Aus der Zugangsstruktur läßt sich somit auch nicht herleiten, daß das Internet ein eigenständiger freier Raum sei.

Weiterhin kann kaum angenommen werden, daß die Internetnutzer eine eigene Regierung aufstellen könnten. Ein Konsens wird durch die Teilnahme von über 200 Nationen<sup>174</sup> mit den kulturellen Verschiedenheiten der Nutzer und der unterschiedlichen Rechtssysteme vereitelt. Jegliche Internetregierung würde machtlos angesichts der realen Welt sein und die Grenzen zum realen Raum würden immer umstritten bleiben<sup>175</sup>. Internetnutzer würden in Rechtsstreitigkeiten nur noch auf die Institutionen des Cyberspace zurückgreifen können, obwohl bislang noch keine funktionierenden und anerkannten Online-Gerichte existieren. Ebenso ist kaum zu erwarten, daß die vielen realen Staatsregierungen Entscheidungen der Internetregierung vorbehaltlos akzeptieren würden. Zusätzlich müßten Einnahmequellen erschlossen werden, um die Regierungsarbeit zu finanzieren.

Als Rechtsmittel zur Durchsetzung eines Internetrechts wird oft die Möglichkeit des Ausschlusses von Nutzern aus dem Internet erwähnt, wenn diese die geltenden Bestimmungen verletzen sollten. Es erscheint allerdings fraglich, ob es möglich ist, einem großen Internet-serviceanbieter seine Verbindung zum Internet zu untersagen. Andere Internetnutzer könnten nach einem Bann erneut am Internet durch einen anderen Internetanbieter teilnehmen.

---

<sup>171</sup> Vgl. *Mankowski*, AfP 1999, 138, 139 und *Christiansen*, MMR 2000, 123, 128.

<sup>172</sup> *Stein*, 32 Int'l Law. 1167, 1170ff.

<sup>173</sup> *Gibbons*, Cornell J.L. & Pub.Pol'y 475, 497.

<sup>174</sup> Siehe *Internet Software Consortiums*, Internet Domain Survey, Fn. 899.

<sup>175</sup> *Goldfoot*, 84 Va. L. Rev. 909, 921.

Schwierig wird es sein, die genauen Grenzen zwischen Internet und realer Welt festzulegen<sup>176</sup>. Welcher Teil eines Internetbuchhändlers würde zum Cyberspace zu rechnen sein und welcher zum Vertragsrecht eines Staates? Soll das Anbieten von Kinderpornographie durch Internetrechtsregeln bestraft werden oder unterfällt es Strafrechtsregeln der realen Welt?

Zum Teil versuchen Autoren den im Internet entstandenen Gemeinschaften (sogenannte Cybercommunities) eine wichtige Bedeutung beizumessen und diese als etwas völlig Neues anzusehen, auf welche die bisherigen Regelungsmechanismen nicht anwendbar wären<sup>177</sup>. Es wird dabei immer wieder auf Diskussionsgruppen oder textbasierte Spiele (MUDs oder MUSHs) abgestellt, in denen man alles tun und lassen kann, solange man nicht gegen die für diese Gruppen jeweils eigenen Regeln verstößt. Dabei ist man völlig unabhängig von Regeln außerhalb der jeweiligen Cybercommunity. Es ist nicht wichtig, welcher Herkunft jemand ist oder wie sein wirklicher Name lautet.

Moore schreibt zum Beispiel<sup>178</sup>:

“You can do anything you want. It is not like society. There is no bias to anything. You can have any name you want. There are no arguments, no fighting. There is, like, no race. You can be yourself.“

Solche „Cybercommunities“ unterscheiden sich jedoch nicht von herkömmlichen Vereinigungen oder Gruppierungen. Vielmehr bildet das Internet eine weitere Plattform für raumübergreifende Kommunikation. Es spielt keine Rolle, ob sich Personen allabendlich zum Skatabend treffen oder über ein MUD miteinander spielen. Dabei hat jeder Verein und jede Gemeinschaft ebenso seine eigenen Regeln, gleichgültig, ob es sich um eine Internetgemeinschaft handelt, oder um eine der realen Welt. Es kommt auch nicht darauf an, ob diese Regeln in einer Art Vertragswerk niedergelegt oder nur Gewohnheitsrechte sind. Zu diskutieren und Informationen auszutauschen, ist ebenso auf postalischem Wege möglich, ohne daß die genaue Identität der einzelnen Kommunikationspartner bekannt sein muß. Außerdem bleiben die einzelnen Teilnehmer an einer Gemeinschaft im Internet den Regeln ihres Herkunftslandes oder Wohnsitzes unterworfen und dürfen zum Beispiel keine Kinderpornographie austauschen oder illegale Glücksspiele<sup>179</sup> betreiben. Wenn sie sich über diese Regeln hinwegsetzen, sind sie ebenso rechtlich verantwortlich, wie in der physikalischen Welt.

Zusammenfassend kann man feststellen, daß das Internet nicht als ein eigener quasi-geographischer Raum betrachtet werden kann, sondern, daß es ein Teil der realen physischen

---

<sup>176</sup> Meyerson, 8 Harv. J.L. & Tech. 129, 130: „Defining a network is like trying to hit a moving target.“

<sup>177</sup> Z.B. sieht Rowland, JILT 1998 (3), Kap. 4, es für problematisch an, daß die verschiedenen Konfliktregelungsmechanismen und Machtkontrollen der herkömmlichen Staaten auf das Internet angewendet werden. Ausführlich zu den Virtual Communities (Cybercommunities): HLRA, 112 Harv. L. Rev. 1586, 1588ff.

<sup>178</sup> Moore, D., The Emperor's virtual clothes: The naked truth about Internet culture, 1995, Chapel Hill, N.C., zitiert in Rowland, JILT 1998 (3), Kap. 4

<sup>179</sup> Vgl. z.B. die Gesetze zum Schutz von Kindern vor sexuellem Mißbrauch, §§ 174, 176, 180, 182 StGB und besonders das Verbot der Kinderpornographie, § 184 Abs. 3 StGB. Zum Glücksspiel siehe §§ 284ff. StGB.

## 2.3. Staatlicher Eingriff vs. Selbstregulierung

---

Welt ist. Das Internet stellt ein Kommunikationsmedium dar, das Menschen verschiedener Orte verbindet. Es besteht bei einer Verletzung von Rechten anderer Personen über das Internet kein Unterschied zu den vielen anderen Möglichkeiten Rechte Dritter zu verletzen<sup>180</sup>. Obwohl es globalen Einflüssen unterliegt, ist es nicht anders als der zwischenstaatliche Handel zu betrachten<sup>181</sup>. Es unterfällt damit den hergebrachten Rechtsregeln und bildet keinen Ausnahmefall sui generis<sup>182</sup>.

### 2.3.4.2. Berechtigung einer Selbstregulierung

Da es sich, wie eben festgestellt, beim Internet nicht um einen eigenständigen Rechtsraum handelt und damit nicht von sich aus ein eigenes Recht besitzt, muß geklärt werden, ob im Internets, ähnlich wie in den sich teilweise selbstregulierenden Wirtschaftssektoren (zum Beispiel dem Finanz- und Börsenbereich oder der Telekommunikation), eigene Rechtsregeln gesetzen werden können. Aus der Tatsache, daß Kommunikation über neue elektronische Wege erfolgt, läßt sich noch nicht schlußfolgern, daß eine Selbstregulierung notwendig und möglich ist. Offene globale Netzwerke laden zunächst zur Selbstregulierung ein, da es für die national orientierten Gesetzgeber und Gerichtsorgane schwierig ist, ein transnationales Netzwerk zu steuern. Für die direkt am Aufbau und dem Betrieb des Internets beteiligten Internetserviceprovider ist es jedoch ebenfalls schwierig das Gesamtnetz zu kontrollieren<sup>183</sup>.

Um sich zwischen einer staatlichen Regulierung und einer Selbstregulierung zu entscheiden, ist die Betrachtung mehrerer Gesichtspunkte notwendig. Da das Regelungsinstrument stark von dem zu regelnden Bereich abhängt, ist es wichtig, diesen genau festzulegen. Zu beachten ist, daß es dabei keine allgemeingültige Lösung für alle Anwendungsbereiche des Internets geben kann. Einer Selbstregulierung kann in der Regel dann Vorrang gewährt werden, wenn

- sie effektiver ist als staatliche Gesetze,
- die schon jetzt im Internet existierenden Regeln stark von den staatlichen abweichen,
- die vorhandenen Regeln der physikalischen Welt nicht auf das Internet übertragbar sind oder
- die Anerkennung selbst entwickelter Regeln in der Internetgemeinschaft höher ist<sup>184</sup>.

Die staatlichen Gesetzgeber müssen sich in ihrer Arbeit mit vielen verschiedenen Sachgebieten auseinandersetzen. Obwohl sie dazu verschiedene Spezialisten heranziehen können, ist es kaum möglich, daß sie (oder die einzelnen Abgeordneten) sich in jedem Fachgebiet optimal auskennen. Besonders im schnellen Internet ist es kaum möglich, die aktuelle Entwicklung zu beobachten und die daraus resultierenden Bedürfnisse zeitgerecht zu erfassen. Nir-

---

<sup>180</sup> Vgl. *Lessing*, 48 Stan. L. Rev. 1403, 1404.

<sup>181</sup> *U.S. District Court, S.D. New York* vom 20. Juni 1997, *American Libraries Association v. Pataki*, 969 F.Supp. 160, 173: „[T]he Internet represents an instrument of interstate commerce“.

<sup>182</sup> *Goldfoot*, 84 Va. L. Rev. 909, 923.

<sup>183</sup> Vgl. *Perritt*, 12 Berkeley Tech. L.J. 413, 419.

<sup>184</sup> Vgl. *Perritt*, 12 Berkeley Tech. L.J. 413, 419; *Goodman*, 10 Harv. J.L. & Tech. 465, 477-490.

gends scheinen der Gesetzgeber, die Verwaltung und die Gerichte die ökonomische und soziale Bedeutung neuer Technik vorausahnen zu können<sup>185</sup>. Aus dieser fehlenden Voraussicht, läßt sich eine Zurückhaltungspflicht der staatlichen Autoritäten herleiten, die Technik unnötigerweise zu regulieren, bevor deren Wirkungen nicht selbst erkennbar sind. Damit wird gleichzeitig Institutionen des Internets Zeit gelassen, Regeln zu entwickeln, welche die Erfordernisse der zugrundeliegenden Technik besser erfassen und den Bedürfnissen des Internets stärker entsprechen.

Das Internet bietet für seine Nutzer effiziente Kommunikationsmöglichkeiten, um auf dem aktuellen Stand der technischen Entwicklung zu bleiben. Betroffene Personen haben direkt über die dem Internet inhärente Kommunikationsstruktur die Möglichkeit, sich mit anderen Nutzern über die Lösung ihrer Probleme auseinanderzusetzen. Vorschläge von neuen Rechtsregeln, die solchen Diskussionen entspringen, können sofort an die verschiedenen Internetnutzer weitergeleitet und online diskutiert werden. Ebenso können Entscheidungen von verschiedenen Internetorganisationen oder Streitschlichtungsorganen sofort der Öffentlichkeit vorgestellt werden<sup>186</sup>, ohne daß es eines kostenintensiven Druckes oder eines langwierigen Verteilungsprozesses bedarf. Diese verschiedenen Vorteile der Internetkommunikation können im Vergleich zur herkömmlichen Regulierung zu einer zeitlichen aber auch inhaltlich effizienteren Regelung von internetspezifischen Sachgebieten führen.

Die Globalisierung der elektronischen Kommunikation und der oft charakteristische technische Hintergrund führen dazu, daß äußerlich ähnliche Sachgebiete häufig sehr stark spezialisiert sind, oder Sachgebiete nur für die Internetnutzung eine Rolle spielen. Um eine reibungslose Kommunikation zu ermöglichen, sind Abweichungen zu herkömmlichen Regeln öfters nötig. Dies erscheint besonders dann sinnvoll, wenn die abweichenden Regeln nicht von außen eingebbracht, sondern durch selbstregulierende Organe entwickelt werden. Zum Beispiel ist es unnötig, daß sich staatliche Organisationen mit den technisch internen Regeln zur Versendung von Emails, dem Internetrouting oder Internetprotokollen beschäftigen<sup>187</sup>.

Entsprechend ist es oftmals auch nicht möglich, schon vorhandene Regeln auf das Internet zu übertragen. Besonders die grenzüberschreitende Kommunikation ist schwierig durch nationale Regelungen zu erfassen. Lassen sich solche eventuellen Konfliktpunkte nicht durch Regeln des Internationalen Privatrechts oder ähnlichen Vorschriften lösen, erscheint eine internetinterne Lösung zufriedenstellender.

Werden die Möglichkeiten einer Selbstregulierung konsequent ausgeschöpft und nicht durch staatliche Vorschriften behindert, so können die einzelnen Regeln auch eine größere Akzeptanz finden.

---

<sup>185</sup> Vgl. *Gordon*, 13 J. Marshall J. Computer & Info. L. 177, 194f.; *Gibbons*, 6 Cornell J.L. & Pub. Pol'y 475, 509.

<sup>186</sup> Die Veröffentlichung könnte z.B. sofort durch Mailinglisten oder WWW-Seiten erfolgen.

<sup>187</sup> Vgl. *Perritt*, 12 Berkeley Tech. L.J. 413, 421.

## 2.3. Staatlicher Eingriff vs. Selbstregulierung

---

tanz bei den betroffenen Personen entfalten. Wie in jedem politischem System, werden eigene Gesetze eine größere Achtung genießen, als von außen „aufgedrängte“ Regeln<sup>188</sup>.

Unter Beachtung der dargestellten Punkte kann man somit feststellen, daß oftmals ein selbstregelnder Ansatz einer staatlichen Gesetzgebung vorzuziehen ist. Auf Grund der vielen verschiedenen Sachgebiete, welche auch im Internet eine Rolle spielen, ist eine Verallgemeinerung allerdings nicht möglich. Zum Beispiel scheint die Herausbildung eines neuen internet-spezifischen Vertragsrechtes nicht notwendig, da sich viele Streitfälle durch die über viele hundert Jahren entwickelten Zivilrechtsnormen lösen lassen. Im Gegensatz dazu, gibt es zum Beispiel keine Ansätze zur Regelung der Kommunikation verschiedener Internetserver untereinander. In diesem Fall ist die eigenständige Entwicklung von Regeln die effektivste Vorgehensweise.

Perritt<sup>189</sup> hat verschiedene Kriterien dargelegt, die ein Modell der Selbstregulierung enthalten sollte, um größtmögliche Anerkennung in der Gesellschaft und bei staatlichen Autoritäten zu erlangen<sup>190</sup>:

- Selbstregulierung muß transparent sein. Entscheidungen und neue Regeln sollten sofort veröffentlicht werden,
- neue Regeln sollten nur durch einen fairen Prozeß entstehen können,
- der Regulierungsmechanismus sollte beständig funktionieren, um die reibungslose Nutzung des Internets zu gewährleisten,
- jeder, welcher personenunabhängige, vorher bestimmbarer Fähigkeiten und Eigenschaften besitzt, muß an der Regulierung teilnehmen können.

---

<sup>188</sup> Vgl. Perritt, 12 Berkeley Tech. L.J. 413, 425.

<sup>189</sup> Nähere Erläuterungen siehe Perritt, Berkeley Tech. L.J. 413, 479ff.; siehe auch mit ablehnender Meinung Mankowski, AfP 1999, 138, 139f.

<sup>190</sup> Für den speziellen Fall des Datenschutzes hat die Europäische Kommission durch ihre Data Protection Working Party Richtlinien für die Beurteilung von selbstregulierenden Regimen als Teil eines internationalen Rechtssystems zur Schutz der Privatsphäre veröffentlicht; *Europäische Kommission* (DG XV), Judging Industry Self-Regulation: When Does it Make a Meaningful Contribution to the Level of Data Protection in a Third Country, Kap. Conclusion, 14. Januar 1998,

[http://europa.eu.int/comm/internal\\_market/en/dataprot/wpdocs/wp7en.htm](http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp7en.htm):

„For a self-regulatory instrument to be considered as a valid ingredient of „adequate protection“ it must be binding on all the members to whom personal data are transferred and provide with adequate safeguards if data are passed on to non-members. The instrument must be transparent and include the basic content of core data protection principles. The instrument must have mechanisms which effectively ensure a good level of general compliance. A system of dissuasive and punitive sanctions is one way of achieving this. Mandatory external audits are another. The instrument must provide support and help to individual data subjects who are faced with a problem involving the processing of their personal data. An easily accessible, impartial and independent body to hear complaints from data subjects and adjudicate on breaches of the code must therefore be in place. The instrument must guarantee appropriate redress in cases of non-compliance. A data subject must be able to obtain a remedy for his/her problem and compensation as appropriate.“

### 2.3.4.3. Transnationale Regulierung durch Organisationen und Regeln

Ohne staatlichen Zwang haben sich verschiedene Strukturen im Internet herausgebildet, um den ungestörten Betrieb des Netzes zu gewährleisten. Eine Regierungsinstitution selbst ist dabei nicht entstanden. Vielmehr haben sich mehrere gleichberechtigte Organisationen herausgebildet, welche verschiedene Aufgaben wahrnehmen. Am nächsten einer Regierungsorganisation stehen die ICANN und die ISOC. Die ICANN überwacht die Vergabe der IP-Nummern und der Domainnamen (siehe Kapitel 3.2.1 unten). Sie stellt kein staatliches oder universitäres Institut dar, sondern ist eine privatrechtlich organisierte, gemeinnützige Organisation<sup>191</sup>. Es ist anzunehmen, daß diese neue Organisation mehr rechtliche Ordnung in die Internetaktivitäten bringt, als dies bislang die nationalen Regierungen geschafft haben. Die Hauptaufgabe der ICANN ist jedoch nicht, die Aktivitäten selbst zu regeln oder den Inhalt der Internetkommunikation zu überwachen, sondern primär die reibungslose Funktionsfähigkeit der Internetkommunikation zu gewährleisten.

Die Aufgabe der ISOC ist es, den Informationsaustausch durch das Internet zu fördern (siehe Kapitel 2.4.1.2.2 unten). Sie ernennt das IAB, das über die Standards des Internets wacht. Die Standards des IAB sind selbstvollziehend, wenn die Mehrheit der Internetnutzer einen neuen Standard übernimmt und die Nutzer, welche einer anderen Lösung folgen, von der Kommunikation nach außen ausgeschlossen sind<sup>192</sup>. In der mit der ISOC lose verbundenen IETF werden die verschiedenen technischen Lösungen diskutiert, um allgemeingültige Standards zu finden. Diese Standards werden dann in den schon erwähnten RFCs (siehe Kapitel 2.4.1.3.1 unten) veröffentlicht.

Die einzelnen Internetprovider stellen oft eigene Nutzungsregeln (*Acceptable Use Policies*, AUP) auf, um den Verkehr zu kontrollieren, der über ihren Teil des Netzes fließt<sup>193</sup>. Gewöhnlich verbieten diese Vorschriften Beleidigungen, betrügerische Nutzung des Zugangs, unerlaubten Zugang zum System oder das massenhafte Versenden von Emails<sup>194</sup>. Zusätzlich existieren die verschiedenen *Network Etiquettes*<sup>195</sup> (Netiquette), *Frequently Asked Questions* (FAQ) und formlose soziale Normen, wie Höflichkeit und Anstand, welche die Kommunikation im Internet regeln, aber weder verbindlich sind, noch sich direkt durchsetzen lassen.

### 2.3.4.4. Nachteile der Selbstregulierung

Die Regulierung des Internets ist historisch gewachsen, ohne frühzeitig staatlichen Eingriffen ausgesetzt gewesen zu sein. Dadurch sind die einzelnen Organisationen am engsten an die Erfordernisse der zugrundeliegenden Netztechnik angepaßt. Eine Reaktion auf technische und gesellschaftliche Veränderungen ist zum größten Teil schnell möglich. Jedoch bietet die der-

<sup>191</sup> Die Privatierung der IANA zur ICANN erfolgte nach dem Plan des US Department of Commerce vom Juni 1998; *US-DoC, NTIA*, White Paper, 63 Fed. Reg. 31741.

<sup>192</sup> Vgl. *Gibbons*, Cornell J.L. & Pub.Pol'y 475, 492.

<sup>193</sup> Die Friedrich-Schiller-Universität als ISP für ihre eigenen Studenten veröffentlicht ihre Nutzungsregeln unter: Nutzerordnung, 1. September 2000, [http://www.uni-jena.de/rz/allg/f\\_nutzer.html](http://www.uni-jena.de/rz/allg/f_nutzer.html).

<sup>194</sup> Vgl. *Gibbons*, Cornell J.L. & Pub.Pol'y 475, 493

<sup>195</sup> In *RFC 1855*, Hambridge werden Network Etiquette für diverse Anwendungsbereiche vorgeschlagen.

## 2.3. Staatlicher Eingriff vs. Selbstregulierung

---

zeitige Struktur der Selbstregulierung einige Angriffspunkte. Eine Folge der Entwicklung des Internets aus dem wissenschaftlichen Kreis ist, daß die Lenkung des Internets nur durch eine kleine Personengruppe wahrgenommen wird, welche ursprünglich universitär mit der Entwicklung von Netzwerktechnik betraut waren<sup>196</sup>. Hinzu kommt, daß die meisten dieser Personen den USA entstammen und auch die Organisationen dort rechtlich verankert sind<sup>197</sup>.

Die wichtigsten generigen TLDs wurden bis Mitte 1999 von einer einzigen Firma (NSI) monopolartig verwaltet und vergeben. Es dauerte bis Herbst 1999, bis ein konkurrierendes System der Domainvergabe entstand (siehe Kapitel 3.1.3 unten). Die Verwaltung der Rootdatenbank der TLD .com verbleibt jedoch weiterhin in den Händen von NSI<sup>198</sup>. Kritisiert wird, daß das Internet keine ausreichenden Mechanismen zum Schutz vor Verletzungen von Namensrechten und geistigem Eigentum bietet<sup>199</sup>. Auch fehlt eine formale und demokratisch legitimierte Struktur (zur ICANN-Wahl siehe Kapitel 3.2.2.4 unten) und eine direkte Legitimation der Organisationen durch staatliche Einrichtungen<sup>200</sup>. Es besteht das Risiko, daß Internetorganisationen von privaten Unternehmen, Interessensgruppen und Lobbyisten im verstärkten und für die Öffentlichkeit nicht erkennbaren Maße beeinflußt werden<sup>201</sup>. Schwächere Parteien und Minderheiten würden somit benachteiligt<sup>202</sup>.

### 2.3.4.5. Formen der Selbstregulierung

Selbstregulierung tritt häufig in zwei Formen auf, der Selbsthilfe und der Regelung durch soziale Zwänge<sup>203</sup>. Die Selbsthilfe ermöglicht es Personen, einerseits Situationen zu unterbinden, die ihnen selbst unangenehm sind oder schaden und andererseits auf Situationen Einfluß zu nehmen, welche sie gern abändern möchten<sup>204</sup>. Soziale Zwänge sind die Begleitregeln, welche beim Zusammenschluß von gleichgesinnten Individuen zu Vereinen, Kommunen oder sonstigen Gruppen entstehen und deren Verhalten untereinander regeln. Die einzelnen Mitglieder müssen sich gewöhnlich an diese Regeln halten, um nicht aus einer solchen Gruppe ausgeschlossen zu werden.

---

<sup>196</sup> Z.B. Jon Postel als ehemaliger Leiter der IANA (siehe <http://www.iana.org>) oder Tim Berners-Lee, Chef des World Wide Web Consortiums (siehe <http://www.w3.org/>).

<sup>197</sup> Die ICANN z.B. hat ihren Sitz im Bundesstaat der USA Kalifornien; siehe ICANN, Articles of Incorporation vom 21. November 1998, <http://www.icann.org/articles-pr23nov98.html>. Mankowski, AfP 1999, 138, 140 sieht darin eine Amerikanisierung des Rechts.

<sup>198</sup> Amendment No. 19 zum Cooperative Agreement zwischen DoC und NSI, <http://www.nsol.com/policy/icann/docnsi/coopagmt-amend19-04nov99.html>.

<sup>199</sup> Gibbons, Cornell J.L. & Pub.Pol'y 475, 495.

<sup>200</sup> Mankowski, AfP 1999, 138, 140.

<sup>201</sup> Vgl. auch Christiansen MMR 2000, 123, 126.

<sup>202</sup> Vgl. die ausführliche Diskussion durch Netanel, 88 Calif. L. Rev. 395, 421ff.

<sup>203</sup> Gibbons, Cornell J.L. & Pub.Pol'y 475, 510.

<sup>204</sup> Verschiedene Beispiele zur Selbsthilfe sind in Roßnagel, ZRP 1997, 26, 29 zu finden.

Besonders im amerikanischen Raum sind für das Internet Möglichkeiten der Selbsthilfe geschaffen worden. Dazu zählen besonders Programme<sup>205</sup>, welche Eltern für die Kontrolle und Filterung der Internetzugriffe ihrer Kinder einsetzen können. Vorrangig soll mit diesen Programmen der Zugriff auf Internetangebote pornographischen oder Rassenhaß verherrlichenden Inhaltes unterbunden werden.

Auf der Seite der Pornographieanbieter bestand die Gefahr gegen Vorschriften zum Schutz von Kindern oder Jugendlichen zu verstößen. Sie entwickelten deshalb Methoden, um nur Personen ab eines gewissen Alters zutritt zu gewähren. Es entstanden Systeme wie *Adult Check*<sup>206</sup> oder *VeriSign*<sup>207</sup>, durch welche sich das Alter der Nutzer verifizieren lassen.

Mit dem durch das am *Massachusetts Institute of Technology's* beheimateten W3C entwickelten PICS-System (*Platform for Internet Content Selection*) geht man noch einen Schritt weiter<sup>208</sup>. Dieses System ermöglicht, Internetinhalte mittels eines Etikettes zu klassifizieren. Wenn ein PICS-Etikett einem Dokument angehängt ist, kann der Webbrowser eines Nutzers entsprechend dem voreingestellten PICS-Rating entscheiden, ob er den Inhalt anzeigt oder ablehnt.

Eine Möglichkeit, um Empfängern von Emails die Korrektheit der abgesendeten Email zu versichern, eröffnet das Verschlüsselungsprogramm *Pretty Good Privacy*. Dazu werden Emails mit einem nur dem Absender bekannten Code verschlüsselt. Der Empfänger kann dann die Email mit einem, bei einer öffentlichen Registrierungsstelle hinterlegten Schlüssel, dekodieren. Eine erneute Verschlüsselung der Email, eventuell mit verändertem Inhalt ist nicht möglich. Eine Manipulation der Email durch Dritte ist folglich ausgeschlossen.

Eine Form der Selbsthilfe stellt aber auch der Aufbau von internetspezifischen Organisationen (siehe Kapitel 2.4.1.2.2 unten) dar. In diesen Organisationen haben einzelne Interessengruppen die Möglichkeit, sich medienwirksam zu äußern und auf die zukünftige Entwicklung des Internets Einfluß zu nehmen. Dies kann durch die Unterstützung bei der Entwicklung von neuen Technologien für das Internet über die IETF oder durch eine Einflußnahme auf die Entwicklung des DNS über die ICANN erfolgen.

---

<sup>205</sup> Z.B. *Cybersitter*, *Solid Oak Software*, <http://www.cybersitter.com/>; *Net Nanny*, <http://www.netnanny.com>; oder *Surfwatch*, <http://www.surfwatch.com>.

<sup>206</sup> Siehe <http://www.adultcheck.com>.

<sup>207</sup> Siehe <http://verisign.com>.

<sup>208</sup> Siehe Platform for Internet Content Selection <http://www.w3.org/PICS/>; vgl. auch *Bager*, c't 1999, Heft 20, 40; *Resnick*, Filtering Information, Kap. „What's in a Label?“. PICS-Etiketten für Webseiten können über die Internet Content Rating Association (ICRA) erstellt werden. Die ICRA ist eine internationale und unabhängige Organisation, welche mittels PICS Eltern ein Mittel zum Schutz ihrer Kinder von potentiell schädlichen WWW-Inhalten in die Hand geben möchte, <http://www.icra.org>. Die ICRA bewertet die Internetinhalte nicht, sondern erstellt die PICS-Etiketten nur aus dem vom Inhalteanbieter gemachten Angaben. Ausführlich zum aktuellen Stand der Gespräche in der ICRA siehe *Krempl*, Telepolis 7344.

## 2.3. Staatlicher Eingriff vs. Selbstregulierung

---

Die zweite Form der Selbstregulierung, die Steuerung durch soziale Zwänge setzt voraus, daß sich Internetnutzer freiwillig zusammengeschlossen und gemeinsame Normen für deren Kommunikation geschaffen haben<sup>209</sup>. Dabei wird normgerechtes Verhalten prämiert und gegen die Normen verstößendes Verhalten bestraft, zum Beispiel durch Ausschluß aus der Gruppe. Die Kontrolle kann durch eine Person erfolgen, welche die Regeln aufstellt und auch die Sanktionen durchsetzt. Als Kontrolle können auch Verträge dienen, deren Bestimmungen durch die einzelnen Mitglieder durchgesetzt werden. Schließlich besteht noch die Möglichkeit soziale Umgangsnormen, Satzungen der Vereinigung oder staatliches Recht als Rahmen zur Kontrolle heranzuziehen.

Zu beachten ist jedoch, daß diese Formen der Selbstregulierung nur eine begrenzte Reichweite haben. Die Filtermöglichkeiten der Selbsthilfe verhindern nur, daß Internetangebote für eine bestimmte Zielgruppe zugänglich sind, nicht jedoch, daß diese Inhalte überhaupt angeboten werden. Für einen technisch versierten Nutzer ist es zusätzlich oft möglich, solche Selbsthilfesysteme zu umgehen und für ihn sonst nicht zugängliche Angebote zu nutzen. Entsprechend gelten die sozialen Zwänge einer Internetgemeinschaft nur für deren Mitglieder. Außenstehende Personen können nicht beeinflußt werden. Aus einer solchen Gemeinschaft ausgestoßene Mitglieder könnten versuchen, unter einem anderen Namen wieder in die Gruppe einzutreten, oder sich einer anderen Gruppe gleichen Ziels anzuschließen.

### 2.3.4.6. Regulierung durch Privatrecht

Wie bislang festgestellt, entspricht eine reine staatliche Regulierung des Internets nicht den Anforderungen an die schnell wachsende Computer- und Informationstechnologie. Ein rein selbstregulierender Ansatz würde sich in Anblick der stark differenzierten Ansichten der verschiedenen beteiligten Nutzergruppen kaum verwirklichen lassen. Auch bleibt die Durchsetzbarkeit der durch eine Internetregierung beschlossenen Maßnahmen sehr zweifelhaft. Dennoch erschufen die ersten Internetnutzer basierend auf ihrem persönlichen Einsatz, auf ihrem privaten Kapital und auf ihren Eigentumsrechten an Leitungen und Computern eigene Administrationsinstitutionen. Daraus läßt sich ein neuer Weg der Regulierung des Internets herleiten. Vereinbarungen im privaten Bereich erfolgen grundsätzlich durch Verträge, welche vor staatlichen Gerichten durchgesetzt werden können<sup>210</sup>. Bis zum Bereich, den die staatliche Regulierung läßt, wird der größte Teil des Internet durch private Vereinbarungen reguliert. Um das Recht des Internets zu analysieren, müssen diese Absprachen herausgearbeitet werden. Weiterhin muß untersucht werden, ob sie durch verschiedene Parteien verletzt werden und ob die Vereinbarungen selbst gegen geltendes Recht verstößen. Das heutige Internet beruht auf einer Kooperation von Privatpersonen, die durch Verträge und Protokolle gesichert sind. Diese Verträge beschreiben die Rechte und Pflichten der verschiedenen Internetnutzer untereinander. Die Protokolle, wie zum Beispiel TCP/IP, sind selbstvollstreckende Vorschriften, welche die Kommunikation der einzelnen Teilnehmer ermöglichen. Am Beispiel des DNS bedeu-

---

<sup>209</sup> Vgl. zum Ganzen *Gibbons*, Cornel J.L. & Pub. Pol'y 475, 518ff.

<sup>210</sup> Ausführlich zur Bedeutung des Privatrechts im Internet siehe Osthäus, AfP 2001, 13.

tetet dies, daß demjenigen, der die Vergaberegeln und Protokolle mißachtet, ein Domainname verweigert oder entzogen und er damit teilweise vom Internet ausgeschlossen werden kann<sup>211</sup>.

Die Festsetzung von Regeln in den verschiedenen Gemeinschaften erfolgt häufig durch private Vereinbarung. Diese Regeln bilden dabei die Quelle für die Organisation der Gemeinschaften, der Verhaltensweisen untereinander und auch der Durchsetzung der Regeln. Auf diese Weise können die Parteien eine gewisse Unabhängigkeit von externen Rechtsregeln und Institutionen erlangen. Richtig angewendet, paßt das Vertragsrecht somit am besten zu einem sich schnell entwickelndem Technologiegebiet wie dem Internet<sup>212</sup>. Dabei bilden die Verträge die Grundlage einer privaten Rechtsordnung. Anders als staatliche Regulierung, kann eine auf Verträgen basierende Regulierung sehr schnell auf sich verändernde ökonomische, technische oder soziale Umstände reagieren<sup>213</sup>. Trotz der nur geringen Regulierung durch den Staat, wächst das Internet exponentiell auf allen Gebieten, zum Beispiel der Anzahl der Nutzer, der über das Internet umgesetzten Waren oder der technologischen Entwicklung. Nahezu sofort wurden beim Auftreten von Problemen oder Gefahren Lösungen auf Softwareebene oder in der Infrastruktur gefunden. Setzt sich dabei ein Standard der Vertragsinhalte bei einer Mehrheit der Nutzer durch, so werden auch weitere Nutzer auf diese Vertragsbestimmungen bestehen, um nicht den Anschluß an die aktuelle Technik zu verlieren.

Ohne nach außen stark in Erscheinung zu treten, stellen Verträge den Mittelpunkt der rechtlichen Verhältnisse bezüglich des Zugangs zum Internet dar. Dabei bilden die Internetserviceprovider die zentrale Rolle in der Vertragsstruktur des Internets<sup>214</sup>. Die häufigsten Formen von Verträgen sind hier die Verträge über Computerverbindungen untereinander, durch welche kleinere ISPs sich mit den größeren ISPs verbinden. Die einzelnen ISPs erzielen dabei Gewinne, indem sie das Recht kaufen, sich an einen anderen ISP und damit zum Rest des Internets anbinden zu dürfen. Im Gegenzug verkaufen sie Rechte an weitere ISPs und Endnutzer, sich mit ihrem eigenen Netz verbinden zu dürfen. In Durchführung dieser Verkäufe werden jeweils Zugangsverträge geschlossen, welche die näheren Bedingungen und den Preis der Verbindung spezifizieren. Zwischen ISPs gleicher Größe werden zum Teil Verträge geschlossen, die eine Verbindung beider Netze vorsehen, um den jeweiligen Nutzern einen schnelleren Zugriff zu den Nutzern des anderen Netzes zu gewährleisten. Um den Austausch zwischen vielen Netzen gleichzeitig zu ermöglichen, existieren Betreiber von Knotenpunkten (Router), welche mit Netzbetreibern Verträge über die Weiterleitung ihrer Daten zu anderen Netzen abschließen.

Nicht nur der Zugang zum Internet wird durch Verträge geregelt. Viele Angebote im Internet sind nur nach Abschluß eines Vertrages zugänglich. Dies kann zum Beispiel das Abonnement

---

<sup>211</sup> *Perritt*, 12 Berkeley Tech. L.J. 413, 436.

<sup>212</sup> *Perritt*, 12 Berkeley Tech. L.J. 413, 432. *Froomkin*, 50 Duke L.J. 17, 173f. sieht sogar das Vertragsrecht als Mittel an, zu verhindern, daß die ICANN politische Funktionen wahrnimmt.

<sup>213</sup> *Gibbons*, Cornell J.L. & Pub.Pol'y 475, 483.

<sup>214</sup> *Goldfoot*, 84 Va. L. Rev. 909, 928. Netanel richtet sich gegen die Vertragsfreiheit als Grundstein für die Selbstregulierung des Internets: *Netanel*, 88 Calif. L. Rev. 395, 436ff.

## 2.3. Staatlicher Eingriff vs. Selbstregulierung

---

eines Newsletters, eines Wirtschaftsdienstes oder einer Zugangsberechtigung zu einer Zeitschriftendatenbank sein. Vertragsabschlüsse und die daraus resultierenden Rechte und Pflichten ziehen sich dabei wie ein Netz durch das gesamte Internet.

Protokolle sind die zweite Ebene der vertraglichen Gestaltung des Internets. Obwohl keine Verpflichtung besteht, entsprechend diesen Protokollen im Internet zu kommunizieren, ist es für einen Nutzer notwendig, zumindest die grundlegenden Protokolle zu beachten, um mit anderen Nutzern Kontakt aufzunehmen. Für einen Endanwender ist das Wissen um die notwendigen Protokolle nur insoweit relevant, wie er neue Computerprogramme verwendet, welche neue Protokolle implementieren oder von herkömmlichen abweichen. Zum Teil werden die Protokolle als die eigentlichen Regulierungsmechanismen des Internets betrachtet<sup>215</sup>. Bei allen Verträgen zwischen den ISPs muß implizit vereinbart sein, daß das Internetprotokoll TCP/IP verwendet wird. Ein Provider, welcher TCP/IP oder ein anderes notwendiges Protokoll nicht verwendet, wird sich nicht mit dem Internet verbinden können, um darin zu kommunizieren<sup>216</sup>.

Um zu verhindern, daß die einzelnen Internetnutzer ihre Rechte ausverkaufen und dadurch die Entwicklung des Internets nachhaltig gestört wird, sind gewisse Grenzen der Vertragsfreiheit notwendig. Ebenso muß verhindert werden, daß stärkere Parteien den schwächeren ihre Vertragsbestimmungen zu deren Nachteil aufzwingen. Den Idealfall stellt ein frei ausgehandelter Vertrag, ohne Bevorteilung einer Partei dar. Gerade diese freie Aushandelbarkeit spricht für eine Regulierung des Internets auf Vertragsbasis<sup>217</sup>. Wenn aber Verträge nur durch AGBs geregelt werden, zu welchen die Internetnutzer unbewußt zustimmen und auf ihre Rechte damit verzichten, um zu den verschiedenen Angeboten Zugang zu erhalten, ist ein Mißbrauch naheliegend.

Eine Analyse der Internetverträge umfaßt auch die Untersuchung, ob die einzelnen Vereinbarungen rechtswirksam sind. Obgleich sich private Verträge durch Gerichtsurteile durchsetzen lassen, können sie nicht Rechte und Pflichten als Vertragsinhalt haben, welche gegen das öffentliche Interesse verstößen. So finden Verträge zum Beispiel am Zivilrecht und am Kartellrecht ihre Grenzen. Das Kartellrecht soll, erstens, horizontale Handelsbeschränkungen verhindern, die durch verbotene Verträge und Konspirationen auftreten (Kartelle), zum Beispiel § 1 GWB<sup>218</sup>, Art. 81 EGV, § 1 Sherman Antitrust Act<sup>219</sup>. Zweitens, untersagt das Kartellrecht den Mißbrauch einer marktbeherrschenden Stellung, zum Beispiel § 19 GWB, Art. 82 EGV, § 2 Sherman Antitrust Act<sup>220</sup>.

---

<sup>215</sup> Vgl. z.B. *Lessing*, 5 CommLaw Conspectus 181, 183f.; *Lessing*, 27 Cumb. L. Rev. 1, S 2f.

<sup>216</sup> *Goldfoot*, 84 Va. L. Rev. 909, 929; *Post*, 1995 J. Online L., Artikel 3 Nr. 20.

<sup>217</sup> *Gibbons*, Cornell J.L. & Pub. Pol'y 475, 524.

<sup>218</sup> Gesetz gegen Wettbewerbsbeschränkungen, 26. August 1998, in der Fassung vom 10. November 2001, BGBl. I 1998, 2521 (2001, 2992).

<sup>219</sup> 15 U.S.C. § 1.

Alle Serviceverträge müssen den Kartellrechtsvorschriften entsprechen. Sie dürfen nicht auf die Bildung von Kartellen ausgerichtet sein, Preisabsprachen, territoriale Zusicherungen oder einen Austausch von Kosten und Preisen enthalten<sup>221</sup>. Da die Vereinbarung von Protokollen eine starke Stabilität der aktuellen Netzwerktechnik hervorruft, erscheint eine Anwendung des Kartellrechts in diesem Bereich der privaten Regulierung ebenso angebracht. Man könnte Protokolle als horizontale Handelsbeschränkungen betrachten, die jeden Anwender automatisch mit dem Ausschluß vom Internet bestrafen, der sich nicht an sie hält<sup>222</sup> (vgl. Kapitel 2.4.1.3.3 unten). Die Angebotsvielfalt an Kommunikationstechniken wird dabei erheblich beschränkt. Neue Techniken werden es schwer haben, Anwender zu finden.

Das Kartellrecht bietet ein Mittel, die privaten Vereinbarungen auf Rechtmäßigkeit hin zu überprüfen. Protokolle und Verträge, welche unnötig den Wettbewerb beschränken, sind rechtswidrig. Auch das sonstige Privatrecht kann herangezogen werden, um die Verträge zur Verwaltung des Internets näher zu prüfen.

Auch in den Regeln des Zivilrechts findet die Vertragsfreiheit der Provider ihre Grenzen. Zivilrechtlich können Verträge schon wegen ihrer Unerfüllbarkeit oder Sittenwidrigkeit nichtig sein. Die Regeln des § 138 BGB verhindern Verträge gegen die guten Sitten sowie Knebelverträge mit unverhältnismäßiger Übervorteilung einer Vertragspartei. Nach § 125 BGB sind alle Verträge, welche einer vorgeschriebenen Form ermangeln, nichtig. Das AGBG verhindert, daß Zugangsprovider ihr Risiko unangemessen auf den Endnutzer verlagern. Schließlich soll das UWG Verstöße gegen den lauteren Wettbewerb unterbinden.

Ein weiterer Nachteil einer Regulierung auf Vertragsbasis ist, daß nur für die Vertragsparteien die vereinbarten Rechte und Pflichten gelten. Das Vertragsrecht ermöglicht zwar auch Dritten Rechte zuzusprechen (zum Beispiel § 328 BGB), Verpflichtungen von Dritten sind jedoch nicht möglich. Mittels Vertragsrecht können diese Personen nicht gezwungen werden, bestimmte Handlungen im Internet vorzunehmen oder Informationsangebote zu unterlassen<sup>223</sup>. Nach dem Konzept des Vertragsrechtes ist dies auch nicht notwendig. Das Internet wird von Vertretern verschiedener Nationen und Kulturen genutzt, jede mit ihrem eigenen Verständnis von Recht und Ordnung. Verträge erlauben dabei jeder Gemeinschaft im Internet ihre eigenen Ansichten zu definieren. Verträge sind für sich gesehen immer gerecht und nicht von Beginn an durch die verschiedenen Ansichten, was moralisch oder unmoralisch ist, geprägt. Die Gerechtigkeit eines Vertrages hängt von dem Erlangen einer freiwilligen Vereinbarung ab. Eine freie Entwicklung des Internets kann also nur gegeben sein, wenn nicht einzelne ihre Marktmacht ausnutzen, um anderen ihre Vertragsansichten aufzuzwängen.

In dem der Staat den Abschluß von komplexen Verträgen zuläßt, welche das Verhalten der einzelnen Vertragsparteien umfassend regeln, fördert er indirekt die private Regulierung von

---

<sup>220</sup> 15 U.S.C. § 2.

<sup>221</sup> Siehe auch *Christiansen*, MMR 2000, 123, 127.

<sup>222</sup> *Goldfoot*, 84 Va. L. Rev. 909, 930.

<sup>223</sup> Vgl. *Christiansen*, MMR 2000, 123, 125.

## 2.3. Staatlicher Eingriff vs. Selbstregulierung

---

verschiedenen Sachverhalten. Die einzelnen Regeln werden dabei nicht durch eine politische Gemeinschaft ausgehandelt, sondern durch die Vertragsparteien untereinander. Dabei ist ihre Vertragsfreiheit nicht unbegrenzt. Sie bleiben an die existierenden Rechtssysteme gebunden, welche ihnen vorschreiben, ob ein Gegenstand privat geregelt werden kann. Private Verträge können somit in beschränktem Maße das Verhalten im Internet regeln. Sie können jedoch nicht bestimmen, wie weit sich ein vorhandenes Rechtssystem erstreckt und ob deren Rechtsregeln, wie Deliktsrecht, Strafrecht oder Kartellrecht, auf die Vertragsparteien anzuwenden sind<sup>224</sup>.

### 2.3.4.7. Erfordernis einer eigenen Jurisdiktion

Ein eigenes Cyberrecht wäre ohne Rechtsprechungs- und Streitschlichtungsmöglichkeiten wirkungslos. Für die Streitschlichtung existieren zwei traditionelle Quellen, die staatlichen Gerichte, zuständig nach Regeln des internationalen Privatrechts und die privaten Schiedsgerichte, zuständig auf Grund vertraglicher Vereinbarungen. Die offenen Fragen um die Zuständigkeit, Gerichtsort oder Instanz sowie die schwierige Durchsetzbarkeit fremdstaatlicher Gerichtsurteile erschweren jedoch den Rückgriff auf die staatlichen Gerichte<sup>225</sup>. Das Vertragsrecht bietet jedoch eine einfache Lösung für die Lösung von Rechtsstreitigkeiten im Internet, die Schiedsgerichtsbarkeit. Obwohl das Rechtsgebiet für die Schiedsgerichtsbarkeit neu ist, handelt es sich um eine etablierte Möglichkeit der Streitschlichtung. Die Richter eines Schiedsgerichtes sind nicht an ein bestimmtes lokales Recht gebunden und können so durch Einbezug aller für das Internet relevanter Rechtsnormen entscheiden. Auch können als Richter Personen auftreten, die besondere Erfahrung mit den Regeln, Bräuchen und der Technik im Internet haben. Von solchen Schiedsrichtern kann erwartet werden, daß sie Streite einer für beide Seiten akzeptablen Lösung zuführen. Die Kosten für ein solches Verfahren liegen zusätzlich weit unter denen eines staatlichen Gerichtsverfahrens.

Die Durchsetzung von Urteilen eines Schiedsgerichtes bleibt jedoch an staatliche Behörden gebunden. Es existiert keine Internetautorität, welche die Macht hat, Urteile von Internetschiedsgerichten durchzusetzen. Da solche Urteile nur auf Grund einer privaten Schiedsgerichtsvereinbarung ergehen können, erhalten die Internetschiedsgerichte nur durch staatliche Gerichte ihre Autorität, welche die Schiedsentscheidungen wie jegliche anderen vertraglichen Bestimmungen durchsetzen können<sup>226</sup>. Ohne das Einverständnis aller Streitparteien kann kein Schiedsgericht (auch kein „Internetgericht“) über den Streit entscheiden. Diese Schiedsabrede muß weiterhin einen Verweis auf das anzuwendende Recht beinhalten, insbesondere ob bestimmte, sich im Internet herausgebildete Regeln anzuwenden sind<sup>227</sup>. Für den deliktischen und gewerblichen Rechtsschutz können jedoch allenfalls nachträgliche Schiedsabreden getroffen werden. Entsprechend kann ein spezielles Internetrecht nur zwischen gleichberechtigten Vertragspartnern bestehen, und nicht in Bezug auf die Verbraucher. Die Effektivität einer

---

<sup>224</sup> Vgl. *Stein*, 32 Int'l Law. 1167, 1170ff.

<sup>225</sup> *Gibbons*, Cornell J.L. & Pub.Pol'y 475, 531.

<sup>226</sup> Vgl. *Stein*, 32 Int'l Law. 1167, 1170ff.

<sup>227</sup> *Mankowski*, AfP 1999, 138, 139.

eigenen Internetjurisdiktion ist somit vollkommen von der Macht und der Autorität der verschiedenen Staaten und der Zustimmung der einzelnen Parteien abhängig.

Zur Zeit existieren mehrere Projekte, Schiedsgerichte im Internet zu etablieren. Zum Beispiel bietet das *Online Ombuds Office*<sup>228</sup> als Mittelsmann Hilfe bei der Streitschlichtung an. Ebenso ist das *Virtual Magistrate Project*<sup>229</sup> ein erster Schritt in Richtung eines richtigen Schiedsgerichtes. Da es nur im Internet existiert und globale Streitigkeiten annimmt, kann es Auseinandersetzungen lösen, ohne sich nur auf ein lokales Recht berufen zu müssen. Um den globalen Schiedsgerichtsservice nutzen zu können, müssen die Parteien sich einigen, daß ihre Dispute durch den *Virtual Magistrate* geschlichtet werden. Als US-amerikanisches Projekt, werden alle Fälle von der *American Arbitration Association* überwacht. Das Schiedsgericht kann sich also den Beistand und die Unterstützung einer langjährig erfahrenen Institution sicher sein.

Das deutsche Projekt *Cybercourt*<sup>230</sup> versucht zunächst eine Online-Plattform für die Streitschlichtung anzubieten. Diese institutionelle Streitschlichtungsstelle will es ermöglichen, daß Streitigkeiten in einem nichtförmlichen Verfahren per Internet in sogenannten Chatboxen erörtert und beigelegt werden können. Jede Partei kann vom Büro oder von Zuhause aus teilnehmen. Der Tätigkeitsschwerpunkt des *Cybercourts* liegt naturgemäß im Bereich des EDV-Rechts. Die Zielgruppe reicht von Privatpersonen, die Probleme mit Software-Herstellern haben, bis zu Großunternehmen mit markenrechtlichen Streitigkeiten. Voraussetzung ist lediglich, daß sich die Parteien einigen, die Sache vor dem *Cybercourt* auszutragen. Die Vision der Betreiber des *Cybercourts* ist es, ein staatlich anerkanntes Online-Schiedsgericht aufzubauen<sup>231</sup>. Die Parteien sollen dabei in einer Art Videokonferenz an der Verhandlung teilnehmen. Um die hohen Anforderungen des Art. 103 Abs. 1 GG in Verbindung mit den Regeln der ZPO zum Schiedsverfahren erfüllen zu können, ist jedoch ein hoher technischer Aufwand erforderlich. Zur Zeit läßt sich dieser noch nicht kostengünstig realisieren, um eine preiswerte Alternative zum Gerichtssaal zu bieten. Einen für die Praxis akzeptablen Anfang bietet jedoch das schon erwähnte Online-Streitschlichtungsverfahren.

Das von der WIPO in Verbindung mit der ICANN ins Leben gerufene Projekt zur Schlichtung von Streitigkeiten um Domainnamen (die UDRP) stellt jedoch das wichtigste Beispiel eines Online-Schiedsgerichtes dar (ausführlich zur UDRP siehe Kapitel 3.3.1.2 unten). Im Vergleich zu den eben erwähnten Institutionen stellt die UDRP jedoch nur einen sehr begrenzten Anwendungsbereich zur Streitschlichtung zur Verfügung. Dennoch ist es mit inzwischen mehreren tausend Endscheidungen eine inzwischen unverzichtbare Rechtsinstitution innerhalb des Internets.

---

<sup>228</sup> Siehe <http://www.ombuds.org>.

<sup>229</sup> Siehe <http://www.vmag.org/>. Näheres zum Verfahren kann in Friedman, 19 Hastings Comm/Ent L.J. 695, 700ff. und Gibbons, Cornell J.L. & Pub. Pol'y 475, 535ff. gefunden werden. Gegen einen Virtual Magistrate richtet sich Mankowski, AfP 1999, 138, 140, verkennt jedoch, daß es sich hierbei um ein normales Schiedsgericht handelt.

<sup>230</sup> Siehe <http://www.cybercourt.org>.

<sup>231</sup> Vgl. <http://www.cybercourt.org/vision.htm>.

### 2.3.5. Regulatorische Mix

Wie dargestellt, differieren die Ansichten über eine optimale Regulierung des Internets stark. Auf der einen Seite wird das nationale Recht als völlig unanwendbar angesehen, andererseits einer Selbstregulierung keine Chancen zugesprochen. Die optimale Lösung läßt sich sicherlich zwischen den Extremmeinungen finden<sup>232</sup>. Die Internetregulierung wird sich wie im realen Raum entwickeln und einen Mix aus lokalem, nationalem und internationalem Recht darstellen, welcher stets durch Selbstregulierungsversuche begleitet sein wird. Der Erfolg der aktuellen Versuche, althergebrachte Rechtsgrundsätze auf das Internet anzuwenden, hängt größtenteils von der zu regulierenden Aktion ab. Da das Internet in vielen Fällen die gesellschaftlichen Grundstrukturen nicht erheblich verändert, sind die althergebrachten Rechtsgrundsätze weiterhin anwendbar. In anderen Fällen muß man beim in Kraft setzen neuer Gesetze Vorsicht walten lassen, da auf Grund der Natur so manche Regulierungsversuche erfolglos sein könnten.

Entsprechend sollten die Worte aus der Erklärung des Weißen Hauses der USA beachtet werden<sup>233</sup>:

Governments can have a profound effect on the growth of commerce on the Internet. By their actions, they can facilitate electronic trade or inhibit it. Knowing when to act and – at least as important – when not to act, will be crucial to the development of electronic commerce.

Wenn eine staatliche Regulierung unumgänglich ist, so sollte auf jeden nationalen Alleingang verzichtet werden und eine internationale Lösung, am besten unter dem Gerüst der WTO, gefunden werden<sup>234</sup>. Eine gute Variante, um den Internetgeschäftsverkehr zu fördern, wäre das Modelrecht der UNCITRAL zum Geschäftsverkehr auf das Internet (siehe Kapitel 2.3.3.1 oben) anzuwenden. Schon vorhandene selbstregulierende Ansätze wie Bräuche und Gewohnheitsrecht dürfen jedoch nicht mißachtet werden und müssen in eine internationale Regulierung mit einbezogen werden.

## 2.4. Verwaltung des Internet

Obgleich immer wieder eine Hervorhebung der anarchistischen oder chaotischen Struktur des Internets erfolgt, wird das Internet von einer Reihe Organisationen gelenkt und verwaltet. Der Begriff Verwaltung ist allerdings nicht im Sinne zu verstehen, daß staatliche Regierungen ihre Verwaltungstätigkeit als Exekutive wahrnehmen. Mangels eines ausgeprägten Zwangsapparates, wie dieser sich in den nationalen Staaten herausgebildet hat, greifen die Internetorganisationen häufig auf internetspezifische Instrumentarien zurück. Hierbei spielt das Streben nach einem Konsens eine besondere Rolle. Verfahren zur Erlangung eines Konsenses bilden die Grundlage vieler im Internet stattfindender Entscheidungsprozesse. Ohne Konsens hätten die

---

<sup>232</sup> So auch *Geist*, Wash. L. Rev. 521, 569ff.; ähnlich *Christiansen*, MMR 2000, 123, 129.

<sup>233</sup> *US-White House*, Framework, Kap. Background.

<sup>234</sup> Vgl. auch *Aragón*, 3 Int. J. Com. L. & Pol'y, Web-Doc 8, 14f.

vielen Standards, auf denen das Internet beruht, nicht umgesetzt werden können. Ohne diese wäre heute das Internet ein zersplittertes System von eigenständigen Netzwerken.

Die Verwaltung des Internets basiert auf drei Säulen, welche sich jedoch organisatorisch nicht klar voneinander trennen lassen. Die reibungslose Kommunikation im Internet funktioniert durch die gemeinsamen technischen Standards, welche gemeinsam die erste Säule bilden. Die Standards werden von einer Reihe von Internetorganisationen entworfen und umgesetzt, welche schon längere Zeit im relativ kurzen Leben des Internets existieren. Die zweite Säule stellt die Vergabe und Verwaltung der IP-Adressen durch die *IP-Registries* dar, die eine Kommunikation über das Internet erst ermöglichen. Das DNS stellt als System, welches Voraussetzung für die meisten Internet-Anwendungen ist, die dritte Säule dar, und untersteht heute vorrangig der ICANN. In der ICANN sind jedoch auch Vertreter der standardsetzenden Organisationen und der *IP-Registries* vertreten. Damit stellt die ICANN das zentrale Organ des Internets dar. In dieser Arbeit soll intensiver auf diese Organisation im Kapitel 3 unten eingegangen werden. Zunächst werde ich aber auf die genannten drei Säulen insbesondere die Standardsetzung eingehen.

### 2.4.1. Standards im Internet

An der Weiterentwicklung des Internets sind eine Reihe von Institutionen beteiligt, deren Aufzählung einem Laien wie ein Buchstabensalat vorkommen mag. In diesen Organisationen wird ständig über neue Standards und Entwicklungen diskutiert. Politische Entscheidungen und die Einführung neuer Standards erfolgen dabei meistens durch Diskussionen im Netz. Eine Rolle spielen hierbei Newsgroups und Mailinglisten sowie die sogenannten *Requests for Comments* (RFCs).

Wie schon erwähnt, stellen die verschiedenen Protokolle die Grundvoraussetzungen einer reibungslosen Kommunikation im Internet dar. Sie definieren bestimmte Kommunikationsregeln für die speziellen Internetanwendungen. Da diese Regeln von keiner Regierungsinstanz vorgeschrieben werden, müssen sie in einem Standardsetzungsverfahren entwickelt werden. Dieses weit verbreitete Verfahren ist ein wichtiges Mittel zur Selbstregulierung im technischen Bereich. Das Internet stellt insoweit eine herausragende Rolle dar, da hier sehr verschiedene Standardisierungsmechanismen zur Anwendung kommen. Im Folgenden soll deshalb die Standardsetzung im Internet näher beleuchtet werden. Zunächst sollen die allgemeinen Grundsätze der Standardsetzung erläutert werden, bevor auf die Standardisierung im Internet und die daran beteiligten Internetorganisationen eingegangen wird.

#### 2.4.1.1. Standardsetzung im Allgemeinen

Um die Grundsätze der Standardsetzung zu erläutern, ist es notwendig, die Wirkungsweise, die Vorteile und die Risiken dieser näher zu beleuchten. Im Anschluß daran sollen Möglichkeiten vorgestellt werden, wie ein Standard sich entwickeln und umsetzen läßt.

### 2.4.1.1.1. Wirkungsweise von Standards

Die Standardisierung ist zu einem notwendigen Bestandteil der heutigen Technologisierung geworden und in fast jedem Bereich zu finden. Dazu zählen unter anderem die gesamte Computer-, Mobilfunk- und Telekommunikationsbranche oder die Automobil- und Maschinenbau-technik. Standards beschreiben Voraussetzungen von Schnittstellen, welche die Interaktion zwischen verschiedenen Produkten ermöglicht<sup>235</sup>. Sie stellen somit technische Lösungen dar, um die Interaktion von verschiedenen Erzeugnissen zu gewährleisten. Häufig existieren konkurrierende Standards, die Lösungen des gleichen technischen Problems zulassen. Zum Beispiel beschreiben die inkompatiblen SECAM- oder PAL-Standards jeweils den Aufbau eines Fernsehsignals, welches von einem Fernsehgerät in eine Bildfolge umgewandelt wird.

Kompatible Schnittstellen ermöglichen die Nutzung von Kernprodukten eines Herstellers mit Peripherie- sowie Zusatzprodukten und Dienstleistungen verschiedener weiterer Hersteller. Zum Beispiel kann ein PC mit den Standards setzenden Betriebssystemen *Windows 2000* von Microsoft oder dem freien *Open Source Linux* betrieben werden und jeder Softwarehersteller kann unter Beachtung der jeweiligen Spezifikationen für diese Systeme eigene Anwendungsprogramme entwickeln.

Je verbreiteter ein Standard ist, desto attraktiver wird es für Neueinsteiger, sich für diesen zu entscheiden. Ein neuer Konsument, welcher sich für die Anwendung eines Systems entscheiden muß, hofft, solange wie möglich mit diesem Standard arbeiten zu können, ohne von technischen Neuerungen überholt zu werden. Produzenten wiederum werden sich für das System entscheiden, welches den größten Absatzmarkt verspricht. Deshalb mußten Anfang der neunziger Jahre Unternehmen wie T-Online oder AOL in ihre proprietäre Kommunikationssysteme einen Internetzugang integrieren, da sie sonst bedeutende Marktanteile verloren hätten. Auch für den Markt von Betriebssystemen gilt, daß je verbreiteter ein System ist und sich auf dem Markt etabliert hat, um so vielfältiger das Angebot von Anwendungssoftware für das jeweilige Betriebssystem sein wird.

Die Verbreitung eines Standards ist dabei nicht statisch, sondern unterliegt dynamischen Marktschranken. Zunächst muß ein Standard so überzeugend sein, daß sich neue Anwender für ihn entscheiden. Je mehr sich für ihn entscheiden, um so attraktiver wird er auch für die bisherigen Nichtanwender. Wenn ein Standard einmal eine bestimmte Verbreitung erreicht hat, kann es zu einem weiteren selbstlaufenden Wachstum kommen (sog. „*tipping effect*“<sup>236</sup>). Sollte er die klare Marktführerschaft erreichen, könnte es zu einem Auslöschen anderer Standards führen.

Für neuere Standards ist es schwierig, sich gegenüber einem solchen Marktführer mit einer ausgeprägten unterstützenden Basis zu behaupten. Solche Standards müssen gravierende innovative Lösungen beinhalten und auch neue, bislang offene, technische Probleme lösen, um

---

<sup>235</sup> Vgl. *Ladeur*, CR 1999, 395, 396; *Grindley/Salant/Wavermann*, 3 Int. J. Com. L. & Pol'y, Web-Doc 2, 9.

<sup>236</sup> Vgl. z.B. *Lemley*, 28 Conn. L. Rev. 1041, 1049; *McGowan*, 18 Hastings Comm. & Ent. L.J. 771.

auf dem Markt akzeptiert zu werden. Entsprechend können Standards viele Jahre bestehen, ehe sie durch neuere Systeme abgelöst werden. Beispiele dafür findet man im täglichen Leben, genauso wie im Internet. In allen deutschen Haushalten werden die Schuko-Steckdosen seit vielen Jahrzehnten verwendet, nachdem sie Steckdosen ohne Schutzkontakte abgelöst hatten und inzwischen die verschiedenen Netzsteckervarianten ohne Erfolg vermarktet wurden sind. Im Internet wird seit vielen Jahren das Standardprotokoll SMTP zur Emailübertragung genutzt, ohne daß neuere Systeme, wie zum Beispiel das *Instant Messaging*, es nur ansatzweise verdrängen konnten.

Der Weg für einen Standard zu einer entsprechenden ökonomischen Verbreitung kann jedoch steinig sein. Einerseits muß er so speziell sein, daß die Interaktivität der darauf basierenden Produkte und Dienstleistungen gewährleistet ist, andererseits besteht das Risiko, von der Technik überholt zu werden und aktuelle Entwicklungen nicht mehr einbinden zu können. Vorhersagen, welche technische Lösung der Marktführer werden wird, sind somit kaum möglich.

#### 2.4.1.1.2. Vorteile für den Verbraucher

Um zu klären, warum für das Internet eine Standardisierung der Kommunikation unerlässlich ist, soll zunächst auf die verschiedenen Vorteile einer Standardisierung für den Endverbraucher eingegangen werden. Dabei sind die vorteilhaften Außenwirkungen von Standards um so größer, je verbreiteter die Anwendung des jeweiligen Standards ist<sup>237</sup>. Folgende Vorteile sind besonders hervorzuheben<sup>238</sup>:

- Erreichbarkeit  
Standards ermöglichen den Zugang zum Netzwerk durch die verschiedenen Endgeräte und Internetprovider. Je mehr Endgeräte (Computer, Telefone, oder sonstige Haushaltsgeräte<sup>239</sup>) mittels TCP/IP kommunizieren können, desto einfacher wird es für einen Nutzer sein, diese an das Internet anzuschließen<sup>240</sup>. Durch das Protokoll *Point to Point Presence*<sup>241</sup> (PPP) ist es mittels eines Computers und eines Telefonanschlusses überall auf der Welt möglich, eine *Datenfernübertragungsverbindung* (DFÜ) zum Internet herzustellen.
- Erweiterter Markt  
Eine Standardisierung ermöglicht eine preiswertere Entwicklung von ergänzenden Produkten. Es wird somit der Umfang der erhältlichen Produkte sowie die Vielfalt der

---

<sup>237</sup> Vgl. z.B. Beck, WuW 1999, 460, 465.

<sup>238</sup> Vgl. hierzu auch die Ausführungen in Grindley/Salant/Wavermann, 3 Int. J. Com. L. & Pol'y, Web-Doc 2, 28. Siehe auch die Vorteile der Standardisierung, wie sie von der ISO gesehen werden: ISO, Why is international standardization needed?

<sup>239</sup> Siehe zur Vernetzung von Haushaltsgeräten über das Internet die Darstellung von Kuri, c't 1999, Heft 22, 178ff.

<sup>240</sup> Beck, WuW 1999, 460, 465.

<sup>241</sup> Dieses Protokoll wurde erstmalig in RFC 1134, Perkins vorgestellt.

Produktpalette erhöht. Diese Vielfalt führt wiederum zu einem Wettbewerb der unterschiedlichen Produktanbieter und folglich zu niedrigeren Preisen.

- Kostensparnis

Da ein Teil der Produktentwicklung durch die Standardisierung entfällt, führt die Standardsetzung zu verringerten Kosten. Die dadurch mögliche Erhöhung der Produktion kann wiederum zu einer Kostenverringerung führen.

- Wettbewerb

Da Standards den Zugang zum Internet bedeutend erleichtern, können Kunden schneller von einem *Internet Service Providers* (ISP) zu einem anderen wechseln. Um die Kunden zu halten, erhöht sich folglich der Wettbewerb der Anbieter untereinander. Dies führt wiederum zu niedrigeren Preisen und besseren Service für die Endanwender.

- Innovation

Ein offener Markt, in welchem hoher Wettbewerb herrscht und durch die Standardisierung eine Austauschbarkeit von Produkten verschiedener Hersteller gegeben ist, wird auch stets zu neuen innovativen Produkten führen. Je größer ein solcher Markt ist, um so anziehender wird er für Verbesserungen und Weiterentwicklungen sein.

Die Bedeutung der einzelnen positiven Effekte lässt sich nicht unabhängig voneinander feststellen. Die Vorteile sind stark mit einander verknüpft. Wird einer durch bestimmte Maßnahmen verstärkt, wirkt sich dies automatisch auf die anderen aus. Der Hauptfaktor für die Ausmaße der einzelnen Effekte ist die Verbreitung des Standards. Die aus den einzelnen Vorteilen herrührende Attraktivität von Standards führt dazu, daß sich ein Konsument für das Produkt entscheiden wird, dessen zugrundeliegender Standard die weiteste Verbreitung gefunden hat, da er hier die optimalen Vorteile herausziehen kann. Soweit andere Standards keine entsprechende Anziehungskraft entgegensetzen können, wird der marktführende Standard immer interessanter für die Anwender werden.

### 2.4.1.1.3. Potentielle Risiken für den Verbraucher

Dieser anziehende Effekt eines marktführenden Standards birgt jedoch einige Risiken in sich. Ein Nachteil ergibt sich aus der Schwierigkeit den bestehenden marktführenden Standard abzuändern oder zu ersetzen. Wie schon erläutert, müssen neue und bessere Problemlösungen oft hoch innovativ sein, um auf dem Markt akzeptiert zu werden. Neue Standards lehnen sich häufig an den alten Marktstandard an und übertragen von diesem wichtige Elemente weiter auf die folgenden Technikgenerationen. Um eine Abwärtskompatibilität zu gewährleisten, ist oft der weitere Entwicklungsweg des Marktes vorgezeichnet. Bei einer näheren Betrachtung der Standardisierung des Marktes lassen sich folgende Probleme finden<sup>242</sup>:

- Fragmentierung

Durch parallele Standardisierung eines technischen Problems kann der Markt in mehrere einzelne Segmente zerfallen. In diesen Segmenten kann sich zwar jeweils ein selbständiger Standard entwickeln, ein Übergriff auf andere Segmente wird jedoch auf Grund einer begrenzten Verbreitung nicht möglich sein.

- Fehlende Weiterentwicklung

Einige Standards könnten in eine Sackgasse führen und von anderen völlig vom Markt verdrängt werden. Obwohl eine Weiterentwicklung nicht mehr möglich ist, bleiben Anwender, welche stark in eine solche Technologie investiert haben, an diese Standards gebunden. Ein Umstieg ist nur durch einen kostenintensiven Aufwand möglich<sup>243</sup>.

- Verfrühte Entwicklung

Ein Standard kann sich für eine Branche zu frühzeitig etablieren, ohne daß die derzeitige Forschung und Entwicklung einen festen Standard schon benötigen würde. Die Entwicklung würde somit frühzeitig in eine Richtung gezwängt, ehe die weiteren Lösungsmöglichkeiten ausgelotet wurden. Eine Behinderung der technischen Entwicklung ist damit inbegriffen.

- Überalterung

Ein voll integrierter Marktstandard kann lange Zeit gegen neuere und bessere Lösungsmöglichkeiten resistent sein oder weiterbestehen, obwohl er auf Grund der technischen Entwicklung obsolet geworden ist. In geringerem Maße kann ein Standard auf weitere Generationen fortwirken, in dem diese eine Abwärtskompatibilität gewährleisten müssen<sup>244</sup>. Eine Weiterentwicklung der Technik wird somit auch durch diesen Effekt gebremst.

- Path Dependence

Nicht nur die Entwickler von Standards sind häufig an ihre früheren Entscheidungen gebunden. Auch die Anwender sind häufig so eng mit einer Produktreihe eines Standards verbunden, daß ihnen ein Wechsel auf einen neuen und besseren Standard nahezu unmöglich ist. Erst wenn sie ihre bisher erstellten Daten oder Anwendungen weiter verwenden können oder diese sich in den neuen Standard übersetzen lassen, wird es zu einem Wechsel kommen.

---

<sup>242</sup> Vgl. *Grindley/Salant/Wavermann*, 3 Int. J. Com. L. & Pol'y, Web-Doc 2, 29f.

<sup>243</sup> In der Computerbranche läßt sich ein Umstieg auf die Hauptstandards leichter durch die Verwendung von Konvertiertools oder Adaptern erreichen.

<sup>244</sup> Das Betriebssystem Windows 98 von Microsoft ermöglicht z.B. die Nutzung von Programmen, welche für das erste von Microsoft entwickelte Betriebssystem MS DOS geschrieben wurden.

- Überstandardisierung

Wie ein Markt durch zu viele Standards zu zersplittern droht, ist es ebenso möglich die Produktvielfalt durch eine unnötige Überregelung einschneidend einzuschränken. Die optimale Reichweite einer Standardisierung ist dabei schwer zu bestimmen und hängt vom jeweiligen Einzelfall sowie dem Ziel der jeweiligen Standardisierung ab. Insbesondere kann der Nachteil einer begrenzten Vielfalt von Kernprodukten durch eine größere Auswahl an Zusatz- und Erweiterungsprodukten aufgehoben werden.

Um solche negativen Effekte zu vermeiden, wird häufig versucht, ausgewogene Standards durch Standardisierungsorganisationen auszuhandeln. Dabei besteht das Risiko, daß Wettbewerber, anstatt konkurrierende Technologien anzubieten, bei der Entwicklung zusammenarbeiten. Ein solcher Prozeß der Standardsetzung birgt einige gesellschaftliche und wettbewerbsrechtliche Risiken in sich, die im folgenden näher beleuchtet werden.

### 2.4.1.1.4. Weg zur Standardisierung

Um ein Produkt zu standardisieren, sind die konträren Vorstellungen der verschiedenen Hersteller und Nutzer untereinander abzustimmen. Zum erreichen dieses Ziel, existieren verschiedene Wege. Einerseits kann ein Standard durch eine staatliche Organisation festgelegt und für die Anwender für verbindlich erklärt werden. Andererseits kann man die Entwicklung von Standards dem Wettbewerb des freien Marktes überlassen, in welchem sich der Standard durchsetzen wird, welcher die meisten Vorteile bietet. Einen Mittelweg stellt die Standardsetzung durch privatrechtliche Standardisierungsorganisationen dar.

Häufig bieten verschiedene Unternehmen konkurrierende Lösungen für die gleiche technische Anwendung. Dabei handelt es sich zunächst nicht um Standards, sondern um eigene auf ihre Produkte beschränkte Entwicklungen. Erst mit Lizenzierung der oft durch Patente geschützten Entwicklungen an andere Unternehmen oder durch Adaptierung und Nachahmung der Produkte durch weitere Unternehmen kommt es zu einer weiteren Verbreitung der Lösungen. Dabei werden sich gewöhnlich die nützlichsten und kosteneffektivsten Entwicklungen auf dem Markt durchsetzen und somit zu Standards werden.

Standardisierungsorganisationen entwickeln Standards hingegen unabhängig vom Markt und den Interessen einzelner. Am Verhandlungsprozeß können Vertreter von Produzenten, Anwendern und Regierungsbehörden beteiligt sein. Die Rechtsformen von Standardisierungsorganisationen sind sehr vielfältig. Sie reichen von Industrie- oder Technikervereinigungen<sup>245</sup> ohne Rechtssetzungsbefugnis bis hin zu staatlichen Regulierungsbehörden<sup>246</sup>. Sie können sich

---

<sup>245</sup> Im Internet ist diese Organisationsform vorwiegend anzutreffen, zum Beispiel die Internet Engineering Task Force (IETF), oder das World Wide Web Consortium (W3C).

<sup>246</sup> Im Telekommunikationsbereich spielt eine staatliche Regulierung eine große Rolle. Für den europäischen Raum ist z.B. European Telecommunication Standards Institute (ETSI) die durch die Europäische Kommission eingesetzte Standardisierungsorganisation für den Telekommunikationsbereich. Im Raum der USA nimmt diese Aufgabe die *Federal Communications Commission* (FCC) wahr.

nur einem speziellen Thema<sup>247</sup> widmen oder allgemeine Normungstätigkeiten<sup>248</sup> für ein breites Band an Normungsproblemen wahrnehmen.

Wird der Standardisierungsprozeß dem freien Markt überlassen, können sich mehrere unabhängige Lösungsmöglichkeiten entwickeln und um Akzeptanz bei den Nutzern kämpfen. Die Bestandteile der Standards werden dann anhand von ökonomischen Kennzahlen bestimmt und richten sich nicht alleine nach technischen Voraussetzungen. Marktstandards entstehen gewöhnlich schnell, da die jeweiligen Standardsetzer die ersten auf dem Markt sein möchten, um ihre Lösung zu etablieren. Entsprechend schnell werden auch neue innovative Produkte auf den Markt gebracht.

Die Standardsetzung mittels einer staatlichen Organisation bietet den Vorteil, daß die verschiedenen Interessen von Produktanbietern und Endnutzern mit in den Standard einfließen. Ebenso ist eine langfristige Planung möglich, da nicht nur kurzfristige Aspekte in die Ausgestaltung des Standards mit einfließen. Es können auch nichtökonomische Aspekte wie zum Beispiel Umwelt- oder Kulturschutz beachtet werden. Durch die umfassendere Planung kann verhindert werden, daß viele inkompatible Produkte entstehen, welche eine weitere Entwicklung bremsen, da solchen Produkten nur eine beschränkte Verwendbarkeit inhärent ist. Konsumenten müßten sich sonst häufiger auf neue Produktreihen einstellen und hätten somit höhere Investitionskosten zu tätigen<sup>249</sup>. Ältere Produkte, die einem Standard angehören, welcher sich auf dem Markt nicht durchsetzen konnte, müßten durch neue Produkte ersetzt werden, um weiterhin Interoperabilität zu gewährleisten. Bei einem Vertrauen auf die Marktentwicklung müßten die einzelnen Firmen jeweils selbst Forschungs- und Entwicklungsarbeit leisten. Durch die parallele auf privater Ebene verlaufende Entwicklungsarbeit würden folglich höhere Kosten entstehen, als dies bei einer zentralen Entwicklung der Fall wäre. Marktstandards können auch zu einem fragmentierten System führen, wenn verschiedene Standards in verschiedenen Marktsegmenten oder verschiedenen geographischen Regionen eingesetzt werden<sup>250</sup>. Schließlich ist es einem Marktführer auf Grund seiner Marktmacht möglich, seine Lösung eines technischen Problems gegenüber der Konkurrenz durchzusetzen, auch wenn bessere Standards existieren<sup>251</sup>.

Wie eben beschrieben, dürfte die Standardisierung von technischen Problemen nicht allein dem Markt überlassen werden, sondern sollte mit Hilfe von Standardisierungsorganisationen

---

<sup>247</sup> Zum Beispiel das *World Wide Web Consortium*.

<sup>248</sup> Wichtige Normungsorganisationen sind in Deutschland das Deutsche Institut für Normung (DIN) oder der Verein Deutscher Ingenieure (VDI)

<sup>249</sup> *Grindley/Salant/Wavermann*, 3 Int. J. Com. L. & Pol'y, Web-Doc 2, 31.

<sup>250</sup> In der Mobilfunkbranche wird z.B. in Europa der Global Standard for Mobile (GSM) verwendet. Im Gegenzug herrschen in Nordamerika die Standards für Mobilfunk Time Division Multiple Access (TDMA) und Code Division Multiple Access (CDMA) vor, vgl. *Grindley/Salant/Wavermann*, 3 Int. J. Com. L. & Pol'y, Web-Doc 2, 4ff. Für den Endanwender offensichtlicher sind die vielen inkompatiblen Varianten von Netzsteckern, welche in den verschiedenen Staaten verwendet werden.

<sup>251</sup> Vgl. *Beck*, WuW 1999, 460, 466.

erfolgen<sup>252</sup>. Der Staat kann einerseits diese Organisationen kontrollieren und regulierend einschreiten. Andererseits kann er diesen Organisationen volle Freiheit zugestehen, ohne in die technischen Angelegenheiten einzutragen. Bei freien Organisationen können die folgenden Vorteile voll zum Tragen kommen:

- **Geregelter Entwicklungs- und Vermarktsprozeß**  
Die Standardisierung durch Organisationen ermöglicht die Festlegung von Standards, bevor einzelne Produkte entwickelt und vermarktet werden. Parallel Entwicklungskosten sowie Kosten, welche durch „Standardisierungskriege“ und Investitionen in Entwicklungssackgassen entstanden sind, entfallen für die einzelnen Firmen und Endkunden<sup>253</sup>. Außerdem können Entwickler und Hersteller von Grundprodukten und Zubehör ihre Produkte in einem stabilen Umfeld entwerfen, mit der Sicherheit, daß der verwendete Standard eine marktführende Stellung einnimmt.
- **Erreichen eines optimalen Netzwerkeffektes**  
Bei einem im Markt vorangetriebenen Standardisierungsprozeß besteht das Risiko, daß der Gewinner den gesamten Markt übernimmt („winner take all“<sup>254</sup>). Als Monopolist hat er dann die Möglichkeit, einen höheren Preis für seine Produkte zu verlangen, als dies unter Wettbewerbsbedingungen möglich wäre. Ebenso kann er die weitere Entwicklung bremsen oder in eine nur für ihn vorteilhafte Richtung lenken. Ein Marktführer kann schließlich einseitig einen Standard setzen. Der daraus für die Gesellschaft resultierende Netzwerkvorteil wird gewöhnlich geringer ausfallen, als bei einer zentralen Standardisierung<sup>255</sup>, in welcher alle Marktteilnehmer die gleiche Ausgangsposition haben.
- **Hilfe für den Markt**  
Produzenten fällt es schwer, die Marktentwicklung vorauszuhahnen. Welche Technologie Marktführer werden wird, ist kaum feststellbar. Deshalb werden viele Marktteilnehmer vorerst die weitere Entwicklung abwarten. Standardisierungsorganisationen können hier einerseits Marktinformationen bieten, andererseits die Wahl für die Hersteller erleichtern, da eine höhere Wahrscheinlichkeit besteht, daß der von ihnen verabschiedete Standard sich im Markt durchsetzen wird<sup>256</sup>.

Ein förmlicher Standardisierungsprozeß birgt jedoch gegenüber der Standardsetzung im freien Markt nicht nur Vorteile in sich. Da Standardisierungsorganisationen die verschiedenen Interessen in Einklang miteinander bringen müssen, ist der Prozeß oft zeit- und kostenaufwendig

---

<sup>252</sup> Vgl. zum Ganzen *Grindley/Salant/Wavermann*, 3 Int. J. Com. L. & Pol'y, Web-Doc 2, 30f.

<sup>253</sup> *Maher*, 3 VA. J.L. & Tech. 5, Art. 5 Rdnr. 27.

<sup>254</sup> Siehe *Maher*, 3 VA. J.L. & Tech. 5, Art. 5 Rdnr. 28 und *Lemley*, 28 Conn. L. Rev. 1041, 1059.

<sup>255</sup> Siehe *Maher*, 3 VA. J.L. & Tech. 5, Art. 5 Rdnr. 28.

<sup>256</sup> Siehe *Maher*, 3 VA. J.L. & Tech. 5, Art. 5 Rdnr. 29.

und das Ergebnis wird kaum alle Teilnehmer befriedigen können. Einige Hürden, welche die Internetorganisationen überwinden müssen, sollen deshalb kurz erläutert werden<sup>257</sup>:

- Einigungsschwierigkeiten

Je größer die Bedeutung eines Standards für Gesellschaft und Wirtschaft ist, um so umfangreicher wird auch das Interesse an einer Teilnahme dieser Gesellschaftskreise am jeweiligen Standardisierungsprozeß sein. Durch die vielen einzubringenden Interessen wird sich das Erreichen einer Einigung entsprechend schwierig erweisen<sup>258</sup>. Auch nach einer Übereinkunft besteht das Risiko, daß viele Produzenten sich nicht an den vereinbarten Standard halten, sondern eigene Versionen bevorzugen<sup>259</sup>.

- Technologieüber- und Technologiefehlbewertung

Es besteht das Risiko, daß sich die Standardisierungsorganisationen nur auf die technischen Aspekte konzentrieren, wirtschaftliche jedoch außer Betracht lassen und damit die Nachfrage unberücksichtigt bleibt. Andererseits kann es dazu kommen, daß zuviel Wert auf das aktuell wirtschaftlich Machbare gelegt wird, und somit Standards produziert werden, welche bald von der technischen Entwicklung überholt sein könnten.

- Politischer Einfluß

In vielen Industriebereichen spielen Regierungsorganisationen eine große Rolle in der Koordination von Standardsetzungsorganisationen. Zum einen ist der Staat von vielen gesetzten Standards selbst betroffen. Zum anderen kann er potentielle Risikoquellen für den optimalen Standardisierungsprozeß abschwächen.

Die Teilnahme des Staates kann dabei auf verschiedene Weise erfolgen, zum Beispiel durch Finanzierung der Organisationen, durch unmittelbare Teilnahme am Diskussionsprozeß, durch Unterstützung bei der Koordination oder durch direkte Festlegung eines bestimmten Standards. Dies bildet zunächst einen Vorteil gegenüber der Standardisierung durch den Markt, da hier auch nichtwirtschaftliche Aspekte mit einbezogen werden können.

Andererseits könnten die fraglichen Körperschaften zu stark aktuelle politische Probleme mit in den Entscheidungsvorgang einbeziehen. Bei einer Überbetonung solcher Aspekte, kann dies zu völlig unwirtschaftlichen Standards führen, die vom Markt nicht akzeptiert werden. Darüber hinaus fehlt es häufig dem Staat am erforderlichen Wissen, welches für komplexe Regulierungen benötigt wird. Gleichzeitig wird aber die Illusion

---

<sup>257</sup> Siehe *Grindley/Salant/Wavermann*, 3 Int. J. Com. L. & Pol'y, Web-Doc 2, 31.

<sup>258</sup> Vgl. *Maher*, 3 VA. J.L. & Tech. 5, Art. 5 Rdnr. 40; *Cooter*, 23 SW. U.L. Rev. 443, 450.

<sup>259</sup> Zum Beispiel sind die Webbrowser von Netscape und Microsoft nicht fähig, alle Features des, durch das für das WWW zuständigen W3C, festgelegten Standards (siehe <http://www.w3.org/MarkUp>) für HTML zu verarbeiten. Zusätzlich bieten sie jedoch proprietäre Werkzeuge (z.B. ActiveX-Controls) zur Homepagegestaltung an.

hervorgerufen, daß der Staat dieses Wissen durch das entsprechende staatliche Verfahren erzeugen könne<sup>260</sup>.

- Wettbewerbsrechtliche Verzerrungen

Die letztgenannten zwei Effekte ließen sich vermeiden, wenn die Mitglieder der standardsetzenden Organisationen nur aus betroffenen Unternehmen bestehen würden. Diese würden kaum technische Aspekte betrachten, ohne deren wirtschaftliche Umsetzbarkeit in den Entscheidungsprozeß einfließen zu lassen. Politische Aspekte würden nur soweit in Standards einfließen, wie dies dem Absatz der Produkte förderlich sein würde.

Das Kartellrecht stellt allerdings für private Standardisierungsorganisationen einige Hürden auf. Diese Organisationen könnten als Mittel zur Bildung von Kartellen und zur Ermöglichung von wettbewerbsrechtlichen Absprachen im Sinne § 1 GWB, Art. 81 EGV, Section 1 Sherman Act angesehen werden. Nicht nur der Austausch von Preisen, auch die Absprache von produktsspezifischen Informationen kann wettbewerbsbeschränkende Auswirkungen haben<sup>261</sup> und somit im Sinne des Kartellrechts illegal sein. Die größten, in der jeweiligen Standardisierungsorganisation vertretenen Firmen könnten zusätzlich versuchen, ihre Interessen auf Kosten der kleineren Teilnehmer durchzusetzen<sup>262</sup> und ihre marktbeherrschende Stellung zu mißbrauchen, § 19 GWB, Art. 82 EGV, Section 2 Sherman Act. So könnten die Zugangsvoraussetzungen für die Organisationen, zum Beispiel durch entsprechende Mitgliedsgebühren, so hoch angesetzt werden, daß kleine Firmen von der Standardsetzung ausgeschlossen werden. Der Zugang zu den Standards wäre dann nur für zahlungskräftige Mitglieder eröffnet („closed standards“). Diese Zugangsbeschränkung käme folglich einem Gruppenboykott oder einem abgestimmten Verhalten in Form einer Verweigerung mit Konkurrenten zu handeln, gleich<sup>263</sup>.

Bevor eine vollständige Verurteilung der Standardisierungsorganisationen als wettbewerbsbehindernde Vereinigungen erfolgt, sollten folgende Punkte beachtet werden: Zum einen kann ein Informationsaustausch auch wettbewerbsfördernd sein, da er erst vielen verschiedenen Firmen ermöglicht, konkurrierende Produkte zu vermarkten, welche unter einem Standard kompatibel sind. Zum Teil wird es auch unmöglich sein, effektiv in Konkurrenzkampf zu treten, solange keine Standardisierung der Produkte

---

<sup>260</sup> Siehe *Ladeur*, CR 1999, 395, 396.

<sup>261</sup> Siehe die US-amerikanischen Entscheidungen: *U.S. District Court, District of Maryland* vom 18. November 1912, Standard Sanitary Mfg. Co. v. United States, 226 U.S. 20; *U.S. District Court, Western District of Tennessee* vom 19. Dezember 1921, American Column & Lumber Co. v. United States, 257 U.S. 377; *Court of Appeals, Hasting* vom 13. April 1965, National Macaroni Mfrs. Ass'n v. FTC, 345 F.2d 421; *U.S. District Court, Middle District of North Carolina* vom 14. Januar 1969, United States v. Container Corp., 393 U.S. 333.

<sup>262</sup> Mit Beispielen siehe *Maher*, 3 VA. J.L. & Tech. 5, Art. 5 Rdnr. 34f. Vgl. auch *Crocker*, Standards, Kap. Comparison with other Efforts.

<sup>263</sup> *Lemley*, 28 Conn. L. Rev. 1041, 1083.

erfolgt ist. Eine Absprache verschiedener Firmen erscheint auch dann notwendig, wenn sich ohne die Standardisierung, nur ein Produkt marktweit durchsetzen würde und auf Grund der daraus resultierenden Monopolstellung ein Wettbewerb schließlich ebenfalls entfallen würde. Schließlich birgt die Standardisierung durch offene Standardisierungsgesellschaften, wie zum Beispiel die *Internet Engineering Task Force* (IETF), durch ihre freiwillige und offene Teilnahmemöglichkeit aller Marktteilnehmer, ein viel geringeres Risiko der einseitigen Ausnutzung des Standards durch verschiedene Marktkräfte<sup>264</sup>. Jedoch überwiegen dabei nicht immer die Vorteile der Standardisierung die Nachteile der Wettbewerbsbeschränkung.

- Patentstreitigkeiten

Die Standardsetzung durch private Industrieorganisationen eröffnet die Möglichkeit, daß sehr viele Marktteilnehmer Rückgriff auf den ausgehandelten Standard nehmen können, ohne hohe Lizenzgebühren an Inhaber von Patentrechten und sonstigen geistigem Eigentum zahlen zu müssen. Teilweise kommt es jedoch vor, daß Firmen, welche am Standardisierungsprozeß innerhalb einer Organisation beteiligt gewesen sind, versuchen, Lizenzgelder für Patente, die sie an Teilen des Standards besitzen, zu erlangen<sup>265</sup>. Eine solche Vorgehensweise führt einen organisierten Standardisierungsprozeß ad absurdum, da der Standard zumindest für die Teilnehmer frei verfügbar sein soll.

Um dies zu verhindern, werden verschiedene Vorgehensweisen diskutiert.

Zum einen könnte man das Patentrecht und das sonstige Recht des geistigen Eigentums dahingehend abwandeln, daß Firmen von der Durchsetzung ihrer Rechte ausgeschlossen sind, wenn sie ihre Erfindungen in offene Standards eingebracht haben<sup>266</sup> oder wenn sie eine dominante Marktposition erlangt haben<sup>267</sup>. Weiterhin könnte man die Standardsetzung im Rahmen eines Quasigesetzgebungsverfahrens mit Ausschluß der Patentrechte durch den Staat durchführen lassen oder die ausgehandelten Standards als verbindlich setzen<sup>268</sup>.

---

<sup>264</sup> Vgl. zum Ganzen *Lemley*, 28 Conn. L. Rev. 1041, 1081.

<sup>265</sup> Mit zwei Beispielen (Dell, Unisys), siehe *Lemley*, 28 Conn. L. Rev. 1041, 1086ff. Ein neues Beispiel stellt die Firma British Telecom dar, welche erst im Juni 2000 behauptete, ein US-Patent (mit der Nummer 4,873,662) auf die kleinen, anklickbaren Text- und Grafik-Bereiche in Web-Seiten, die zu weiteren Informationen, anderen Seiten oder Servern führen (die sogenannten Hyperlinks), zu besitzen. British Telecom versucht nun, für die Verwendung von Hyperlinks, auf welchen das WWW basiert, von US-amerikanischen Internetprovidern Patentgebühren zu erhalten. Vgl. *Heise-Newsticker*, Hyperlink-Patent: British Telecom macht ernst, 17. Dezember 2000. Auch die US-Firma Geoworks beruft sich auf eigene Patente, um von verschiedenen Internetbetreibern Patentgebühren für die Verwendung des erst 1999 veröffentlichten Standards für den Internetzugang mittels Mobiltelefonen (Wireless Application Protocol, WAP) zu verlangen. Vgl. *VNU Net, Gerald*, Wap patent 'owner' extends licence deadline, 7. Juni 2000.

<sup>266</sup> *Maher*, 3 VA. J.L. & Tech. 5, Art. 5 Rdnr. 29.

<sup>267</sup> Mit näheren Ausführungen hierzu siehe *Lemley*, 28 Conn. L. Rev. 1041, 1060.

<sup>268</sup> Einige Beispiele aus dem amerikanischen Raum werden in *Lemley*, 28 Conn. L. Rev. 1041, 1062f. erwähnt.

Standardisierungsorganisationen könnten allerdings in ihren Organisationsregeln die Rechte ihrer Mitglieder am geistigen Eigentum, welches in Standards verwendet wurde, einschränken<sup>269</sup>. Dies kann durch ein Verbot des Besitzes von Patenten und Urheberrechten auf Elemente von Standards erfolgen. Die Organisationen können auch die generelle Geltendmachung dieser Rechte gegen jeden Verwender des Standards oder zumindest eine Geltendmachung gegen die eigenen Mitglieder untersagen. Dieser quasi kostenfreien Lizenzierbarkeit steht in einigen Organisationen die Pflicht deren Mitglieder gegenüber, die Nutzung ihrer Patente zu vernünftigen und undiskriminierenden Bedingungen zu ermöglichen. Schließlich können Standardisierungsorganisationen von ihren Mitgliedern verlangen, daß diese ihre Patente offenlegen, so daß entschieden werden kann, welche Reichweite ein neuer Standard aufweisen soll.

- **Unflexibler Zeitplan**

Die Suche nach einem optimalen Vermarktungszeitpunkt zwingt viele Firmen einem flexiblen Zeitplan zu folgen. Organisationen sind häufig an einen festen Zeitplan gebunden und können nur eingeschränkt auf veränderte Marktsituationen reagieren. Im Falle von neuen Entdeckungen und Entwicklungen ist der Zeitplan häufig auf zu langer Sicht festgesetzt und Entscheidungen werden zu spät gefällt. Bei einer nicht vorhergesehenen Weiterentwicklung der Technik, könnte sich der Standard als obsolet und überholt erweisen. Andererseits kann die Entscheidung für einen Standard zuzeitig erfolgen, ohne daß eine preiswerte technische Umsetzung möglich ist.

Die voranschreitende Technologisierung unserer Umwelt erfordert immer neuere Standards, um die Interoperabilität von Vermittlungsstellen, Endgeräten oder Zubehör zu gewährleisten. Dabei werden die Zeiträume der einzelnen Entwicklungsschritte immer kürzer. Ebenso wird, durch die immer intensivere Verschmelzung der technischen Bereiche, die Notwendigkeit der Interoperabilität von zum Beispiel Computern, Telekommunikationsgeräten oder HiFi-Geräten immer ausgeprägter. Die Hauptaufgabe der Standardisierungsorganisationen wird in immer geringerem Maße die Vereinheitlichung von schon bestehenden Standards sein. Vielmehr erscheint es immer wichtiger, schon vor der entgültigen Entwicklung von Soft- und Hardwareprodukten Standards festzulegen<sup>270</sup>. Nur so kann verhindert werden, daß durch In-

---

<sup>269</sup> Vgl. mit näheren Ausführungen Lemley, 14 Berkeley Tech. L.J. 745, 752f. Die IETF schränkt z.B. in ihren Vertragsregeln, die Berufung auf Patente ihrer Mitglieder ein, wenn Standards durch die Gruppierung beschlossen wurde. *RFC 2026*, Bradner, Kap. 10.3.1.1.: „[...] However, to the extent that the submission is or may be subject to copyright, the contributor, the organization he represents (if any) and the owners of any proprietary rights in the contribution, grant an unlimited perpetual, non-exclusive, royalty-free, world-wide right and license to the ISOC and the IETF under any copyrights in the contribution. This license includes the right to copy, publish and distribute the contribution in any way, and to prepare derivative works that are based on or incorporate all or part of the contribution, the license to such derivative works to be of the same scope as the license of the original contribution.“

<sup>270</sup> Der Entwicklung von z.B. Webbrowsern für Mobiltelefone oder ähnlichen Anwendungen gingen lange Diskussionen über das sogenannte *Wireless Application Protocol* (WAP) voraus. Ebenso mußte der Nachfolgestan-

vestitionen in technische Sackgassen hohe Kosten entstehen. Inzwischen wird von Standardisierungsorganisationen ein Weitblick in die Zukunft gefordert, um die technischen Entwicklungen hervorzusehen; eine Aufgabe, die bislang den untereinander konkurrierenden Unternehmen zustand. Dies trifft besonders auf die Standardisierung der Internetkommunikation zu, welche globale Reichweite hat. Die starren Regelungsansätze der herkömmlichen Standardisierungsinstitute können unter der fortschreitenden Globalisierung, einem solchen Auftrag nicht mehr gerecht werden<sup>271</sup>. Neuere Ansätze gewähren einen stärkeren Rückgriff auf die Marktkräfte, welche sich gewöhnlich schneller ändernden Sachlagen anpassen können.

#### 2.4.1.2. Standardsetzende Organisationen im Internet

Wie oben aufgezeigt, können Standardisierungsorganisationen für die Entwicklung eines technischen Bereiches sehr bedeutsam sein. Entsprechend wurden die meisten Kommunikationsregeln im Internet durch solche Organisationen entworfen. Bevor auf nähere Probleme bei der Standardsetzung im Internet eingegangen wird, soll zunächst ein Überblick über die relevanten Organisationen geschaffen werden. Dabei kann zwischen zwei Gruppen unterschieden werden, den traditionellen und den modernen Organisationen. Zusätzlich existieren viele weitere Organisationen, die sich mit spezifischen Themen befassen und unabhängig arbeiten<sup>272</sup>.

##### 2.4.1.2.1. Traditionelle Organisationen

Zu der traditionellen Gruppe sind Organisationen mit langer Erfahrung in der Standardsetzung zu zählen, welche zusätzlich in der Internetstandardisierung involviert sind. Zu ihnen gehören folgende Verbände:

- ISO – *International Organization for Standardization*<sup>273</sup>

Die *International Organization for Standardization* (ISO) ist eine weltweite Vereinigung von Standardisierungsorganisationen von über 130 Staaten<sup>274</sup>. Die ISO ist eine nichtstaatliche Organisation, welche 1947 gegründet wurde und in Genf beheimatet ist. Sie entwickelt internationale Standards, welche den internationalen Austausch von Waren und Dienstleistungen erleichtern sollen und von den meisten Regierungen anerkannt sind. Die Arbeit der ISO resultiert in internationalen Verträgen, die als *Inter-*

---

dard für das *Internet Protocol* (IP), das *Internet Protocol v6* (Ipv6) erst genau spezifiziert werden, ehe man mit der Entwicklung und Einführung neuer Internetserver beginnen konnte; siehe *Ermert, c't 2000, Heft 1, 32f.*

<sup>271</sup> Siehe *Grindley/Salant/Wavermann, 3 Int. J. Com. L. & Pol'y, Web-Doc 2, 34.*

<sup>272</sup> Zum Beispiel beschäftigen sich die beiden Organisationen Secure Electronic Marketplace for Europe (SEMPER) und End to End Security (E2s) mit Sicherheitsaspekten bei der Internetübertragung von Daten. An der Standardisierung von Electronic Commerce Anwendungen sind viele weitere Organisationen beteiligt: z.B. Collision Industry Electronic Commerce Association (CIECA), Commerce Net (CN), Data Interchange Standards Association (DISA), European Initiative in Electronic Commerce (EIEC) und Financial Services Technology Consortium (FSTC).

<sup>273</sup> Die Webseite der ISO kann unter <http://www.iso.ch> eingesehen werden.

<sup>274</sup> Vgl. mit näheren Informationen: ISO, About ISO, <http://www.iso.ch/iso/en/aboutiso/introduction/index.html>.

*national Standards* publiziert werden. Viele ISO-Standards sind inzwischen weitverbreitet und geben der Industrie, dem Handel und den Verbrauchern klare Vorteile<sup>275</sup>.

Um dem schnellen Wachstum der Informationstechnologie gerecht zu werden, bildete die ISO zusammen mit der *International Electrotechnical Commission* (IEC) im Jahr 1987 das *ISO/IEC Joint Technical Committee 1* (JTC1). Das JTC1 arbeitet mit der *International Telecommunications Union* und anderen Verbänden zusammen, um Standards für die Informationstechnologie zu entwerfen. Dazu zählen Standards für die Netzwerktechnik, für Datenbanken, für Computersprachen, Hard- und Software.

Die ISO setzt sich aus ihren Mitgliedsorganisationen zusammen, welche in drei Kategorien unterteilt werden. Die *Member Bodies of ISO*<sup>276</sup> stellen den jeweils am repräsentativsten in der Standardsetzung eines Landes tätigen Verband dar. Nur eine Organisation je Land kann als ISO-Mitglied anerkannt werden<sup>277</sup>. Die Mitglieder haben das volle Teilnahme- und Stimmrecht in jedem technischen und politischen Komitee der ISO. Für Länder, welche keine voll entwickelte nationale Standardisierungsaktivitäten haben, steht die Möglichkeit offen, sogenannte *Correspondent Members* zu entsenden, welche keine aktive Rolle in der Entwicklungsarbeit einnehmen können. Länder mit nur gering entwickelter Ökonomie können eine sogenannte *Subscriber Membership* eingehen, um den Kontakt zur internationalen Standardisierung zu wahren.

Die technische Entwicklungsarbeit wird in einer Hierarchie von circa 2850 technischen Komitees, Unterkomitees und Arbeitsgruppen ausgeführt<sup>278</sup>. Diese Komitees setzen sich aus qualifizierten Personen der Industrie, der Wissenschaft, von Regierungen und Verbraucherverbänden zusammen. Das *Central Secretariat* in Genf ist für die Überwachung des Informationsflusses, für die Klärung von Streitigkeiten, für die Bearbeitung und Veröffentlichung der in den Komitees erreichten Vereinbarungen sowie für Koordination der Treffen der technischen Komitees zuständig.

Die technischen Komitees entwickeln die ISO-Standards nach den folgenden Prinzipien<sup>279</sup>:

- Konsens

Die Ansichten aller interessierten Parteien werden berücksichtigt (zum Bei-

---

<sup>275</sup> Als Beispiele sollen folgende wichtige Anwendungsbereiche genannt werden: das ISO 9000 für Qualitätsmanagement und Qualitätssicherheit, das ISO 14000 für Umweltmanagement, die sieben Grundeinheiten (m, kg, s, A, K, mol, cd) der internationalen Maßsysteme (Système international d’unités), die Papiergrößen und die ISO Codes für Ländernamen, Währungen und Sprachen.

<sup>276</sup> Siehe die Liste der Member Body der ISO unter <http://www.iso.ch/adresse/membodies.html>.

<sup>277</sup> Deutschland wird z.B. vom Deutschen Institut für Normung (DIN) vertreten.

<sup>278</sup> Siehe die Liste der technischen Komitees unter <http://www.iso.ch/meme/memento.html>.

<sup>279</sup> Siehe ISO, How are ISO standards developed?

- spiel Hersteller, Verkäufer, Nutzer, Konsumentengruppen, Testlabors, Regierungen, Forschungseinrichtungen)
- Globalisierung  
Globale Lösungen werden gefunden, um Industrie und Konsumenten weltweit zu befriedigen.
  - Freiwilligkeit  
Internationale Standardisierung wird vom Markt vorangetrieben und basiert deshalb auf einer freiwilligen Teilnahme aller Interessenten des Marktes.
- ITU – *International Telecommunications Union*<sup>280</sup>  
Mit ihrer Gründung 1865 durch die erste „*International Telegraph Conference*“ in Paris ist die *International Telecommunications Union* (ITU) die älteste Sonderorganisation der Vereinten Nationen<sup>281</sup> zur Regelung und Planung der weltweiten Telekommunikation. Die ITU nimmt unter anderem die Aufgabe der Frequenzzuteilung für die verschiedenen Fernmeldedienste (zum Beispiel Amateurfunk) wahr. Ihr Ziel ist die Erhaltung und der Ausbau der internationalen Zusammenarbeit auf dem Gebiet der Telekommunikation. Ihr Sitz ist in Genf. Neben 188 Mitgliedsstaaten können Repräsentanten von Wissenschafts- und Industrieorganisationen durch ein spezielles Verfahren an den ITU-Aktivitäten teilnehmen. Sie arbeiten gewöhnlich in verschiedenen *Study Groups* mit, in welche sie Forschungs- und Entwicklungsarbeit ihrer eigenen Institute einbringen<sup>282</sup>. Die zunehmende Privatisierung der Telekommunikation führte dabei zu einer immer stärkeren Rolle der privaten Organisationen innerhalb der ITU. Die relevanten Partner bei der Umsetzung der ITU-Regeln sind nicht mehr die einzelnen Nationen. Vor allem Netzbetreiber und Gerätehersteller (vor allem multinationale Konzerne) üben Druck zur Verabschiedung verbindlicher Rahmenregelungen aus<sup>283</sup>. Die letztendlich betroffenen privaten Unternehmen sehen ihre Interessen durch die Repräsentanten der Mitgliedsstaaten nicht ausreichend vertreten.  
Eine wichtige Rolle in der Standardisierung der Telekommunikation nimmt der ITU *Telecommunication Standardization Sector*<sup>284</sup> (ITU-T) wahr. Der ITU-T erfüllt hierbei den Zweck, die Standardisierung der Telekommunikation durch wissenschaftliche Untersuchungen sowie der Verabschiedung von Standardisierungsvorschlägen auf globaler Basis voranzutreiben. Eines der wichtigsten internetrelevanten Arbeitsbereiche der ITU-T stellt die notwendige Angleichung des Fernsprechverkehrs an die Kommunikation über das *Internet Protokoll* dar. Das explosive Wachstum des Internets und and-

---

<sup>280</sup> Siehe die WWW-Seite der ITU: <http://www.itu.int>. Zur Bedeutung der ITU: *White/Lauria* 32 Cal. W. L. Rev. 1, 1-3.

<sup>281</sup> *Noll*, MMR 1999, 465 gibt einen guten Überblick über die historische Entwicklung der ITU.

<sup>282</sup> Vgl. *Noll*, MMR 1999, 465, 467.

<sup>283</sup> Siehe *Sietmann*, c't 1999, Heft 9, 180, 183f.

<sup>284</sup> Siehe *ITU-T*, The ITU Telecommunication Standardization Sector, <http://www.itu.int/ITU-T/index.html>. Die Schwesternsektoren sind der Radiocommunication Sector (ITU-R) und der Telecommunications Development Secort (ITU-D).

rer auf dem *Internet Protokoll* basierender Netzwerke führt zu einem Überdenken herkömmlicher Konzepte der verschiedenen Kommunikationsmöglichkeiten. Besonders im Bereich Ecommerce ist die Verwendung des Internets und deren Applikationen ein wichtiger Faktor für die Entwicklung von Telekommunikationsnetzwerken geworden. So bilden der digitale Telefondienst über das Internet sowie der Zugriff von Mobilfunkgeräten auf das Internet eine große Herausforderung für die nächsten Jahre<sup>285</sup>.

Der ITU-T arbeitet nicht getrennt von den einzelnen Internetorganisationen, sondern in umfassender Zusammenarbeit mit der wichtigen und noch zu erläuternden *Internet Engineering Task Force* (IETF) zusammen. Weder die IETF noch die ITU-T sind voneinander unabhängig in der Lage die anstehenden Probleme zu lösen. Durch eine Zusammenarbeit können die Stärken beider Organisationen optimal ausgenutzt werden. So besitzt die IETF einen enormen Wissensvorsprung in der Erarbeitung von Protokollen und Anwendungen, während die ITU-T ihr beträchtliches Wissen in der Netzwerkarchitektur und Netzwerkentwicklung beisteuern kann.

- **ANSI – American National Standards Institute**<sup>286</sup>

Das *American National Standards Institute* (ANSI) ist der Verwalter und Koordinator des freiwilligen Standardisierungssystems der USA<sup>287</sup>. Es wurde 1918 durch fünf Ingenieursvereinigungen und drei staatlichen Behörden als privatrechtliche gemeinnützige Organisation gegründet. ANSI wird von einer hohen Anzahl von Firmen, privaten Verbänden und staatlichen Behörden unterstützt. Es hat seinen Sitz in Washington, D.C. und ihr Büro in New York City.

Das ANSI entwickelt selbst keine Standards, sondern unterstützt die Konsensbildung bei der Entwicklungsarbeit von entsprechend qualifizierten Gruppen und erkennt die Ergebnisse als *American National Standards* (ANSs) an. Dabei sorgt es dafür, daß die Hauptprinzipien Konsens, faires Verfahren und Offenheit durch die akkreditierten Verbände eingehalten werden. Weiterhin fördert es die Verbreitung der ANSs auf internationaler Ebene und ermutigt die Anwendung von internationalen Standards auf der Ebene der USA. Zu diesem Zweck ist die ANSI der alleinige US-amerikanische Repräsentant in der ISO<sup>288</sup>.

---

<sup>285</sup> Weiterführende Dokumente zur Anwendung der IP-Technologie in der Telekommunikationsbranche können unter *ITU-T*, Internet Protocol (IP) Documents, <http://www.itu.int/ITU-T/studygroups/com13/ip/index.html> gefunden werden.

<sup>286</sup> Siehe die WWW-Seite des ANSI: <http://www.ansi.org>.

<sup>287</sup> Vgl. die weiteren Angaben unter *ANSI*, About ANSI, <http://web.ansi.org/public/about.html>.

<sup>288</sup> Vgl. die weitergehenden Ausführungen unter *ANSI*, International Standardization, [http://web.ansi.org/public/ansi\\_info/ansi\\_iso.html](http://web.ansi.org/public/ansi_info/ansi_iso.html).

- ETSI – *European Telecommunications Standards Institute*<sup>289</sup>

Das *European Telecommunications Standards Institute* (ETSI) ist eine gemeinnützige Organisation, welche als Ziel die Entwicklung von langlebigen europäischen und internationalen Telekommunikationsstandards hat<sup>290</sup>. Es hat seinen Sitz im Technologiezentrum Sophia Antipolis im südlichen Frankreich. Die ETSI setzt sich aus fast 800 Mitgliedern aus über 50 Ländern zusammen und repräsentiert damit Produzenten, Serviceprovider, Netzwerkbetreiber, Forschungseinrichtungen und Endnutzer. Es steht jeglichem europäischen Verband offen, welcher an der Unterstützung von Telekommunikationsstandards interessiert ist. Bei der Standardentwicklung wird insbesondere auf die Bedürfnisse der Mitglieder eingegangen, um auf die Anforderungen eines schnell wachsenden Marktes reagieren zu können.

Auf Grund der freiwilligen Standards besteht jedoch keine Verpflichtung der Mitgliedsverbände die Ergebnisse umzusetzen. Gleichwohl dienen einige Standards der ETSI als technische Grundlage für die Regulierungsbestrebungen der *Europäischen Kommission*.

ETSI fördert die Entwicklung und Anwendung von weltweiten Standards. Zu diesem Zweck wird die Arbeit mit weiteren internationalen Standardsetzungsorganisationen, insbesondere der ITU, abgestimmt.

Neben den erwähnten Organisationen existieren noch eine Reihe weiterer Verbände, die für die Standardsetzung im Internet relevant sind. Dazu zählen neben vielen anderen<sup>291</sup> die *European Computer Manufacturers Association*<sup>292</sup> (ECMA) in Genf, das *Institute for Electrical and Electronics Engineers*<sup>293</sup> (IEEE) in New Jersey oder die *Object Management Group*<sup>294</sup> (OMG) aus Framingham, Massachusetts.

#### 2.4.1.2.2. Moderne Organisationen

Aus der dezentralisierten Natur des Internets lässt sich nicht schließen, daß es sich auf unkoordinierte Weise entwickelt hat. Besonders im Bereich der technischen Steuerung und Standardisierung hat sich im Laufe der Entwicklung des Internets eine verwirrende Anzahl von Organisationen gebildet. Diese sichern die Stabilität und die Weiterentwicklung des Internets. Entweder widmen sie sich der Entwicklung von neuen Standards oder nehmen organisatorische Aufgaben wahr. Die folgende Aufstellung soll einen Überblick über die wichtigsten Organisationen geben. Eine vollständige Aufzählung ist auf Grund der sich ständig weiter entwickelnden Struktur nicht möglich und für den Zweck dieser Arbeit nicht erforderlich.

---

<sup>289</sup> Siehe die WWW-Seite der ETSI: <http://www.etsi.org>.

<sup>290</sup> Vgl. ETSI, About ETSI, <http://www.etsi.org/aboutetsi/aboutetsi.htm>.

<sup>291</sup> Das World Standards Services Network gibt einen umfangreichen Überblick über die nationalen und internationalen Standardisierungsorganisationen: <http://www.wssn.net>.

<sup>292</sup> Siehe European Computer Manufacturers Association, <http://www.ecma.ch>.

<sup>293</sup> Siehe Institute for Electrical and Electronics Engineers, <http://www.ieee.org>.

<sup>294</sup> Siehe Object Management Group, <http://www.omg.org>.

- **IETF – Internet Engineering Task Force**

Das wichtigste Organ für die Standardsetzung ist die *Internet Engineering Task Force*<sup>295</sup> (IETF). Sie ist eine offene internationale Gemeinschaft von Netzwerkspezialisten, Internetprovidern, Geschäftsleuten und Wissenschaftlern, die sich mit der Entwicklung der Internetarchitektur und der Internetnutzung auseinandersetzen. Sie wurde im Jahre 1989 von dem *Internet Activities Board* gegründet<sup>296</sup> und ist seitdem die bedeutendste Körperschaft, die sich mit der Entwicklung und Verbesserung von neuen internetspezifischen Standards auseinandersetzt. Sie wird traditionell von hochqualifizierten und unabhängigen Freiwilligen betrieben. Strukturiert in *Working Groups* tauschen diese Ingenieure Ideen und Erfahrungen aus und versuchen durch Diskussionen (über Email und direkte Treffen) einen Konsens zu erreichen. Umgesetzt in Computerprogrammen werden ihre Ideen getestet und als Internetstandards verabschiedet.

Die Aufgaben der IETF werden im *Tao of IETF*<sup>297</sup> ausführlich definiert:

- Identifying, and proposing solutions to, pressing operational and technical problems in the Internet;
- Specifying the development or usage of protocols and the near-term architecture to solve such technical problems for the Internet;
- Making recommendations to the Internet Engineering Steering Group (IESG) regarding the standardization of protocols and protocol usage in the Internet;
- Facilitating technology transfer from the Internet Research Task Force (IRTF) to the wider Internet community; and
- Providing a forum for the exchange of information within the Internet community between vendors, users, researchers, agency contractors and network managers.

Die IETF ist derzeit in acht verschiedene Bereiche (*Areas*) mit unterschiedlichen Forschungsschwerpunkten unterteilt. Diese sind Anwendungen, Internet, Netzwerkmanagement, operationale Voraussetzungen, Routing, Sicherheit, Transport und Nutzerservice<sup>298</sup>. Jeder Bereich hat ein oder zwei Bereichsdirektoren (*Area Directors*). Sie werden durch ein Nominierungskomitee (*Nomcom*) gewählt, welches den Vorsitzenden der IETF bestimmt<sup>299</sup>. Diese Bereichsdirektoren, zusammen mit dem IETF-Chair bilden die *Internet Engineering Steering Group* (IESG).

---

<sup>295</sup> Die IETF ist im Internet unter [www.ietf.org](http://www.ietf.org) zu finden.

<sup>296</sup> Kurzer geschichtlicher Abriss sowie Informationen über die Organisationsstruktur der IETF in Crocker, Standards, Kap. The IETF Standards Process.

<sup>297</sup> RFC 3160, Harris, Kap. 1. What is the IETF?

<sup>298</sup> RFC 3160, Harris, Kap. 1.2.2 IESG; RFC 2028, Hovey, Kap. 3.2 IETF Working Groups; RFC 2418, Bradner, Kap. 1. Introduction.

<sup>299</sup> Der Nominierungsprozeß wird ausführlich im RFC 2727, Galvin beschrieben.

Jeder Bereich besteht wiederum aus verschiedenen Arbeitsgemeinschaften (*Working Groups*). Eine solche *Working Group* setzt sich aus einer Anzahl von Personen zusammen, die gemeinsam an einem durch eine Satzung festgelegtem Problem arbeiten (siehe weiter unten). Dabei kann das Ziel dieser Zusammenarbeit im Entwurf eines bestimmten Netzwerkprotokolls oder in der Lösung eines bestimmten Problems bezüglich des Internets liegen.

Die einzelnen *Areas* können eine *Birds of a Feather* (BOF) Session abhalten<sup>300</sup>. Eine BOF ist eine Zusammenkunft während eines IETF-Treffens<sup>301</sup>, die eine Marktuntersuchung und eine Art technisches „Brainstorming“ erlaubt. Sie ähnelt den *Working Groups*, hat jedoch keine Satzung und die teilnehmenden Personen treffen sich gewöhnlich nur ein- oder zweimal. Eine Session wird zum Beispiel häufig abgehalten, um einzuschätzen, ob genügend Interesse an der Bildung einer neuen Arbeitsgemeinschaft besteht. Eine BOF kann gleichfalls als ein Forum für eine alleinige Präsentation oder Diskussion dienen, ohne die Absicht eine Arbeitsgemeinschaft zu gründen. Jede Person kann bei einem relevanten Bereichsdirektor die Genehmigung für die Abhaltung einer BOF einholen.

Die verwaltungstechnischen Aufgaben, welche für die Aktivitäten der IETF notwendig sind, werden durch ein Sekretariat wahrgenommen<sup>302</sup>. Dieses besteht aus dem *Executive Director* und seinen Angestellten. Der *Executive Director* ist der Anlaufpunkt für alle Belange, welche den Internet-Standardsetzungsprozeß betreffen. Er ist für die Protokollierung der Standardsetzung zuständig.

Die wichtigsten technischen Aktivitäten der IETF finden in den schon erwähnten *Working Groups* statt. Zur Zeit beherbergt die IETF mehr als 100 dieser Gruppen. Die Mehrzahl der Arbeitsgemeinschaften konzentriert sich auf die Lösung aktueller Probleme, mit der Folge, daß sie nur eine begrenzte Zeit bestehen bleiben. Mit Erfüllung ihrer spezifischen Aufgabe werden sie gewöhnlich geschlossen. Die einzelnen Arbeitsgemeinschaften sind wiederum entsprechend ihrem Thema zu verschiedenen Bereichen zusammengefaßt und stehen unter der Leitung eines *Area Directors*.

Die IETF ermöglicht keine direkte Mitgliedschaft<sup>303</sup>. Jeder kann sich registrieren und an den dreimal im Jahr stattfindenden Treffen teilnehmen. Am nächsten einer Mitgliedschaft kommt jedoch die Teilnahme an den Diskussionen mittels der verschiedenen Mailinglisten, welche durch die einzelnen Arbeitsgruppen betrieben werden. Zum Teil wird auch die Technik der Videokonferenz eingesetzt, um die einzelnen entfernten Teilnehmer zusammenzuführen. Die Teilnahme an den *Working Groups* ist grund-

---

<sup>300</sup> RFC 3160, Harris, Kap. 4. BOF.

<sup>301</sup> RFC 2418, Bradner, Kap. 2.4. Birds of a Feather (BOF).

<sup>302</sup> RFC 2028, Hovey, Kap. 3.3. IETF Secretariat.

<sup>303</sup> RFC 3260, Harris, Kap. What is the IETF?

sätzlich für jeden offen. Darüber hinaus sind die einzelnen Gruppen jedoch autonom und bestimmen die einzelnen Details ihrer Arbeitsweise selbst. Die Hauptregel der Arbeitsweise ist, daß die Anerkennung der einzelnen Entscheidungen durch einen „*rough consensus*“ erfolgt<sup>304</sup>. Damit Streitigkeiten um geistige Eigentumsrechte nicht den fairen und offenen Prozeß der Standardsetzung unterminieren, müssen die einzelnen Teilnehmer jegliche ihnen diesbezüglich bekannten Rechte dem Vorsitzen der jeweiligen Arbeitsgruppe bekannt geben<sup>305</sup>.

Eine neue *Working Group* kann auf Initiative eines *Area Directors* oder durch einzelne potentielle Teilnehmer gegründet werden. Dazu muß jeder, der eine Arbeitsgruppe initiieren möchte, die Zustimmung des entsprechenden *Area Directors* erhalten, in dessen Bereich die neue Gruppe fallen würde. Um zu bestimmen, ob es angebracht ist, eine neue Arbeitsgruppe zu gründen, haben die entsprechenden *Area Directors* verschiedene Punkte zu beachten<sup>306</sup>. Unter anderem muß das Thema der zu konstituierenden Gruppe eindeutig und relevant für die Internet-Gemeinschaft sein. Ebenso muß das Ziel mit vernünftigem Aufwand und in einem angemessenen Zeitraum erreichbar sein. Weiterhin benötigt jede Gruppe eine Satzung, welche hauptsächlich zwischen voraussichtlichen Vorsitzenden und dem relevanten *Area Director* ausgehandelt wird. Die endgültige Zustimmung gibt jedoch die IESG.

Der Vorsitzende jeder *Working Group* hat auf ein Voranschreiten des Standardsetzungsprozesses sowie auf Fairneß und Offenheit zu achten. Er muß sicherstellen, daß die einzelnen Aufgaben korrekt erfüllt werden. Er hat das Recht für die Gruppe Entscheidungen zu treffen, soweit sie mit den allgemeinen Regeln der IETF übereinstimmen<sup>307</sup>.

Die bereits schon erwähnten Mailinglisten der Arbeitsgruppen sind mit der IETF-Hauptmailingliste die zentralen Diskussionsmittel für die IETF-Aktivitäten. In der IETF werden jedoch eine große Anzahl weiterer Listen betrieben, in denen langfristig anstehende Probleme diskutiert werden. Um die wiederholte Diskussion einzelner Themen zu vermeiden, werden die meisten Diskussionslisten archiviert.

- **IESG – Internet Engineering Steering Group**

Die *Internet Engineering Steering Group*<sup>308</sup> (IESG) ist für das Management der technischen Aktivitäten der IETF verantwortlich<sup>309</sup>. Sie hat den Standardsetzungsprozeß

---

<sup>304</sup> RFC 2028, Hovey, Kap. 3.2. IETF Working Groups, RFC 2418, Kap. 3. Working Group Operation.

<sup>305</sup> RFC 2028, Hovey, Kap. 3.2. IETF Working Groups.

<sup>306</sup> RFC 2418, Bradner, Kap. 2.1. Criteria for formation.

<sup>307</sup> RFC 2418, Bradner, Kap. 6.1. WG Chair.

<sup>308</sup> Die IESG ist im Internet unter <http://www.ietf.org/iesg.html> zu finden.

<sup>309</sup> RFC 3160, Harris, Kap. 1.2.2 IESG; RFC 2028, Hovey, Kap. 3.5 Internet Engineering Steering Group.

<sup>310</sup> RFC 2026, Bradner.

<sup>311</sup> Vgl.: RFC 2418, Bradner, Kap. 8. Review of documents.

entsprechend der im RFC 2026<sup>310</sup> festgelegten Regeln zu überwachen. Sie nimmt entsprechende Aktionen vor, die sich während der Standardsetzung ergeben. Dazu ist die Anerkennung neuer *Working Groups* und die endgültige Verabschiedung von Internet-Standards zu zählen.

Die IESG überprüft alle Dokumente, welche als *Request for Comments* (RFC) veröffentlicht werden sollen. Im Gegensatz zu informellen und experimentellen Dokumenten werden potentielle RFCs, welche einen Standard beschreiben, einer gründlichen Untersuchung unterzogen. Die Entscheidungen der IESG reichen von der kritiklosen Annahme über konstruktive Kritik des Inhalts bis zur grundsätzlichen Ablehnung der vorgeschlagenen RFCs<sup>311</sup>. Gegen diese Entscheidung kann, nach dem im RFC 2026 bestimmten Verfahren, Beschwerde eingelegt werden.

Die IESG besteht aus den acht *Area Directors* und dem *Chair* der IETF. Die Wahl dieser Personen erfolgt in der Weise, wie sie oben bei der IETF geschildert wurde<sup>312</sup>.

- **IRTF – Internet Research Task Force**

Die *Internet Research Task Force*<sup>313</sup> (IRTF) ist nicht direkt in den Standardsetzungsprozeß im Internet eingegliedert. Vielmehr beschäftigt sie sich mit Themen, welche zu unsicher, zu fortgeschritten oder noch ungenügend erforscht sind, um Objekte der Standardsetzung zu sein. Ihre Tätigkeit ist auf langfristige Themen ausgerichtet<sup>314</sup>. Die IRTF will über verschiedene Organisationen hinweg die Zusammenarbeit fördern, um in wichtigen Bereichen des Internets eine intensive Forschung und Entwicklung zu ermöglichen. Sie setzt sich wie die IETF aus mehreren Forschungsgruppen (*Research Groups*) zusammen. Struktur und Organisation der IRTF ist jedoch bedeutend weniger formal und durchorganisiert, wie in der IETF. Die Teilnahme an der Diskussion erfolgt auch hier, wie in der IETF, als Individuum anstatt als Organisation.

Die IRTF setzt keine Standards. Die Ergebnisse der *Research Groups* bilden eher die Grundlage für theoretische Artikel, White Papers oder informelle RFCs. Weiterhin können sie in die Arbeit von IETF-Arbeitsgruppen Eingang finden, obgleich sie keine größere Gewichtung als Ideen anderer Personen entfalten<sup>315</sup>.

---

<sup>312</sup> Siehe RFC 2727, Galvin.

<sup>313</sup> Die IRTF ist im Internet unter <http://www.irtf.org> zu finden.

<sup>314</sup> RFC 2028, Hovey, Kap. 3.8 Internet Research Task Force; RFC 2014, Weinrib, Kap. 1. Introduction, 1.1. IRTF approach.

<sup>315</sup> RFC 2014, 1.1. IRTF approach.

<sup>316</sup> RFC 2028, Hovey, Kap. 3.8 Internet Research Task Force; RFC 2014, Weinrib, Kap. 1. Introduction.

Die IRTF wird von ihrem *Chair* geleitet und von der *Internet Research Steering Group* (IRSG) überwacht, welche sich aus den Vorsitzenden der einzelnen Arbeitsgruppen sowie dem Vorsitzenden der IRTF und möglichen weiteren Personen (*Members at large*) zusammensetzt<sup>316</sup>.

Der *Chair* der IRTF wird von dem IAB ernannt. Die Vorsitzenden der *Research Groups* werden im Zuge der Gründung neuer Gruppen ernannt. Die IRSG-*Members at large* werden durch den Vorsitzenden der IRTF ausgesucht und von der IAB zugelassen. Der *Chair* der IRTF ist dafür verantwortlich, daß die *Research Groups* entsprechend ihren Forschungsschwerpunkten koordinierte, konsistente und mit der Entwicklung der Internetarchitektur im Zusammenhang stehende Ergebnisse in vertretbarer Zeit veröffentlichen<sup>317</sup>.

Die Aktivitäten der IRTF laufen hauptsächlich in den einzelnen Forschungsgruppen ab. In diesen Gruppen werden Themen in Bezug zu Internetprotokollen, zu Anwendungen und zur Internetarchitektur diskutiert. Die *Research Groups* können für jeden offen oder nur für einen bestimmten Personenkreis zugänglich sein<sup>318</sup>. Dies steht im Kontrast zu der generellen Offenheit der Arbeitsgruppen der IETF. Die Eingrenzung der Mitgliedschaft kann für den Zusammenhalt der Arbeitsgruppen auf langer Basis vorteilhaft sein und die Forschungstätigkeit unterstützen. Aber sie darf nur mit Vorsicht eingeschränkt werden, um eine Fragmentierung der Arbeit innerhalb der Forschungsgemeinschaft zu verhindern.

Alle Forschungsgruppen müssen regelmäßig über den Fortschritt ihrer Arbeit berichten und sind angehalten, offene Treffen zu veranstalten. Eine Gruppe kann auf Initiative jeglicher Person gegründet werden<sup>319</sup>. Dazu muß zunächst eine Satzung zuzüglich einer Liste der Gründungsmitglieder der vorgeschlagenen Gruppe an den Vorsitzenden der IRTF übermittelt werden. Die Satzung wird dann von der IRSG und dem IAB überprüft, ob die neue *Research Group* für die Entwicklung des Internets relevant ist und genügend personelle Unterstützung erhält, um signifikante Ergebnisse zu erarbeiten. Die einzelnen Forschungsgruppen sind völlig unabhängig und bestimmen den größten Teil ihrer Arbeitsweise selbst. Da die Ergebnisse der *Research Groups* keine Internetstandards sondern Forschungsergebnisse darstellen, ist ein Konsens nicht erforderlich<sup>320</sup>, stellt jedoch eine hohe Qualität der Forschungs- und Zusammenarbeit dar.

Die Überwachung der Forschungstätigkeit übernimmt der *Chair* der jeweiligen Forschungsgruppe. Dabei hat er ein weites Ermessen, wie er seine Forschungsgruppe leit-

---

<sup>317</sup> RFC 2014, Weinrib, Kap. 5.1. IRTF Chair.

<sup>318</sup> Vgl. zum ganzen RFC 2014, Weinrib, Kap. 1.1. IRTF approach.

<sup>319</sup> Vgl. zum ganzen RFC 2014, Weinrib, Kap. 2. Research Group Formation.

<sup>320</sup> Siehe RFC 2014, Weinrib, Kap. 3. Research Group Operation.

tet, solange er sicherstellt, daß eine Anzahl an Aufgaben erfüllt wird. Dazu gehören folgende Punkte<sup>321</sup>:

- Ensuring the Research Group process and content management
- Moderate the Research Group email list
- Organize, prepare and chair face-to-face and on-line formal meetings
- Communicate results of meetings
- Distribute the work
- Document development
- Document publication

Die Arbeit der Forschungsgruppen führt schließlich zur Veröffentlichung eines Forschungsberichtes, welcher auch als informeller oder experimenteller RFC publiziert werden kann. Dieses Dokument kann von einem Gruppenmitglied oder auch von mehreren Forschern, beziehungsweise einem ernannten Editor entworfen werden.

- **IRSG – Internet Research Steering Group**

Die *Internet Research Steering Group* (IRSG) ist das Managementkomitee der IRTF. Ebenso wie die IRTF ist die Arbeit der IRSG von einer starken Informalität geprägt. Das Ziel ist die Forschungstätigkeiten zu unterstützen und zu verstärken, ohne durch unnötige Bürokratie gebremst zu werden. Sie setzt sich aus den Vorsitzenden der einzelnen Arbeitsgruppen der IRTF sowie dem *Chair* der IRTF zusammen.

Sie ist verantwortlich, dem IRTF-Vorsitzenden bei der Gründung neuer Forschungsgruppen und anderen Angelegenheiten zu beratschlagen und somit eine reibungslose Forschungstätigkeit zu ermöglichen<sup>322</sup>.

- **IANA – Internet Assigned Numbers Authority**

Viele Protokollspezifikationen des Internets beinhalten Nummern, Schlüsselwörter und andere Parameter, welche einheitlich zugewiesen und verwendet werden müssen. Dazu sind zum Beispiel Versions-, Protokoll- und Portnummern zu zählen. Die einzelnen Arbeitsgruppen der IETF hatten nicht die Autorität, diese Werte den von ihnen entwickelten Protokollen zuzuweisen. Um eine einheitliche Numerierung über die verschiedenen Protokolle und Anwendungsbereiche hinweg zu gewährleisten, sollte diese durch eine eigenständige Anlaufstelle vorgenommen werden. Die Wahrnehmung dieser Aufgabe erfolgt durch die *Internet Assigned Numbers Authority*<sup>323</sup> (IANA)<sup>324</sup>. IANAs Autorität innerhalb der Internetgemeinde beruht größtenteils auf ihrer jahrelangen Verwaltungstätigkeit des DNS. Die Internetgemeinde respektiert die IANA und

---

<sup>321</sup> Siehe *RFC 2014*, Weinrib, Kap. 5.3. Research Group Chair.

<sup>322</sup> Vgl. *RFC 2014*, Weinrib, Kap. 5.2. IRSG Member.

<sup>323</sup> Die IANA ist im Internet unter <http://www.iana.org> zu finden.

<sup>324</sup> *US-GAO*, Report, S. 5; *RFC 2028*, Hovey, Kap. 3.7 Internet Assigned Numbers Authority; *RFC 2360*, Scott, Kap. IANA Considerations; vgl. auch <http://www.iana.org>.

im Gegenzug profitiert sie von einem stabilen System der Verwaltung der Internetadressen.

Die Funktion der IANA kann durch ein oder mehrere Individuen oder durch eine Organisation erfolgen. Die IANA ist somit entgegen geläufiger Meinung keine rechtlich eigenständige Einrichtung<sup>325</sup>. Ins Leben gerufen wurde die IANA durch das *US Federal Network Council* (FNC)<sup>326</sup> und die *Internet Society* (ISOC)<sup>327</sup>. Die IANA war zunächst als funktionale Abteilung der *High-Performance Computing and Communications Division* des *Information Sciences Institute*<sup>328</sup> (ISI) an der *University of Southern California*<sup>329</sup> (USC) beheimatet<sup>330</sup> und wurde zu 90% durch die *Defense Advanced Research Projects Agency* (DARPA) finanziert<sup>331</sup>. Seit ihrer Gründung nahm sie als wichtigste Aufgabe die Zuweisung der numerischen Internetadressen (IP-Nummern) und die Kontrolle sowie das Management der internationalen TLDs wahr<sup>332</sup>. Sie stellt damit die Spitze der Pyramide im DNS dar.

In den Anfangszeiten des Internets überwachte Dr. Jon Postel, einer der wichtigsten Internetpioniere<sup>333</sup> (am 16. Oktober 1998 verstorben), die Zuweisung der Internetnummern und -namen. Er veröffentlichte kontinuierlich eine Liste der technischen Parameter, welche von ihm für die Verwendung in Protokollen zugewiesen wurden (jeweils als RFC unter dem Namen „Assigned Numbers“). Heutzutage wird die Funktion der IANA durch die ICANN wahrgenommen. Die ICANN erhielt das Recht die IANA zu leiten durch eine Reihe von Verträgen mit dem US-DoC, die im Kapitel 3.1.3.1 erörtert werden. Auch die IETF erkannte am 1. März 2000 die ICANN als neues Dach der IANA mittels eines *Memorandum of Understanding Concerning the Technical Work of the Internet Assigned Numbers Authority*<sup>334</sup> an.

---

<sup>325</sup> Siehe *Gordon*, Controlling the Internet, Kap. 3.2.; ebenda auch näheres zur Finanzierung der IANA.

<sup>326</sup> Das FNC bestand aus Vertretern 16 verschiedener US-amerikanischer Bundesbüros. Das FNC war für die Koordination und Finanzierung dem Internet zugehörender Organisationen zuständig. Zu diesen gehörte unter anderem das IETF Sekretariat, das Computer Emergency Response Team (1988 durch die DARPA in Folge des Auftretens eines Internetwurmes gegründet) und am bedeutsamsten die IANA. Näheres zum FNC siehe *ITRD*, Archiv – FNC Material, <http://www.itrd.gov/archive/fnc-material.html> und Background Materials, [http://www.itrd.gov/fnc/fnc\\_background.html](http://www.itrd.gov/fnc/fnc_background.html).

<sup>327</sup> Siehe *Bettinger*, GRUR Int. 1997, 402, 404ff. sowie *Gordon*, Controlling the Internet, Kap. 3.1.

<sup>328</sup> Siehe <http://www.isi.edu>.

<sup>329</sup> Siehe <http://www.usc.edu>.

<sup>330</sup> Vgl.: *Goldfoot*, 84 Va. L. Rev. 909, 913; *Wenning*, JurPC Web-Doc 31/1998, Abs. 2.

<sup>331</sup> Vgl. *Gigante*, 15 J. Marshall J. Computer & Info. L. 413, 416.

<sup>332</sup> Vgl. *RFC 1591*, Postel.

<sup>333</sup> Dr. Jon Postel baute 1969 mit weiteren graduierten Studenten der University of California das erste experimentelle Computernetzwerk - das ARPANet. Während der nächsten zehn Jahre half Postel, das Internet Protocol und das Domain Name System zu entwickeln. Er überwachte die Entwicklung des Internets und konnte sich des Respekts der Internetgemeinde sicher sein. Zum Gedenken an Dr. Jon Postel siehe <http://www.postel.org>.

<sup>334</sup> Zur Anerkennung der ICANN siehe das IETF-ICANN Memorandum of Understanding Concerning the Technical Work of the Internet Assigned Numbers Authority, *RFC 2860*, Carpenter/Baker/Roberts.

- **RFC-Editor**

Die *Requests for Comments*<sup>335</sup> (RFC), eine Publikationsserie, wird durch einen *Editor* verwaltet. Dieser ist zum einen für die technische Ausführung, zum anderen jedoch für die Aufrechterhaltung des traditionell hohen technischen und editoriellen Standards verantwortlich<sup>336</sup>. Der *RFC-Editor* kann aus einem oder mehreren Personen bestehen. Er untersteht dem IAB.

- **IAB – Internet Architecture Board**

Das *Internet Architecture Board*<sup>337</sup> (IAB) überwacht die Architektur des Internets und ihrer Protokolle und dient während des Standardsetzungsprozesses als Richter, welcher bei Entscheidungen der IESG angerufen werden kann<sup>338</sup>. Es ist eine Organisation der ISOC, mit der Aufgabe technische Beratungen durchzuführen. Das IAB ernennt den IETF-*Chair* und ist für die Genehmigung weiterer IESG-Kandidaten, die durch das IETF-*Nomcom* vorgeschlagen werden, zuständig. Das IAB ist aus dem *Internet Activities Board* hervorgegangen, das 1983 gegründet wurde<sup>339</sup>. Im Gegensatz zur IETF ist das IAB keine Organisation, welche Standards entwickelt, vielmehr fällt ihm eine unterstützende Rolle im Standardsetzungsprozeß zu.

Als Überwachungsorgan im Standardsetzungsprozeß nimmt das IAB eine Reihe von Aufgaben wahr<sup>340</sup>. Das IAB überprüft die von der IETF nominierten *Chairs*. Es überwacht die Architektur der Protokolle und Verfahren und die Entwicklung der Standards, welche im Internet genutzt werden. Das IAB dient als Berufungsinstanz für Beschwerden über Verfahrensfehler. Der RFC-Editor untersteht dem IAB. Es wirkt bei der Bestimmung der Organisation mit, die als IANA auftreten soll. Darüber hinaus berät es das *Board of Trustees* der ISOC in technischen und verfahrensmäßigen Fragen.

Das IAB wird insbesondere in der langfristigen Planung und Koordinierung der verschiedenen Bereiche der IETF-Aktivitäten tätig<sup>341</sup>. Es hat die Entwicklung verschiedener langfristiger Themen zu überwachen, die besonders im Internet eine wichtige Rolle spielen. Dabei hat es sicherzustellen, daß die entsprechenden Gruppen über die für sie wichtigen Themen informiert werden.

Die anstehenden Aktivitäten der IETF und der *BoF-Sessions* werden besonders von den Mitgliedern des IAB beachtet. Dabei wird die IESG in der Bewertung solcher Ak-

---

<sup>335</sup> Der RFC-Editor ist im Internet unter <http://www.rfc-editor.org> zu finden.

<sup>336</sup> Siehe *RFC 2028*, Hovey, Kap. 2.1 The Request for Comments Editor.

<sup>337</sup> Das IAB ist im Internet unter <http://www.iab.org> zu finden.

<sup>338</sup> *RFC 3160*, Harris, Kap. 1.2.3 IAB; *RFC 2028*, Hovey, Kap. 3.6 Internet Architecture Board.

<sup>339</sup> Einen guten Überblick über das damalige Internet Activities Board und eine kurze Geschichte wird vom *RFC 1160*, Cerf gegeben.

<sup>340</sup> Vgl. zum Ganzen: *RFC 2850*, IAB, Kap. 2. The Role of the IAB.

<sup>341</sup> *RFC 2850*, IAB, Kap. 2.1 Architectural oversight in more detail.

tivitäten unterstützt und ihr bei der Entscheidung mitgeholfen, ob ein Thema einer Gruppe der IETF oder der IRTF zuzuordnen ist. Das IAB überprüft die Satzungen der neu zu gründenden Arbeitsgruppen der IETF und reicht entsprechende Ratschläge an die IESG weiter.

Die IRTF wird von dem IAB finanziert und organisiert. Dazu bestimmt das IAB den Vorsitzenden der IRTF für die Dauer von jeweils zwei Jahren<sup>342</sup>. Ebenso wie bei der IETF werden für die IRTF neu vorgeschlagene Gruppierungen durch das IAB einer näheren Prüfung unterzogen.

Das IAB besteht aus dreizehn Vollmitgliedern, welche sich aus zwölf gewählten Personen und dem *Chair* der IETF/IESG zusammensetzen<sup>343</sup>. Der *Chair* der IETF/IESG ist jedoch von der Ernennung weiterer IESG-Mitglieder und von Streitschlichtungsverfahren gegen IESG-Entscheidungen ausgeschlossen. Die Mitglieder des IAB treten als Privatpersonen auf und können nicht als Vertreter von Firmen oder anderen Organisationen agieren.

Die einzelnen Mitglieder werden entsprechend der *Nomcom*-Regeln<sup>344</sup> für die Dauer von zwei Jahren nominiert und eingesetzt. Die Mitgliedschaft muß durch das *Board of Trustees* der ISOC anerkannt werden.

Die Mitglieder wählen eine Person von ihnen als *Chair* des IAB aus<sup>345</sup>. Er hat die Aufgabe, die Aktivitäten und die Treffen des IAB zu leiten. Er wird für die Dauer von einem Jahr gewählt. Eine Wiederwahl ist nicht ausgeschlossen. Mit der Mehrheit von zwei Dritteln der Mitglieder des IAB kann der Vorsitzende wieder abgewählt werden. Der *Chair* des IAB wählt einen *Executive Director* für die Dauern von einem Jahr aus. Diese Person verwaltet die internen Belange des IAB, zum Beispiel die Organisation der Treffen und die entsprechende Berichterstattung.

Das IAB versucht seine Entscheidungen während persönlichen Treffen, Telefon- oder Internetkonferenzen zu treffen<sup>346</sup>. Sollte dies nicht möglich sein, so werden vom Vorsitzenden inoffizielle Umfragen durchgeführt, um einen Konsens zu erreichen. Entscheidungen können getroffen werden, wenn mindestens sieben Mitglieder mit höchsten zwei gegenteiligen Stimmen zustimmen.

Von allen Treffen des IAB werden im Internet Protokolle veröffentlicht. Zusätzlich werden öffentliche Konferenzen bei jedem IETF-Treffen abgehalten. Um einen öffent-

---

<sup>342</sup> *RFC 2850*, IAB, Kap. 3.3 Selection of the IRTF chair.

<sup>343</sup> *RFC 2850*, IAB, Kap. 1. IAB Membership.

<sup>344</sup> Siehe *RFC 2027*, Galvin. Um eine kontinuierliche Arbeit zu ermöglichen werden gewöhnlich jedes Jahr nur sechs Mitglieder gewählt.

<sup>345</sup> *RFC 2850*, IAB, Kap. 3.1 IAB Chair.

lichen Prozeß zu gewährleisten, werden alle Ergebnisse als RFCs oder in Mailinglisten publiziert.

Zwischen der IETF und dem IAB besteht eine enge Zusammenarbeit (vgl. auch Abbildung 2 unten). Beide Organisationen haben Abgeordnete, welche als Vermittlungspersonen in der jeweils anderen Organisation auftreten. Das IAB ernennt den Vorsitzenden der IETF sowie alle weiteren Mitglieder der IESG entsprechend einer vom *Nomination Committee* vorgeschlagenen Liste. Dem *Board of Trustees* (BoT) der ISOC dient das IAB als Ratgeber in technischen und architektonischen Details des Internets. An den Tagungen selbst nehmen zusätzlich Vertreter der IANA und des *RFC-Editors* sowie der Vorsitzende der IRTF teil.

Schließlich bestehen auch nach Außen über die IETF Verbindungen zu verschiedenen standardsetzenden Organisationen, wie zur ISO-IEC/JTC1 oder zur ITU-T (siehe Kapitel 2.4.1.2.1 oben).

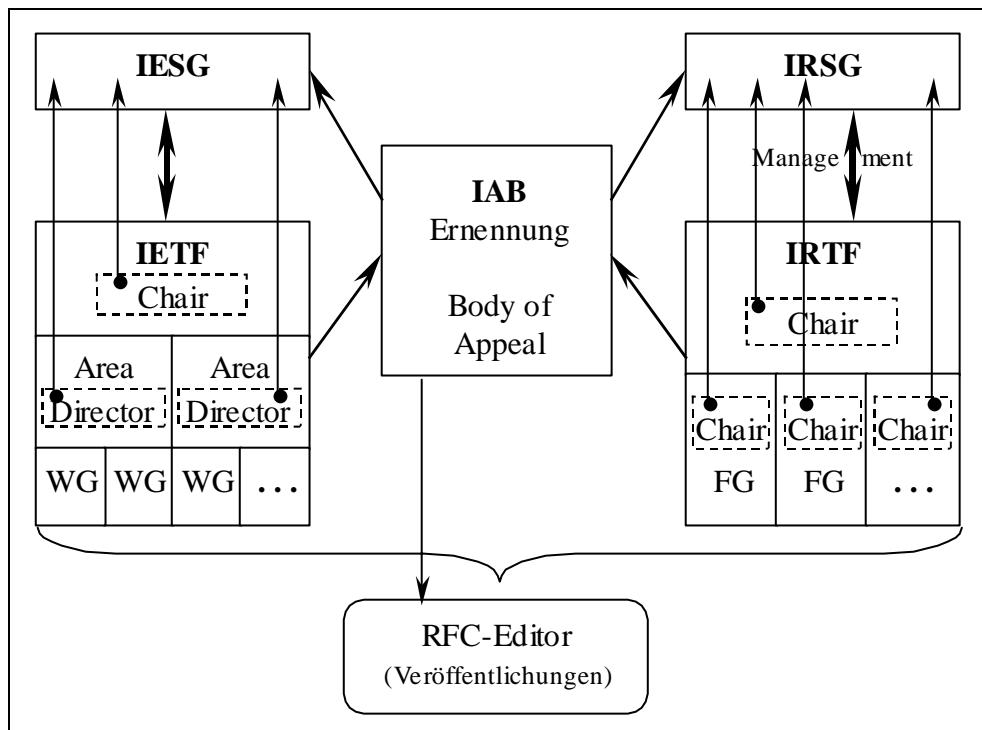


Abbildung 2 – Verhältnis des IAB zu den untergeordneten Organisationen.

- **ISOC – Internet Society**

Die *Internet Society*<sup>347</sup> (ISOC) wurde 1992 als gemeinnützige Vereinigung in Washington, D.C. gegründet, um die globale Kooperation und Kommunikation über das

<sup>346</sup> Näheres zu den Treffen des IAB während der Veranstaltungen der IETF/IESG siehe Conexions, Now what the meetings really like?

<sup>347</sup> Die ISOC ist im Internet unter <http://www.isoc.org> zu finden.

## 2.4. Verwaltung des Internet

---

Internet zu fördern und voranzutreiben<sup>348</sup>. Besonders im amerikanischen Raum wird die ISOC gern als Dachorganisation des Internets gesehen (vgl. Abbildung 3 unten), obwohl sie erst viel später als die bisher genannten Organisationen entstanden ist<sup>349</sup>.

Als internationale Organisation ist sie mit der Entwicklung des Internets betraut<sup>350</sup>. Dabei betrachtet sie soziale, politische und technische Themen. Da Anfang der 90er-Jahre keine Organisation bestand, welche das „Internet“ auf internationaler Ebene vertreten konnte, sollte die ISOC diese Aufgabe übernehmen. Insbesondere im Bereich der Telekommunikation, der durch etablierte Organisationen wie die ITU oder die ISO repräsentiert wurde, war ein Ansprechpartner nötig<sup>351</sup> (vgl. Abbildung 3 unten). Mit der Internationalisierung und Privatisierung des Internets sah zusätzlich die US-amerikanische Regierung keine Notwendigkeit mehr, finanzielle und organisatorische Unterstützung den verschiedenen Organisationen zu gewähren. Die ISOC sollte deshalb sicherstellen, daß neue und dauerhafte Finanzierungsmöglichkeiten gefunden werden<sup>352</sup>.

---

<sup>348</sup> Vgl.: *RFC 2134*, ISOC-BoT, Kap. 3.: „The purpose or purposes for which the corporation is organized are as follows: [...] To exercise all the powers conferred upon corporations formed under the District of Columbia Non-Profit Corporation Act in order to accomplish the corporation’s educational, charitable and scientific purposes; and to take other actions necessary or convenient to effect any or all of the purposes for which the corporation is organized“; auch unter <http://www.isoc.org/isoc/general/trustees/incorp.shtml> zu finden. Siehe auch ISOC, Frequently Asked Questions: What ist the Internet Society?, <http://www.isoc.org/whatis/what-is-isoc.html> und *RFC 3160*, Harris, Kap. 1.2.1 ISOC.

<sup>349</sup> Siehe z.B. *Gigante*, J. Marshall J. Computer & Info. L. 413, 418.

<sup>350</sup> *RFC 2028*, Hovey, Kap. 3.4 Internet Society.

<sup>351</sup> Vgl. *Werle/Leib*, The Internet Society, S. 8.

<sup>352</sup> Vgl. *Werle/Leib*, The Internet Society, S. 12.

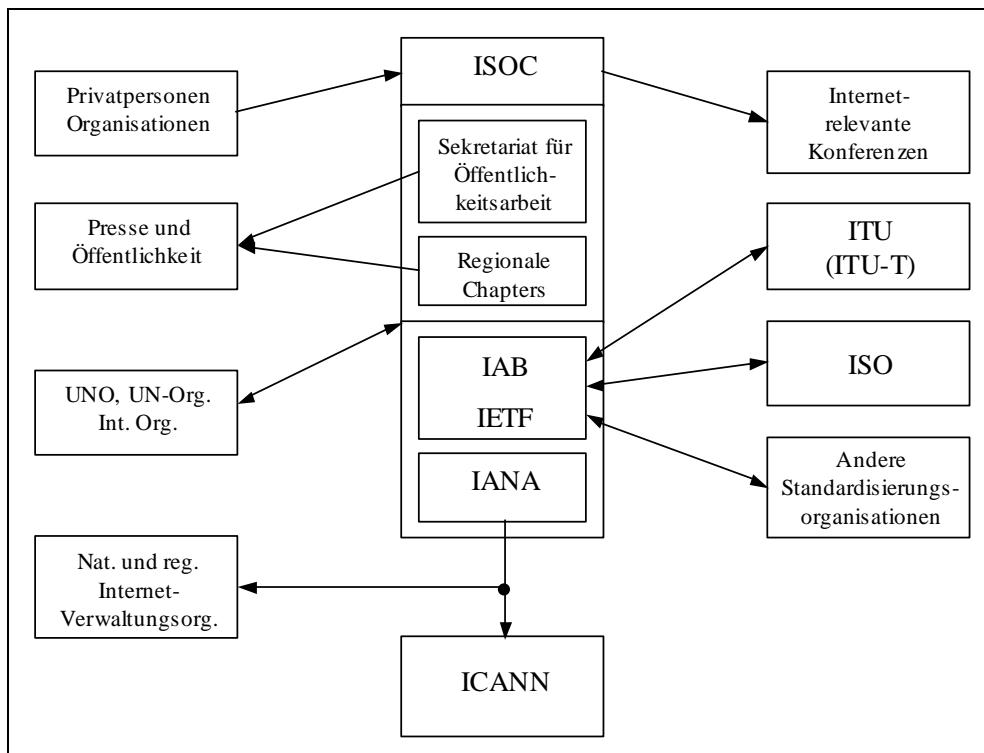


Abbildung 3 – Externe Verbindungen der ISOC.

Privatpersonen und Organisationen, wie zum Beispiel Unternehmen, Behörden oder Vereinigungen, können Mitglied der ISOC werden. Sie wird von dem *Board of Trustees* (BoT) geleitet. Das BoT ist seit 1995 für die Verabschiedung von Regeln für den Standardsetzungsprozeß<sup>353</sup> im Internet verantwortlich.

Näheren Aufschluß, welchem Zweck die ISOC dienen soll, geben die „*Articles of Incorporation of Internet Society*“<sup>354</sup>:

To be a non-profit corporation (without capital stock), which shall be operated exclusively for educational, charitable and scientific purposes. Such educational, charitable, and scientific purposes shall include carrying on activities:

- A. To facilitate and support the technical evolution of the Internet as a research and education infrastructure, and to stimulate the involvement of the scientific community, industry, government and others in the evolution of the Internet;
  - B. To educate the scientific community, industry and the public at large concerning the technology, use and application of the Internet;

<sup>353</sup> Siehe Kap. 2.4.1.3.

<sup>354</sup> *RFC 2134*, ISOC-BoT, Kap. 3. The purpose or purposes for which the corporation is organized are as follows.

C. To promote educational applications of Internet technology for the benefit of government, colleges and universities, industry, and the public at large;

D. To provide a forum for exploration of new Internet applications, and to stimulate collaboration among organizations in their operational use of the global Internet.

Mit der Expansion des Internets und der gewachsenen Bedeutung von Internetstandards ging gleichzeitig ein Wachstum der IETF einher. Mit dem Zuwachs der Verantwortung für die IETF mußte der Standardsetzungsprozeß stärker strukturiert werden, da untechnische Themen, wie rechtliche Streitigkeiten oder Öffentlichkeitsarbeit und Lobbyismus, vermehrt in die Arbeit einflossen. Hätte sich die IETF mit diesen Themen selbst beschäftigen müssen, so wäre sie im großen Umfang von ihrer technischen Arbeit ferngehalten worden. Sie konnte diese Problembereiche jedoch auch nicht ignorieren, da sie entweder durch andere Organisationen verdrängt oder durch Rechtsstreitigkeit stark beeinträchtigt worden wäre<sup>355</sup>.

Mitte 1995 wurde deshalb die *Poised95 Working Group* in Leben gerufen, welche versuchen sollte, den IETF-Prozeß neu zu strukturieren, um den Forschern der IETF maximale Flexibilität und Freiheit in der bisher erfolgreichen Weise zu gewährleisten<sup>356</sup>. Als wichtigstes Ergebnis empfahl die *Poised95 Working Group*, alle untechnischen Belange auf eine verwandte Organisation und zwar auf die ISOC zu übertragen. Im Dezember 1995 wurde dieser Vorschlag dann von der IETF angenommen.

Die IETF blieb für die Entwicklung der Internetstandards weiter verantwortlich. Die ISOC sollte keinen direkten Einfluß auf diesen Prozeß erlangen. Die ISOC gewährt ihr jedoch einen rechtlichen Schutz, um ihre Arbeit und die entwickelten Standards zu schützen. Der rechtliche Rahmen umfaßt nach dem Ergebnisreport der *Poised95 Working Group* dabei folgende Punkte<sup>357</sup>:

- legal insurance for all IETF officers (IAB, IESG, Nomcom and WG chairs);
- legal protection of the RFC series of documents; In such a way that these documents can be freely (i.e. no restrictions financially or otherwise) distributed, copied etc. but cannot be altered or misused. And that the right to change the document lies with the IETF.
- legal protection in case of Intellectual property rights disputes over Internet Standards or parts thereof.

---

<sup>355</sup> *RFC 2031*, Huizer, Kap. Security considerations.

<sup>356</sup> Vgl. zum Ganzen *RFC 2031*, Huizer, Kap. Introduction. Das Verhältnis der ISOC zur IETF vor Dezember 1995 sowie ein geschichtlicher Überblick wird in Cerf, IETF and ISOC erläutert.

<sup>357</sup> Entnommen aus *RFC 2031*, Huizer, Kap. The legal umbrella.

Die IETF wird zusätzlich von der ISOC in der Benennung der *Nomcom Chairs* und der IAB-Kandidaten unterstützt und dient als letzte Rechtsinstanz bei Streitigkeiten im Standardsetzungsprozeß<sup>358</sup>.

Geleitet und verwaltet wird die ISOC von dem *Board of Trustees* (BoT) und diversen Verwaltungspersonal (*Chair*, *Vice-Chair*, *President/CEO*, *Secretary*, *Treasury*<sup>359</sup>). Das BoT besteht aus höchstens zwanzig Treuhändern, welche jeweils für die Dauer von drei Jahren im Amt sind<sup>360</sup>. Mit Ausnahme des Präsidenten werden alle Treuhänder von den regulären Mitgliedern der ISOC gewählt. Das BoT kann jedoch einen Treuhänder ernennen, um mit ihm eine freie Stelle, welche durch den Ausfall eines Treuhänders entstanden ist, aufzufüllen. Die Treuhänder nehmen ihre Position als Ehrenamt wahr, so daß sie für ihre Tätigkeit keinen Lohn erhalten. Sie leiten die Geschäfte der ISOC, wobei sie sich mindestens einmal jährlich treffen. Bei Entscheidungen reicht dabei die einfache Mehrheit der abstimgenden Mitglieder aus, soweit die ISOC-Satzung<sup>361</sup> nicht ein anderes bestimmt. Entscheidungen, die ohne Treffen erfolgen, müssen jedoch im schriftlich erteilten einstimmigen Konsens erfolgen. Zur Wahrung der Öffentlichkeit werden alle Treffen und Entscheidungen protokolliert und können bei der ISOC eingesehen werden.

Mit Ausnahme des Präsidenten, wird das Verwaltungspersonal für den Zeitraum von einem Jahr vom BoT gewählt<sup>362</sup>. Der *Chair* wird aus den Mitgliedern des BoT gewählt. Dieser wiederum ernennt den Präsidenten, welcher von der Mehrheit des BoT anerkannt werden muß. Der *Chair* hat die volle Autorität die ISOC nach Außen zu vertreten oder auf verschiedenen Treffen, bei denen die ISOC stimmberechtigt ist, für sie abzustimmen. Der Präsident übernimmt als Chef der Verwaltung die laufenden Geschäfte der ISOC. Er unterliegt dabei der Direktion des BoT, welches auch seine Vergütung bestimmt. Die anderen Verwaltungsposten werden jedoch nicht vergütet.

Das *Advisory Council* ist das Organ, welches die Mitgliedsorganisationen der ISOC repräsentiert und das BoT berät<sup>363</sup>. Jede Organisation kann einen Repräsentanten und einen Vertreter für das *Advisory Council* bestimmen. Praktisch spielte bislang dieses Organ der ISOC keine aktive Rolle, so daß es nicht mit dem BoT vergleichbar ist.

---

<sup>358</sup> Siehe *RFC 2031*, Huizer, Kap. The standards process role.

<sup>359</sup> Siehe die aktuelle Liste der ISOC-Officers: *ISOC*, Officers, <http://www.isoc.org/isoc/general/officers>.

<sup>360</sup> Nähere Ausführungen zum Board of Trustees können in der Satzung, *RFC 2135*, ISOC-BoT, Article II - Board of Trustees nachgelesen werden.

<sup>361</sup> Siehe *RFC 2135*, ISOC-BoT, Fn. 360.

<sup>362</sup> Vgl. die Ausführungen zum Verwaltungspersonal in *RFC 2135*, ISOC-BoT, Article IV - Officers.

<sup>363</sup> Siehe die Satzung des Advisory Council vom 24. November 1998 unter: *ISOC*, ISOC Advisory Council Documents, <http://www.isoc.org/orgs/iacdocs.shtml>.

Mitglieder der ISOC können Organisationen und Einzelpersonen werden<sup>364</sup>. Der Beitragssatz für Organisationen beträgt mindestens 10.000 US\$, beziehungsweise für gemeinnützige Organisationen die Hälfte. Einzelpersonen haben als Unterstützung für die ISOC 35 US\$ (beziehungsweise einen Studententarif) zu zahlen. Die Mitglieder treffen sich unregelmäßig zu den vom BoT festgelegten Terminen. Diese zweigeteilte Mitgliedschaftsstruktur führt jedoch in der ISOC zu einem internen Mißverhältnis<sup>365</sup>. Die Einzelpersonen haben das Recht, das BoT zu wählen, während den Organisationen das Recht zusteht, einen Repräsentanten in das *Advisory Council* zu entsenden. Die Einzelpersonen haben folglich durch die Wahl die direkte Möglichkeit, über die Politik der ISOC zu entscheiden. Im Gegensatz dazu stehen den Organisationen durch die nur beratende Funktion des *Advisory Council's* kaum Einflußchancen offen.

Nicht nur auf internationaler Ebene versucht die ISOC zu agieren. Vielmehr haben sich auch auf regionaler und nationaler Ebene verschiedene *Regional Chapters* gebildet, welche auf ihrer Ebene die gleichen Ziele wie die ISOC verfolgen. Zum Beispiel ging das deutsche *Chapter* der ISOC<sup>366</sup> (ISOC.DE) 1995 aus der *Deutschen Interessen-Gemeinschaft Internet* (DIGI e.V.) hervor. Die DIGI e.V. wurde 1992 zeitgleich mit der ISOC gegründet, um die Ausbreitung des Internets in Deutschland zu fördern<sup>367</sup>. Zum Beispiel wurde durch sie das *Deutsche Network Information Center* DENIC zur Verwaltung der TLD .de eingerichtet. Die ISOC.DE veranstaltet kontinuierlich technische und politische Diskussionen über die Fortentwicklung des Internets in Deutschland.

Obgleich nicht jedes Mitglied der ISOC einem regionalen *Chapter* zugeordnet werden kann, sind alle Mitglieder eines *Chapters* gleichzeitig Mitglieder der ISOC. Die ISOC tritt zwar als Dachorganisation auf, die *Chapter* können aber ihre Ziele selbst bestimmen und somit auf lokale Zwecke ausrichten<sup>368</sup>. Um als regionale Gruppierung der ISOC auftreten zu können, muß eine Anerkennung durch das BoT erfolgen.

Zur Zeit existieren über 60 *Chapters*, die verschiedene Aufgaben erfüllen. Sie nehmen auf die nationale Politik Einfluß, stellen den Internetbetrieb sicher oder richten Serviceangebote an ihre Mitglieder. Auch die regionalen Zielgruppen sind nicht näher bestimmt. Während für Deutschland die ISOC.DE allein auftritt, existieren für Spanien sogar mehrere Organisationen<sup>369</sup>. Die Genfer Gruppe ist wiederum auf die Mitgliedschaft von verschiedenen internationalen Organisationen (ITU, WHO, CERN,

---

<sup>364</sup> Eine ausführliche Erklärung der Mitgliedschaft gibt die Satzung der ISOC, *RFC 2135*, ISOC-BoT, Article V - Members; auch unter <http://www.isoc.org/isoc/general/trustees/bylaws.shtml> zu finden.

<sup>365</sup> Vgl. *Werle/Leib*, The Internet Society, S. 14.

<sup>366</sup> Siehe die Internetseite <http://www.isoc.de>. Näheres zur Organisation und Mitgliedschaft kann in der Satzung der ISOC.DE vom 9. November 1998 nachgelesen werden, <http://www.isoc.de/verein/satzung/>.

<sup>367</sup> Siehe *Birkenbihl*, ISOC.DE Backgrounder.

<sup>368</sup> Siehe *Werle/Leib*, The Internet Society, S. 14.

<sup>369</sup> Siehe die Liste der ISOC-Chapters unter [http://www.isoc.org/isoc/chapters/ch\\_active.php](http://www.isoc.org/isoc/chapters/ch_active.php).

UNCTAD, etc.) ausgerichtet und möchte das Internet besonders in Entwicklungsländern verbreiten<sup>370</sup>. Es existiert somit keine klare Kompetenzverteilung zwischen den *Chapters* und der ISOC, ein Wettbewerb zwischen den Organisationen bleibt nicht ausgeschlossen. Diese schlecht definierte interne Struktur führt unweigerlich zu einer Schwächung der ISOC und verhindert eine Bündelung der verschiedenen Kräfte um gemeinsam die gewünschten Ziele zu erreichen.<sup>371</sup>

Um eine Angleichung der verschiedenen Standards innerhalb der Telekommunikationsindustrie zu erreichen, vereinbarten die ITU-T und die ISOC/IETF auf dem TSAG-Treffen vom September 1998 in Genf, verstärkt miteinander zu arbeiten, um den neuen Herausforderung der Verbindung von Telekommunikation und Internet zu begegnen und doppelte Forschungsarbeit bei beiden Organisationen zu vermeiden<sup>372</sup>. Um dies zu realisieren, sind die einzelnen Arbeitsgruppen beider Organisationen angehalten, mögliche Gebiete der Zusammenarbeit herauszufinden und näher zu bestimmen sowie Delegierte in die jeweils andere Organisation zu entsenden und gegenseitig Arbeitspapiere auszutauschen. Die ISOC wurde mit Abschluß dieser Vereinbarung ihrem Auftrag gerecht, als Vertreter der Internetorganisationen nach außen aufzutreten.

Weniger erfolgreich war die Einflußnahme der ISOC auf die Restrukturierung des DNS (siehe ausführlich hierzu Kapitel 3.1.2.3 unten). Zunächst initiierte die ISOC das *International Ad Hoc Committee* (IAHC), um die Möglichkeiten einer neuen Verwaltung des DNS näher zu untersuchen. Nach Abschluß der Arbeit wurde ein *Memorandum of Understanding* (MoU) von mehr als 200 Organisationen verabschiedet und die Verwaltung des DNS sollte auf ein neues System übertragen werden. Obgleich die ISOC eine führende Rolle in der Konstruktion dieses neuen Systems übernommen hatte, konnte sie nicht die Bedenken der US-amerikanischen Regierung ausräumen, die sich besonders gegen die Teilnahme von UN-Organisationen richtete. Um sich aus der Verwaltung des DNS zurückzuziehen, entwickelte die Regierung der USA deshalb eigene Pläne, welche eine völlige Ignoranz des bislang durch die ISOC und des IAHC Geleisteten darstellten<sup>373</sup>. Obwohl die ISOC an den folgenden Diskussionen teilnahm, war ihr weiterer Einfluß auf die Gründung der ICANN sehr gering. Als die US-Regierung in die Arbeit der ISOC intervenierte, war diese nicht stark genug, die internationale Debatte in Richtung des ursprünglichen Verwaltungsmodells zu lenken<sup>374</sup>. Dieses Versagen zeigt, daß die ISOC es auch zukünftig schwer haben wird, sich gegenüber mächtigeren Organisationen und Regierungen durchzusetzen.

---

<sup>370</sup> Vgl. *Werle/Leib*, The Internet Society, S. 15.

<sup>371</sup> Vgl. auch *Werle/Leib*, The Internet Society, S. 16.

<sup>372</sup> Vgl. hierzu *RFC 2436*, Brett/Bradner/Parsons zur Zusammenarbeit von ITU-T und ISOC/IETF.

<sup>373</sup> In dem zunächst veröffentlichten Green Paper (siehe Kap. 3.1.2.4) wurde das IAHC nicht einmal erwähnt.

<sup>374</sup> Vgl. zum Ganzen ausführlich: *Werle/Leib*, The Internet Society, S. 18ff., insbesondere S. 20.

- **ICANN – Internet Corporation for Assigned Names and Numbers**

Die inzwischen weltweit bedeutendste Organisation für die Verwaltung des Internets stellt die *Internet Corporation for Assigned Names and Numbers* dar. Sie wurde als Reaktion auf das *White Paper*<sup>375</sup> des *U.S. Department of Commerce* vom Juni 1998 als privatrechtliche gemeinnützige Organisation gegründet. Sie wird häufig als die zukünftige Internetregierung betrachtet. Zu ihren eigentlichen Aufgaben sind jedoch die Vergabe der IP-Adressen und Protokollspezifikationen sowie die Verwaltung des DNS zu zählen. Da der ICANN, insbesondere ihrer Bedeutung und Entwicklung ein eigenes Kapitel gewidmet wurde (siehe Kapitel 3 unten), soll an dieser Stelle keine weitere Erörterung erfolgen.

- **W3C – World Wide Web Consortium**

Eine weitere Standardisierungsorganisation des Internets ist das *World Wide Web Consortium*<sup>376</sup> (W3C). Diese Organisation ist unabhängig von den Organisationen der ISOC. Sie wurde 1994 von Tim Berners-Lee<sup>377</sup> am *Massachusetts Institute of Technology* (MIT) in Zusammenarbeit mit dem CERN, mit Unterstützung durch die DARPA und durch die Europäische Kommission gegründet, um für das *World Wide Web* allgemein gültige Protokolle zu entwickeln<sup>378</sup>. Das W3C ist eine gemeinnützige internationale Körperschaft, welche aus Firmen, Forschungseinrichtungen, Universitäten und weiteren Organisationen besteht.

Die Mission des W3C ist die Evolution des WWW als eine der wichtigsten Anwendungen des Internets voranzutreiben. Die Arbeit des W3C richtet sich dabei auf drei Hauptziele<sup>379</sup>. Erstens will es durch die Förderung von Interoperabilität und durch die Ermutigung zur offenen Diskussion die Entwicklung des Webs vorantreiben. Zweitens sollen so viele Nutzer wie möglich Zugriff auf das WWW erlangen. Die zugrundeliegende Technologie soll dabei die großen Unterschiede in der Kultur, der Bildung, des Könnens aber auch der materiellen Ressourcen und physikalischen Beschränkungen der Nutzer mit in Betracht ziehen. Drittens soll die Entwicklung des WWWs im Einklang mit neuen rechtlichen, wirtschaftlichen oder sozialen Problematiken erfolgen.

An der Verwirklichung seiner Visionen von einem „universal information space“<sup>380</sup> arbeiten Hunderte von Forschern und Ingenieuren nicht nur vom W3C-Team, sondern auch von den einzelnen Mitgliedsorganisationen sowie von der Internetgemeinschaft. Das W3C entwickelt Webtechnologien in denen existierende und Ideen von zukünfti-

---

<sup>375</sup> US-DoC, NTIA, White Paper, 63 Fed. Reg. 31741ff.

<sup>376</sup> Das W3C ist im Internet unter <http://www.w3.org> zu finden.

<sup>377</sup> Tim Berners-Lee ist der Erfinder des WWW. Näheres zu ihm ist unter <http://www.w3.org/People/Berners-Lee/> zu finden.

<sup>378</sup> Vgl. W3C, About the World Wide Web Consortium, Kap. Background, <http://www.w3.org/Consortium/>.

<sup>379</sup> Siehe W3C, WWW Consortium Process Document, Kap. 1.2 W3C's mission.

<sup>380</sup> Siehe W3C, About the World Wide Web Consortium, Kap. W3C's Role, Fn. 378.

gen Technologien verschmelzen. Das Ziel ist es diese durch Spezifikationen oder *Recommendations*, die für alle Internetnutzer frei zugänglich sind, zu standardisieren.

Das W3C ist in drei Schichten aufgebaut. Die wichtigste Ebene bilden die einzelnen Mitglieder, welche durch ihr Investment und ihre Mitarbeit in den *W3C Activities* (siehe unten) die Forschungsrichtungen des Konsortiums näher bestimmen. Die zweite Ebene bildet das sogenannte *Team*, das für den laufenden Betrieb und die laufende Forschungsarbeit des Gremiums sorgt. Die *Offices*<sup>381</sup> bilden die dritte Ebene. Sie beraten potentielle Mitglieder aus den verschiedenen Regionen der Welt, sorgen für eine Verbreitung der Ziele des W3Cs und liefern eine entsprechende Rückantwort von den verschiedenen nationalen Einheiten. Öffentlich tritt das W3C besonders durch Workshops, Symposien und Konferenzen auf.

Um die Mission, das WWW für alle zugänglich zu machen, sucht das W3C Mitglieder von der ganzen Welt, darunter Händler, Produzenten, Serviceanbieter, Forschungslabors, Standardisierungsorganisationen oder Regierungsbehörden. Im Gegensatz zur IETF können jedoch nur Organisationen der W3C beitreten, welche wiederum Personen in die einzelnen Gremien senden können. Mitglieder haben einen Sitz im *Advisory Committee*, das Recht an den *W3C Activities* teilzunehmen und damit die strategische Ausrichtung des W3Cs zu bestimmen. Außerdem besitzen sie die Möglichkeit auf die *Member Web Site* des W3C mit allen Nachrichten, Ankündigungen und Informationen zu Technologien und Software zuzugreifen<sup>382</sup>. Einzelpersonen können an den Diskussionen in den öffentlichen W3C-Mailinglisten teilnehmen. Als *Invited Experts*<sup>383</sup> können sie auch Zugriff auf die mitgliedsspezifischen Informationen erhalten. Das erwähnte *Advisory Committee* überwacht und überprüft vorgeschlagene *Activities*, den Jahresplan sowie den Vorschritt der Forschungsarbeit und bestimmt die weitere Arbeit des W3C.

Das W3C *Team* besteht aus dem *Chairman*, dem *Director* und dem Personal<sup>384</sup>. Der *Chairman* verwaltet den generellen Lauf des W3C und leitet die Treffen des *Advisory Committee* und des *Advisory Boards*. Außerdem vertritt er das W3C nach außen. Der *Director* (derzeit Tim Berner-Lee) ist für die Leitung der technischen Forschungsarbeit zuständig. Er nimmt eine sehr starke Stellung innerhalb des W3Cs wahr. So hat er letztendlich die Entscheidungsgewalt über wichtige Verfahrensschritte und über die Entwicklungsrichtungen inne. Das *Team* besteht aus circa 50 Forschern, welche die technische Forschung vorantreiben, die Organisation verwalten und den Informationsfluß zu den Mitgliedern des W3C aufrechterhalten. Das *Communication Team*, das aus dem Personal des W3C gebildet wird, sorgt für den reibungslosen Betrieb der

---

<sup>381</sup> Vgl. die Liste der Offices unter <http://www.w3.org/Consortium/Offices/>.

<sup>382</sup> Vgl. W3C, WWW Consortium Process Document, Kap. 2.1.1 Member benefits.

<sup>383</sup> Vgl. W3C, WWW Consortium Process Document, Kap. 2.1.4 Participation in W3C by individuals.

<sup>384</sup> W3C, WWW Consortium Process Document, Kap. 2.2 The W3C Team.

WWW-Seiten und der Mailinglisten und veröffentlicht Pressemitteilungen und Newsletter.

Das 1998 eingesetzte *Advisory Board* bietet Unterstützung in strategischen, geschäftlichen und rechtlichen Fragen, Verfahrensproblemen und Konfliktlösung an. Es stellt sicher, daß das W3C sich nach den Bedürfnissen der Mitglieder ausrichtet. Die Mitglieder dieses Gremiums werden auf Zweijahresbasis vom *Advisory Committee* gewählt.

Wenn das W3C entscheidet, die Forschungsarbeit in einem Gebiet der Webtechnologie aufzunehmen, initiiert es eine sogenannte *Activity*<sup>385</sup> in diesem Bereich<sup>386</sup>. Jede *Activity* wird von einem *Activity Leader* gelenkt. Gewöhnlich wird die Arbeit der *Activities* durch eine oder mehrere Arbeitsgruppen ausgeführt, dessen jeweiliger Typ (*Working Groups, Interest Groups, Coordination Groups*) von der Aufgabe der Gruppe abhängig ist. Die Aufgaben und die Ziele der Gruppe werden durch die Satzung definiert. Durch einen *Chair* werden sie geleitet, der wiederum durch den *Director* des W3C ernannt wird. Die Kommunikation der Gruppenmitglieder erfolgt durch persönliche Treffen oder durch Onlinekonferenzen. Ebenso werden Mailinglisten und Veröffentlichungen durch WWW-Seiten herangezogen. Im Vergleich zu den *Working Groups* der IETF müssen Personen, welche an der Gruppenarbeit des W3C teilnehmen wollen, durch einen Vertreter des *Advisory Committees* nominiert werden. Auf diese Weise sollen nur Experten zur Diskussion zugelassen werden.

Vom W3C werden verschiedene Arten technischer Reports veröffentlicht<sup>387</sup>. Zum einen sind dies die Dokumente des *Recommendation Track*, die zum Beispiel technische Spezifikationen oder Richtlinien darstellen<sup>388</sup>. Zum anderen werden die sogenannten *Notes* veröffentlicht, die Ideen und Kommentare von Mitgliedern des W3C beinhalten. Alle diese Dokumente werden in englischer Sprache im WWW veröffentlicht und für unbestimmte Zeit archiviert.

Der *Recommendation Track* bestimmt das Verfahren, nach welchem die *Working Groups* des W3C ihre Dokumente veröffentlichen können. Es ist der Weg vom einfachen Arbeitspapier zum endgültigen Standardvorschlag, welcher dann den RFC-Standards der IETF entspricht. Obgleich sich das Verfahren der Standardsetzung im W3C durch die geschlossene Struktur stark von der Arbeit der IETF unterscheidet, soll hier nur kurz auf die einzelnen Entwicklungsebenen der Standarddokumente eingegangen werden. Zu Beginn der Arbeit einer *Working Group* wird ein *Working Draft*

---

<sup>385</sup> W3C, WWW Consortium Process Document, Kap. 3 W3C Activities and Groups.

<sup>386</sup> Eine Liste aller derzeitigen Activities kann unter <http://www.w3.org/Consortium/Activities> eingesehen werden.

<sup>387</sup> W3C, WWW Consortium Process Document, Kap. 6 W3C Technical Reports.

<sup>388</sup> Vgl. auch zum Normierungsverfahren des W3C: Mayer, K&R 2000, 13, 18f.

veröffentlicht, welcher eine Ausgangslösung darstellt, ohne von einem Konsens getragen zu werden. Die folgende *Candidate Recommendation* stellt ein beständiges *Working Draft* dar, das der *Director* zu Testzwecken und zum Feedback veröffentlicht hat. Intensiv diskutiert und von der experimentellen Umsetzung verbessert, kann ein solches Dokument vom *Advisory Committee* überprüft werden und als *Proposed Recommendation* veröffentlicht werden. Sollte schließlich ein vom *Director* bestätigter Konsens innerhalb des W3Cs erreicht werden, kann eine endgültige *Recommendation* veröffentlicht werden. Dieses Dokument soll die Mission des W3Cs erfüllen und einen einheitlichen Standard für das WWW setzen. Obgleich vorgesehen ist, daß jedes *Working Draft* zu einer *Recommendation* weiterentwickelt wird, impliziert dies nicht die volle Durchschreitung des *Recommendation Track* bis zum endgültigen Standard.

Wie in der Entwicklung von RFCs durch die IETF ist im W3C-Prozeß die Idee eines Konsenses integraler Bestandteil. Damit soll es ermöglicht werden, eine einzige akzeptable Lösung für die Öffentlichkeit zu entwickeln. Es ist während der Diskussion eines Themas wichtig, daß alle Ansichten und Einwände der beteiligten Personen betrachtet werden. Während Einstimmigkeit erwünscht ist, genügt für einen Konsens ein mehrheitliches Einverständnis durch die Teilnehmenden. Lösungen von *Working Groups*, welche zu einer Marktplatzierung führen würden, können folglich nicht als *Recommendation* veröffentlicht werden.

Da neben dem W3C viele weitere Organisationen existieren, die Standards im Internet setzen, ist zunächst eine klare Definition der zu bearbeitenden Themen nötig, um eine effiziente Kommunikation der Organisationen zu ermöglichen. Zum Beispiel darf sich die Arbeit der IETF nicht mit den Aktivitäten des W3Cs überschneiden. Die IETF beschäftigt sich daher besonders mit Internetprotokollen, während das W3C die Architektur des WWW vorantreibt. Das W3C definiert das WWW, die Dokumente des WWW sowie die Protokolle zu dessen Zugang und Verteilung. Es versucht, nicht in die Spezifikation von IP, TCP oder DNS einzugreifen. Das für das WWW wichtige *Hypertext Transport Protocol* (HTTP) wurde unter Teilnahme des W3C durch die in der Protokollentwicklung erfahrene IETF entwickelt. Weitergehende Definitionen, wie die URI-Bestimmungen oder die *Hypertext Mark Up Language* (HTML), die Kerndefinition aller WWW-Dokumente, liegen im alleinigen Arbeitsbereich des W3Cs. Besonders im Grenzbereich dieser Aufgabenbereiche ist jegliche Anstrengung für eine offene Kommunikation und Kooperation zwischen den beiden Organisationen nötig, um eine doppelte Definition einer Anwendung zu verhindern. Eine solche mehrfache Bestimmung würde dem grundsätzlichen Ziel der Interoperabilität beider Gruppen widersprechen.

Eine Zusammenarbeit erfolgt nicht nur mit der IETF. Vielmehr werden eine Reihe verschiedener Organisationen in die Arbeit des W3Cs mit einbezogen, wie die ISO, das *Unicode Consortium*, das *WAP-Forum* oder diverse Regierungsbehörden, wie die *Europäische Kommission* oder die US-Regierung.

### 2.4.1.3. Standardsetzung im Internet

Die im Internet verfolgte Standardisierungsstrategie unterscheidet sich maßgeblich von den im Kapitel 2.4.1.1.4 oben erwähnten herkömmlichen Verfahrensweisen (als Überblick vgl. Abbildung 4 unten). Die Besonderheiten der im Internet beheimateten Standardisierungsorganisationen, zum Beispiel W3C oder IETF, liegen in einer nicht-hierarchischen Struktur und einem offenen Teilnehmerkreis<sup>389</sup>. Dieser ist nicht auf vorher festgelegte Mitglieder beschränkt, sondern jeder Internetteilnehmer darf selbst Vorschläge zu bestimmten Themen in dafür vorgesehenen Diskussionsforen machen sowie die Anregungen anderer kommentieren. Standards werden somit gemeinsam entworfen und die Ergebnisse auch im Internet jedem Interessenten zur Verfügung gestellt. Entsprechend basiert die Standardsetzung im Internet stark auf einem gemeinsamen Konsens und einem Vertrauen auf Erfahrung<sup>390</sup>. Computerwissenschaftler, Ingenieure und Programmierer finden sich zusammen, um verschiedene technische Themen zu diskutieren. Ein „Rough Consensus“<sup>391</sup> wird bezüglich eines spezifischen Standards erreicht und im Internet veröffentlicht. Diese in den Schlußdokumenten veröffentlichten Standards strahlen eine stark bindende Wirkung aus. Sie werden gewöhnlich von der Mehrzahl der potentiellen Anwender beachtet und umgesetzt. Der Vorteil dieser öffentlichen Ausarbeitung der Kommunikationsstandards liegt in der schnellen Reaktionsmöglichkeit auf aktuelle technische Entwicklungen. Die Entwicklungsarbeit ist nicht auf die Ziele eines bestimmten Personenkreises fixiert, sondern involviert die verschiedenen Anwendungsbereiche des diskutierten Standards.

---

<sup>389</sup> Vgl. *Ladeur*, CR 1999, 395, 400 ; *Crocker*, Standards, Kap. The IETF standards process.

<sup>390</sup> Vgl. *Liu*, 74 Ind. L.J. 587, 595.

<sup>391</sup> *David C. Clark*, Massachusetts Institute of Technology: „We do not worry about presidents and kings. We work by rough consensus and running code.“.

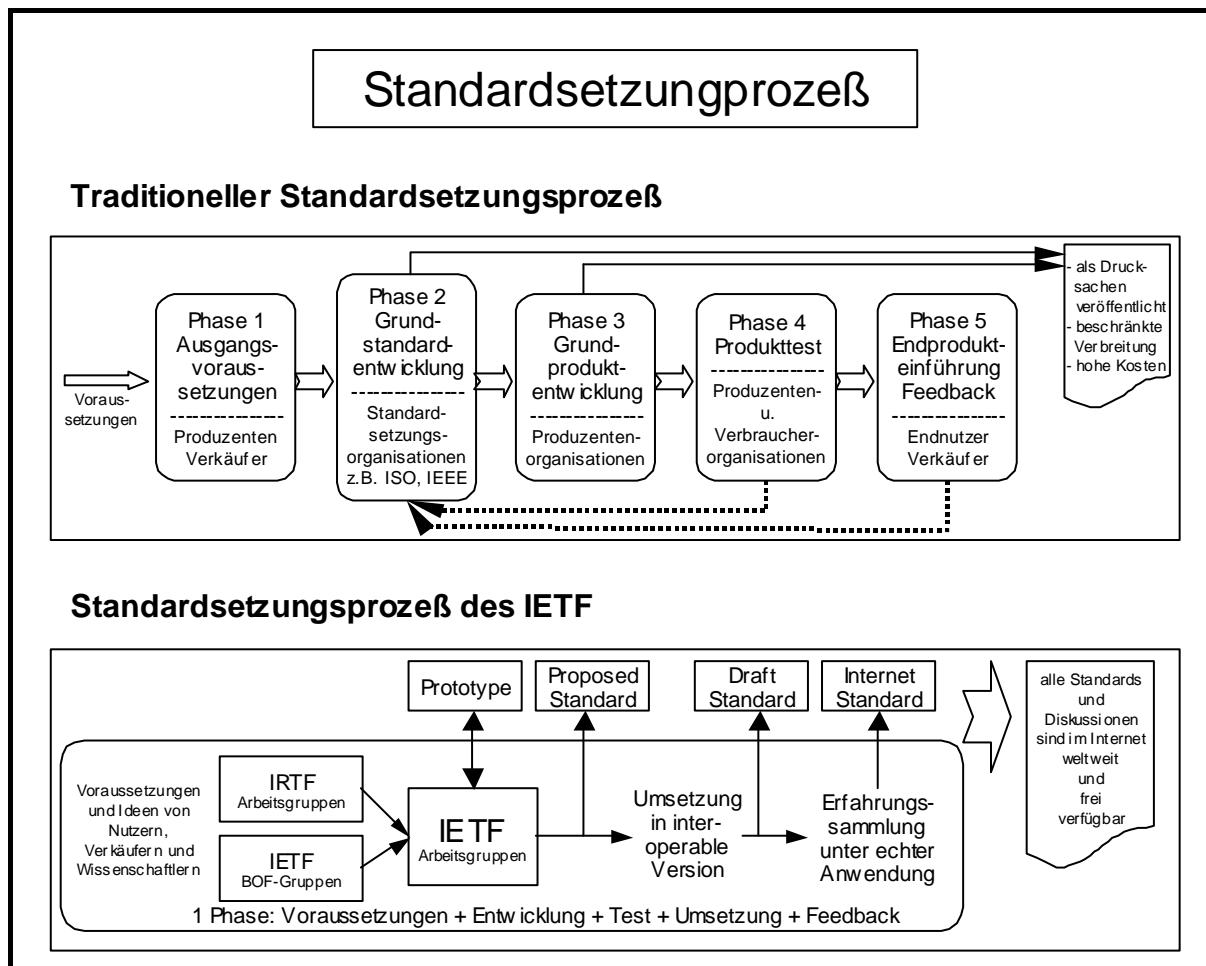


Abbildung 4 – Vergleich zwischen traditioneller und internetinterner Standardsetzung<sup>392</sup>.

Von einem Zwang zur Standardisierung sind im Internet besonders die Internetprotokolle und das DNS betroffen. Je mehr Nutzer sich unter Beachtung der verschiedenen Protokolle zu einem Netzwerk verbinden, desto anziehender wird es auch für weitere Anwender sich anzuschließen. Dies wiederum führt zum Anreiz, eine immer ausgefeilte Interoperabilität im Internet herbeizuführen. Da der Wert einer Internetanbindung für Konsumenten so stark von der Anbindung anderer Nutzer abhängt, stellt das Internet ein einzigartiges Beispiel für einen Effekt der Netzwerkexternalität dar<sup>393</sup>. Entsprechend ist die optimale Anzahl von Internetsystemen nur ein einziges System.

Durch die damit einhergehende stärkere Abhängigkeit von bestehender und etablierter Technologie besteht folglich das Risiko, daß der weitere Entwicklungsweg vorgeschrieben ist (*Path dependence*). Die rapide Entwicklung des Internets könnte allerdings diesem Effekt entgegenwirken, da neue Nutzer häufig eher bereit sind, neue Techniken und Standards zu verwenden, welche nicht voll kompatibel mit alten Standards sind<sup>394</sup>.

<sup>392</sup> Vgl. auch *RFC 2026*, Bradner, Kap. 4.1, Kap. 6 sowie <http://www.isoc.org/images/process.gif>.

<sup>393</sup> Vgl. Lemley, 28 Conn. L. Rev. 1041, 1045; Katz/Shapiro, 75 Am. Econ. Rev. 424.

<sup>394</sup> Siehe Lemley, 28 Conn. L. Rev. 1041, 1051.

Mit dem Risiko der *Path dependence* sah sich zum Beispiel die IETF bei der Entwicklung eines erweiterten Internetadreßraumes konfrontiert. Von der Annahme ausgehend, daß der heutige IP-Adreßraum bald durch die exzessive Nutzung erschöpft sei, wurde die *Internet Protocol Version 6* (IPv6) entwickelt und soll Ipv4 ersetzen<sup>395</sup> (vgl. Kapitel 2.2.2.1 oben). Angeichts der derzeitigen Anzahl der Internetnutzer, ist es praktisch unmöglich geworden, auf einmal IPv6 einzuführen. Entsprechend muß der neue Internetadreßraum mit dem herkömmlichen kompatibel sein, um eine kontinuierliche Einführung zu ermöglichen. IPv6 stellt somit eine Erweiterung des IPv4 dar. Die Einführung neuerer und inkompatibler Features könnte jedoch verhindert werden, wenn eine zu große Nutzerzahl nicht auf die neue Version umsteigt. Die veraltete Version würde dann weiterhin bestehen bleiben, obwohl eine neue und verbesserte Version zur Verfügung steht<sup>396</sup>.

Der sehr lange Diskussionsprozeß zur Entwicklung von IPv6 mit 2½ Jahren wurde durch die große Anzahl an Teilnehmern verursacht. Die sehr unterschiedlichen Ansichten haben die Entwicklung entsprechend verlangsamt. Es wird aber allgemein angenommen, daß durch die Beteiligung aller betroffenen Parteien, die optimale Lösung gefunden wurde<sup>397</sup>.

Somit zeigt sich auch die Grenze des auf einem Konsens beruhenden Standardsetzungsverfahrens. Ein Konsens kann gewöhnlich nur in einer relativ kleinen Gemeinschaft von Teilnehmern mit einem gemeinsamen Ziel erreicht werden. Zum Beispiel stellen die Forscher der IETF eine solche Gemeinschaft dar. Ein Konsens wird auch leichter erreicht, wenn das behandelte Thema technischer Natur ist. Eine Einigung der Teilnehmer ist jedoch sehr schwierig zu erreichen, wenn diese eine Vielzahl unterschiedlicher Interessen mit konkurrierenden ökonomischen und politischen Ideen vertreten<sup>398</sup>. In die Entwicklungsarbeit können dann nicht mehr alle Interessen aufgenommen werden. Einige Gesichtspunkte werden ganz von der stattfindenden Diskussion ausgeschlossen sein. Sollte man jedoch versuchen, alle relevanten Parteien in den Diskussionsprozeß einzubeziehen, wird ein Konsens nicht mehr erreichbar sein.

Die meisten technischen Standardspezifikationen blieben bislang für den Normalanwender verborgen. Für ihn spielt es nur eine geringe Bedeutung, mittels welchen Protokolls Daten übers Internet übertragen werden, solange eine Beachtung seiner Bedürfnisse erfolgt und er auf einfache Weise mit anderen Nutzern kommunizieren kann. Einige Technologien wie das DNS oder das WWW haben jedoch direkte Auswirkungen auf den Endnutzer. Für ihn spielt es zum Beispiel eine Rolle, ob er einen bestimmten Domainnamen unproblematisch reservieren kann oder sich dem Risiko eines Verfahrens nach der *Uniform Domain Name Dispute Resolution Policy* (UDRP) ausgesetzt sieht. Die Parteien, die früher geringe Anteilnahme an der Ausgestaltung der größtenteils unsichtbaren Standards haben, zeigen jetzt direktes Interesse

---

<sup>395</sup> Siehe *Ermert*, c't 2000, Heft 1, 32f.; *Kreml*, c't 1999, Heft 20, 212ff.; *RFC 2460*, Deering/Hinden.

<sup>396</sup> Zu der schleppenden Umsetzung von IPv6 siehe *Ermert*, c't 2000, Heft 1, 32f.

<sup>397</sup> Vgl. *Maher*, 3 Va. J.L. & Tech. 5, Art. 5 Rdnr. 83.

<sup>398</sup> Siehe auch ausführlich anhand des DNS *Liu*, 74 Ind. L.J. 587, 610ff.

resse an der zukünftigen Gestaltung des Internets und insbesondere des DNS<sup>399</sup>. Bei der Erweiterung des DNS und der dieses System verwaltenden Organisation spielen nunmehr nicht nur technische Fragen eine Rolle<sup>400</sup>, sondern es werden auch gesellschaftliche und politische Fragen aufgeworfen, die einer nichttechnischen Lösung bedürfen.

Probleme bereitet auch, daß durch die steigende Popularität des Internets die Freiwilligkeit einer Implementierung von Standards immer hypothetischer wird. Durch die weite Verbreitung vieler Internetstandards ist ein Abweichen von diesen immer weniger möglich, ohne selbst von der Kommunikation abgeschnitten zu werden. Diese potentielle Zwangswirkung der Internetstandards veranlaßt deshalb unablässig politische und gesellschaftliche Organisationen in den technischen Entwicklungsprozeß einzugreifen, um eigene Positionen für die Zukunft bindend durchzusetzen.

Da es sich bei vielen Internetstandards um offene Standards handelt, kann folglich nicht angenommen werden, daß es von einem einzigen Unternehmen oder einer einzigen Gruppierung betrieben wird. Vielmehr setzt sich das Internet aus einer Vielzahl von Telefon- und Kabelgesellschaften, Internetserviceprovidern, Unternehmen sowie Universitäten zusammen<sup>401</sup>. Das Internet kann in dieser verteilten Organisation nur existieren, da alle Teilnehmer indirekt eingewilligt haben, die Standard-Internetprotokolle zu verwenden. Ohne dieses unbewußte Einverständnis könnte das Internet in der jetzigen Form nicht bestehen<sup>402</sup>. Dieser Zwang gilt nicht nur für die Internetbetreiber selbst. Um auf die Informationen, die über das Internet erreichbar sind, zugreifen zu können, müssen die Endnutzer die entsprechende Software (zum Beispiel Webbrower oder Email-Programme) installieren, welche die jeweils notwendigen Internetprotokolle korrekt anwendet.

Um den Standardisierungsprozeß im Internet besser zu verstehen, soll im Folgenden auf das Diskussions- und Entscheidungsverfahren näher eingegangen werden.

#### 2.4.1.3.1. *RFCs, BCPs und STDs als Grundlage*

Die bedeutendsten Richtlinien für die Entwickler von Anwendungen für das Internet sind die schon öfters erwähnten standardsetzenden *Requests for Comments* (RFC). Diese werden häufig von Organisationen, welche im Standardsetzungsprozeß des Internets involviert sind, geschrieben. Autoren können jedoch auch Mitglieder anderer Organisationen oder privat auftre-

---

<sup>399</sup> Dies zeigt auch die hohe Beteiligung an den ICANN-Wahlen im Oktober 2000. Obgleich man nur von einer maximalen Teilnehmerzahl von 10.000 Wählern ausging, hatten sich über 158.000 zur Wahl registriert, 76.000 ihre Mitgliedschaft aktiviert und ca. 35.000 bei der Endwahl ihre Stimmen abgegeben, vgl. die Statistik der ICANN unter *ICANN@Large*, Final Total of Activated At Large Members,

<http://members.icann.org/activestats.html> und die graphische Auswertung unter *ICANN Channel*, At-Large-Statistik, <http://www.icannchannel.de/stats2000.htm>. Siehe auch der Bericht von *Hack*, Telepolis 8892.

<sup>400</sup> Vgl. *Liu*, 74 Ind. L.J. 587, 612.

<sup>401</sup> Die Untersuchungen der Cybergeographen weisen jedoch daraufhin, daß das Internet-Backbone im Eigentum weniger Unternehmen liegt. 30% des gesamten Internet-Backbones gehört z.B. UUNet. Vgl. *Bleich*, c't 2000, Heft 9, 212, 217.

<sup>402</sup> Siehe *Bar*, 4 Info. Inf. & Pol. 235, 236.

## 2.4. Verwaltung des Internet

---

tende Personen sein. Sie werden vom RFC-Editor (siehe Kapitel 2.4.1.2.2 oben) herausgegeben und verwaltet. Als Person hinter dem RFC-Editor stand ursprünglich Dr. Jon Postel, welcher später durch Joyce K. Reynolds abgelöst wurde. Der erste RFC wurde von Steve Crocker im April 1969 als Bestandteil des ursprünglichen ARPANET geschrieben. Obgleich das Thema „*Host Software*“ für die Entwicklung des Internets unbedeutend gewesen ist, war der erste RFC der Grundstein für eine lang anhaltende Diskussion über technische Lösungsmöglichkeiten im Internet<sup>403</sup>. Inzwischen existieren über 3000 Veröffentlichungen. Um eine leichte Deklaration zu ermöglichen, wird jedem neuen RFC eine laufende Nummer zugewiesen.

Es existieren verschiedene Varianten von RFCs, deren Kategorien jeweils am Kopf eines RFCs wiedergegeben werden. Nicht in jedem RFC wird ein Internetstandard dokumentiert. Zum Beispiel werden neben den Internetstandards in RFCs auch Verfahrensweisen von Organisationen niedergelegt und für den Endanwender wichtige Informationen veröffentlicht.

Nach RFC 2026 werden Internetstandards nach folgenden Kriterien definiert<sup>404</sup>:

In general, an Internet Standard is a specification that is stable and well-understood, is technically competent, has multiple, independent, and interoperable implementations with substantial operational experience, enjoys significant public support, and is recognizably useful in some or all parts of the Internet.

Die RFCs, welche einen Internetstandard beschreiben, werden der Unterserie der *Standards* (STD) zugeordnet. Sie erhalten die zusätzliche Numerierung „STDxxx“, behalten jedoch ihre RFC-Nummer und ihren Platz in der RFC-Serie. Wird eine neue Version eines schon bestehenden Standards verabschiedet, so erhält dieses Dokument zwar eine neue RFC-Nummer, die STD-Numerierung bleibt dagegen erhalten.

Ursprünglich haben Internetstandards der IETF sich mit technischen Spezifikationen von Hard- und Software auseinandergesetzt. Seit das Internet sich selbst verstärkt aus verschiedenen Organisationen mit unterschiedlichen Zielen und Regeln zusammensetzt, wurden öffentliche Richtlinien für deren Funktionen und Verfahrensweisen publiziert. Einige RFCs standardisieren oder beschreiben deshalb das Diskussions- oder Wahlverfahren, beziehungsweise diverse Prinzipien von verschiedenen Internetorganisationen. Diese RFCs sind der Unterserie der *Best Current Practice* (BCP) zuzuordnen und erhalten ebenfalls eine zusätzliche Numerierung in der Form „BCPxxx“<sup>405</sup>. Ein BCP-Dokument unterfällt den gleichen Prinzipien des Standardsetzungsprozesses der IETF wie die STDs.

---

<sup>403</sup> Zur Geschichte der RFCs siehe die Essay-Sammlung im *RFC 2555*, RFC-Editor.

<sup>404</sup> Siehe *RFC 2026*, Bradner, Kap. 1.1 Internet Standards.

<sup>405</sup> Siehe die nähere Beschreibung der BCP-Dokumente in *RFC 2026*, Bradner Kap. 5. Best Current Practice (BCP) RFCs.

Andere Dokumente sind nicht den Regeln der Internetstandardisierung der IETF unterworfen und werden deshalb mit den Kategorien *Experimental* oder *Informational* bezeichnet. Zu den *Informational*-RFCs zählen zum Beispiel die Dokumente der Unterserie *For Your Information* (FYI) mit der zusätzlichen Numerierung in der Form „FYIxxx“<sup>406</sup>. Die FYI-Serie soll den Internetnutzern als zentrale Informationsquelle über die verschiedenen Themen, welche im Zusammenhang mit dem Internet stehen, dienen. Dabei werden zum einen Anfänger, zum anderen auch fortgeschrittene Internetnutzer angesprochen.

Alle RFCs werden online veröffentlicht<sup>407</sup> und sind für jeden zugänglich. Um einem weiten Interessenskreis das Lesen der gespeicherten RFC-Dateien zu ermöglichen, werden sie traditionell in einem reinen Textformat (ASCII) gespeichert und publiziert. Darüber hinaus sind auch moderne Textversionen mit Grafiken und Formatierungen verbreitet (zum Beispiel für das WWW). Der Aufbau eines RFCs ist nach RFC 2223 genau festgelegt, um spätere Mißverständnisse und Streitigkeiten zu vermeiden. Ein solches Dokument muß unter anderen den Autor, das Veröffentlichungsdatum und die Kategorie ausweisen. Ebenso muß das Dokument eine Copyrightbestimmung zugunsten der ISOC enthalten.

#### 2.4.1.3.2. Verfahrensgang der Standardsetzung

Das Verfahren der Standardsetzung durch die IETF wird im BCP 9, *The Internet Standards Process -- Revision 3* (RFC 2026), ausführlich festgelegt. Beim aktuellen Verfahren handelt es sich um eine durch längerer Diskussion und Anwendung in weiten Kreisen der Internetorganisationen anerkannte Prozedur. Änderungen des Verfahrens sind somit über den gleichen Prozeß vorzunehmen, der für Änderungen aller sonstigen BCP-Dokumente gilt (siehe weiter unten). Mit Festlegung dieses Prozesses sollen folgende Ziele erreicht werden<sup>408</sup>:

- Hervorragendes technisches Ergebnis;
- Vorhergehende Implementation und sowie ausführliche Tests;
- Klare, prägnante und leicht verständliche Dokumentation;
- Offenheit und Fairneß und
- Zügige Entwicklung.

Das Verfahren zur Entwicklung von Internetstandards muß zwei gegensätzliche Bedingungen ausbalancieren. Zum einen beansprucht das Ziel der technischen Vollkommenheit und das Erfordernis des ausführlichen Testens und Implementierung genügend Zeit und Arbeit. Andererseits gebietet der schnelle Fortschritt in der Netzwerktechnologie eine schnelle Entwicklung von Standards. Das Verfahren muß somit einfach und zügig sein, ohne auf einen Testdurchlauf oder auf Offenheit und Fairneß zu verzichten.

---

<sup>406</sup> Siehe die nähere Beschreibung der FYI-Dokumente in *RFC 1150*, Malkin/Joyce.

<sup>407</sup> Eine Veröffentlichung erfolgt z.B. unter <http://www.rfc-editor.org>.

<sup>408</sup> Siehe *RFC 2026*, Bradner, Kap. 1.2 The Internet Standards Process.

Spezifikationen von Internetstandards können in zwei Kategorien eingeteilt werden: *Technical Specifications* und *Applicability Statements*<sup>409</sup>. Eine *Technical Specification* beschreibt Protokolle, Dienste, Verfahren, Übereinkünfte oder Formate. Ein *Applicability Statement* spezifiziert wie und unter welchen Umständen eine oder mehrere *Technical Specification* angewendet werden sollen, um eine bestimmte Internetanwendung zu ermöglichen.

Damit eine Ausgangsidee sich zu einem Internetstandard entwickelt, muß sie eine Anzahl von Entwicklungsniveaus (*Proposed Standard*, *Draft Standard* und *Standard*) durchlaufen, welche als *Standards Track* bekannt sind. Auch ein endgültiger Standard kann Gegenstand weiterer Entwicklung sein. Bevor eine Spezifikation, gleich welchen Niveaus, als RFC veröffentlicht wird, werden durch die IETF die Entwürfe (sogenannte *Internet-Drafts*) zur Diskussion und Kommentierung auf verschiedenen Servern bereitgestellt. Diese *Internet-Drafts* können zu jeder Zeit entfernt oder durch eine neue Version aktualisiert werden. *Internet-Drafts* sind kein Mittel zur endgültigen Veröffentlichung von Spezifikationen und Anwendungen. Softwarehersteller dürfen sich folglich nicht auf die darin festgelegten Bestimmungen berufen<sup>410</sup>. Ein ausdiskutierter *Internet-Draft* kann dann als RFC innerhalb der verschiedenen Niveaus der *Standards Track* veröffentlicht werden.

Der niedrigste Level für eine Spezifikation ist der *Proposed Standard*. Jede Spezifikation der IESG muß auf diesem Niveau beginnen. Ein *Proposed Standard* ist verständlich gestaltet, hat ausreichend Überprüfung durch die Internetgemeinschaft erfahren und wird von dieser für wertvoll befunden. Eine solche Spezifikation kann Gegenstand weiterer Veränderungen oder gar eines Rückrufes sein. Obgleich erwünscht, ist weder eine vorherige Implementation, noch Erfahrung im täglichen Betrieb notwendig, um eine Spezifikation dieses Levels zuzuweisen. Eine Spezifikation sollte mindestens sechs Monate auf dem Level des *Proposed Standards* verbleiben, ehe sie in eine höhere Kategorie wechselt kann.

Wurden von diesem *Proposed Standard* mindestens zwei unabhängige und interoperable Anwendungen entwickelt und genügend Erfahrung während des Einsatzes gesammelt, kann dieser Standard auf das Niveau eines *Draft Standards* erhoben werden. Eine solche Aufwertung des Status geschieht aus der Überzeugung, daß die Spezifikation ausgereift und nützlich ist. Der Vorsitzende der entsprechenden *Working Group* der IETF ist für eine ausführliche Dokumentation der spezifischen Implementierungen sowie der Tests der Interoperation beider Anwendungen zuständig. Ein *Draft Standard* wird gewöhnlich als endgültige Spezifikation verstanden und Änderungen sollten nur zur Lösung von spezifischen Problemen vorgenommen werden. Auf dem Niveau des *Draft Standards* sollte ein solches Dokument mindestens vier Monate verbleiben, um eine adäquate Überprüfung durch die Öffentlichkeit zu ermöglichen.

---

<sup>409</sup> Vgl. *RFC 2026*, Bradner, Kap. 3. Internet Standard Specification.

<sup>410</sup> Vgl. *RFC 2026*, Bradner, Kap. 2.2 Internet-Drafts.

Soweit der *Draft Standard* umgesetzt wurde und erfolgreich angewendet wird, kann dieser auf das Niveau der *Internet Standards* erhoben werden. Dies bedeutet, daß das standardisierte Protokoll oder der Service ein hohes Niveau an technischer Ausgereiftheit erlangt hat und für das Internet von wichtigem Vorteil ist. Ein solcher *Internet Standard* wird in die RFC-Unterserie der STD aufgenommen und erhält eine eigene STD-Nummer.

Die Hauptentscheidungsgewalt, ob eine Spezifikation in den *Standard Track* aufgenommen oder von einem Standardniveau zum nächsten erhoben wird, beziehungsweise ob ihr die Standardqualität aberkannt wird, obliegt der IESG. Die lange Erfahrung und das gemeinsame Urteil der IESG-Mitglieder spielt im Entscheidungsprozeß dabei eine entscheidende Rolle<sup>411</sup>.

Das Verfahren wird auf Empfehlung einer *Working Group* der IETF durch den verantwortlichen *Area Director* eingeleitet. Dazu muß die neue Spezifikation zunächst als *Internet-Draft* veröffentlicht werden, um eine ausreichende Überprüfung durch die Öffentlichkeit zu ermöglichen. Die IESG entscheidet, ob der zugeleitete Vorschlag den Kriterien des gewünschten Standardniveaus entspricht. Zur Unterstützung ihrer Entscheidung kann die IESG eine Kommission zur technischen Überprüfung der Spezifikation einrichten. Um eine endgültige Kontrolle durch die Öffentlichkeit zu ermöglichen, wird ein sogenannter *Last-Call* zur Hauptmailingliste der IETF durch die IESG gesendet. Dieser *Last-Call* soll der IESG ermöglichen, eine Entscheidung über die Annahme als Standard zu treffen. Bei einer positiven Entscheidung wird der *RFC-Editor* und die IETF benachrichtigt und die Veröffentlichung als RFC angewiesen. Auch bei jeder Änderung des Status eines Standards sollte eine erneute Publikation als RFC erfolgen. Einige Änderungen jedoch erzwingen eine sofortige Korrektur des aktuellen RFC (zum Beispiel wesentliche Tippfehler). In diesem Falle wird der entsprechende RFC durch den *RFC-Editor* erneut publiziert, ohne erneut dem herkömmlichen Standardsetzungsverfahren unterworfen zu sein. Eine neue Version (im Unterschied zur Erhöhung des Levels) eines etablierten Standards muß jedoch den ganzen *Standard Track* erneut durchlaufen, als wäre es eine völlig neue Spezifikation. Wenn die neue Version das Niveau des *Internet Standard* erreicht hat, ersetzt sie gewöhnlich die Vorgängerversion, welche dann den *Historic Status* erhält. Auch einem Standard, der durch technologische Änderungen und Entwicklungen überflüssig geworden ist, kann durch das IESG der *Historic Status* zugewiesen werden.

Das beschriebene Verfahren läßt sich nicht auf die Verabschiedung von BCP-Dokumenten übertragen. Um den reibungslosen Betrieb der verschiedenen Internetorganisationen unter der ISOC zu gewährleisten, ist eine sofortige Umsetzung und Anwendung eines BCP notwendig. Die Entwicklung eines BCP-Dokumentes ist ähnlich der eines *Proposed Standards*. Das Dokument muß nach Entwurf und Diskussion an die IESG zur Überprüfung geleitet werden. Wurde das BCP von der IESG angenommen, endet das Verfahren und das Dokument wird veröffentlicht. Da ein BCP ebenso wie ein STD den Konsens der Internetgemeinschaft wiederspiegelt, jedoch bedeutend schneller verabschiedet wird, muß auf eine sorgfältige Untersuchung und Diskussion wert gelegt werden.

---

<sup>411</sup> Vgl. zum Ganzen: *RFC 2026*, Bradner, Kap. 6. The Internet Standards Process.

Durch den offenen Prozeß bei der Einführung der Standards besteht ein beträchtliches Konfliktpotential. Zum einen kann jemand mit einer Aktion einer *Working Group* der IETF nicht einverstanden sein. Weiterhin kann eine Person der Ansicht sein, daß die IESG den im RFC 2026 festgeschriebenen Verfahrensgang verletzt hat. Schließlich könnte dieser Verfahrensgang selbst als unvereinbar mit einem fairen und offenen Standardsetzungsprozeß gehalten werden. Um die Hauptziele Offenheit und Fairneß zu gewährleisten, muß auf eine sorgfältige Lösung dieser Kontroversen geachtet werden<sup>412</sup>. Auf diese verschiedenen Probleme soll im Folgenden näher eingegangen werden.

Eine Person, welche nicht mit der Entscheidung einer *Working Group* einverstanden ist, sollte dies zunächst mit dem *Chair* der entsprechenden Arbeitsgruppe diskutieren. Sollte die Diskrepanz nicht mittels des *Chairs* gelöst werden, kann das Anliegen dem zuständigen *Area Director* zur Streitschlichtung vorgetragen werden. Gegen die Entscheidung des *Area Directors* kann wiederum bei der IESG Beschwerde eingelegt werden, welche die volle Autorität hat, die Streitigkeit nach eigener Wahl zu entscheiden. Als höchste Entscheidungsinstanz kann jede involvierte Partei das IAB anrufen, die den Konflikt im Ganzen überprüft und die Befugnis hat, ihn selbst zu lösen. Somit fällt das IAB in Verfahrensfragen und ebenso in technischen Fragen die endgültige Entscheidung.

Die Hauptaufgabe der IESG besteht darin, zu sichern, daß das festgesetzte Verfahren und die Voraussetzungen zur Standardsetzung eingehalten wurden. Sollte die Ansicht einer Person mit Entscheidungen der IESG nicht übereinstimmen, muß die Diskrepanz zunächst mit dem *Chair* der IESG diskutiert werden. Kann der Vorsitzende das Problem nicht zur Zufriedenheit der betroffenen Person lösen, soll die gesamte IESG die Streitfrage betrachten und zu lösen versuchen. Auch hier bildet das IAB die höchste Streitschlichtungsinstanz und kann durch die beteiligten Parteien angerufen werden. Diese entscheidet nach ausführlicher Betrachtung des Falles nach eigenem Ermessen. Das IAB kann eine Entscheidung der IESG annullieren oder eine eigene Empfehlung an die IESG weiterleiten. Ausgeschlossen sind davon nur Angelegenheiten, welche in die Gewalt der IESG fallen.

Die letzte Möglichkeit, auf das Verfahren einzuwirken, besteht darin, einen Einspruch zu erheben, daß das festgesetzte Verfahren nicht mit den Grundsätzen von Offenheit und Fairneß zu vereinbaren ist. Klagen über die Verletzung dieser Grundsätze sind an das BoT der ISOC zu richten. Der Präsident der ISOC soll eine solche Klage innerhalb von zwei Wochen annehmen und den Beschwerdeführer über die voraussichtliche Bearbeitungszeit informieren. Die *Trustees* haben den Streitgegenstand im eigenen Ermessen zu untersuchen und endgültig zu entscheiden.

Alle Rechtsbeschwerden müssen eine detaillierte Beschreibung des Streitgegenstandes beinhalten. Sie müssen innerhalb von zwei Monaten nach öffentlichem Bekanntwerden der betrof-

---

<sup>412</sup> Vgl. zum Ganzen: *RFC 2026*, Bradner, Kap. 6.5 Conflict Resolution and Appeals.

fenen Entscheidung eingeleitet werden. Die Ausgestaltung des Verfahrens der Streitschlichtung steht im Ermessen der jeweils angerufenen Person oder Körperschaft. Alle Entscheidungen müssen jedoch innerhalb angemessener Zeit erfolgen.

#### 2.4.1.3.3. Wettbewerbsbeschränkungen durch öffentliche Standards

Obwohl die in den RFCs veröffentlichten Standards keine direkte Bindungswirkung für Softwarehersteller und Anwender besitzen, könnten sie dennoch kartellrechtliche Bedeutung erlangen, wenn sie ihre Anhänger in der Weise motivieren, daß diese andere Standards „boykottieren“. Dieser „Boykott“ besteht in einer gemeinsamen und selektiven Verweigerung von Internetserviceprovidern an verschiedene Interessenten ihre Dienstleistungen und Produkte anzubieten, solange diese nicht die offiziellen Internetstandards erfüllen<sup>413</sup>. Die Gefahr einer Wettbewerbsbeschränkung ergibt sich dabei schon aus der Natur der Netzwerkprotokolle, da diese die Möglichkeit ausschließen, mit anderen inkompatiblen Anwendungen zu kommunizieren.

Diesem Problem sah sich 1988 die ISO ausgesetzt, als sie ihr *Open Systems Interconnection*<sup>414</sup> (OSI) Protokoll verabschiedete, ein umfassendes, jedoch zu TCP/IP inkompatibles Internetprotokoll. Obwohl OSI durch die ISO verabschiedet und von einigen europäischen Regierungen eingesetzt wurde, konnte es sich nicht gegen das ältere und weiter verbreitete TCP/IP durchsetzen. Für ältere Internetserviceprovider war es nicht möglich, verschiedenen europäischen Providern Internetdienste anzubieten, solange diese sich nicht für eine Datenübertragung mittels des TCP/IP entschieden hatten. Auf Grund des Selbstvollzuges der technischen Protokolle war keine direkte Verweigerung des Datenaustausches notwendig. Die technischen Protokolle beschränken somit faktisch zunächst den Wettbewerb.

Die Einigung auf bestimmte Netzwerkprotokolle ist jedoch aus der Natur der Standards notwendig. Da ein weltweiter Datenaustausch ohne die Einigung auf einen einzigen Datenübertragungsstandard unmöglich ist, wäre der Aufbau eines globalen Internets nicht möglich. Die Entwicklung eines umfassenden Netzwerkes ist nur möglich, wenn die Betreiber sich darauf einigen können, wie sie ihre Computer zusammenschließen wollen. Das Gleiche gilt auch bei höheren Internetprotokollen, wie FTP, HTTP oder SMTP (siehe Kapitel 2.4.1.3 oben). Ein globaler Mailaustausch ist nur möglich, wenn für die Softwareproduzenten klar ist, wie eine Email aufgebaut ist und wie diese zu versenden ist. Ebenso muß bestimmt sein, nach welchem Schema der Zugriff auf einen Webserver oder einen FTP-Server zu erfolgen hat. Zu beachten ist jedoch, daß die Kommunikation im Internet nicht auf die festgelegten Anwendungsstandards begrenzt ist. Das auf dem TCP/IP beruhende Internet ist für neue und erweiterte Anwendungsstandards völlig offen. Jeder kann seinen eigenen Anwendungsstandard verwenden, allerdings mit der Folge, nur mit den Teilnehmern kommunizieren zu können, welche diesen

---

<sup>413</sup> Vgl. zum Ganzen *Goldfoot*, 84 Va. L. Rev. 909, 945.

<sup>414</sup> Vgl. zum Open Systems Interconnection: ISO, List of ICS fields, 35.100 - Open Systems Interconnection (OSI), <http://www.iso.ch/iso/en/CatalogueListPage.CatalogueList?ICS1=35&ICS2=100>.

## 2.4. Verwaltung des Internet

---

proprietären Standard verstehen<sup>415</sup>. Damit ist ein interner Konkurrenzkampf zwischen den verschiedenen alten und neuen Anwendungsstandards eröffnet. Erst die Einigung auf die Verwendung von TCP/IP ermöglichte den intensiven Wettbewerb der Internetprovider untereinander. Die anfängliche Wettbewerbsbeschränkung der Netzwerkprotokolle führte schließlich zu einer Intensivierung des Wettbewerbs. Die Einigung auf die Internetprotokolle war somit für den internationalen Konkurrenzkampf unerlässlich. Durch die öffentlichen Standards wurde im Ergebnis keine Wettbewerbsbeschränkung bewirkt.

### 2.4.1.3.4. Überblick über Vorteile des offenen Standardisierungsprozesses

Um einen Vergleich zum traditionellen Standardsetzungsprozeß zu ermöglichen, soll abschließend ein Überblick über die Vorteile des offenen Standardisierungsprozesses im Internet gegeben werden<sup>416</sup>:

- Personifizierte Teilnahme  
Der Internet-Standardisierungsprozeß ist durch die Teilnahme von natürlichen Personen gekennzeichnet, da Ansichten von Organisationen und Unternehmen keine Rolle spielen sollen.
- Offener Teilnehmerkreis  
Jeder hat sofortigen Zugriff auf alle relevanten Informationen, um sich unmittelbar in die Diskussion einzuschalten. Die Teilnahme kann durch Diskussion in Mailinglisten über das Internet oder durch Teilnahme an den verschiedenen Treffen geschehen. Eine Teilnahmegebühr ist nicht vorgesehen. Diese außergewöhnliche Teilnahmemöglichkeit hat zum Zusammenschluß von Tausenden von Experten geführt, welche frei ihre Ideen und Entwicklungen austauschen.
- Optimale Tests  
Die im Internet beschlossenen Standards sind während ihrer Entwicklung den verschiedenen Tests unterzogen worden, um die Ausfallsicherheit und Interoperabilität zu gewährleisten.
- Beachtung der Endnutzerbedürfnisse  
Durch die Teilnahme von Interessensgruppen und die Beteiligung von Nutzern, welche die zu standardisierende Technologie nutzen, können Standards entwickelt werden, die den Bedürfnissen der Nutzer am nächsten kommen („bottom up“-Entwicklung).

---

<sup>415</sup> Verschiedene Onlineprovider, wie AOL oder Microsoft bieten z.B. ihren Kunden das Emailsystem Instant Messaging an. Der Zugriff auf diese Systeme ist nur für die Kunden dieser Provider möglich. Andere Internetnutzer sind von dieser Möglichkeit der Emailversendung ausgeschlossen.

<sup>416</sup> Vgl. zum Ganzen Rutkowski, Standards, Kap. Internet Standards Making as a Model. Siehe auch RFC 2026, Bradner.

- Geleiteter Entwicklungsprozeß  
Standards werden in spezifischen Arbeitsgruppen entwickelt, welche jeweils von einem Vorsitzenden geleitet werden.
- Flexible Organisationsstruktur  
Die Struktur der Arbeitsgruppen ist nicht starr festgelegt, sondern einzelne Gruppen werden entsprechend den aktuellen Erfordernissen neu gegründet oder nach Erfüllung ihrer Aufgaben wieder aufgelöst.
- Annahmeerfordernis durch IAB und IESG  
Die entworfenen Internetstandards müssen durch das IAB und die IESG akzeptiert werden. Durch diese Prüfung erfolgt eine weitere Absicherung, daß der Standard wie vorgesehen funktioniert. Alle Standards werden zusätzlich durch die ISOC elektro-nisch und auf Papier veröffentlicht und erhalten somit eine zusätzliche Bestätigung.
- Sofortiger freier Zugang zu allen Materialen  
Die Internetstandards und die dazugehörenden Diskussionsbeiträge können über das Internet sofort eingesehen werden. Sie werden auf FTP- und WWW-Seiten zur Verfü-gung gestellt. Ein freier und offener Diskussionsprozeß ist damit sichergestellt.
- Aufbau einer Internetkultur  
Schließlich wird durch diesen offenen Standardisierungsprozeß eine eigene Internetkultur gefördert. Es entsteht ein familiäres Zusammengenährigkeitsgefühl, bei welchem kulturelle Unterschiede nur eine geringe Rolle spielen<sup>417</sup>. Dennoch dürfen die von den Internetingenieuren mitgebrachten kulturellen Grundverständnisse nicht außer Acht gelassen werden, da sie auch einen Faktor für die Produktivität und die Innovativität der Arbeitsgruppen darstellen.

#### **2.4.2. Vergabe der IP-Nummern durch ARIN, RIPE-NCC und APNIC**

Die Entwicklung von Standards und deren Implementation stellt nur eine Säule der Selbstregulierung im Internet dar. Obgleich die Standardsetzung das wichtigste Element der technisch-gesellschaftlichen Struktur des Internets darstellt, ist eine geordnete Verwaltung der den Standards zugrundeliegenden Protokollparameter und des Internetadreßraumes ein ebenso unverzichtbarer Bestandteil des Internetbetriebs. Diese Verwaltungstätigkeit stellt die zweite Säule der Selbstregulierung des Internets dar.

Die gesamte Verwaltung und die koordinierte Vergabe des Internetadreß- und -namensraumes gingen zunächst von der *Internet Assigned Numbers Authority* (IANA) aus. Die IANA hatte die einzelnen Verwaltungsaufgaben an verschiedene Organisationen verteilt und schon damals zwischen der Verwaltung des IP-Adreßraumes und des DNS unterschieden. Heute ist die

---

<sup>417</sup> Zu beachten ist jedoch, daß kulturelle Ansichten in Bezug auf technische Entwicklungen von sich aus nur eine geringe Bedeutung entfalten können.

## 2.4. Verwaltung des Internet

---

IANA ein Teil der ICANN und nimmt als technisches Organ nur noch die Zuweisung von Protokollparametern vor. Die von der IANA vorgenommenen Delegierungen haben auch heute noch bestand, obgleich inzwischen einige Erweiterungen erfolgten.

Die Delegierung der Verwaltung des IP-Adreßraumes richtet sich nach den Richtlinien des RFCs 2050. Die IP-Adressen werden entsprechend dieses Dokumentes nach folgenden Zielen verteilt<sup>418</sup>:

- 1) Conservation: Fair distribution of globally unique Internet address space according to the operational needs of the end-users and Internet Service Providers operating networks using this address space. Prevention of stockpiling in order to maximize the lifetime of the Internet address space.
- 2) Routability: Distribution of globally unique Internet addresses in a hierarchical manner, permitting the routing scalability of the addresses. This scalability is necessary to ensure proper operation of Internet routing, although it must be stressed that routability is in no way guaranteed with the allocation or assignment of IPv4 addresses.
- 3) Registration: Provision of a public registry documenting address space allocation and assignment. This is necessary to ensure uniqueness and to provide information for Internet trouble shooting at all levels.

Die Verwaltungshierarchie der IP-Adressen besteht aus drei untergeordneten Ebenen: der ICANN, den regionalen *Internet Registries* (IRs), und den lokalen IRs<sup>419</sup>. Die ICANN stellt die oberste Autorität über den Nummernraum des Internets dar. Sie weist Teile dieses Adreßraumes den regionalen IRs entsprechend dem aktuellen Bedarf zu. Die regionalen IRs operieren in einem großen geopolitischen Umfeld (zum Beispiel Kontinente) und sind in der ICANN durch die *Address Supporting Organization* (ASO) vertreten. Es existieren zur Zeit drei regionale IRs: *American Registry for Internet Numbers*<sup>420</sup> (ARIN) für Nordamerika, das *Réseau IP Européen – Network Coordination Center*<sup>421</sup> (RIPE-NCC) für Europa und das *Asia Pacific Network Information Center*<sup>422</sup> (APNIC) für die asiatisch-pazifische Region<sup>423</sup>. Die übrigbleibenden Gebiete werden von diesen drei vorhandenen *Registries* mit bearbeitet. Jedoch hat die ICANN dem *African Network Information Center*<sup>424</sup> (AfriNIC) und dem *Registro Regional de Direcciones IP Latinoamericano y Caribeño*<sup>425</sup> (LACNIC) einen Beobach-

---

<sup>418</sup> Siehe *RFC 2050*, Hubbart, Kap. 1. Introduction.

<sup>419</sup> Vgl. die Angaben in *RFC 2050*, Hubbart, Kap. 1. Introduction.

<sup>420</sup> Siehe <http://www.arin.net>.

<sup>421</sup> Siehe <http://www.ripe.net>.

<sup>422</sup> Siehe <http://www.arin.net>.

<sup>423</sup> Die letzteren beiden wurden vom InterNIC abgespalten um eigene Verwaltungsorganisationen für Europa und Asien zu schaffen, Völker/Weidert WRP 1997, 652, 653.

<sup>424</sup> Siehe <http://www.afrinic.org>.

<sup>425</sup> Siehe <http://www.lacnic.org>.

tungsstatus in der ASO zuerkannt<sup>426</sup>. Die regionalen IRs wurden unter der Autorität der IANA und durch einen Konsens in der Internetgemeinschaft gebildet. Die regionalen IRs haben die Arbeit der lokalen IRs zu koordinieren und vertreten diese öffentlich in ihrer Region. Ihr Wirkungskreis beschränkt sich gewöhnlich auf nationaler Ebene. In Deutschland obliegt die Verwaltung der Internetnummern dem *Deutschen Network Information Center (DENIC)*<sup>427</sup>.

*Internet Service Providers (ISPs)*, welche mehrere Verbindungen zum Internet unterhalten und keine vorgegebenen Datenrouten besitzen, können Blöcke von Internetadressen direkt von einer lokalen IR erhalten. Alle anderen sollten Adressblöcke direkt von ihren Zugangsprovidern zugewiesen bekommen, um das *Routing* im Internet zu erleichtern<sup>428</sup>. Die ISPs haben mit der Verwendung des zugewiesenen Adressraumes sparsam umzugehen und die Zuweisungen zu dokumentieren, um bei Anfrage der zuständigen IR die sorgfältige Verwendung nachweisen zu können. Bei der Verteilung und Verwendung der Adressen sind neue Routing-Technologien zu verwenden, um dem beschränkten Angebot an freien IPv4-Adressen gerecht zu werden. Zuweisungen an Endnutzer erfolgen mit der Maßgabe, daß diese Adressen nicht weiter delegiert, sondern nur intern verwendet werden. Die Anzahl der zugewiesenen Adressen sollte nicht mehr als das vierfache der aktuell benötigten Adressen und nicht mehr als das doppelte der voraussichtlich in einem Jahr benötigten Adressen betragen<sup>429</sup>. Die IANA (beziehungsweise ICANN) hat sich das Recht vorbehalten, IP-Adresszuweisungen für ungültig zu erklären, wenn die Voraussetzungen für die jeweils erfolgte Zuteilung nicht mehr existieren. Bevor eine Zuweisung an einen Endnutzer erfolgt, muß jede Nachfrage durch die jeweilige IR nach dem *Network Engineering Plan* des Nutzers beurteilt werden<sup>430</sup>. Dieser muß die erwartete Verwendungsrate von Adressen über einen angemessenen Zeitraum enthalten.

Da die regionalen *Registries* als Hauptfunktion die Verwaltung des IP-Adressraumes wahrnehmen, können sie für diesen Service eine Gebühr verlangen, die den Kosten der Dienstleistung entsprechen sollte. Die regionalen IRs können zusätzliche Richtlinien über die Verwendung der IP-Adressen verabschieden, nach denen sich die lokalen IRs sowie die ISPs zu richten haben<sup>431</sup>.

Schließlich haben betroffene Organisationen nach dem RFC 2050 das Recht, eine Beschwerde gegen die Entscheidungen der IRs einzureichen, wenn die IR ihre Aufgaben nicht korrekt wahrgenommen hat. Dazu hat die betroffene IR alle relevanten Dokumente der übergeordneten *Registry* zur Verfügung zu stellen. Nach ergebnisloser Überprüfung durch diese, kann

---

<sup>426</sup> Am 1. Oktober 2000 hat die ASO Kriterien für die Etablierung neuer regionaler IRs verabschiedet, siehe ICANN, ASO Recommendation Concerning Establishment of New Regional Internet Registries, <http://www.icann.org/aso/emerging-rirs-01oct00.htm>.

<sup>427</sup> Deren Homepage ist unter <http://www.denic.de> zu finden.

<sup>428</sup> RFC 2050, Hubbard, Kap. 2.1 Guidelines for Internet Service Providers (ISPs) enthält ausführliche Regeln, welche bei der Zuweisung von Adressen an ISPs zu beachten sind.

<sup>429</sup> Siehe RFC 2050, Hubbard, Kap. 3.1 Common Registry Requirements.

<sup>430</sup> Zu den Voraussetzungen der Vergabe von IP-Adressen siehe RFC 2050, Hubbard, Kap. 3.2 Network Engineering Plans und ff. Kap.

<sup>431</sup> Vgl. zum Ganzen: RFC 2050, Hubbard, Kap. 4. Operational Guidelines For Registries.

Rechtsbeschwerde an die IANA (beziehungsweise ICANN) zur endgültigen Entscheidung weitergeleitet werden.

### 2.4.3. Vergabe und Verwaltung der Domainnamen

Die Struktur und die Verwaltung des DNS ist 1994 im RFC 1591 beschrieben worden. Dabei wurde zwischen den gTLDs und den ccTLDs unterschieden. Darüber hinaus wurden im RFC 1591 Regelungen über die Einführung neuer TLDs, insbesondere von ccTLDs getroffen. Für die Koordination und das Management des *Domain Name System* war viele Jahre die IANA verantwortlich. Sie delegierte nicht nur die IP-Nummernvergabe, sondern auch die Administration der Vergabe und Eintragung der Domainnamen an sogenannte *Network Information Centers* (NICs)<sup>432</sup>. Da die Vergabe und die Verwaltung von Domainnamen die dritte wichtige Säule der Selbstregulierung des Internets darstellt, sollen in den folgenden Ausführungen die Vergabe- und Verwaltungsaufgaben der NICs beleuchtet werden. Des weiteren soll auf die Problematik bei der Einführung neuer ccTLDs eingegangen werden.

#### 2.4.3.1. Verwaltung und Vergabe von Domains unter gTLDs

Die TLDs .com, .net und .org werden auf Grund eines Vertrages mit der ICANN durch *VeriSign Global Registry Services* (Verisign) verwaltet<sup>433</sup>. Die Firma Verisign ist das derzeitige Dachunternehmen der Firma *Network Solutions, Inc.* (NSI). Im folgenden Text soll also weiterhin anstatt auf Verisign direkt auf NSI Bezug genommen werden.

NSI soll die *Registry* .org nur noch bis Ende 2002 weiterführen dürfen<sup>434</sup>. Die TLD .int ist nur für Organisationen zugänglich, welche durch internationale Verträge zwischen Regierungen gegründet worden und wird von der IANA verwaltet<sup>435</sup>. Die Verwaltung der TLD .gov wurde an die *US General Services Administration* delegiert<sup>436</sup>. Eine Registrierung unter .gov ist exklusiv nur Regierungsbehörden der USA gestattet. Die TLD .edu wird von dem nichtkommerziellen Konsortium *Educause* verwaltet<sup>437</sup>. Unter .edu können sich nur US-amerikanische Bildungseinrichtungen registrieren lassen. Die Verwaltung der TLD .mil erfolgt durch das *US Department of Defense* (US-DoD)<sup>438</sup>. Sie ist für das US-Militär reserviert.

---

<sup>432</sup> Siehe *RFC 1591*, Postel, Kap. 3. The Administration of Delegated Domains. Vgl. auch *Bettinger*, GRUR Int. 1997, 402, 404ff.

<sup>433</sup> Vgl. die Homepage von VeriSign Global Registry Services: <http://www.verisign-grs.com/>. Siehe auch *ICANN-Announcement*, ICANN and VeriSign Sign on the Dotted Line, 25. Mai 2001.

<sup>434</sup> Vgl. *ICANN*, ICANN Stockholm Meeting Topic: Referral of .org Issues to DNSO, 3. Juni 2001, <http://www.icann.org/stockholm/org-topic.htm>.

<sup>435</sup> Vgl. *IANA*, Root-Zone Whois Information - .gov Top-Level Domain, <http://www.iana.org/root-whois/int.htm>.

<sup>436</sup> Vgl. die Homepage des US General Services Administration NIC: <http://www.nic.gov/>. Siehe auch *IANA*, Root-Zone Whois Information - .gov Top-Level Domain, <http://www.iana.org/root-whois/gov.htm>.

<sup>437</sup> Siehe Educause, <http://www.educause.edu/edudomain/> verwaltet. Zu .edu vgl. auch den Beschuß des *US-DoC, NTIA*, Cooperative Agreement with EDUCAUSE.

<sup>438</sup> Vgl. *RFC 1956*, Engebretson/Plzak. Siehe auch *IANA*, Root-Zone Whois Information - .mil Top-Level Domain, <http://www.iana.org/root-whois/mil.htm>.

Ursprünglich erfolgte nach dem RFC 1591 die Verwaltung der gTLDs .com, .net und .org weltweit durch das *Internet Network Information Center* (InterNIC). Das InterNIC war zu Beginn eine Institution amerikanischer Universitäten. Die Trägerschaft und Rechtsform des InterNIC wurde jedoch in den letzten Jahren mehrfach verändert. Zuletzt stellte das InterNIC eine Kooperation aus der NSF, der Telefongesellschaft AT&T, Inc.<sup>439</sup>; und des Internetproviders NSI dar. Die Finanzierung erfolgte größtenteils durch die US-Regierung. NSI, als Hauptbetreiber des InterNIC verwaltete neben der zentralen Rootdatenbank auch die *Registry* für die gTLDs .com, .net und .org<sup>440</sup>. Alle anderen *Name Server* verwiesen auf diese Hauptdatenbanken zur Abgleichung ihres Datenbestandes. NSI behauptete immer, daß man ihr die Verantwortung übertragen habe, obwohl unklar war, ob überhaupt jemand die Verantwortung über das DNS jemandem Dritten übertragen konnte. NSI trat als Betreiber der *Registry* für die wichtigsten gTLDs und auch als alleiniger *Registrar* für diese auf. Alle Interessenten an einem Domainnamen unter einer gTLD waren gezwungen, diesen bei NSI zu reservieren. Ein freier Wettbewerb fand nicht statt und war der Anlaß für eine Vielzahl von Reformversuchen bezüglich des DNS. Durch das auf Bestreben der ICANN eingeführte *Shared Registry Systems* (nähere Ausführungen erfolgen im Kapitel 3.3.2) erfolgt inzwischen die Domainvergabe unter der gTLD .com und anderer gTLDs durch eine Vielzahl von NSI unabhängiger Unternehmen.

Hierbei sind die Funktionen der *Registries* klar von den Funktionen der sogenannten *Registrars* zu trennen. Während die *Registries* die Datenbanken für die jeweiligen TLDs zu betreiben haben, registrieren die *Registrars* die einzelnen Domainnamen, in dem sie Verträge mit Endkunden (den zukünftigen Domaininhabern) schließen und die jeweiligen TLDs vermarkten<sup>441</sup>. Innerhalb nationaler TLDs werden die Funktionen von *Registry* und *Registrar* noch häufig durch ein Unternehmen wahrgenommen.

Das InterNIC vergab die Domainnamen ursprünglich gebührenfrei. Da eine Doppelvergabe technisch nicht möglich ist, wurde das sogenannte Prinzip „first come, first served“ angewendet. Das heißt, die Person, welche einen Namen zuerst zur Registrierung anmeldete, erhielt diesen. Ein Name durfte, wie auch heute noch nicht länger als 256 Zeichen sein und außer Buchstaben, Zahlen und Bindestrichen keine weiteren Zeichen enthalten. Eine Pflicht zur Nutzung der registrierten Domainnamen bestand nicht. Diesen Umstand nutzten sogenannte *Domain Grabber* aus, um Namen und berühmte Marken verschiedener Unternehmen zu registrieren. Viele Unternehmen war es deshalb verwehrt, ihren eigenen Namen zu reservie-

---

<sup>439</sup> Siehe zur AT&T, Inc.: <http://www.att.com>.

<sup>440</sup> Wenning, JurPC Web-Doc 31/1998, Abs. 2.

<sup>441</sup> Eine gesetzliche Definition von Registry und Registrar erfolgt durch die EU-Verordnung zur Einführung der Domäne oberster Stufe „.eu“: „[Registry]: die Einrichtung, die mit der Organisation und Verwaltung der [jeweiligen] TLD [...], einschließlich der Wartung der entsprechenden Datenbanken und der damit verbundenen öffentlichen Abfragedienste, der Registrierung von Domänennamen, des Betriebs des Domänenamensregisters, des Betriebs der Namens-Server [...] für die TLD und der Verbreitung der TLD-Zonendateien betraut wird; [Registrar]: eine Person oder Einrichtung, die durch Vertrag mit [der Registry] die Registrierung von Domänennamen für Registrierungsbewerber vornimmt“; siehe Fn. 781.

ren<sup>442</sup>. Diese extensive Nutzung des DNS führte zu einem drastisch Anstieg der Reservierungen von Domainnamen<sup>443</sup>.

Um einen weiteren Mißbrauch zu verhindern, wurde seit Juli 1995 vom InterNIC eine einmalige Registrierungsgebühr in Höhe von 100 US\$ sowie eine jährliche Verlängerungsgebühr von 50 US\$ verlangt. Diese Gebühr mußte bis zum Ablauf von zwei Monaten nach Fälligkeit gezahlt werden, sonst wurde die Registrierung des Domainnamens aufgehoben. Auf Grund des eingeführten Wettbewerbs ist der Preis für einen Domainnamen inzwischen auf unter 10 US\$ gefallen. Um die Verletzung fremder Marken- und Kennzeichenrechte zu vermeiden, führte NSI zusätzlich ein *Domain Name Dispute Policy Statement* ein (siehe Kapitel 3.3.1.1 unten). Diese Regelung ist inzwischen durch ein außergerichtliches Streitschlichtungsverfahren nach der *Universal Domain Name Dispute Resolution Policy* (UDRP) abgelöst worden (siehe Kapitel 3.3.1.2 unten).

### 2.4.3.2. Delegation neuer ccTLDs

Auf der Seite des national betriebenen DNS existieren derzeit über 100 landesspezifische TLDs. Jedoch werden bislang nicht unter allen nach der ISO-3166-Norm möglichen Landeskennungen entsprechende TLDs betrieben. Folglich können sich für die noch freien TLDs die jeweilig korrespondierenden Länder bewerben. Die IANA weißt dabei jede Entscheidungsgewalt von sich, zu bestimmen, ob ein Land völkerrechtlich anerkannt ist<sup>444</sup>. Vielmehr wird durchweg auf einen Eintrag in der ISO-3166-Liste abgestellt. Die Auswahl der ISO-3166-Liste als Basis für die ccTLDs wurde getroffen, da die ISO selbst ein bewährtes Verfahren hat, um zu entscheiden, welche staatliche Einheit in die Liste aufgenommen werden sollte.

Eine neue TLD wird gewöhnlich von der IANA eingerichtet und das Management als Ganzes an einen *designated Manager* übertragen. Die Voraussetzungen werden im RFC 1591 näher erläutert. So hat der *designated Manager* die Domainvergabe zu überwachen und das landesspezifische DNS zu betreiben. Er tritt als Treuhänder der ccTLD für sein Land und für die Internetgemeinschaft auf. Er hat alle Antragsteller eines Domainnamens gleich zu behandeln. Das heißt, daß die gleichen Regeln für alle Anfragen anzuwenden sind. Die Nachfragen müssen in einer nichtdiskriminierenden Weise behandelt werden, insbesondere stehen kommerzielle und akademische Nutzer auf gleicher Stufe. Alle wichtigen Parteien sollen der Auswahl eines bestimmten *designated Manager* zustimmen und die weiteren Handlungen sollen im Einvernehmen mit diesen relevanten Interessensvertretern erfolgen. Die technische Arbeit bezüglich des Betriebs des DNS soll für die Internetgemeinschaft in

---

<sup>442</sup> Bettinger, GRUR Int. 1997, 402, 406.

<sup>443</sup> Veranschaulicht wird die Nutzung des DNS mittels des monatlichen DNS-Hostcountes des RIPE, Monthly host progression, <ftp://ftp.ripe.net/ripe/hostcount/RIPE-Hostcount-Mo.gif>.

<sup>444</sup> Siehe RFC 1591, Postel, Kap. 4. Rights to Names, Kap. 2) Country Codes: „The IANA is not in the business of deciding what is and what is not a country.“

zufriedenstellender Weise erfolgen. Vor jeder Übertragung von Aufgaben von einem *designated Manager* an eine neue Betreiberorganisation soll die IANA konsultiert werden.

#### 2.4.3.3. Die deutsche TLD .de

Das RIPE NCC wurde ursprünglich vom InterNIC beauftragt, die Länder-Domainnamen für den europäischen Raum zu verwalten. Da jedoch die Nachfrage nach neuen Domains Ende der achtziger Jahre immer stärker zunahm, wurde die Domainvergabe nach Ländern untergliedert und auf nationale NICs übertragen, die vorrangig von wissenschaftlichen Einrichtungen betrieben wurden. Die Verwaltung der .de TLD oblag der zuerst an der *Universität Dortmund* ansässigen Institution DENIC<sup>445</sup>. Nach einer Ausschreibung übernahm 1994 das Rechenzentrum der *Universität Karlsruhe* die technische Betreibung des DENIC<sup>446</sup>, wobei die Verwaltung seit 1. Januar 1994 durch den *Interessenverband Deutsches Network Information Center* (IV-DENIC) durchgeführt wird<sup>447</sup>. Zu diesem Verband haben sich viele große deutsche Internetprovider zusammengeschlossen. Insgesamt sind es momentan 154 Mitglieder<sup>448</sup>. Aus dem IV-DENIC ging wiederum die *DENIC Domain Verwaltungs- und Betriebsgesellschaft eG, Frankfurt a.M.*, kurz DENIC eG hervor, welche seit dem 29. September 1997 als Genossenschaft eingetragen ist<sup>449</sup> und ab diesem Zeitpunkt das DENIC verwaltet. Der Vertrag mit der *Universität Karlsruhe* wurde am 1. Januar 1997 neu geschlossen und lief Ende 1998 aus. Seit diesem Zeitpunkt werden auch die technischen Geräte durch die DENIC eG selbst betrieben<sup>450</sup>.

Wie bei der Vergabe von Domainnamen unterhalb von internationalen TLDs erfolgt beim DENIC die Vergabe nach dem Prinzip „first come, first served“, ohne daß eine Kollisionsprüfung auf bestehende Kennzeichenrechte erfolgt. Auch in Deutschland sind Gebühren für die Registrierung zu entrichten<sup>451</sup>. Diese sind jedoch im internationalen Vergleich um ein Vielfaches höher. Um ein Zurücknehmen der Registrierung zu verhindern, müssen diese Gebühren ebenfalls rechtzeitig beglichen werden. Der Antragsteller ist nach den Regeln der DENIC selbst für die Einhaltung fremder Namensrechte verantwortlich<sup>452</sup>. Dabei versichert er, daß er keine Rechte Dritter wissentlich verletzt und verpflichtet sich, Streitigkeiten um eingetragene oder geschützte Namen zu beheben. In den Richtlinien wird erklärt, daß das DENIC nicht für

---

<sup>445</sup> Kilian, DZWir 1997 381, 383. Die Homepage des DENIC ist unter <http://www.denic.de> zu finden.

<sup>446</sup> Koch, Internet-Recht, S. 577; Bettinger, GRUR Int. 1997, 402, 404ff.

<sup>447</sup> Hoeren, Rechtsfragen des Internet, Rdnr. 48.

<sup>448</sup> Stand 1. September 2001. Im Internet läßt sich die Entwicklung der Mitgliederzahl über die letzten Jahre gut unter <http://www.denic.de/doc/DENIC/mitgliedszahlen.html> verfolgen.

<sup>449</sup> Die aktuelle Satzung vom 25. April 2001 kann unter <http://www.denic.de/doc/DENIC/statuten.html> eingesehen werden.

<sup>450</sup> Hoeren, Rechtsfragen des Internet, Rdnr. 48.

<sup>451</sup> Derzeit kostet eine Registrierung einer Domain direkt beim DENIC 116,- Euro. Vgl. die aktuelle Preisliste des DENIC: <http://www.denic.de/DENICdb/domainreg/DENICdirect/preisliste.html>.

<sup>452</sup> Vgl. *DENIC eG*, DENIC-Registrierungsrichtlinien, 15. August 2000, <http://www.denic.de/doc/faq/vergaberichtlinie.html>.

## 2.4. Verwaltung des Internet

---

Namenskonflikte verantwortlich gemacht werden kann<sup>453</sup>. Eine dem *Domain Name Dispute Policy Statement* entsprechende Widerspruchsmöglichkeit besteht noch nicht.

---

<sup>453</sup> DENIC eG, DENIC-Registrierungsrichtlinien, Fn. 452.

*Although cyberspace is no longer populated by a small group of like-minded individuals, traditions of openness, consensus, trust, and legitimacy still pervade the thoughts and actions of many Internet stakeholders and can help to unify a variety of Internet interests*

– Harvard Law Review Association –

*Inshort, ICANN should be as non-exclusionary, non-coercive, non-governmental, non-hierarchical, non-adversarial and decentralized as the internet itself.*

– David R. Johnson and Susan P. Crawford – The Idea of ICANN –

*Was ist ICANN, die „Internet Corporation for Assigned Names and Numbers“? Eine Art Internet-UNO? Nein! Ein Welt-Unternehmen? Nein! Eine NGO? Auch nicht. ICANN, oft fälschlicherweise als die „Weltregierung des Internet“ apostrophiert, ist eine „private nicht-kommerzielle Gesellschaft unter kalifornischem Recht“.*

– Wolfgang Kleinwächter – ICANN: „Blaupause“ für ein neues Politikmodell? –

## 3. ICANN als neue Verwaltungsstruktur

Im folgenden Kapitel soll auf die ICANN als eine der für das Internet bedeutendsten Organisation eingegangen werden. Die ICANN erhält in letzter Zeit eine hohe Aufmerksamkeit seitens der Politik und der Wirtschaft durch die Einführung eines außergerichtlichen Streitschlichtungsverfahrens und der kürzlich erfolgten Einführung neuer TLDs. Stark umstritten ist auch die von vielen staatlichen Regierungen gewünschte Beteiligung an Entscheidungen der ICANN. Um die Organisation und die Funktion der ICANN zu verstehen, wird zunächst auf die Entwicklung eingegangen und die Hintergründe der Bildung dieser neuen Organisation dargestellt. Daraufhin wird auf die Struktur und Arbeitsweise der ICANN eingegangen und spezielle Leistungen gesondert hervorgehoben.

### 3.1. Geschichtlicher Hintergrund der ICANN

In den Anfangsjahren des Internet von 1982 bis 1994 hatte das DNS keine öffentliche Bedeutung. Wie schon erwähnt, war das in den USA beheimatete und noch sehr kleine Computernetzwerk für die Öffentlichkeit und die Wirtschaft nicht zugänglich gewesen. Nur Wissenschaftler verschiedener US-amerikanischer Universitäten hatten eine Anbindung. Als ARPA-Net wurde es vom US-Militär und später als *NSFNet Backbone* durch die NSF finanziert.

### 3.1. Geschichtlicher Hintergrund der ICANN

---

Staatliche Behörden hatten die zentrale Koordinationsposition inne. Die Aufgaben wurden zum Teil an privatrechtliche Vertragspartner delegiert (zum Beispiel an die NSI). Die Namens- und Adreßzuweisung, als eigentliche staatliche Verwaltungstätigkeit, wurde vertraglich durch private Unternehmen wahrgenommen. Institutionelle Streitigkeiten und Probleme gab es angesichts des geringen Wachstums des DNS (zum Beispiel im Jahre 1991 nur 645 registrierte SLDs<sup>454</sup>) nicht. Die seit 1992 eingeleitete Privatisierung durch das NSF führte 1995 schließlich zur Schließung des *NSFNet Backbone* und der Übernahme durch private Telekommunikationsunternehmen<sup>455</sup>. Das Jahr 1995 war schließlich eines der bedeutendsten für das Internet. Mit der Verbreitung von WWW-Anwendungen (*Mosaic Browser* oder *Netscape Navigator*) ging eine explosionsartige Verbreitung an Webseiten einher. Um diese zu hosten wurde eine Vielzahl neuer Domainnamen benötigt. Wenn 1992 weltweit nur 300 neue SLDs registriert wurden, waren dies 1995 schon 45.000 je Monat und 1996 kamen 637.000 neue SLDs hinzu. 60% liefen davon unter der TLD .com. Inzwischen wurde die Registrierung von Domainnamen und die Verwaltung der Rootdatenbank von gTLDs durch die Firma NSI wahrgenommen. Die NSI war Vertragspartner der US-Regierung<sup>456</sup>. Die Registrierungskosten übernahmen die amerikanischen Steuerzahler. Mit dem immer stärkeren Einfluß der Wirtschaft im Internet war eine Beihilfe nicht mehr erforderlich. Unter Abstimmung mit der NSF mittels des *Amendment No. 4* des *Cooperative Agreement*<sup>457</sup> erhob NSI seit 1995 eine Registrierungsgebühr von 50 US\$, von denen sie 35 US\$ einbehält und 15 US\$ zur Förderung weiterer Internetprojekte an die NSF weiterreichte<sup>458</sup>. Die *Registries* der verschiedenen ccTLDs verlangten zur Deckung der Kosten schon seit langem recht hohe Gebühren. Für alle wurde die Registrierung von Domainnamen zum Millionengeschäft. Insbesondere die NSI erhielt durch ihren Vertrag mit der US-Regierung ein staatlich geschütztes Monopol<sup>459</sup> an einem sehr lukrativen Geschäft.

Ursprünglich stellten die Domainnamen nur eine anwenderfreundliche Form einer Computeradresse dar. Das DNS sollte die schlecht einprägsamen IP-Adressen in leicht merkbare alphanumerische Zeichenketten umsetzen. Im wirtschaftlichen Umfeld wurden die Domainnamen jedoch schnell als Marketingwerkzeug eingesetzt. Immer mehr Unternehmen erkannten, daß sie recht einfach unter www.unternehmensnamen.com gefunden werden konnten. Die SLDs

---

<sup>454</sup> Vgl. *Mueller*, 5 Int. J. Com. L. & Pol'y, Web-Doc 1, 8.

<sup>455</sup> Vgl. *Mueller*, 5 Int. J. Com. L. & Pol'y, Web-Doc 1, 8.

<sup>456</sup> Siehe das Cooperative Agreement zwischen *NSI* und der *US-Regierung* sowie die zugehörigen Amendments unter [http://www.networksolutions.com/en\\_US/legal/internic/cooperative-agreement](http://www.networksolutions.com/en_US/legal/internic/cooperative-agreement).

<sup>457</sup> Siehe *NSI*, Cooperative Agreement, Amendment No. 4,

[http://www.networksolutions.com/en\\_US/legal/internic/cooperative-agreement/amendment4.html](http://www.networksolutions.com/en_US/legal/internic/cooperative-agreement/amendment4.html).

<sup>458</sup> In *U.S. District Court, Columbia Circuit* vom 8. Juli 1999, *Thomas vs. NSI und NSF*, 176 F.3d 500 wurde der Einzug dieser 15 US\$ als mit dem Independent Offices Appropriation Act unvereinbar und für rechtswidrig erklärt.

<sup>459</sup> Siehe *U.S. Court of Appeals, Second Circuit* vom 21. Januar 2000, *Name.Space, Inc. v. NSI und NSF*, 202 F.3d 573.

wurden zu einer Handelsware, vertrieben über Domainbörsen und Auktionen<sup>460</sup>. Viele sogenannte Namensspekulanten und *Domain Grabber* versuchten durch massenhaftes Reservieren von Allgemeinbegriffen und Markennamen an diesem Geschäft teilzunehmen. Andererseits versuchten einige Großunternehmen legitime Domainbesitzer durch Androhung von Klagen mit hohem Streitwert zur Übertragung der SLD an sie zu erpressen<sup>461</sup>. Um selbst rechtlichen Streitigkeiten zu umgehen und nicht für Markenverletzungen als mitverantwortlich verurteilt zu werden, führte die NSI im Juni 1995 ihre *Dispute Policy* ein (siehe Kapitel 3.3.1.1 unten). Diese ermöglichte die vorläufige Löschung vieler .com, .net und .org Adressen aus der Root-datenbank. Über die Anzahl der gesperrten Domains liegt allerdings kein Bericht seitens der NSI vor. Auch ist nicht nachvollziehbar, wie streng diese Politik angewendet wurde<sup>462</sup>.

Der ökonomische Wert eines Domainnamens ist vom *Root Server System* abhängig. Er ergibt sich aus der weltweiten Erreichbarkeit, solange ein koordinierter autoritativer *Root Server* existiert, auf welchen alle anderen *Root Server* verweisen. Dieser sogenannte *A Root Server* steht unter der Aufsicht der US-Regierung<sup>463</sup> (aktuell dem *Department of Commerce*) und wird durch die NSI verwaltet. Dieser *Root Server* wird von den meisten ISPs als alleinige Autorität angesehen. Obgleich der Aufbau alternativer Systeme ohne weiteres möglich ist, sind diese und die zusätzlich eingeführten TLDs ohne Anbindung an das *Root Server System* von der NSI für den größten Teil der Internetnutzer unsichtbar. Mehrere selbständige Systeme stellen zusätzlich ein hohes Risiko einer Fragmentierung des Internets dar, sollten sich die Betreiber nicht untereinander abstimmen, nicht gegenseitig aufeinander verweisen oder gar TLDs doppelt vergeben. Die Domainnamen würden damit an ihrer Einzigartigkeit und somit an Wert verlieren.

---

<sup>460</sup> Siehe die Handelspreise für diverse Verkäufe von SLDs unter *Mueller*, 5 Int. J. Com. L. & Pol'y, Web-Doc 1, 9.

<sup>461</sup> Sogenanntes Reverse Domain Name Highjacking. In einem der letzten Fälle versuchte die Deutsche Welle über die Schiedsprozedur der WIPO die Adresse dw.com freizuklagen. Dieses Ansinnen wurde jedoch von den Schiedsrichtern als böswille Anrufung des Schiedsgerichtes zurückgewiesen, siehe *Heise-Newsticker*, WIPO rügt Deutsche Welle wegen Reverse Domain Hijacking, 20. Januar 2001. Auch versuchte die Firma Ferrero Österreich bislang erfolglos die Adresse Kinder.at freizuklagen unter welcher ein WWW-Portal mit Kinderinhalten entstehen soll, siehe Beschuß des Handelgerichts Wien, AZ: 38 Cg 90/001, <http://www.kinder.at/beschluss.pdf> und das Urteil vom 10. Dezember 2001, <http://www.kinder.at/urteil20011210.PDF> sowie *Heise-Newsticker*, Rückschlag für Ferrero im „kinder.at“-Markenstreit, 15. Januar 2001 und *Heise-Newsticker*, Niederlage für Ferrero im Streit um "Kinder.at", 18. Dezember 2001.

<sup>462</sup> Im Oktober 1996 hätte die Anwendung der Dispute Policy durch NSI auf juno.com, ein kostenloser Email-service der Firma Juno Online zur Löschung einer halben Million Email Accounts geführt. NSI versprach vor Gericht, die Adresse juno.com nicht zu blockieren, die von Juno Online angestrebte einstweilige Verfügung gegen NSI wurde abgelehnt. Vgl., *U.S. District Court, Northern District of Illinois* vom 29. September 1997, *Juno Online Services v. Juno Lighting, Inc.*, 979 F.Supp. 684 und *U.S. District Court, Eastern District of Virginia* vom 18. Oktober 1996, *Juno Online Services, L.P. v. Juno Lighting, Inc and Network Solutions, Inc.*, <http://www.patents.com/juno/juno.sht>. Nähere Ausführungen zum Fall siehe *Rony/Rony*, Domain Name Handbook, S. 407ff.

<sup>463</sup> Siehe *US-GAO*, Report, S. 8f.

#### 3.1.1. Notwendigkeit einer Strukturreform

Das lange Zeit unter der IANA bestehende Verwaltungssystem des DNS wies allerdings aus politischer Sicht einige Mängel auf. Zum einen gab es immer wieder Proteste gegen das monopolartige Betreiben des DNS durch die NSI. Zum anderen wollten weitere Firmen in das lukrative Geschäft der Domainvergabe einsteigen<sup>464</sup>. Außerdem erschienen die 35 US\$ Gebühr, welche NSI zuflossen, nicht durch den geringen Aufwand einer Domainregistrierung gerechtfertigt. Durch die maßlose Ausuferung an Reservierungen während der letzten Jahre waren freie Domainadressen recht knapp geworden. Viele unbenutzte Namen waren derzeit (und sind es auch heute noch) durch *Domain Grabber* reserviert, welche hofften, diese meistbietend verkaufen zu können. Nur die Einführung neuer TLDs hätte dieser Knappheit Abhilfe verschaffen können, obgleich sich Markeninhaber dann noch häufiger<sup>465</sup> gegen die Reservierung ihrer Markennamen als Domainnamen gerichtlich zu wehren hätten<sup>466</sup>.

Bei der damaligen (und auch noch gegenwärtigen) Krise handelte es sich folglich nicht um eine technisch bedingte. Man hätte ohne technische Schwierigkeiten viele weitere TLDs dem derzeitigen System hinzufügen und auch Alternativen zum DNS schaffen können. Es lag vielmehr eine institutionelle und politische Krise vor, welcher die ursprüngliche Organisationsstruktur der Nummern- und Namensverwaltung nicht mehr gerecht werden konnte<sup>467</sup>. Die Ansichten wie das DNS reformiert werden sollten, klafften zum Teil wie eine Schere auseinander. Die Einführung neuer TLDs wurde sehr restriktiv gehandhabt (siehe Kapitel 3.3.2 unten) und es wurde versucht, jegliche Dezentralisierungsversuche des DNS (wie zum Beispiel die alternativen DNS-Systeme von Alternic<sup>468</sup> oder Name.Space<sup>469</sup>) zu mißachten oder gar im Keime zu ersticken (siehe Kapitel 5.1 unten). Dieses Prinzip der „verteilten Entwicklung und Verantwortung“ hatte jedoch erst den Aufschwung des Internets ermöglicht (siehe Kapitel 2.4.1.3.4 oben). Die Markenrechtslobby plädierte zudem, die Anzahl neuer TLDs möglichst gering zu halten, da sie viele neue Streitigkeiten um Namen fürchtete. Es wurde damit eine künstliche Knappheit an Namensraum erzeugt, der weder der nichttechnischen Welt entsprach, noch durch die Technik selbst bedingt war<sup>470</sup>. Hätte man frühzeitig dezentrale Regis-

---

<sup>464</sup> Siehe die Name.Space, Inc. v. NSI und NSF, Fn. 459.

<sup>465</sup> Siehe z.B. die Entscheidungssammlung von Strömer Rechtsanwälte unter *NetLaw*, Entscheidungssammlung Online-Recht, <http://www.netlaw.de/urteile/index.html> und von *Rony/Rony*, Domain Name Handbook, <http://www.domainhandbook.com/dd.html>.

<sup>466</sup> Dabei gehen sie oft über das Ziel des Markenschutzes hinaus und nehmen auch rechtmäßige Verwender von Namen, so z.B. Fanseiten oder Protestseiten, auf Übertragung der Domain in Anspruch; vgl. *Heise-Newsticker*, AOL Time Warner gegen Harry Porter Fanseiten, Warner lenkt im Streit um Harry-Potter-Sites ein, 19. März 2001; siehe auch Walmart gegen Walmartsucks, *Simon*, Telepolis 8447.

<sup>467</sup> So auch *Recke*, DNS, Kap. Was ist eigentlich das Problem?

<sup>468</sup> Siehe <http://www.alternic.org>.

<sup>469</sup> Siehe <http://www.namespace.org>.

<sup>470</sup> Ein Name kann in der untechnischen Welt mehrfach verwendet werden, ohne daß es zu Überschneidungen kommen kann. Eine SLD kann unter einer TLD nur einmal vergeben werden, so daß alle anderen Interessenten für diesen Namen leer ausgehen. Jedoch ist es technisch ohne Probleme machbar, viele hundert TLDs gleichzeitig einzuführen, unter denen die einzelnen Interessenten die Möglichkeit haben, unter ihrem eigenen Namen aufzutreten.

*tries* geschaffen, ohne der Firma NSI die alleinige Verwaltungsmacht über die gTLDs zu übertragen, wäre der enorme kommerzielle Wert, den eine Namens-*Registry* heute darstellt, nicht entstanden. Folgende Probleme bei der Einführung neuer TLDs stellen sich bislang<sup>471</sup>:

- Wer hat die Autorität über den *A Root Server*?
- Wieviele neue TLDs sollten dem DNS hinzugefügt werden?
- Nach welchen Kriterien sollten neue TLDs geschaffen werden?
- Wer sollte eine neue TLD verwalten dürfen, wer nicht? Kann die Registrierung und Verwaltung der Domainnamen im Wettbewerb durchgeführt werden?
- Wieviele neue *Registries/ Registrars* sollte es geben und sollten diese als profitable oder als *non-profit*-Unternehmen geführt werden?
- Kann geistiges Eigentum an einer Zeichenkette innerhalb einer TLD entstehen?
- Sollen die *Registrars* allein Domainnamen einer bestimmten TLD registrieren dürfen, oder müssen sie der Konkurrenz Zugang gewähren?
- Gehört den *Registries* die Datenbank der Domainnamen unter der jeweiligen TLD?
- Wie soll verfahren werden, wenn ein Unternehmen unter einer TLD, registriert und ein erfolgreiches Angebot entwickelt hat, jedoch eine konkurrierende Firma den gleichen Namen unter einer anderen TLD registrieren will?

Die Hauptziele einer Reform des DNS sollten ein offener und freier Markt sowie ein Wettbewerb unter den *Internet Registries* schaffen. Ein in der Internetgemeinde üblicher *rough consensus* bezüglich eines neuen Systems konnte sich jedoch bis Herbst 1996 nicht herausbilden. Zu viele gegensätzliche Positionen wurden durch die inzwischen stark angewachsenen Interessensgruppierungen vertreten<sup>472</sup>. Das Standardsetzungsmodell des Internets (vgl. Kapitel 2.4.1.3 oben) schien zu versagen.

### 3.1.2. Von der IANA zur ICANN

Es gab mehrere Versuche die Organisationsstrukturen im Internet zu reformieren. So wurde 1994 versucht, die Funktion der IANA auf die ISOC zu übertragen. Dr. Jon Postel schlug 1995 die Einführung einer Vielzahl neuer TLDs vor, konnte sich aber nicht gegen den Widerstand der inzwischen auf das Internet aufmerksam gewordenen Markenrechtslobby durchsetzen. Ein etwas später ins Leben gerufenes Projekt namens *International Ad Hoc Committee* (IAHC) scheiterte an der strikten Ablehnung durch die Regierung der USA, welche sich insbesondere gegen die Teilnahme der internationalen Organisation ITU sträubte. Der von ihr in Gang gesetzte Diskussionsprozeß führte schließlich im September 1998 zur Gründung der ICANN. Da auf die Hintergründe der fehlgeschlagenen Umstrukturierungsversuche in der deutschen Literatur kaum eingegangen wurde, möchte ich diese im Folgenden aufzeigen.

---

<sup>471</sup> Siehe *Mueller*, 5 Int. J. Com. L. & Pol'y, Web-Doc 1, 12 und *Recke*, DNS, Kap. Die aktuelle Debatte um die Zukunft des DNS.

<sup>472</sup> Vgl. auch *Recke*, DNS, Kap. Die aktuelle Debatte um die Zukunft des DNS.

#### 3.1.2.1. 1994 – Versuch der Übertragung der IANA Aufgaben an die ISOC

Die IANA-Funktionen wurden ursprünglich unter Vertrag mit der US-Regierung<sup>473</sup> durch das USC-ISI wahrgenommen. Dr. Jon Postel schlug allerdings schon im Juli 1994 vor, diese Funktionen der ISOC zu übertragen. Dazu entwarf er eine Satzung der IANA und stellte sie auf übliche Weise zur Diskussion<sup>474</sup>:

Die IANA sollte damit auf die Basis einer sicheren und unabhängigen Finanzierung gestellt werden und einen rechtlichen Rahmen erhalten<sup>475</sup>. Postels Vorschlag führte jedoch zu einer heftigen Debatte in den US-amerikanischen Regierungsbehörden, ob die ISOC die Jurisdiktion und die Verantwortung über das Namens- und Adreßsystem besitzt. Zwar beanspruchte die ISOC ein Recht an einer Kontrolle der IANA. Es existierte jedoch keine rechtliche Grundlage, die eine Übertragung der Aufgaben der IANA auf sie rechtfertigen konnte. Zu diesem Zeitpunkt war es stark umstritten, wer die Autorität über das DNS innehatte. Dr. Jon Postel konnte für die Übertragung der IANA-Aufgaben auf die ISOC keinen Konsens finden<sup>476</sup>. Die Diskussion hatte zwar keine weiteren Auswirkungen auf die Verteilung der Autorität über die IANA, führte jedoch dazu, daß die IANA sich in RFCs auf eine Gründung durch die ISOC berief<sup>477</sup>.

#### 3.1.2.2. Dr. Jon Postels Vorschlag von 150 neuen TLDs

Ein Fünfjahres-Vertrag mit der NSF von 1993 gab der NSI die Autorität über das InterNIC<sup>478</sup>. Dies beinhaltete die Kontrolle über den Sitz der *Domain Name Registry* für die meisten gTLDs und über das maßgebliche *Root Server System*. Die NSI stellte im Gegensatz zu den anderen im Internet engagierten Organisationen ein kommerzielles und profitorientiertes Unternehmen dar. Dieses Unternehmen war nicht wie die IANA oder IETF mit der Internetgemeinschaft verbunden. Am 13. September 1995 schlossen die NSF und die NSI eine Erweiterung ihres Vertrages ab (*Amendment No. 4*<sup>479</sup>), die der NSI erlaubte, für die Registrierung und Verwaltung der Domainnamen eine Gebühr zu verlangen. Die wirtschaftliche Ausnutzung der Registrierung von Domainnamen führte zu einer strikten Ablehnung der NSI durch die traditionelle Internetgemeinschaft. Dr. Jon Postel schlug daraufhin die Erweiterung der gTLDs und die Einführung konkurrierender *Internet Registries* mit folgenden Argumenten vor<sup>480</sup>:

---

<sup>473</sup> Siehe *US-GAO*, Report, S. 5.

<sup>474</sup> IANA Charter: „[...] The Internet Assigned Numbers Authority (IANA) is chartered by the Internet Society to act as the clearinghouse to assign and coordinate the use of numerous Internet protocol parameters [...].“ Eine Kopie der IANA Charter ist auf Rutkowskis Webseite <http://www.wia.org/pub/postel-iana-draft1.htm> zu finden.

<sup>475</sup> Vgl. *Mueller*, 5 Int. J. Com. L. & Pol'y, Web-Doc 1, 14 und *Mueller*, 1 info 6, 497, 500.

<sup>476</sup> Siehe die verschiedenen Diskussionsdokumente, welche durch Rutkowski unter <http://www.wia.org/> archiviert und erläutert werden.

<sup>477</sup> *Rony/Rony*, Domain Name Handbook, S. 120ff. gehen sehr ausführlich auf das Verhältnis der IANA zur ISOC ein.

<sup>478</sup> Siehe das Cooperative Agreement zwischen *NSI* und der *US-Regierung*, Fn. 456.

<sup>479</sup> Siehe *NSI*, Cooperative Agreement, Amendment No. 4, Fn. 457.

<sup>480</sup> Email vom 15. September 1995 von Postel an die ISOC Trustees. Archiviert unter <http://www.wia.org/pub/postel-iana-draft13.htm>.

I think this introduction of charging by the Internic for domain registrations is sufficient cause to take steps to set up a small number of alternate top level domains managed by other registration centers.

I'd like to see some competition between registration services to encourage good service at low prices.

Dazu entwarf er einen RFC zur Einführung von 150 neuen und beschreibenden gTLDs über den Zeitraum von drei Jahren<sup>481</sup>. Diese TLDs sollten von konkurrierenden privaten *Registries* geführt werden, die an einen durch die ISOC betreuten Fond eine Gebühr von 2.000 US\$ nebst 2% des Einkommens zahlen sollten. Diese Erträge hätten zur weiteren Finanzierung der IANA gedienten. Die neuen gTLDs sollten als generischen Namen, die kategorisierbaren Merkmale der netznutzenden Organisationen abbilden<sup>482</sup>. Im Gegensatz zum vorhergehenden Vorschlag Postels, vertrat er nunmehr die Ansicht, daß die IANA weiterhin die Kontrolle über alle gTLDs behalten solle. Diesem Plan wurde während des 36. Treffens der IETF im Juni 1996 durch die ISOC zugestimmt. Eine erweiterte Version eines Satzungsentwurfes der IANA wurde im August 1996 veröffentlicht<sup>483</sup>. In diesem wurde besonders die Notwendigkeit einer Markttöffnung für kommerzielle gTLDs hervorgehoben, um einen Wettbewerb zu ermöglichen. Dabei sollten folgende sechs in der Satzung festgelegte Ziele erreicht werden:

draft-postel-iana-itld-admin-02.txt

## 2. Goals

[...]

The specific measures to achieve this objective are as follows:

- 2.1. Provide the IANA with the international legal and financial umbrella of the Internet Society (ISOC),
- 2.2. Allow open competition in domain name registration in the iTLDs, which will then allow registries to charge for their services,
- 2.3. Allow multiple registries to operate cooperatively and fairly in the existing iTLDs and/or other multi-registry iTLDs which may be created,
- 2.4. Facilitate creation of new iTLDs in a fair and useful, but reliable, fashion,
- 2.5. Provide for reliable maintenance of the registrants of an iTLD should the current delegatee no longer wish to maintain it, and
- 2.6. Define iTLD policies and procedures by open methods, modeled on the IETF process and/or using IETF mechanisms when appropriate.

---

<sup>481</sup> Siehe Postel, New Registries and the Delegation of International Top Level Domains vom Juni 1996, draft-postel-iana-itld-admin-01.txt. Als RFC-Draft hatte dieses Dokument nur eine zeitlich begrenzte Gültigkeit und wurde entsprechend aus den meisten RFC-Archiven gelöscht. Noch zu finden ist es unter

<http://www.newdom.com/archive/draft-postel-iana-itld-admin-01.txt>.

<sup>482</sup> Vgl. auch Recke, DNS, Der Vorschlag der IANA: Draft Postel.

<sup>483</sup> Postel, draft-postel-iana-itld-admin-02.txt, zu finden unter <http://www.newdom.com/archive/draft-postel-iana-itld-admin-02.txt>. Die Bezeichnung iTLD in diesem Vorschlag ist als Synonym zu gTLD zu verstehen.

### 3.1. Geschichtlicher Hintergrund der ICANN

---

Auch dieser Versuch, das DNS zu reformieren hatte keinen Erfolg. Die Einführung neuer TLDs und das Betreiben dieser durch unabhängige *Registries* kam einer erneuten Privatisierung des *Root Server Systems* gleich<sup>484</sup>. IANA und ISOC betrachteten die *Root Server Administration* als langfristige Einnahmequelle zur Unterstützung dieser Organisationen. Wiederum trat eine Anzahl von Interessensgruppen diesem Plan entgegen. Insbesondere die im Internet inzwischen erstarkte Markenrechtslobby lehnte die Erweiterung des DNS aus Angst vor einem explosionsartigen Anstieg von Markenrechtskonflikten und -verletzungen grundätzlich ab. Auch potentielle *Registries* für die neuen TLDs protestierten gegen die geplanten Gebühren und zweifelten IANAs Legitimation zur Auferlegung dieser an. In den nächsten Monaten wurde klar, daß weder die IANA noch die ISOC die notwendige Autorität zur Einführung neuer gTLDs besaß<sup>485</sup>.

#### 3.1.2.3. *International Ad Hoc Committee* – IAHC

Die von Dr. Jon Postel entworfenen Dokumente zur Einführung eines Wettbewerbes im DNS bildeten die Grundlage für den bislang fortschrittlichsten Versuch, das DNS zu reformieren. Das *generic TLD Memorandum of Understanding*<sup>486</sup> (gTLD-MoU<sup>487</sup>) als Ergebnis des von der ISOC initiierten *International Ad Hoc Committee* (IAHC) stellte, meines Erachtens, die für den Endanwender nützlichste Erweiterung des TLD-Adreßraumes dar. Es mußte jedoch wie noch zu erläutern sein wird, auf Grund des Widerstandes verschiedener Interessensgruppen scheitern.

Am 12. November 1996 schloß sich die IANA mit weiteren in die Internetregulierung involvierten Organisationen (WIPO, ITU, INTA, FNC, IETF, ISOC und IAB<sup>488</sup>) zum IAHC<sup>489</sup> zusammen. Ziel war die Entwicklung des DNS voranzutreiben und dabei die Problematiken und Bedenken, welche durch Postels Vorschläge aufgeworfen wurden, zu untersuchen und Lösung zu finden.

In den nächsten Monaten drängte das IAHC auf Eile und veröffentlichte schon einen Monat nach Gründung den ersten Vorschlag zur Reform des DNS namens *Draft Specification for Administration and Management of Generic Top Level Domains (gTLDs)*<sup>490</sup>. Neue Registraturen sollten nach diesem Dokument durch Los gewählt werden, um dann alle neuen gTLDs zu registrieren. Dazu wurde im Gegensatz zu Dr. Jon Postels 150 TLDs nur die Einführung von

---

<sup>484</sup> Vgl. *Mueller*, 1 info 6, 497, 500f und *Mueller*, 5 Int. J. Com. L. & Pol'y, Web-Doc 1, 15.

<sup>485</sup> Siehe *Mueller*, 1 info 6, 497, 500f und *Mueller*, 5 Int. J. Com. L. & Pol'y, Web-Doc 1, 15.

<sup>486</sup> Siehe *gTLD-MoU*, 28. Februar 1997, <http://www.gtld-mou.org/gTLD-MoU.html>.

<sup>487</sup> Zu diesem Ungetüm von Abkürzung schreibt die FAQ des *gTLD-MoU* vom 1. Juni 1998, <http://www.gtld-mou.org/docs/faq.html>: „1.7 How do you pronounce gTLD-MoU? -- "gee tee el dee em o you" And yes, this wins the Internet's worst acronym contest.“

<sup>488</sup> *Rony/Rony*, Domain Name Handbook, S. 524 gibt einen ausführlichen Überblick über die Mitglieder des IAHC.

<sup>489</sup> Siehe die Charter des IAHC auf der WWW-Seite der Organisation: <http://www.iahc.org/iahc-charter.html>.

<sup>490</sup> Siehe *International Ad Hoc Committee*, 19. Dezember 1996, <http://www.iahc.org/draft-iahc-gTLDspec-00.html>.

sieben neuen gTLDs vorgeschlagen. In den nächsten sechs Wochen erfolgte eine intensive Diskussion der IAHC-Vorschläge in Mailinglisten und öffentlichen Kommentaren.

Der entgültige Plan wurde am 4. Februar 1997 von dem IAHC veröffentlicht und enthielt zum ursprünglichen Vorschlag noch einige gravierende Abänderungen<sup>491</sup>. Angenommen wurde der Vorschlag zur Einführung sieben neuer TLDs. 28 zunächst bestimmte *Registrars* sollten darunter SLDs registrieren. Schließlich sollten Schiedsgerichtsstellen zur Lösung von Domainstreitigkeiten, sogenannte *Administrative Domain Name Challenge Panels* (ACPs), unter Aufsicht der WIPO eingeführt werden.

### 3.1.2.3.1. Zeitplan

Innerhalb kürzester Zeit folgte der Abschluß weiterer Vereinbarungen. Die Reformbestrebungen schritten innerhalb eines Jahres rasch voran, bis sie durch die Veröffentlichung des sogenannten *Green Papers* der US-Regierung unter völliger Mißachtung des Prozesses und der erreichten Ergebnisse des IAHC ein jähes Ende fanden. Im Folgenden soll deshalb zunächst ein Überblick über die veröffentlichten Dokumente und Vereinbarungen gegeben werden<sup>492</sup>.

- 4. Februar 1997: Schlußreport des IAHC: *Recommendations for Administration and Management of Generic Top Level Domains (gTLDs)*<sup>493</sup>,
- 28. Februar 1997: Vorschlag des *Generic Top Level Domains – Memorandum of Understanding*<sup>494</sup>,
- 26. März 1997: Erster Vorschlag zu den ACPs: *Proposed Guidelines Concerning Administrative Domain Name Challenge Panels*,<sup>495</sup>
- 1. Mai 1997: Unterzeichnung des gTLD-MoU und Auflösung des IAHC,
- 12. Mai 1997: Definierung der Struktur für die Verwaltung des Domainadreßraumes,
- 19. Mai 1997: Vorschlag für *Council of Registrars (CORE) Memorandum of Understanding*,
- 27. Mai 1997: Vorschlag für *Council of Registrars (CORE) Articles of Association*<sup>496</sup>,
- 1. Juli 1997: Veröffentlichung des RFCs *Requests for Comments in the matter of Registration and Administration of Internet Domain Names* durch das US-DoC<sup>497</sup>,
- 18. Juli bis 16. Oktober 1997: Bewerbungszeitraum für die gTLD Registraturen,
- 3. Oktober 1997: Gründung des CORE, Anerkennung des Dokumentes *Council of Registrars (CORE) Articles of Association*,<sup>498</sup>

---

<sup>491</sup> Siehe Final Report of the *International Ad Hoc Committee: Recommendations for Administration and Management of gTLDs*, 4. Februar 1997, <http://www.iahc.org/draft-iahc-recommend-00.html>.

<sup>492</sup> Vgl. auch die ausführlichen Übersichten bei Rony/Rony, Domain Name Handbook, S. 525ff.; des IAHC unter <http://www.iahc.org/iahc-docs.html> und des gTLD-MoU unter <http://www.gtld-mou.org/docs/gtld-docs.html>.

<sup>493</sup> Siehe Final Report of the *International Ad Hoc Committee*, Fn. 491.

<sup>494</sup> Vgl. *gTLD-MoU*, Fn. 486.

<sup>495</sup> Im WWW unter <http://www.iahc.org/docs/acp-guide.html>. Weiter Versionen folgten am 16. Mai 1997, 2. Oktober 1997 und am 16. Januar 1998.

<sup>496</sup> Siehe *gTLD-MoU interim Policy Oversight Committee*, 27. Mai 1997, <http://www.gtld-mou.org/docs/core-as1.htm>.

<sup>497</sup> *US-DoC, NTIA*, RFC, 62 Fed. Reg. 35896ff.

### 3.1. Geschichtlicher Hintergrund der ICANN

---

- 19. Oktober 1997: Endgültige Version des *Council of Registrars (CORE) Memorandum of Understanding*<sup>499</sup>, offen zur Signierung durch neue Registraturen,
- 16. Januar 1998: letzter Vorschlag zu ACPs: *Substantive Guidelines Concerning Administrative Domain Name Challenge Panels*<sup>500</sup>,
- 20. Februar 1998: Veröffentlichung des *Green Paper: Improvement of Technical Management of Internet Names and Addresses*<sup>501</sup> durch die US-Behörde NTIA.

#### 3.1.2.3.2. gTLD-MoU

Das IAHC sollte die Entwicklung einer Verwaltungsstruktur des DNS vorantreiben. Entsprechend veröffentlichte das IAHC am 28. Februar 1997 das *Memorandum of Understanding on the Generic Top Level Domain Name Space of the Internet Domain Name System*, bekannt als das gTLD-MoU<sup>502</sup>. Die Verabschiedung dieses Dokumentes stellte die Fortsetzung der Reformbestrebungen hin zu einer fairen und stabilen Internetadreßvergabe dar. Das gTLD-MoU wurde am 1. Mai 1997 durch 57 Organisationen<sup>503</sup> unterzeichnet<sup>504</sup>. Mit diesem Erfolg wurde das IAHC an diesem Tage förmlich aufgelöst<sup>505</sup>. Administrative Aufgaben wurden von nun an durch das gTLD-MoU *interim Policy Oversight Committee* (iPOC) wahrgenommen.

Um die Öffentlichkeit von der Notwendigkeit der Arbeit zu überzeugen, veröffentlichte man auf der Webseite des gTLD-MoU nähere Erläuterungen zu diesem Dokument<sup>506</sup>. Unter anderem erfolgte eine Definition, was das gTLD-MoU darstellt, welche Ziele angestrebt werden und wie man am Verfahren teilnehmen kann<sup>507</sup>:

The Generic Top Level Domain Memorandum of Understanding (gTLD-MoU) is the international governance framework in which policies for the administration and enhancement of the Internet's global Domain Name System (DNS) are developed and deployed.

In ihren Aufgabenbereich sollte die Einführung neuer gTLDs in das DNS, die Auswahl der zugehörigen *Registrars* und die Entwicklung eines fairen Streitschlichtungsverfahrens fallen.

---

<sup>498</sup> Die aktuelle Fassung der Articles of Association des *CORE* vom 23.-24. Januar 1998 sind unter <http://www.gtld-mou.org/docs/core-aoa.htm> zu finden.

<sup>499</sup> Im WWW unter <http://www.gtld-mou.org/docs/core-mou.htm>.

<sup>500</sup> Im WWW unter *Policy Oversight Committee*, 16. Januar 1998, <http://www.gtld-mou.org/docs/tracps.htm>.

<sup>501</sup> *US-DoC, NTIA, Green Paper*, 63 Fed. Reg., 8826ff.

<sup>502</sup> Vgl. *gTLD-MoU*, Fn. 486.

<sup>503</sup> Die Liste aller Teilnehmer am gTLD-MoU kann unter <http://www.itu.int/net-itu/gtld-mou/simple.htm> eingesehen werden.

<sup>504</sup> Siehe die Pressemitteilungen der *ITU: Changes to Internet Domain Names will Encourage Competition, Foster Growth and Stability*, 29. April 1997 sowie *ITU, 80 organizations Sign MoU to Restructure the Internet*, 1. Mai 1997.

<sup>505</sup> Vgl. Pressemitteilungen der *ITU* vom 29. April 1997 und 1. Mai 1997, Fn. 504.

<sup>506</sup> Siehe die FAQ des *gTLD-MoU* vom 1. Juni 1998, <http://www.gtld-mou.org/docs/faq.html>.

<sup>507</sup> Weitere vom gTLD-MoU bezweckte Prinzipien befinden sich im Dokument selbst, siehe *gTLD-MoU*, Fn. 486, Section 2. – Principles. Siehe auch *gTLD-MoU*, FAQ, Kap. 1.1 What is the gTLD-MoU?, Fn. 506.

Diese Aufgaben sollten in Kooperation mit der IANA erfüllt werden. Für die neue Verwaltung des DNS enthielt das *Memorandum of Understanding* folgende Vorschläge:

- gTLDs sollten als öffentliches Gut betrachtet und entsprechend behandelt werden.
- Es sollten sieben neue gTLDs zu den bereits drei existierenden allgemein zugänglichen gTLDs (.com, .org, .net) hinzugefügt werden, um der wachsenden Nutzerzahl gerecht zu werden und um die Zuweisung von Domainnamen besser zu organisieren. Diese neuen Namen sollten .firm, .store, .web, .arts, .rec, .info und .nom sein.
- Es wurden selbstregulierende Organisationen innerhalb des Internets geplant. Sie sollten für die Registrierung (als *Registrars*), für die Überwachung der *Registries* (CORE), für die Untersuchung öffentlicher Belange und der durch sie notwendigen Politik (*Policy Oversight Committee* und *Policy Advisory Board*) und für schiedsrichterliche Entscheidungen (*Administrative Domain Name Challenge Panels*) zuständig sein.
- In der ersten Phase sollten bis zu 28 neue *Registrars* weltweit ausgesucht werden, welche im Wettbewerb zueinander Domainnamen registrieren würden. Sie alle sollten Zugang zu den TLDs durch eine gemeinsame und neutrale Datenbank haben. Solange das exklusive *Cooperative Agreement* mit NSI bestehen würde, wären die TLDs .com, .net und .org vom MoU ausgeschlossen. Weitere *Registrars* sollten so schnell wie möglich zugelassen werden.
- Geplant war ein Rat der *Registrars* (*Council of Registrars*, CORE), um gemeinsam allgemein gültige Richtlinien für die Domainvergabe zu entwerfen und um die gemeinsame Datenbank zu verwalten. Es wurde angedacht, CORE in der Schweiz als gemeinnützige Organisation zu gründen.
- Weitere Institutionen sollten etabliert werden, um die Arbeit des CORE zu beaufsichtigen und um als Regulierungsbehörde öffentliche Belange in die zukünftige Entwicklung des DNS zu integrieren. Diese Aufgabe sollte vom *Policy Oversight Committee* unter Beihilfe des *Policy Advisory Body* wahrgenommen werden.
- Es wurden Mechanismen entworfen, um das Sammeln beziehungsweise Horden von Domainnamen und die Reservierung von Marken durch Nichtmarkeninhaber zu verhindern.
- Zusätzlich war ein Schiedsgerichtsverfahren geplant, welches mit Hilfe des *Arbitration and Mediation Centre* der WIPO entwickelt werden sollte. Die unter diesem Verfahren eingerichteten Panels hätten unabhängig entscheiden können und wären für die Registraturen bindend.

### 3.1. Geschichtlicher Hintergrund der ICANN

---

- Die ITU sollte die Hinterlegungsstelle des gTLD-MoU sein.

Die grundlegende Struktur des beabsichtigten IANA-Nachfolgers bestand aus folgenden Elementen<sup>508</sup>:

- Hinterlegungsstelle des gTLD-MoU

Als Hinterlegungsstelle des gTLD-MoU fungierte das Hauptsekretariat der ITU in Genf, Schweiz. Dieses hatte sich als weltweiter Koordinator des internationalen Telefonverkehrs intensiv an den Vorbereitungen zum MoU beteiligt.

- *Council of Registrars* (CORE)

Wie bereits erwähnt, war das CORE zur Verwaltung und zum Betrieb der zentralen Datenbank für jede neue gTLD<sup>509</sup> angedacht. Es sollte am Ende des Transformationsprozesses aus anerkannten Registraturen, welche die Zuweisung der neuen gTLDs übernehmen, zusammengesetzt sein.

- *gTLD Policy Oversight Committee* (POC)

Dieses Gremium hatte die Arbeit und die Verfahrensweise des CORE und der Registraturen zu überwachen. Die POC-Mitglieder waren Personen, welche innerhalb des Umfeldes der Domainvergabe als Experten anerkannt waren. Diese wurden durch die am Reformprozeß beteiligten Organisationen (IANA, ISOC, ITU, IAB, CORE, WIPO, INTA) entsandt. Das POC sollte das Recht erhalten, die Anzahl der gTLDs festzulegen (beziehungsweise neue gTLDs einzuführen), die Bedingungen für Bewerbungen neuer Registraturen (insbesondere Gebühren für die Zulassung) zu bestimmen, neue Registraturen zuzulassen sowie nach Konsultation des PAB und des CORE Registraturen auszuschließen, die gegen die Regeln des gTLD-MoU oder des CORE-MoU<sup>510</sup> verstößen.

- *gTLD Policy Advisory Body* (PAB)

Das PAB hätte dem POC Anleitungen und Empfehlungen in generellen Verfahrensweisen betreffend der gTLDs und dem DNS gegeben. Im PAB sollten nach dem *rough-consensus*-Modell die Ratschläge entwickelt werden. Allen Unterzeichnern des gTLD-MoU hätte die Teilnahme am PAB offengestanden.

- *Administrative Domain Name Challenge Panels* (ACPs)

Jede Person sollte die Vergabe eines Domainnamens vor einem ACP angreifen können. Die ACPs sollten entsprechend nach den durch das WIPO *Arbitration and Media*-

---

<sup>508</sup> Siehe zur Struktur des gTLD-MoU: *Mewes*, 13 Berkeley Tech. L.J. 235, 239ff. und *Rony/Rony*, Domain Name Handbook, S. 530f.

<sup>509</sup> Zu einer näheren Bestimmung der Aufgaben und Befugnisse des CORE siehe dessen Satzung in der Fassung vom 23.-24. Januar 1998, Fn. 498 und das *CORE-MoU*, Fn. 499.

<sup>510</sup> Siehe *CORE-MoU*, Fn. 499.

*tion Centre* festgelegten Verfahrensweisen arbeiten und durch schiedsrichterliche Urteile Streitigkeiten um Domainnamen lösen<sup>511</sup>. Der CORE und die Registraturen wären verpflichtet gewesen, den ACPs alle benötigten Informationen zu überlassen, um durch diese die Streitschlichtung bezüglich Domainnamen zu ermöglichen. Die von den ACPs gefällten Urteile wären wiederum von den *Registrars* anzuerkennen gewesen.

Neben einer Reform der DNS-Verwaltung schlug das IAHC und das gTLD-MoU die Einführung neuer gTLDs vor<sup>512</sup> (vgl. Tabelle 3 unten). Dabei wurde aus einer großen Anzahl an Kommentaren, vorherigen Vorschlägen und anschließenden Diskussionen aus einer Vielzahl von Namensvorschlägen folgende Sieben ausgewählt:

Tabelle 3 – Die vom IAHC vorgeschlagenen neuen gTLDs.

Top Level Domain	Zielnutzergruppe
.firm	Unternehmen
.shop	Verkäufer, Händler
.web	WWW basierte Angebote
.arts	Kultur und Unterhaltung
.rec	Erholung und Vergnügen
.info	Informationsservice
.nom	Individuelle oder personelle Nomenklatur

Es wurde zunächst nur eine beschränkte Anzahl von TLDs bestimmt, da das DNS ein Herzstück des Internet darstellt und es von den Initiatoren für weise gehalten wurde, die ersten Veränderungen nur langsam vorzunehmen<sup>513</sup>. Damit sollte später eine Evaluation und Modifikation leichter möglich sein. Mit dem Kompromiß zwischen der Einführung keiner und vieler neuer TLDs wollte man auch den Bedenken der Markenrechtslobbyisten entgegenkommen, die einen erhöhten Aufwand in der Verteidigung ihrer Namensrechte befürchteten. Das vorgeschlagene Streitschlichtungsverfahren sollte zunächst entsprechend dem gTLD-MoU eingeführt und angewendet werden, bevor man mit der weiteren Erweiterung des DNS forschreiten wollte.

Der zweitwichtigste Vorschlag zur Erweiterung des DNS bestand in der Zulassung von im Wettbewerb stehenden *Registries*. Dies sollte Kunden den Vergleich von Angeboten und Preisen erlauben und ihnen die Möglichkeit geben, die Registraturen zu wechseln, ohne den Domainnamen zu verlieren. Der Bewerbungsprozeß wurde durch das iPOC am 18. Juli 1997 eröffnet und endete am 16. Oktober. Zum Ende der Bewerbungsperiode hatten sich 65 Unternehmen qualifiziert. Die strittigste Regelung bei der Zulassung neuer Registraturen war eine

<sup>511</sup> Siehe auch *POC*, Substantive Guidelines Concerning Administrative Domain Name Challenge Panels, Third Revised Draft, Fn. 500.

<sup>512</sup> Siehe *IAHC*, Final Report of the International Ad Hoc Committee, Kap. 3.1 Recommendations, Fn. 491.

<sup>513</sup> Siehe *gTLD-MoU*, FAQ, Kap. 2.2 Why did you choose these names and why only seven?, Fn. 506.

### 3.1. Geschichtlicher Hintergrund der ICANN

---

Bewerbungsgebühr in Höhe von 10.000 US\$. Als Folge der anhaltenden Kritik wurden jedoch die Bewerbungsregeln dahin geändert, daß erfolglose Antragsteller den größten Teil der Gebühr zurück erhalten sollten. Erfolgreiche Antragsteller hatten sich dem CORE-MoU zu unterwerfen, welches detailliert die Betriebs- und Verfahrensprinzipien bestimmte.

#### 3.1.2.3.3. Kritikpunkte

Die Reformbestrebungen des DNS betrafen eine Reihe von Gesellschaftskreisen, die grundsätzlich verschiedene Positionen vertraten. Das IAHC und das gTLD-MoU sahen sich vielen Kritikpunkten ausgesetzt, welche schließlich zum Scheitern des Projektes führten. Darunter waren auch Kritiken von Interessensvertretern, die einen starken Eingriff in ihre aktuellen Positionen befürchteten. Die wichtigsten Argumente sollen zunächst aufgelistet werden.

- Fehlende Autorität

Die Hauptkritik bestand darin, daß das IAHC kein Mandat durch die US-Regierung erhalten habe, um regulierend in das DNS einzutreten, Gebühren zu erheben, Namen zuzuweisen oder Lizenzgebühren zu verlangen. Weder aus der Legitimation der IANA noch der Legitimation der ISOC ließe sich das Recht herleiten, solch weitreichende Entscheidungen zu treffen<sup>514</sup>. Es wurde moniert, daß die Legitimation durch die USA selbst fehle, in internationalen Gremien wie der ITU aufzutreten<sup>515</sup>:

However, the Internet Assigned Numbers Authority does not exist as a legal entity, but is the name of an activity of the U.S. government performed under contract by the University of Southern California. The Internet Society is a non-profit corporation chartered in the District of Columbia to be “[...] operated exclusively for educational, charitable and scientific purposes.” As such, neither entity can lawfully even sign such an instrument, much less possess the authority under domestic U.S. or international law to convey it to the ITU to be circulated as an intergovernmental agreement.

Andererseits wurde auf das DNS als internationale öffentliche Ressource abgestellt und das Fehlen einer Autoritätsübertragung durch die staatlichen Regierungen oder das Fehlen eines Konsenses in der Internetgemeinschaft hervorgehoben<sup>516</sup>:

---

<sup>514</sup> Vgl. z.B. *Rutkowski, Anthony M.*, Meeting of the ITU-Council – Position of the U.S. Administration Regarding ITU Involvement in Internet Domain Name Matters, Punkt 16, <http://www.wia.org/pub/itu-council.html>: „Neither any of the individuals in the group, nor the non-profit organization, had any known legal authority for undertaking the creation of such an instrument.“

<sup>515</sup> Siehe *Rutkowski*, Fn. 514, Punkt 17. Zur fehlenden Autorität des IAHC siehe auch *Mewes*, 13 Berkeley Tech. L.J. 235, 242f.

<sup>516</sup> Siehe z.B. *Fenello, Jay*, in einem Brief an [domain-policy@list.internic.net](mailto:domain-policy@list.internic.net), 15. Juni 1997, zitiert in *Rony/Rony*, Domain Name Handbook, S. 537: „The IAHC proponents are attempting to usurp the public resources that have supported the public root for their own purposes. They are attempting to do so with out any legitimate authority, process, or consensus.“

- Autoritätsanmaßung

Entsprechend sah man in der Arbeit des IAHC eine Anmaßung von Autorität<sup>517</sup>:

This ad hoc committee is being run by ISOC, but even there, you're talking about a new organization with fewer than 10,000 members out of the millions of Internet users. It smells of the old-boy network.

- Unzureichende öffentliche Diskussion

In einem weiteren Kritikpunkt wurde die Diskussionen hinter verschlossenen Türen bemängelt. Dies entsprach nicht den Gepflogenheiten, wie sie die Internetingenieure gewohnt waren<sup>518</sup>:

The IAHC says it followed an open process because it solicited comment. I have a little trouble with this, since the closed IAHC meetings don't seem open to me. It's like they were behind a one-way mirror.

The deliberations of the IAHC were closed and not conducted in public. In my opinion, there has been no “rough consensus” developed by the Internet community through its tradition of self-governance regarding the content of the Memorandum of Understanding or the IAHC’s Final Recommendations. The authority which IANA, IAHC, and the Internet Society now claim to execute and implement the Memorandum of Understanding is, as far as my investigation has revealed, self-ordained.<sup>519</sup>

- Sitz in der Schweiz

Da der Sitz des CORE in der Schweiz sein sollte, befürchteten besonders amerikanische Akteure, schweizerischem Recht ausgesetzt zu sein. Diese Situation war für viele Amerikaner neu und schien besonders gefährlich<sup>520</sup>:

It finds a basis to declare domain names to be a “limited global public resource” like radio spectrum that is managed as a public trust by a Swiss-based cartel under the aegis of U.N. intergovernmental organizations. It takes us back to the PTT-driven international telecommunication models cast for the telegraph in 1850, the telephone in 1903, and radio in 1906 - where

---

<sup>517</sup> Kashpureff, Eugene zitiert in Nettyme, Crysler, Maverick Registries Threaten an Internet Monopoly, 14. Januar 1997.

<sup>518</sup> Mockapetris, Paul, Entwickler des DNS, zitiert in Rony/Rony, Domain Name Handbook, S. 539. Liu, 74 Ind. L.J. 587, 601 sieht jedoch den Standardsetzungsprozeß der technischen Internetorganisationen in der Erarbeitung des gTLD-MoU analog verwirklicht: „Although the process took place outside the normal standard-setting process, it was in some ways analogous to the process in that it sought to build a consensus and voluntary participation.“

<sup>519</sup> Siehe auch Stefferud, Einard, Erklärung zu Image Online Design v. IANA, <http://www.wia.org/dns-law/pub/stef-io-declaration.html>.

<sup>520</sup> So Rutkowski, Testimony Before the Committee on Commerce.

### 3.1. Geschichtlicher Hintergrund der ICANN

---

the new “public resources” were declared and managed over succeeding generations by Swiss-based international regimes.

- **Verwirrung der Endnutzer**

Schließlich befürchtete man eine Verwirrung der Konsumenten, wenn neue TLDs eingeführt würden. Auch seien einzelne Kategorien, wie .com zu .shop und .firm, untereinander verwechselbar. Einzelne Firmen müssten sich unter allen TLDs registrieren, um von Konkurrenzfirmen getrennt werden zu können<sup>521</sup>:

The namespace [...] exists to serve the consumer, not to serve the interests of the domain name owner. The primary operating principle of it is that the consumer is not supposed to be confused by a plethora of hosts with vastly different content all bearing what appear to be similar domain names.

Unter den Hauptkritikern befand sich die NSI, welche ihr lukratives Geschäft mit den .com-Domainnamen durch die Einführung neuer TLDs bedroht sah. Von ihr wurde als entsprechende Reaktion eine Lobbykampagne gegen das gTLD-MoU gestartet, die schließlich zu einer Anhörung vor dem US-Kongreß führte<sup>522</sup>. Die USA lehnte das Projekt wegen der intensiven Beteiligung der ITU ab, der sie jegliche Legitimation durch die Mitgliedsstaaten absprach. Die Europäische Kommission wiederum konnte sich dem Plan nicht anschließen, da sie im Vorschlag europäische Interessen nicht weit genug repräsentiert sah<sup>523</sup>.

Die Folge aller Kritiken war, daß das gTLD-MoU nur teilweise umgesetzt werden konnte. Mit Veröffentlichung des sogenannten *Green Papers* durch die USA wurde jegliche Legitimation dem gTLD-MoU entzogen. Die sieben vorgeschlagenen neuen TLDs konnten nie eingeführt werden. Das vorgesehene CORE wurde zwar gegründet und die beteiligten Unternehmen hatten ihren finanziellen Beitrag geleistet, weitere Anstrengungen das Projekt umzusetzen verliefen jedoch im Sande. CORE versuchte schließlich an der späteren Gründung der ICANN mitzuwirken und ist heute ein *Registrar* von vielen im *Shared Registry System* der ICANN.

#### 3.1.2.4. Intervention der US-Regierung – *Green Paper*

Die anhaltende Kontroverse über das gTLD-MoU und die erwähnte Lobbykampagne gegen das Projekt durch die NSI führte schließlich zum Eingriff der US-Regierung in das Geschehen. Am 1. Juli 1997 wurde der Report *A Framework for Global Electronic Commerce* veröffentlicht<sup>524</sup>. Obgleich geschichtlich die US-Regierung im Internetbereich nur im Hintergrund

---

<sup>521</sup> Siehe *Higgs, Why Care About The Namespace?* Siehe auch *Gole*, 51 Fed. Comm. L.J. 403, 424 und *Mewes*, 13 Berkeley Tech. L.J. 235, 245.

<sup>522</sup> *U.S. House of Representatives, Committee On Science, Subcommittee On Basic Research*, Hearing on Internet Domain Names, 30. September 1997, Science Committee Hearings, Markups and Testimony, [http://www.house.gov/science/hearing\\_105.htm](http://www.house.gov/science/hearing_105.htm).

<sup>523</sup> Siehe auch *Mueller*, 5 Int. J. Com. L. & Pol'y, Web-Doc 1, 17 und 23.

<sup>524</sup> *US-White House*, Framework.

auftrat, sah sie nun die Notwendigkeit, in das aktuelle Geschehen aktiv mitzustalten. Neben vielen weiteren Themen schlug der Report und seine einhergehenden Direktiven die Privatisierung des DNS vor<sup>525</sup>. Das *Department of Commerce* sollte dabei eine Schlüsselrolle spielen und als Anlaufstelle für interessierte Gruppen und Konsumenten dienen.

Um die in der Öffentlichkeit vertretenen Meinungen zur Erweiterung des DNS zu analysieren und das weitere Vorgehen zu planen, veröffentlichte das *Department of Commerce* mit dem oben genannten Report ein *Request for Comments*<sup>526</sup>, welcher zu über 430 Kommentierungen führte<sup>527</sup>.

Während die Umsetzung des gTLD-MoU vorangeschritten war, publizierte schließlich die *National Telecommunications and Information Administration* (US-NTIA) des *Department of Commerce* am 20. Februar 1998 einen ersten Vorschlag namens *Improvement of Technical Management of Internet Names and Addresses*<sup>528</sup>, bekannt als *Green Paper*<sup>529</sup>. Dieses Papier stellte den bedeutendsten Rückschlag für die gTLD-MoU-Initiative dar<sup>530</sup>. Darin schlug die US-NTIA die Gründung einer privaten und gemeinnützigen Organisation zur Koordinierung der Funktionen des DNS in einem stabilen und offenen Rahmen vor, ohne den IAHC-Plan mit einem Wort zu erwähnen. Es sollten die Funktionen der IANA zu einer *not-for-profit*-Organisation, beheimatet in den USA, transferiert<sup>531</sup> und Wettbewerb auf der Ebene der *Registrars* sowie auf der Ebene der *Registries* eingeführt werden<sup>532</sup>. Die US-Regierung sollte während der Übertragungsphase voraussichtlich bis September 2000 als Aufsichtsorgan dienen. Es war geplant, daß die neue Organisation von einem internationalen Vorstand geleitet wird, welcher seine Legitimation durch die Teilnahme von wichtigen Interessensgruppen erhalten würde und in welchem Internetnutzer durch eine Mitgliedsorganisation repräsentiert wären.

Man dachte an drei Vorteile, die eine Privatorganisation gegenüber einer internationalen öffentlichrechtlichen Organisation (wie der ITU) hat: Erstens entspricht die privatrechtliche Or-

---

<sup>525</sup> Nach *US-GAO*, Report, S. 36 zitiert: „support efforts to make the governance of the domain names system private and competitive and to create a contractually based self-regulatory regime that deals with potential conflicts between domain name usage and trademark laws on a global basis.“

<sup>526</sup> *US-DoC, NTIA*, RFC, 62 Fed. Reg. 35896ff.

<sup>527</sup> Die Zusammenfassung der eingesendeten Kommentare ist unter: *US-DoC, NTIA*, Summary of Comments, [http://www.ntia.doc.gov/ntiahome/domainname/DNSComments\\_SUM.htm](http://www.ntia.doc.gov/ntiahome/domainname/DNSComments_SUM.htm) abfragbar.

<sup>528</sup> Zur Legitimation des DoC gegenüber dem US-amerikanischem Staat siehe *Froomkin*, 50 Duke L.J. 17, 65f.

<sup>529</sup> Ein Green Paper stellt nach dem *Merriam-Webster Dictionary* „a government document that proposes and invites discussion on approaches to a problem“ dar; <http://www.m-w.com>.

<sup>530</sup> Siehe *Werle/Leib*, The Internet Society, S. 19. *Weinberg*, 50 Duke L.J. 187, 205, sieht das endgültige Aus der CORE-Bemühungen mit dem Abschluß des Amendment No. 11 zum Cooperative Agreement zwischen DoC und NSI, [http://www.networksolutions.com/en\\_US/legal/internic/cooperative-agreement/amendment11.html](http://www.networksolutions.com/en_US/legal/internic/cooperative-agreement/amendment11.html). Hierin wurde explizit bestimmt, daß jegliche Änderungen am DNS-Root die Genehmigung des DoCs benötigen: „While NSI continues to operate the primary root server, it shall request written direction from an authorized USG official before making or rejecting any modifications, additions or deletions to the root zone file.“

<sup>531</sup> *US-DoC, NTIA*, Green Paper, 63 Fed. Reg. 8826, 8828.

<sup>532</sup> *US-DoC, NTIA*, Green Paper, 63 Fed. Reg. 8826, 8828f.

### 3.1. Geschichtlicher Hintergrund der ICANN

---

ganisation des DNS dem allgemeinen Trend, bislang staatlich wahrgenommene Aufgaben, wie zum Beispiel Post- und Telekommunikationswesen oder Straßenreinigung und Müllbeseitigung, zu privatisieren und diese damit dem freien Wettbewerb auszusetzen. Die privatrechtliche Struktur vermag zweitens gegenüber einer großen und damit tragen internationalen Organisation eine schnellere Entscheidungsfindung zu ermöglichen. Drittens ist es einer kleinen Gruppe von Spezialisten eher möglich, auf technische Entwicklungen zeitgerecht zu reagieren.

Nach dem *Green Paper* sollte die neue Organisation dabei folgende Aufgaben wahrnehmen<sup>533</sup>:

1. To set policy for and direct the allocation of number blocks to regional number registries for the assignment of Internet addresses;
2. To oversee the operation of an authoritative root server system;
3. To oversee policy for determining, based on objective criteria clearly established in the new organization's charter, the circumstances under which new top-level domains are added to the root system; and
4. To coordinate the development of other technical protocol parameters as needed to maintain universal connectivity on the Internet.

Obgleich es auch für die US-Regierung unmöglich schien, eine perfekte Repräsentation der Internetgemeinschaft innerhalb der neuen Organisation zu realisieren, ging man davon aus, daß eine Legitimierung der neuen Organisation nur durch eine Teilnahme aller Schlüsselorganisationen möglich ist. Da die Organisation mit der Verwaltung von IP-Nummern, Domainnamen und Internetprotokollen betraut werden sollte, war angedacht, daß Organisationen aus diesen drei Bereichen Mitglieder werden, genauso wie Organisationen, welche die direkten Interessen der Internetnutzer widerspiegeln<sup>534</sup>.

Bis zum Schluß des Diskussionsverfahrens um das *Green Paper* wurden 650 Einwände und Verbesserungsvorschläge eingereicht. Das Papier begegnete vielen alten, schon gegenüber dem gTLD-MoU erhobenen, aber auch vielen neuen Kritikpunkten<sup>535</sup>. Zum einen wurde wiederum die Einführung neuer TLDs bemängelt<sup>536</sup>. Zum anderen wurde das Diktieren von De-

---

<sup>533</sup> US-DoC, NTIA, Green Paper, 63 Fed. Reg. 8826, 8828.

<sup>534</sup> US-DoC, NTIA, Green Paper, 63 Fed. Reg. 8826, 8828.

<sup>535</sup> Vgl. zum ganzen *HLRA*, 112 Harv. L. Rev. 1657, 1666 und *Weinberg*, 50 Duke L.J. 187, Fn. 103.

<sup>536</sup> Gegen die Einführung neuer TLDs richteten sich, z.B. *Bell Atlantic*, Comments of Bell Atlantic Corporation on Improvement of Technical Management of Internet Names and Addresses, 23. März 1998, <http://www.ntia.doc.gov/ntiahome/domainname/130dftmail/Bell.htm>, „The creation of up to five new generic Top-level domains (gTLDs) is fundamentally flawed and ought to be reconsidered“. Siehe auch *America Online, Inc.*, DNS Comments on Improvement of Technical Management of Internet Names and Addresses, 23. März 1998, <http://www.ntia.doc.gov/ntiahome/domainname/130dftmail/scanned/AOL.htm>. Diese bemerkte, daß keine „concrete need exists that would justify an increase in the number of gTLDs in the near term“. Andererseits wurde die Begrenzung auf nur fünf neue TLDs z.B. von *Capital Networks* (CORE Registrar), Response to the Green

tails für das neue System als zu weitgehend empfunden<sup>537</sup> oder die fehlende Repräsentation internationaler Interessen gerügt<sup>538</sup>.

### 3.1.2.5. *White Paper* der US-Regierung

Als Antwort zu den öffentlichen Kommentaren zum *Green Paper* veröffentlichte die Clinton-Regierung einen überarbeiteten Vorschlag zum zukünftigen DNS, das *White Paper*<sup>539</sup>. Im Gegensatz zum *Green Paper*, welches eine Lösung der Internetprobleme durch einen *Top-Down* Ansatz vorsah, legte das *White Paper*<sup>540</sup> auf die etablierten Normen und Gebräuche des Internets wert. Die US-Regierung wollte sich deshalb bei den Verhandlungen von den folgenden Prinzipien leiten lassen<sup>541</sup>:

- Stabilität

Die Involvierung der US-Regierung in die Systeme der IP-Nummern und der Domännamen sollte in der Weise erfolgen, daß die Stabilität des Internets gewährleistet bleibt. Insbesondere während der Einführung der neuen Organisationsstruktur sollte die Stabilität des Internets die oberste Priorität darstellen. Dabei sollte die Einführung einer neuen Verwaltung nicht zu einer Unterbrechung des bislang bestehenden DNS führen. Auch sollte kein konkurrierendes DNS eingeführt werden.

---

Green Paper, 10. März 1998, [http://www.ntia.doc.gov/ntiahome/domainname/130dftmail/03\\_09\\_98.htm](http://www.ntia.doc.gov/ntiahome/domainname/130dftmail/03_09_98.htm) kritisiert.

<sup>537</sup> Gilmore, John: „[The government wants to] dictate the details, which is the imposition of authority“, zitiert in *TechWeb, MacLachlan*, Analysts Cautious But Positive On Green Paper, 2. Februar 1998.

<sup>538</sup> Z.B. Maher, David, damaliger Vorsitzender des Policy Oversight Committee des COREs, zit. in *TBTF, Keith*, TBTF for 1998-02-02: Lie down with trains, Kap. US Government green paper on domain names, 2. Februar 1998: „[It is] too protective of NSI and other US interests [...] If this is treated as a US solution to US problems, people outside the US are not going to be happy. I think that's a very severe limitation on the viability of the [proposal]“. Siehe auch Europäische Kommission, Reply to US Green Paper, welche feststellt, daß das Green Paper nicht „recognize[s] the need to implement an international approach“, und vorschlägt, daß „the US Administration limit[s] its direct regulatory intervention in the Internet only to those relationships which fall clearly under existing contract between the Agencies of the US Government and their contractors and that all other decisions be referred to an appropriate internationally constituted and representative body“; sowie *America Online, Inc.*, Fn. 536, „AOL does not believe that the U.S. proposal adequately reflects the legitimate need and desire for the larger international community, including stakeholders in Europe, Asia, Africa and Latin America, to be directly involved in decisions regarding the future administration of the DNS and management of the coordinated functions of the Internet. In this regard, AOL notes with interest that the U. S. Green Paper does not mention or appear to borrow from other proposals for managing the DNS including the much-debated generic Top Level Domain - Memorandum of Understanding (gTLD-MoU). The failure to even acknowledge the existence of such proposals, around which a great deal of consensus has been built in the international community, sends an inappropriate signal that the U.S. intends to essentially exclude non-U.S. stakeholders from developing and implementing an acceptable plan for the upcoming transition“.

<sup>539</sup> US-DoC, NTIA, White Paper, 63 Fed. Reg. 31741ff.

<sup>540</sup> Nach dem *Merriam-Webster Dictionary* stellt ein White Paper einen „government report on any subject; especially: a British publication that is usually less extensive than a blue book“ oder einen „detailed or authoritative report“ dar. Vgl. die zusammenfassenden Darstellungen von Froomkin, 50 Duke L.J. 17ff. und HLRA, 112 Harv. L. Rev. 1657ff.

<sup>541</sup> Siehe US-DoC, NTIA, White Paper, 63 Fed. Reg. 31741, 31749.

### 3.1. Geschichtlicher Hintergrund der ICANN

---

- Wettbewerb

Besonders der dezentralisierte Aufbau des Internets ermutigte zu vielen Innovationen und maximierte die persönlichen Freiheiten. Wo immer möglich, sollte deshalb auf Marktmechanismen zurückgegriffen werden, welche freien Wettbewerb und freie Produktwahl bei den Konsumenten ermöglichen.

- Private, *Bottom-Up* Koordinierung

Die Koordinierung des Internets sollte anstatt durch staatliche Kontrolle aus dem privaten Wirtschaftssektor heraus erfolgen. Ein privater Koordinierungsprozeß ist flexibler als dies eine Regierung gewährleisten könnte. Dies würde wiederum erst ein schnelles Reagieren auf die sich ständig ändernden Rahmenbedingungen im Internet ermöglichen. Die privatorientierte Koordinierung des Internets sollte dabei die bislang im Internet verankerte *bottom-up* Regulierung reflektieren.

- Repräsentation

Schließlich sollte die neue Organisation als eine privatrechtliche Einheit zum Vorteil der Internetgemeinschaft als Ganzes arbeiten. Grundlage der Koordinierung sollten faire und weitläufig akzeptierte Verfahrensregeln bilden. Die Verabschiedung solcher Verfahrensregeln ist jedoch von der Mitarbeit der breiten Basis der Internetnutzer abhängig. Die neuen Verwaltungsstrukturen sollten also die funktionale und geographische Vielfalt der Internetnutzer widerspiegeln. Mechanismen sollten eingeführt werden, welche eine internationale Teilnahme am Entscheidungsprozeß sicherstellen konnten.

Wie auch im *Green Paper* sprach sich die US-Regierung für die Bildung einer privaten *non-profit* Organisation aus, welche die Schlüsselfunktionen des Internets, wie die Verwaltung der IP-Adressen und der Rootserver, die Erweiterung des DNS oder das Festlegen von Protokollparametern, übernehmen sollte<sup>542</sup>.

Da man befürchtete, daß die Stabilität des Internets nicht gesichert sei, wenn die neue Organisation sich außerhalb der USA niederlassen würde, sollte sie im Ursprungsland des Internets weiterhin verbleiben. Jedoch wurde verlangt, daß das *Board* (die Vorsitzenden) und die Mitglieder aus der ganzen Welt kommen sollten. Im *Board of Directors* sollten gleichmäßig die Interessensgruppen der *IP-Registries* (ARIN, RIPE-NCC and APNIC), der *Domain Name Registries*, der *Domain Name Registrars*, der technischen Entwicklungsgremien, der ISPs sowie der Internetnutzer vertreten sein. Eine direkte Beteiligung offizielle Vertreter von Regierungen und staatlichen Organisationen an diesem Vorstandsgremium war jedoch nicht vorgesehen. Diese hätten jedoch die Möglichkeit zur Teilnahme durch ein eigenes *Advisory Committee*<sup>543</sup>. Dieser Aufbau spiegelte die Befürchtungen wieder, Regierungen könnten einen ungewollten Einfluß auf die Politik des neuen Gremiums ausüben. Das *Board of Directors* sollte

---

<sup>542</sup> Siehe *US-DoC, NTIA*, White Paper, 63 Fed. Reg. 31741, 31749.

<sup>543</sup> Siehe *US-DoC, NTIA*, White Paper, 63 Fed. Reg. 31741, 31750.

sich zunächst aus vorläufigen Mitgliedern zusammensetzen, ehe die Vorstandsmitglieder gewählt werden würden. Das *interim Board of Directors* würde „policies for the addition of TLDs“ entwickeln und „the qualifications for domain name registries and domain name registrars within the system“ festschreiben<sup>544</sup>. Um die Handlungsfähigkeit der neuen Organisation zu gewährleisten, sollte diese das Personal der IANA übernehmen. Unterstützt würde sie weiterhin durch zwei getrennte Räte, dem *Name Council* und dem *Numbers Council*.

Nach dem *White Paper* sollten die Domainregistranten verpflichtet werden, sich einem alternativen Streitschlichtungsverfahren zu unterwerfen<sup>545</sup>. Dazu sollte die WIPO Empfehlungen für eine einheitliche Lösung von Markenrechtsstreitigkeiten entwickeln.

Schließlich erläutert das *White Paper* die notwendigen Schritte für eine Übertragung des DNS in eine private Verwaltung<sup>546</sup>. Dabei wird zwischen den Schritten durch die US-Regierung und durch den privaten Sektor selbst unterschieden. Zum einen sah das Dokument eine Beendigung des Vertrages mit der NSI unter den Bedingungen vor, daß diese die Entwicklung eines Wettbewerbs in der Domainregistrierung zuläßt, die Rolle der neuen Organisation anerkennt und die DNS-Datenbank sowie die Software der angestrebten Organisation zugängig macht. Zum anderen sollte die Regierung einen neuen Vertrag mit der zukünftigen Organisation bezüglich der Übertragung des Managements des DNS auf diese unterzeichnen.

Da die traditionellen Verfahren des Internet anerkannt wurden, waren die Reaktionen überwiegend positiv<sup>547</sup>. Auf diese Weise bildete die auf das *White Paper* einsetzende Diskussion ein öffentliches Forum, um die verschiedenen Ansichten über die Zukunft des DNS zu erörtern<sup>548</sup>. Entsprechend wurde eine schnelle und öffentliche Weiterentwicklung gefordert, da die Verträge mit der NSI auszulaufen drohten. Auch die ursprünglich das *Green Paper* stark ablehnende *Europäische Union* stimmte den überarbeiteten Plänen des *US-Department of Commerce* weitestgehend zu<sup>549</sup>, da die notwendige Repräsentation internationaler Interessen durch das *Board of Directors* in der neuen Organisation gewährleistet wäre. Hervorgehoben wurden besonders die schiedsmäßige Lösung von Domainstreitigkeiten und die Einführung neuer im Wettbewerb stehender Registraturen.

Die vorgesehene Übertragung des DNS-Managements auf eine private gemeinnützige Organisation rief jedoch die Befürchtung hervor, daß die US-Regierung sich aus ihrer Verantwor-

---

<sup>544</sup> Siehe *US-DoC, NTIA, White Paper*, 63 Fed. Reg. 31741, 31750.

<sup>545</sup> Siehe *US-DoC, NTIA, White Paper*, 63 Fed. Reg. 31741, 31750f.

<sup>546</sup> Siehe *US-DoC, NTIA, White Paper*, 63 Fed. Reg. 31741, 31751.

<sup>547</sup> Zusammenfassend: *CNet, Kornblum*, Magaziner: Domain consensus possible, 5. Juni 1998; *TechWeb, Borland, Registrars Applaud New Domain Name Policy*, 5. Juni 1998 sowie *ZDNet, Broersma*, Domain plan draws industry reaction, 5. Juni 1998.

<sup>548</sup> *Liu*, 74 Ind. L.J. 587, 616.

<sup>549</sup> *TechWeb, Andrew*, European Commission OKs Domain Proposal, 30.Juli 1998 sowie Conclusions of the European consultative meeting in Brüssel, 7. Juli 1998, <http://europa.eu.int/ISPO/eif/dns/conclusions.html>: „The EU has welcomed the US White Paper because the US Government has acknowledged many of the concerns and criticisms voiced by the EU and the position has been rectified“.

### 3.1. Geschichtlicher Hintergrund der ICANN

---

tung gegenüber ihren Wählern entziehen würde<sup>550</sup>. Bei der Regulierung in den verschiedenen Bereichen durch staatliche Behörden kann die Öffentlichkeit ihre Meinung und Ansicht bei den Wahlen der Legislaturen kundtun. Im Gegensatz zu einer öffentlichrechtlichen Organisation hat die Gesellschaft keinen direkten Einfluß auf die Aktionen eines privaten Gremiums. Sie kann nicht direkt kontrollieren, ob eine private Organisation die Interessen der Internetgemeinschaft als Ganzes adäquat vertritt<sup>551</sup>. Dieses Problem kann nur gelöst werden, wenn die Regeln des offenen Prozesses und der Konsensbildung die Strukturen und Verfahrensweisen des neuen Gremiums bestimmen würden<sup>552</sup>.

#### 3.1.2.6. IFWP gegen Dr. Jon Postels ICANN-Plan

Dem *White Paper* folgend, war es Aufgabe der verschiedenen Interessensgruppen im Internet einen Konsens für den Ersatz der IANA zu finden. In Antwort auf das Schreiben des US-DoC wurden zwei parallele Initiativen zur Übertragung der IANA-Funktionen auf eine neue Organisation veranlaßt<sup>553</sup>. Die erste wurde durch die IANA ins Leben gerufen und arbeitete unter der Obhut von Dr. Jon Postel. Die zweite Initiative, das *International Forum on the White Paper* (IFWP), wurde von einer Reihe von Unternehmen gegründet, unter anderem auch durch die NSI. Die Bemühungen der IANA beinhalteten das Betreiben einer Mailingliste, um Ansichten für eine Satzung der neuen Organisation zu sammeln. Das IFWP veranstaltete vor allem öffentliche Treffen während des Sommers 1998<sup>554</sup>. Auf diesen Treffen wurden vom *White Paper* nicht geklärte Themen erörtert wie die Bildung der Organisation, die Zusammensetzung des Direktoriums und der Mitglieder, Entwicklung eines neuen Systems der *Domain-Registry* und eines Streitschlichtungsverfahrens. In Genf bildete sich innerhalb des IFWP ein grundlegender Konsens über die Struktur des neuen Systems heraus<sup>555</sup>. Es sollte ein *Domain Name Council* gebildet werden, welcher sich der Domainpolitik zum Beispiel bezüglich der Grundvoraussetzungen und der zu untersuchenden offenen Themen annehmen sollte. Eine Portabilität des DNS sollte erreicht werden, um den Wettbewerb zu sichern. Im Gegenzug arbeitete die IANA entgegen den Traditionen im Internet und versuchte hinter geschlossenen Türen mit der ISOC, NSI und weiteren Beteiligten Vereinbarungen zu treffen<sup>556</sup>. Vorangetrieben wurden die Verhandlungen durch das bevorstehende Ende des Vertrages des US-DoC mit der NSI Ende September 1998.

---

<sup>550</sup> Lessing, Lawrence: „...the implications of creating a special non-profit agency seems like a substitute for government, but one that does not have to answer to an electorate.“, zit. in *TechWeb*, *Krochmal*, Magaziner, Lessig Spar Over Domain Name Plan, 11. Juni 1998.

<sup>551</sup> Vgl. zum Problemkreis *Liu*, 74 Ind. L.J. 587, 616f.

<sup>552</sup> *HLRA*, 112 Harv. L. Rev. 1657, 1670 und *Liu*, 74 Ind. L.J. 587, 617.

<sup>553</sup> Siehe auch *US-GAO*, Report, S. 7.

<sup>554</sup> Siehe weitere Erörterungen bei *HLRA*, 1672 und *Milton Internetdebris*.

<sup>555</sup> Siehe *TechWeb*, *Mosquera*, Groups Build Unity, Lay Down Swords, 3. Juli 1998, Konferenz Chair Tamar Frankel: „We are beginning to build a real trust and dependence on each other [...] The cultures of the Internet -- the corporate and service provider cultures -- are slowly merging.“ Siehe auch *UnixInsider*, *Essick*, Steps made in formation of new domain name organization, August 1998.

<sup>556</sup> Kritisiert besonders durch *Mueller*, 1 info 6, 497, 506f.

Obgleich die Prozesse von der IANA und dem IFWP parallel verliefen, wurden durch die gegenseitige Teilnahme an den Beratungen die Verbindungen zueinander immer stärker. Das Verschmelzen dieser beiden Diskussionsrunden wurde jedoch durch die schließlich ablehnende Haltung der IANA verhindert<sup>557</sup>. Zu einem ursprünglich geplanten Schlußtreffen zwischen IANA und IFWP kam es auf Grund der einseitigen Verhandlungen der IANA mit der US-Regierung nicht mehr. Das IFWP wurde schließlich ohne Ergebnis aufgelöst. Die IANA veröffentlichte Mitte September 1998 ihren letzten Vorschlag<sup>558</sup> für eine neue internationale und gemeinnützige Organisation zur Verwaltung des DNS<sup>559</sup>. Im September wurde schließlich die *Internet Corporation for Assigned Names and Numbers* (ICANN) von der IANA gegründet.

Am 2. Oktober 1998 übermittelte Dr. Jon Postel Dokumente über die Organisation und Struktur der ICANN an das US-DoC (an die US-NTIA) als Vorschlag für den IANA-Nachfolger<sup>560</sup>. Neben diesen erhielt die US-NTIA drei weitere Vorschläge. Ein Vorschlag wurde von der *Open Root Server Confederation* (ORSC) eingereicht<sup>561</sup>, einer Gruppe alternativer *Registries* (siehe Kapitel 5.1 unten). Der nächste kam von einer unabhängigen und informellen Gruppe von ICANN-Kritikern, der *Boston Working Group* (BWG)<sup>562</sup>. Der dritte wurde von der *Information Network Engineers Group* (INEG Inc.) eingereicht und stellte einige Verbesserungsvorschläge zum Vorschlag der IANA dar<sup>563</sup>. Alle Dokumente wurden von der US-NTIA zunächst kurzfristig öffentlich zur Diskussion gestellt und die inzwischen gegründete ICANN wurde aufgefordert, mit der BWG und der ORSC<sup>564</sup> Verhandlungen zu führen, um einen Konsens in der Internetgemeinschaft zu erreichen<sup>565</sup>. Dr. Jon Postel ernannte inzwischen die Mitglieder des *Interim Boards* der ICANN. Am 18. Oktober 1998, mit dem plötzlichen Tod Dr. Jon Postels als eine der treibenden Kräfte des Internets, erfuhren die Bemühungen der IANA einen personellen und fachkundigen Rückstoß<sup>566</sup>. Dennoch wurde am 25. November 1998 die ICANN vom US-DoC offiziell als die Organisation anerkannt, wel-

---

<sup>557</sup> Siehe *Mueller*, 1 info 6, 497, 507.

<sup>558</sup> Die Vorschläge zum Gründungsdokument und zur Satzung sind unter *IANA*, <http://www.iana.org/description2.html> zu finden.

<sup>559</sup> Siehe *Wired*, *McKay*, New Internet Government Forged, 17. September 1998 sowie *UnixInsider*, *Mills*, Proposal for new Internet organization goes public, September 1998.

<sup>560</sup> Siehe *Postel*, Proposal for the Internet Corporation for Assigned Names and Numbers (ICANN), 2. Oktober 1998, <http://www.ntia.doc.gov/ntiahome/domainname/proposals/icann/icann.html>.

<sup>561</sup> Siehe *ORSC*, Re: Management of Internet Names and Addresses, 8. Oktober 1998, [http://www.ntia.doc.gov/ntiahome/domainname/proposals/orsc/ORSC\\_PRO.htm](http://www.ntia.doc.gov/ntiahome/domainname/proposals/orsc/ORSC_PRO.htm).

<sup>562</sup> Siehe *Boston Working Group*, Re: Management of Internet Names and Addresses, 28. September 1998, <http://www.ntia.doc.gov/ntiahome/domainname/proposals/bosgrp/submission-letter.html>.

<sup>563</sup> Siehe *Jeff Williams*, *INEG. INC.*, Proposal Bylaws Proposal for the ICANN, 5. Oktober 1998, <http://www.ntia.doc.gov/ntiahome/domainname/proposals/ineginc/ineginc.htm>.

<sup>564</sup> Beide Organisationen wurden nach dem gescheiterten Treffen zur Vereinigung von IANA und IFWP gegründet.

<sup>565</sup> Vgl. die Ausführungen in *Mueller*, 1 info 6, 497, 508, Fn. 37 und *US-GAO*, Report, S. 38.

<sup>566</sup> Zu Dr. Jon Postel siehe auch Fn. 333.

### 3.1. Geschichtlicher Hintergrund der ICANN

---

che die Nachfolge der IANA antreten sollte<sup>567</sup>. In einem *Memorandum of Understanding* wurde die ICANN aufgefordert, Mechanismen, Methoden und Verfahren zum Transfer des DNS auf den privaten Sektor zu entwickeln.

#### 3.1.3. Vertragliche Grundlagen der Autorität der ICANN

Die Satzung der ICANN verlangte die Entwicklung von völlig neuen Strukturen um Verantwortung, Repräsentation und Regulierung auf globaler Ebene zu ermöglichen<sup>568</sup>. Dazu sollten drei *Supporting Organizations* und ein *Board of Directors* eingesetzt werden. Das einberufene *interim Board* mußte zunächst den Richtlinien des *White Papers* folgen, um die Anerkennung der ICANN durch das US-DoC nicht zu gefährden. Das *White Paper* verlangte von der ICANN und der WIPO die Entwicklung einer Schiedsgerichtsregelung zur Lösung von Markenrechtskonflikten<sup>569</sup>. Ebenso wurde im Papier verlangt, daß von der ICANN ein *shared Registry System* für die Teilnahme von konkurrierenden *Registrars* an der Vergabe von .com, .net und .org Domainnamen zu entwickeln sei. Um diese Aufgaben zu lösen, benötigte die ICANN zunächst die Kontrolle über den gesamten Registrierungsprozeß. Eine Kollision mit den Interessen von NSI blieb folglich unausweichlich.

##### 3.1.3.1. NSI/DoC-Amendment Nr. 11 und ICANN/US-DoC-MoU

Das *White Paper* ließ in seinen Forderungen den zukünftigen Status der *NSI-Registry* offen. Das DNS sollte jedoch zumindest durch den privaten Sektor auf freiwilliger Basis durch die Teilnahme der verschiedenen Interessensgruppen verwaltet werden. Entsprechend war die Gründung der ICANN der erste Schritt zu einem privaten Management des DNS. Ursprünglich stand NSI mit der US-NSF<sup>570</sup> in einem *Cooperative Agreement*<sup>571</sup>. Unter diesem Vertrag hatte die NSI als *Registrar* das exklusive Vergaberecht von Domainnamen unter den TLDs .com, .org und .net und war gleichzeitig der Verwalter (als *Registry*) der dazugehörenden Domaindatenbank (vgl. Abbildung 5 unten).

---

<sup>567</sup> US-DoC/ICANN, Memorandum of Understanding Between the U.S. Department of Commerce and the Internet Corporation for Assigned Names and Numbers, <http://www.ntia.doc.gov/ntiahome/domainname/icann-memorandum.htm>.

<sup>568</sup> Die originale Fassung der Satzung der *ICANN* vom 6. November 1998 befindet sich unter ICANN Adopted Bylaws, <http://www.icann.org/general/archive-bylaws/bylaws-06nov98.htm>.

<sup>569</sup> US-DoC, NTIA, White Paper, 63 Fed. Reg. 31741, 31747.

<sup>570</sup> 1998 zum US-DoC übertragen.

<sup>571</sup> Siehe Cooperative Agreement zwischen NSI und der US-Regierung, Fn. 456.

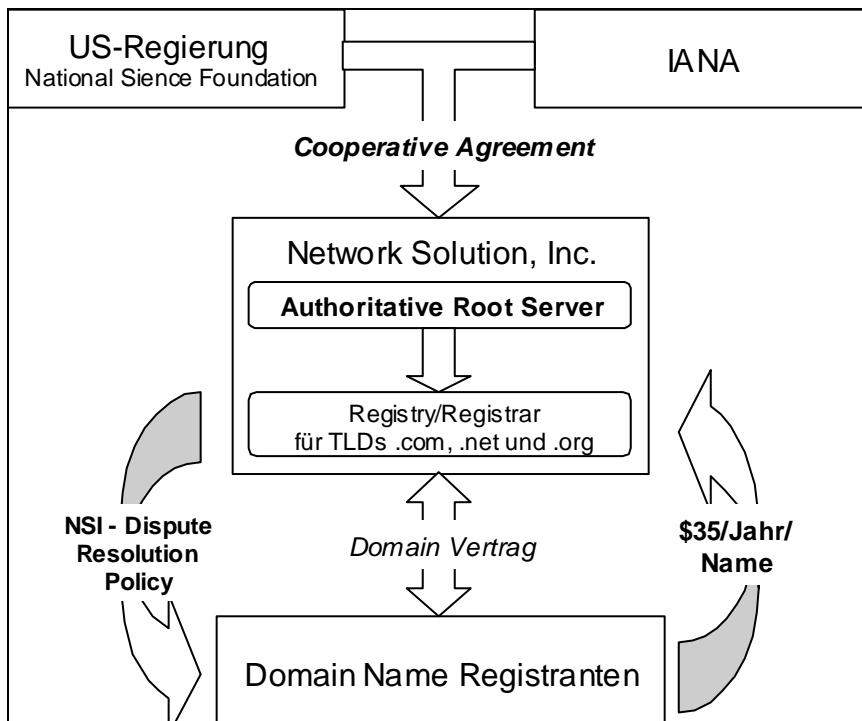


Abbildung 5 – Verhältnis NSI-IANA-NSF bis 1998.

Das Recht der NSI Domainnamen zu registrieren, sollte nach den Verträgen mit der US-NTIA am 31. März 1998 enden, jedoch bestand die Option einer Verlängerung des Vertrages durch die US-Regierung. NSI nutzte dabei den Besitz an der Domaindatenbank aus, um sein Vergabemonopol zu sichern. So behauptete die NSI regelmäßig, daß sie ein Recht an der Datenbank erworben hätte und somit nicht verpflichtet wäre, die Datenbank dem US-DoC oder der ICANN zu überlassen. Vielmehr drohte die NSI, eigenständig tätig zu werden und ein alternatives *Root Server System* zu installieren. Die NSI nutzte dazu geschickt ihren Besitz an der Domaindatenbank als Druckmittel in den Verhandlungen mit dem US-DoC aus, um eine für sie vorteilhafte Verlängerung des *Cooperative Agreement* zu erlangen.

Ende 1998 wurde schließlich das *Cooperative Agreement* zwischen der NSI und dem US-DoC bis zum 30. Oktober 2000 verlängert<sup>572</sup>. Innerhalb der neuen Vereinbarung wurde NSI verpflichtet, ein *Shared Registry System* zu erstellen, welches im Wettbewerb stehenden *Registrars* die gleichberechtigte Vergabe von Domainnamen unter den TLDs .com, .org und .net ermöglichen sollte. NSI selbst sollte jedoch zunächst weiter als *Registry* fungieren und gleichzeitig als *Registrar* Domainnamen registrieren dürfen. NSI versprach weiter, der US-Regierung eine Kopie der Registrierungsdaten zu überlassen und keine Veränderungen am *Root Server* ohne schriftliche Autorisierung durch das US-DoC vorzunehmen. Als wichtigsten Punkt beinhaltete die neue Vereinbarung, daß NSI die vom US-DoC zu benennende neue Verwaltungsorganisation anerkennt. Einmal benannt, sollte NSI darüber hinaus bei der Entwicklung des *Shared Registry System* mit der neuen Organisation intensiv zusammenarbeiten

<sup>572</sup> NSI, Cooperative Agreement, Amendment No. 11, Fn. 530. Der Zeitplan richtete sich nach dem Amendment No. 12, [http://www.networksolutions.com/en\\_US/legal/internic/cooperative-agreement/amendment12.html](http://www.networksolutions.com/en_US/legal/internic/cooperative-agreement/amendment12.html).

### 3.1. Geschichtlicher Hintergrund der ICANN

---

und der Verwaltungsorganisation in diesem Bereich technische Assistenz bieten. ICANNs wichtigste Aufgabe bestand nun darin, vom US-DoC formell anerkannt zu werden. Mit einer solchen Anerkennung als neue Verwaltungsorganisation konnte dann die NSI mit seinen Pflichten aus *Amendment No. 11* zum *Cooperative Agreement*<sup>573</sup> in Anspruch genommen werden.

Am 25. November 1998 traten die ICANN und das US-DoC in ein *Memorandum of Understanding*<sup>574</sup> zur Sicherung der Übertragung des DNS-Managements auf die ICANN ein. Im ICANN/US-DoC-MoU vereinbarten die Parteien, daß ICANN die Privatisierung des DNS untersucht, indem es aktiv die dazu notwendigen Funktionen wahrnimmt. Der Zweck und die Aufgaben der Zusammenarbeit zwischen US-DoC und ICANN werden in diesem Vertrag ausführlich erläutert:

#### II. ... B. Purpose

Before making a transition to private sector DNS management, the DOC requires assurances that the private sector has the capability and resources to assume the important responsibilities related to the technical management of the DNS. [...]

In the DNS Project, the parties will jointly design, develop, and test the mechanisms, methods, and procedures to carry out the following DNS management functions:

- a. Establishment of policy for and direction of the allocation of IP number blocks;
- b. Oversight of the operation of the authoritative root server system;
- c. Oversight of the policy for determining the circumstances under which new top level domains would be added to the root system;
- d. Coordination of the assignment of other Internet technical parameters as needed to maintain universal connectivity on the Internet; and
- e. Other activities necessary to coordinate the specified DNS management functions, as agreed by the Parties.

Das *Memorandum of Understanding* bildete den Beginn des Aufbaues eines verwobenen und komplizierten Vertragsgebildes mit Privilegien für bestimmte Interessensgruppen und an der Organisation beteiligten Unternehmen<sup>575</sup>. Der erste Schritt, die Anerkennung der ICANN durch das US-DoC, war mittels dieses Vertrages in die Wege geleitet worden, obgleich es dem US-DoC noch offen stand, die Verbindung zur ICANN wieder zu beenden und eine andere Körperschaft zur Ausübung der IANA-Funktionen zu finden. Mit der Aufgabe, ein Studium über die Möglichkeiten einer Privatisierung des DNS durchzuführen, war gewissermaßen schon eine Autorisierung der ICANN verbunden<sup>576</sup>. ICANN konnte entsprechend dem

---

<sup>573</sup> NSI, Cooperative Agreement, Amendment No. 11, Fn. 530.

<sup>574</sup> US-DoC/ICANN Memorandum of Understanding, Fn. 567.

<sup>575</sup> Vgl. Froomkin, 50 Duke L.J. 17, 71.

<sup>576</sup> Vgl. Froomkin, 50 Duke L.J. 17, 84f.

MoU als die im *White Paper* erwähnte gemeinnützige Organisation unter den dort bestimmten Prinzipien<sup>577</sup> agieren. Das *Transition-MoU* sollte bis 30. September 2000 laufen, wurde aber bis zum 30. September 2002 verlängert<sup>578</sup>. Sollte ICANN die vom US-DoC im MoU bestimmten Auflagen erfüllen, kann es mit der vollständigen Übertragung der Kontrolle über das DNS rechnen.

Nach einer erfolgreichen Anerkennung durch das US-DoC übernahm die ICANN IANAs Rolle in der DNS-Verwaltung und mußte schließlich die Anerkennung der NSI erringen. Erst durch die Unterordnung der NSI unter die ICANN war es möglich, allgemeingültige Regeln (wie die *Universal Domain Name Dispute Resolution Policy* der WIPO) für alle Domainnamensinhaber verpflichtend umzusetzen.

Um die Übernahme der IANA-Funktionen zu ermöglichen, wurden zwischen der ICANN und dem US-DoC im September 2000 zwei weitere Verträge geschlossen<sup>579</sup>, das *Cooperative Research and Development Agreement*<sup>580</sup> (CRADA) und der *Contract Between ICANN and the United States Government for Performance of the IANA Function*<sup>581</sup> vom 2. September 2000. Im CRADA vereinbarten beide Parteien, daß die ICANN untersuchen solle, wie die Funktionen der IANA verbessert werden könnten. Diese Aufgabe konnte nur wahrgenommen werden, soweit die Funktionen der IANA bereits durch die ICANN ausgeführt wurden<sup>582</sup>. Obgleich schon auf Grund eines Vertrages mit der USC die ICANN die Funktionen der IANA wahrnahm und für die Zahlungsverpflichtungen der IANA aufkam<sup>583</sup>, hatte das US-DoC noch nicht offiziell dem Transfer zugestimmt. Eine solche vertragliche Regelung erfolgte im Dezember 1998 mittels des sogenannten *Sole Source Contract*<sup>584</sup>, um die Dienste der IANA auf die ICANN zu übertragen. Der Vertrag wurde im Februar 2000 mit der Bestimmung ergänzt, daß ICANN die IANA-Funktionen aufzukaufen hat (zum Preis von 0 US\$<sup>585</sup>). Eine Anerkennung der ICANN als Betreiber der IANA erfolgte durch die von ihr betroffene IETF am 1. März 2000 mittels eines *Memorandum of Understanding Concerning the Technical Work of the Internet Assigned Numbers Authority*<sup>586</sup>.

---

<sup>577</sup> Diese Prinzipien des White Papers (siehe Kap. 3.1.2.5.) waren auch Bestandteil dieses MoU: Stabilität des Internets, private bottom-up Koordination, Wettbewerb und Repräsentation der Internetgemeinschaft, siehe *US-DoC/ICANN Memorandum of Understanding*, Fn. 567, Kap. II. C.

<sup>578</sup> Vgl. *ICANN-Announcement*, ICANN and U.S. Government Agree to Extend Agreements, 4. September 2000 und *ICANN*, Ammendment 4, 24. September 2001, <http://www.icann.org/general/amend4-jpamou-24sep01.htm>.

<sup>579</sup> Siehe auch die Erörterungen in *US-GAO*, Report, S. 12ff.

<sup>580</sup> Siehe *US-DoC, NTIA/ICANN Cooperative Research & Development Agreement*, <http://www.icann.org/committees/dns-root/crada.htm>.

<sup>581</sup> Siehe *Contract Between ICANN and the US-DoC for Performance of the IANA Function*, 2. September 2000, <http://www.icann.org/general/iana-contract-09feb00.htm>.

<sup>582</sup> Vgl. auch *Froomkin*, 50 Duke L.J. 17, 85f. und *US-GAO*, Report.

<sup>583</sup> Vgl. auch *Froomkin*, 50 Duke L.J. 17, 86. und *US-GAO*, Report, S. 17ff.

<sup>584</sup> *US-DoC/ICANN Memorandum of Understanding*, Fn. 567.

<sup>585</sup> Siehe die Kopie der Vertragsurkunde: *Contract Between ICANN and the United States Government for Performance of the IANA Function*, 9. Februar 2000, Fn. 581.

<sup>586</sup> Vgl. *RFC 2860*, Carpenter/Baker/Roberts.

#### 3.1.3.2. Verhältnis zwischen NSI, ICANN und US-DoC

Im Februar 1999 veröffentlichte die ICANN eine Reihe von Regeln<sup>587</sup> für die Teilnahme am *Shared Registry System* von der NSI. In diesen wurden finanzielle und wirtschaftliche Voraussetzungen festgelegt. Eine einmalige Gebühr von 5.000 US\$ sollte an ICANN gezahlt werden, sowie je registrierten Namen 1 US\$ im Jahr. Um die geplanten WIPO-Regeln vorwegzunehmen, enthielten die *Registration Accreditation Guidelines* schon Bestimmungen zum Schutz von Markenrechtsinhabern. Am 21. April 1999 wurden schließlich fünf *Registrars*<sup>588</sup> für die sogenannte *Testbed Shared Registry* zugelassen. Deren Verhältnis zur NSI wurden zur gleichen Zeit mittels einer weiteren Vereinbarung dem *Amendment No. 13* zwischen dem US-DoC und der NSI geregelt<sup>589</sup>:

The Department of Commerce and Network Solutions, Inc. agree that for the Phase I deployment of the Shared Registration System, NSI's prices for Registry Services through the Shared Registration System in the gTLDs for which NSI now acts as the Registry, will be no more than \$9 per year per second level domain name registered, payable at \$18 for new registrations and \$9 per year on the anniversary date of the original registration beginning at the end of the second year and for every year thereafter.

Neben dem Preis für die Domainregistrierung von 9 US\$ wurde ein *Registrar License and Agreement*<sup>590</sup> bestimmt, welches zwischen NSI und den neuen Registraturen zur Anwendung kommen sollte. NSI konnte jedoch immer noch aus eigener Hand *Registry- und Registrar-Service* anbieten. Die Einführung neuer Registraturen war damit nur ein kleiner Schritt hin zum freien Wettbewerb in der Domänenamensvergabe. Zunächst bestand nur für die NSI der Zwang an eine kleine Auswahl an Unternehmen, die an ICANN Gebühren für dieses Privileg zahlten, einen regulierten Rabatt zu gewähren. Für NSI hatte die Teilnahme weiterer *Registrars* den Vorteil, daß mehr Domänenamen vergeben wurden und NSI in der Funktion als *Registry* der TLDs .com, .net und .org mehr Umsatz verbuchen konnte<sup>591</sup>. ICANN erhielt deshalb ungeachtet die Autorität über die *Registrars* und damit die Möglichkeit die Vergabe von Konzessionen für *Registrars* als Einnahmequelle zu nutzen.

Im nächsten Schritt sollte NSI mit ICANN ein *Registrar Accreditation Agreement* schließen und damit ein weiterer *Registrar* neben den schon akkreditierten *Registrars* werden. Gleich-

---

<sup>587</sup> Guidelines for Accreditation of Internet Domain Name Registrars and for the Selection of Registrars for the Shared Registry System Testbed for .com, .net and .org domains, 8. Februar 1999,

<http://www.icann.org/draftguidelines.html>.

<sup>588</sup> Siehe *ICANN-Announcement*, ICANN Names Competitive Domain-Name Registrars, 21. April 1999. Die neuen Registraturen sind: America Online, CORE (Internet Council of Registrars), France Telecom/Oléane, Melbourne IT und register.com.

<sup>589</sup> Amendment No. 13 zum Cooperative Agreement,

[http://www.networksolutions.com/en\\_US/legal/internic/cooperative-agreement/amendment13.html](http://www.networksolutions.com/en_US/legal/internic/cooperative-agreement/amendment13.html).

<sup>590</sup> US-DoC, NTIA, Registrar License and Agreement, 4. November 1999,

<http://www.ntia.doc.gov/ntiahome/domainname/rla42199.htm>.

<sup>591</sup> Vgl. Mueller, 1 info 6, 497, 511.

falls sollte NSIs *Registry* der ICANN untergeordnet werden und die NSI diese nur noch in Übereinstimmung mit ICANN weiterführen dürfen. Damit würde NSI die exklusive Kontrolle über die gTLDs entzogen werden. Sollte sich die NSI weigern, ein Vertragsverhältnis mit der ICANN einzugehen, bestände das Risiko, daß die NSI als Besitzer der Domainindatenbank für die gTLDs ohne Autorisierung durch die ICANN oder durch das US-DoC weiter mit der Registrierung von Domainnamen fortfahren und ein alternatives *Root Server System* errichten würde<sup>592</sup>.

Die NSI reagierte auf die Gefahr einer Entmachtung mit einer Lobbykampagne vor dem *US-Congress* und erreichte eine Anhörung mit dem Thema „Is ICANN out of control?“<sup>593</sup>. Dabei sollte die von der ICANN ursprünglich vorgesehene Gebühr von 1 US\$ je Domainnamen und die Machtanmaßung von ICANN und US-DoC erörtert werden. Im Gegenzug nutzten ICANN-Befürworter die Gelegenheit zu einer offenen Kritik an dem Ex-Monopolisten NSI. Insbesondere wurde die Verzögerungstaktik seitens der NSI bei der Inbetriebnahme des *Shared Registry Systems* hervorgehoben und angemerkt, daß die ICANN ihre Aufgabe, Sicherheit für den Internetbetrieb und freien Wettbewerb zu gewährleisten, nur nach Anerkennung durch die NSI optimal erfüllen könne. Ende September 1999 konnten die drei Parteien NSI, US-DoC und ICANN eine Serie von Kompromissen schließen<sup>594</sup> und somit die Streitigkeiten beilegen (vgl. Abbildung 6 unten). Die vereinbarten Hauptpunkte sind<sup>595</sup>:

- NSI erkennt ICANN an und willigt ein, die *gTLD-Registry* unter Einhaltung eines *Registry Agreement* mit ICANN zu führen.
- Im Gegensatz stimmt ICANN zu, NSI als *gTLD-Registry* zu lizenziieren.
- NSI stimmt zu, nur von ICANN akkreditierte *Registrars* zu akzeptieren.
- Weiterhin verpflichtet NSI sich, kein alternatives *Root Server System* zu entwickeln.
- Der Registrierungspreis eines Domainnamen sollte ab 15. Januar 2000 statt 9 US\$ nur noch 6 US\$ betragen.
- Ebenso willigte NSI ein, an die ICANN eine *Registrar*-Gebühr von 1,25 Mio. US\$ zu zahlen.
- Schließlich soll NSI weiterhin den *Authoritative Root Server* in Übereinstimmung mit dem US-DoC führen.

---

<sup>592</sup> Vgl. ausführlich *Mueller*, 1 info 6, 497, 513f.

<sup>593</sup> Siehe *Internet Intern*, NSI unter Beschuß, 17. November 1999 und *Ermert*, Telepolis 5107.

<sup>594</sup> Die einzelnen Verträge sind das Amendment No. 19 zum US-DoC/NSI Cooperative Agreement, das Amendment No. 1 zum *US-DoC/ICANN* Memorandum of Understanding, das NSI/ICANN Registry Agreement und das ICANN/NSI Registrar Transition Agreement. Die vom *ICANN-Board* anerkannten Fassungen vom 4. November 1999 können unter Tentative Agreements among ICANN, the U.S. Department of Commerce, and Network Solutions, Inc., <http://www.icann.org/nsi/tentative-agreements.htm> eingesehen werden. Siehe auch die Zusammenfassung *NTIA*, Fact Sheet, <http://www.ntia.doc.gov/ntiahome/domainname/agreements/summary-factsheet.htm>.

<sup>595</sup> Siehe auch die ausführlichen Erörterungen unter *Froomkin*, 50 Duke L.J. 17, 90ff.

### 3.1. Geschichtlicher Hintergrund der ICANN

- Das US-DoC wird jedoch nicht in absehbarer Zeit die Autorität über den *Root Server* an eine unabhängige Institution abgeben<sup>596</sup>.

Im Gegenzug wurden ICANN verschiedene Pflichten auferlegt:

- ICANNs Autorität über die *gTLD-Registry* soll beendet werden können, wenn es ICANN nicht gelingt, die *ccTLD-Registries* in das Vertragsgebilde der ICANN einzugliedern und NSI dadurch wettbewerblich benachteiligt würde.
- Eine Bindung an Verfahrensgrenzen war vorgesehen. Insbesondere sollten bestimmte Entscheidungen der ICANN von der Mehrheit der sogenannten *Supporting Organizations* getragen werden.
- Die Gebühren, welche ICANN von den *Registrars* verlangt, müssen gleichmäßig verteilt sein.
- Die *Registrar*-Gebühr seitens der NSI soll auf maximal 2 Mio. US\$ begrenzt sein.

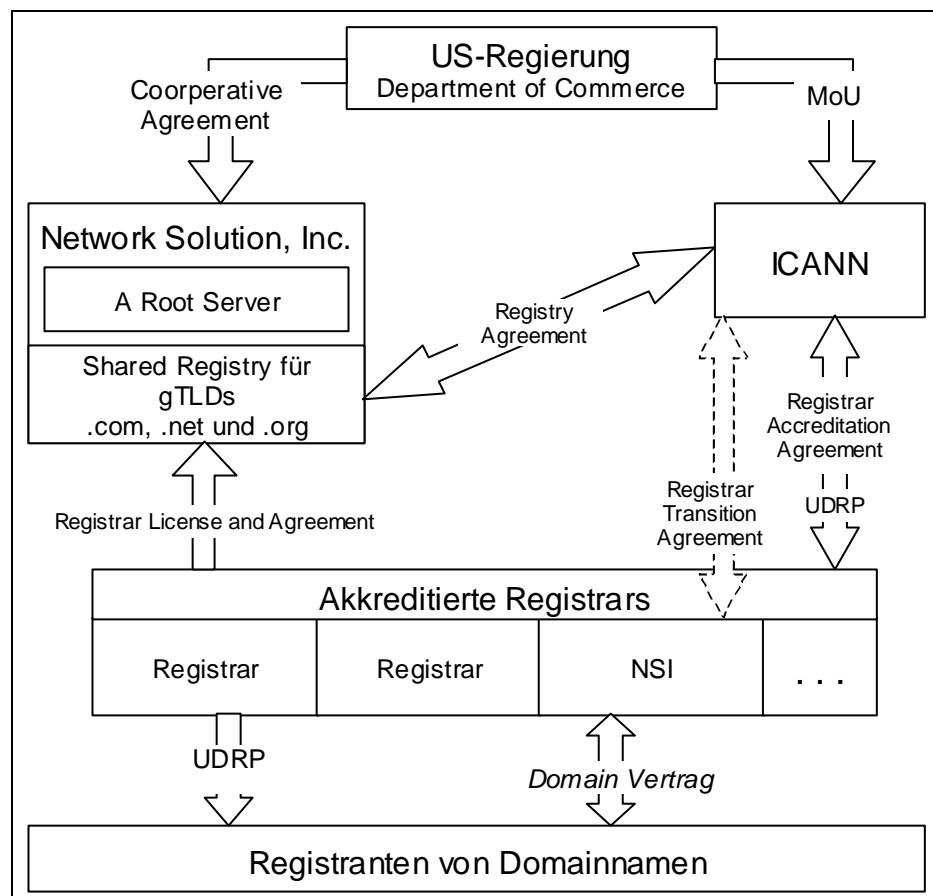


Abbildung 6 – Verhältnis NSI/ICANN/US-DoC nach September 1999.

Zwei Einschränkungen verhinderten die vollständige Übernahme der Kontrolle über das DNS. Zum einen hatte sich das US-DoC ein Kontrollrecht über die Entscheidungen der

<sup>596</sup> Siehe *US-GAO*, Report, S. 27ff.

ICANN bezüglich des DNS zurückbehalten. Zum anderen sollten das ICANN/US-DoC-MoU und der *Sole-Source Contract* im September 2000 auslaufen.

### 3.2. Arbeit der ICANN

Die im Oktober 1998 gegründete ICANN stellt derzeit eine der meist diskutierten Organisationen des Internets dar. Die ICANN ist eine *Nonprofit Public Benefit Corporation*<sup>597</sup> im Sinne der §§ 5110 bis 6910 des *California Corporations Codes*<sup>598</sup> (hier Abschnitt 2: *Nonprofit Corporation Law*, Teil 2: *California Nonprofit Public Benefit Corporation Law*). Die Organisationsstrukturen und das Verfahren innerhalb der ICANN werden durch die *Articles of Incorporation*<sup>599</sup> und die Satzung<sup>600</sup> der ICANN festgelegt.

Als privatrechtlich organisierte Gesellschaft gemeinnützigen Charakters bindet sie eine Reihe von Internetakteuren, denen Vertreter aus Technik und Wissenschaft sowie der Nutzerseite angehören. Die ICANN koordiniert vier Schlüsselbereiche der Internet-Verwaltung: das *Domain Name System*, die Internet-Protokoll-Adressierung (IP-Adressierung), die Verwaltung des *Root Server Systems* und die Vergabe von Protokoll-Nummern. Dabei hat sie die Stabilität des Internetbetriebes sicherzustellen und den Wettbewerb zu fördern. Umstritten ist jedoch, ob die ICANN dabei nur technische Aufgaben wahrnehmen soll, oder auch politische Konzepte entwickeln darf<sup>601</sup>. Von dieser Problemlage ausgehend, wirft die ICANN als Organisation weitere Fragen auf. Strittig ist, inwieweit ICANN die Internetgemeinschaft umfassend und vollständig zu repräsentieren hat, ob sich ICANN demokratischen Strukturen zu unterwerfen hat und inwieweit Regierungsvertreter am Arbeitsprozeß der ICANN teilzunehmen haben.

Ursprünglich sollte ICANN, wie die Internetorganisationen, auf internetspezifischen Prinzipien aufgebaut werden. Sie sollte offen sein, auf freiwilliger Basis agieren, Standards als Grundlage haben und einem dezentralisierten auf Konsens basierenden Entscheidungsprozeß folgen. Die Einhaltung dieser Prinzipien könnte Lösungswege für viele Probleme bieten, welche sich aus ICANNs Struktur und Funktion ergeben<sup>602</sup>. Die ICANN sollte offen im Sinne sein, daß jeder Interessent, der gewillt ist, konstruktiv mitzuarbeiten, sich Arbeitsgruppen innerhalb der ICANN anschließen kann. ICANNs Entscheidungen sollten nicht den Zwang einer gesetzlichen Regelung beinhalten, sondern vielmehr eine freiwillige Teilnahme an gesetz-

---

<sup>597</sup> Die Anerkennung der Gemeinnützigkeit erfolgte durch das *US-Department of Treasury* mittels des IRS Letter Granting Tax Exemption vom 28. August 2000, <http://www.icann.org/financials/tax/us/irs-letter-grant-28aug00.htm>.

<sup>598</sup> Der Gesetzestext des California Corporations Code ist unter *California Law* einsehbar, <http://www.leginfo.ca.gov/cgi-bin/calawquery?codesection=corp>.

<sup>599</sup> ICANN, Articles of Incorporation of Internet Corporation for Assigned Names and Numbers, 21. November 1998, <http://www.icann.org/general/articles.htm>.

<sup>600</sup> ICANN, Bylaws for Internet Corporation for Assigned Names and Numbers, Fassung vom 16. Juli 2000, <http://www.icann.org/general/bylaws.htm>.

<sup>601</sup> So *Europäisches Parlament*, Entschließungsantrag, A5-0063/2001, (KOM(2000)202 – 2000/2140/COS), 19. Februar 2001, Einleitung.

<sup>602</sup> Siehe *Johnson/Crawford*, The Idea of Icann.

ten Standards ermöglichen. Standardbasierend bedeutet, daß die ICANN sich nicht einer Gruppe von Interessensvertretern oder Mitgliedern unterwerfen darf, sondern nach allgemeinen, im Internet anerkannten Regeln agieren sollte. Soweit ICANN Richtlinien verabschiedet, sollte sie beachten, daß die meisten Handlungen, welche die Funktionalität und den Wert des Internets beeinflussen, durch unabhängige Parteien vorgenommen werden. Globale Richtlinien sollten folglich nur verabschiedet werden, wenn eine Notwendigkeit zur uniformen Umsetzung von Aufgaben besteht. Das Streben nach Konsens bildet eines der Erfolgsprinzipien des Internets. Es sollte möglichst die ganze Palette an Interessen in die Entscheidungsfindung der ICANN Eingang finden und der Weg des Kompromisses gesucht werden.

Um den Entscheidungsprozeß der ICANN zu verdeutlichen, sollen deshalb im Folgenden Ausführungen zu den Aufgaben, der Struktur und der Legitimation der ICANN gegeben werden.

#### 3.2.1. Funktionen der ICANN

Wie schon erwähnt, liegt der grundlegendste Streitpunkt in der Frage, ob es sich bei der ICANN um ein Kommitte zur technischen Koordinierung von Internetfunktionen handelt oder ob ICANN als politischer Entscheidungsträger anzusehen ist. ICANN selbst charakterisiert ihre Arbeit als technische Koordination<sup>603</sup> und will damit der langen und erfolgreichen Tradition der Standardsetzung durch die Internetingenieure folgen. Die *Articles of Incorporation* vom 21. November 1998 sehen eine kurze Definition der Aufgaben vor<sup>604</sup>:

3. [... T]he Corporation shall [...] pursue the charitable and public purposes of lessening the burdens of government and promoting the global public interest in the operational stability of the Internet by
  - (i) coordinating the assignment of Internet technical parameters as needed to maintain universal connectivity on the Internet;
  - (ii) performing and overseeing functions related to the coordination of the Internet Protocol (“IP”) address space;
  - (iii) performing and overseeing functions related to the coordination of the Internet domain name system (“DNS”), including the development of policies for determining the circumstances under which new top-level domains are added to the DNS root system;
  - (iv) overseeing operation of the authoritative Internet DNS root server system; and
  - (v) engaging in any other related lawful activity in furtherance of items (i) through (iv).

---

<sup>603</sup> Siehe z.B. *ICANN*, Fact Sheet, 17. Februar 2001, <http://www.icann.org/general/fact-sheet.htm>. Deutlich drückte dies ICANN-Board Mitglied *Hans Kraaijenbrink* auf dem öffentlichen Forum der ICANN in Kairo, Ägypten vom 9. März 2000 aus: „[The] [m]ission of ICANN is the technical coordination of certain essential parameters for the Internet names and addresses, nothing more, nothing less. Anyone who says it is more is confusing the Internet community.“, *Scribe’s Notes*, ICANN Public Forum, <http://cyber.law.harvard.edu/icann/cairo/archive/scribe-icann-030900.html>.

<sup>604</sup> Siehe *ICANN*, Articles of Incorporation, Fn. 599.

Diese Aufgabenaufstellung läßt zunächst annehmen, daß ICANN auf die technische Verwaltung des Namens- und Adreßraumes beschränkt sei. Soweit sich ICANN an diese technischen Punkte hält, besteht ein nur geringes Risiko, daß sie sich mit politischen Aktionen in Konkurrenz und Mißkredit zu nationalstaatlichen Regierungen begibt. Aus der eigenen Charakterisierung als technisches Gremium kann man schlußfolgern, daß beschlossene Regelungen, wie bei den Internetstandards üblich, vom Konsens der Internetgemeinschaft getragen werden müßten<sup>605</sup>. Regelungen würden wie bei der IETF (siehe Kapitel 2.4.1.2.2 oben) in Arbeitsgruppen, entworfen, durch die sogenannten *Supporting Organizations* anerkannt und von der Internetgemeinschaft umgesetzt. Auch das US-DoC charakterisierte im *White Paper*, daß die damals noch zu gründende Organisation, für die „narrow issues of management and administration of Internet names and numbers on an ongoing basis“ zuständig sein sollte<sup>606</sup>. Das DNS mit seinem Rootserver und den verschiedenen Domainnamensservern stellt jedoch eines der wichtigsten Organe des Internets dar. Die eigentliche Beschränkung der Aufgaben auf reines technisches Management heißt damit nicht, daß die ICANN durch die Teilnahme verschiedener Interessensvertreter nicht zu Handlungen gedrängt wird, welche auch politische Bedeutung innehaben<sup>607</sup>. Auch ist zu bedenken, daß die eigentliche technische Arbeit, die Entwicklung von Protokollen in anderen Organisationen, wie in der IETF oder in der ITU geschieht. Die ICANN ist vielmehr ein Gremium, in dem den Protokollorganisationen eine Möglichkeit zum Gedankenaustausch und zur Zusammenarbeit gegeben werden kann. Die ICANN kann somit für die globale Harmonisierung sorgen. Die Diskussion über die Protokolle sollte jedoch weiterhin den Standardisierungsorganisationen überlassen werden.

Könnte man ICANNs Tätigkeit auf technische Thematiken einschränken, dann würde die Notwendigkeit einer ausgeprägten demokratischen Repräsentation innerhalb der ICANN entfallen. Da letztendlich der Markt entscheiden wird, welche technische Lösung die optimale darstellt, ist es nicht notwendig über technische Protokolle abzustimmen. Würde allerdings die Tätigkeit von ICANN nicht auf technische Thematiken begrenzt werden, wäre eine umfangreiche demokratische Repräsentation innerhalb der ICANN notwendig<sup>608</sup>. Die Grenzlinie zwischen technischen und politischen Aufgaben ist jedoch sehr verschwommen. Zunächst müßte geklärt werden, welche technischen Tätigkeiten die ICANN wahrnehmen muß. Als Ausgangspunkt kann dabei die Definition technischer Tätigkeit des gewählten ICANN-Boardmitglieds Karl Auerbach dienen<sup>609</sup>:

---

<sup>605</sup> Vgl. *Weinberg*, 50 Duke L.J. 187, 250f. Siehe z.B. auch *Dyson, Ester*, Interim Chairman der ICANN in einem Brief an Rep. Bliley, Thomas J., Jr., Chairman des US-House Commerce Committee, 8. Juli 1999, <http://www.icann.org/correspondence/dyson-letter-08july99.htm>: „ICANN is nothing more than a vehicle or forum for the development and implementation of global consensus on various policy issues related to the DNS“.

<sup>606</sup> *US-DoC, NTIA*, White Paper, 63 Fed. Reg. 31741, 31749.

<sup>607</sup> Vgl. *Post*, Governing Cyberspace.

<sup>608</sup> Vgl. *Froomkin*, 50 Duke L.J. 17, 171.

<sup>609</sup> *Auerbach*, Email an ICANN wg-c Mailingliste, 29. Dezember 1999, <http://www.dns.org/wgroups/wg-c/Arc01/msg00456.html>.

A matter is “technical coordination” of the Internet if: A wrong decision has a [...] direct impact on the ability of the Internet to deliver its fundamental service, i.e. the end-to-end transport of IP packets. Otherwise it is a policy matter.

Festzustellen, ob ein Einfluß auf die Internetstabilität bei falscher Entscheidung besteht, fällt jedoch bei vielen technischen Entscheidungen schwer. Besonders bei langfristiger Betrachtung können technisch motivierte Entscheidungen ein starkes politisches Moment entfalten. Dies zeigt zum Beispiel die Einführung des DNS als einfache Merkhilfe mit der Folge, daß man heute intensiv um Domainnamen und Markenrechte streitet (siehe Kapitel 4.3 unten)<sup>610</sup>.

Als weiteres Beispiel kann die Entscheidung für einen *Single Root Server* herangezogen werden. Dieses System birgt die Möglichkeit inne, auch nichttechnische Ansichten weltweit im Internet umzusetzen. Dies betrifft zum Beispiel das Löschen von Domains unter denen Pornographie zu finden ist oder die Vermarktung von Registrierungsdaten sowie die Unterdrückung staatskritischer Internetangebote. Über das DNS und den *A Root Server* wäre es möglich, Internetpolitik zu betreiben, ohne den komplexen Problemen der Umsetzung und Jurisdiktion ausgesetzt zu sein, mit welchen sich jede staatliche Gesetzgebung konfrontiert sieht<sup>611</sup>. Zusätzlich kann der Betreiber des *A Root Servers* von allen Betreibern von Domainnameservern eine jährliche Gebühr und die Anwendung von bestimmten Regeln verlangen, ansonsten diesen den Zugriff verweigern.

Auch zeigt die Erweiterung der verfügbaren TLDs durch die ICANN, daß eine an sich technische Materie ein hohes politisches Potential beinhalten kann. Nach jahrelanger Diskussion hatte die ICANN auf ihrer Tagung in Marina del Rey die Einführung sieben neuer TLDs gefällt (siehe Kapitel 3.3.2 unten). Das Kernziel war es, zusätzliche Möglichkeiten der Registrierung von SLDs zu schaffen. Bei der Entscheidung mußte das Spannungsverhältnis zwischen den Nutzer- und den Industrieinteressen an attraktiven TLDs abgewogen werden. Schon in der öffentlichen Diskussion stellte sich die Frage, nach welchen Kriterien die neuen TLDs eingeführt werden sollten: politische, wirtschaftliche oder nur technische. So entschied man sich gegen die Einführung einer .kids TLD nach inhaltlichen Kriterien, da es nicht möglich sei, weltweit zu kontrollieren, daß keine jugendgefährdenden Inhalte darüber veröffentlicht würden. Hier stellte sich die politische Frage (ebenso bei einer .sex oder .xxx TLD), ob inhaltlich geschlossene und kontrollierbare TLDs geschaffen werden sollten, obgleich die Kontrolle global selbst sich sehr schwierig gestalten würde und auch rechtliche Konsequenzen nach sich ziehen könnte. Ebenso wurde auf Betreiben mehrerer Industrievertreter keine TDL für Gewerkschaften (.union) eingeführt. Angebracht wurde das Argument, daß die breite Unterstützung der Gewerkschaften weltweit nicht gewährleistet sei, obgleich hinter dem An-

---

<sup>610</sup> Das gewählte ICANN-Board-Mitglied Andy Müller-Maguhn geht sogar soweit zu behaupten: „Letzlich haben die Entscheidungen von ICANN immer politische Bedeutung“, zitiert in *Handelsblatt-Online*, Kupilas, Netzdemokraten kämpfen um ihren Einfluss bei ICANN, 4. Februar 2001.

<sup>611</sup> Siehe auch *Post*, Governing Cyberspace, Fn. 607 und *Hanloser*, JurPC Web-Dok. 158/2000, Abs. 23.

trag die belgische *International Confederation of Free Trade Unions*<sup>612</sup> stand, welche 216 Gewerkschaften aus 145 Ländern repräsentiert. Schließlich stellte sich die Frage, warum zunächst nur sieben neue TLDs geschaffen werden sollten, obgleich eine Vielzahl neuer TLDs ohne technische Probleme hätten eingeführt werden können. Technische Einwände gegen viele Vorschläge mögen zwar berechtigt gewesen sein, doch wurde die überwiegende Zahl der Entscheidungen auch unter wirtschaftlichen und besonders politischen Überlegungen gefällt<sup>613</sup>.

Als letztes Beispiel der politischen Relevanz der Tätigkeit ICANNs soll die Einführung der *Uniform Domain Name Dispute Resolution Policy* (UDRP) als Verfahren zur außergerichtlichen Lösung von Streitigkeiten um Domainnamen genannt werden. Mit der Einführung dieser, überschritt die ICANN ihren technischen Aufgabenbereich. Alle *Registrars* haben die Verpflichtung die UDRP anzuwenden, so daß auch jeder Endnutzer gezwungen ist, sich den Regeln dieses Schiedsverfahrens zu unterwerfen. Die UDRP bezweckt zunächst keine endgültige Regelung eines Streites um Marken- und Namensrechte<sup>614</sup>. Ein der Klage stattgebender Urteilsspruch hat jedoch die Auswirkung, daß ein SLD-Inhaber, welcher danach seine Domain an den Kläger übertragen soll, diese vor einem staatlichen Gericht zurückzuerstreiten hat. Schließlich beinhalten diese Regeln Entscheidungen, welche weit über technische Belange hinausgehen und auch einigen nationalstaatlichen Regeln zum Markenrecht entgegenstehen.

Zusammenfassend kann man feststellen, daß die besonders brisanten von ICANN behandelten Thematiken nicht nur technische Belange darstellen, sondern auch rechtliche Probleme lösen sollen. Die reine technische Arbeit, wie die Zuweisung von Protokollparametern wurde über viele Jahre hinweg unbeachtet von der Öffentlichkeit von der IANA ausgeführt. Im Gegensatz hierzu stellte die Einführung von neuen TLDs oder einer UDRP eine größtenteils im politischen Bereich angesiedelte Leistung dar.

### 3.2.2. Struktur der ICANN

ICANNs verworrene Struktur besteht aus einer Vielzahl von Unterorganisationen und Gruppierungen. Sie wird von einem aus 19 Mitgliedern bestehenden Vorstand geleitet und dieser von drei sogenannten *Supporting Organizations* unterstützt: die *Address Supporting Organization* (ASO), die *Domain Name Supporting Organization* (DNSO) und die *Protocol Supporting Organization* (PSO). Jede der drei Organisationen setzt sich wiederum aus Vertretern einzelner unabhängiger Organisationen zusammen. Ein Teil des Vorstandes wird regelmäßig von den *Supporting Organizations* entsendet. Der andere Teil des Vorstands wurde von der *At-Large Membership* gewählt. Ferner kann sich die ICANN auf mehrere beratende Ausschüsse stützen: zum Beispiel das *Advisory Committee on Membership* (MAC), das *Advisory Committee on Independent Review* (IRAC), das *Governmental Advisory Committee (GAC)* und das *DNS Root Server System Advisory Committee* (RSSAC). Einen

<sup>612</sup> Die *International Confederation of Free Trade Unions* ist im WWW unter <http://www.icftu.org/> zu finden.

<sup>613</sup> Zum Ganzen siehe auch Ahlert, Telepolis 4344.

<sup>614</sup> Siehe § 4 k Uniform Domain Name Dispute Resolution Policy, 24. Oktober 1999, <http://www.icann.org/udrp/udrp-policy-24oct99.htm>.

### 3.2. Arbeit der ICANN

und das *DNS Root Server System Advisory Committee* (RSSAC). Einen Überblick über die ICANN-Struktur soll Abbildung 7 vermitteln:

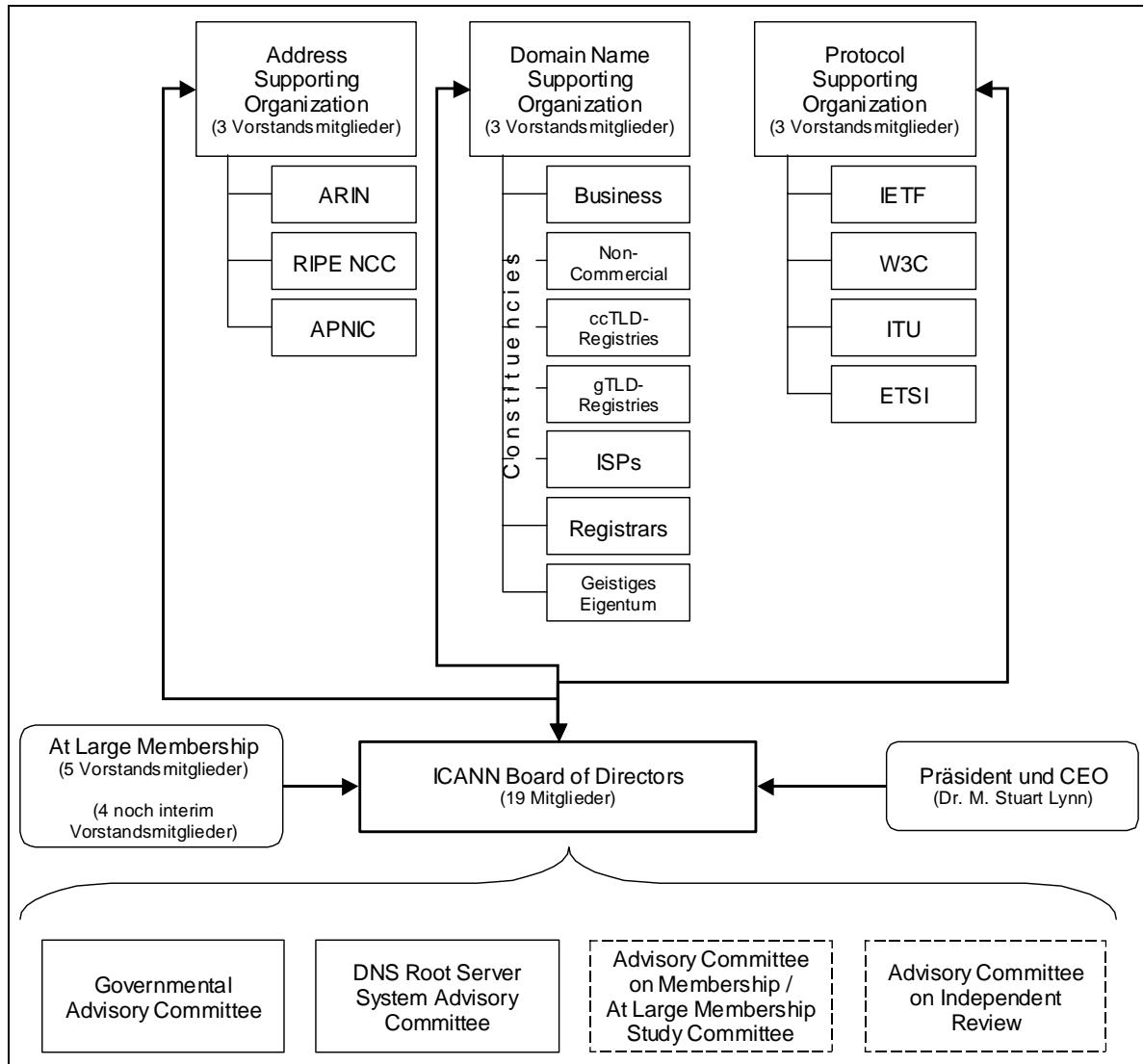


Abbildung 7 – Übersicht über die ICANN-Struktur.

Im Folgenden wird näher auf die einzelnen Organe der ICANN eingegangen und die Struktur als Ganzes näher beleuchtet.

#### 3.2.2.1. *Board of Directors* und der Präsident der ICANN

ICANNs Vorstand besteht aus 19 Mitgliedern, davon werden neun von den *Supporting Organizations* gestellt, fünf wurden von der *At-Large Membership* im November 2000 gewählt und vier Mitglieder stellen noch *interim Board Members* dar, das heißt, sie wurden 1998 von Dr. Jon Postel ausgewählt. Als Vorstandsvorsitzender wurde letztlich Vinton G. Cerf gewählt<sup>615</sup>, ein Internetpionier, welcher in den siebziger Jahren das TCP/IP-Protokoll

wählt<sup>615</sup>, ein Internetpionier, welcher in den siebziger Jahren das TCP/IP-Protokoll mitentwickelt hat. Das 19. Mitglied ist der Präsident und *Chief Executive Officer* (CEO) der ICANN. Dieses Amt wird derzeit von Dr. M. Stuart Lynn wahrgenommen<sup>616</sup>.

Nach Art. IV, Sec. 1 (a) der ICANN-Satzung stellt das *Board of Directors* die eigentliche Entscheidungsgewalt dar. Es hat die Leitung, Kontrolle und die Vertretung der ICANN inne. Die wichtigsten Beschlüsse werden gewöhnlich während der Jahresversammlungen mit einfacher Mehrheit der Vorstandsmitglieder gefaßt. Hinzu kommen regelmäßige ordentliche sowie außerordentliche Vorstandssitzungen, die auch als Telefon- und Videokonferenzen stattfinden können.

Die Herkunft des ersten Vorstandes der ICANN scheint etwas mysteriös zu sein, da nicht klar ist, auf welcher Basis die einzelnen Mitglieder des sogenannten *interim Board of Directors* ausgewählt wurden. Obwohl von der Internetgemeinschaft Vorschläge für die Vorsitzenden gemacht wurden, war es schließlich die Entscheidung der ICANN-Gründer, insbesondere Dr. Jon Postels, die endgültige Auswahl zu treffen<sup>617</sup>. Eigentlich sollte jeder Vorschläge unterbreiten können, um anschließend das *Board of Directors* nach dem Konsensprinzip mit weiterer Unterstützung der Internetgemeinschaft zusammenzustellen. Um den verschiedenen Interessensvertretern gerecht werden zu können, hatte sich Dr. Jon Postel jedoch für einen Ansatz entschieden, nach welchem Persönlichkeiten gewählt werden sollten, die qualifiziert genug waren, aber bislang eine neutrale Rolle eingenommen und sich möglichst nicht an den Debatten um das DNS beteiligt hatten. Nach der Auswahl sendete am 2. Oktober 1998 Dr. Jon Postel an das US-DoC schließlich einen Vorschlag für das *interim Board of Directors*. Am 25. Oktober 1998 konstituierte es sich schließlich offiziell<sup>618</sup>.

Im Laufe der Zeit wurden neun der vorläufigen Vorstandsmitglieder durch die *Supporting Organizations* neu gewählt. Im Oktober 2000 erfolgte schließlich eine Wahl von fünf neuen Vorstandsmitgliedern durch die *At-Large Membership* (siehe ausführlich im Kapitel 3.2.2.4 unten). Für Europa schaffte der deutsche Andy Müller-Maguhn, der derzeitige Sprecher des *Chaos Computer Clubs*, mit großer Mehrheit den Sprung in den Vorstand der ICANN. Die Ersetzung der vier übrigen vorläufig besetzten Vorstandsstellen ist jedoch noch umstritten und soll mittels einer Studie durch das *At-Large Membership Study Committee* (ALSC) geklärt werden<sup>619</sup>.

---

<sup>615</sup> Vinton G. Cerf ersetzte dabei die lange als Vorsitzende dienende Esther Dyson, welche als Wagniskapitalgeberin im Internet eine schillernde Rolle spielte; zu Esther Dyson siehe auch <http://www.thestandard.com/people/display/0,1157,1372,00.html>.

<sup>616</sup> Er folgte damit Michael Roberts, welcher in ICANNs Startphase das Amt übernommen hatte; zu Stuart Lynn siehe auch *Heise-Newsticker*, Die ICANN hat einen neuen Präsidenten, 24. Januar 2001.

<sup>617</sup> Vgl. *ICANN, Response to Chairman Bliley*, 8. Juli, 1999, Antwort zu Frage 4, <http://www.icann.org/correspondence/bliley-response-08july99.htm>.

<sup>618</sup> *US-GAO*, Report, S. 13.

<sup>619</sup> Siehe *Heise-Newsticker*, Gewählte ICANN-Direktoren stehen zur Disposition, 9. November 2000.

### 3.2. Arbeit der ICANN

---

Die oberste Verwaltungsposition steht dem Präsidenten und CEO der ICANN zu. Er ist gleichzeitig ein Vorstandsmitglied von Amts wegen. Als CEO nimmt er die organschaftliche Geschäftsführung und Vertretung der ICANN wahr. Ausgeschlossen hiervon sind dabei alle Sachentscheidungen, welche nicht mit der laufenden Verwaltung verbunden sind. Unterstützt wird nach Art. VIII der ICANN-Satzung die Verwaltung von den *Officers*, die bestimmte Bereichsaufgaben wahrnehmen. Hierzu zählen der *Secretary*, *Chief Financial Officer* und der *Chief Technical Officer*. Der Sekretär ist für die Protokollierung der Vorstandssitzungen verantwortlich und erfüllt die regelmäßigen, vom Präsidenten oder vom Vorstand bestimmten Aufgaben. Der *Chief Financial Officer* ist für die Finanzen und die Buchführung der ICANN verantwortlich. Für die aktuellen technischen Fragen steht dem Vorstand der *Chief Technical Officer* beratend zur Seite. Problematisch an der ICANN-Belegschaft ist jedoch, daß diese größtenteils aus US-Amerikanern besteht. Auch wenn diese Situation von den Schwierigkeiten, eine Arbeitserlaubnis für Ausländer in den USA zu erlangen, herrühren mag und man dem Verwaltungspersonal auch keine US-zentralistischen Entscheidungen vorwerfen kann, ist jedoch von einer unbewußten US-amerikanischen Ausrichtung auszugehen. Als erster europäischer Mitarbeiter in der Belegschaft der ICANN wurde Herbert Vitzthum eingestellt, welcher von Salzburg aus die ICANN bei der weiteren Zusammenarbeit mit den nationalen Registrierstellen (ccTLDs) unterstützen wird<sup>620</sup>.

#### 3.2.2.2. Supporting Organizations

Die eigentliche Hauptarbeit der ICANN soll nach Art. VI der ICANN-Satzung durch die drei *Supporting Organizations* (ASO, DNSO, PSO) erfolgen. Jede der drei Unterorganisationen benennt jeweils drei Vorstandsmitglieder. Die drei *Supporting Organizations* spiegeln die drei Regulierungssäulen des Internets wieder: die Standardsetzung sowie die Verwaltung der IP-Adressen beziehungsweise des DNS. Mittels dieser im Folgenden zu erläuternden *Supporting Organizations* soll die ICANN ihre Funktion als Dachorganisation des Internets gerecht werden.

- *DNSO – Domain Name Supporting Organization*

Die wichtigste ist die DNSO. Sie setzt sich aus Vertretern von sieben unabhängigen *Constituencies*, unter anderem der ccTLDs, der gTLDs, sowie ISPs und der nicht-kommerziellen Domaininhabern zusammen und hat Vorschläge für die Domainvergabe-Policies, für die Erweiterungen des DNS und für neue gTLDs zu erarbeiten<sup>621</sup>. Sie nimmt somit eine Beraterstellung gegenüber dem *Board of Directors* ein.

Jede der sieben *Constituencies* wählt drei Vertreter in das *Names Council*, welcher das Beratungsorgan der DNSO bildet. Jedoch darf kein indirekt vertretenes Unternehmen

---

<sup>620</sup> Siehe *Heise-Newsticker*, ICANNs Mann in Europa, 22. Januar 2001. Ein Überblick über das Verwaltungspersonal wird unter: About ICANN, <http://www.icann.org/general/abouticann.htm> gegeben.

<sup>621</sup> Im Internet ist die DNSO unter <http://www.dns.org> vertreten. Ausführlich zur Struktur und zu den Aufgaben der DNSO siehe *DNSO Names Council*, Domain Name Supporting Organization of ICANN, <http://www.dns.org/dns/aboutdns.html>.

mehr als einen Platz im *Names Council* wahrnehmen<sup>622</sup>. Die Bildung der *Constituencies* sollte sich als schwierig erweisen, da jede einzelne durch das *Board of Directors* anerkannt werden mußte. Dabei ist festzustellen, daß innerhalb der *Constituencies* in einem starken Ungleichgewicht kommerzielle Interessen vertreten sind<sup>623</sup> und nur die *Non-Commercial Domain Name Holders-Constituency* (NCDNH) nach langem Zögern aufgenommen wurde, um private Domainnameinhaber und deren Interessen zu vertreten. Eine Zustimmung für eine nicht-kommerziellen *Individual Domain Name Owners-Constituency* (IDNO) wurde jedoch verweigert<sup>624</sup>. Darüber hinaus besteht durch die Starrheit des Systems kaum die Möglichkeit, auf neue Thematiken mit einer Veränderung der Sitzverhältnisse oder der Gründung neuer *Constituencies* zu reagieren.

Darüber hinaus hat am 1. Juni 2001 die *ccTLD Constituency* entschieden, aus der DNSO auszutreten<sup>625</sup>. Seitdem verlangt sie ein direktes Mitspracherecht im ICANN-Board. Dazu schlagen die Verantwortlichen für die ccTLDs die Umwandlung ihrer *ccTLD Constituency* in eine eigenständige *Supporting Organization* vor. Sie sind der Ansicht, daß die vorgeschlagene *Country Code Supporting Organization* besser den Interessen der lokalen TLDs dienen wird. Die ccTLDs kritisierten an der DNSO vor allem ihre grundlegende Ausrichtung auf die Belange der gTLDs und die entsprechende Vernachlässigung von landesspezifischen Interessen. Obgleich die ccTLDs ein Drittel aller Domainnamen beherbergen und auch ein Drittel des Finanzhaushaltes der ICANN beisteuern sollen, hatten sie bisher nicht die Möglichkeit über die DNSO einen eigenen Vertreter in das ICANN-Board zu entsenden.

Alle Interessenten können durch das offene Forum der DNSO-*General Assembly* an der Arbeit der DNSO teilnehmen. Die Teilnehmer zeichnen sich durch ihr Wissen und Interesse an speziellen Themen bezüglich des DNS aus. Die DNSO-*General Assembly* trifft sich mindestens einmal im Jahr, möglichst in Verbindung mit den regulären Treffen des ICANN-Vorstands.

- **PSO – *Protocol Supporting Organization***

Die PSO ist aus Vertretern der IETF, dem W3C, der ITU-T und der ETSI zusammengesetzt und legt die Standards für Protokolle sowie deren Zuordnung zu einzelnen Diensten fest. Sie fördert die einheitliche Entwicklung der Internet-Protokoll-Parameter und sonstiger technischer Normen, die den Datenaustausch im Internet ermöglichen. Die PSO wurde durch ein *Memorandum of Understanding* zwischen ICANN und den teilnehmenden Standardisierungsorganisationen am 14. Juli 1999 ge-

---

<sup>622</sup> Damit wurde 1999 unterbunden, daß die NSI als einzige Registry für die gTLDs und damit einziges Mitglied dieser Untergruppe der DNSO drei Sitze im Names Council zu besetzen konnte.

<sup>623</sup> Vgl. auch Weinberg, Review of DNSO, Kap. B. Constituencies.

<sup>624</sup> Siehe auch Kleinwächter, MMR 1999, 10.

<sup>625</sup> ccSO Formation Statement, 1. Juni 2001,

[http://www.wwtld.org/ongoing/ccso\\_formation/ccSO\\_formation\\_statement\\_01Jun01.html](http://www.wwtld.org/ongoing/ccso_formation/ccSO_formation_statement_01Jun01.html).

gründet<sup>626</sup>. Als leitendes Organ fungiert der *Protocol Council*. Auch die PSO veranstaltet jährlich ein offenes Treffen, die *PSO-General Assembly*, auf welcher alle interessierten Personen teilnehmen können.

- **ASO – Address Supporting Organization**

Die ASO<sup>627</sup> setzt sich aus den Vertretern der regionalen *Internet Registries*, dem APNIC, dem RIPE NCC und dem ARIN zusammen. Sie soll die globalen Bestimmungen für die Vergabe des IP-Adreßraumes (Ipv4 und Ipv6) und die damit zusammenhängenden Numerierungen überwachen. Sie beschäftigt sich mit der künftigen Gliederung, Zuweisung und Verwaltung der IP-Adressen. Die ASO wurde durch ein *Memorandum of Understanding* zwischen der ICANN und der drei regionalen *Internet Registries* am 18. Oktober 1999 gegründet<sup>628</sup>. Zentrales Organ der ASO ist der *Address Council*. Die für alle Interessenten offenen Treffen finden auch in der ASO durch eine *General Assembly* statt.

#### 3.2.2.3. Advisory Committees

Unterstützt wird die Arbeit der *Supporting Organizations* durch die *Advisory Committees*. Inzwischen hat das Board der ICANN vier solche Ausschüsse geschaffen, welche nachfolgend kurz betrachtet werden sollen.

- **IRAC – Advisory Committee on Independent Review**

Die Satzung der ICANN verlangt die Einführung eines Verfahrens zur Überprüfung der Entscheidungen des Direktoriums durch eine unabhängige dritte Partei. Das Ziel eines solchen *Independent Review Panel*<sup>629</sup> (IRP) ist es, die beanstandeten Handlungen des ICANN-Boards auf Vereinbarkeit mit der Satzung und den *Articles of Incorporation* zu überprüfen. Das IRP soll ebenso überwachen, ob Beschlüsse auf einem Konsens beruhen. Es soll in einer offenen und wirkungsvollen Weise agieren. Das IRAC hatte die Aufgabe, einen solchen Mechanismus für die ICANN zu entwickeln. Mit dem endgültigen Report vom 6. August 1999 wurde die Arbeit des IRACs beendet<sup>630</sup>. Ein daraufhin gegründetes *Independent Review Panel Nominating Committee* rief jedoch erst im Juni 2001 zur Nominierung von Kandidaten für das IRP auf<sup>631</sup>.

---

<sup>626</sup> Siehe *RFC 2961*, Bradner.

<sup>627</sup> Die ASO ist im Internet unter <http://www.aso.icann.org> vertreten.

<sup>628</sup> Siehe ASO, Memorandum of Understanding - ICANN Address Supporting Organization, 18. Oktober 1999, <http://www.aso.icann.org/docs/aso-mou.html>.

<sup>629</sup> Vgl. auch zum Independent Review Panel: *Post, ICANN and Independent Review*.

<sup>630</sup> Principles for Independent Review: *IRAC*, Final Report of the Advisory Committee on Independent Review, 6. August 1999, <http://www.icann.org/santiago/irac-final-report.htm>.

<sup>631</sup> *ICANN*, Open Call For Nominations to the ICANN Independent Review Panel, 26. Juni 2001, <http://www.icann.org/committees/indreview/open-call-26jun01.htm>.

- **MAC – *Membership Advisory Committee***

Das MAC war mit der Erarbeitung eines Verfahrens zur Wahl der neun Vorstände des Direktoriums der ICANN betraut worden. Es veröffentlichte am 26. Mai 1999 die „*Principles of the At-large Membership*“ in Zusammenarbeit mit dem *Berkman Center for Internet & Society* der *Harvard Law School*<sup>632</sup>. Dieses Dokument bildete den Grundstein für die dann im Oktober 2000 stattgefundene Wahl der fünf ICANN-Vorsitzenden. Abgelöst wurde das MAC durch das *At-Large Membership Study Committee* (ALSC). Dieses Organ soll unter breiter Teilnahme der Internetgemeinschaft eine Methode entwickeln, die Internetnutzer als Individuen in der ICANN zu vertreten und das System der *At-Large Membership*<sup>633</sup> zu überarbeiten (siehe Näheres im Kapitel 3.2.2.4 unten).

- **RSSAC – *DNS Root Server System Advisory Committee***

Das RSSAC<sup>634</sup> hat das Board der ICANN über die Betreibung der *Root Name Server* des DNS zu beraten. Es untersucht die Voraussetzungen der *Root Name Server*, der Hardwarekapazitäten, der Betriebssysteme, der zugrundeliegenden Software und die Anbindung an das Netzwerk. Dabei hat es Aspekte wie die Sicherheit, die Anzahl, die Verfügbarkeit und die Zuverlässigkeit der Server und deren Lokalisierung zu beachten.

- **GAC – *Governmental Advisory Committee***

Das umstrittenste Gremium stellt das GAC dar<sup>635</sup>. Es ist aus Vertretern der nationalen Regierungen und der internationalen staatlichen Organisationen zusammengesetzt. Das GAC soll die Belange der Regierungen im *Board of Directors* der ICANN repräsentieren, Art. VIII, Sec. 3 (a) der ICANN Satzung. Als *Advisory Committee* hat das GAC keine rechtliche Autorität, die ICANN zu kontrollieren. Da weder nationale Regierungen noch zwischenstaatliche Organisationen nach der ICANN-Satzung das Recht haben, Direktoren in den ICANN Board zu entsenden, bleibt eine solche Entsendung auch durch das GAC ausgeschlossen. Es ist ungeklärt, inwieweit jedoch das ICANN Board auf die Beratungen des GAC Rücksicht nehmen muß. Deshalb verursachen ihre Reporte große Aufmerksamkeit in der Internetgemeinschaft, welche häufig mit der Angst vor einer zu starken Einmischung der Nationalregierungen verbunden ist. Diese Angst ist nicht unberechtigt, da die Aktivitäten des GAC nicht klar öffentlich erkennbar sind. Vielmehr agiert das GAC hinter verschlossenen Türen. Nur *Executive Minutes* von den Tagungen sind einsehbar und eine öffentliche Diskussion ist nicht möglich.

---

<sup>632</sup> Siehe ICANN, *Membership Advisory Committee Commentary on the Principles of the At-large Membership*, <http://www.icann.org/macberlin.htm>. Vgl. auch die umfangreiche Studie des *Berkman Center for Internet & Society*, *Representation in Cyberspace Study*, 26. Mai 1999, <http://cyber.law.harvard.edu/rcc/>.

<sup>633</sup> Siehe ICANN *At Large Membership Study Committee*, <http://www.atlargestudy.org/>.

<sup>634</sup> Siehe auch die WWW-Seite des RSSAC, <http://www.icann.org/dnsroot-com.html>.

<sup>635</sup> Das GAC tritt im WWW unter <http://www.icann.org/committees/gac/index.html> und unter <http://www.noie.gov.au/projects/international/DNS/gac/index.htm> auf.

Aufsehen erregte die wiederholte Darlegung der Standpunkte des GAC zu den ccTLDs in einem Kommuniqué anlässlich der 4. Tagung des ICANN *Interim Board* in Santiago de Chile, im August 1999<sup>636</sup>:

- b. With regard to principles for the delegation of management for country code top level domains:
  1. The GAC reaffirmed its May resolution that the Internet naming system is a public resource and that the management of a TLD Registry must be in the public interest.
  2. Accordingly, the GAC considers that no private intellectual or other property rights inhere to the TLD itself nor accrue to the delegated manager of the TLD as the result of such delegation.
  3. The GAC also reaffirmed that the delegation of a ccTLD Registry is subject to the ultimate authority of the relevant public authority or government. The GAC discussed the development of best practices for the administration of ccTLDs and agreed to continue this discussion.

Auch ohne rechtliche Verbindlichkeit, liegt diesen Äußerungen ein deklaratorischer Charakter zugrunde, über welchen sich die ICANN nicht einfach hinwegsetzen kann. Insbesondere der dritte Standpunkt kann bei Redelegation bestehender ccTLDs eine Relevanz entfalten<sup>637</sup>. Wenn die Einführung neuer TLDs soweit vorangeschritten sein wird, daß diese neuen TLDs eine klare Alternative für viele ccTLD-Nutzer darstellen würden, wird der Versuch nationaler Regierungen die ccTLDs unter ihre Kontrolle zu bekommen, nicht besonders gefährlich sein. Auf nationale Interessen ausgerichtete TLDs werden dann nur einen weiteren Aspekt zur Diversität des Internets bieten. Bis eine solche Konkultanzsituatton besteht, ist es jedoch notwendig, jegliches Ansinnen nationaler Regierungen, in die offene Struktur des Internets durch stark regulierte ccTLDs eingreifen zu wollen, zurückzuweisen.

Da eine eigene ccTLD im Interesse jedes Nationalstaates liegt und ein gewisses nationales Selbstbewußtsein unter den Nutzern besteht, ist der Wunsch der verschiedenen Regierungen an einer Mitbestimmung verständlich. Aus europäischer Sicht ist dabei ein einheitliches Auftreten der *Europäischen Union* und der Mitgliedstaaten notwendig. Das *Europäische Parlament* wies deshalb in einem Entschließungsauftrag vom 19. Februar 2001 daraufhin, daß es Aufgabe der Europäischen Kommission sei, zum

---

<sup>636</sup> GAC, Communique of the Government Advisory Committee, 24. August, 1999, <http://www.icann.org/committees/gac/communique-24aug99.htm>. Siehe auch umfassend ICANN, Principles for the Delegation and Administration of Country Code Top Level Domains, 23. Februar 2000, <http://www.icann.org/committees/gac/gac-cctldprinciples-23feb00.htm>.

<sup>637</sup> Ein solcher Streit entstand zwischen der philippinischen Regierung und der Registry für die .ph-TLD, nachdem diese entschieden hatte, nicht mehr für die Phillipiner einen flachen Namensraum anzubieten, sondern diese auf com.ph, org.ph und net.ph zu verweisen um den Namensraum unter .ph als Telefondomain international zu vermarkten. Näheres siehe ICANNWatch, .ph Dispute Escalates: Government, ICANN to be Involved.

einen an den Verhandlungen mit den USA teilzunehmen, sowie eine aktive Rolle im GAC einzunehmen<sup>638</sup>. Das GAC gibt folglich die Möglichkeit, auf die Unabhängigkeit der ICANN von der nordamerikanischen Regierung hinzuwirken, sowie ihre Neutralität zu fördern. Auch Deutschland nimmt durch einen Vertreter des Bundesministeriums für Wirtschaft und Technologie die Chance wahr, am ICANN-Prozeß über das GAC teilzunehmen<sup>639</sup>. Unter anderem finanzierte die Bundesregierung die zweite Sitzung des GAC im Frühjahr 1999 in Berlin. Die Bundesregierung bemüht sich um einen geschlossenen Auftritt unter Wortführung der jeweiligen EU-Präsidentschaft und der ebenfalls an den GAC-Sitzungen teilnehmenden EU-Kommission. Eine Abstimmung erfolgt hierbei durch die *Informelle Arbeitsgruppe Internet Governance* der EU-Kommission.

Zu den *Advisory Committees* treten eine Reihe weiterer Komitees hinzu<sup>640</sup>, die dem *Board of Directors* unterstehen und diesem in seiner Arbeit unterstützen. Nach Art. V, Sec. 7 der ICANN-Satzung zählen dazu zum Beispiel das *Finance Committee*, um für den Haushaltsplan der ICANN Vorschläge zu unterbreiten oder das *Committee on Conflicts of Interest* zur Implementierung der *Conflicts of Interest Policy*<sup>641</sup>. Eine wichtige Rolle spielt auch das *Committee on Reconsideration*, welches ein Anfechtungsverfahren bezüglich Entscheidungen der ICANN im Rahmen der *Reconsideration Policy*<sup>642</sup> entwickeln soll.

### 3.2.2.4. At-Large Membership – ALM-Direktoren

Die Basis einer Organisation bilden nicht nur nach dem deutschen Recht die Mitglieder, sondern auch die §§ 5310ff. des *California Nonprofit Public Benefit Corporation Law* sehen eine dispositive Mitgliedschaft vor. Nach der ICANN-Satzung vom 16. Juli 2000 wurde diese Mitgliedschaft zugunsten einer reinen Wählerschaft vollständig abgedungen<sup>643</sup>. Weder soll es eigene Rechte und Obliegenheiten noch ein eigenes Organ für die Mitglieder (*At-Large Council*) geben. Obgleich man den Internetnutzern eine sogenannte Mitgliedschaft ermöglichen wollte, handelt es sich eher nur um Teilnehmer an der Auswahl der „wahren“ ICANN-

---

<sup>638</sup> Europäisches Parlament, Entschließungsantrag, Fn. 601.

<sup>639</sup> Siehe Antwort der Bundesregierung auf eine kleine Anfrage der FDP vom 14. August 2000, BT-Drs. 14/3966.

<sup>640</sup> Eine aktuelle Liste aller Komitees ist unter ICANN, Advisory Committees, <http://www.icann.org/committees/> ersichtlich.

<sup>641</sup> Siehe ICANN, Conflicts of Interest Policy, 4. März 1999, <http://www.icann.org/committees/coi/coi-policy-04mar99.htm>.

<sup>642</sup> Siehe ICANN, Reconsideration Policy, vom 4. März 1999, <http://www.icann.org/committees/reconsideration/recon-policy-04mar99.htm>. Vgl. auch ICANN-Satzung, Art III, Sec. 4 (a), Fn. 600: „Any person affected by an action of the Corporation may request review or reconsideration of that action by the Board. The Board shall adopt policies and procedures governing such review or reconsideration, which may include threshold standards or other requirements to protect against frivolous or non-substantive use of the reconsideration process.“

<sup>643</sup> ICANN-Satzung, Art II, Sec. 1, Fn. 600: „The Corporation shall not have members as defined in the California Nonprofit Public Benefit Corporation Law [...]“

### 3.2. Arbeit der ICANN

---

Mitglieder, der Mitglieder des ICANN *Board of Directors*<sup>644</sup>. Diese Regelung birgt für die ICANN mehrere Vorteile inne, indem sie sich den Pflichten gegenüber der Mehrheit der Internetnutzer entledigt. Unter kalifornischem Recht<sup>645</sup> müssen Mitglieder einer Kooperation Änderungen der Satzung und der Gründungsdokumente genehmigen, es müssen Mitgliederlisten erstellt und Protokolle geführt werden. Mitglieder können Vorsitzende wählen und auch wieder abwählen. Schließlich können Mitglieder rechtliche Schritte im Namen der Vereinigung gegen Organe dieser vornehmen, um Entscheidungen zu überprüfen und um festzustellen, ob eine Entscheidung sie als gesamte Gruppe verletzt hat<sup>646</sup>. Da es sich um Klagen im Namen der Gesellschaft handelt, kann besonders für finanzienschwache Gesellschaften eine Vielzahl solcher Verfahren der Bankrott bedeuten, wenn diese sogar dafür selbst aufkommen müssen, wenn sie die Klagen gewinnen sollten. Das oben erwähnte MAC (Kapitel 3.2.2.3 oben) kam zu der Ansicht, daß eine solche Ausweitung der Mitgliedschaft ein „high potential (assuming a large membership) of wasting very limited time and resources“<sup>647</sup> darstelle und der Stabilität des Internets abträglich wäre.

Schon das *White Paper* sah vor, daß die Mitglieder des *Board of Directors* ihre Aufgabe nur vorübergehend wahrnehmen werden und das vorläufige *Board of Directors* im Laufe der Zeit durch gewählte Vertreter ersetzt werde<sup>648</sup>. Geplant war, daß nur die eine Hälfte der ICANN-Vorsitzenden (neun Sitze), durch die sogenannte *At-Large Membership* (ALM) gewählt würde und so die Interessen der Endnutzer aus den verschiedenen Weltregionen vertreten wären. Die andere Hälfte sollte von den drei *Supporting Organizations* gestellt werden. Mit diesem System sollte der geographischen und funktionalen Vielfalt des Internets Rechnung getragen und gleichzeitig die Flexibilität gegenüber weiteren Entwicklungen gewährleistet werden<sup>649</sup>. Strittig blieb jedoch der Zweck einer Wahl durch die Internetgemeinschaft. Die die Internetgemeinschaft vertretenden ICANN-Vorsitzenden (sogenannte ALM-Direktoren) sind für die Ausführung der technischen Aufgaben der ICANN nicht unbedingt notwendig. Andere technische Gremien, wie die IETF benötigen keine im großen Maßstab gewählten Vertreter, sondern beruhen auf der Teilnahme fachlich kompetenter Personen. Durch eine Wahl würde jedoch auch allen Personen die Möglichkeit der Einflußnahme gegeben, welche weder eine fachliche Kompetenz aufweisen noch die Funktion der ICANN ansatzweise verstanden haben. Andererseits führt die Wahrnehmung der technischen Aufgaben der ICANN (wie schon im Kapitel 3.2.1 oben festgestellt) zu einer Reihe von politischen Auswirkungen auf die breite Masse der Internetnutzer und rechtfertigt eine breite Partizipation an der ICANN. Nur durch

---

<sup>644</sup> Mit diesem Verständnis siehe auch *Cook Report*, ISOC's ICANN Coalition Widens Its Control, Kap. Above All Be Certain You Do Not Permit Checks on Your Power.

<sup>645</sup> Siehe die §§ 5065, 5510ff. California Nonprofit Corporation Law, vgl. Fn. 598. Vgl. die ausführliche Auflistung der Rechte der sogenannten Statutory Members in der Analyse des MAC, Statutory Members versus Nonstatutory Members for the ICANN At Large Membership, 11. August 1999, Kap. II. Rights of Statutory Members, <http://www.icann.org/santiago/membership-analysis.htm>.

<sup>646</sup> Siehe *Cook Report*, ISOC's ICANN Coalition Widens Its Control, Fn. 644.

<sup>647</sup> Siehe MAC, Fn. 645.

<sup>648</sup> *US-DoC, NTIA*, White Paper, 63 Fed. Reg. 31741, 31750.

<sup>649</sup> *US-GAO*, Report, S. 41.

eine breite Wahl ist eine Legitimation der ICANN durch die von ihren Entscheidungen betroffenen Personengruppen erreichbar. Die Teilnahme der ALM-Direktoren im ICANN-Board sichert die Repräsentation der verschiedenen Internetnutzer und deren Interessen direkt im Entscheidungszentrum der ICANN. Die ALM-Direktoren können einen Ausgleich zu den vertretenen wirtschaftlichen Interessen im ICANN-Board bieten und als Machtkontrolle dienen. Ohne offene Mitgliederstruktur würde die ICANN schließlich das Risiko eingehen, wie jedes andere Wirtschaftsunternehmen behandelt zu werden und voll dem Wettbewerbsrecht zu unterfallen<sup>650</sup>. Die Wahl soll folglich mehrere zusammenhängende Ziele erfüllen:

- Es sollen die Personen eine Stimme bei den ICANN-Entscheidungen erhalten, die durch diese gebunden oder betroffen sind und durch die *Supporting Organizations* nicht in der ICANN-Struktur ausreichend repräsentiert sind.
- Es soll in der ICANN ein möglichst weites Meinungsspektrum vertreten sein.
- Es soll vermieden werden, daß das ICANN-Direktorium durch unproportionale Vertretung von Interessensgruppen einseitig beeinflußt wird.
- Es soll ein hochqualifiziertes Direktorium bestimmt werden, welches fähig ist, die Stabilität des Internets zu gewährleisten und die technischen Komponenten zu verwalten.
- Die Wählerschaft soll zur Beurteilung der Kandidaten möglichst engagiert und erfahren sein.

Um zu klären, wer ein Internetnutzer und ein potentiellen *At-Large Member* sein könnte, wurde vom ICANN-Board im Januar 1999 das oben erwähnte MAC (Kapitel 3.2.2.3 oben) gebildet. Es wurde schließlich entschieden, daß jeder Person älter als 16 Jahre mit einer Email und einer Postadresse die Möglichkeit gegeben werden sollte *At-Large Member* zu werden<sup>651</sup>.

Auf der Tagung des ICANN-Boards in Santiago de Chile, am 26. August 1999 wurde die Einführung eines sehr umstrittenen indirekten Wahlsystems beschlossen. Dazu sollte die ALM ein *Membership Council* aus 18 Personen wählen, das seinerseits dann die neun ALM-Direktoren bestimmen sollte<sup>652</sup>. Diese indirekten Wahlen spiegeln das US-amerikanische System der Wahlmänner wieder und hat den entscheidenden Nachteil, daß die Wählerschaft ihren Kandidaten nicht direkt wählen kann und darauf angewiesen ist, daß die Wahlmänner die von Ihnen im Wahlkampf offerierten Personen auch wirklich wählen. Das System eines *Membership Council* wurde nach heftiger Kritik im März 2000 in Kairo, Ägypten wieder zugunsten direkter Wahlen aufgegeben. Allerdings wurden die Partizipationsrechte der ALM hierbei

---

<sup>650</sup> So der damalige Vorsitzende des GAC, *Paul Twomey*: „The organization runs the risk of potentially becoming a de facto industry association. If it were to do so, it would need to recognize, I think, that governments and competition and consumer protection organisations would make much more attention to the activities of ICANN and would begin to apply tests to ICANN around consumer protection issues and around monopoly problems“, zitiert in *TBTF, the roving reporter*, ICANN Journal 1, Kap. PFIR, ICANN; ICANN, PFIR.

<sup>651</sup> Siehe auch die Studie des *Berkman Center for Internet & Society*, Fn. 632.

<sup>652</sup> ICANN, Resolutions Approved by the Board Santiago Meeting, 26. August 1999, Resolution 99.87, <http://www.icann.org/santiago/santiago-resolutions.htm>.

### 3.2. Arbeit der ICANN

---

soweit eingeschränkt, daß zunächst nur fünf Boardmitglieder als Repräsentanten der ICANN-Regionen (Nordamerika, Südamerika, Afrika, Europa und Asien) gewählt werden sollten. Nach einer Evaluierungsstudie durch das *At-Large Membership Study Committee* sollte dann die weitere Besetzung der verbleibenden vier Boardsitze geklärt werden.

Zur Überwachung der Nominierungsphase wurde ein Komitee eingesetzt, welches größtenteils aus ICANN-Direktoren bestand. Ein öffentlicher *Call of Interest* für die Ausschreibung der Stellen erfolgte jedoch nicht und zog wiederum den Protest verschiedener Bürgerrechtsorganisation<sup>653</sup> auf sich. Nach den Plänen der ICANN sollten pro Region sieben Kandidaten zur Wahl gestellt werden. Bis zum 20. Juli 2000 wurden vom NoCom erste Vorschläge entgegengenommen und am 1. August 2000 in einer ersten Kandidatenliste veröffentlicht. Diese bestand aus 18 Kandidaten, darunter schon fünf von maximal sieben für die europäische Region. Es blieben also in Europa nur zwei Plätze für die folgende offene Nominierungsphase übrig. Mit der Vornominierung der Mehrzahl der Kandidaten sprach die ICANN dem Wahlvolk größtenteils die Kompetenz zur eigenen Beurteilung der Kandidaten ab. Vielmehr hatten einflußreiche Interessensvertreter die Möglichkeit gehabt, an den Internetnutzern vorbei, den größten Anteil der Kandidaten zu bestimmen. Bis zum 15. August 2000 konnten sich dann Kandidaten selbst nominieren.

Die Registrierung der Mitglieder startete im Januar 2000. Bis zur Wahl hatten sich fast 160.000 Internetnutzer registrieren lassen. Vorgesehen waren maximal 20.000 Anmeldungen, so daß das Registrierungssystem unter einem Nutzeransturm im Juli 2000 völlig überlastet war. Insbesondere verleitet durch ein „Wettrennen“ zwischen den Industriestaaten in Asien und einer massiven Unterstützung von Regierungen und Computerunternehmen registrierten sich viele tausend Internetnutzer aus dieser Region. Auch Deutschland konnte durch eine Kampagne des Spiegels, der Bertelsmannstiftung und des Heise-Verlages über die Hälfte der europäischen Mitgliedsanmeldungen verbuchen<sup>654</sup>. Dieser Ansturm aus einzelnen Ländern zeigte die Schwäche und das Risiko jeder Wahl, daß sich in der Thematik unerfahrende Wähler zugunsten einseitiger politischer oder wirtschaftlicher Interessen instrumentalisieren lassen. Allerdings spiegelt diese Verteilung auch den Nutzungsgrad und die Bedeutung des Internets in den einzelnen Regionen wieder.

Aus den rund 200 Selbstdnominierungen mußten in der ersten Wahletappe 17 Kandidaten für die noch offenen Plätze in den Regionen gewählt werden. Die Kandidaten mußten zusätzlich eine Unterstützung von zwei Prozent der eingeschriebenen *At-Large Members*, aus mindestens zwei verschiedenen Ländern ihrer Region nachweisen. Die geringe Wahlbeteiligung von nur circa 17.000 Wählern führte allerdings dazu, daß es nur neun Selbstdnominierungskandidaten

---

<sup>653</sup> Z.B. von Common Cause und das Center for Democracy and Technology. Siehe auch *Faussett, Secret Committee*.

<sup>654</sup> Von 35.942 Registrierungen für Europa entfielen 20.475 auf Deutschland, siehe *ICANN@Large, Total At-Large Membership Applications (Unverified)*, 23. Juli 2000, [http://members.icann.org/pubstats\\_unverified.html](http://members.icann.org/pubstats_unverified.html).

ten gelang, die Hürde der zwei Prozent Unterstützung zu erfüllen<sup>655</sup>. Am 8. September wurde von der ICANN dann die endgültige Wahlliste mit 27 Kandidaten (je sieben in Nordamerika und Europa<sup>656</sup>, je fünf in Asien und Lateinamerika und drei in Afrika) veröffentlicht<sup>657</sup>. Von den Kandidaten konnten 13 der Industrie und 14 nutzerorientierten Gruppen zugeordnet werden<sup>658</sup>.

Die eigentliche Wahl<sup>659</sup> fand Anfang Oktober 2000 statt, an welcher sich von den registrierten Internetnutzern „nur“ circa 34.000 beteiligten. Jedoch hatten sich von den registrierten Nutzern, viele beschwert, daß sie ihre Freischaltungsnummer nicht erhalten hatten oder die Freischaltung durch überlastete Server nicht möglich war. Wie voraussehbar, gewannen in Europa und Nordamerika zwei von den *At-Large Members* selbst nominierte Kandidaten. In den anderen Regionen setzten sich vom Nominierungskomitee vorgeschlagene Kandidaten durch<sup>660</sup>. Andy Müller-Maguhn ist das online gewählte Mitglied des ICANN-Boards für Europa (5.948 von 11.309 Stimmen), Karl Auerbach das Mitglied für Nordamerika (1.738 von 3.449 Stimmen) (vgl. Tabelle 4 unten zur Verteilung der registrierten Mitglieder und Wähler). Beide Sieger waren schon im Vorfeld der Wahl als beharrliche ICANN-Kritiker aufgetreten. Die Wahl dieser beiden Personen spiegelt auch den Mißmut der europäischen und nordamerikanischen Internetnutzer über die anderen ihnen vom Nominierungskomitee aufgedrängten Kandidaten wieder. Nur diese beiden Kandidaten können als umfassend demokratisch legitimierte ICANN-Direktoren betrachtet werden, da nur sie sich allen Stufen des Wahlverfahrens ausgesetzt und dort gewonnen haben.

---

<sup>655</sup> Ursprünglich war eine 10%-Hürde vorgesehen, was zur Nominierung von nur zwei Personen geführt hätte.

<sup>656</sup> Zu den zwei Siegern des 1. Wahlganges und den sieben europäischen Kandidaten siehe *Rötzer, Telepolis 8696*.

<sup>657</sup> Siehe *ICANN@Large*, Regional Nominees, <http://members.icann.org/nominees.html>.

<sup>658</sup> Zu den erfolgten Wahlkampf und den drei deutschen Kandidaten (Andy Müller-Maguhn, Jeanette Hofmann und Winfried Schüller) siehe *Heise-Newsticker*, Hintergrund: Der ICANN-Wahlkampf läuft an, 21. September 2000.

<sup>659</sup> Die ICANN hatte sich für das Wahlsystem Single Transferable Vote durch Thomas Hare in England und Carl George Andrae in Dänemark um 1850 erfunden, entschieden, welches auf einer Umverteilung der Stimmen beruht. Dieses System muß sich jedoch der Kritik aussetzen, daß die Umverteilung der Stimmen dazu führen kann, daß der Kandidat mit den meisten Stimmen überhaupt nicht gewählt wird. Siehe ausführlich hierzu:

*Brams/Fishburne, Alternative Voting Systems*.

<sup>660</sup> Die Ergebnisse werden unter *ICANN@Large*, Results of the 2000 At Large Membership Vote, <http://www.election.com/us/icann/icannresult.html> und in der Analyse des *ICANN Channel*, Müller-Maguhn für Europa gewählt, <http://www.icannchannel.de/wahl2000/index.htm> ausführlich dargestellt.

Tabelle 4 – Verteilung der *At-Large Membership* bis zur Endwahl.

Regionen	Registrierte Mitglieder	Aktivierte Mitglieder	Teilnahme an der Vorwahl	Teilnahme an der Endwahl
Asien	93.782	38.397	4.994	17.745
Europa	35.942	23.519	9.109	11.309
Nordamerika	21.596	10.694	2.143	3.449
Lateinamerika	6.486	3.571	1.082	1.402
Afrika	787	321	73	130
Gesamt	158.593	76.502	17.401	34.035

Im Ganzen wurde die Durchführung der Wahl als positiv und als wichtiges Demokratieexperiment empfunden. Kritisiert wurden die technischen Probleme, welche der unerwartete Ansturm auf die Wahl hervorgerufen hatte<sup>661</sup>. Weiterhin sahen sich viele teilnehmende Länder durch die massive Teilnahme von Internetnutzern anderer Staaten (insbesondere Deutschland, Japan und Brasilien) benachteiligt. Es wurde der Vorwurf erhoben, die Deutschen hätten die europäischen Wahlen dominiert, obgleich man sich vorbildlich für einen demokratischen Prozeß engagiert hatte. Besonders die Wahl des Deutschen Andy Müller-Maguhn beruht zum großen Teil auf den konzentrierten Medienkampagnen in Deutschland zur Internetwahl, dessen Schlagzeilen er regelmäßig beherrschte. Da in anderen europäischen Staaten die Internetgemeinschaft bedeutend weniger Interesse an der ICANN-Wahl gezeigt hatte und sich entsprechend auch weniger mobilisieren ließ, ist diese Kritik ungerechtfertigt. Die öffentlichen Medien in Deutschland konnten zumindest für einen Zeitraum bei den Internetbenutzern ein Bewußtsein für die verschiedenen Regulierungsversuche im Internet schaffen. Ferner spiegelt die Entscheidung, jeder Region einen Sitz im ICANN-Board zuzuweisen, nicht das Interesse der Internetnutzer an einer Mitwirkung wieder. Für Afrika mag die geringe Wahlbeteiligung die Ursache in der geringen Computerisierung und damit der geringen Verbreitung des Internets liegen. Einer Region mit einer Wahlbeteiligung von einem Hunderstel gegenüber Asien oder Europa, einen eigenen Sitz zuzubilligen mag aus entwicklungspolitischen Gründen sehr wichtig sein, entspricht aber nicht dem demokratischen Gedanken, der mit dieser Wahl beabsichtigt war. Die gleichen Überlegungen gelten auch für Nordamerika. Obgleich hier das Internet die weiteste Verbreitung gefunden hat, haben sich bedeutend weniger Internetnutzer für die Hauptwahl mobilisieren lassen als in Asien oder Europa.

Mit der Wahl waren erst fünf ALM-Direktoren eingesetzt. Ursprünglich sollte jedoch die Hälfte der ICANN-Vorsitzenden dieser Weise gewählt werden, damit die Interessen der Endnutzer vertreten ausreichend vertreten wären. Die drei *Supporting Organizations* sollten die andere Hälfte der ICANN-Vorsitzenden stellen. Zur Bekräftigung der Absicht, eine breite Vertretung der Nutzerinteressen in der ICANN zu ermöglichen, enthielt die frühere ICANN-Satzung eine Bestimmung, daß die Wahl bis 30. September 1999 zu erfolgen habe und nur im

<sup>661</sup> Siehe z.B. *Froomkin, Replacing the ICANN Board Squatters.*

Ausnahmefall eine Verlängerung der Amtszeit bis spätestens 30. September 2000 möglich sei<sup>662</sup>.

Diese Verlängerungsmöglichkeit wurde während des Treffens des ICANN-Boards in Santiago de Chile am 26. August 1999 durch die Resolution 99.86 wahrgenommen, jedoch weiterhin betont, daß die Vorsitzenden nicht länger als bis zum 30. September 2000 im Amt bleiben sollen<sup>663</sup>. Diese Beschränkung wurde schließlich entgegen den Satzungsbestimmungen auf dem ICANN-Treffen im Juli 2000, ohne öffentliche Diskussion vollständig aufgegeben. Die nach der Wahl im Oktober 2000 übrig gebliebenen vier Direktoren sollten für maximal weitere zwei Jahre im Amt bleiben<sup>664</sup>. Dazu wurden die Zahl der zu wählenden Mitglieder des *Board of Directors* von zunächst neun auf fünf herabgesetzt. Die offenbleibenden vier Sitze sollten weiterhin von den *interim Directors* besetzt bleiben, bis durch eine Studie deren Besetzung geklärt wäre. Ohne öffentliche Diskussion hatte die ICANN dann auch im Oktober 2000 die vier Direktoren benannt, deren Amtszeit entgegen der ursprünglichen Satzungsvorschriften noch einmal bis 2002 verlängert wurde. Von der Mitentscheidung, welche Boarddirektoren für die neuen ALM-Direktoren das Vorstandsgremium verlassen sollten, waren die gewählten ALM-Direktoren, sowie alle Direktoren, die inzwischen durch die *Supporting Organizations* delegiert waren, ausgeschlossen. Die Entscheidung erfolgte im Geheimen durch die übrig gebliebenen neun *interim-Direktoren*. Die zur Begründung der Amtsverlängerung herangezogene Notwendigkeit der Kontinuität des ICANN-Gremiums kann nicht überzeugen, da diese auch durch die neun Direktoren der *Supporting Organizations* gewährleistet worden wäre. Auch weisen die gewählten fünf ALM-Direktoren exzellenten technischen Sachverstand auf, um eine kontinuierliche Arbeit sicherzustellen<sup>665</sup>. Würde es jedoch zu einem Rücktritt der vier Direktoren kommen, so müßten, wie vorgesehen, die dann frei werdenden Plätze mittels Neuwahlen ersetzt werden, um einen Leerstand zu verhindern. Dieser birgt das Risiko, daß man diese Stellen nicht in kürzester Zeit neu besetzen kann und im weiteren Verlauf ganz auf diese Direktorenstellen verzichtet<sup>666</sup>. Die Amtsverlängerung der vier Direktoren erscheint somit als ein raffinierter Ausweg, um weitere Wahlen auf unbestimmte Zeit zu verschieben. ICANN kann dieser Unterstellung nur entgehen, wenn sie so schnell wie möglich die übrigen vier Direktoren durch Wahlen ersetzen läßt.

Das im März 2000 in Kairo, Ägypten, beschlossene ALMC soll „a consensus on the best method for representing the world's Internet users as individuals (“At-Large Members”) within ICANN“ ausarbeiten<sup>667</sup>. Die Studie soll nach der geänderten Satzung klären<sup>668</sup>, ob das

---

<sup>662</sup> *Bylaws for ICANN*, 6. November 1998, Art. V, Sec. 1, Fn. 568.

<sup>663</sup> *ICANN*, Resolutions Approved by the Board Santiago Meeting, 26. August 1999, <http://www.icann.org/santiago/santiago-resolutions.htm>.

<sup>664</sup> *ICANN*, Minutes, Meeting of the Board, 16. Juli 2000, <http://www.icann.org/minutes/minutes-16jul00.htm>, Resolution 00.52, „Section 3. Terms of „At Large“ Directors - The five „At Large“ Directors seated as described in Section 2 shall serve terms that expire at the conclusion of the Annual Meeting of the Corporation in 2002“.

<sup>665</sup> Vgl. *Froomkin*, Beware the ICANN Board Squatters.

<sup>666</sup> Vgl. mit einer Erörterung zur Besetzung der freien Stellen: *Froomkin*, Replacing the ICANN Board Squatters.

<sup>667</sup> Vgl. *ICANN At Large Membership Study Committee*, Fn. 633.

### 3.2. Arbeit der ICANN

---

ICANN-Board ALM-Direktoren haben soll und inwieweit eine Repräsentation der Internetnutzer in der ICANN für erforderlich gehalten wird. Unter Vorsitz des ehemaligen schwedischen Ministerpräsident Carl Bildt soll das ALMC als neunköpfige Expertengruppe bis November 2001 Erörterungen zur Notwendigkeit einer *At-Large Membership* durchführen<sup>669</sup>. Erst an zweiter Stelle soll das „Wie“ einer Repräsentation näher untersucht werden. Durch die Studie sollen folgende Fragen geklärt werden<sup>670</sup>:

- (a) Should the ICANN Board include At Large Directors?
- (b) If so, how many such At Large Directors should there be?
- (c) How should any such At Large Directors be selected?
- (d) If selection by an At Large membership is recommended, what processes and procedures should be used to create that At Large membership? What minimum criteria, if any, should be required for membership? Precisely how should an At Large membership select At Large Directors?
- (e) If an At Large membership is to exist, what should its structure, role and functions be? How should it be funded?

Hierbei müssen die Probleme der ersten Onlinewahl geklärt werden, insbesondere auch Aspekte der Wahlbeeinflussung, der geographischen Repräsentation und der Bildung eines *Membership Councils*. Eine wichtige Frage stellt schließlich die Finanzierung einer eventuellen *At-Large Membership* dar. Im Ganzen soll das Bestehen dieser Gruppierung nicht als eine Vorbedingung betrachtet werden. Vielmehr soll eine generelle Überprüfung, inwieweit eine Beteiligung der Nutzer Sinn ergibt, erfolgen. Mit dieser Prioritätssetzung ist klar, daß das System der ALM-Direktoren, als Ergänzung zu den neun von diversen Interessens- und Unternehmensvertretern über die *Supporting Organizations* gestellten Direktoren, weiterhin zur Disposition steht. Inzwischen hat das ALMC jedoch in einem Diskussionspapier die Notwendigkeit einer wie auch immer gearteten Involvierung einzelner Internetnutzer in die Formulierung von Regeln und in die Entscheidungsfindung, einhergehend mit einer Repräsentation dieses Nutzerkreises im ICANN-Board, erkannt<sup>671</sup>.

Meines Erachtens ist die dem ALMC vorgegebene Prüfungsreihenfolge zwingend, da die Frage nach der Art und Weise einer Vertretung der breiten Masse von Internetnutzern, erst beantwortet werden kann, wenn geklärt ist, ob diese notwendig ist und welchen Zweck sie erfüllen soll. Nach der ICANN-Satzung sind weltweit Organisationen in die Studie einzubziehen.

---

<sup>668</sup> *Bylaws for ICANN*, Art. II, Sec. 5 der Satzung der ICANN vom 16. Juli 2000, Fn. 600.

<sup>669</sup> *Heise-Newsticker*, ICANN startet Studie zur Mitbestimmung durch Internet-Nutzer, 28. Januar 2001. Siehe auch *ICANN*, Charter for the At Large Membership Study Committee, 22. Januar 2001,

<http://www.icann.org/committees/at-large-study/charter-22jan01.htm>. Bei der Zusammensetzung sind die von der Studie betroffenen Internetnutzer wieder vor vollendete Tatsachen gestellt worden, ohne daß eine öffentliche Diskussion zuvor über die Kandidaten ermöglicht wurde.

<sup>670</sup> Siehe *ICANN*, Charter for the At Large Membership Study Committee, Kap. 2. Scope of the At-Large Study, Fn. 669.

<sup>671</sup> *At-Large Membership Study Committee*, Discussion Paper #1, 12. Juli 2001, <http://www.atlargestudy.org/DiscussionDraftRev.5.4.htm>.

hen. Das ALMC hat von verschiedenen Seiten finanzierte Einzelstudien anregen. Vorschläge und Einwendungen der Internetnutzer sollen auf Mailinglisten und bei Konferenzen zusammengetragen werden.

Entsprechend hat sich auch gleich eine Konkurrenzorganisation gegründet, die *NGO and Academic ICANN Study* (NAIS), welche sich kritisch mit der Prioritätssetzung der ICANN auseinandersetzt<sup>672</sup>. An ihr sind unter anderem auch das *Center for Democracy and Technology* und *Common Cause* beteiligt, die beide maßgeblich zur Ausgestaltung der ersten ICANN-Wahl beigetragen hatten. Eine Beteiligung der breiten Schicht der Internetnutzer stellt die NAIS nicht in Frage. Nach ihrer Ansicht kollidiert die von der ICANN selbst initiierte Studie grundsätzlich mit den Interessen der *At-Large Membership*. Einen ersten Report hat die NGO Ende Mai 2001 veröffentlicht<sup>673</sup>. Obgleich es sich bislang nur um einen Zwischenbericht handelt, stellt dieser fest, daß die ICANN in ihre Aktivitäten ausgeprägte Verfahren für eine öffentliche Beteiligung integrieren müsse.

Ergänzend zur NAIS hat sich ein Teil der *At-Large Membership* mit Unterstützung der fünf ALM-Direktoren und einer Reihe von NGOs zu einem *Interim Coordinating Committee* (ICC) zusammengeschlossen, um gemeinsam ihre Interessen gegenüber der ICANN zu vertreten<sup>674</sup>. Dieses neue Gremium will bis Ende 2001 ein Forum für alle Teilnehmer an der *At-Large Membership* schaffen. Das ICC will die Kooperation innerhalb dieses Personenkreises in den verschiedenen Regionen fördern und Modelle einer ALM-Struktur innerhalb von ICANN erarbeiten und diskutieren.

### **3.2.3. Probleme rund um die ICANN**

Die ICANN ist immer wieder schwerer Kritik und anhaltender Diskussion ausgesetzt. Im Folgenden sollen vier Hauptproblematiken diskutiert werden. Als erstes stellt sich die Frage, wie Entscheidungen innerhalb der ICANN zustande kommen und inwieweit diese durch die betroffenen Internetnutzer legitimiert sind. Zweitens ist zu erörtern, inwieweit sich die ICANN gegen die Vormachtstellung der NSI behaupten kann. Hier werden die Verträge zwischen beiden Organisationen kurz dargestellt. Das dritte Problem besteht im schwierigen Verhältnis der ICANN gegenüber den ccTLDs, denn sie möchte für ihre Verwaltungsarbeit Gebühren erheben, obgleich die Basis eines solchen Anspruches bisher zu fehlen scheint. Im letzten Punkt geht es um die Autorität über den *A Root Server*, der immer noch der USA untersteht, und um die Frage, welche Auswirkungen dies auf die Arbeit der ICANN hat.

---

<sup>672</sup> Siehe <http://www.naisproject.org>. Vgl. auch *NAIS, Overview of the NGO and Academic ICANN Study*, 7. Februar 2001, <http://www.naisproject.org/010207overview.shtml> und *ICANN Channel*, NAIS-Gruppe plant At-Large-Studie, 5. Februar 2001.

<sup>673</sup> *NAIS, Interim Report*, 30. Mai 2001, <http://www.naisproject.org/report/interim/>.

<sup>674</sup> Ausführlich hierzu *Heise-Newsticker*, Komitee für die Organisierung der ICANN-Mitglieder gegründet, 13. November 2000.

#### 3.2.3.1. Legitimation durch Mehrheitsentscheidungen oder Konsens

Der Grundgedanke der ICANN soll die Schaffung von technischen Regeln sein. Da in ihren Entscheidungen auch politische und rechtliche Aspekte mit einbezogen werden müssen und damit auch gesellschaftliche Auswirkungen auf eine Vielzahl von Internetnutzern einhergehen, bedürfen diese einer wie auch immer gearteten Legitimation.

Nach unserem heutigen Verständnis von Demokratie erlangen herkömmliche rechtssetzende Organe (Legislative) ihre Legitimation durch die Entsendung gewählter Volksvertreter. Um am Demokratieprozeß teilzunehmen, schließen sich gleichgesinnte Bürger zu Parteien zusammen und versuchen durch Fraktionsbildung gemeinsam ihre Interessen zu artikulieren und zu vertreten. Der Beschuß eines Gesetzes erfolgt mit der jeweils erforderlichen Mehrheit der Abgeordneten. Wenn diese Mehrheit erlangt wurde, kann die Umsetzung und Einhaltung der von der Legislative erlassenen Regelungen innerhalb eines Staatsgebildes durch die Exekutive und Judikative erzwungen werden. Einer solchen Entscheidung müssen sich auch alle Personen unterwerfen, die im Rechtssetzungsprozeß eine abweichende Meinung vertreten haben. Die Regeln entfalten somit eine Art Allgemeingültigkeit. Mehrheitsentscheidungen führen (ohne Kontroll- und Balancesystem) gewissermaßen zur Mißachtung der Interessen der Minderheiten.

Im Internet, in welchem exekutive und judikative Elemente wenig Verbreitung gefunden haben und Normen sich entsprechend schwer durchsetzen lassen, kann ein demokratisches Verfahren kaum zum Erfolg führen<sup>675</sup>. Unterlegene Parteien sind kaum gehalten, sich Beschlüssen der Mehrheit zu unterwerfen und können entgegenstehende Handlungen ungehindert vornehmen. Soweit keine Zwangsmittel existieren, ist es somit wichtig, schon im Vorfeld alle wichtigen Meinungen in die Überlegungen zur Gestaltung von Normen mit einzubeziehen. Folglich gehen die im Internet beheimateten Standardisierungsorganisationen nicht nach dem Prinzip der Mehrheitsentscheidung vor. Um eine möglichst breite Umsetzung der beschlossenen technischen Normen und Standards zu erlangen, wird schon während der Erarbeitung dieser auf das im Kapitel 2.4.1.3.2 oben erörterte Verfahren der Konsensbildung abgestellt. Die Bildung eines Konsenses divergiert maßgeblich von dem Prozeß einer repräsentativen Demokratie. Alle Vorschläge müssen zwischen den betroffenen Parteien diskutiert werden. Einwände müssen zur Zufriedenheit aller gelöst werden, anstatt sie zu überstimmen. Der mit der Suche nach einem besseren Ergebnis verbundene Dialog führt zu einer Lösung, welcher alle Parteien zustimmen können. Ein solches Verfahren kann zu einem besseren Ergebnis führen, als dies durch eine Mehrheitsentscheidung möglich ist. Besonders dann ist das Konsensverfahren vorteilhaft, wenn die am Dialog beteiligten Parteien einen größeren Sachverstand und tieferes Wissen in die Diskussion einbringen, als demokratisch gewählte Repräsentanten dies könnten<sup>676</sup>.

---

<sup>675</sup> Vgl. zum Ganzen auch *Johnson/Crawford, Why Consensus Matters*.

<sup>676</sup> Siehe *Johnson/Crawford, Why Consensus Matters*.

Die ICANN ist so strukturiert, daß eine Entscheidung des *Boards of Directors* durch eine einfache Mehrheit gefällt wird. Somit erfolgen alle Abstimmungen zentralisiert und werden zu Lasten derer gefällt, welche nicht direkt im Vorstand vertreten sind. Entgegen des äußeren Anscheines, sind die ICANN-Direktoren nur zu einem geringen Anteil entsendete Repräsentanten der betroffenen Internetnutzer. Da jedoch die ICANN das DNS verwaltet, hat diese das Druckmittel potentielle *Registries* und *Registrars* abzuweisen, wenn diese die von ihr entwickelten Regeln (Policies<sup>677</sup>) ablehnen würden. Alle akkreditierten *Registries* and *Registrars* mußten zustimmen, sich entsprechen den Policies zu verhalten. Über die *Registries* und *Registrars* sind wiederum die Endnutzer an die Policies der ICANN gebunden. Nach der Satzung müssen diese Regeln im Konsens entwickelt worden sein, ohne den das ICANN-Board sie nicht in Kraft setzen darf. Sollte das Bestehen eines Konsenses bestritten werden, steht die Entscheidung einer Überprüfung durch das noch mit Mitgliedern zu besetzende *Independent Review Panel* (siehe Kapitel 3.2.2.3 oben) offen. Ein solches Organ stellt einen notwendigen Kontrollmechanismus in der Struktur der ICANN dar, ohne den die Ansichten von Minderheiten mühelos übergangen werden könnten.

Die Satzung der ICANN definiert das Konsensverfahren außerdem für die DNSO, speziell für deren Repräsentationsorgan, dem *Name Council*<sup>678</sup>. Für die anderen zwei *Supporting Organizations* konnte auf eine nähere Ausformulierung des Verfahrens verzichtet werden, da die in ihnen sitzenden Organisationen als im Internet beheimatet, bestimmungsgemäß das Konsensprinzip anwenden, beziehungsweise dieses Prinzip ihren Ursprung in diesen Organisationen hat<sup>679</sup>.

Einen Konsens zu einem bestimmten Thema im Kontext des DNS zu finden, ist kein leichtes Unterfangen. Im traditionellen Umfeld der Internetstandardsetzung erreichte man ein Einvernehmen der Diskutierenden insbesondere durch die relativ kleine und homogene Gemeinschaft der Internetingenieure, die durch die gemeinsamen Werte und Berufsnormen (wie der Anerkennung technischer Erfahrung) geprägt war. Zum anderen waren die zu lösenden Probleme rein technischer Natur und gesellschaftliche Standpunkte blieben außen vor.<sup>680</sup> An der Lösung von strittigen Fragen innerhalb der ICANN, wie die Einführung neuer TLDs oder der UDRP, sind eine Vielzahl an Interessensvertretern beteiligt, deren Vorschläge zum Teil extrem voneinander divergieren. In der Diskussion treffen rein wirtschaftliche auf entgegenstehende gesellschaftspolitische Aspekte. Hier einen Konsens zu erlangen, scheint unmöglich<sup>681</sup>. In ein solches Dilemma verwickelt, versuchte die ICANN oftmals erst gar nicht einen Konsens zu erreichen und entschied besonders umstrittene Thematiken mit gesellschaftspolitischer Tragweite häufig durch eine einfache Abstimmung im ICANN-Board. Obgleich die

---

<sup>677</sup> Hierzu gehört z.B. die Uniform Domain Name Dispute Resolution Policy der ICANN, vgl. Kap. 3.3.1.2.

<sup>678</sup> *Bylaws of ICANN*, 16. Juli 2000, Art. VI-B, Sec. 2, Fn. 600.

<sup>679</sup> Vgl. die Ausführungen zur IETF und zum W3C im Kap. 2.4.1.2.2.

<sup>680</sup> Vgl. Weinberg, 50 Duke L.J. 187, 252. Siehe auch F. 319 in Liu, 74 Ind. L.J. 587, 598f.

<sup>681</sup> Z.B. Weinberg, 50 Duke L.J. 187, 252f. sieht im Rahmen des DNS das Erreichen eines Konsens als unmöglich an.

### 3.2. Arbeit der ICANN

---

ICANN damit ihre Handlungsfähigkeit wahrte, traf sie Entscheidungen, die durch die betroffenen Internetnutzer nicht ausreichend legitimiert waren.

Weitreichende Entscheidungen der ICANN sollten jedoch nur umgesetzt werden, wenn diese im Einvernehmen mit den meisten Internetnutzern stehen und den Interessen einer nur sehr geringen Personenanzahl widersprechen. Dabei ist nicht ein einhelliges Zustimmen der Internetnutzer erforderlich. Vielmehr muß eine substantiierte Unterstützung gegeben sein. Diese wird insbesondere dann möglich sein, wenn den betroffenen Parteien die Gründe für eine Lösung plausibel gemacht werden können, um bestehende Zweifel seitens der Internetnutzer an der Konsenserlangung zu überwinden. Ein ausführlicher Bericht<sup>682</sup> über die differenzierten Meinungen und Lösungsvorschläge sowie ein darauf ansetzender transparenter Diskussionsprozeß kann auch außenstehende Personen, welche nicht an der Entwicklung bestimmter Regelungen teilgenommen haben, von der Notwendigkeit des erzielten Ergebnisses überzeugen. Beispiele gelungener Dokumentationen stellen die Begründungsreporte zur UDRP durch die WIPO dar<sup>683</sup>. Diese dokumentierten ausführlich die Diskussionen derer, die vom Vorschlag einer UDRP betroffen waren. Er zeigte die Für- und Gegenargumente auf und verwies auf weitere Hintergrundinformationen. Der Report macht deutlich, daß das Streitschlichtungsverfahren durch die Internetgemeinschaft erarbeitet und durch einen Konsens beschlossen wurde.

Eng mit einer ausreichenden Dokumentation der Diskussionen ist die Offenheit dieser verbunden. Ein Konsens kann nur erreicht werden, wenn alle Parteien ihre Ansichten beisteuern können und für diese auch der Entscheidungsweg völlig transparent ist<sup>684</sup>. Folglich müßten alle Treffen des ICANN-Board öffentlich veranstaltet werden. Der Versuch der ICANN, eine transparente Diskussion durchzuführen, mußte sich allerdings einiger Kritik aussetzen. Auf dem Board-Treffen in Santiago de Chile wurde der Öffentlichkeit voller Zugang zur Diskussion gewährt, indem die Sitzung mit Kameras aufgenommen und live ins Internet übertragen wurde. Der Zuschauer konnte jedoch bei dieser Veranstaltung leicht den Eindruck gewinnen, daß die Direktoren schon vor der Sitzung wichtige Programmpunkte ausgehandelt hatten<sup>685</sup>. In der Sitzung selber erfolgten kaum die eigentlich erwarteten hitzigen Diskussionen. Bei einem solch geschlossenen Personenkreis, wie dem ICANN-Direktorium kann geschlußfolgert werden, daß transparente Entscheidungen nicht erzwungen werden können, da diese Personen bei grundlegenden Diskussionen regelmäßig der Öffentlichkeit ausweichen können. Ein anderes Ergebnis würde sich ergeben, wenn sich viele Personen an den Diskussionen beteiligen können. Dann würde es keine Rolle spielen, ob sich einige Diskussionsteilnehmer zusammen-

---

<sup>682</sup> Zu den Kriterien eines solchen Konsensreportes siehe *Johnson/Crawford*, ICANN Consensus Report. Zum Erfordernis einer ausführlichen Dokumentation siehe auch *Post*, ICANN and the Consensus.

<sup>683</sup> WIPO, Internet Domain Names, Request for Comments, <http://wipo2.wipo.int/process2/rfc/index.html>.

<sup>684</sup> Siehe *Post*, ICANN and the Consensus.

<sup>685</sup> Vgl. die kritische Untersuchung des Board-Treffens in Santiago im *Cook Report*, ISOC's ICANN Coalition Widens Its Control, Kap. Open Meetings or „Performing an Act?“.

schließen und untereinander ihre Beiträge abstimmen, da andere Teilnehmer nicht daran gehindert werden, ihre eigenen Ansichten in der Diskussion darzustellen.

Ein Nachteil ergibt sich allerdings aus dem Konsensverfahren. Um eine Einigung zu erreichen, sind oft viele Diskussionsrunden nötig, zum einen, um eine Lösung weiterzuentwickeln oder, zum anderen, um Alternativen zu finden. Bei stark umstrittenen Problemen kann die Suche nach einem Konsens zu einem langwierigen Verfahren werden, ohne daß eine Lösung in greifbarer Nähe erscheint. In einer repräsentativen Demokratie ziehen stark umstrittene Positionen eine Abstimmung nach sich. Allerdings würde eine mehrheitliche Entscheidung nicht zu einem schnelleren Erfolg führen, wenn keine zwangsweise Durchsetzung des Ergebnisses möglich ist. Um möglichst einem großen Personenkreis eine Identifizierung mit dem Ergebnis zu ermöglichen, muß, wenn auch in einem langen Verfahren, ein Konsens zwischen den Parteien erreicht werden, denn die ICANN hat auf Dauer genauso wenig die Gewalt, alle ihre Entscheidungen mittels Zwang durchzusetzen, wie die standardsetzenden Organisationen. Sie ist somit auf einen Konsens angewiesen. Da die ICANN-Direktoren größtenteils keine gewählten Vertreter der Internetnutzer sind, kann in den Fällen, in denen ein Konsens sich scheinbar durch eine Abstimmung ersetzen ließe, nicht sichergestellt werden, daß die gefundene Meinungsverteilung derjenigen des betroffenen Personenkreises entspricht. ICANN müßte ihre Struktur stark abändern, um glaubwürdig behaupten zu können, alle von den Entscheidungen betroffenen Nutzerkreise zu repräsentieren. Auch muß die Zusammensetzung der betroffenen Parteien von Thematik zu Thematik variieren dürfen, solange die Internetnutzer in der ICANN nicht als Ganzes repräsentiert sind. Als weiterer Punkt muß hier beachtet werden, daß die von den Entscheidungen der ICANN betroffenen Personen dem Recht ihrer Staaten unterliegen. Das heißt, auch eine demokratisch legitimierte ICANN kann nur im begrenzten Maße verbindliche Regeln entwerfen. Eine weltweite Umsetzung ihrer Entscheidungen wird häufig an entgegengesetzten nationalstaatlichen Rechten scheitern.

Wenn man das letzte Kriterium unbeachtet läßt, sind viele Entscheidungen der ICANN nicht legitim, da den Meinungen der Internetnutzer zu wenig Aufmerksamkeit geschenkt wurde. Zusammenfassend geben David R. Johnson and Susan P. Crawford einen näheren Aufschluß wie ICANN allseits in der Internetgemeinschaft Anerkennung durch ein konsensuales Verfahren erringen kann<sup>686</sup>:

The goal of all who wish the ICANN experiment well is to enhance the legitimacy of ICANN decisions. That legitimacy will come from two sources.

First, those required to comply with ICANN policies will voluntarily have entered into contracts that commit them to abide by consensus policies on appropriate topics.

Second, the policies that are adopted and can be enforced will have been supported by detailed reports that show that such policies reflect very broad agreement and that opposition is either very limited, unreasoned, or comes from those who are not in fact adversely impacted.

---

<sup>686</sup> Siehe *Johnson/Crawford, Why Consensus Matters.*

Es ist ICANN somit anzuraten, ihre Entscheidungen transparent und repräsentativ zu fällen und bewährte Konsensmechanismen bei ihrer Arbeit zu beachten.

#### 3.2.3.2. Verhältnis der ICANN zur NSI

Wie oben erörtert, wurde das Verhältnis der ICANN zur NSI durch zwei Vertragswerke, dem *NSI/ICANN Registry Agreement*<sup>687</sup> und dem *ICANN/NSI Registrar Transition Agreement*<sup>688</sup> näher ausgestaltet. Nach diesen Verträgen hätte sich die NSI bis 1. April 2001 entweder von der *Registry* oder der *Registrar*funktion trennen müssen. Durch die Trennung des Datenbank- und *Root Server*-Managements (als *Registry*) von der Vermarktung der Adressen (als *Registrar*) sollte der Wettbewerb auf dem Domainmarkt angekurbelt und die Vormachtstellung von NSI gebrochen werden. Diese Regelung beruht besonders auf der Einflußnahme der Europäischen Union, welche 1999 ein Verfahren gegen die NSI erst eingestellt hatte<sup>689</sup>, nachdem das Unternehmen den Verkauf entweder von der *Registry*- oder der *Registrar*-Funktion in Verträgen mit dem US-DoC und der ICANN zugesichert hatte.

Am 2. März 2001 schlugen ICANN und NSI gemeinsam vor, daß NSI sowohl die *Registry* als auch *Registrar*-Funktion für die TLD .com dauerhaft behalten solle<sup>690</sup>. Im Gegenzug soll das Unternehmen ab 2002 die .org-*Registry* an eine eigenständige Organisation abgeben, welche die TLD .org wieder seiner ursprünglich zugedachten Funktion, der Registrierung nichtkommerzieller Organisationen, zuführen soll. Während NSI die TLD .net noch bis zum 1. Januar 2006 verwalten und sich dann einer Ausschreibung stellen will, möchte man die TLD .com bis 2007 und, sofern die ICANN keine Beanstandungen am Service hat, auch darüber hinaus behalten. Dieser Vorschlag wurde damals von der DNSO, insbesondere dem *Names Council* sowie einer großen Anzahl weiterer Interessensvertreter unter Protest zurückgewiesen<sup>691</sup>. Kritisiert wurde zunächst der zeitliche Druck, der auf die beteiligten Organe der ICANN ausgeübt wurde. Es bestand für die meisten ICANN-Direktoren sowie für den *Names Council* kaum Zeit, die Vorschläge zu prüfen. Änderungen konnten nicht mehr umgesetzt werden.

---

<sup>687</sup> Siehe Fn. 594.

<sup>688</sup> Siehe Fn. 594.

<sup>689</sup> Die Kommission der EU hatte im Juli 1999 ein Verfahren eröffnet, um die Vereinbarkeit der zwischen ICANN und NSI geschlossenen Verträge mit Art. 81 und 82 EGV zu prüfen, siehe Mitteilung der *Kommission: Kommission prüft Internet-Lizenzverträge auf Vereinbarkeit mit EU-Wettbewerbsregeln*, 29. Juli 1999, IP/99/596, [http://europa.eu.int/rapid/start/cgi/guesten.ksh?p\\_action=gettxt&gt;&doc=IP/99/596|0|AGED&lg=DE](http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action=gettxt&gt;&doc=IP/99/596|0|AGED&lg=DE). Auf Beschwerde mehrerer Unternehmen hin, sollte überprüft werden, inwieweit die weiteren Registrare diskriminiert würden. Das Verfahren wurde im November 1999 eingestellt, nachdem die von der Kommission vorgeschlagenen Änderungen in die Verträge übernommen wurden, siehe *Buigues/Urrutia, Gazette Européenne* Nr. 24, Juni 2000, 6.

<sup>690</sup> Siehe den aktuellen Vorschlag *ICANN, Revised VeriSign Registry Agreements*, 16. April 2001, <http://www.icann.org/tlds/agreements/verisign/>.

<sup>691</sup> Siehe *Heise-Newsticker*, ICANN-Fachgruppe gegen neue Verträge zu .com-Domains, 29. März 2001.

Auch begründeten die auch heute noch bestehenden vertraglichen Unterschiede<sup>692</sup> zu den weiteren Registraren das Risiko einer Wettbewerbsverzerrung zu Gunsten der NSI. Dennoch entschied sich das ICANN-Board am 2. April 2001 den Verträgen stattzugeben, mit dem Hinweis, die Beständigkeit des DNS zu sichern<sup>693</sup>. Die notwendige Zustimmung zu den Verträgen durch das US-DoC erfolgte am 18. Mai 2001 unter Maßgabe einiger Veränderungen<sup>694</sup>. NSI soll die *Registry* der TLD .net nur bis zum 30. Juni 2005 behalten dürfen und soll sich danach einer öffentlichen Ausschreibung für die Kontrolle über .net stellen. Sollte sich im *Registry*-Geschäft bis zum 31. Dezember 2002 kein ausreichender Wettbewerb entfaltet haben, so soll NSI die *Registry* für .net schon 2003 abgeben. Schließlich stimmte NSI ausdrücklich zu, daß die Genehmigung des US-DoC keine Zusicherung einer Immunität gegenüber dem Wettbewerbsrecht beinhaltet.

### 3.2.3.3. Verhältnis der ICANN zu den ccTLDs

Die länderspezifischen TLDs sind von einem Dreiecksverhältnis zwischen ihnen, der ICANN und dem GAC geprägt. Streitpunkte zwischen ihnen sind vor allem das vertragliche Dienstleistungsverhältnis zwischen der ICANN und den ccTLDs sowie die Frage der Delegierung und Re-Delegierung des Managements von ccTLDs. Das ICANN/US-DoC-MoU<sup>695</sup> bestimmt, daß die Übertragung des DNS zur ICANN nur nach Klärung des Verhältnisses der ICANN zu den ccTLDs vollendet werden kann. Auch die ICANN selbst hat ein direktes Interesse an der Klärung der Streitigkeiten, da sie die ccTLDs zu ihrer Finanzierung mit heranziehen möchte. Ein Versuch der ICANN Ende Mai 2000 die ccTLDs zur Zahlung einer Gebühr zu zwingen, scheiterte vor allem am Widerstand der europäischen ccTLDs<sup>696</sup>. Die Berechnung der Gebühr erfolgte nach der Zahl der registrierten Subdomains. Da die TLD .de die größte ccTLD ist, hätte die deutsche DENIC den Höchstbetrag von einer halben Million US\$ zahlen müssen<sup>697</sup>. Bei diesem Verfahren kann zunächst die Berechnungsgrundlage kritisiert werden, da die Subdomains von den ccTLDs verwaltet werden und damit der *Root Server*-Service der ICANN nicht abhängig von der Anzahl der Subdomains unter den jeweiligen ccTLDs ist. Außerdem erbringt die ICANN gegenüber den ccTLDs keine Extraleistungen (zum Beispiel keine Überprüfung der Registare oder Organisation eines Streitschlichtungsverfahrens) wie gegenüber den gTLDs. Das Betreiben eines *Root Servers* erfordert darüber hinaus kaum einen techni-

---

<sup>692</sup> Dingell, John D. und Markey, Edward J. stellen in ihrem Brief an das US-DoC die bestehenden Unterschiede zwischen den Verträgen der ICANN zur NSI und zu den anderen Registries und Registrars der TLDs heraus, [http://www.house.gov/commerce\\_democrats/press/107ltr53.htm](http://www.house.gov/commerce_democrats/press/107ltr53.htm).

<sup>693</sup> Siehe *ICANN-Announcement*, ICANN Announces Decision on Registry Agreement for .com/.net/.org Domains, 2. April 2001. Cerf, Vinton weist hier noch einmal auf die Bedeutung privatrechtlicher Betreibung des DNS hin: „[...] The normalization of this relationship is an important step toward the Internet community's goal in establishing ICANN -- creating a mechanism to ensure effective private-sector administration of this critical global resource for communication and commerce.“

<sup>694</sup> Siehe näheres zur Zustimmung des US-DoC unter *US-DoC*, *NTIA*, *Commerce*, *ICANN* und *VeriSign* Agreement in Principle, <http://www.ntia.doc.gov/ntiahome/domainname/agreements/termssheet51801.htm>.

<sup>695</sup> Zum ICANN/US-DoC-MoU siehe Kap. 3.1.3.1.

<sup>696</sup> Siehe die Pressemitteilung des Zusammenschlusses der europäischen ccTLDs, *Council of European National Top-Level Domain Registries* (CENTR), European ccTLD registries respond to ICANN invoices, 5. Juni 2000.

<sup>697</sup> *Heise-Newsticker*, ICANNs Verhältnis zu Länder-Domains ungeklärt, 16. Juni 2000.

### 3.2. Arbeit der ICANN

---

ischen oder finanziellen Aufwand, der eine Rechnungslegung von mehreren Millionen für die ccTLDs rechtfertigen würde. Eine Beitragspflicht zum Finanzaushalt der ICANN kann vom Gesichtspunkt der ccTLDs nur nach vertraglicher Abklärung beiderseitiger Rechte und Pflichten begründet werden, da bislang die ccTLDs keinerlei Verpflichtungen gegenüber ICANN eingegangen sind. Unter anderem muß der *Root Server*-Service der ICANN abgeklärt werden, da es darüber immer wieder zu Mißstimmungen unter den ccTLDs gekommen ist. Auch wünschen sich die ccTLDs, verstärkt an der ICANN-Arbeit mitwirken zu dürfen. Insbesondere möchte man direkt eigene Direktoren in das ICANN-Board entsenden, da die ccTLDs über ihre *Constituency* in der DNSO kaum die Chance haben, einen Vertreter entsenden zu können. Auf Grund des erwarteten hohen Finanzierungsbeitrages wurde zum Beispiel verlangt, daß die vier noch freien Sitze, welche der *At-Large Membership* zustehen sollten, an die ccTLDs vergeben werden, oder daß eine eigene *Supporting Organization* den ccTLDs zur Verfügung gestellt wird, um auf den Haushaltsplan der ICANN Einfluß nehmen zu können.

Andererseits wurden die Vertragsabschlüsse zwischen der ICANN und den Managern der ccTLDs bislang durch die Forderung des GAC blockiert, die Regierungen als oberste Autorität über die ccTLDs anzuerkennen und in die Verträge die *Principles for Delegation and Administration of ccTLDs*<sup>698</sup> des GAC mit einzubeziehen (Siehe Kapitel 3.2.2.3 oben). Kernpunkt dieser Prinzipien ist, daß die ccTLDs der nationalen Souveränität eines Staates unterstehen und damit auch die Regierungen die letztendliche Entscheidungshoheit haben, wenn es um die Delegation oder Re-Delegation von Rechten für das Management einer ccTLD geht. Die vom GAC gestellten Ansprüche sind jedoch für demokratisch legitimierte Länder nicht nachzuvollziehen, da hier die Betreiber der ccTLDs sowieso an das nationale Recht gebunden sind. Im Gegensatz dazu wird die Regierung in autoritären Staaten sich auch ohne Verträge das Recht anmaßen, in die Vergabe landesspezifischer Domains einzutreten. In Staaten, welche sich in einem gesellschaftlichen Wandel befinden, würde eine solche Anerkennung der Regierung als oberste Autorität, dieser die Möglichkeit geben, gesellschaftlich fortschrittlichen Kräften das Auftreten im Internet zu erschweren. Eine solche Regelung würde es undemokratischen Regierungen erlauben, das Management der entsprechenden ccTLD nach Belieben auszuwechseln und würde damit die Instabilität des DNS herbeiführen. Es besteht aber auch das Risiko, daß *Registries* von ccTLDs, die nicht im jeweiligen Land angesiedelt sind und damit nicht den nationalen Regeln unterworfen werden können, ihre Position zu mißbrauchen und zum Nachteil der nationalen Nutzer und Interessen auszunutzen. Die Re-Delegation einer ccTLD sollte sich deshalb nur nach technischen Kriterien richten und den Nutzern der jeweiligen ccTLD vom Vorteil sein.

Auf Grund der Diversität der rechtlichen Verankerung der ccTLDs in den Heimatländern<sup>699</sup>, muß deshalb auch ein differenziertes Verfahren bei den Verträgen mit der ICANN angewandt

---

<sup>698</sup> Siehe Fn. 636.

<sup>699</sup> Das Management der einzelnen ccTLDs unterscheidet sich z.B. hinsichtlich der Struktur (privatrechtliche Einheiten, öffentlichrechtliche Körperschaften oder Genossenschaften/Vereine), der Involvierung der entsprechenden nationalen Regierung, des zugrundeliegenden staatlichen Rechtssystems (Common Law oder kodifiziertes Recht).

werden. Zwei grundsätzliche Wege sind deshalb möglich<sup>700</sup>: Zum einen reichen bilaterale Verträge zwischen der ICANN und dem ccTLD-Management aus, wenn die nationalen Regierungen kein Interesse an einer Beteiligung an ihrer ccTLD zeigen. Dieselbe Regelung soll gelten, wenn sich die Verwaltung der ccTLD sich selbst im Land befindet und damit den nationalen Gesetzen unterworfen ist. Zum anderen wäre eine trilaterale Vereinbarung unter der Beteiligung der entsprechenden Landesregierung notwendig, um die Interessen der nationalen Nutzer der jeweiligen ccTLD vor Mißbrauch zu schützen, soweit sich das Management der ccTLD außerhalb des jeweiligen Landes befindet.

Die Verträge könnten sich in drei Komplexe gliedern. Der erste Komplex würde die Pflichten der ccTLDs als sogenannte *Best Practice Guidelines* enthalten<sup>701</sup>. Insbesondere sollten diese Richtlinien Regelungen enthalten, wie die Domainnamen zu registrieren wären<sup>702</sup>:

### 3.2 Registration of Domain Names

#### ccTLD Managers:

- must register domain names in an efficient and timely manner, following policies rules and procedures that have been established and published in a transparent manner in consultation with the Local Internet Community.
- must collect the necessary information to ensure that the Registrant can be authoritatively identified.
- should have a standard contract with Registrants.
- should recognise that some of the functions of the registry may be considered to be a monopoly and should not abuse its special position.

Der zweite Komplex würde Regelungen zur Re-Delegation von ccTLDs beinhalten. Die ICANN hatte sich bislang nach den RFC 1591 und dem Dokument ICP-1<sup>703</sup> gerichtet, welche die Delegationspraxis der IANA wiedergeben. In neuen Verträgen mit der ICANN sollten nun Bestimmungen aufgenommen werden, wer eine Re-Delegation beantragen darf und nach welchen Kriterien sie sich richten soll. Das GAC fordert, wie schon erwähnt, die Einbeziehung ihrer *Principles for Delegation and Administration of ccTLDs*. Um zu vermeiden, daß das Management einer ccTLD politisiert wird, sollten entsprechende technische Kriterien der Betreibung einer ccTLD in den *Best Practice Guidelines* aufgenommen werden. Eine Re-Delegation dürfte nur dann legitim sein, wenn die Verwaltung der ccTLD diesen technischen

---

ziertes Recht romanischen Ursprungs) und der Umsetzung von landesspezifischen Rechtsprinzipien (wie Datenschutz, Markenrechtsschutz, Verbraucherschutz).

<sup>700</sup> Vgl. *Heise-Newsticker*, Wer kontrolliert die Länder-Domains?, 14. März 2001.

<sup>701</sup> Zu den Anforderungen siehe *CENTR*, Introduction to Best Practice Guidelines, Fassung vom 10. Mai 2001, <http://www.centr.org/docs/legal/bp-intro.html> und *ICANN*, Best Practices Guidelines for ccTLD Managers (1st Draft) Presented by CENTR, 24. Februar 2000, <http://www.icann.org/cairo2000/centr-cctldbestpractices-24feb00.htm>.

<sup>702</sup> Siehe *ICANN*, Best Practices Guidelines for ccTLD Managers (1st Draft) Presented by CENTR, Fn. 701.

<sup>703</sup> *ICANN*, Internet Domain Name System Structure and Delegation, Mai 1999, <http://www.icann.org/icp/icp-1.htm>.

Anforderungen nicht gerecht wird. Die Re-Delegation sollte einem fairen Verfahren unterliegen, um voreilige und rechtswidrige Übertragungen auszuschließen.

Schließlich ist zwischen der ICANN und den ccTLDs ein Service-Vertrag notwendig, welcher die Leistungen und Gegenleistungen zwischen der ICANN und den ccTLDs definiert. Insbesondere muß der Betrieb des *Root Servers* geklärt und die Berechnungsmethode der Beiträge der ccTLDs zum Finanzaushalt der ICANN bestimmt werden.

#### 3.2.3.4. Autorität über den A Root Server

Eine aus internationaler Sicht weitere Problematik stellt die Autorität über den *A Root Server*<sup>704</sup> dar. Der *A Root Server* untersteht derzeit der US-Regierung, insbesondere dem US-DoC. Die Autorität über den *A Root Server* erhielt das US-DoC im September 1998 von der NSF<sup>705</sup>. Schon damals war vorgesehen, daß das US-DoC den *A Root Server* übernehmen solle, um planmäßig den vollständigen Ausstieg der US-Regierung aus der Kontrolle des DNS zu ermöglichen. Hierzu wurde das *Cooperative Agreement* zwischen NSI und der US-Regierung erweitert<sup>706</sup>. In diesem verpflichtete sich die NSI, das US-DoC als oberste Autorität anzuerkennen und den *A Root Server* weiter für die US-Regierung zu betreiben. Außerdem wurde festgelegt, daß die NSI jegliche Entscheidungen über Änderungen der Datenbank des *A Root Servers* nur nach schriftlicher Autorisierung durch das US-DoC vornehmen kann.

In der Vereinbarung zwischen ICANN, NSI und dem US-DoC vom Herbst 1999<sup>707</sup> wurde das *Cooperative Agreement* auf zunächst vier Jahre befristet und sollte bei gewissen Umständen auf weitere vier Jahre verlängert werden. Auch diese Vereinbarung stellte klar, daß das US-DoC die Autorität über den *A Root Server* behält. ICANN sollte dem US-DoC einen Vorschlag unterbreiten, wie die Verwaltung des *A Root Servers* auf die ICANN zu irgendeinem zukünftigen Zeitpunkt übertragen werden kann. Hierzu ist das US-DoC in den oben schon erörterten *Sole Source Contract* getreten<sup>708</sup>, wonach ICANN die Administration des *A Root Servers* obliegt. Doch auch dieser Vertrag schränkte die Rechte der ICANN stark ein:

This [administrative] function, however, does not include authorizing modifications, additions, or deletions to the root zone file or associated information that constitute delegation or redelegation of top-level domains. The purchase order will not alter root system responsibility defined in amendment 11 of the Cooperative Agreement.

Pläne, den *A Root Server* vollständig auf die ICANN zu übertragen und damit die Autorität über den *Root Server* an eine privatrechtliche Organisation abzugeben, gibt es derzeit nicht. Besonders im amerikanischen Raum wird dem US-DoC das Recht abgesprochen, eigenstän-

---

<sup>704</sup> Zum Root Server System siehe Kap. 2.2.2.3.

<sup>705</sup> US-GAO, Report, S. 27.

<sup>706</sup> NSI, Cooperative Agreement, Amendment No. 11, siehe Fn. 530.

<sup>707</sup> Siehe Fn. 594.

<sup>708</sup> Siehe Kap. 3.1.3.1.

dig den *A Root Server* zu privatisieren<sup>709</sup>. Vielmehr wird er als Staatseigentum der USA angesehen und bei einer Privatisierung die Zustimmung des US-Kongresses gefordert. Unter dem Gesichtspunkt, daß das US-DoC weder durch Gesetze noch durch internationale Abkommen die Autorität über den *A Root Server* erlangt hat, fällt die Beantwortung der Frage, ob das US-DoC das Recht hat, den Server zu privatisieren, schwer. Wie schon erwähnt (Kapitel 2.1 oben) stammte das DNS aus US-amerikanischen Forschungseinrichtungen und wurde ursprünglich durch die US-Regierung stark finanziert und seit 1993 durch die NSI verwaltet. Hieraus kann zwar ein Recht zur Verwaltung des *A Root Servers* hergeleitet werden, es besteht jedoch keine Verpflichtung der US-Regierung, das DNS und damit den *A Root Server* zu betreuen<sup>710</sup>. Die Abgabe der Autorität an eine internationale Organisation scheitert am Interesse der Vereinigten Staaten, ein potentielles Druckmittel aus der Hand zu geben. So ist es möglich, daß die USA im Falle einer Auseinandersetzung mit anderen Staaten, ein Abschalten bestimmter TLDs ihrer Kontrahenten als Sanktion einsetzt. Wer die Autorität über den *A Root Server* besitzt, kann unter Umständen auch andere Interessen im Internet umsetzen, wie ein Verbot von Pornographie oder US-feindlicher Kritik. Eine solche einseitige Verteilung der Machtverhältnisse über das DNS widerspricht jedoch der internationalen Bedeutung des Internets. Beschränkungen der Kommunikation über das Internet würde inzwischen in vielen Staaten eine wirtschaftliche Rezession bewirken. Deshalb sollte die USA in nächster Zeit den Server aus ihrer Hand geben und damit ihren schon im White Paper geäußerten Vorstellungen nachkommen<sup>711</sup>:

#### The Coordinated Functions

[...] Coordination of the root server network is necessary if the whole system is to work smoothly. While day-to-day operational tasks, such as the actual operation and maintenance of the Internet root servers, can be dispersed, overall policy guidance and control of the TLDs and the Internet root server system should be vested in a single organization that is representative of Internet users around the globe.

#### 3.2.3.5. Finanzierung der ICANN

Um die Koordinationsarbeit der einzelnen am ICANN-Verfahren teilnehmenden Organisationen, die rechtliche Absicherung der ICANN in Streitigkeiten und die internationale Präsenz der ICANN zu sichern, ist ein hoher finanzieller Aufwand notwendig. Die Bereitstellung des dafür erforderlichen Budgets ist auch heute noch zum Teil ungeklärt. Der größte Teil des ICANN-Finanzetats wird derzeit von den *Registries* und den *Registrars* der generischen TLDs erbracht. Ein Teil der Finanzen wurde in letzter Zeit von großen US-Firmen, wie IBM oder MCI zur Verfügung gestellt. Darüber hinaus sollten ursprünglich von jedem Domaininhaber 1 US\$ an die ICANN abgeführt werden. Auch die ccTLDs sollen sich an einer Finanzierung der ICANN beteiligen.

---

<sup>709</sup> Z.B. *Froomkin*, 50 Duke L.J. 17, 175.

<sup>710</sup> *US-GAO*, Report, S. 25f.

<sup>711</sup> *US-DoC, NTIA*, White Paper, 63 Fed. Reg. 31749.

Die vorgeschlagene 1 US\$ Gebühr wurde von vielen Organisationen als indirekte Steuer abgelehnt und wurde deshalb am 19. Juli 1999 als nicht einführbar durch die ICANN verworfen<sup>712</sup>. Zur Überwindung des nun entstandenen Finanzierungstiefs, mußte die ICANN verstärkt auf private Kredite zurückgreifen, so daß sie bis zu 2 Mio. US\$ an Darlehen, besonders von Unternehmen aus dem Computer- und Netzwerkbereich, aufnehmen mußte<sup>713</sup>. Eine Task Force, von der ICANN eingesetzt, um Lösungen zur Finanzierung zu finden, schlug im Oktober 1999 schließlich vor, daß der Etat zu 55% von den *Registries* und den *Registrars* der gTLDs, 35% von den *Registries* der ccTLDs und 10% von den IP-*Registries* zur Verfügung gestellt werden soll<sup>714</sup>. Entsprechend konnten in der Folgezeit mit verschiedenen Organisationen Verträge zur Finanzierung der ICANN geschlossen werden. Wie oben schon erwähnt (Kapitel 3.2.3.3 oben) wurde dieses Finanzierungsschema von den im CENTR zusammenge schlossenen ccTLDs scharf kritisiert<sup>715</sup>. Zum einen wird eine an Hand der registrierten Domains berechnete Abgabe abgelehnt, da dies einer indirekten Besteuerung auf Domainnamen gleicht. Andererseits wird ein klares Vertragsverhältnis gefordert, welches die Leistungen und Gegenleistungen der Vertragsparteien näher festlegt.

#### 3.2.4. ICANN in der Zukunft

Im Laufe ihres Bestehens hat die ICANN häufig Anlaß zu Kritik gegeben. Es können dabei folgende Einwände zusammengefaßt aufgeführt werden:

- die Einsetzung eines ungewählten *interim Boards of Directors* dessen Mitglieder von Dr. Jon Postel ohne Transparenz eingesetzt wurden;
- die völlige Überrepräsentation kommerzieller Interessensgruppen in den *Supporting Organizations*;
- die Tagungen des *Board of Directors* hinter geschlossenen Türen;
- die fundamentalen Veränderungen an den Gründungsdokumenten der ICANN durch das *Board of Directors* ohne Konsens in den betroffenen Nutzerschichten des Internets;
- die spärliche und kurzfristige Benachrichtigung der Öffentlichkeit über wichtige Entscheidungen der ICANN;
- die Verschiebung der Wahl weiterer vier ALM-Direktoren und die Einsetzung eines Überprüfungskomitees der *At Large Membership*;
- die Mißachtung von Entscheidungen der *Supporting Organizations* durch das *Board of Directors* und
- die gelegentliche Verletzung der Satzung durch das *Board of Directors*.

---

<sup>712</sup> US-GAO, Report, S. 23.

<sup>713</sup> US-GAO, Report, S. 43.

<sup>714</sup> ICANN President's Task Force on Funding, Report and Recommendations on ICANN Permanent Funding Arrangements, 30. Oktober 1999, <http://www.icann.org/committees/tff/final-report-draft-30oct99.htm>, Kap. IV. Allocating the ICANN Budget, C. Aggregate shares among classes of registries and registrars.

<sup>715</sup> Siehe CENTR, Statement from 6th General Assembly, 1./2. Juni 2000, <http://www.centr.org/docs/statements/ga-6.html>.

Bei der Äußerung der Kritikpunkte wird jedoch häufig die Bedeutung der ICANN über- schätzt. Nach der Einführung neuer TLDs und der endgültigen Privatisierung des DNS werden kaum neue Aufgaben für die ICANN hinzukommen. Die Entwicklung neuer Internetstandards wird weiterhin von der IETF und von dem W3C wahrgenommen werden können, die sich auch schon vor dem Bestehen der ICANN gegenseitig abgestimmt hatten. Das Angebot eines Streitschlichtungsmechanismus wird weiter unter der Schirmherrschaft der WIPO erfolgen können. Notwendig wird die ICANN im Tagesgeschäft bezüglich der Abstimmung der einzelnen *Registries* und *Registrars* bleiben, auch wenn nach der Einführung eines ausreichenden Wettbewerbs kaum noch Raum für neue Streitigkeiten bleiben wird. Hinzu kommt, daß nach einer vollständigen Privatisierung des DNS die beteiligten Unternehmen dem europäischen und amerikanischen Wettbewerbsrecht unterliegen und damit wettbewerbsbeschränkenden Maßnahmen auch außerhalb der ICANN eine Grenze gesetzt wird. Mit der Zulassung vieler neuer TLDs würde auch die Vielfalt der Organisationsstrukturen erhöht werden, so daß sich Raum für rein kommerzielle oder rein private TLDs eröffnet. Solange jedoch die ICANN in ihrer Tätigkeit als Verwalter des DNS auch politisch motivierte Entscheidungen zu treffen hat, muß sie sich an rechtstaatliche Prinzipien halten. Nur auf diese Weise kann sie die Anerkennung der verschiedenen im Internet vertretenen Interessensgruppen erlangen. Eine Zusammenfassung von Richtlinien, nach denen sich die ICANN richten sollte, wurde deshalb vom *Internet Democracy Project* ausgearbeitet<sup>716</sup>:

#### Guiding Values

1. ICANN must be representative.
2. ICANN must be transparent.
3. ICANN must use bottom-up processes.
4. Intellectual property rights are not privileged over other rights.
5. ICANN must limit itself to technical policy-making.
6. The domain name space is not an exclusively public resource.
7. Artificial scarcity and centralization should be avoided.
8. ICANN must respect privacy.
9. Costs should be minimal and equitable.

Dabei handelt es sich keineswegs um die Formulierung neuer Forderungen an die ICANN. Schon das *White Paper* der US-Regierung enthielt ähnliche Bedingungen für die Restrukturierung der Verwaltung der IP-Nummern und des DNS. Hervorzuheben sind hierbei besonders die ersten drei Punkte, welche Grundprinzipien der Selbstregulierung des Internets darstellen. Eine erfolgreiche Reform des DNS wird sich deshalb nur unter Beachtung dieser Anforderungen verwirklichen lassen.

---

<sup>716</sup> Siehe *Internet Democracy Project*, Draft Yokohama Statement on Civil Society and ICANN Elections, 27. Juni 2000, [http://www.cpsr.org/internetdemocracy/yoko\\_statement.html](http://www.cpsr.org/internetdemocracy/yoko_statement.html) mit ausführlicher Erläuterung der einzelnen Richtlinien.

### **3.3. Reform des DNS durch die ICANN**

Mit Gründung der ICANN konnte die lang geforderte Reform des DNS voranschreiten. Auch wenn die Bestrebungen der ICANN immer eine Reihe von Kritikpunkten aufwiesen, so konnte sie einige wichtige Änderungen am DNS umsetzen. Hierzu gehört das schon erörterte *Shared Registry System* (Kapitel 3.1.3 oben), das einer Vielzahl von *Registrars* den direkten Zugang zu den *Registries* ermöglicht. Ein weiterer Punkt stellt die Einführung eines Verfahrens zur Schlichtung von Streitigkeiten um Domainnamen dar, welches in diesem Kapitel erläutert wird. Zu den Neuerungen gehört auch die Einführung neuer TLDs. Dieser Prozeß befindet sich derzeit noch in der Anfangsphase, so daß der weitere Weg noch offen ist. Ebenso dringend ist die Einführung multilingualer Domainnamen in das DNS, da man im bisherigen System weder die in Europa gebräuchlichen Umlaute, noch Zeichen anderer Schriftsprachen als Elemente von Domainnamen verwenden kann. Auch auf diese Reformbestrebungen wird in diesem Kapitel kurz eingegangen.

#### **3.3.1. Uniform Domain Name Dispute Resolution Policy**

Die *Uniform Domain Name Dispute Resolution Policy*<sup>717</sup> (UDRP) regelt ein Verfahren zur außergerichtlichen Streitschlichtung vor einem Schiedsgericht zwischen Inhabern von Domainnamen und einem Dritten, welcher der Ansicht ist, daß der Inhaber des Domainnamens diesen zu Unrecht verwendet. Dieses Verfahren ist innerhalb der gTLDs .com, .net und .org anwendbar. Hinzu kommen einige kleine ccTLDs, die das Verfahren freiwillig übernommen haben.

Streitigkeiten um Domainnamen sind bis 1994 zurückzuführen, nachdem das Internet für die Wirtschaft zugänglich wurde und sich verstärkt unter Privatnutzern verbreitete<sup>718</sup>. Den Unternehmen wurde allmählich klar, daß der Wert eines Domainnamens außerordentlich hoch sein kann, obwohl man ihn auf der Basis „first come, first served“ zu einem vergleichsmaßig niedrigen Preis reservieren könnte. Zum einen wurde das Wachstum des Internets durch die preiswerte und offene Registrierungsmöglichkeit von Domainnamen gefördert, andererseits wurde durch die freie Namenswahl der Mißbrauch fremder Namensrechte begünstigt. Je mehr sich die Nutzung des auf Domainnamen basierenden WWWs verbreitete, um so mehr wurden Personen ermutigt, Domainnamen im großen Umfang für sich zu reservieren und diese erneut über einen sekundären Markt zu veräußern. Bei diesem sogenannten *Domain Grabbing* (oder *Cyber Squatting*) ist jedoch zwischen zwei Varianten zu unterscheiden. Zum einen werden Gattungsbezeichnungen (wie Börse, Mitwohnzentrale oder Wirtschaft) reserviert. Obgleich hiermit eine bewußte Ausnutzung des DNS vorliegt, werden mit der Reservierung von generischen Namen keine Namensrechte anderer verletzt. Eine Veräußerung dieser Namen erfolgt gewöhnlich über Domainbörsen. Zum anderen werden jedoch im großen Maße zum Beispiel Marken, Produktbezeichnungen oder Ortsbezeichnungen reserviert, um diese an den rechtmäßigen Namensinhaber zu verkaufen. Auf nationaler Basis würde ein einfacher Rückgriff auf

---

<sup>717</sup> Uniform Domain Name Dispute Resolution Policy, 24. Oktober 1999, Fn. 614.

<sup>718</sup> Zu einem der ersten Fälle von Domaingrabbing der Domain „mcdonalds.com“ siehe *Mueller, Rough Justice*, Kap. Six years and counting.

die sich historisch entwickelten Rechtsinstitute ausreichen, um eigene Namensrechte gegen mißbräuchliche Nutzung durchzusetzen. Das nationale Rechtssystem fand jedoch schnell beim internationalen Internet seine Grenzen. Die Verfolgung von Namensmißbräuchen über die Ländergrenzen hinweg erwies sich schon frühzeitig als äußerst aufwendig und teuer. Es wurde deshalb zunächst versucht, bei den die TLDs betreibenden *Registries* Rückgriff zu nehmen und diese zu einer Sperrung oder Übertragung der entsprechenden Domain zu verurteilen. Jene versuchten aber drohenden Gerichtstreitigkeiten durch vorläufige Sperrungen der Domainnamen zu entgehen.

Die NSI führte zu diesem Zweck die *Dispute Resolution Policy* ein. Dieser *On Hold* genannte Status half jedoch den Namensinhabern nicht, auf internationaler Ebene ihre Ansprüche durchzusetzen, da diese immer noch ein Gerichtsurteil benötigten, um von NSI die Umschreibung der Domain verlangen zu können. Beim ersten auf internationaler Basis beruhenden Ansatz versuchte man in Zusammenarbeit mit der WIPO (mittels des schon erwähnten gTLD-MoU), das sogenannte *Administrative Domain Name Challenge Panels* einzuführen. Vor einem solchen Gremium sollte in Form eines Schiedsverfahrens über die Rechtmäßigkeit der Registrierung eines strittigen Domainnamens entschieden werden können. Mit Scheitern des gTLD-MoU konnte dieses Schiedsverfahren jedoch erst durch die ICANN in erweiterter Form mittels der *Uniform Domain Name Dispute Resolution Policy* (UDRP) eingeführt werden. Dieses Schiedsgerichtsverfahren wurde sehr schnell von der Wirtschaft angenommen, muß sich jedoch insbesondere der Kritik eines möglichen *Forum Shopping's* und Bevorzugung von Markenrechtsinhabern aussetzen. Um ein Verständnis für das Regelungsinstrument der UDRP zu ermöglichen, soll zunächst auf die Regelungen durch die NSI und durch das gTLD-MoU eingegangen werden, bevor die Implementierung der UDRP näher erörtert wird. Im Rahmen dieser Arbeit soll jedoch nicht näher auf den marken- und namensrechtlichen Hintergrund eingegangen, sondern vielmehr die Funktionalität der UDRP dargestellt werden.

### 3.3.1.1. Lösungen durch die NSI und das gTLD-MoU

Für eine *Registry* ist es nicht möglich, jeglichen Antrag auf einen Domainnamen weltweit auf Verletzung von Marken- und Namensrechten zu prüfen. Zum einen wäre ein solches Prüfungsverfahren sehr zeit- und kostenaufwendig und zum anderen nicht mit dem Zweck eines Domainnamens vereinbar, zunächst nur eine einfache Merkhilfe für eine IP-Adresse darzustellen. Um jedoch dem Anliegen der Markenrechtsinhaber entgegenzukommen und um Klagen zu umgehen<sup>719</sup>, führte die NSI im Juli 1995 die *Domain Name Dispute Policy* (DNDP) ein, um die Lösung von Domainstreitigkeiten zu vereinfachen<sup>720</sup>. Die DNDP regelte die Eintragungsvoraussetzungen für Domainnamen und das Verfahren bei Kennzeichenkonflikten. Im Laufe der Zeit folgten drei Revisionen der DNDP, die letzte Version trat am 25. Februar 1998 in Kraft<sup>721</sup>. Die vier wichtigsten Regelungen lassen sich wie folgt zusammenfassen<sup>722</sup>:

---

<sup>719</sup> Z.B. wurde die NSI in den Rechtsstreit *Knowledgenet Inc. v. D. L. Boone* wegen Beihilfe mit einbezogen, vgl. dazu Fn. 32f. in *Bettinger*, GRUR Int. 1997, 402.

<sup>720</sup> NSI Domain Name Dispute Policy, Revision 3, 25. Februar 1998, <http://www01.worldnic-jp.com/regist/domain.html>.

<sup>721</sup> Siehe NSI Domain Name Dispute Policy, Fn. 720.

- Der Antragsteller hatte eine Erklärung abzugeben, daß der gewünschte Domainnamen, soweit er davon Kenntnis hat, nicht Rechte anderer Parteien verletzt.
- Er mußte die Absicht haben, den Domainnamen im Guten Glauben zu verwenden.
- Er durfte den Domainnamen nicht zu gesetzeswidrigen Zwecken registrieren.
- Schließlich konnte ein Besitzer einer Handelsmarke die Zuweisung einer Domain durch NSI angreifen, soweit der Inhaber des Domainnamens erst nach der Registrierung der Handelsmarke mit der Nutzung seiner Domain begonnen hatte.

Der Beschwerdeführer mußte hierzu einen Nachweis der Registrierung seiner Handelsmarke an die NSI senden. Innerhalb von 30 Tagen mußte dann der Inhaber des Domainnamens nachweisen, daß die Nutzung der Domain entweder vor der Registrierung und Nutzung der Handelsmarke erfolgte oder, daß er ein eigenes Markenrecht an dem Namen besitzt. Kann er jedoch keinen dieser zwei Fälle nachweisen, hatte er die Nutzung der Domain innerhalb von 90 Tagen einzustellen. Die strittige Domain ging dann in den *Hold Status*, das heißt, sie stand während der Schwebezeit des Rechtsstreits zwischen den Parteien niemanden zur Verfügung. Bevor ein Gerichtsurteil oder eine Entscheidung eines Schiedsgerichtes ergangen war, konnte ein Beschwerdeführer nicht die Übertragung der Domain verlangen. Aus der Anzahl der gegen die NSI gerichteten Klagen<sup>723</sup> kann jedoch geschlußfolgert werden, daß dieses Verfahren häufig keine der Parteien befriedigte. Besitzer berühmter Marken konnten auch ohne die DNDP die Einstellung der Nutzung des Domainnamens verlangen, während kleine Unternehmen ohne Registrierung einer Handelsmarke nicht nach der DNDP vorgehen konnten. Außerdem waren etablierte Firmen, welche einen Domainnamen lange Zeit genutzt hatten, aber kein Markenrecht besaßen, der DNDP schutzlos ausgeliefert<sup>724</sup>.

Da die DNDP keinen ausreichenden Schutz für Markenrechtsinhaber bot und andererseits Domainnamensinhaber mißbräuchlicher Verwendung der DNDP ausgesetzt waren, dachte man über Alternativen nach. Die Möglichkeit zur Implementierung einer solchen Alternative bot im Mai 1997 das IAHC mit seinem gTLD-MoU. Neben der Einführung neuer gTLDs und

---

<sup>722</sup> Ausführlich wird auf die DNDP in *Albert*, 16 J. Marshall J. Computer & Info. L. 781, 786ff., *Leaffer*, 6 Ind. J. Global Legal Stud. 139, 151ff. und *Bettinger*, GRUR Int. 1997, 402ff. eingegangen.

<sup>723</sup> Neben vielen Verfahren siehe nur: *U.S. District Court, Middle District of Tennessee* vom 5. August 1998, *Data Concepts, Inc. v. Digital Consulting, Inc., and Network Solutions, Inc.*, 150 F.3d 620; *U.S. District Court, District of Colorado* vom 29. Oktober 1996, *Network Solutions, Inc. v. Clue Computing, Inc.*, 946 F.Supp. 858; *U.S. District Court, Central District of California* vom 17. November 1997, *Lockheed Martin Corp. v. Network Solutions, Inc.*, 985 F.Supp. 949; *U.S. District Court, Northern District of Illinois* vom 29. September 1997, *Juno Online Services v. Juno Lighting, Inc.*, 979 F.Supp. 684.

Ausführlich werden 19 Verfahren vor US-amerikanischen Gerichten in *Rony/Rony*, Domain Name Handbook, S. 380 bis 447 erörtert. Siehe auch *Oppedahl & Larson LLP*, NSI Flawed Domain Name Policy information page, 21. Dezember 1999, <http://www.patents.com/nsi.htm>.

<sup>724</sup> Z.B. sollte die Domain juno.com, unter welchem ein öffentlicher Emailservice angeboten wurde, durch NSI abgeschaltet werden, solange ein Markenrechtsverfahren der Juno Lightning, Inc. gegen den Inhaber von juno.com, der Juno Online Inc. anhängig war. Dies hätte für 500.000 Kunden den Verlust ihres Emailkontaktes bedeutet. Siehe *Rony/Rony*, Domain Name Handbook, S. 407ff.

eines freien Wettbewerbs im Domaingeschäft, sollte ein Verfahren zu einer online erfolgenden Lösung von Streitigkeiten um Domainnamen unter Mitwirkung des *WIPO Arbitration and Mediation Center* in Genf eingeführt werden<sup>725</sup>. Im Gegensatz zu den Regeln von NSI sollten die Registrierenden detaillierte Informationen über den Server, welchen sie verwenden wollten und eine vollständige Kontaktmöglichkeit angeben. Damit sollte einem Beschwerdeführer die Lokalisierung des Domainnamensinhabers erleichtert werden. Die Anmeldungen der SLDs sollten dann auf einer Webseite veröffentlicht werden, um Markenrechtsinhabern eine Überwachungsmöglichkeit zu bieten. Unter dem schließlich vorgeschlagenen Streitschlichtungsverfahren sollte ein Markenrechtsinhaber direkt nach der Antragsstellung, unabhängig ob die Domain schon zugewiesen wurde oder noch nicht, gegen den Antragsteller vorgehen können. Das gTLD-MoU sagte hierzu aus<sup>726</sup>:

[A] policy shall be implemented that a second-level domain name in any of the CORE gTLDs which is identical to or closely similar to an alphanumeric string that, for purposes of this policy, is deemed to be internationally known, and for which demonstrable intellectual property rights exist, may be held or used only by, or with authorization of, the owner of such demonstrable intellectual property rights. Appropriate consideration shall be given to possible use of such a second-level domain name by a third party that, for purposes of this policy, is deemed to have sufficient rights.

Sobald die Rechtmäßigkeit einer SLD bestritten werden würde, sollten Markenrechtsexperten durch ein *Administrative Challenge Panel* (ACP) über die Rechte der Parteien entscheiden<sup>727</sup>. Die WIPO sollte für die Bereitstellung der ACPs verantwortlich sein und jeder Antragsteller sich verpflichten, an der Streitschlichtung online teilzunehmen. Auf Grund des Scheiterns des gTLD-MoU konnten die ACPs nicht eingeführt werden. Das *Green Paper* und das *White Paper* der US-Regierung griffen jedoch den Vorschlag einer Streitschlichtung unter der Führung der WIPO auf, so daß der Vorschlag des gTLD-MoU die Grundlage der weiteren Entwicklung bildete.

### 3.3.1.2. Streitschlichtung unter Führung der WIPO

Die inzwischen in Zusammenarbeit mit der US-Regierung und der ICANN angelaufene Diskussion bei der WIPO um ein Streitschlichtungsverfahren startete offiziell am 8. Juli 1998 und wurde mit dem Schlußreport vom 30. April 1999 beendet<sup>728</sup>. Hierzu wurden weltweit Anhörungen durchgeführt und verschiedene Experten auf dem Gebiet des Markenrechts konsultiert<sup>729</sup>. Die Vorschläge der WIPO wurden an die DNSO weitergeleitet und dort durch eine

<sup>725</sup> Vgl. ausführlich zum gTLD-MoU Kap. 3.1.2.3.2. Ausführlich zur Dispute Resolution Policy des gTLD-MoU siehe *Albert*, 16 J. Marshall J. Computer & Info. L. 781, 795ff. und *Leaffer*, 6 Ind. J. Global Legal Stud. 139, 154ff.

<sup>726</sup> *gTLD-MoU*, Section 2. - Principles, vgl. Fn. 486.

<sup>727</sup> Diese ACPs sollten sich nach den Substantive Guidelines concerning administrative Domain Name Challenge Panels, vgl. Fn. 500, entwickelt durch das iPOC, richten.

<sup>728</sup> *WIPO*, Final Report. Näheres zum WIPO-Final-Report bei *Bettinger*, CR 1999, 445ff.

<sup>729</sup> Vgl. *Lee*, 7 Rich. J.L. & Tech. 2, 24.

### 3.3. Reform des DNS durch die ICANN

---

Arbeitsgruppe weiteren Änderungen unterzogen<sup>730</sup>. Die DNSO reichte den Report zur Anerkennung an die ICANN weiter<sup>731</sup>. Nach vorläufiger Bestätigung veröffentlichte die ICANN bis zum 13. Oktober 1999 einen ersten Diskussionsentwurf der UDRP. Die entgültige Anerkennung unter Beachtung der öffentlichen Einwürfe erfolgte schließlich am 24. Oktober 1999. In der ersten Entscheidung vom 14. Januar 2000, *World Wrestling Federation Entertainment, Inc. v. Michael Bosman*, wurde auf Übertragung des Domainnamens *worldwrestlingfederation.com* zu Gunsten des Antragsstellers entschieden<sup>732</sup>.

Beim Verfahren der UDRP handelt es sich um ein freiwilliges Schiedsverfahren. Die UDRP wird durch die *Rules for Uniform Domain Name Dispute Resolution Policy* ergänzt, welche das Verfahren für die einzelnen Streitschlichter definiert. Eine Anwendbarkeit ist nur für Streitigkeiten bezüglich Namens- und Kennzeichenrechten vorgesehen. Ein Schiedsverfahren kann jedoch nur zur Anwendung kommen, wenn es zwischen den Streitparteien vereinbart wurde. Inhaber des Domainnamens und der Namens- oder Kennzeicheninhaber stehen jedoch in keinem Vertragsverhältnis zueinander, insbesondere haben sie auch keine Schiedsvereinbarung untereinander geschlossen. Um dennoch zur Anwendbarkeit der UDRP zu kommen, muß zwingend jeder Registrierende mit dem *Registrar*, welcher eine Domain auf den Namen des Registrierenden bei einer *Registry* eintragen läßt, eine Schiedsvereinbarung zu Gunsten Dritter schließen. Beim mit dieser Schiedsklausel vereinbarten Streitschlichtungsverfahren handelt es sich um eine Alternativvereinbarung. Der Inhaber eines Namens- oder Kennzeichenrechts ist nicht verpflichtet, im Rahmen der UDRP seine Rechte einzuklagen, sondern er kann diese weiterhin vor einem nationalen Gericht geltend machen. Nach Art. 4. k. UDRP ist keine der beiden Streitparteien gehindert, zu jedem Zeitpunkt des Schiedsgerichtsverfahrens ein staatliches Gericht anzurufen. Eine klagestattgebende Entscheidung wird von der entsprechenden *Registry* erst nach zehn Tagen umgesetzt, damit dem betroffenen Inhaber des Domainnamens Zeit zur Anrufung eines nationalen Gerichts bleibt. Die Klage setzt schließlich den Vollzug der Schiedsgerichtsentscheidung für die weitere Zeit der Anhängigkeit aus.

Die Streitschlichtung wird von im gegenseitigen Wettbewerb stehenden *Dispute-Resolution Service Providers* vorgenommen, die von der ICANN anerkannt sind. Seit Oktober 1999 sind vier dieser Schiedsgerichte zugelassen worden, das *WIPO Arbitration and Mediation Center*<sup>733</sup>, das *National Arbitration Forum*<sup>734</sup> (NAF), das *CPR Institute for Dispute Resolution*<sup>735</sup>

---

<sup>730</sup> Zum Ablauf der Implementierung der UDRP siehe *ICANN, Timeline for the Formulation and Implementation of the Uniform Domain-Name Dispute-Resolution Policy*, <http://www.icann.org/udrp/udrp-schedule.htm>.

<sup>731</sup> Siehe *DNSO, WG-A Final Report to the ICANN Board*, 4. August 1999, <http://www.dns.org/dns/note/19990804.NCwga-to-ICANN.html>.

<sup>732</sup> World Wrestling Federation Entertainment, Inc. v. Michael Bosman, WIPO Arbitration and Mediation Center, Case No. D99-0001, 14. Januar 2000, <http://arbiter.wipo.int/domains/decisions/html/1999/d1999-0001.html>.

Siehe ausführlich zum Fall *Lee*, 7 Rich. J.L. & Tech. 2, 45ff.

<sup>733</sup> Siehe im Internet unter <http://arbiter.wipo.int>.

<sup>734</sup> Siehe im Internet unter <http://www.arbforum.com>.

<sup>735</sup> Siehe im Internet unter <http://www.cpradr.org>.

(CPR) sowie *eResolution*<sup>736</sup>. Bei den ersten drei Organisationen handelt es sich um etablierte Schiedsgerichte, die schon mehrere Jahre bestehen. Die letztere wurde ausschließlich zur Streitschlichtung bezüglich der Verwendung von Domainnamen im Jahre 1999 gegründet<sup>737</sup>.

Die Entscheidung über die Rechtmäßigkeit der Nutzung eines Domainnamens erfolgt in sogenannten *Panels*. Diese bestehen entweder aus einem oder aus drei Schiedsrichtern. Dies sind häufig Richter, Rechtsanwälte oder Professoren, welche unparteiisch und erfahrenen im Bereich des Markenrechts sein müssen. Bei der WIPO sind zum Beispiel derzeit über 120 dieser Schiedsrichter aus über 30 Ländern anerkannt. Eine Zuweisung der *Panels* erfolgt durch das Schiedsgericht und kann von den Streitparteien nicht beeinflußt werden. In die Zuweisungsentscheidung können jedoch Gesichtspunkte wie Sprache und Nationalität mit einfließen. Bei einem *Panel* aus drei Richtern haben die Parteien jedoch die Möglichkeit jeweils einen Richter selbst auszuwählen. Das Verfahren wird in Art. 4. a. bis k. UDRP durch zwölf Einzelschritte vorgeschrieben und beginnt damit, daß der Beschwerdeführer sich ein Schiedsgericht aussucht und dort die Klage durch Zusendung des Klageschreibens erhebt<sup>738</sup>. Während des ganzen Verfahrens ist es nicht erforderlich, daß eine der Parteien persönlich am Schiedsgericht erscheint, so daß hohe Kosten für die Rechtsverfolgung im Ausland entfallen. Der Streit kann vollständig über das Internet ausgetragen werden. Nach Entscheidung durch das *Panel* kann ein stattgebendes Urteil<sup>739</sup> von der dem Domainnamen zugehörigen *Registry* umgesetzt werden. Dem Verlierer steht unter Aussetzung des Vollzugs schließlich die Möglichkeit eines Verfahrens vor einem nationalen Gericht offen. Eine Entscheidung über die Verletzung von Marken- und Namensrechten wird nach drei in Art. 4. a. UDRP bestimmten Kriterien gefällt, welche in unterschiedlicher Intensität von den Schiedsgerichten umgesetzt werden:

- (i) your domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and
- (ii) you have no rights or legitimate interests in respect of the domain name; and
- (iii) your domain name has been registered and is being used in bad faith.

Die ersten beiden Kriterien der Namens- oder Kennzeichenidentität, sowie fehlender eigenen Rechte am Namen lassen sich relativ leicht klären. Schwierigkeiten bereitet die Auslegung des Kriteriums einer Registrierung und Nutzung in bösem Glauben. Es besteht die Gefahr, daß bei einer zu weiten Definition die individuellen Freiheiten der Namenswahl zu stark eingeschränkt werden. Besonders Privatpersonen und finanzschwache Unternehmen wären dann begüterten Markeninhabern ausgeliefert, obgleich sie nach nationalen Regeln im Recht wä-

<sup>736</sup> Siehe im Internet unter <http://www.eresolution.ca>.

<sup>737</sup> Ausführlich erörtert *Lee*, 7 Rich. J.L. & Tech. 2, 28ff. die Zusammensetzung und Erfahrung in der Streitschlichtung der einzelnen Dispute-Resolution Service Provider.

<sup>738</sup> Zusammenfassend zum Verfahren *Lee*, 7 Rich. J.L. & Tech. 2, 39. Siehe auch *Strömer*, ICANN-Schiedsverfahren.

<sup>739</sup> Die bislang ergangenen Entscheidungen der Schiedsgerichte sind bei der ICANN, Uniform Domain-Name Dispute-Resolution Policy, <http://www.icann.org/udrp/udrp.htm> einsehbar.

### 3.3. Reform des DNS durch die ICANN

---

ren. Zur Klärung dieses Tatbestandsmerkmals soll nach Art. 4. b. UDRP erörtert werden, ob der Domaininhaber den Domainnamen dem Namens-/Markenrechtsinhaber oder Konkurrenten zum Kauf anbietet und, ob die Domain geschäftsschädigend gegenüber dem Beschwerdeführer eingesetzt wird:

- (i) circumstances indicating that you have registered or you have acquired the domain name primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant who is the owner of the trademark or service mark or to a competitor of that complainant, for valuable consideration in excess of your documented out-of-pocket costs directly related to the domain name; or
- (ii) you have registered the domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that you have engaged in a pattern of such conduct; or
- (iii) you have registered the domain name primarily for the purpose of disrupting the business of a competitor; or
- (iv) by using the domain name, you have intentionally attempted to attract, for commercial gain, Internet users to your web site or other on-line location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of your web site or location or of a product or service on your web site or location.

Nach Art. 4. c. UDRP kann sich der Inhaber des Domainnamens auf ein schützenswertes Interesse berufen, soweit er seine Produkte schon vor der Klageerhebung gutgläubig unter dem streitigen Namen angeboten hat, seine Produkte schon vor Klageerhebung unter diesem Namen allgemein bekannt waren oder er den Domainnamen ohne wirtschaftlichen Hintergrund oder Irreführungsabsichten nutzt.

Das Verfahren der UDRP birgt gegenüber einem herkömmlichen Gerichtsverfahren vor einem nationalen Gericht einige gravierende Vorteile<sup>740</sup>. Das Verfahren zeichnet sich besonders durch seine Schnelligkeit aus, da mit einer Verfahrensdauer von circa einem Monat zu rechnen ist. Im staatlichen Verfahren mit mehreren Instanzen kann sich die Dauer schnell auf mehrere Jahre summieren. Die Kosten belaufen sich für das Schiedsgericht auf circa 2.000 DM für eine Entscheidung durch einen Einzelschiedsrichter. Hinzuzurechnen sind die Kosten für den eigenen Anwalt. Vor einem staatlichen Gericht ist in Folge des häufig sehr hohen Streitwertes hingegen mit Kosten über 10.000 DM zu rechnen. Unter der Voraussetzung eines fairen Verfahrens haben auch finanziell schwache Beklagte hiervon einen großen Vorteil, da es ihnen mangels Finanzierung oftmals nicht möglich wäre, sich in einem Prozeß vor einem staatlichen Gericht zu verteidigen. Schließlich lässt sich das Urteil des mit dem Fall betrauten Schiedsgerichtes innerhalb weniger Tage weltweit umsetzen, währenddessen die

---

<sup>740</sup> Zu den Vorteilen wird bei *Hanloser*, JurPC Web-Dok. 158/2000, Abs. 39 und besonders bei *Meyer-Hauser/Zuberbühler*, Domain Name-Streitigkeiten ausführlich Stellung genommen.

Umsetzung eines nationalstaatlichen Urteils auf internationaler Ebene mit Schwierigkeiten verbunden ist.

Diese Vorteile des Verfahrens der UDRP werden jedoch durch einige Nachteile gemindert. So kann im Verfahren nur die Übertragung des Domainnamens gefordert werden. Die Zusprensung eines Schadensersatzes kann nicht gefordert werden. Auch können keine einstweiligen Verfügungen beantragt werden, da das Verfahren an sich schon sehr kurz ist. Auch ist das gesamte Verfahren nur auf Fälle aus dem Bereich des sogenannten *Domain Name Grabbing* anwendbar. Sonstige internetspezifische Konflikte können noch nicht mittels eines von der ICANN anerkannten Verfahrens gelöst werden. Eine Ausdehnung auf andere Bereiche würde erfordern, daß ICANN ihre schon mit der Einführung der UDRP stark beanspruchte Regelungskompetenz überschreitet, um die zur Streitentscheidung notwendigen materiellen Rechtsregeln festzulegen. Schließlich ist das Beweisverfahren auf die Vorlage von Urkunden beschränkt, so daß Zeugen nicht verhört oder Gutachter nicht beauftragt werden können.

Ein weiterer Hauptkritikpunkt ist die Möglichkeit eines Forum Shoppings aus der Bestimmung heraus, daß im Gegensatz zum herkömmlichen Schiedsverfahren nur der Beschwerdeführer das zuständige Schiedsgericht auswählen kann. Dem Verklagten bleibt eine Duldungspflicht übrig. Schaut man sich die Statistiken der einzelnen *Dispute-Resolution Service Provider* vom Juni 2001 an<sup>741</sup> (siehe Tabelle 5 unten), so ist zu erkennen, daß die Marktführer WIPO und NAF die meisten Entscheidungen zu Gunsten der Antragsteller entschieden haben. Während das unparteiischere Institut *eResolution*, ein Konsortium von kanadischen und US-amerikanischen Rechtsprofessoren, nur bei 64% zu Gunsten der Antragsteller entschied<sup>742</sup>. Diese Diskrepanz ist unter dem Blickwinkel einer gleichen rechtlichen Entscheidungsgrundlage für alle Schiedsgerichte der UDRP zunächst verwunderlich. Das vage formulierte dritte Entscheidungskriterium der bösgläubigen Nutzung läßt jedoch einen großen Auslegungsspielraum zu. Besonders finanzschwache Domaininhaber haben es hier schwer, ihren legitimen Verwendungsanspruch zu begründen. Zusätzlich ist umstritten, inwieweit alle drei Entscheidungskriterien voll erfüllt sein müssen. Während die WIPO und die NAF auch Entscheidungen basierend auf der alleinigen Existenz eines Markenrechts des Antragsstellers fällen<sup>743</sup>, bestätigen die Richter von *eResolution* Ansprüche nur bei der Erfüllung aller drei Entscheidungskriterien<sup>744</sup>. Die Schiedsgerichte können so ihre eigenen Vorstellungen von den Tatbestandsmerkmalen entwickeln und somit auf ihre Statistik Einfluß nehmen. Die Anspruchstel-

---

<sup>741</sup> Siehe WIPO, Case Results: gTLDs, <http://arbiter.wipo.int/domains/statistics/results.html>; NAF, Forum Domain Dispute Case Search <http://www.arbforum.com/domains/domain-decisions.asp>; CPR, Dispute Resolution for Internet Domain Names, [http://www.cpradr.org/ICANN\\_Cases.htm](http://www.cpradr.org/ICANN_Cases.htm) und *eResolution*, Domain Name Administrative Decisions, <http://www.eresolution.ca/services/dnd/decisions.htm>. Siehe auch die tagesaktuelle Gesamtstatistik der ICANN, Summary of Status of Proceedings, <http://www.icann.org/udrp/proceedings>.

<sup>742</sup> Vgl. auch die umfassende Studie zur Verteilung der Entscheidungen bei den einzelnen Schiedsgerichten von Mueller, Rough Justice, Kap. 3. Outcomes, Who wins and who loses?

<sup>743</sup> Dies widerspricht den herkömmlichen Rechtsregeln. Z.B. ist nach § 14 MarkenG nur eine Nutzung im geschäftlichen Verkehr untersagt. Damit bleibt es möglich, den Markennamen für Kritik oder für Sympathiebekundungen (z.B. als Fansite) zu verwenden.

<sup>744</sup> Vgl. King, Telepolis 8694.

### 3.3. Reform des DNS durch die ICANN

ler werden schließlich das Schiedsgericht mit der höchsten Erfolgsrate wählen und die meisten Fälle werden bei den derzeitigen Marktführern anhängig<sup>745</sup>. Das aktuelle System der UDRP führt damit zu einer Voreingenommenheit der Schiedsgerichte gegen die ursprünglichen Domaininhaber und Klagegegner.

Tabelle 5 – Verhältnis der Stattgaben zu Abweisungen.

	Entschiedene Fälle	Davon Stattgabe zu Gunsten Antragsteller	Davon Abweisung zu Gunsten Inhaber	Verhältnis Stattgabe/ Abweisung
WIPO	2009	1284	299	81 % – 19 %
NAF	1221	818	171	83 % – 17 %
CPR	22	12	8	60 % – 40 %
eResolution	216	121	69	64 % – 36 %
Gesamt	3468	2235	547	80 % – 20 %

Mit den wenigen Bestimmungen der UDRP hat die ICANN in Zusammenarbeit mit der WIPO eine rechtliche Regelung in einem zwar sehr begrenzten Anwendungsbereich jedoch mit weitreichender Wirkung auf internationaler Basis geschaffen. Auch wenn nationale Rechtsgedanken mit in die Regeln eingeflossen sind, so handelt es sich um eigenständige Normen über Ansprüche auf einen Domännamen und das entsprechende Prozeßrecht zur Durchsetzung und Verteidigung dieser Ansprüche. Auf Grund der genannten Schwierigkeit eine „Berufung“ gegen das Schiedsurteil vor einem nationalen Gericht über Ländergrenzen hinweg zu führen, entfaltet die UDRP eine Bindungswirkung an alle Parteien. Diese Bindungswirkung besteht auf globaler Ebene, unabhängig, wo die Domain registriert wurde und wo der Registrierende oder der Namensrechtsinhaber seinen Wohnsitz hat. Es handelt sich somit bei der UDRP um einen neuen Corpus internationalen Markenrechts. Dieser ihr innenliegenden Bedeutung wird die UDRP aus rechtsstaatlichen Erwägungen zum Teil nicht gerecht, da die ICANN und die WIPO nicht ausreichend von den Betroffenen legitimiert wurden. Ebenso benötigen die Schiedsrichter eine Art Legitimation, um den Entscheidungsprozeß zu führen. Zur Zeit existiert kein Mechanismus, in welchem die Betroffenen Einfluß auf die Auswahl der Schiedsrichter durch die *Dispute-Resolution Service Provider* nehmen können. Es besteht auch nicht die Möglichkeit, die Schiedsrichter zu evaluieren und diejenigen aus der Auswahlliste zu entfernen, die aus dem Blickwinkel der Öffentlichkeit ihre Entscheidungsbefugnis mißbraucht haben. Sicherlich wiegen die erwähnten Vorteile eines online stattfindenden Schiedsverfahrens die genannten Nachteile und Einwendungen auf. Ein entspanntes Zurücklehnen ist jedoch nicht gerechtfertigt, da es sich bei der UDRP erst um den Anfang einer neuen Variante der Rechtssetzung handelt und sicherlich auch als Vorlage zur außerstaatlichen Regelung weiterer, diesmal komplexerer und relevanterer Rechtsgebiete, dienen wird.

<sup>745</sup> Mueller, Milton stellt in seine Studie einen starken Rückgang des Marktanteils während des Untersuchungszeitraumes fest: *Mueller, Rough Justice*, Kap. 4. Forum Shopping and Bias, Variations in market share and what explains it.

Im Rahmen des Streitschlichtungsverfahrens der UDRP stehen einige Erweiterungen an. Zum einen wird überlegt, die UDRP auf eine Vielzahl weiterer Bezeichnungen auszudehnen und andererseits Regelungen für Streitigkeiten unter den ccTLDs zu schaffen.

Zunächst hat die WIPO einen erneuten Diskussionsprozeß in Gang gebracht<sup>746</sup>, dessen Ergebnis Regeln zum Schutz von geographischen Namen, Unternehmenskennzeichen, Namen berühmter Persönlichkeiten, Namen von internationalen zwischenstaatlichen Organisationen und von pharmazeutischen Begriffen sein sollen<sup>747</sup>. Diese Regeln finden zum Teil keine Parallelen in den nationalen Rechtsordnungen. Wie die Regelungen zu den Personennamen und den Unternehmenskennzeichen aussehen sollen, ist derzeit noch umstritten. Es ist auf Grund der vielen Namensdoppelgänger kaum möglich, persönliche Namen im Internet zu schützen. Allerdings sollen zum Beispiel Politiker und berühmte Künstler vor Verletzung ihrer Persönlichkeitsrechte besser bewahrt werden. Die Schaffung allgemeingültiger Regelungen bezüglich Unternehmenskennzeichen erweist sich, auf Grund der sehr differenzierten rechtlichen Behandlung dieser in den einzelnen Staaten, als sehr schwierig. Aus der Sicht der WIPO scheint der Schutz von Namen pharmazeutischer Wirkstoffe wichtig zu sein, welche bei der *World Health Organization* (WHO) verzeichnet sind<sup>748</sup>. Da diese Namen der eigennützigen Verwertung durch Pharmazieunternehmen entzogen sind, sollen sie auch nicht als Domannamen registrierbar sein. Auch die Namen und Abkürzungen internationaler Organisationen sollen einen besonderen Schutz unter allen ccTLDs erhalten. Obgleich eine Registrierung unter der TLD .int für ausreichend erscheint, soll für diese Namen ein Freihaltebedürfnis unter allen ccTLDs bestehen. Schließlich erwägt man, Bestimmungen für die Whois-Datenbanken einzuführen, um eine leichtere Recherche zu ermöglichen und eine eindeutig bestimmbarer Kontaktperson für jede registrierte Domain zu haben. Ein Verstoß gegen das Europäische Datenschutzrecht ist allerdings bei einer öffentlich zugänglichen Whois-Datenbank unausweichlich. Als Ergebnis der inzwischen stattgefundenen letzten Konsultationsrunde zu den Vorschlägen der WIPO wurde der Öffentlichkeit am 3. September 2001 der zweite *Final Report* repräsentiert<sup>749</sup>. In diesem werden die genannten Vorschläge bestätigt und das weitere Verfahren zur Umsetzung dieser näher ausgeführt.

Zusätzlich zum Schutz weiterer Bezeichnungen versucht die WIPO ihren Einfluß auf die ccTLDs auszudehnen. Die WIPO hat ein *Best Practice*-Dokument entworfen<sup>750</sup>, um für alle

---

<sup>746</sup> Siehe *WIPO*, Second WIPO Internet Domain Name Process, <http://wipo2.wipo.int/process2/index.html>.

<sup>747</sup> Siehe *WIPO*, Interim Report - Second Process. Vgl. auch zu den Vorschlägen der WIPO: *Heise-Newsticker*, WIPO will strikteren Namenschutz im Web, 18. April 2001.

<sup>748</sup> Hierbei handelt es sich um die sogenannten International Nonproprietary Names, wovon ca. 8.000 Namen bei der WHO registriert sind, siehe *WHO*, International Nonproprietary Names, <http://www.who.int/medicines/organization/qsm/activities/qualityassurance/inn/innguide.shtml>.

<sup>749</sup> Report of the Second WIPO Internet Domain Name Process, <http://wipo2.wipo.int/process2/report/index.html>.

<sup>750</sup> Siehe *WIPO*, ccTLD Best Practices for the Prevention and Resolution of Intellectual Property Disputes, 20. Juni 2001, <http://ecommerce.wipo.int/domains/cctlds/bestpractices/bestpractices.html>. Vgl. auch zu den Vorschlägen: *Heise-Newsticker*, WIPO schlägt Schlichtungsstellen für Länder-Domains vor, 4. März 2001.

### 3.3. Reform des DNS durch die ICANN

---

ccTLDs einen weltweiten Mindeststandard für Domainregistrierung und Whois-Datenbanken zu schaffen. Die Organisation selbst bietet zusätzlich ihr *WIPO Arbitration and Mediation Center* als neutrale Schiedsstelle für Domainstreitigkeiten unter ccTLDs an. Da diesen Service zur Zeit nur über 20 vorrangig kleine ccTLDs anwenden, fordert die WIPO einheitliche Regelungen, nach denen sich jeder Nutzer eines Domainnamens gleichzeitig einem Schiedsverfahren unterwerfen solle und zudem versichern müsse, nicht bösgläubig mit der Registrierung fremde Markenrechte zu verletzen. Einheitliche Regelungen berauben jedoch den ccTLDs ihrer Diversifizierungsmöglichkeiten. Hinzu kommt, daß die Vergabepraxis der ccTLDs häufig an die nationalen Regelungen angepaßt wurde und diese sich stark voneinander unterscheiden. Darüber hinaus ist die Notwendigkeit zum Schutz von Markennamen über Ländergrenzen hinweg auch in den ccTLDs sehr fragwürdig, wenn die streitige Marke in den betroffenen Ländern selbst nicht eingetragen wurde.

In vielen ccTLDs wurden in den letzten Jahren eigene Verfahren zur Lösung von Streitigkeiten um Domainnamen eingeführt. Zum Beispiel besitzen die ccTLDs .uk (Großbritannien) und .dk (Dänemark) eigene sogenannte *Local Dispute Resolution Policy* (LDRP)<sup>751</sup>. Das DENIC hingegen setzt streitige Domains in einen Disput-Status<sup>752</sup>, der den Transfer von umstrittenen Domains auf dritte Personen während der Anhängigkeit von Rechtsstreiten blockieren soll. Eine LDRP hingegen wird in Deutschland für nicht notwendig befunden, da sich inzwischen eine gefestigte Rechtsprechung zum *Domain Grabbing* herausgebildet hat und entsprechend die Verfahrensdauer vor den deutschen Gerichten recht kurz ist. Durch die inzwischen erfolgte Etablierung des DNS hat in letzter Zeit die Bedeutung dieser Rechtsstreite stark abgenommen. Dies zeigt auch die inzwischen recht geringe Diskussionsbereitschaft der Internetgemeinschaft an der zweiten Diskussionsrunde der WIPO<sup>753</sup>.

#### 3.3.2. Einführung neuer TLDs

Ein weiterer wichtiger Punkt zur Reform des DNS stellt die Einführung neuer TLDs dar. Zu unterscheiden ist dabei zwischen der Zuweisung neuer ccTLDs und der Einführung länderübergreifender gTLDs. Zwischen den ccTLDs und den gTLDs ist die neue TLD .eu für Europa einzuordnen, deren Einführung bislang durch die bürokratischen Hürden der Europäischen Union blockiert wird.

##### 3.3.2.1. Neue ccTLDs

Am umstrittensten ist bislang die Einführung von neuen ccTLDs für Länder und Regionen gewesen, da sie den Länder- und Regionsabkürzungen der ISO-Norm 3166 entsprachen (sie-

---

<sup>751</sup> Der Verwalter *Nominet* für die britische ccTLD .uk bietet einen freien Dispute Resolution Service unter <http://www.nominet.org.uk/ref/drs.html> an. Für die dänische ccTLD .dk wird durch das *Dansk Internet Forum* ein Entscheidungsgremium in Fragen der Rechtmäßigkeit von Domainnamen angeboten, <http://www.difo.dk>.

<sup>752</sup> Vgl. *DENIC eG*, DENIC-Registrierungsbedingungen, § 2 (3), 15. August 2000, <http://www.denic.de/doc/DENIC/agb.html> und die FAQ der *DENIC eG*, Kap. Was kann die DENIC unterdessen für mich tun? und ff. Kap., 21. Mai 2001, <http://www.denic.de/doc/recht/faq/ansprueche.html>.

<sup>753</sup> Siehe *WIPO*, Second WIPO Internet Domain Name Process, Fn. 746.

he Kapitel 2.2.2.2 oben). So wurde im März 2000 von der ICANN die Zulassung der TLD .ps für die Region Palästina beschlossen<sup>754</sup>. Zusätzlich ergab sich aus der Knappheit der noch unter den gTLDs verfügbaren Domainnamen, eine Reihe von Versuchen, ccTLDs unter einer generischen Bedeutung zu vermarkten. Das bekannteste Beispiel stellt die ccTLD .tv dar, welche dem Inselstaat Tuvalu zugewiesen ist. Das private Unternehmen .tv Corporation<sup>755</sup> vermarktet seit April 2000 im Auftrag des Inselstaates deren ccTLD an Fernsehsender, Filmproduzenten oder Fernsehgerätehersteller. In den ersten Monaten konnte das Unternehmen über 250.000 Domains vermarkten, die von 50 US\$ bis eine halbe Million US\$ kosteten und stellt damit die Hauptfinanzquelle für den Inselstaat dar. Diesem Beispiel versuchen weitere Kleinstaaten nachzueifern, wie zum Beispiel die pazifischen Inselstaaten Tonga mit der ccTLD .to und Niue mit .nu sowie in Asien Turkmenistan mit .tm und Laos mit .la.

### 3.3.2.2. Neue gTLDs

Das *White Paper* der US-Regierung sah die Einführung neuer länderunabhängiger gTLDs vor. Da frühere Versuche bislang am Widerstand verschiedener Interessensgruppen gescheitert waren, mußte die ICANN nun einen Weg finden, um im Konsens aller, diese neuen TLDs zu ermöglichen. Inzwischen war es auf breiter Ebene anerkannt, daß man eine Erweiterung des DNS-Namensraumes benötigte, da zum einen die verfügbaren Namen besonders unter .com und .net knapp geworden waren und zum anderen man einen freien Wettbewerb innerhalb des DNS ermöglichen wollte. Mit der Einführung der UDRP konnten auch die Bedenken der Markenrechtslobby zum größten Teil beseitigt werden, welche bislang aus Angst vor einer Explosion der Markenrechtsstreitigkeiten um Domainnamen jegliche Einführung weiterer TLDs abgelehnt hatte. Strittig blieb, wieviele gTLDs zunächst eingeführt und mittels welchen Verfahrens die neuen gTLDs ausgewählt werden sollten. Wichtige Entscheidungskriterien waren, daß bei der Einführung der neuen gTLDs die Stabilität des Internets gewährleistet bleibt und die neuen gTLDs über das ganze Internet hinweg erreichbar sind. Um zunächst bei der Erweiterung des DNS Erfahrungen zu sammeln, empfahl der *Names Council* der DNSO im April 2000 die Einführung einer geringen Anzahl an TLDs<sup>756</sup>. Darüber hinaus mußte geklärt werden, inwieweit man thematisch beschränkte Domains, sogenannte *chartered* TLDs, einführen solle. *Chartered* TLDs brächten das Problem mit, daß in Grenzfällen eine Organisation benötigt wird, die zu entscheiden hätte, ob ein beantragter Domainnamen unter der gewählten TLD registriert werden darf. Themenbeschränkte TLDs hätten allerdings den Vorteil, daß der Nutzer anhand des Namens eines WWW-Angebotes einen gewissen Inhalt der Homepage erwarten könne.

Bis zum 3. Oktober 2000 konnten sich nun verschiedene Interessenten bei der ICANN bewerben, welche als *Registry* für eine von sieben neuen TLDs fungieren wollten. Eine gleich-

---

<sup>754</sup> Siehe IANA, IANA Report on Request for Delegation of the .ps Top-Level Domain, 22. März 2000, <http://www.icann.org/general/ps-report-22mar00.htm>.

<sup>755</sup> Siehe The .tv Corporation, <http://www.tv>. Vgl. auch *Heise-Newsticker*, Länder-Domain .tv kostete 50 Millionen US-Dollar, 9. April 2000.

<sup>756</sup> Siehe ICANN, Consideration of Introducing New Generic Top-Level Domains, 20. April 2000, <http://www.icann.org/dnsorgtld-topic-20apr00.htm>.

### 3.3. Reform des DNS durch die ICANN

zeitige Bewerbung für mehrere TLDs war nicht ausgeschlossen worden. Obgleich die ICANN eine Bewerbungsgebühr von 50.000 US\$ vorgeschrieben hatte, um das Evaluationsverfahren finanzieren zu können, waren 44 gültige Bewerbungen eingegangen. Ab 13. Oktober wurde es der Öffentlichkeit ermöglicht, die eingereichten Vorschläge zu diskutieren. Über 4.000 Emails generierte die anschließende öffentliche Diskussion. Als Entscheidungsgrundlage für das ICANN-Direktorium wurde am 10. November 2000 ein vorläufiger Bericht über die eingegangenen Bewerbungen veröffentlicht<sup>757</sup>. Die TLD-Anträge wurden in diesem Bericht vorrangig nach technischen und finanziellen Aspekten untersucht. Insbesondere gingen die technische Erfahrungen der Antragsteller, die Zweckmäßigkeit des Geschäftsplanes oder die zur Verfügung stehenden Ressourcen in die Bewertung ein. Am 16. November 2000 entschied schließlich das ICANN-Direktorium, welche der beantragten TLDs in der ersten Phase eingeführt werden (siehe Tabelle 6 unten)<sup>758</sup>.

Tabelle 6 – Neue *Top Level Domains*.

Top Level Domain	Zielnutzergruppe	Zugangsbeschränkt
.biz	Geschäftliche Nutzung	Nein
.info	Informationsdienste	Nein
.name	Individuen	Nein
.coop	Genossenschaftliche Unternehmen	Ja
.pro	Berufsgruppen (Professionals)	Ja
.aero	Flugverkehr	Ja
.museum	Museen	Ja

Die Ausgestaltung der ausgewählten TLDs wird sich in einigen relevanten Punkten unterscheiden. Zunächst ist zwischen den offenen und den zugangsbeschränkten TLDs zu unterscheiden. Zum Beispiel wird die TLD .coop nur für genossenschaftlich organisierte und betriebene Unternehmen und Organisationen zugänglich sein, währenddessen unter der TLD .aero nur Angebote aus dem Bereich des Luftverkehrs entstehen sollen. Weiterhin kann zwischen strukturierten und unstrukturierten TLDs differenziert werden. Unter den TLDs .biz und .info wird eine Registrierung direkt als Second Level Domain möglich sein, während unter der TLD .name die Domain nach dem Prinzip Vorname.Nachname.name organisiert werden und der Kunde nur den Vornamen als *Third Level Domain* registrieren kann. Auch in der beschränkten TLD .pro soll keine direkte Registrierung als SLD möglich sein, sondern eine Spezifizierung nach Berufsgruppen erfolgen (zum Beispiel für Mediziner unter .med.pro und für Juristen unter .law.pro). Bei den TLDs ließen sich zudem verschiedene *Registrar-Registry*-Modelle feststellen. Während die meisten TLDs allen *Registrars* offen stehen und

<sup>757</sup> Siehe ICANN, Report on New TLD Applications, 9. November 2000, <http://www.icann.org/tlds/report/>. Zusammenfassend zum Bericht siehe auch *Heise-Newsticker*, ICANN-Bericht: Keine Chance für Sex- und Kids-Domain, 10. November 2000.

<sup>758</sup> Siehe mit weiteren Hintergrundinformationen zu den neuen TLDs: *ICANN Channel*, Domains, <http://www.icannchannel.de/tlds/>.

die Gewinne der *Registry* zum Teil an die *Registrars* verteilen, will zunächst der Betreiber der TLD .coop keine weiteren *Registrars* zulassen. Außerdem können die TLDs daraufhin unterschieden werden, ob sie für Markenrechtsinhaber gewisse Schutzmechanismen anbieten.

Das Auswahlverfahren des ICANN-Direktoriums mußte sich jedoch herber Kritik aussetzen. Schon die Vorentscheidung, sich auf sieben neue TLDs zu begrenzen, führte dazu, daß man auch sehr gute Vorschläge rigoros aus der Vorschlagsliste herausstreichen mußte. Für viele wurde die kurze Vorstellungszeit während der ICANN-Jahrestagung in Los Angeles zum Verhängnis. Zwar hatte man sich sechs Stunden Zeit genommen, um die Bewerber einzeln anhören zu können, jedoch entfielen effektiv ganze drei Minuten auf jeden Bewerber, um sein Projekt zu erläutern. Es ist kaum möglich, in einem derart kurzen Zeitraum, eine komplexe Geschäftsidee darzulegen<sup>759</sup>. Die Bewerber konnten eventuelle durch die Beurteilung entstandene Mißverständnisse beim ICANN-Vorstand nicht ausräumen. Die eigentlichen Entscheidungsgründe seitens des Direktoriums blieben im Verborgenen<sup>760</sup>. In den Begründungen, warum einzelne Vorschläge abgewiesen wurden, ließ sich kaum eine rationale Entscheidungsstruktur erkennen<sup>761</sup>. Für viele Bewerber war es unverständlich, warum gerade sie abgewiesen wurden<sup>762</sup>. Darüber hinaus kann man die Auswahl als nicht besonders geglückt ansehen, denn die TLDs .coop, .aero oder .museum sind in der Anfangsphase der Einführung neuer TLDs zu speziell ausgerichtet, um für den größten Teil der Internetnutzer von Vorteil zu sein. Durch die Zugangsbeschränkung werden sie nur wenigen tausend Interessenden zur Verfügung stehen und damit kaum zur Entlastung der überfüllten TLDs .com und .net führen<sup>763</sup>.

Die intensive Kritik durch die Verlierer führte zwar zu einer Anhörung im Januar 2001 vor der EU-Kommission<sup>764</sup> und im Februar 2001 vor dem US-Kongreß<sup>765</sup>, aber die Einführung der neuen TLDs konnte dadurch bislang jedoch nicht gestoppt werden. Die von einem Teil der Verlierer angestrebte Annulierung der Wahl würde der Einführung neuer TLDs kontraproduktiv entgegenstehen, da der ganze Prozeß erneut verzögert würde. Bei einer erneut entfachten Diskussion wäre mit einer neuen Entscheidung erst in mehreren Jahren zu rechnen.

---

<sup>759</sup> Zum Auswahlverfahren siehe *Heise-Newsticker*, ICANN: Hitzige Diskussionen über neue Domain-Namen, 16. November 2000.

<sup>760</sup> Vgl. *Heise-Newsticker*, Hintergrund: Der Ärger mit den Domain-Namen, 19. November 2000.

<sup>761</sup> So meinte Vint Cerf mit Blick auf den alternativen Root Server, welchen Chris Amblers seit 1996 mittels Image Online Design, Inc. unter .web betreibt: „Ich würde mich doch wohler fühlen, wenn wir .web nicht vergeben“, zitiert in *Heise-Newsticker*, Sieben neue Top Level Domains beschlossen, 17. November 2000. Siehe zum Auswahlverfahren auch *Ermert*, c’t 2000, Heft 25, S. 66ff.

<sup>762</sup> Die Firma Image Online Design, Inc. (vgl. Fn. 761) legte in einer Beschwerde vor dem Reconsideration Committee ausführlich dar, daß man bei ihr, trotz ähnlichem Geschäftsmodell, vergleichsweise höhere Ansprüche gestellt habe, als bei einigen Mitbewerbern: IOD’s Request for Reconsideration with ICANN, 16. Dezember 2000, <https://www.webtld.com/News/2000-12-16.asp>.

<sup>763</sup> Siehe auch *Byfield*, Telepolis 4402 mit einer ausführlichen Darstellung des Presseechos auf die Wahl der TLDs durch die ICANN.

<sup>764</sup> Siehe *Heise-Newsticker*, Neue Top Level Domains - die EU will genau wissen, 3. Dezember 2000.

<sup>765</sup> Siehe *The House Committee On Energy and Commerce*, Is ICANN’s New Generation of Internet Domain Name Selection Process Thwarting Competition?, 8. Februar 2001, <http://www.house.gov/commerce/hearings/telecom02082001.htm>.

### 3.3. Reform des DNS durch die ICANN

---

Die jetzige Debatte kann vielmehr dazu dienen, für die Zukunft einen fairen, transparenten Prozeß zu entwickeln.

Am 15. Mai 2001 wurden durch die ICANN die ersten Verträge mit NeuLevel<sup>766</sup> für die TLD .biz und mit Afilias<sup>767</sup> für die TLD .info geschlossen<sup>768</sup>. Mit diesen Verträgen erhalten die TLD-Betreiber jedoch nicht das Recht, völlig eigenständig *Registries* zu betreiben, sondern bleiben an die Politik der ICANN gebunden. Insbesondere sieht Art. 4.1.1. eine Bindung an die konsensualen Entscheidungen der ICANN vor. Mit dieser Klausel wird erneut die schon erörterte Bedeutung (siehe Kapitel 3.2.3.1 oben) einer Entscheidung auf Basis eines Konsenses für die ICANN und deren Anerkennung durch die betroffenen Internetnutzer deutlich<sup>769</sup>.

Die Registrierung von Domainnamen konnte, wie bei den schon bestehenden gTLDs, über die von ICANN akkreditierten *Registrars* vorgenommen werden. Die Registrierung von Domainnamen unter der TLD .info hat am 25. Juli 2001 bis zum 27. August 2001 mit sogenannten *Sunrise Period* begonnen<sup>770</sup>. In diesem einmonatigen Zeitraum stand Markenrechtsinhabern die Möglichkeit offen, sich für TLD .info bevorzugt vor Normalverbrauchern zu bewerben. In den darauffolgenden Tagen konnten sich, mittels eines eigens für Afilias von der WIPO eingerichteten Verfahren, die Markenrechtsinhaber noch einmal um die schon zugewiesenen Domainnamen streiten. Dieses Verfahren kostete für jede Seite 295 US\$. Dem ursprünglichen Inhaber wurde die Gebühr jedoch bei einem Obsiegen zurückerstattet. Ab dem 12. September 2001 war es schließlich für jegliche Interessenten möglich, bei Afilias einen Domainnamen auf Basis des bewährten Prinzips „first come, first served“ im voraus zu registrieren<sup>771</sup>, bevor zum 1. Oktober 2001 das vollständig freie Registrierungsverfahren eröffnet wurde<sup>772</sup>. Bei der TLD .biz konnten Markeninhaber vom 21. Mai bis 6. August 2001 gegen eine Gebühr von 90 US\$ eine Blockierung von Domainnamen mittels einer eigens dafür eingerichteten Datenbank vornehmen. Ab 25. Juni konnten Domainnamen direkt bei .biz beantragt werden, bevor zum 7. November 2001 eine Aktivierung und Onlineschaltung der Domainnamen erfolgen sollte<sup>773</sup>. Die beiden TLDs .info und .biz wurden nach der Zustimmung des US-DoC am 27. Juni 2001 in den *A Root Server* eingetragen und waren damit für das DNS freigeschaltet<sup>774</sup>. Seit 16. Januar 2002 ist auch die TLD .name im Internet erreichbar<sup>775</sup>.

---

<sup>766</sup> Siehe *NeuLevel, Inc.*, <http://www.neulevel.com> bzw. <http://www.neulevel.biz>.

<sup>767</sup> Siehe *AfiliasLtd.*, <http://www.afilias.com> bzw. <http://www.afilias.info>.

<sup>768</sup> Siehe *ICANN-Announcement*, ICANN Accredits New Top-Level Domains—.biz and .info Registration Process To Begin This Summer, 15. Mai 2001. Die Verträge mit einer Vielzahl von Anhängen befinden sich unter *ICANN*, New TLD Program, <http://www.icann.org/tlds/>.

<sup>769</sup> Vgl. *ICANN*, Proposed Unsponsored TLD Agreement, 11. Mai 2001,

<http://www.icann.org/tlds/agreements/unsponsored/registry-agmt-11may01.htm>.

<sup>770</sup> *Afilias*, Afilias Announces Sunrise Period, 25. Juli 2001.

<sup>771</sup> *Afilias*, Afilias Opens .INFO Registrations to General Public, 12. September 2001.

<sup>772</sup> *Afilias*, Afilias Announces Opening Day, 1. Oktober 2001.

<sup>773</sup> Siehe *Neulevel*, .bis goes live, 7. November 2001.

<sup>774</sup> *ICANN-Announcement*, Two New Top-Level Domains for the Internet: .biz and .info to be Activated Tomorrow, 26. Juni 2001.

<sup>775</sup> Siehe Heise-Newsticker, Neue Domain .name im Netz, 16. Januar 2002.

Im Rückblick auf die Auswahl der neuen TLDs muß man jedoch an ICANN die Frage stellen, warum sie sich von vornherein auf nur sieben TLDs beschränkt hat. ICANN begründete die Begrenzung auf zunächst sieben TLDs mit der fehlenden Erfahrung, die sie bei der Einführung neuer TLDs habe. Es gelte primär die Sicherheit und Stabilität des *Root Server Systems* zu gewährleisten. Aus technischer Sicht bestehen jedoch keinerlei Einschränkungen bei einer Erweiterung des obersten Namensraumes des DNS. Wie Tests ergeben haben, könnten Millionen neuer TLDs auf einmal eingeführt werden, ohne daß es zu technischen Komplikationen käme<sup>776</sup>. Eine Zulassung des größten Teils der 44 gültigen Bewerbungen hätte somit kaum zu einer Gefährdung des technischen Betriebes des DNS und damit des Internets geführt. Insbesondere sind im *Root Server System* mehrere hundert ccTLDs eingetragen, deren Freischaltung in den letzten Jahren ebenfalls nicht zu technischen Problemen geführt hat. ICANN hätte sich nicht schon vor Beginn des Bewerbungsverfahrens die neuen TLDs auf maximal sieben beschränken dürfen, sondern klar feststehende objektive Kriterien für die *Registries* verabschieden sollen. Damit hätte sie alle TLDs zulassen können, welche die festgelegten Kriterien erfüllt hätten. Diese Kriterien hätten aus einer Definition der technischen und finanziellen Ausstattung und den Maßstäben für Offenheit und Transparenz bestehen können. Anstatt nach undurchsichtigen Gesichtspunkten die Liste der Anträge zusammenzustreichen, wäre eine nachzuvollziehende Entscheidung möglich gewesen. Damit wäre nicht nur die Reputation der ICANN gesichert gewesen, sondern auch der Einführung eines freien Wettbewerbs genüge getan.

Jede Begrenzung des DNS bewirkt, daß an der gesamten Vergabe von Domainnamen weniger Unternehmen teilhaben können. Auf diese Weise wird künstlich der Wettbewerb eingeschränkt. Besonders plausibel wird dies bei einer Betrachtung der die *Registries* betreibenden Unternehmen. Mit dem derzeitig bestehenden System wird jede *Registry* von nur einem Unternehmen betrieben. Weitere Firmen sind folglich gehindert, in einen Preis- und Servicewettbewerb zu den bestehenden *Registry*-Betreibern zu treten<sup>777</sup>. Zum Beispiel stellt bei einem Preis von circa zehn US\$ für einen Domainnamen unter der gTLD .com, die von der NSI verlangte Jahresgebühr von 6 US\$ den hauptsächlichsten Anteil für den Registrierungspreis dar. Erst die Einführung einer Vielzahl neuer TLDs kann zu einem Zwang führen, diese Jahresgebühr abzusenken. Die von ICANN beschlossenen TLDs sind jedoch nur bedingt ausreichend, um einen Preiswettbewerb gegenüber der NSI in Gang zu setzen. Erstens stellen sie nur eine begrenzte Anzahl von TLDs dar. Zweitens sind sie zum Teil nur einem ausgewählten Personenkreis zugänglich. Drittens sehen die meisten neuen TLDs Beschränkungen des Anwendungsbereiches vor und verlangen teilweise eine Registrierung unterhalb der SLD. Unter einer Vielzahl von neuen TLDs würde auch der Markt der *Registrars* weiterem Wettbewerb ausgesetzt, da mit neuen TLDs eine weitere Diversifizierung im Endkundengeschäft der *Registrars* möglich ist. Schließlich wäre von neuen TLDs der Sekundärmarkt von Domainnamen

---

<sup>776</sup> Vgl. unter anderem Auerbach, Karl, Email an DNSO-WG, [wg-c] Initial Numbers, 15. Dezember 1999, <http://www.dns.org/wgroups/wg-c/Arc01/msg00195.html>.

<sup>777</sup> Vgl. Froomkin, Thwarting Competition, Kap. The Three Relevant Markets, (1) The market for registry services.

### 3.3. Reform des DNS durch die ICANN

---

betroffen, auf welchem momentan durch die *Domain Grabber* hohe Preise bei der Weiterveräußerung von Domainnamen erzielt werden<sup>778</sup>. Durch die dann bestehende Ausweichmöglichkeit auf andere TLDs wäre den *Domain Grabbern* die Geschäftsgrundlage weitestgehend entzogen.

#### 3.3.2.3. Eine TLD für Europa

Nicht so zügig wie die Schaffung neuer gTLDs geht die Errichtung der geplanten TLD .eu für den europäischen Raum voran. Die TLD .eu soll eine Alternative zu den ccTLDs der einzelnen Mitgliedsstaaten der *Europäischen Union* anbieten und den elektronischen Geschäftsverkehr in Europa weiter ankurbeln<sup>779</sup>. Insbesondere soll eine europäische TLD im Einklang mit den Art. 154 und 155 EGV die Interoperabilität sogenannter Transeuropäischer Netze stärken. Obgleich die Einführung einer .eu TLD seit 1999 von der europäischen Wirtschaft gefordert wurde, wird die Umsetzung bislang durch bürokratische Hürden in der EU-Verwaltung gebremst, die das gesamte Projekt in Frage stellen könnten. Der EU-Ministerrat stimmte einer Einführung der TLD .eu erst am 27. Juni 2001 zu<sup>780</sup>. Am 7. November 2001 erließ der *Rat der Europäischen Union* nach Anhörung des *Europäischen Parlaments* (nach Art. 251 EGV) eine Verordnung zur Einführung von .eu<sup>781</sup>. Umstritten war vor allem, inwieweit die TLD für Europa unter politischer Kontrolle stehen solle. Während die EU-Kommission eine starke Selbstregulierung der *Registry* vorsah, wurde im Rat dagegen die Meinung vertreten, daß eine Kontrolle durch ein spezielles Aufsichtsgremium erforderlich sei. Um die Einführung der TLD .eu voranzutreiben, haben sich inzwischen verschiedene europäische ISPs zu einer eigenen Organisation namens *Council of European Registrars*<sup>782</sup> (CO-EUR) zusammengeschlossen. Diese Organisation will zum einen beratend die *Europäische Union* bei der Formulierung der Registrierrichtlinien unterstützen und zum anderen, sich selbst als Betreiber für die *Registry* der TLD .eu bewerben<sup>783</sup>.

Ermöglicht hat die ICANN eine TLD .eu mit der Entscheidung, daß zweistellige Länderdomains auch an Territorien vergeben werden können, welche nicht in der mit ISO 3166-1 stan-

---

<sup>778</sup> Vgl. *Froomkin*, Thwarting Competition, Kap. The Three Relevant Markets, (3) The market for domain names.

<sup>779</sup> Siehe *EU-Kommission*, Kommission berichtet über Fortschritte bei der Schaffung des Bereichsnamens „.EU“ zur Förderung des elektronischen Geschäftsverkehrs in Europa, 5. Juli 2000, IP/00/708 und *Europäische Kommission*, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Einführung des Internet-Bereichs oberster Stufe „.EU“, 12. Dezember 2000, KOM(2000) 827 - 2000/0328/COD sowie deren Amendment vom 2. Oktober 2001, KOM(2001) 535. Siehe auch die Information Society Website der *Europäischen Kommission*, Internet Governance and the Domain Names System, [http://europa.eu.int/ISPO/intcoop/i\\_govern.html](http://europa.eu.int/ISPO/intcoop/i_govern.html).

<sup>780</sup> *Heise-Newsticker*, .eu kommt – sicher, aber langsam ..., 28. Juni 2001.

<sup>781</sup> *Rat der Europäischen Union*, Verordnung zur Einführung der Domäne oberster Stufe ".eu", C5-0548/2001, noch nicht im Amtsblatt veröffentlicht. Siehe jedoch [http://www.europarl.eu.int/commonpositions/2001/pdf/c5-0548-01\\_de.pdf](http://www.europarl.eu.int/commonpositions/2001/pdf/c5-0548-01_de.pdf).

<sup>782</sup> Der CO-EUR tritt im Internet unter <http://www.co-eur.org> auf.

<sup>783</sup> Vgl. *Heise-Newsticker*, Vereinigung europäische Registrare will .eu-Registry, 13. Januar 2001 sowie *Heise-Newsticker*, EU-Kommission warnt vor Alleingang bei .eu-Domains, 5. Juni 2001.

dardisierten Liste der Länderkürzel stehen, sondern nur auf der Liste für reservierte Codes bei der *ISO 3166 Maintenance Agency* des *Deutschen Instituts für Normung* genannt sind<sup>784</sup>. Ein erster umfassender Vorschlag zum Management der TLD .eu wurde von dem *European Community Panel of Participants in Internet Organisation and Management* (EC-POP) im Oktober 2000 eingereicht, der eine Verbindung zum Territorium und den Institutionen der *Europäischen Union* vorsieht<sup>785</sup>:

Since the Dot EU Registry will carry with it a clear implication of a link with the European Union both territorially and institutionally, it is also of particular importance that the Registry should respect the laws and policies of the European Union.

Nach der *Verordnung zur Einführung der Domäne oberster Stufe „.eu“* soll die *Europäische Kommission* mit der Errichtung TLD .eu betraut werden. Es soll ihr möglich sein, allgemeine politische Grundsätze zur Verhinderung der spekulativen und mißbräuchlichen Registrierung von Domainnamen zu verabschieden<sup>786</sup>. Außerdem soll sie ein Verfahren zur außergerichtlichen Streitlösung von Konflikten zwischen Urheberrechts- und Domaininhabern entwickeln<sup>787</sup>. Die einzusetzende *Registry* soll nach einer öffentlichen Ausschreibung durch die *Europäische Kommission* auf der Basis eines offenen, transparenten und nichtdiskriminierenden Verfahrens ausgewählt werden. Sie soll eine gemeinnützige Organisation mit Sitz in der Europäischen Gemeinschaft sein<sup>788</sup>. Die *Registry* selbst soll sich ebenfalls an die Regeln für das öffentliche Auftragswesen und an transparente und nichtdiskriminierende Verfahren halten<sup>789</sup> sowie die relevanten Prinzipien, welche das GAC der ICANN verabschiedet hat, beachten<sup>790</sup>. Auch bei der Verwaltung der TLD .eu soll zwischen *Registry* und den *Registrars* differenziert werden<sup>791</sup>. Anspruchsberechtigt auf eine .eu-Domain sollen vor allem im EU-Gebiet niedergelassene Unternehmen, Organisationen mit Sitz in der EU oder Einwohner der EU-Mitgliedsstaaten sein<sup>792</sup>. Schließlich sollen der Europäischen Gemeinschaft alle Rechte in Verbindung mit der TLD .eu, insbesondere die Rechte des geistigen Eigentums und sonstigen Rechte an der Registrierungsdatenbank und das Recht, ein anderes Register zu benennen, erhalten bleiben<sup>793</sup>.

---

<sup>784</sup> Beschuß 00.74 des ICANN Board of Directors, 25. September 2000, Preliminary Report - Special Meeting of the Board, <http://www.icann.org/minutes/prelim-report-25sep00.htm#00.74>. Zur Reservierung des Kürzels EU bei der ISO siehe *ISO 3166 Maintenance Agency*, Request for Extension of Reservation of ISO 3166-1 Code Element EU, 7. September 1999,

[http://europa.eu.int/ISPO/eif/InternetPoliciesSite/DotEU/Reservation\\_of\\_EU.pdf](http://europa.eu.int/ISPO/eif/InternetPoliciesSite/DotEU/Reservation_of_EU.pdf).

<sup>785</sup> *EC Panel of Participants in Internet Organisation and Management* (EC-POP), The Dot EU TLD Registry Proposal, 10. Oktober 2000, <http://www.ec-pop.org/1009prop/index.htm>.

<sup>786</sup> Siehe TLD .eu Verordnung, Art. 5 Nr. 1, Fn. 781.

<sup>787</sup> Siehe TLD .eu Verordnung, Art. 4 Nr. 2. (d), Fn. 781.

<sup>788</sup> Siehe TLD .eu Verordnung, Art. 3 Nr. 2, Fn. 781.

<sup>789</sup> Siehe TLD .eu Verordnung, Art. 4 Nr. 1, Fn. 781.

<sup>790</sup> Siehe TLD .eu Verordnung, Art. 3 Nr. 3, Fn. 781.

<sup>791</sup> Siehe TLD .eu Verordnung, Art. 3 Nr. 4. und Art. 4 Nr. 2 (a), Fn. 781.

<sup>792</sup> Siehe TLD .eu Verordnung, Art. 4 Nr. 2. (b) (i) – (iii), Fn. 781.

<sup>793</sup> Siehe TLD .eu Verordnung, Art. 7, Fn. 781.

#### 3.3.3. Multilinguale Domainnamen

Das dritte Element der Reform des DNS stellt die Einführung multilingualer Domainnamen dar. Da es hierbei vorrangig nur um die Einführung neuer technischer Standards für die Kodierung von Umlauten und Betonungszeichen (zum Beispiel ä, ó, ç), Zeichen, welche nicht zur lateinischen Schrift gehören (zum Beispiel kyrillische oder arabische Buchstaben) sowie Wortzeichen (zum Beispiel aus der chinesischen oder japanischen Schriftsprache), handelt, soll in dieser Arbeit nur kurz darauf eingegangen werden.

Die Einführung internationaler Schriftzeichen in das DNS ist eine schon lange, besonders aus dem asiatischen Sprachraum erhobene Forderung. Bislang war die Registrierung von Domainnamen auf die 26 Zeichen des englischen Alphabets, den zehn Ziffern und dem Bindestrich begrenzt. Diese Einschränkung führte dazu, daß sich das Internet im asiatischen Raum nicht so schnell verbreitete wie in Europa und Amerika. Seit 2000 versuchen Ingenieure der IETF einen gemeinsamen Standard für die Kodierung der Vielzahl von Schriftzeichen zu finden. Außerdem muß die dem DNS zugrundeliegende Software auf diese neuen Standards angepaßt werden. Trotz des Fehlens eines gemeinsamen Standards versuchen einige Firmen aus der schon jetzt bestehenden Nachfrage nach internationalisierten Domainnamen Gewinn zu schlagen. Seit November 2000 ist es zum Beispiel möglich, über die NSI chinesische Domainnamen registrieren zu können, welche jedoch zunächst in einer getrennten Datenbank gespeichert werden<sup>794</sup>. Seit Februar 2001 lassen sich auch Domainnamen mit Umlauten bei NSI reservieren. Da jedoch noch kein IETF-Standard verabschiedet und umgesetzt wurde, bleiben diese Domainnamen für die meisten Internetnutzer verborgen. Ein Zugriff ist nur mittels eines speziellen Zusatzprogramms für die WWW-Browser möglich. Damit geht eine Fragmentierung des DNS einher, die man vermeiden wollte. Da mehrere Firmen inzwischen eine Vorregistrierung von internationalen Domainnamen in eigene Datenbanken anbieten, kann ein Domainname bei mehreren Anbietern registriert sein. Dies kann schließlich dazu führen, daß registrierte Namen nicht in einen eventuell verabschiedeten Standard umgesetzt werden können. Die Inkompatibilität der einzelnen Kodierungsverfahren erfordern somit, daß vor einer weltweiten Umsetzung einer Kodierungslösung, die Ergebnisse der IETF abgewartet werden müssen.

---

<sup>794</sup> Siehe *Heise-Newsticker*, Domain-Namen auf Chinesisch, 10. November 2000.

*How many legs does a horse have if I call the tail a leg? The answer is four, because the calling the tail a leg doesn't make it one.*

– US-Präsident Abraham Lincoln –

*Aber lassen sie uns mit ihren Juristen in Ruhe. Die Geschäftsleute haben sie leider mitgebracht, diese Jungs die schon im Kauf einer Packung Gummibärchen eine Vertragshandlung sehen, und die den nun wirklich nicht zu beanstandenden natürlichen Akt der nicht einmal sexuellen Vermehrung von Bits mit so garstigen Begriffen wie „Raubkopien“ verstehen.*

– Andy Müller-Maguhn – Regierungserklärung –

## 4. Die Domainnamen

Obgleich ein Domainname ursprünglich ein Set von numerischen IP-Adressen ersetzen sollte, hat er eine weit darüber hinaus gehende Bedeutung erlangt. Er stellt eine Mischung zwischen Lokator und Identifikator dar. Er führt einen Internetnutzer zu einer bestimmten Webseite, FTP-Adresse oder gibt ihm Hinweise, welche Inhalte eine spezielle Homepage beinhalten könnte. Er ermöglicht das Ermitteln von Adressen der verschiedenen Firmen, Organisationen oder Bildungseinrichtungen.

Zunächst soll deshalb auf die Bedeutung von Namensbezeichnungen eingegangen und einige, den Domainnamen ähnliche Produkt- und Adressbezeichnungen, erläutert werden, um ein Verständnis für die namensrechtlichen Probleme der Domainnamen zu ermöglichen. Aufbauend auf dieser Darstellung wird ein Überblick über die kennzeichenrechtlichen Streitpunkte gegeben. Die einzelnen Problembereiche und Anspruchsgrundlagen diskutierte man in der wissenschaftlichen Literatur bislang sehr ausführlich. Inzwischen sind sehr viele Streitigkeiten gerichtlich entschieden worden, so daß man zum Teil von einer gefestigten Rechtsprechung ausgehen kann. Da jedoch für das Verständnis der Entwicklung des *Domain Name Systems* und dessen Verwaltung eine Kenntnis der namens- und markenrechtlichen Zusammenhänge unumgänglich ist, soll eine zusammenfassende Darstellung erfolgen<sup>795</sup>.

---

<sup>795</sup> Ausführlich werden die kennzeichenrechtlichen Probleme in Bücking, Domainrecht erläutert.

## 4.1. Bedeutung von Namensbezeichnungen

Namen bezeichnen Personen, Lebewesen oder Sachen zur eindeutigen Identifikation und Zuordnung. Durch die sprachliche Kennzeichnung eines Individuums dienen sie als Unterscheidung des Namensträgers von anderen Personen<sup>796</sup>. Sie sollen leicht zu merken sein und entsprechen häufig dem aktuellen Zeitgeist.

So wurden Anfangs diesen Jahrhunderts Rückgriff auf lateinische Bezeichnungen genommen, wie zum Beispiel der Markenname Audi für Fahrzeuge von Horch. In den zwanziger Jahren sollten Namen Größe und Macht demonstrieren, zum Beispiel die 1923 in die *International Business Machines Corporation* (IBM) umgenannte *Computing, Tabulating and Recording Company*<sup>797</sup>.

In den sechziger Jahren waren besonders Abkürzungen eine beliebte Wahl für die Bezeichnung von Produkten und Firmen, zum Beispiel IBM für *International Business Machines Corporation* oder USX für die *United Steel*, gefolgt von Namen mit X wie *Xerox*, *Kleenex* oder *Exxon* sowie Namen mit „a“ als Endung: *Optima*, *Optiva*, *Adapta* oder *Maxima*.

Im Zeitalter des Internets und der Hochtechnologie wurden wohlklingende Namen wichtig, wie *Rhapsody*, *Java*, *Excite*, *Cloun* oder *Yahoo*<sup>798</sup>. Es wurden Namen, entsprechend dem Begriff Cyberspace, in Anlehnung an geographische Begriffe gewählt, wie *Netscape*, *Gateway*, *Altavista* oder *Global Village*. Produkte zur „Navigation“ im Internet erhielten Namen wie *Microsoft InternetExplorer*, *Pathfinder* oder *WebCompass*.

Viele der erwähnten Produkte wären sicherlich weniger erfolgreich, hätten sie sich anstatt mit einem einprägsamen Namen mit einer Nummer (wie einer IP-Nummer) begnügen müssen. Oft werden durch die Konsumenten ganze Produktbereiche mit einem Namen gleichgesetzt, wie *Kleenex* für Taschentücher, *Hoover* für Staubsauger oder der *Microsoft InternetExplorer* für den gesamten Zugriff auf das WWW. Folglich sind Eigennamen kaum aus unserer Gesellschaft wegzudenken.

## 4.2. Bisher verwendete Kurzbezeichnungen

Numerierungssysteme und alphanumerische Merkhilfen wurden nicht zuerst zur Adressierung von Computern im Internet eingesetzt. Schon Anfang des 19. Jahrhunderts setzten Telegrapheoperatoren Aktienkurzbezeichnungen ein, um Übertragskapazitäten zu sparen. Die Post ermöglichte Anfang des 20. Jahrhunderts normale Postadressen für den Telegrammverkehr durch leicht zu merkende Kürzel zu ersetzen. Die Kenntnis der historischen Entwicklung solcher Systeme ermöglicht die Bedeutung des DNS näher zu verstehen. Im Folgenden soll deshalb auf einige Beispiele von Numerierungs- und Abkürzungssystemen eingegangen werden.

---

<sup>796</sup> RG vom 3. Dezember 1917, RGZ 91, 350, 352; BGH vom 5. Dezember 1958, NJW 1959, 525.

<sup>797</sup> Vgl. hierzu und zur folgenden Darstellung: Rony/Rony, Domain Name Handbook, S. 18f.

<sup>798</sup> Yahoo ist heute eines der größten Internetportale: <http://www.yahoo.com> und <http://www.yahoo.de>.

### 4.2.1. Aktiensymbole an den Börsen

Aktiensymbole stellen Abkürzungen oder Abstraktionen von börsengelisteten Unternehmen dar, um den aktuellen Aktienkurs platzsparend der jeweiligen Aktiengesellschaft zuweisen zu können. Diese Symbole werden während des Handels, um Aktienkurse abzufragen oder um Unternehmensnachrichten zu veröffentlichen, verwendet. Jede Börse<sup>799</sup> weist diese Symbole ihren gelisteten Aktien zu. Aktiensymbole bestehen gewöhnlich aus drei bis fünf Buchstaben, einem Trennsymbol und der Börsenkürzbezeichnung<sup>800</sup>. Sie wurden Anfang des 19. Jahrhunderts von den Telegrafieoperatoren eingeführt, um Zeit und Bandbreite zu sparen<sup>801</sup>. Die Aktiensymbole werden auf nach Nachfrage vergeben. Welches Unternehmen zuerst Interesse für ein bestimmtes Kürzel zeigt, erhält dieses, soweit sich das Unternehmen mit diesem Kürzel identifizieren lässt. Wie im DNS kann es Wiederholungen nicht geben. Ein Aktiensymbol, verwendet für ein Unternehmen kann nicht für ein weiteres vergeben werden. Dies schließt auch eine Vergabe des Symbols an einer anderen Börse aus.

### 4.2.2. Alphanumerische Telegrammadressen und Fernschreiberkennungen

Zu Beginn des 20. Jahrhunderts wurde für das *Deutsche Reich* mittels § 3 Abs. 7 und 8 Telegraphenordnung<sup>802</sup> das Recht auf eine abgekürzte Adresse für den Telegrammverkehr eingeführt<sup>803</sup>. Die abgekürzte Telegrammadresse war durch eine Vereinbarung mit der Telegraphenanstalt des Wohnortes und durch eine dortige Hinterlegung der Adresse erhältlich. Diese Kurzform trat nunmehr im Telegrammverkehr an die Stelle des Namens und der Wohnadresse. Bei einem Telegramm an eine solche alphanumerische Telegrammadresse wurde im zuständigen Postamt manuell die dazugehörige Postanschrift herausgesucht und das Telegramm zugestellt. Damit bestehen im Grundprinzip starke Ähnlichkeiten zum DNS, bei welchem einem Domainnamen die IP-Adresse des entsprechenden Computers zugeordnet wird.

Die Abkürzung kann dabei willkürlich die Person oder dessen Geschäft bezeichnen und dabei einen bürgerlichen Namen, eine Firma oder einen freien Namen darstellen. Schon das Reichsgericht<sup>804</sup> stellte fest, daß diese Kurzbezeichnungen wie normale Namen dem Namenschutz

<sup>799</sup> Z.B. die *Deutsche Börse* in Frankfurt, die *New York Stock Exchange* (NYSE) oder die *National Association of Securities Dealers Automated Quotation System* (NASDAQ).

<sup>800</sup> Das Unternehmen Mannesmann AG verwendet z.B. das Kürzel MMN, das Unternehmen DaimlerChrysler AG das Kürzel DCX. DCX.FSE kennzeichnen die an der Frankfurter Parkettbörse gehandelten Aktien der DaimlerChrysler AG, DCX.NYS die an der NYSE gehandelten Aktien.

<sup>801</sup> Rony/Rony, Domain Name Handbook, S. 23.

<sup>802</sup> Telegraphenordnung für das Deutsche Reich, vom 16. Juni 1904, Abl. des Reichspostamtes 1904, S. 171; § 3 Abs. 7: „Die Anwendung einer abgekürzten Adresse ist zulässig, wenn sie vorher vom Empfänger mit der Telegraphenanstalt seines Wohnortes vereinbart worden ist. Wer eine mit der Telegraphenanstalt vereinbarte, abgekürzte Adresse hinterlegt hat, ist berechtigt, diese Adresse in den für ihn bestimmten Telegrammen an Stelle seines vollen Namens und der Wohnungsangabe anwenden zu lassen...“ Eine Neufassung erfolgte am 22. Juni 1926 und war bis in die Anfangszeiten der BRD in der Fassung vom 22. Dezember 1938 (Abl. des Reichspostministerium Nr. 144, 849, § 4 Abs. 5) gültig.

<sup>803</sup> Wertheimer, GRUR 1907, 348; Nietzold, GRUR 1925, 1ff. mit näheren Angaben zur Vergabe.

<sup>804</sup> RG vom 12. April 1921, RGZ 102, 89f.; RG vom 27. Mai 1909, DJZ 1909, 1091.

## 4.2. Bisher verwendete Kurzbezeichnungen

---

aus § 12 BGB unterfallen. Diese Kurzadresse sei ebenso wie Namen und Firmenangaben ein eigenes Individualisierungsmittel des Geschäfts, als dessen Bezeichnung. Auch als Kennzeichen genoß es den Schutz des damaligen § 16 UWG<sup>805</sup> gegen eine Benutzung durch andere, wenn dem beteiligten Verkehrskreis die Telegrammanschrift als Kennzeichen bekannt war.

Demselben Prinzip folgten die ab den siebziger Jahren häufigen Fernschreiberkennungen. Fernschreiber waren elektrische Geräte, ähnlich den heutigen Faxgeräten, welche zum Empfang von Textnachrichten dienten. Der Fernschreibteilnehmer suchte sich eine Kennung selbst aus, die in ihrer Buchstabenzusammensetzung auf ihn hinwies. Sie erscheint dann zu Beginn und am Ende eines fernschriftlich übertragenen Textes. Zusätzlich wurden die Fernschreiberkennungen in einem amtlichen Fernschreibverzeichnis aufgenommen, um ein schnelles Auffinden der Kennungen zu ermöglichen. Auch hier bestehen Ähnlichkeiten zum DNS. Die Fernschreiberkennung wurde aber im Vergleich zu den Domainnamen kaum rechtlich relevant. In der einzigen Entscheidung des BGH<sup>806</sup> („Fernschreibkennung“) ging dieser davon aus, daß die Benutzung einer Fernschreiberkennung in ein prioritätsälteres Kennzeichen eingreifen könne, wenn diese Benutzung kennzeichenmäßig erfolge.

### 4.2.3. ISO-Nummern für Publikationen

Die ISO hat Identifizierungsstandards für verschiedene Publikationstypen definiert. Dazu zählen die *International Standard Book Number* (ISBN) für Bücher, die *International Standard Serial Number* (ISSN) für Periodika, die *International Standard Music Number* (ISMN) für Musikprodukte oder der *International Standard Recording Code* (ISRC) für Tonaufnahmen. Die ISO beauftragte für jeden Numerierungsstandard eine internationale Agentur, welche die Kontrolle über die Vergabe von Nummernkontingenten an nationale Organisationen überträgt. Verlage wiederum können bei den nationalen Organisationen Nummern für ihre Publikationen beantragen.

#### 4.2.3.1. International Standard Book Number

Bei der ISBN, der wichtigsten Anwendung von ISO-Numerierungen, handelt es sich um eine internationale Numerierung von Büchern und ähnlichen Produkten. Es ist anhand der ISBN möglich, ein Buch genau zu spezifizieren und dessen Verleger sowie weitere bibliographische Angaben zu erfahren. Für die Verwaltung der ISBN ist die *International ISBN Agency* in Berlin zuständig<sup>807</sup>. Für Deutschland nimmt die *Buchhändler-Vereinigung* in Frankfurt am Main die Vergabe wahr.

Die Entwicklung eines einheitlichen Buchnumerierungssystems geht auf den größten Buchhändler Großbritanniens, W. H. Smith, zurück<sup>808</sup>. Um 1965 ein elektronisches Warenhaus

---

<sup>805</sup> Siehe RG vom 12. April 1921, RGZ 102, 89f.

<sup>806</sup> BGH vom 18. Dezember 1985, GRUR 1986, 475ff.; vgl. auch OLG Hamburg vom 16. September 1982, GRUR 1983, 191ff.

<sup>807</sup> Zur *International ISBN Agency* siehe deren Webseite unter <http://www.isbn.org>.

<sup>808</sup> Vgl. den Überblicke zur Geschichte der ISBN unter ISBN - International, History, <http://www.isbn.org/standards/home/isbn/international/history.asp>.

aufzubauen, benötigte er ein Numerierungssystem für die zu vertreibenden Bücher. Mittels dem *British Publishers Association's Distribution and Methods Committee* und weiteren Experten entwickelte er das *Standard Book Numbering* (SBN) System, welches 1967 umgesetzt wurde.

Das *ISO Technical Committee on Documentation* (TC 46) setzte daraufhin eine Arbeitsgruppe ein, die sich mit der Umsetzung des britischen SBN auf internationaler Ebene beschäftigen sollte. Dazu erfolgte 1968 ein erstes Treffen von Vertretern aus Dänemark, Frankreich, Deutschland, Irland, Niederlande, Norwegen, Großbritannien und den USA in London. Unter Teilnahme weiterer Länder an verschiedenen Treffen in Berlin und Stockholm wurde 1969 die *International Standard Book Number* (ISBN) als Standard (ISO 2108) von der ISO verabschiedet. Obgleich der Standard zum Teil überarbeitet wurde, um ihn an die neuen buchähnlichen elektronischen Medienformen anzupassen, blieb die Grundstruktur bis heute erhalten und wird in über 150 Ländern weltweit angewendet.

Die Verwaltung des ISBN-Systems erfolgt auf drei Ebenen: international, regional und auf Verlegerebene<sup>809</sup>. Entsprechend dem hierarchischen Aufbau der Verwaltung setzt sich die zehnstellige ISBN zusammen. Die erste Nummer bestimmt die regionale Administration, zum Beispiel 3 für Deutschland, 2 für Frankreich und 0 beziehungsweise 1 zusammen für USA und Großbritannien. Der folgende Nummernblock spiegelt den Verleger mittels einer eigenen Nummer wieder. Schließlich verwenden die Verlage den dritten Nummernblock für die herausgegebenen Buchtitel. Die letzte Zahl stellt eine Prüfziffer, berechnet aus den ersten Zahlen, dar.

#### 4.2.3.2. International Standard Serial Number

Die *International Standard Serial Number*<sup>810</sup> (ISSN) hat eine ähnliche Bedeutung wie die ISBN. Sie ist der standardisierte internationale Code, welcher die Identifikation jeglicher Periodika (Zeitschriften, Zeitungen, Jahrbücher u.s.w.) erlaubt, unabhängig vom Land ihrer Publikation, ihrer Sprache oder Erscheinungsfrequenz. Die ISSN stellt wie die ISBN einen numerischen Code dar, beinhaltet jedoch in sich keinerlei Informationen, die einen Rückschluß auf die Herkunft der Publikation zulassen. Eine ISSN kann jedem Periodikum zugewiesen werden, unabhängig ob es sich um gedruckte Produkte oder um andere Medien handelt (zum Beispiel CD-ROM oder elektronische Publikation). Das Hauptkriterium, das die Zuweisung von ISSN ermöglicht, ist, daß das Produkt regelmäßig unter demselben Titel erscheint und keine Ausgabebegrenzung beim Start der Herausgabe geplant ist.

Die ISSN ist ebenso als Standard durch die ISO definiert worden (ISO 3297). Sie besteht aus zwei mal vier Ziffern, welche durch einen Bindestrich getrennt werden. Die achte Ziffer bildet einen Kontrollwert, der sich aus den ersten sieben Ziffern ergibt.

---

<sup>809</sup> Vgl. den ausführlicheren Überblick bei ISBN, ISBN – International, Administration of the ISBN System, <http://www.isbn.org/standards/home/isbn/international/administration.asp>.

<sup>810</sup> Die Homepage des ISSN International Centre befindet sich unter <http://www.issn.org>.

## 4.2. Bisher verwendete Kurzbezeichnungen

Das *ISSN International Centre* ist die Registrierungsorganisation, die durch die ISO zur Verwaltung des ISSN-Systems eingesetzt wurde. Die Vergabe in Deutschland erfolgt durch das *Nationale ISSN-Zentrum für Deutschland* in Frankfurt.

### 4.2.4. Alphanumerische Telefonnummern – Vanity-Nummern

Ein dem DNS sehr ähnliches Verfahren stellt die Ersetzung von Telefonnummern durch sogenannte Vanity-Nummern dar<sup>811</sup>. Dabei werden von Wortkombinationen die einzelnen Zeichen nach dem von der ITU empfohlenen Verfahren E.161 Option A<sup>812</sup> in Zahlen übersetzt. Durch Abdruck von drei bis vier Buchstaben auf je einer Telefonzifferntaste von Telefongeräten wird es dem Anwender ermöglicht, selbst die alphanumerische Umsetzung von Namen und Begriffen vorzunehmen.

Eine solche Ersetzung hat den Vorteil, daß anstelle einer langen Telefonnummer nur ein einziges Wort gemerkt werden muß. Der in der Entscheidung des OLG Stuttgart<sup>813</sup> relevanten Vanity-Nummer „Rechtsanwalt“ liegt zum Beispiel die unhandliche Telefonnummer 732487269258 zugrunde.

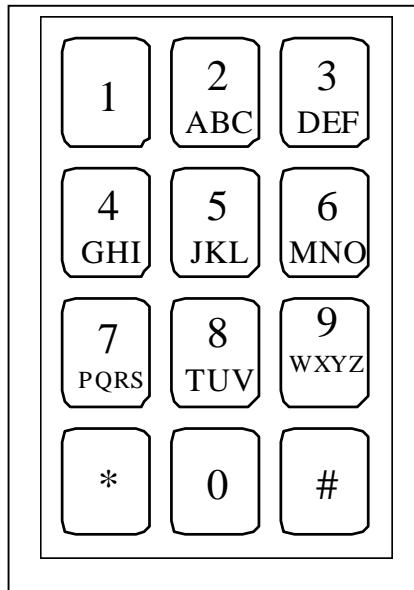


Abbildung 8 – Standardtelefontastatur und deren Entsprechung in Buchstaben

Die leicht zu merkenden Rufnummern dienen vor allem der unkomplizierten Erreichbarkeit des Gesprächspartners. Diese Mnemoniks besitzen deshalb einen nicht unerheblichen wirtschaftlichen Wert. Je einfacher sie sind, um so ausgeprägter ist ihre Werbe- und Kommunikationsfunktionalität. Der Ursprung der Vanity-Nummern liegt in den USA, wo sie seit 1967 eingesetzt werden<sup>814</sup>. Alphanumerische Tastaturen sind in den USA weit verbreitet, so daß dort Buchstabenaufdrucke auf jedem Telefongerät zu finden sind<sup>815</sup>. In Deutschland setzte sich diese Technik bislang nur schleppend durch, mit der beginnenden Vermarktung von Vanity-Nummern durch Telekommunikationsunternehmen kann jedoch eine schnelle Verbreitung in nächster Zukunft erwartet werden.

Seit dem 1. Januar 1998 vergibt die *Regulierungsbehörde für Telekommunikation und Post* (RegTP) in Deutschland Telefonnummern, § 43 Abs. 3 TKG<sup>816</sup>, welche auch Vanity-

<sup>811</sup> Zu Telefonnummern direkt: *BGH* vom 30. Januar 1953, „Telefonnummern“, BGHZ 8,387.

<sup>812</sup> Vgl. die Empfehlungen der ITU zur Standardisierung des Buchstabenwahlverfahrens unter Recommendation E.161, Fassung vom Februar 2001, <http://www.itu.int/itudoctitu-t/rec/e/e161.html>.

<sup>813</sup> Siehe *OLG Stuttgart* vom 15. Oktober 1999, MMR 2000, 164ff.

<sup>814</sup> Vgl. *Demmel/Stroboz*, MMR 1999, 74, 75.

<sup>815</sup> Vgl. die vielen Beispiele aus den USA, welche in *Rony/Rony, Domain Name Handbook*, S. 20ff. vorgestellt werden.

<sup>816</sup> Telekommunikationsgesetz, 25. Juli 1996, in der Fassung vom 10. November 2001, BGBI. I 1996, 1120 (2001, 2992).

Nummern darstellen können. Entsprechend der Vergabe von Domainnamen erfolgt die Zuteilung der Rufnummern in der Reihenfolge der Antragseingänge. Wenn mehrere gleichberechtigte Antragsteller zeitgleich die Zuteilung der gleichen Rufnummer beantragen, entscheidet das Los über die Zuweisung<sup>817</sup>. Dabei übernimmt die RegTP nur die Zuteilung der entsprechenden Telefonnummern. Die Zugangsgewährung zum Telefonnetz unter der zugewiesenen Nummer erfolgt durch die verschiedenen Telefonnetzbetreiber (zum Beispiel Deutsche Telekom).

Ebenso wie Domainnamen kann die alphanumerische Umsetzung von registrierten Vanity-Nummern mit dem Namens- oder Markenrechten einer dritten Person kollidieren. Bestimmungen für die Lösung solcher Konflikte enthalten die Vergabebestimmungen der RegTP nicht. Die noch spärliche Literatur zu diesem Problem versucht eine Lösung im Vergleich zu den Domainnamen zu finden. Vanity-Nummern dienen weniger der Erreichbarkeit eines bestimmten Endgerätes, sondern verweisen vielmehr auf einen bestimmten Netzteilnehmer. Dies ähnelt den Domainnamen, die einer Person gehören und der entsprechende Computer erst über das DNS bestimmt werden kann<sup>818</sup>. Die technische Komponente der Adressierung wird in beiden Fällen durch Zahlenkombinationen erreicht, denen Buchstabenfolgen entsprechen. Obgleich der Nutzer einer Vanity-Nummer diese selbst in die entsprechende Zahlenkombination umsetzt, indem er die zum jeweiligen Buchstaben gehörende Zifferntaste auf seinem Telefon wählt, ergibt sich zunächst kein Unterschied zu einem Domainnamen, beim die zugehörige IP-Adresse erst durch Nachfrage in der DNS-Datenbank ermittelt wird. Beide Namensangaben werden zentral verwaltet, einerseits durch die RegTP, andererseits durch das DENIC. Ebenso, wie mehrere Domainnamen auf eine IP-Adresse verweisen dürfen, können mehrere Vanity-Nummern derselben Telefonnummer zugeordnet werden.

Domainnamen, welche derselben IP-Adresse zugeteilt sind, können von verschiedenen Personen genutzt werden. Der Internetserver, der über die IP-Adresse angesprochen wurde, nimmt die entsprechende Verweisung auf die jeweilige Homepage vor. Hierin könnte ein grundlegender Unterschied zu den Vanity-Nummern bestehen. Einer Telefonnummer können sehr viele Vanity-Nummern zugeordnet werden, ohne daß ein Eintrag in einer Datenbank nötig ist. Ein Interessent beantragt bei der RegTP nicht die alphanumerische Vanity-Nummer selbst, sondern eine Telefonnummer mit einer bestimmten numerischen Folge. Es ist ihm freigestellt, ob und wie er dann diese Nummer in eine oder mehrere mit der Telefonnummer zu vereinbarende Vanity-Nummern übersetzt oder nur die Ziffernkombination selbst verwendet. Auf der Seite des später angerufenen kann nicht differenziert werden, welche Variante durch den Anrufenden eingesetzt wurde. Soweit es auf die technische Komponente der Adressierung ankommt, können die beiden Systeme somit nicht verglichen werden<sup>819</sup>.

---

<sup>817</sup> Siehe *RegTP*, Vorläufige Regelung für die Zuteilung von Rufnummern für entgeldfreie Mehrwertdienste, Antragsverfahren, [http://www.regtlp.de/reg\\_tele/start/in\\_05-06-03-01-02\\_m/](http://www.regtlp.de/reg_tele/start/in_05-06-03-01-02_m/).

<sup>818</sup> Vgl. *Demmel/Strobotz*, MMR 1999, 74, 76.

<sup>819</sup> Vgl. auch *Demmel/Strobotz*, MMR 1999, 74, 77.

#### 4.3. Rechtsnatur der Domainnamen

---

Für die Verwendung einer Vanity-Nummer im öffentlichen Verkehr, unter Verletzung fremder Namens- und Markenrechte, kann es jedoch keinen Unterschied geben. Für einen Laien kommt es nicht darauf an, wie die technische Umsetzung funktioniert. Er wird gewöhnlich das zum Namen passende Angebot erwarten, ohne sich bewußt zu sein, daß auch noch weitere Vanity-Nummern für die von ihm unbewußt umgesetzte Telefonnummer geben mag. Unterlassungsansprüche aus dem Marken- und Namensrecht müssen folglich die gleiche Wirkung entfalten können<sup>820</sup>. Analoge Ansprüche auf Übertragung der Telefonnummer werden auf Grund der technischen Differenz zum DNS wohl kaum in Frage kommen<sup>821</sup>.

Zusammenfassend kann man feststellen, daß die Vanity-Rufnummern eine starke Ähnlichkeit zum DNS aufweisen. In einigen Punkten wäre deshalb eine Gleichbehandlung gerechtfertigt. Auf Grund der nicht unerheblichen Unterschiede der technischen Ausgestaltung muß bei der analogen Anwendung von Grundsätzen, die aus der Rechtsprechung zum Domainrecht gewonnen wurden, vorsichtig vorgegangen werden.

### **4.3. Rechtsnatur der Domainnamen**

Entsprechend der wirtschaftlichen Bedeutung der Domainnamen, ist es nicht ausgeblieben, daß die Rechtsprechung zu verschiedenen Streitigkeiten um einen Namen Stellung beziehen mußte. Bislang fehlt es noch an ausreichend höchstrichterlichen Urteilen, jedoch kann man bei den meisten Streitpunkten bereits Anzeichen einer gefestigten Rechtsprechung und Literaturmeinung erkennen. Als Folge der unterschiedlichen Auffassungen zur Reichweite des Marken- und Kennzeichenschutzes nutzten viele Markeninhaber die Unerfahrenheit und Unkenntnis besonders kleinerer Unternehmen und von Privatpersonen aus, um von ihnen im Wege der Abmahnung und des einstweiligen Rechtschutzes die Freigabe von Domainnamen zu erpressen. Viele legten freiwillig die von ihnen betriebene Domain still, in der Angst, in Rechtsstreitigkeiten mit sehr hohem Streitwert hineingezogen zu werden. Inzwischen hat sich bezüglich der Nutzung von Domainnamen eine stabile Rechtssprechung herausgebildet. Die Möglichkeit, unliebsame Webseiten durch eine einstweilige Verfügung zu schließen, besteht aber weiterhin<sup>822</sup>. Viele Anspruchsgrundlagen greifen jedoch erst, wenn die Domainnamen eine Kennzeichen- oder Namensfunktion wahrnehmen und nicht bloße Adreßfunktion innehaben. Es soll deshalb zunächst auf diesen Punkt eingegangen werden, ehe der Namenschutz nach § 12 BGB sowie die markenrechtlichen Implikationen nach den Regeln des MarkenG<sup>823</sup>

---

<sup>820</sup> Zu den Unterschieden bei der Anwendung der einzelnen Tatbestände vgl. *Jonas/Schmitz*, GRUR 2000, 183, 184ff.

<sup>821</sup> Auf die einzelnen Ansprüche kann im Rahmen dieser Arbeit thematisch nicht eingegangen werden. Zur Lösung der einzelnen Probleme kann auf die oben genannte Literatur verwiesen werden.

<sup>822</sup> So wurde Greenpeace von dem Ölkonzern TotalFinaElf zur Schließung der Protestseite <http://www.oil-of-elf.de> mittels einer einstweiligen Verfügung des Landgerichts Berlin gezwungen. Den Streitwert hatte TotalFinaElf in ihrem Antrag mit 100.000 DM angegeben. Greenpeace reagierte mit einer Verlagerung der Seite auf <http://www.zensiert-durch-elf.de>. Näheres zu aktuellen Verfahren siehe *Greenpeace*, Der Streit um oil-of-elf.de, [http://www.greenpeace.de/GP\\_DOK\\_3P/BRENNPUN/F0011D.HTM](http://www.greenpeace.de/GP_DOK_3P/BRENNPUN/F0011D.HTM).

<sup>823</sup> Gesetz über den Schutz von Marken und sonstigen Kennzeichen, 25. Oktober 1994 in der Fassung vom 13. Dezember 2001, BGBl. I 1994, 3082, (1995, 156; 2001, 3656).

behandelt werden. Schließlich soll erläutert werden, ob das Verwenden eines Domainnamens, welcher der Marke eines Konkurrenten entspricht, wettbewerbsrechtliche Konsequenzen mit sich bringt. Auf Grund der umfangreichen Ausführungen in der Literatur zum Schutz von Marken und Kennzeichen vor dem *Domain Grabbing* sollen die folgenden Ausführungen sehr kurz gehalten werden. Als Überblick beanspruchen sie deshalb kein Recht auf Vollständigkeit<sup>824</sup>.

#### 4.3.1. Domainnamen als technische Angaben oder klassische Namen

Ein Namenschutz erfolgt hauptsächlich über § 12 BGB und stellt somit einen wichtigen Anhaltspunkt für die weitere Betrachtung dar. Hauptschutzobjekt bildet der Name natürlicher Personen sowie unterscheidungskräftige Berufs- und Künstlernamen<sup>825</sup>. Hinzu kommt der Schutz der Bezeichnung juristischer Personen, insbesondere Vereine<sup>826</sup>, juristische Personen des öffentlichen Rechts<sup>827</sup>, des Handelsrechts<sup>828</sup> und sonstiger gesetzlich anerkannter Personenvereinigungen<sup>829</sup>. Geschützt werden zusätzlich alle anderen namensartigen Kennzeichen, die unabhängig vom gesetzlichen Namen geführt werden<sup>830</sup>. Allen aufgeführten Gruppen ist gemeinsam, daß die entsprechenden Namen im wesentlichen Zuordnungs- und Individualisierungsfunktion wahrnehmen. Adressen wiederum nehmen Leitfunktionen wahr, um ein bestimmtes Objekt oder Subjekt zu erreichen. Sie stellen häufig Werte dar, die auf einen bestimmten realen oder virtuellen Ort verweisen. Domainnamen müssen somit der ersten Kategorie zuordenbar sein, um geschützte Namensrechte zu beeinträchtigen.

Wie im Kapitel 2.2.2.2 oben erläutert, wurden die Domainnamen als Ersatz für die unhandlichen IP-Adressen eingeführt. Technisch gesehen bezeichnen sie die Position eines Servers im Internet, der die entsprechenden Dienste (zum Beispiel Email, FTP oder WWW) anbietet. Sie kann zum Beispiel die Adresse eines Computers darstellen, auf welchem der Adressat seine Homepage gespeichert hat. In der frühen Literatur zum Verhältnis von Domains zum Kennzeichenrecht wurde deshalb für Domainnamen die Namenseigenschaft abgelehnt. Die Verwendung einer Domain als Zieladresse sei losgelöst von einem bestimmten Produkt oder ei-

---

<sup>824</sup> Zum aktuellen Stand der Rechtsprechung siehe vor allem *Bottenschein*, MMR 2001, 286ff. und *Ernst*, MMR 2001, 368.

<sup>825</sup> *BGH* vom 24. November 1993, „Namenschutz für ‚römisch-katholisch‘ und ‚katholisch‘“, BGHZ 124, 173, 178; *LG Düsseldorf* vom 18. März 1986, „Heino“, NJW 1987, 1413f.

<sup>826</sup> Vgl. für den eingetragenen Verein: *RG* vom 7. Juli 1910, RGZ 74, 114, 115; vgl. für den nichtrechtsfähigen Verein: *RG* vom 13. Dezember 1911, RGZ 78, 101f.

<sup>827</sup> *BGH* vom 24. November 1993, „Namenschutz für ‚römisch-katholisch‘ und ‚katholisch‘“, BGHZ 124, 173, 178; *BVerfG* vom 31. März 1994, NJW 1994, 2346f.

<sup>828</sup> *RG* vom 26. September 1924, RGZ 109, 213, 214; *RG* vom 11. Januar 1927, RGZ 115, 401, 406.

<sup>829</sup> Z.B. Gewerkschaften: *BGH* vom 24. Februar 1965, BGHZ 43, 245, 252; politische Parteien: *BGH* vom 28. Januar 1981, BGHZ 79, 265ff.; OHGs sowie KG: *RG* vom 11. Juni 1926, RGZ 114, 93 und die Handelsfirma: *BGH* vom 6. Juli 1954, „Kölnisch Wasser“, BGHZ 14, 155, 159.

<sup>830</sup> Z.B. aus dem Firmennamen abgeleitete Abkürzungen: *BGH* vom 8. Dezember 1953, „Abkürzungen – Kennzeichnungsschutz“, BGHZ 11, 214, 215; *BGH* vom 14. Mai 1957, BGHZ 24, 238, 240; *BGH* vom 24. Februar 1965, BGHZ 43, 245, 252; Werktitel: *BGH* vom 26. Mai 1994, GRUR 1994, 908ff. oder Haus- und Hotelnamen: *BGH* vom 9. Januar 1976, MDR 1976, 998; *KG* vom 10. November 1987, NJW 1988, 2892, 2893.

#### 4.3. Rechtsnatur der Domainnamen

---

ner Dienstleistung<sup>831</sup>. Auf Grund des fehlenden Bezuges zu einer Ware, Dienstleistung oder einem Unternehmen, könne der Domainname keine kennzeichenrechtliche Qualität innehaben. Weiterhin würde die Domain nicht einen Namensträger, sondern nur einen Computer bezeichnen, beziehungsweise ein Mittel zum schnellen und einfachen Zugriff auf einen bestimmten Rechner des Adressaten darstellen. Der Schutzbereich des Namens- und Markenrechts könne somit hier nicht eingreifen<sup>832</sup>.

Einige der ersten Entscheidungen zur Kennzeichenfunktion von Domainnamen sind vom Landgericht Köln ergangen und sprechen ebenfalls den Domains die Namensfunktion ab<sup>833</sup>. Auf Grund der freien Wählbarkeit der Buchstabenkombinationen, könne ein Internetnutzer keinen Hinweis auf die Person des Namensträgers aus der Buchstaben zusammensetzung herleiten. Ein direkter Zusammenhang zwischen der Kombination mit dem Namen des Benutzers bestände nicht. Vielmehr wären sie mit einer Telefonnummer oder Postleitzahl vergleichbar. Obgleich ein gut gewählter Domainname häufig im Zusammenhang mit Namen oder Funktion des Benutzers steht, komme diese Namensfunktion nicht durchgängig zur Anwendung. Deshalb könne nicht erwartet werden, daß hinter einer Domain der entsprechende Namensinhaber steht.

Die Frage, ob Domainbezeichnungen Namen im klassischen Sinne des BGBs sind, kann jedoch nicht daran festgemacht werden, inwieweit eine einheitliche Verkehrsansicht bezüglich der Unterscheidungskraft besteht. Vielmehr ist zwischen den einzelnen Typen von Domainnamen zu unterscheiden. Sicherlich kann ein Internetnutzer bei einem Domainnamen, welcher aus einer TLD zuzüglich eines Gattungsbegriffes besteht (zum Beispiel [www.buch.de](http://www.buch.de)), nicht auf den dahinter stehenden Benutzer schließen. Das Gleiche gilt für lange zusammengesetzte Domains, welche aus der TLD und der SLD sowie aus weiteren Unterdomains und zuzüglich tieferer Pfadangaben bestehen (zum Beispiel [www.yyy.xxx.de/abc/def/index.html](http://www.yyy.xxx.de/abc/def/index.html))<sup>834</sup>. Andererseits ist bei Domainnamen, welche Firmennamen entsprechen, häufig anzunehmen, daß hinter ihnen die zum Namen gehörenden Unternehmen stehen. So haben Domainnamen inzwischen die Bedeutung von Marketinginstrumenten. Sie werden bewußt zur Kennzeichnung von Unternehmen und Produkten im WWW eingesetzt<sup>835</sup>.

Es muß somit gefragt werden, ob die jeweiligen Internetadressen Unterscheidungskraft entfallen können<sup>836</sup>. Auf Abweichungen vom Verständnis eines durchschnittlichen Internetnutzers kann es dabei nicht ankommen. Ein Internetnutzer, auf der Suche nach der Homepage einer

---

<sup>831</sup> Graefe, Markenartikel 1996, 100ff.

<sup>832</sup> Strömer, CR 1997, 290; Schneider, Domain- und Namensrecht.

<sup>833</sup> Urteile des LG Köln vom 17. Dezember 1996, BB 1997, 1121, „kerpen.de“, <http://www.onlinerecht.de/vorent.html?LGKoeln961217b> und „huerth.de“, GRUR 1997, 377, <http://www.onlinerecht.de/vorent.html?LGKoeln961217a> sowie der Beschlüß „pulheim.de“, CR 1997, 291, <http://www.onlinerecht.de/vorent.html?LGKoeln961217>.

<sup>834</sup> Vgl. Wegner, CR 1999, 250, 253; mit Beispiel: *Omsels*, GRUR 1997, 328, 334.

<sup>835</sup> Hoeren, Rechtsfragen des Internet, Rdnr. 52; Kilian DZWIR 1997, 381, 387 und 389.

<sup>836</sup> Vgl. Bücking, Domainrecht, Rdnr. 71.

Firma oder einer Organisation, wird zunächst versuchen, diese durch Kombination des Namens mit einer TLD zu erraten. Dieses Erraten ist besonders in neuerer Zeit einfacher geworden, da sich immer mehr Firmen und Organisationen, auf Grund der gefallenen Kosten für die Registrierung von Domains, für einen Internetauftritt unter eigenem Namen entschieden haben.

Da Domainnamen eine technische Aufgabe wahrnehmen, diese jedoch zusätzlich häufig mit einer kennzeichenrechtlichen Funktion bedacht sind, ist mit der herrschenden Meinung von einer Doppelfunktion auszugehen<sup>837</sup>. Domainnamen entfalten somit zusätzlich eine Namensfunktion.

### 4.3.2. Namensschutz nach § 12 BGB

Anfang 1996, wurde das erste Urteil erlassen, welches sich mit der Problematik der Domainnamen auseinandersetzte. Es betraf den Schutz eines Städtenamens, gegenüber der Verwendung als Domainname. In diesem, durch einstweilige Verfügung ergangenem Urteil, stellte das Gericht fest, daß die Stadt Heidelberg in ihrem Namensrecht aus § 12 BGB verletzt sei<sup>838</sup>. Ein Internetnutzer, so daß Gericht, würde unter der Adresse heidelberg.de ein Angebot der Stadt Heidelberg erwarten und nicht, wie es hier der Fall war, ein privates Unternehmen, welches Informationen zur Region Rhein-Neckar zur Verfügung stellen wollte. Die Benutzung der Domain heidelberg.de durch ein privates Unternehmen würde somit zu Zuordnungsverwirrungen führen und sei ein unbefugter Gebrauch des Stadtnamens. Schutzwürdige Interessen der Stadt Heidelberg seien somit verletzt.

Anders entschied das LG Köln in den Fällen „hürth.de“, „kerpen.de“ und „pullheim.de“<sup>839</sup>. Dabei stellte das Gericht pauschal fest, daß eben nicht jeder Internetnutzer erwarten könne, daß hinter einer entsprechenden Adresskennung auch der bezeichnete Namensträger stände. Wie oben festgestellt, kann man nicht die Benutzung der Domainnamen verallgemeinern. Vielmehr kommt es auf den für die Domain verwendeten Namen an, so daß die Meinung des LG Köln zumindest für Städtenamen abzulehnen ist<sup>840</sup>.

Nach herrschender Rechtsprechung<sup>841</sup> greift der Namensschutz nicht nur dann ein, wenn durch die Verwendung des Namens bestimmte Güter, Produkte oder Einrichtungen als zum Namensträger gehörend betrachtet werden müßten. Es genügt, wenn ein objektiver Dritter von einer Einwilligung in den Gebrauch eines Namens durch einen anderen ausgehen müßte. Überträgt man diesen Grundsatz auf das Internet, kann man nicht in jeder Benutzung eines

<sup>837</sup> Vgl. statt vieler: *Hoeren*, Rechtsfragen des Internet, Rdnr. 52, *Nordemann*, NJW 1997, 1891, 1892; *Bettinger*, GRUR Int. 1997, 402, 409; *Bücking*, NJW 1997, 1886, 1887.

<sup>838</sup> *LG Mannheim* vom 9. März 1996, „heidelberg.de“, GRUR 1997, 377ff.

<sup>839</sup> Siehe Fn. 833.

<sup>840</sup> Vgl. auch *Bücking*, NJW 1997, 1886, 1890, sowie *Nordemann*, NJW 1997, 1891, 1892; *Bettinger*, GRUR Int. 1997, 402, 415; *Wegner* CR1999, 250, 251.

<sup>841</sup> *BGH* vom 18. März 1959, „Caterina Valente“, BGHZ 30, 7ff.; *BGH* vom 4. März 1960, „Promonta“, MDR 1960, 901 sowie *BGH* vom 23. September 1992, „Universitätsemblem“, BGHZ 119, 237ff.

#### 4.3. Rechtsnatur der Domainnamen

---

fremden Namens als Domainname bereits eine Verletzung des § 12 BGB annehmen. Insbesondere ist die *Top Level Domain* mit in die Betrachtung einzubeziehen, da zum Beispiel nicht erwartet werden kann, daß eine deutsche Stadt unter der TLD .com auftritt oder eine andere Landeskennung als .de gewählt hat. Wird der fremde Name in der Art und Weise verwendet, daß die angebotenen Produkte oder Dienstleistungen nicht dem namentlich Genannten in irgendeiner Weise zugeordnet werden können, so kann darin keine Aneignung des Namens für die eigenen Produkte gesehen werden<sup>842</sup>. Es bleibt aber der richterlichen Würdigung unterworfen, ob eine solche zufällige Zuordnung vorliegt oder der öffentliche Verkehr von einem Zusammenhang zwischen Namensinhaber und dem Angebot unter dem Domainnamen ausgeht. Die Gerichte können dabei nicht uneingeschränkt den Prioritätsgrundsatz des Namensrechts auf das Internet ausdehnen, da sie sonst den Bedürfnissen und der technischen Struktur, insbesondere der Eindimensionalität des *Domain Name Systems* nicht gerecht werden würden<sup>843</sup>. Insbesondere Personen, welche Domainnamen aus eigener Phantasie entworfen haben und dadurch unbewußt einen Namen einer anderen Person verwenden, müssen sich regelmäßig auf ein berechtigtes Interesse an der Benutzung des Domainnamens berufen können.

Nach § 12 BGB kann der Domaininhaber auf Freigabe des Domainnamens verurteilt werden, da es sich in der Registrierung um die eigentliche Störung handelt. Der § 12 BGB trägt ihm aber nicht die Pflicht auf, die Rechtsstellung des Verletzten in Hinsicht auf den Domainnamen zu verbessern<sup>844</sup>. Der Verletzende muß zwar seine Sperrposition, die er mit der Registrierung und Nutzung seiner Domainadresse ausübt, aufgeben. Er ist aber nicht verpflichtet, dafür zu sorgen, daß der eigentliche Namensinhaber die umstrittene Domainadresse erhält.

##### 4.3.3. Markenrechtliche Implikationen

Bei der Verwendung von Domainnamen im geschäftlichen Verkehr kann es zu zwei Konfliktpunkten kommen. Einerseits stellt sich die Frage, ob der Benutzer, welcher ausschließlich im Internet auftritt, mit seiner selbstgewählten und kennzeichenrechtlich unbeanstandeten Domain ein Markenrecht im Sinne § 4 MarkenG erwirbt. Andererseits kann er durch Verwendung einer Domain das Markenrecht eines anderen verletzen und sich Ansprüchen nach §§ 14 und 15 MarkenG aussetzen.

###### 4.3.3.1. Domainnamen als Marken im Sinne § 4 MarkenG

Domainnamen selbst entfalten zunächst keine markenrechtliche Qualität. Voraussetzungen und Rechtsfolgen der Registrierung von Domainnamen und Marken sind gänzlich verschieden<sup>845</sup>. Die Registrierung von Domainnamen erfolgt entsprechend den wirtschaftlichen An-

---

<sup>842</sup> Vgl. *BGH* vom 18. März 1959, „Caterina Valente“, *BGHZ* 30, 7ff.; *BGH* vom 15. März 1963, „Dortmund grüßt mit Hansa-Bier“, *GRUR* 1964, 38ff.; *BGH* vom 26. Juni 1981, „Rennsportgemeinschaft“, *BGHZ* 81, 75.

<sup>843</sup> Vgl. *Bücking*, *NJW* 1997, 1886, 1890.

<sup>844</sup> Siehe *OLG Hamm* vom 13. Januar 1998, „krupp.de“, *MMR* 1998, 214ff.

<sup>845</sup> Vgl. die Antwort der *Bundesregierung* auf die kleine Anfrage des Abgeordneten Dr. Manuel Kiper (BÜNDNIS 90/DIE GRÜNEN) im Bundestag vom 11.07.1997, BT-Drs. 13/8203, S. 15.

forderungen in einem schnellen und unbürokratischen Verfahren<sup>846</sup>. Die Folgen sind rein tatsächlicher Art, da ein Domainname innerhalb derselben TLD nur ein einziges Mal zugewiesen werden kann. Ein Markenrecht erwirbt ein Interessent nach § 4 MarkenG durch Antrag beim Deutschen Patentamt, durch den Erwerb von Verkehrsgeltung oder durch offenkundige Bekanntheit. Im Falle der Verletzung seiner Marke hat der Inhaber Unterlassungs- und Schadensersatzansprüche nach § 14 MarkenG. Ein Domainname muß folglich eine der Voraussetzungen des § 4 Nr. 1 bis 3 MarkenG erfüllen, um gleichzeitig den Markenschutz zu genießen. Die Verwendung einer Kennzeichnung im Internet selbst, begründet deshalb gewöhnlich kein Markenrecht<sup>847</sup>.

#### 4.3.3.2. Ansprüche nach §§ 14 und 15 MarkenG

Die meisten rechtlichen Streitigkeiten werden jedoch auftreten, wenn ein Domainname einer gleichlautenden Marke registriert wurde, ohne daß der Registrierende das Markenrecht besaß oder sonstig berechtigt war. Dazu muß die Domain im geschäftlichen Verkehr eingesetzt werden, §§ 14 und 15 MarkenG. Wird zum Beispiel unter der Domain Handel oder Werbung betrieben, oder wird sie selbst zum Kauf angeboten, so liegt ein Handeln im geschäftlichen Verkehr vor<sup>848</sup>. Von einer Benutzung im geschäftlichen Verkehr ist auch dann auszugehen, wenn der Domainname nur zum Zweck des späteren Weiterverkaufens registriert wurde, ohne die Absicht darunter ein Angebot zu schalten<sup>849</sup>. Rein private Nutzung scheidet hingegen aus. Gegen die geschäftlichen Nutzer von Domainnamen stehen Markeninhabern nach §§ 14 Abs. 5, 15 Abs. 4 Unterlassungsansprüche bei Verletzungen des Markenrechtes nach §§ 14 Abs. 2 bis 4, 15 Abs. 2, 3 MarkenG zu. Die einzelnen Fälle sollen im Folgenden kurz erörtert werden.

Den einfachsten Fall eines Unterlassungsanspruches stellt § 14 Abs. 2 Nr. 1 i.V.m. § 14 Abs. 5 MarkenG dar. Danach ist das Benutzen eines mit einer fremden Marke identischen Domainnamens untersagt, wenn die darunter angebotenen Waren oder Dienstleistungen mit denen unter der Marke angebotenen ebenfalls identisch sind. In einem solchen Fall hat der Markeninhaber regelmäßig einen Unterlassungsanspruch gegen den unberechtigten Markennutzer.

Komplizierter gestaltet sich die Anwendung von § 14 Abs. 2 Nr. 2 i.V.m. § 14 Abs. 5 MarkenG. Hier muß zunächst festgestellt werden, ob eine Ähnlichkeit zwischen Marke und dem zu betrachtenden Domainnamen besteht. Wenn dies gegeben ist, ist weiterhin zu prüfen, ob zwischen den Waren oder Dienstleistungen, welche unter den streitigen Kennzeichen angeboten werden, eine Verwechslungsgefahr besteht.

<sup>846</sup> Dieses Kriterium heben insbesondere das *OLG Frankfurt a.M.* vom 14. September 1999, „ambiente.de“, MMR 2000, 36, 38 und *OLG Dresden* vom 28. November 2000, „kurt-biedenkopf.de“, GRUR-RR 2001, 130 hervor.

<sup>847</sup> Vgl. *Omsels* GRUR 1997, 328, 329.

<sup>848</sup> Vgl. *Bettinger*, GRUR Int. 1997, 402, 408; *Nordemann*, NJW 1997, 1891, 1893; *Wegner*, CR 1999, 250, 254; *Kilian* DZWir 1997, 381, 387.

<sup>849</sup> Vgl. *Nordemann*, NJW 1997, 1891, 1893 mit weiteren Erörterungen zur reinen Registrierung einer Domain.

Im ersten Prüfungspunkt ist strittig, wie ähnlich sich die Verletzerdomain und die Marke sein müssen. Anders als bei den herkömmlichen Anwendungsgebieten des Markenrechts darf bei den Domainnamen nicht der technische Hintergrund außer Acht gelassen werden. Zum einen ist die TLD nicht mit in die Betrachtung einzubeziehen, da es sich bei ihr eher um eine technische Bezeichnung, unter welcher der Domainname registriert wurde, handelt<sup>850</sup>. Die Einbeziehung der TLD in die Untersuchung würde in fast allen Fällen zu einer Verneinung der Ähnlichkeit zwischen Marke und Domainnamen führen und folglich die Anwendung von § 14 Abs. 2 Nr. 2 MarkenG gänzlich aushöhlen.

Zweitens müssen die Domain und sämtliche Zusatzangaben absolut fehlerfrei eingegeben werden, um das entsprechende Angebot zu erreichen. Schon der Unterschied in einem Zeichen führt zur Nacherreichbarkeit der gewünschten Homepage. So ist <http://www.yahoo.com/> nicht gleich <http://www.yaho.com/>. Obgleich diese Bedingung den Internetnutzern bekannt ist und diese auf eine korrekte Schreibweise achten, wird es immer wieder zu Schreibfehler kommen, die zum Beispiel auf eine unerwünschte Homepage führen würden. Diese Schreibfehler und die darauf beruhende Fehlleitung könnten von anderen Anbietern ausgenutzt werden, um Internetnutzer auf ihre Homepage umzuleiten. Andererseits würde die Anwendung des üblichen markenrechtlichen Ähnlichkeitsmaßstabes, zum Beispiel eine sprachliche Assoziation, zu einer weitreichenden Blockade von Domainnamen führen. Eine darauffolgende, nur noch restriktiv mögliche Vergabe von Domainnamen, würde der begrenzten Ressource des DNS nicht gerecht werden. Die Namensengpässe, welche heute schon bestehen, würden um ein Vielfaches erhöht werden. Deshalb ist der Ähnlichkeitsbegriff im Internet bedeutend enger zu fassen als sonst üblich.

Eine vollständige Einschränkung, welche schon in der Abänderung eines Buchstabens die Verneinung einer Ähnlichkeit bedeuten würde<sup>851</sup>, ist dennoch abzulehnen. Ebenso lassen sich einer Marke gewisse Zusätze, zum Beispiel die Gesellschaftsform des Unternehmens, zuordnen. Kleine Abweichungen in der Schreibweise verhindern noch nicht die fehlende Assoziation mit dem Markeninhaber und müssen deshalb noch unter den Ähnlichkeitsbegriff fallen<sup>852</sup>.

Bei der Beurteilung der Ähnlichkeit der angebotenen Waren oder Dienstleistungen kann es nicht auf das Bestehen einer Homepage selbst ankommen<sup>853</sup>, da diese nur ein technisches Instrument für das Angebot darstellt. Vielmehr ist auf den Inhalt der Homepage und die sonstige Produktpalette des fraglichen Unternehmens abzustellen, da diese das eigentliche Angebot von Waren oder Dienstleistungen darstellen<sup>854</sup>. Hauptkriterium für die in

---

<sup>850</sup> Vgl. Wegner, CR 1999, 250, 254.

<sup>851</sup> Siehe Hoeren, Rechtsfragen des Internet, S. 99.

<sup>852</sup> Vgl. Nordemann, NJW 1997, 1891, 1894; Wegner, CR 1999, 250, 254f.

<sup>853</sup> So jedoch LG Düsseldorf vom 4. April 1997, „epson.de“, GRUR 1998, 159.

<sup>854</sup> H.M.: LG München vom 18. Juli 1997, „freundin.de“, CR 1997, 540; OLG München vom 2. April 1998, „freundin.de“, MMR 1998, 668ff.; OLG Hamm vom 13. Januar 1998, MMR 1998, 214ff.; OLG Karlsruhe vom

§ 14 Abs. 2 Nr. 2 MarkenG geforderte Verwechselungsgefahr stellt die Branchenähnlichkeit der Unternehmen dar, sowie der Bekanntheitsgrad und die Kennzeichnungskraft der Marken<sup>855</sup>. Ebenso spielt die Wahl der TLD eine Rolle, da mit dieser auf die Zielgruppe des Angebotes geschlossen werden kann.

Werden unter einem Domainnamen, der einer Marke entspricht, Waren oder Dienstleistungen angeboten, die nicht denen der Marke ähneln, so kommt nur noch ein Unterlassungsanspruch nach § 14 Abs. 2 Nr. 3 i.V.m. § 14 Abs. 5 MarkenG in Betracht. Diese Norm des Markenrechts schützt den Inhaber einer berühmten Marke zum einen vor der Rufausbeutung und zweitens vor einer Verwässerung beziehungsweise Beeinträchtigung seiner Marke. Zur Bestimmung des Ausgangskriteriums, der Ähnlichkeit zwischen Marke und Domain, gelten auf Grund der Besonderheiten des Internets die gleichen Erwägungen wie bei § 14 Abs. 2 Nr. 2 MarkenG<sup>856</sup>.

Im Internet wird häufig versucht, den Ruf einer Marke in der Weise auszunutzen, indem mit einer fremden Marke Internetnutzer auf Homepages gelockt werden, auf denen für andere Produkte Werbung betrieben wird. Hier wird der aus dem guten Ruf der Marke entstehende Aufmerksamkeitseffekt ausgenutzt<sup>857</sup>. Es wird die auf der Bekanntheit und dem Renommee der Marke basierende Kanalisierungsfunktion ausgebeutet<sup>858</sup>. Da ein solcher Anbieter die Aufmerksamkeit der Internetnutzer nur auf diese Art und Weise auf sich ziehen kann, nutzt er in nicht zustehender Art und Weise den Ruf dieser Marke aus.

Die Gefahr der Verwässerung tritt gewöhnlich parallel zur Rufausnutzung auf<sup>859</sup>. Sie ist anzunehmen, wenn ein Internetnutzer, durch Erraten einer Homepageadresse mittels Kombination mit einer Marke, auf das Angebot eines anderen Anbieters geroutet wird. Erst jetzt wird dem Suchenden bewußt, daß sich hinter der Marke auch noch ein weiteres Unternehmen verbirgt. Die Unterscheidungskraft der Marke gegenüber anderen Unternehmen wird auf diese Art beeinträchtigt und es tritt eine Verwässerung ein.

Die weite Anwendbarkeit des § 14 Abs. 2 Nr. 3 MarkenG wird durch das weitere Tatbestandsmerkmal, der Beeinträchtigung ohne rechtfertigenden Grundes in unlauterer Weise, eingeschränkt. Es wird somit eine im Einzelfall interessengerechte Abwägung ermöglicht. In die Betrachtung sind die Bekanntheit der Marke, die Ähnlichkeit zwischen Marke und Domain sowie das Bestehen eigener Kennzeichenrechte mit einzubeziehen. Wird die fremde Marke nur beiläufig verwendet, ohne sich dem Betrachter aufzudrängen, so ist die Verwerf-

---

24. Juni 1998, „*zwilling.de*“, MMR 1999, 171f.; *Nordemann*, NJW 1998, 1891, 1893ff.; *Wegner*, CR 1999, 250, 255; *Völker/Weidert* WRP 1997, 652, 658.

<sup>855</sup> Vgl. *Wegner* CR 1999, 250, 255.

<sup>856</sup> *Wegner*, CR 1999, 250, 255.

<sup>857</sup> Vgl. *BGH* vom 9. Juni 1994, „*McLaren*“, BGHZ 126, 208, 211 sowie vom 10. Februar 1994, „*Mars-Kondom*“, BGHZ 125, 91, 95.

<sup>858</sup> *Wegner*, CR 1999, 250, 256.

<sup>859</sup> Vgl. *Völker/Weidert* WRP 1997, 652, 659.

#### 4.3. Rechtsnatur der Domainnamen

---

lichkeit abzulehnen<sup>860</sup>. Soll jedoch der gute Ruf ausgenutzt werden, oder wird die Domain nur zum Zwecke des Verkaufes an den Markeninhaber reserviert, so wird das Fehlen des Rechtfertigungsgrundes zu bejahen sein.

Ähnlich der oben aufgeführten Erörterungen, kommt es bei § 15 Abs. 2 i.V.m. Abs. 4 MarkenG auf das Vorliegen einer Verwechslungsgefahr zwischen Unternehmenskennzeichen oder Werktiteln im Sinne § 5 MarkenG und Domainnamen an. Bei besonders markanten Kennzeichen, ist eine Verwechslungsgefahr sogar auf Grund des Gesamteindrucks einer Homepage zu bejahen, ohne daß eine Branchennähe erforderlich ist<sup>861</sup>. § 15 Abs. 3 schützt ein bekanntes Zeichen zusätzlich vor unlauterer Beeinträchtigung der Unterscheidungskraft und Wertschätzung, wenn es an einer Ähnlichkeit nach § 15 Abs. 2 MarkenG mangelt. Dieser Schutz von Kennzeichen entspricht dem Schutz von Marken nach § 14 Abs. 2 Nr. 3 MarkenG.

##### 4.3.4. Verstoß gegen das Wettbewerbsrecht

Bei der Registrierung von Domainnamen kann es nicht nur zu einer Verletzung von Kennzeichenrechten kommen. Häufig liegt mit der Benutzung eines Domainnamens auch ein Verstoß gegen das Wettbewerbsrecht vor. Ein solcher Verstoß spielt besonders in den Fällen eine große Rolle, in denen ein Unternehmen eine auch für andere Konkurrenten interessante Domain registriert. In Frage kommt bei einer solchen Handlung insbesondere ein Verstoß gegen § 1 UWG, als sittenwidrige Wettbewerbshandlung und ein Verstoß gegen § 3 UWG durch irreführende Angaben.

###### 4.3.4.1. Sittenwidrige Wettbewerbshandlung, § 1 UWG

Anspruchsvoraussetzungen für § 1 sowie § 3 UWG ist das Handeln im geschäftlichen Verkehr (vgl. Erörterung unter 4.3.3.2 oben) und das Vorliegen eines Wettbewerbsverhältnisses. Entsprechend dem BGH wird dabei weder Branchengleichheit der Parteien noch eine Behinderung des Absatzes bestimmter Waren verlangt<sup>862</sup>. Es genügt irgendein Wettbewerbsverhältnis gegenüber dem Verletzten. Die Internetnutzung selbst reicht jedoch für ein solches Verhältnis nicht aus, da das Internet nur das Kommunikationsmedium darstellt<sup>863</sup>. Schwieriger ist jedoch die Frage, ob die Reservierung eines Unternehmenskennzeichens durch eine Privatperson ein Wettbewerbsverhältnis begründet, wenn diese weiter verkauft werden soll. Obgleich hier ein Handeln im geschäftlichen Verkehr vorliegt, tritt der Reservierende jedoch nicht in den Wettbewerb des anderen ein. Meines Erachtens liegt damit keine Wettbewerbshandlung vor<sup>864</sup>.

---

<sup>860</sup> BGH vom 9. Dezember 1982, „Rolls-Royce“, BGHZ 86, 90, 95.

<sup>861</sup> Wegner, CR 1999, 250, 257.

<sup>862</sup> Vgl. BGH vom 29. November 1984, „DIMPLE“, BGHZ 93, 96; BGH vom 10. Februar 1994, „Markenverunglimpfung I“, GRUR 1994, 808, 809.

<sup>863</sup> LG Hamburg vom 10. Juni 1998, „emergency.de“, MMR 1998, 485.

<sup>864</sup> Vgl. Bücking, Domainrecht, Rdnr. 201; a.A. Kilian, DZWir 1997, 381, 389. In dem Beschuß des LG Köln vom 23. September 1999, „bahnhof.de“, MMR 2000, 45 wurde ohne Begründung ein Wettbewerbsverhältnis zwischen einer Privatperson und der Deutschen Bahn AG angenommen.

Nach Klärung, ob eine Wettbewerbshandlung vorliegt, muß diese auf ihre Sittenwidrigkeit hin untersucht werden. Das Tatbestandsmerkmal ist gegeben, wenn der Mitbewerber Vertriebshindernisse errichtet, für die kein sachlicher Grund vorliegt. Dabei soll der Konkurrent in seiner kennzeichenrechtlichen Position behindert und geschwächt werden<sup>865</sup>. Im Falle der Registrierung einer Internetadresse liegt die Sittenwidrigkeit dann vor, wenn die Registrierung in Kenntnis der Vorteile des Namensinhabers vorgenommen wird und beabsichtigt wird, daß dieser sein Kennzeichen im Internet nicht nutzen kann<sup>866</sup>. Entsprechend muß der Registrierende keinesfalls den Weiterverkauf des Namens beabsichtigen. Vielmehr reicht die Reservierung der Domain zur alleinigen Blockade des Mitbewerbers<sup>867</sup>. Allerdings kann nicht in jeder wirtschaftlichen Behinderung eine Sittenwidrigkeit gesehen werden. Die Sittenwidrigkeit fehlt zumindest dann, wenn die Domain aus der eigenen Marke oder Geschäftsbezeichnung abgeleitet wurde oder der Inhaber ein sonstiges berechtigtes Eigeninteresse vorweisen kann<sup>868</sup>. Bei der Feststellung der Sittenwidrigkeit ist auf die Umstände des Einzelfalles abzustellen. Insbesondere sind Möglichkeiten einen Ausweichnamen zu wählen, oder die Priorität und die Verkehrsgeltung eines außerhalb des Internets schon benutzten Kennzeichens zu beachten<sup>869</sup>.

#### 4.3.4.2. Irreführende Angaben, § 3 UWG

Neben einer sittenwidrigen Wettbewerbshandlung kann ein Nutzer eines Domainnamens auch gegen das Verbot der Irreführung, § 3 UWG verstößen. Diese kann auftreten, wenn die Öffentlichkeit hinsichtlich des Inhaltes oder Anbieters oder hinsichtlich des Erzeugers des beworbenen Produktes getäuscht wird<sup>870</sup>. Vor allem Domainnamen, welche aus beschreibenden Angaben oder Gattungsbegriffen bestehen (zum Beispiel [www.buch.de](http://www.buch.de), [www.mitwohnzentrale.de](http://www.mitwohnzentrale.de)<sup>871</sup>), bergen eine solche Gefahr, insbesondere, wenn Name und Inhalt in keinem Zusammenhang zueinander stehen oder bei den Nutzern die Assoziation einer Alleinstellung geweckt wird. In der Literatur wird darauf hingewiesen, daß Internetnutzer die Anbieter der Webseiten unter solchen Gattungsbegriffen als die alleinigen oder wichtigsten Betreiber betrachten könnten. Unerfahrene Nutzer werden verleitet anzunehmen, daß nur solche Anbieter die Berechtigung für die speziellen Produktgruppen hätten<sup>872</sup>.

---

<sup>865</sup> Vgl. zu Markenanmeldungen: *BGH* vom 3. November 1994, „Neutrex“, *BGHZ* 127, 262, 267; *BGH* vom 28. September 1979, „Torch“, *GRUR* 1980, 110ff.; *BGH* vom 11. November 1966, „Siroset“, *GRUR* 1967, 304ff.

<sup>866</sup> Vgl. *Bücking*, Domainrecht, Rdnr. 212; *Völker/Weidert* WRP 1997, 652, 660.

<sup>867</sup> Siehe *Kilian*, DZWir 1997, 381, 389.

<sup>868</sup> Siehe *Bücking*, Domainrecht, Rdnr. 209.

<sup>869</sup> Vgl. *Bücking*, Domainrecht, Rdnr. 209f.

<sup>870</sup> Vgl. *Kilian*, DZWir 1997, 381, 389.

<sup>871</sup> In seinem Grundsatzurteil „mitwohnzentrale.de“, vom 17. Mai 2001, *BGHZ* 148, 1 hat der *BGH* die Zulässigkeit der Nutzung von Gattungsbezeichnungen als Domainnamen im Hinblick auf einen möglichen Verstoß gegen das Verbot von Handlungen die gegen die guten Sitten verstößen (§ 1 UWG) bejaht. A.A. *OLG Hamburg* vom 13. Juli 1999, „mitwohnzentrale.de“, *CR* 1999, 779ff.

<sup>872</sup> Siehe *Bücking*, Domainrecht, Rdnr. 215.

#### 4.3. Rechtsnatur der Domainnamen

---

Obgleich daß Risiko einer Irreführung besteht, ist nach mehr als sechs Jahren Internetnutzung durch die breite Öffentlichkeit, die Anwendung und Bedeutung von Domainnamen allgemein bekannt. Manche neue Internetnutzer mögen zunächst davon ausgehen, daß zum Beispiel [www.buch.de](http://www.buch.de) der einzige Buchhändler im Internet sei. Es ist jedoch davon auszugehen, daß es der Mehrzahl der Nutzer bewußt ist, daß es eine bedeutende Anzahl weiterer Anbieter (zum Beispiel: [www.buecher.de](http://www.buecher.de), [www.bol.de](http://www.bol.de), [www.amazon.de](http://www.amazon.de)), gibt. Es wird zwar in der Regel ein Angebot erwartet, welches im sachlichen Zusammenhang mit dem Domainnamen steht, aber selbst neue Internetnutzer dürften auf Grund der intensiven Werbekampagne der einzelnen Konkurrenten, in den seltensten Fällen von einer Alleinstellung der Anbieter ausgehen. Sollte das Angebot jedoch nicht in Beziehung zum Domainnamen stehen, kann ein Internetnutzer extrem einfach und schnell die Webseite wechseln. Ein solcher Anbieter geht damit eher das Risiko ein, daß ein enttäuschter WWW-Nutzer nicht wieder auf seine Webseite zurückkehrt. Eine Irreführung im Sinne des § 3 UWG wird deshalb in den seltensten Fällen zu bejahen sein.

##### 4.3.5. Verstoß gegen das Deliktsrecht

In der Literatur<sup>873</sup> wird vertreten, daß ein Unternehmen sich auf den Schutz des eingerichteten und ausgeübten Gewerbebetriebes (eaG) nach § 823 Abs. 1 BGB analog berufen könne, wenn sein Name durch einen Dritten als Domainadresse registriert wurde. Der Schutzbereich des eingerichteten und ausgeübten Gewerbebetriebes umfaßt alles, was, bezogen auf die betriebliche Gesamtheit, den wirtschaftlichen Wert des Betriebes ausmacht<sup>874</sup>. Bücking rechnet hierzu die Möglichkeit des Internetmarketings<sup>875</sup>. Erfolgt eine unberechtigte Behinderung dieser Marketingmöglichkeit, so ist ein betriebsbezogener Eingriff in den Schutzbereich anzunehmen.

Der Schutz des eaG ist jedoch nicht direkt in § 823 Abs. 1 BGB erwähnt. Vielmehr handelt es sich hier um einen Auffangstatbestand, der eine sonst bestehende Rechtslücke insbesondere im gewerblichen Rechtsschutz schließen soll<sup>876</sup>. Er stellt eine analoge Anwendung der Grundsätze des Deliktsrechts in Bezug auf den Gewerbebetrieb dar. Es muß somit eine ungewollte Regelungslücke vorliegen. Das Markenrecht gewährt den Markeninhaber nach § 14 Abs. 1 und § 15 Abs. 1 MarkenG ein ausschließliches Recht. Dieses ist wiederum direkt durch § 823 Abs. 1 BGB geschützt<sup>877</sup>. Ein Rückgriff auf die Figur des eaG ist im Falle der Durchsetzung einer Marke damit überflüssig. Das Gleiche gilt für einen Schutz des Namensrechtes nach § 12 BGB<sup>878</sup>. Im Falle, daß ein Unternehmen, keine eigenen Rechte an einer Bezeichnung besitzt, erscheint es allerdings auch nicht schlüssig, eine Regelungslücke zu beja-

---

<sup>873</sup> Vgl. Bücking, Domainrecht, Rdnr. 225.; ders. NJW 1997, 1886, 1887.

<sup>874</sup> BGH vom 8. Februar 1971, BGHZ 55, 261.

<sup>875</sup> Vgl. Bücking, Domainrecht, Rdnr. 225.

<sup>876</sup> BGH vom 21. Juni 1966, BGHZ 45, 296, 307 und BGH vom 14. April 1965, BGHZ 43, 359, 361.

<sup>877</sup> Vgl. Müko-Mertens, § 823 Rdnr. 153 und Fn. 323; ebenso Wegner, CR 1999, 250, 257.

<sup>878</sup> Vgl. BGH vom 5. Dezember 1958, NJW 1959, 525f.; BGH vom 4. März 1960, „Promonta“, MDR 1960, 901; RG vom 27. Mai 1909, RGZ 71, 262, 265.

hen und damit den Anwendungsbereich des § 823 Abs. 1 BGB zu eröffnen. Ein Kennzeicheninhaber kann sich somit direkt auf den Schutz durch § 823 Abs. 1 BGB berufen.

Der Inhalt und Umfang des nach § 823 Abs. 1 BGB möglichen Schadensersatzes bestimmt sich nach den §§ 249ff. BGB. Es kann somit nicht nur ein finanzieller Ersatz des Schadens, welcher durch eine verspätete Internetpräsenz entstanden ist, verlangt werden, sondern auch eine Naturalrestitution, die eine Freigabe der reservierten Domain bedeutet<sup>879</sup>. Eine unmittelbare Verpflichtung zur Übertragung des Domainnamens auf den Anspruchsteller<sup>880</sup> lässt sich jedoch mittels §§ 249ff. BGB nicht begründen, da die Domain auf diesen selbst nie registriert war.

Werden Domainnamen in großer Anzahl und zum Zweck des anschließenden Verkaufs an den eigentlichen Rechtsinhaber registriert, kann dieses Verhalten die Sittenwidrigkeit nach § 826 BGB indizieren<sup>881</sup>. Auch bei rein privatem Handeln, kann § 826 BGB angewendet werden, wenn dem Handelnden die Motivation einer vorsätzlichen und sittenwidrigen Schädigung nachgewiesen werden kann. Eine solche sittenwidrige Handlung scheint dann erwägenswert, wenn der Registrierende die Domain aus reinem Behinderungswillen für sich registriert hat<sup>882</sup>.

#### 4.4. Rechtliche Verantwortung der DENIC eG

Neben den Domainnamen an sich birgt auch die eigentliche Vergabe der Domainnamen einige rechtliche Probleme. Die in den letzten Jahren stark angestiegenen Streitigkeiten um Domainnamen führten auch zu einer Involvierung der deutschen Domainvergabestelle DENIC eG in einzelne Gerichtsverfahren<sup>883</sup>, obgleich die DENIC eG einige Mechanismen zur Begrenzung des *Domain Grabbing*s in ihre Vergabebedingungen eingeführt hat. Deshalb soll zunächst in einem kurzen Exkurs auf die Vergabepraxis der DENIC eG eingegangen und auch geprüft werden, ob eine rechtliche Verpflichtung zum staatlichen Eingriff in die deutsche Domainvergabe besteht. Schließlich soll geklärt werden, ob die DENIC eG selbst zur Verantwortung wegen Marken- beziehungsweise Namensrechtsverletzungen herangezogen werden kann<sup>884</sup>.

---

<sup>879</sup> *OLG München* vom 2. April 1998, „freundin.de“, MMR 1998, 668ff.; *LG Lüneburg* vom 29. Januar 1997, „celle.de“, GRUR 1997, 470; Vgl. *Bücking*, Domainrecht, Rdnr. 228.

<sup>880</sup> Dies wird z.B. von *Hoeren*, Rechtsfragen des Internet, S. 31 gefordert.

<sup>881</sup> *Bettinger*, GRUR Int. 1997, 402, 414; *Wegner*, CR 1999, 250, 258; mit Einschränkungen: *Bücking*, Domainrecht, Rdnr. 227ff.

<sup>882</sup> Vgl. *Bücking*, Domainrecht, Rdnr. 227; *Völker/Weidert* WRP 1997, 652, 660f.

<sup>883</sup> Vgl. u.a. *OLG Frankfurt a.M.* vom 14. September 1999, „ambiente.de“, MMR 2000, 36, 38; *OLG Dresden* vom 28. November 2000, „kurt-biedenkopf.de“, GRUR-RR 2001, 130; *LG Magdeburg* vom 18. Juni 1999, „foris.de“, MMR 1999, 607ff.; *LG Frankfurt a.M.* vom 24. Mai 2000, „Dresdner-Hypovereinsbank.de“, CR 2001, 51f.

<sup>884</sup> nähereres dazu *Hoeren*, Rechtsfragen des Internet, Rdnr. 68 und *Bettinger/Freytag*, CR 1999, 28ff.

### 4.4.1. Exkurs 1: Vergabe von Domainnamen durch die DENIC eG

Das Verfahren zur Vergabe von Domainnamen richtet sich vor allem nach den DENIC-Registrierungsbedingungen<sup>885</sup> und den DENIC-Registrierungsrichtlinien<sup>886</sup>. Das Hauptprinzip der Vergabe lautet „first come, first served“. Soweit der Domainname noch frei ist, hat der erste Interessent das Recht auf diese Domain. Eine Registrierung eines Domainnamens unter der TLD .de kann über einen ISP vorgenommen werden, welcher Mitglied der DENIC eG ist oder mit einem solchen Mitglied zusammenarbeitet. Eine Registrierung ist aber auch direkt über die DENIC möglich, jedoch bieten in der Regel die einzelnen Provider die Domainregistrierung und -verwaltung zu erheblich günstigeren Preisen an als die DENIC selbst<sup>887</sup>. Der Antragsteller muß wie bei jedem Abschluß eines Vertrages voll geschäftsfähig sein. Juristische Personen müssen durch ihre Geschäftsführer beziehungsweise Vorstandsmitglieder vertreten sein. Durch die Registrierung kommt der Registrierungsvertrag zwischen dem künftigen Domaininhaber und der DENIC eG zustande.

Bei Abschluß des Registrierungsvertrages hat der Kunde der DENIC eG zu versichern, daß seine Angaben richtig sind und er zur Nutzung der Domain berechtigt ist, insbesondere, daß die Domain keine Rechte Dritter verletzt und nicht gegen allgemeine Gesetze verstößt<sup>888</sup>. Er hat einen in Deutschland ansässigen Zustellungsbevollmächtigten im Sinne von §§ 174f. ZPO als administrativen Ansprechpartner mit Zustellanschrift anzugeben, soweit er seinen Sitz nicht in Deutschland hat. Dieser ist als sein Bevollmächtigter berechtigt und verpflichtet ist, sämtliche den Domainnamen betreffende Angelegenheiten verbindlich zu entscheiden. Er ist damit der Ansprechpartner der DENIC eG. Sollte der Kunde falsche Angaben gemacht haben, zum Beispiel eine unzutreffende Adresse oder einen unkorrekten Namen angegeben haben, berechtigt dies die DENIC eG zur fristlosen Kündigung des Domainregistrierungsvertrags<sup>889</sup>.

Der Kunde hat sicherzustellen, daß die technischen Voraussetzungen zur Konnektierung der Domain im Internet bestehen<sup>890</sup>. Eine Registrierung ohne Nutzung ist seit Februar 1997 ausgeschlossen<sup>891</sup>. Damit soll ausgeschlossen werden, daß die Domain nur zum Zwecke des Weiterverkaufs registriert wird. Da es technisch und rechtlich erforderlich ist, werden die Kontaktdata des Domaininhabers in die öffentliche DENIC-Datenbank (Whois) aufgenommen und im Rahmen des DENIC-Abfrageservice weitergegeben<sup>892</sup>.

---

<sup>885</sup> Siehe *DENIC eG*, DENIC-Registrierungsbedingungen, 15. August 2000,  
<http://www.denic.de/doc/DENIC/agb.html>.

<sup>886</sup> Siehe *DENIC eG*, DENIC-Registrierungsrichtlinien, 15. August 2000,  
<http://www.denic.de/doc/faq/vergaberichtlinie.html>.

<sup>887</sup> Zu den Preisen der DENIC siehe DENICdirect, Preisliste, gültig ab 22. August 2000,  
<http://www.denic.de/DENICdb/domainreg/DENICdirect/preisliste.html>.

<sup>888</sup> § 3 (1) DENIC-Registrierungsbedingungen, Fn. 885. Vgl. auch *Hoeren*, Rechtsfragen des Internet, Rdnr. 48.

<sup>889</sup> § 7 (2) f)-i) DENIC-Registrierungsbedingungen, Fn. 885.

<sup>890</sup> § 3 (2) DENIC-Registrierungsbedingungen, Fn. 885.

<sup>891</sup> *Hoeren*, Rechtsfragen des Internet, Rdnr. 49.

<sup>892</sup> Diese Kontaktadressen können dann über die sogenannte Whois-Abfrage ermittelt werden: DENIC-Datenbank / Whois-Suche, <http://www.denic.de/servlet/Whois>.

Domainnamen, welche existierenden TLDs entsprechen (zum Beispiel .com, .net) können nicht registriert werden. Die DENIC eG verweist hierbei auf technische Probleme, die durch einen Fehler in einer bestimmten und stark verbreiteten DNS-Software bei der Anwahl von Domains des Musters „TLD.TLD“ auftreten können<sup>893</sup>. Aus diesem Grund registriert die DENIC eG auch keine ein- und zweistelligen Domains, da besonders hinsichtlich zweistelliger Domainnamen die Verwechslung mit länderbezogenen TLDs besteht und auch hier die eben erwähnten technischen Probleme auftreten können. Da sich der Bestand der ccTLDs regelmäßig ändert, hat sich die DENIC eG nicht nur auf Kürzel von bestehenden ccTLDs beschränkt, sondern sieht eine Sperrung von allen zweistelligen Domainnamen vor. Darüber hinaus befürchtet man bei den einstelligen Domainnamen für die Inhaber einen gegenüber den sonstigen Internetnutzern nicht akzeptablen Wettbewerbsvorteil<sup>894</sup>. Auch eine Registrierung von Domainnamen entsprechend den deutschen Kfz-Kennzeichen ist nicht zugelassen, da sich die DENIC eG eine eventuelle Erweiterung des deutschen DNS durch regionale Unterteilung des Namensraums offenhalten will<sup>895</sup>. Schließlich müssen Domainnamen aus technischen Gründen mindestens einen Buchstaben enthalten, da die allein aus Ziffern bestehenden Domainnamen mit IP-Nummern verwechselt werden können. Solche Konfusionen können zu technischen Schwierigkeiten führen, die nicht nur die Erreichbarkeit der Webseite des Domaininhabers gefährden, sondern darüber hinaus auch andere Internet-Nutzer beeinträchtigen würden<sup>896</sup>.

Es bestehen keine Einschränkungen in der Namenswahl. Es existieren keine Beschränkungen gegenüber generischen, ordinären oder beleidigenden Begriffen. Die gewählten Domainnamen müssen nicht in Verbindung mit deren Inhabern stehen. Es besteht keine Limitierung der Anzahl von angemeldeten Domainnamen je Inhaber. Der Inhaber muß weder Deutscher sein, noch seinen Sitz in Deutschland haben. Die fehlenden Einschränkungen ermöglichen es der DENIC eG den Registrierungsprozeß sehr schnell und billig zu gestalten. Die Genossenschaft muß keinen aufwendigen Verwaltungsapparat führen, um rechtliche Implikationen der Domainnamen zu prüfen. Durch die Neutralität der DENIC eG sollen alle Internetnutzer die gleichen Chancen haben und gleichzeitig die Kreativität in der Namenswahl gefördert werden.

Da die DENIC eG nicht selbst entscheiden kann, ob ein Dritter ein Vorrecht auf einen Domainnamen, gegenüber dem gegenwärtigen Inhaber hat, ist dieser Dritte zunächst gehalten, sich selbst mit dem Domaininhaber auseinanderzusetzen und diesen zur Übertragung des

---

<sup>893</sup> Vgl. die detaillierte Beschreibung des technischen Problems in *RFC 1535*, Gavron.

<sup>894</sup> Siehe *DENICeG*, FAQs / Domainregistrierung, Warum sind Domains unzulässig, die aus weniger als drei Zeichen bestehen?, 18. September 2001, <http://www.denic.de/doc/recht/faq/domainregistrierung.html#d0006>.

<sup>895</sup> Siehe *DENICeG*, FAQs / Domainregistrierung, Warum sind Domains unzulässig, die deutschen Kfz-Kennzeichen entsprechen?, 18. September 2001,

<http://www.denic.de/doc/recht/faq/domainregistrierung.html#d0008>.

<sup>896</sup> Das *LG Frankfurt a.M.* lehnte deshalb in einer Entscheidung vom 22. März 2000 auch einen Anspruch einer Telefongesellschaft auf die Domain 01051.de ab, MMR 2000, 627.

#### 4.4. Rechtliche Verantwortung der DENIC eG

---

Domainnamens auf sich beziehungsweise zur Freigabe zu bewegen. Obgleich die DENIC eG den Domainnamen erst nach einem Gerichtsurteil freigeben oder übertragen kann, ist es für den Dritte möglich, bei der DENIC eG einen sogenannten *Disput-Eintrag* für die streitbefangene Domain zu beantragen<sup>897</sup>. Mit einem solchen Eintrag wird vor allem verhindert, daß der Domaininhaber die Domain auf einen weiteren Dritten übertragen kann und sich somit der Auseinandersetzung mit einem eventuellen Anspruchsinhaber entzieht. Außerdem gewährleistet der zu Gunsten eines Dritten eingerichtete *Disput-Eintrag*, daß dieser automatisch neuer Domaininhaber wird, wenn der bisherige Domaininhaber die Domain freigibt. Mit dieser Regelung wird der Tatsache Rechnung getragen, daß einige Gerichte den bisherigen Domaininhaber nur zur Freigabe verpflichten, jedoch nicht zur Übertragung der streitgegenständlichen Domain verurteilen. Zur Beantragung eines *Disput-Eintrages* muß der eventuelle Anspruchsinhaber, neben der Versicherung, mit dem bisherigen Domaininhaber im rechtlichen Streit um die Domain zu stehen, Unterlagen (zum Beispiel Markenurkunden, Handelsregisterauszüge oder Kopie des Personalausweises) beifügen, aus denen sich ergibt, daß ihm an dem Domainnamen ein Recht zustehen könnte<sup>898</sup>. Mangels Prüfungsmöglichkeit durch die DENIC eG genügen jedoch nur Anhaltspunkte. Ein *Disput-Eintrag* ist auf ein Jahr befristet und wird danach wieder automatisch aufgehoben, kann jedoch verlängert werden, wenn die Auseinandersetzung mit dem Domaininhaber noch andauert. Wenn die Auseinandersetzung zu Ungunsten des dritten Anspruchstellers endet, ist dieser verpflichtet, dies der DENIC eG mitzuteilen und den *Disput-Eintrag* aufheben zu lassen. Das Erstellen sowie die Aufhebung des *Disput-Eintrages* sind derzeit kostenlos.

Schließlich ist es für einen Endkunden und Domaininhaber interessant zu wissen, wie er seinen ISP, über welchen er seinen Domainnamen angemeldet hat und welcher die technische Administration seines Domainnamens vornimmt, wechselt. Ein Wunsch zum Wechseln mag entstehen, wenn der Domaininhaber nicht mehr mit dem Service seines bisherigen Providers zufrieden ist oder eine preisgünstigere Alternative für ihn besteht. Um einen Providerwechsel zu erreichen, muß die Domain anstatt durch den alten ISP durch den Neuen gehostet werden. Ein Umzug der Domain ist natürlich nur unter den Voraussetzungen, welche im Vertrag mit dem bisherigen ISP bestimmt sind, möglich. Grundsätzlich muß zunächst der bisherige Provider über den Wechsel informiert und mit dem neuen Provider ein Vertrag über die Verwaltung der Domain geschlossen werden. Sodann sendet der neue ISP an die DENIC eG einen sogenannten KK-Auftrag (KK = Konnektivitätskoordination). Die DENIC eG fragt wiederum beim bisherigen Provider nach, ob der Domaininhaber dem Wechsel zugestimmt hat. Bei Bejahung der Zustimmung werden die technischen Angaben des Domainnamens auf den neuen Provider umgeschrieben. Die Domain ist damit übertragen.

---

<sup>897</sup> § 2 (3) DENIC-Registrierungsbedingungen, Fn. 885.

<sup>898</sup> Näheres zur Beantragung des Dispute-Eintrages siehe DENICeG, FAQs / Ansprüche, Wie bekomme ich einen Dispute-Eintrag (früher WAIT)?, 21. Mai 2001, <http://www.denic.de/doc/recht/faq/ansprueche.html#a0006>.

#### 4.4.2. Exkurs 2: Hoheitlicher Belang oder Privatsache

Wie eben festgestellt, erfolgt die Vergabe und Verwaltung der Domainnamen unter der TLD .de durch eine privatrechtliche Gesellschaft. Staatliche Akteure sind weder an dieser Gesellschaft noch an der eigentlichen Erfüllung der Aufgaben dieser Organisation beteiligt. Nach deutschem Recht könnte jedoch gerade eine Verpflichtung zur Involvierung staatlicher Gewalt bestehen. Dies läge nahe, wenn die DENIC eG durch ihre Arbeit deutsche Hoheitsbelange verletzt. Im Folgenden soll deshalb festgestellt werden, ob eine Vergabe durch den deutschen Staat technisch möglich wäre und ob eine Verpflichtung zur Vergabe von .de-Domainnamen durch die deutsche staatliche Verwaltung besteht.

Zunächst stellt sich die Frage, ob die Verwaltung des Internetnamensraumes, insbesondere die Vergabe von Domainnamen, durch den deutschen Staat selbst erfolgen kann. Auf Grund der jahrelangen technischen Betreuung durch die *Universität Karlsruhe* ist ersichtlich, daß eine staatliche Einrichtung in der Lage war, diese Aufgabe wahrzunehmen. Andererseits ist der Internetbetrieb in den letzten Jahren rasant angestiegen<sup>899</sup>. Geht man von einem weiteren durchschnittlichen jährlichen Wachstum der Domainadressen von 30% aus, so wäre eine Unterabteilung einer Universität bald überfordert. Ebenso müßten kontinuierlich hohe finanzielle Mittel in eine ausreichende technische Infrastruktur investiert werden. Auf Grund des derzeitigen Finanzmangels an deutschen Universitäten wäre zumindest zeitweise mit Engpässen zu rechnen. Nur eine eigenständige Einrichtung zur Vergabe der Domainnamen ist in der Lage, selbst für Personal und Finanzierung zu sorgen. Staatlicherseits müßten ihr genug finanzielle Mittel zur Verfügung gestellt werden, um einen gut laufenden Betrieb zu gewährleisten. Mit den derzeitigen Sparplänen des Bundes ist dies zwar kaum zu vereinbaren, im Hinblick auf die Verwaltung von Patenten und Marken durch staatliche Patent- und Markenämter jedoch keine undenkbare Aufgabe.

Eine Verpflichtung zum staatlichen Eingriff besteht, wenn durch die Vergabepaxis hoheitliche Belange tangiert werden. Dies könnte in der Verletzung von Normen des öffentlichen Rechts vorliegen. Der Staat ist selber verpflichtet, die Vergabe ganz oder teilweise zu übernehmen, wenn sie hoheitlichen Zwecken dienen würde.

Aus geschichtlicher Sicht erfolgte die Entwicklung und das Betreiben des DNS unter Förderung durch staatliche Stellen, insbesondere durch die Regierung der USA, in Deutschland, wie schon erwähnt, durch die *Universität Karlsruhe*. Die IANA erhielt zum Beispiel über 90% ihres Finanzhaushaltes durch den amerikanischen Staat<sup>900</sup>. Daraus ließe sich ableiten, daß auch die Vergabe der Domainnamen Aufgabe des Staates sei. Die Förderung von neuen Techniken und Verfahren fällt zwar in den staatlichen Aufgabenbereich, ist jedoch nicht zwingend ein hoheitlicher Belang. Ebenso wie viele andere wissenschaftliche Entwicklungen erfolgte der weitere Ausbau des DNS überwiegend im Privatsektor. Insbesondere erfolgt die

---

<sup>899</sup> Vgl. aktuelle DNS-Statistik des *Internet Software Consortiums*, Internet Domain Survey, <http://www.isc.org/ds>.

<sup>900</sup> Vgl. *Gigante*, J. Marshall J. Computer & Info. L. 413, 416 und 423 sowie *Goldfoot*, 84 Va. L. Rev. 909.

#### 4.4. Rechtliche Verantwortung der DENIC eG

---

Verwaltung der Namensräume der dem breiten Publikum zugänglichen internationalen *Top Level Domains* .com, .net und .edu seit Ende 1989 durch private Unternehmen. Aus der Entstehung des DNS im wissenschaftlich-staatlichen Bereich lässt sich kein hoheitlicher Zweck herleiten.

Man könnte den Domainnamensraum selbst als gesellschaftliches Gemeinvermögen ansehen<sup>901</sup>. Der Staat würde dann als Verwalter auftreten. Eine solche Verwaltung wäre erforderlich, wenn es nur eine begrenzte Anzahl an möglichen Domainnamen geben würde. Für jede praktische Anwendung lässt sich jedoch ein Domainnamen finden, da die Anzahl der Domainnamen unbegrenzt ist<sup>902</sup>. Ein Grund zur begrenzten Vergabe besteht nicht. Eine staatliche Verwaltung ist aus diesem Grund nicht notwendig.

Die Notwendigkeit eines einheitlichen DNS-Systems spricht dafür, daß es nur von einer einzigen Organisation betrieben wird. Auf diese Weise kann sichergestellt werden, daß der Namensraum des Internets nicht in mehrere Teile zerfällt und jeder Rechner im Internet erreicht werden kann. Um eine einheitliche Betreibung zu gewährleisten, spräche es dafür, den Staat als Regulierer oder Verwalter einzusetzen<sup>903</sup>. Um das Risiko einer monopolartigen staatlichen Vergabe zu vermindern, sollte jedoch eine offene privatrechtlich organisierte Gemeinschaft zugelassen werden, deren Mitglieder zwar eine einheitliche Datenbank der Domainnamen verwenden, aber bei der Namensregistrierung im freien marktwirtschaftlichen Wettbewerb stehen.

Würde allerdings der Staat die Vergabeaktivität kontrollieren, so hätte die Öffentlichkeit die Möglichkeit, auf die Politik der Vergabegesellschaft Einfluß zu nehmen, in dem sie in Wahlen für diejenigen Personen stimmt, welche die gewünschte Position vertreten. Im Gegensatz dazu, hat die Öffentlichkeit keine formale Möglichkeit auf die Tätigkeiten und Aktionen einer privaten Gesellschaft Einfluß zu nehmen. Diesem Problem können jedoch verschiedene Punkte entgegengestellt werden. Zum einen muß eine solche Vergabegesellschaft den Internetnormen eines offenen Prozesses und freier Beteiligung unterliegen. Zweitens stehen die einzelnen Mitglieder einer Vergabegesellschaft im marktwirtschaftlichen Wettbewerb zueinander. Um Kunden zu akquirieren, werden sie versuchen, kundenfreundliche und marktkonforme Entscheidungen zu treffen. Schließlich bildet das Kartellrecht eine Grenze, die wettbewerbsbehindernde Absprachen der einzelnen Mitglieder untereinander verhindert.

Ein hoheitlicher Grund zur staatlichen Verwaltung könnte sich jedoch durch die Beteiligung von UN-Organisationen am Weiterentwicklungsprozeß des DNS ergeben. Seit 1998 liefern Verhandlungen zwischen der IANA beziehungsweise jetzigen ICANN und dem Generalsekretariat der *International Telecommunications Union* (ITU) sowie der *World Intellectual Property Organization* (WIPO) über eine Neugestaltung des DNS. Inzwischen wurde ein

---

<sup>901</sup> Vgl. *Gigante*, J. Marshall J. Computer & Info. L. 413, 423.

<sup>902</sup> Vgl. *NSI*, Enhancing Internet, Kap. The Goals, 3.

<sup>903</sup> Vgl. *Gordon*, Controlling the Internet, Kap. 2.3.

neues Vergabeverfahren eingeführt, welches einen Wettbewerb bei der Vergabe zuläßt und ebenso einen Streitbeilegungsmechanismus bei Namensstreitigkeiten beinhaltet (siehe die UDRP der WIPO, Kapitel 3.3.1.2 oben). Auch die *Bundesrepublik Deutschland* gehörte den bei den Verhandlungen beteiligten UN-Organisationen an und war damit indirekt in die Beratungen integriert. Im Unterschied zur UNO-Generalversammlung oder anderen Unterorganisationen (zum Beispiel zur *World Health Organization*) beschäftigen sich diese beiden Organisationen auch mit rein privatrechtlichen Fragen. Eine Aufgabe der ITU ist es zum Beispiel, die Zusammenarbeit im Telefondienst zu fördern und dabei einheitliche Bestimmungen durchzusetzen<sup>904</sup>. Die WIPO bemüht sich um den Schutz von geistigen Eigentum<sup>905</sup>, welches regelmäßig dem privaten Bereich entspringt. Somit läßt sich auch aus einer Teilnahme dieser Organisationen am Beratungsprozeß nicht schließen, daß es sich bei der Verwaltung der Domainnamen um hoheitliche Angelegenheiten handelt<sup>906</sup>.

Schließlich könnte sich die Verpflichtung zu einer staatlichen Verwaltung der deutschen TLD direkt aus dem Grundgesetz, insbesondere dem Art. 87f Abs. 1 GG beziehungsweise aus dem korrelierenden TKG ergeben. Gemäß dem im Jahre 1994 eingeführten Art. 87f Abs. 1 GG gewährleistet der Bund im Bereich der Telekommunikation flächendeckend angemessene und ausreichende Dienstleistungen. Dann müßte der Betrieb des DNS als Teil des Internets zur Telekommunikation zu rechnen sein. Umstritten ist jedoch schon inwieweit die Anbindung an das Internet selbst unter die Telekommunikation zu zählen ist. Das BVerfG hatte schon in seinem „Ersten Rundfunkurteil“ von 1960 unter den Vorgängerbegriff der Telekommunikation, dem Fernmeldewesen nur den sendetechnischen Akt der Übermittlung von Daten, also das Senden und Empfangen, eingeordnet<sup>907</sup>. Das Fernmeldewesen umfaßt nach dieser Entscheidung nur die der Übermittlung von Signalen dienenden technischen Vorgänge. Es beginnt erst mit der Übermittlung des fertigen Signals. Zunächst ist hier zwischen dem reinen Übertragungstechnischen Bereich und dem Bereich des Inhaltes zu unterscheiden. Um das Internet betreiben zu können, ist aus technischer Sicht zunächst ein Akt der Datenübertragung im Sinne eines Empfangens und Sendens von digitalen Informationen erforderlich. Die nach dem Schichtenmodell des Internets als Basis dienende Ebene der Hardware (wie zum Beispiel die Telefonleitungen oder Glasfaserkabel) läßt sich zweifellos zur Übertragungstechnik zuordnen. Folglich wird die technische Seite der Übertragung von Daten im Internet vom Telekommunikationsbegriff des Art. 87f Abs. 1 GG erfaßt<sup>908</sup>. In diesen Bereich fällt die Ermöglichung eines Netzzuganges, wie die Verbindung des heimischen Computers zu einem Internetprovider. Diese Grundvoraussetzungen für den Heimgebrauch des Internets lassen sich heutzutage über die ebenfalls dem Art. 87f Abs. 1 GG unterfallende Telefonkommunikation gewährleis-

---

<sup>904</sup> Zur ITU siehe deren Informationsseite: *ITU*, About the International Telecommunication Union, 6. März 2000, <http://www.itu.int/aboutitu/>. Siehe auch *Harbecke*, 50 Jahre UNO, S. 83f. Auf die ITU wird im Kap. 2.4.1.2.1 näher eingegangen.

<sup>905</sup> Vgl. die eigene Kurzdarstellung der WIPO: *WIPO*, About WIPO, <http://www.wipo.org/about-wipo/en/>. Siehe auch *Harbecke*, 50 Jahre UNO, S. 85.

<sup>906</sup> Ebenso DBT-Dr. 13/7764 vom 27. Mai 1997.

<sup>907</sup> *BVerfG* vom 28. Februar 1991, *BVerfGE* 12, 205, 226f. Vgl. auch *Röger*, *ZRP* 1997, 203, 204.

<sup>908</sup> So auch *Röger*, *ZRP* 1997, 203, 205.

#### 4.4. Rechtliche Verantwortung der DENIC eG

---

ten. Es besteht damit eine gewisse Parallelität zwischen der Verpflichtung einer Grundversorgung mit Sprachtelefonie und der technischen Internetanbindung<sup>909</sup>. Erfaßt vom Begriff der Telekommunikation wird jedoch nicht die inhaltliche Seite der übertragenen Daten. Nach Art. 87f Abs. 1 GG ist der Bund nicht verpflichtet, ein bestimmtes inhaltliches Angebot im Internet zu gewährleisten<sup>910</sup>.

Schwieriger unter den Telekommunikationsbegriff einzuordnen ist jedoch die dem Internet inhärente Grundstruktur, wie die das Internet charakterisierenden TCP/IP-Protokolle oder das der Anwendungsschicht zuzuordnende DNS. Ohne diese Grundstrukturen ist eine Kommunikation im Internet nicht möglich. Insbesondere erfolgt mittels dem TCP/IP sowie dem DNS, die eigentliche Adressierung des Zielobjekts (wie zum Beispiel Mailboxen oder WWW-Seiten). Der Betrieb dieser Grundstrukturen, wie die Zuweisung von IP-Adressen oder Domainnamen ist folglich nicht der eigentlichen Inhaltsanbietung gleichzustellen. Das Routing von Informationen im Internet mittels IP-Adressen und Domainnamen erfolgt nicht auf der Ebene der Hardware, vielmehr entscheidet die zugrundeliegende Software im Einzelfall über das anzuwendende Adressierungsverfahren oder den zu nutzenden Übertragungsweg im Internet. Das System des TCP/IP ist so konstruiert worden, daß es unabhängig von den aktuell benutzten Leitungen agieren kann. So kann ein Datenstrom im Internet bei Ausfall eines Übertragungsweges auf einen anderen umgeleitet werden. Darüber hinaus sind die kommunizierenden Rechner nur soweit zur Einhaltung der Standardspezifikationen des DNS verpflichtet, wie sie fremde Dienste in Anspruch nehmen. Es steht folglich Nutzern offen, über das grundgesetzlich gesicherte Telefonnetz ein eigenes internetähnliches Datennetz aufzubauen, das gegenüber dem herkömmlichen Internet abweichende Spezifikationen aufweist. Die das Internet charakterisierenden Protokolle und Adressierungsmechanismen unterfallen damit nicht dem Telekommunikationsbegriff des Art. 87f Abs. 1 GG, sondern stellen vielmehr ein zwischen Inhaltsanbietung und Telekommunikation liegende dritte Kategorie dar. Die Verwaltung des DNS wird folglich nicht von der Grundversorgungsverpflichtung des Art. 87f Art. 1 GG erfaßt.

Sollte man die Infrastruktur dennoch der Telekommunikation zuordnen, ist zu bedenken, daß zwar der Staat Adressat des von Art. 87f GG geforderten Grundversorgungsauftrages ist, dieser aber nicht verpflichtet ist, die Grundversorgung selbst durch eigene staatliche Organisationen sicherzustellen. Er darf vielmehr die Adreß- und Namensvergabe nicht selbst bewältigen, sondern muß sich vielmehr nach Art. 87f Abs. 2 GG darauf beschränken, die Dienstleistungen durch private Unternehmen erbringen zu lassen<sup>911</sup>. Ein Eingreifen wäre nur dann gerechtfertigt, wenn die Grundversorgung nicht mehr gewährleistet ist. Sollte man das DNS dem Grundversorgungsauftrag zuordnen, so wäre ein staatliches Eingreifen nur dann möglich, wenn die DENIC eG ihren Service einstellen oder extrem hohe Gebühren verlangen sollte.

---

<sup>909</sup> Zur darüber hinausgehenden Verpflichtung zum Aufbau eines staatlichen Backbone-Netzes siehe *Mecklenburg*, ZUM 1997, 525, 534f.

<sup>910</sup> *Mecklenburg*, ZUM 1997, 525, 533.

<sup>911</sup> Vgl. *Röger*, ZRP 1997, 203, 206.

Auf Grund der Bedeutung von Domainnamen ist derzeit jedoch nicht mit einer Einstellung der deutschen TLD .de zu rechnen. Weiterhin sind die Mitglieder des DENIC eG vorrangig dem Wettbewerbsrecht ausgesetzt. Sollte die DENIC eG unberechtigt ihre Preise in die Höhe treiben, käme zunächst ein Eingreifen staatlicher Behörden gemäß dem GWB in Betracht, ehe der Staat eine eigene Regelungsautorität bezüglich der Domainvergabe an sich ziehen könnte.

Offen bleibt, ob das 1996 eingeführte TKG über die Verfassungsvorgaben hinausgehende Verpflichtungen setzt. Das TKG soll zunächst die Vorgaben des Art. 87f Abs. 1 GG einer Grundversorgung im Bereich der Telekommunikation umsetzen<sup>912</sup>. Die §§ 1 und 18 TKG sehen deshalb die Gewährleistung „angemessener und ausreichender Dienstleistungen“ vor. Eine nähere Begriffsbestimmung erfolgt im § 17 TKG, welcher Universaldienstleistungen im Sinne des TKG als Telekommunikationsdienstleistungen aus den Bereichen des Sprachtelefondienstes und des Betreibens von Übertragungswegen bestimmt, soweit deren Erbringung für die Öffentlichkeit als Grundversorgung unabdingbar geworden ist<sup>913</sup>. Darüber hinaus ist die Bundesregierung ermächtigt, mittels einer Verordnung weitere Dienstleistungen als Universaldienstleistungen zu bestimmen, § 17 Abs. 1 Satz 3, Abs. 2 TKG. In der Telekommunikations-Universaldienstleistungsverordnung (TUDLV<sup>914</sup>) von 1997 werden jedoch neben ISDN-Zusatzleistungen (§ 1 Nr. 1 TUDLV), dem Betreiben von Auskunftsstellen und Telefonzellen (§ 1 Nr. 2 a und c TUDLV) sowie der Herausgabe von Telefonbüchern keine Bestimmungen hinsichtlich des Betreibens des Internets aufgestellt. Damit folgen aus diesem Mindestkatalog hinsichtlich des Internets keine über Art. 87f Abs. 1 GG hinausgehenden Pflichten für den Bund.

Schließlich weist § 43 Abs. 1 Satz 1 TKG der deutschen RegTP die Aufgabe der Numerierung zu. Sollten sich die IP-Adressen als solche Nummern klassifizieren lassen, so könnte man eine entsprechende Autorität der RegTP auch über das deutsche DNS annehmen. Insbesondere obliegt der RegTP die Strukturierung und Ausgestaltung des Nummernraumes mit dem Ziel, jederzeit den Anforderungen von Nutzern, Betreibern von Telekommunikationsnetzen und Anbietern von Telekommunikationsdienstleistungen zu genügen, § 43 Abs. 1 Satz 2 TKG. Nach § 3 Nr. 10 TKG sind Nummern Zeichenfolgen, die in Telekommunikationsnetzen Zwecken der Adressierung dienen. Auch hier ist in Bezug auf Art. 87f Abs. 1 GG auf die zugrundeliegende Technik zur Datenübermittlung abzustellen und nicht auf die in den übermittelten Daten beinhalteten Adressinformationen des Internets. Nummern im Sinne des § 43 Abs. 1 TKG sind somit nur als die herkömmlichen Rufnummern zur Adressierung der Sprachtelefonie zu verstehen<sup>915</sup>. Diese Auslegung wird auch vom historischen Hintergrund des TKG gedeckt. Das TKG sollte zur Entflechtung des ursprünglichen Telefondienstmonopols der *Deutschen Bundespost* und der aus dieser abgespaltenen *Telekom AG* beitragen. Diese zwei Unternehmen nahmen zu keinem Zeitpunkt die Vergabe von IP-

---

<sup>912</sup> Siehe *Kubicek*, CR 1997, 1, 8.

<sup>913</sup> Zu § 17 TKG siehe *Kubicek*, CR 1997, 1, 8 und *Mecklenburg*, ZUM 1997, 525, 532ff.

<sup>914</sup> Telekommunikations-Universaldienstleistungsverordnung, 30. Januar 1997, BGBl. I 1997, 141.

<sup>915</sup> So auch *Koenig/Neumann*, K&R 1999, 145, 148ff. Auch die Bundesregierung ist der Ansicht, daß zumindest Domainnamen nicht unter § 3 Nr. 10 TKG fallen, DBT-Dr. 13/7764 vom 27. Mai 97.

#### 4.4. Rechtliche Verantwortung der DENIC eG

---

Adressen beziehungsweise Domainnamen vor<sup>916</sup>. Aus historischen Gesichtspunkten ist somit nicht gerechtfertigt, daß nunmehr der Bereich der Internetnumerierung staatlicher Regulation unterfallen soll. Darüber hinaus erscheint es wenig sinnvoll, die IP-Adressierung unter nationalstaatlicher Verwaltung zu stellen, obwohl gerade die IP-Adressen in keinem staatlichen Zusammenhang stehen und nicht wie die Telefonnummern an Ländergrenzen gebunden sind. Der § 43 Abs. 1 TKG weist folglich der RegTP keine Autorität über das IP-System und dem darauf beruhenden DNS zu.

Bei der Reservierung und Verwaltung von Domainnamen im Internet werden damit keinerlei Belange hoheitlicher Art tangiert. Eine Verpflichtung zur staatlichen Vergabe besteht nicht.

##### **4.4.3. Unterlassungs- und Freigabeansprüche**

Das Recht Domainnamen ohne staatlichen Einfluß zu vergeben und zu verwalten entbindet die DENIC eG jedoch nicht vor Rückgriffen von Marken- und Namensrechtsinhabern, soweit diese gehindert sind, gegen die eigentlichen Domaininhaber rechtlich vorzugehen. Gegen die DENIC eG könnten dabei eine Reihe von Anspruchsgrundlagen auf Freigabe von Domainnamen oder Unterlassung der Reservierung einschlägig sein. Man kann eine täterschaftliche oder mittäterschaftliche Verletzung kennzeichen- oder wettbewerbsrechtlicher Tatbestände (zum Beispiel §§ 14, 15 MarkenG, § 12 BGB gegebenenfalls in Verbindung mit § 823 BGB, § 1 UWG), eine Beihilfe zu derartigen Verletzungshandlungen (§ 830 Abs. 2 BGB), eine Störerhaftung analog § 1004 BGB in Verbindung mit den verletzten kennzeichen- oder markenrechtlichen Normen und schließlich Ansprüche aus kartellrechtlichen Vorschriften (§§ 20 Abs. 1, 33 GWB) erwägen.

Aus objektiver Sicht, ist für eine Verletzung von Kennzeichen- beziehungsweise Markenrechten genügend, wenn der Handelnde an der Schaffung oder Aufrechterhaltung eines rechtswidrigen Zustandes mitwirkt. Dazu ist es ausreichend, wenn der in Anspruch Genommene die eigenverantwortliche Handlung eines Dritten unterstützt oder ausgenutzt hat und die zur Vermeidung der Rechtsverletzung gebotenen und zumutbaren Maßnahmen unterläßt<sup>917</sup>. Insoweit kommt eine mittelbare Markenbenutzung auch durch die DENIC eG in Betracht, weil sie mit der Vergabe von Domainnamen einen Verursacherbeitrag für die Zeichenverletzung der Person leistet, die den jeweiligen Domainnamen anmeldet<sup>918</sup>. Auch eine Namensanmaßung im Sinne § 12 BGB könnte durch die DENIC eG vorliegen, soweit sie unbefugt den Namen eines Dritten gebraucht und dadurch ein schutzwürdiges Interesse des Namensträgers verletzt. Eine Bejahung einer direkten Namensverletzung erscheint allerdings unter dem Blickwinkel schwierig, daß die DENIC eG die Domainnamen nicht selbst erfindet oder auswählt, sondern

---

<sup>916</sup> Vgl. *Koenig/Neumann*, K&R 1999, 145, 149.

<sup>917</sup> Vgl. *BGH* vom 12. Oktober 1989, „Schönheitschirurgie“, GRUR 1990, 373ff.; *OLG München* vom 9. März 1995, „Die 500 besten Anwälte“, WRP 1995, 866ff. und *OLG Düsseldorf* vom 21. November 1995, WRP 1996, 559, 562f.

<sup>918</sup> Vgl. *OLG Frankfurt a.M.* vom 14. September 1999, „ambiente.de“, MMR 2000, 36, 38; *LG Frankfurt a.M.* vom 24. Mai 2000, „Dresdner-Hypovereinsbank.de“, CR 2001, 51f. Ausführlich hierzu *Bettinger/Freytag*, CR 1999, 28, 32.

diese nur auf Wunsch der Interessenten in den Namensserver einträgt<sup>919</sup>. Jedoch ist diese Eintragung kausal für die Namensverletzung durch den Domainbenutzer. Ohne die Eintragung sind Namensverletzungen nicht möglich, so daß eine mittäterschaftliche Namensverletzung im Sinne §§ 830 Abs. 1 und 2, 12 BGB vorliegen kann. Für ein objektiv wettbewerbswidriges Verhaltens im Sinne § 1 UWG reicht wiederum aus, wenn die DENIC eG vorsätzlich den ebenfalls vorsätzlich begangenen Verstoß eines Dritten fördern will oder billigend in Kauf nimmt. Dazu würde genügen, wenn die DENIC eG nach Kenntnis der Rechtswidrigkeit eines besetzten Domainnamens diesen nicht sperren, beziehungsweise erneut freigeben würde<sup>920</sup>.

Ohne näher auf die einzelnen Tatbestandsmerkmale der oben genannten Anspruchsgrundlagen einzugehen, käme ein Ausschluß der Haftung gegebenenfalls nach § 5 Abs. 2 und 3 TDG in Betracht. Nach § 5 Abs. 1 TDG sind Diensteanbieter für eigene Inhalte stets nach den allgemeinen Gesetzen verantwortlich. Halten Diensteanbieter fremde Inhalte bereit, sind sie nur dann verantwortlich, wenn sie Kenntnis von diesen Inhalten erlangt haben und ihnen zumutbar ist, die Nutzung zu verhindern, § 5 Abs. 2 TDG. Sollte der Diensteanbieter lediglich den Zugang zu fremden Inhalten vermitteln, stellt § 5 Abs. 3 TDG schließlich diese von der Haftung frei. Das TDG stellt jedoch auf den Inhalt gespeicherter Daten ab. Internetadressen stellen jedoch eher Daten dar, welche dem technischen Übermittlungsvorgang dienen, beinhalten aber keinen darüber hinausgehenden Inhalt. Als Inhalt im Sinne des TDG sind erst diejenigen Informationen zu betrachten, die von den adressierten Computern abgerufen werden können. Eine gesetzliche Haftungsregelung ist nur für diese Informationen vorgesehen worden. Damit entfällt eine direkte Anwendung des § 5 Abs. 2 und 3 TDG<sup>921</sup>. Auch für eine analoge Anwendung des TDG ist kein Raum, da keine planwidrige Regelungslücke ersichtlich ist. Insoweit stellt das TDG klar auf eine Inhaltsregelung ab, obgleich schon 1997 bei der Verabschiedung des Gesetzes die Haftung der DENIC eG in Frage gestellt wurde<sup>922</sup>.

Bei der Klärung, ob die DENIC eG endgültig gegenüber den in ihren Rechten verletzten Personen haftet, ist es jedoch gerechtfertigt, die Grundsätze des Presserechts heranzuziehen<sup>923</sup>. Danach ist die Prüfungspflicht eines Verlegers bei Veröffentlichungen von Werbeanzeigen auf grobe und eindeutige Rechtsverstöße beschränkt<sup>924</sup>. Eine volle Haftung kommt danach nur unter besonderen Umständen in Betracht, insbesondere muß es der DENIC eG möglich sein, die spezielle Rechtsverletzung zu verhindern<sup>925</sup>. Bei der Beurteilung der rechtlichen und

<sup>919</sup> Im Ganzen ablehnend hierzu *Bettinger/Freytag*, CR 1999, 28, 32f. und *OLG Dresden* vom 28. November 2000, „kurt-biedenkopf.de“, GRUR-RR 2001, 130.

<sup>920</sup> Vgl. *OLG Frankfurt a.M.* vom 14. September 1999, „ambiente.de“, MMR 2000, 36, 38 und *OLG Dresden* vom 28. November 2000, „kurt-biedenkopf.de“, GRUR-RR 2001, 130.

<sup>921</sup> Vgl. auch *OLG Frankfurt a.M.* vom 14. September 1999, „ambiente.de“, MMR 2000, 36, 38; *Nordemann*, NJW 1997, 1897, 1900f. und *Bettinger/Freytag*, CR 1999, 28, 31.

<sup>922</sup> So z.B. durch *Nordemann*, NJW 1997, 1897, 1900f. Vgl. auch *Bettinger/Freytag*, CR 1999, 28, 31.

<sup>923</sup> So schon *Bücking*, Domainrecht, Rdnr. 249. Vgl. auch *OLG Frankfurt a.M.* vom 14. September 1999, „ambiente.de“, MMR 2000, 36, 37f.

<sup>924</sup> Zur Haftung im Presserecht siehe *BGH* vom 26. April 1990, „Pressehaftung I“, GRUR 1990, 1012 und vom 7. Mai 1992, „Pressehaftung II“, GRUR 1992, 618.

<sup>925</sup> Vgl. *BGH* vom 10. April 1997, „Branchenbuch-Nomenklatur“, GRUR 1997, 909.

#### 4.4. Rechtliche Verantwortung der DENIC eG

---

tatsächlichen Möglichkeiten zur Verhinderung der Rechtsverletzung ist darauf abzustellen, ob erfolgversprechende Maßnahmen mit zumutbarem Aufwand zu treffen wären. Entsprechend der Haftung im Presserecht ist es nicht gerechtfertigt, der DENIC eG unzumutbare Prüfungspflichten aufzuerlegen. Abzuwägen ist hierbei das Interesse der Rechtsinhaber gegenüber dem Interesse der Allgemeinheit an einer effektiven und reibungslosen Vergabapraxis. Die Hauptaufgabe der DENIC eG besteht in der kostengünstigen und schnellen Verwaltung des deutschen DNS und der Registrierung neuer Domainnamen unter der TLD .de. Derzeit werden monatlich über hunderttausend neue Domainnamen bei der deutschen Vergabestelle reserviert. Dabei kann es der DENIC eG nicht zugemutet werden, umfangreiche rechtliche Prüfungen anzustellen und sogar Rechtsbeziehungen zwischen Antragssteller und der Person, welche eine Rechtsverletzung geltend macht, zu prüfen. Bei der Prüfung jedes einzelnen Domainnamens käme zum einen die Zulassung neuer Domainnamen fast zum erliegen und würde zum anderen die Kosten für diese erheblich in die Höhe treiben. Die damit einhergehende Verhinderung der zur Gesamtanzahl an Domainnamen verhältnismäßig wenigen Streitigkeiten, würde schließlich auf Kosten der Mehrzahl der Internetnutzer gehen. Ein Anspruch auf Löschung und Neuvergabe eines Domainnamens gegenüber der DENIC eG kann deshalb nur dann in Betracht kommen, wenn die Registrierung offensichtlich rechtswidrig war. Ein offensichtlicher Rechtsverstoß kann aber erst bei Vorliegen eines Gerichtsurteils oder bei der Verwendung von berühmten Kennzeichen als Domainnamen angenommen werden<sup>926</sup>. Es kann nicht Aufgabe einer privaten Vereinigung sein, selbst zu untersuchen, ob ein gewählter Domainname fremde Rechte verletzt. Eine solch weitgehende Prüfung muß weiterhin den staatlichen Gerichten vorbehalten bleiben. Deshalb kann es nicht genügen, wenn ein Kennzeicheninhaber gegenüber der DENIC eG zum Beispiel mittels eines Abmahn schreibens diese Feststellungen selbst behauptet. Der Vergabestelle ist es auch nicht möglich, zum Beispiel bestehende Markenrechte untereinander in Bezug auf Priorität oder Branchenähnlichkeit und Zuordnungsverwirrung hin zu überprüfen<sup>927</sup>. Nur bei Vorlage eines rechtskräftigen Urteils kann es für die DENIC eG evident sein, daß eine entgegensätzliche Rechtslage nicht besteht<sup>928</sup>. In einem solchen Fall wäre sie dann zur Freigabe des Domainnamens verpflichtet.

---

<sup>926</sup> So auch *OLG Frankfurt a.M.* vom 14. September 1999, „ambiente.de“, MMR 2000, 36, 38 und *OLG Dresden* vom 28. November 2000, „kurt-biedenkopf.de“, GRUR-RR 2001, 130.

<sup>927</sup> *OLG Frankfurt a.M.* vom 14. September 1999, „ambiente.de“, MMR 2000, 36, 38.

<sup>928</sup> Inzwischen hat der *BGH* vom 17. Mai 2001, „ambiente.de“, BGHZ 148, 13 die Entscheidung des *OLG Frankfurt a.M.* vom 14. September 1999, „ambiente.de“, MMR 2000, 36, 38 bestätigt.

*Change is possible. I don't doubt that revolutions lie in our future. The open source code movement is just such a revolution. But I fear. . . that too much is at stake to allow the revolutionaries to succeed.*

– Lawrence Lessing – *Code: and Other Laws of Cyberspace* –

*Aber die Regierung, ICANN, hat das nicht gewollt. Weil, sie bestand selbst aus Juristen. Und, sie trugen Krawatten, die ja bekanntlich die Sauerstoffzufuhr zum Gehirn einschränken. Und deswegen hatten Sie keine Phantasie und haben das auch gar nicht verstanden, wozu man so einen öffentlichen Raum braucht, oder was ein Paralleluniversum ist.*

– Andy Müller-Maguhn – *Regierungserklärung* –

## 5. Alternativen zum jetzigen DNS

Die derzeitige hierarchische Organisation des DNS ist nicht unbedingt notwendig. Alternative Formen der Organisation sind technisch möglich und würden einen intensiveren Wettbewerb ermöglichen. Einen ersten und wichtigen Schritt in diese Richtung stellte die Umstellung des Registrierungssystems der generischen TLDs von der alleinigen Vergabe der Domains durch die NSI auf ein System von vielen im Wettbewerb stehenden *Registrars* dar. Außerdem wurden neue *Registries* zugelassen und damit der Wettbewerb bei der Domainvergabe erneut erhöht. Eine Akkreditierung neuer *Registrars* und neuer *Registries* ist jedoch auch weiterhin durch die ICANN nötig. Niemand kann effektiv Domainnamen registrieren und vergeben, ohne in die zugrundeliegenden Datenbanken eingreifen zu können. Eine freie Erweiterung des TLD-Namensraumes ist ohne Genehmigung durch die ICANN nur in begrenzten Umfang möglich, da ein Eintrag neuer TLDs im *A Root Server* erforderlich ist, um einen Zugriff auf diese für alle Internetnutzer zu gewährleisten. Die ICANN ist nicht nur ein Wächter über das Produkt „Domainname“. Sie kann bestimmen, welche Unternehmen am lukrativen Geschäft der Domainvergabe teilnehmen dürfen und welchen Service die Registrierungsstellen anbieten müssen. Folglich ist sie mehr als eine Standardisierungsorganisation<sup>929</sup>. Dies führt zu einer verstärkten Suche nach Alternativen zum von der ICANN verwalteten DNS, die in diesem letzten Kapitel erörtert werden sollen. Man kann zwischen zwei Gruppierungen unterscheiden. Zum einen existiert eine Anzahl von Ansätzen, welche die Technik des DNS verwenden

---

<sup>929</sup> Goldfoot, 84 Va. L. Rev. 909 951

## 5.1. Alternativen innerhalb des DNS

---

beziehungsweise erweitern. Zum anderen existieren außerhalb des DNS Verzeichnissysteme, die nur bedingt auf dem DNS der ICANN basieren.

### 5.1. Alternativen innerhalb des DNS

Ein Hauptproblem des DNS stellt für den Endanwender die begrenzte Verfügbarkeit von gTLDs dar. Unter den zwei wichtigsten gTLDs .com und .net sind fast alle prägnanten Wörter und Abkürzungen belegt. Viele neue Internetnutzer müssen feststellen, daß ihr geplanter Internetauftritt unter der von ihnen vorgesehenen Internetadresse nicht mehr möglich ist, da die Domain bereits registriert wurde. Ein Ausweichen auf ccTLDs erweist sich wegen der inzwischen ähnlich hohen Registrierungsdichte häufig als schwierig und entspricht zweitens oft nicht einer gewünschten internationalen Repräsentation.

Ein sogenanntes *Domain Sharing* sollte für mehrere Interessenten dieselbe Domain zugänglich machen, indem auf der Startseite einer Homepage auf verschiedene Angebote unter diesem Namen hingewiesen würde. Dieses Verfahren konnte sich nur in den seltensten Fällen durchsetzen. Die Vergabe nach dem Prinzip „first come, first served“ an private Personen führte dazu, daß Personen, welche eine begehrte Adresse registriert hatten, sich auch schnell deren Wert bewußt wurden und folglich nicht bereit waren, diesen Vermögenswert mit anderen zu teilen. Ein *Domain Sharing* kann nur unter Zwang durchgesetzt werden. Dazu wäre aber eine Organisation notwendig, die zu entscheiden hätte, welche Angebote einem Domännamen zuzuordnen wären. Die hohen Kosten des notwendigen Verwaltungsaufwand müßten an die Registrierenden weitergegeben werden und würden folglich zu einer Preiserhöhung der Registrierungskosten für die einzelnen Domains führen. Dies würde schließlich dem Ziel einer möglichst wettbewerbsfördernden und preissenkenden Erweiterung des DNS widersprechen.

Als Folge der schwerfälligen Einführung neuer TLDs durch die das DNS verwaltenden Organisationen gibt es immer wieder Versuche, ein alternatives *Root Server System* einzuführen. Hinter diesen *Alternative Roots* stehen zum größten Teil private Unternehmen, welche ebenfalls mit der Registrierung von Domännamen Geld verdienen möchten, ohne offiziell von der ICANN (damals von der US-NSF und der IANA) anerkannt zu sein. *Alternative Roots* sollen die Möglichkeit bieten, auch Angebote unter Adressen wie [www.antitrust.law](http://www.antitrust.law) in das Internet stellen zu können. Um eine alternative TLD für alle Nutzer des Internets zugänglich zu machen, müßten diese in die von der ICANN offiziell anerkannte Datenbank der *Root Server* eingetragen werden. Ein solche Eintragung ist nur für die von der ICANN akzeptierten TLDs vorgesehen, so daß die Betreiber von *Alternative Roots* eigene *Root Server* betreiben müssen. Domains unter den inoffiziellen TLDs können von einem Anwender nur erreicht werden, wenn der ISP des Endnutzers die Auflösung von Domännamen in IP-Nummern der korrespondierenden Computer über einen solchen alternativen *Root Server* vornimmt oder der Endnutzer eine spezielle Software zur Umsetzung der Domännamen verwendet.

Einen der ersten *Alternative Roots* wurde durch *AlterNIC, Inc.* betrieben<sup>930</sup>. Dieser *Root Server* und die damit zusammenhängende *Registry* für die alternativen TLDs gingen im März 1996 online. Kashpureff, der Gründer von AlterNIC, wollte mittels seines alternativen *Root Servers* eine dezentralisierte Verwaltung der TLDs gründen. Dazu bot er selbst neun neue TLDs an<sup>931</sup> und ließ zu, daß seine Kunden ebenfalls ihre eigenen TLDs mittels *AlterNIC* anbieten konnten und verwies zusätzlich auf weitere alternative *Registries*. Mit verschiedenen kleinen ISPs und weiteren Betreibern alternativer *Registries* erfolgte im Januar 1997 ein Zusammenschluß zum *Enhanced Domain Name System* (eDNS)<sup>932</sup>. Wie schon *AlterNIC*, wollte man mit eDNS ein Modell des freien Marktes für TLDs einführen, in welchem eine unbegrenzte Anzahl von *Registrars* eine unbegrenzte Anzahl von TLDs anbieten sollten. Da man sich auf Dauer jedoch nicht einigen konnte, wie das eDNS betrieben werden sollte, zerbrach das Projekt und *AlterNIC* und weitere ISPs gründeten das *Universal Domain Name System* (uDNS)<sup>933</sup>. Die Organisationen eDNS und uDNS betrieben in der Folgezeit im gegenseitigen Wettbewerb alternative *Root Server* und standen damit auch im Wettbewerb zum offiziellen *Root Server* der damaligen IANA. Zur Verwirrung der Endnutzer kam hinzu, daß durch das IAHC und des gTLD-MoU die Einführung weiterer TLDs geplant waren, welche zum Teil schon von alternativen *Registries* betrieben wurden.

Einen solchen Fall stellte die TLD .web dar, welche durch das gTLD-MoU und des IAHC eingeführt werden sollte, aber als alternative TLD seit 1. August 1996 von *Image Online Design* (IOD) unter Leitung von Christopher Ambler betrieben wird<sup>934</sup>. IOD gehört zu den ausdauernden Firmen, welche auch heute noch versuchen, eine Alternative zum DNS der ICANN zu bieten. Als Betreiber der .web TLD mußte IOD befürchten, der Grundlage ihrer TLD beraubt zu werden. Im Gegensatz zu IODs .web TLD sollten die im gTLD-MoU beschlossenen neuen TLDs direkt in das Rootverzeichnis der IANA eingehen. Solange für IOD keine Möglichkeit bestand, vom gTLD-MoU als *Registry* für die TLD .web anerkannt zu werden, wäre der von ihr angebotene Service wertlos geworden. Um die Umsetzung des gTLD-MoU zu verhindern, verklagte IOD daraufhin die an dem neuen Projekt beteiligte IANA und das IAHC sowie deren Vorsitzende<sup>935</sup>. IODs Ziel war es, IANA davon abzuhalten, anderen Unternehmen ein Vermarktungsrecht der TLD .web zu gewähren und gegebenenfalls einen Schadensersatz wegen Geschäftsschädigung durch Einführung von .web zugesprochen zu bekommen. Darüber hinaus wollte IOD vom Gericht feststellen lassen, daß die IANA die *Registry* von IOD für .web autorisiert habe. Als Hintergrundinformation muß jedoch erwähnt wer-

---

<sup>930</sup> AlterNIC ist unter <http://www.alternic.org> zu erreichen. Näheres zu AlterNIC siehe *Rony/Rony, Domain Name Handbook*, S. 517ff. Zur Gründung von AlterNIC siehe auch *UnixInsider, Lawton, New top-level domains promise descriptive names*, September 1996.

<sup>931</sup> Siehe *AlterNIC, Supported TLDS*, <http://www.alternic.org/TLDS/>.

<sup>932</sup> Zum eDNS siehe *Rony/Rony, Domain Name Handbook*, S. 543ff.

<sup>933</sup> Zum uDNS siehe *Rony/Rony, Domain Name Handbook*, S. 546.

<sup>934</sup> Näheres zu Image Online Design siehe *Rony/Rony, Domain Name Handbook*, S. 546ff.

<sup>935</sup> Vgl. die Klageschrift, *Image Online Design v. Internet Assigned Numbers Authority, u. a., Superior and Municipal Court of the State of California for the County of San Luis Obispo*, 27. Februar 1997,

<http://www.jmls.edu/cyber/cases/iod1.html>. Weitere Ausführungen zur Klage siehe auch *Rony/Rony, Domain Name Handbook*, S. 548ff.

## 5.1. Alternativen innerhalb des DNS

---

den, daß IOD 1996 eine Autorisierung der TLD .web von der IANA durch einen Scheck von 1.000 US\$ erreichen wollte. Dieser wurde aber von Dr. Jon Postel zurückgewiesen, so daß keine Anhaltspunkte für eine Genehmigung bestanden. Ambler beschuldigte außerdem die IANA und das IAHC, in sein Eigentumsrecht einzugreifen<sup>936</sup>:

27. Plaintiff is informed and believes and thereon alleges that Defendant IANA and Defendant IAHC that they either collectively or individually will adopt and implement the IAHC report and the procedures set forth therein, thereby wrongfully, and illegally, usurping, taking, misappropriating, seizing, confiscating, and damaging Plaintiff's proprietary investments and first/prior use of ".web".

Nachdem die US-Regierung ihre Bedenken an der Einführung neuer TLDs und der Teilnahme der ITU und WIPO äußerte, zog IOD am 6. Mai 1997 die Klage ohne Abwarten einer Entscheidung zurück. IOD war zu der Ansicht gelangt, auf Grund der ausgedehnten Kritiken zum gTLD-MoU nicht mehr in der Geschäftsausübung bedroht zu sein. Durch diesen cleveren Schritt hielt sie sich offen, erneut gegen die Internetorganisationen vorgehen zu können. Durch die Rücknahme der Klage konnte kein Grundsatzurteil gefällt werden, welches spätere Gerichtsprozesse beeinflussen könnte. Besonders vor dem Hintergrund, daß die ICANN eine TLD .web einführen und an ein anderes Unternehmen vergeben könnte, erweist sich der Entschluß zur Klagerücknahme als weitsichtig. IOD hält auch weiterhin die TLD .web aufrecht und nahm auch (jedoch erfolglos) am ersten Ausschreibungsverfahren der ICANN zur Einführung neuer TLDs teil.

Einen weiteren ambitionierten Versuch, alternative TLDs zu vermarkten, stellte die Initiative von *PG Media, Inc.* (PGM) unter der Leitung von Paul Garrin dar. Ende 1995/ Anfang 1996 gründete er die *Registry Name.Space*, unter der ein Zugriff auf mehrere hundert alternativer TLDs ermöglicht wurde<sup>937</sup>. PGM versuchte im Gegensatz zu den anderen alternativen *Registries* nicht, ein paralleles TLD-System aufzubauen, sondern sah von Beginn an vor, daß der autoritative *Root Server* der Öffentlichkeit zugänglich gemacht wird. Garrin schlug dazu ein dezentralisiertes *Registry*-Modell vor, welches lokalen *Registries* den gemeinsamen Zugriff auf alle TLDs ermöglichen sollte. Um einen Zugang zum *A Root Server* zu erhalten, verlangte er von der NSI, daß diese auch auf die Nameserver von *Name.Space* verweist. Da die NSI damit einen Konkurrenten hätte zulassen müssen, lehnte diese die Forderung ab. Die NSI befreit sich auf ihre Verträge mit der US-NSF und verwies *Name.Space* an die IANA. PGM erhob daraufhin am 20. März 1997 Klage gegen die NSI auf Hinzufügung eines Verweises auf *Name.Space* in die Rootdatenbank. PGM beschuldigte NSI einer Verletzung des amerikanischen Wettbewerbsrechts durch Verweigerung eines Zugangs zum *A Root Server* für Wettbewerber. Garrin behauptete, daß diese Weigerung eine Handelsbeschränkung im Sinne Sec-

---

<sup>936</sup> Vgl. die Klageschrift, Fn. 935.

<sup>937</sup> Näheres zu PG Media, Inc. siehe *Rony/Rony, Domain Name Handbook*, S. 550ff. und *Froomkin*, 50 Duke L.J. 17, 61f. Vgl. auch die Webseite von Name.Space unter <http://namespace.pgmedia.net>.

tion 1 und 2 des Sherman Act darstelle. NSI verlangte daraufhin von der IANA eine Genehmigung für die notwendigen Veränderungen an der Rootdatenbank. IANA wies jedoch jede Autorität über NSIs Management des *A Root Servers* zurück<sup>938</sup> und verwies auf die US-NSF. Auf Nachfrage von NSI wies die US-NSF daraufhin am 25. Juni 1997 die NSI an, keine neuen TLDs der Rootdatenbank hinzuzufügen.

PGM hatte mit der Klage gegen NSI keinen Erfolg. Schon das erstinstanzliche Gericht stellte fest, daß die NSI unter der *Federal Instrumentality Doctrine* Immunität gegen Wettbewerbsklagen besäße, soweit sie Aufgaben unter dem *Cooperative Agreement* zwischen ihr und der US-NSF wahrnehme<sup>939</sup>. Auch die Berufungsinstanz hielt an einer Wettbewerbsimmunität von NSI fest<sup>940</sup>:

In sum, NSI is entitled to implied antitrust immunity for the conduct at issue in this case, as such conduct was expressly directed by the government and the terms of the Cooperative Agreement, and because it is in furtherance of the government's policy with respect to the management of the DNS.

Trotz der Abweisung der Klage von PGM konnten zwei wichtige Feststellungen getroffen werden. Zum einen hatte die IANA keine Autorität über die NSI und zum anderen konnte NSF ihre Kontrollmacht über NSI und die Rootdatenbank des DNS festigen<sup>941</sup>.

Nachdem es im Zeitraum der ICANN-Gründung keine neuen Versuche gab, alternative TLDs zu vermarkten, lebte diese Idee im neuen Jahrtausend wieder auf. Die erneut entflamme Diskussion um alternative DNS-Angebote beruht vor allem auf dem langsamem und schwer durchschaubaren Prozeß der Einführung neuer TLDs durch die ICANN. Unternehmen versuchen dabei, die durch die Diskussion um die neuen TLDs angeregte Nachfrage bei den Endnutzern auszunutzen. Für den deutschen Sprachraum tritt zum Beispiel *BeatNIC* auf, welche Registrierungen unter TLDs wie .bahn, .gbr oder .oeko anbietet. Diese sollen für die deutschen Internetnutzer einen höheren Nutzen als die von der ICANN beschlossenen TLDs haben. Erreicht werden können die TLDs über Nameserver der *Open Root Server Confederation, Inc.*<sup>942</sup> (ORSC), einem Zusammenschluß alternativer *Registries*. Die ORSC ist offen für alle Betreiber einer gTLD-*Registry*, ohne selbst TLDs zu vermarkten. Das Ziel dieser ist, einen offenen Markt für gTLDs zu schaffen und die bestehenden Beschränkungen auf das notwendige Minimum herabzusenken, um weiterhin die Stabilität des DNS zu gewährleisten<sup>943</sup>.

---

<sup>938</sup> Zum geschichtlichen Hintergrund siehe, *U.S. Court of Appeals, Second Circuit* vom 21. Januar 2000, Name.Space, Inc. v. Network Solutions, Inc. and National Science Foundation, 202 F.3d 573, 579f.

<sup>939</sup> Siehe *U.S. District Court, S.D. New York* vom 16. März 1999, PGMedia, Inc. D/B/A Name.Space tM v. Network Solutions, Inc. and the National Science Foundation, 51 F.Supp.2d 389, 406f.

<sup>940</sup> Siehe *U.S. Court of Appeals, Second Circuit* vom 21. Januar 2000, Name.Space, Inc. v. Network Solutions, Inc. and National Science Foundation, 202 F.3d 573, 584.

<sup>941</sup> Vgl. *Froomkin*, 50 Duke L.J. 17, 62.

<sup>942</sup> Siehe <http://www.open-rsc.org>. Eine weitere Root Server Confederation stellt das *SuperRoot Consortium* dar, <http://www.superroot.net>.

<sup>943</sup> Vgl. ORSC, Openness is a Key Aspect of the ORSC, <http://www.open-rsc.org/draft/v5/v5.1/openness/>.

Den Unmut über das zögerliche Verhalten der ICANN ausnutzend, wurde ein weiteres und sehr erfolgversprechendes Projekt zur Vermarktung alternativer TLDs von dem Unternehmen *New.net, Inc*<sup>944</sup> ins Leben gerufen. Um die Domainnamen von *New.net* nutzen zu können, ist entweder ein Zusatzprogramm für den WWW-Browser nötig oder ein Internetprovider, der die Domains freigeschaltet hat. Hierzu hat das Unternehmen einerseits Vereinbarungen mit einer Reihe von Softwareherstellern getroffen, welche in ihren Programmen die notwendige Zusatzsoftware integrieren sollen. Andererseits ist über kooperierende Internetprovider der Zugriff auf die DNS-Server von *New.net* möglich<sup>945</sup>.

Das Betreiben alternativer *Root Server* birgt allerdings für die Stabilität des DNS und damit für das Internet einige Risiken inne. Die Gefahren bestehen darin, daß gleiche TLDs unter dem ICANN-*Root Server* und den alternativen *Root Servers* mit unterschiedlichen Inhalten geführt werden können.

Zum Beispiel könnten unter der schon lange im alternativen DNS-Bereich bestehenden TLD .biz und unter der im ICANN-*Root Server* eingetragenen TLD .biz gleichzeitig die Domains mueller.biz von verschiedenen Firmen geführt werden. Diese würden von einander unabhängig betrieben. Dann könnten gleiche DNS-Anfragen (zum Beispiel nach mueller.biz) an verschiedene DNS-Server zu unterschiedlichen Antworten führen, davon abhängig, welche IP-Adresse für die nachgefragte Domain gespeichert wurde. Die Einmaligkeit einer Domain ist dann nicht mehr gewährleistet<sup>946</sup>. Eine Webadresse kann dann nicht mehr eindeutig einem Internetangebot zugeordnet werden. Eine Email kann, von verschiedenen Computern im Internet abgesendet, auf verschiedene Rechner mit gleicher Domain geleitet werden und gegebenenfalls den gewünschten Empfänger nicht erreichen.

Als globales Netzwerk benötigt das Internet auch weiterhin einen eindeutigen Namensraum. Dieser beruht auf einem hierarchischen System mit einem einzelnen autoritären *A Root Server* an der Spitze. Solange die Alternativen zum DNS keine weite Verbreitung gefunden haben, muß diese Beschränkung hingenommen werden. Um die Stabilität des Internets zu wahren, ist es erforderlich, daß es keine weiteren *Root Server* im öffentlichen DNS-Namensraum gibt. Dieses öffentliche DNS erfordert wiederum eine Organisation, die als alleinige Autorität Änderungen am zugrundeliegenden TLD-Verzeichnis vornehmen darf. Aus dem geschichtlichen Hintergrund kann die ICANN diese Autorität herleiten, weil sie von dem US-DoC mit der Verwaltung des *A Root Servers* betraut wurde. Aus den oben genannten Gründen sollte es

---

<sup>944</sup> Siehe <http://www.new.net>. *New.net* erläutert ihre Ansicht eines offenen DNS in ihrem Policy Paper: A Proposal to Introduce Market-Based Principles into Domain Name Governance,

<http://www.new.net/NewnetPolicyPaper.pdf>. Eine ausführliche Kritik zum Vorschlag New.Net wurde von der ICANN am 9. Juli 2001 veröffentlicht: *ICANN, Keeping the Internet a Reliable Global Public Resource: Response to New.net „Policy Paper“*, <http://www.icann.org/icp/icp-3-background/response-to-new.net-09jul01.htm>.

<sup>945</sup> Siehe *Heise-Newsticker*, new.net forciert unautorisierte Top-Level-Domains, 9. April 2001. Zu den involvierten Internetprovidern zählen inzwischen marktstarke Firmen wie Prodigy, Inc. Juno, Inc. oder Earthlink, Inc.

<sup>946</sup> Vgl. *Lynn*, Authoritative Root; *RFC 2826*, IAB sowie *Crispin*, Alt-Roots.

soweit wie möglich vermieden werden, überschneidende parallele TLD-Systeme zu betreiben. Im freien Wettbewerb unter den *Root Servern*<sup>947</sup> sollte beachtet werden, daß diese nicht auf gleichnamige TLDs unterschiedlichen Inhalts verweisen.

Die ICANN darf jedoch alternative Projekte nicht völlig unbeachtet lassen und in Zukunft bedenkenlos TLDs einführen, welche schon im alternativen DNS-Raum Verbreitung gefunden haben. Sollte sie diese unberücksichtigt lassen, würde die ICANN selbst zur Fragmentierung des DNS beitragen. Damit ist sie in einen schwer lösbar Konflikt geraten. Zum einen soll eine Vielzahl neuer TLDs in einem fairen Prozeß eingeführt und jedem Bewerber die gleichen Chancen gegeben werden. Zum anderen ist die ICANN faktisch an schon bestehende Zustände im DNS gebunden. Sie kann eine TLD erneut vergeben, wenn die alternative TLD nur von einer sehr geringen Anzahl von Internetnutzern verwendet wird. Die im ICANN-Root beheimatete TLD würde ihren Doppelgänger in kurzer Zeit verdrängen, da sie im Gegensatz zur alternativen TLD von allen Internetnutzern erreicht werden könnte. Als offizielle TLD hätte sie eine hohe Anziehungskraft auf Kunden und ein schnelles Wachstum wäre wahrscheinlich. Schwierig wird es jedoch mit Systemen wie dem TLD-Angebot von *New.net*, das schon heute circa 50 Mio. Internetnutzer erreicht<sup>948</sup>. Bei einer möglichen Überschneidung des ICANN-Namensraumes mit dem von *New.net* käme es unweigerlich zu den oben genannten Instabilitäten im DNS. Bislang hat ICANN es abgelehnt, die TLDs von *New.net* mit in ihre Liste der gTLDs aufzunehmen. Auch lehnt es die ICANN ab, diese TLDs in Zukunft nicht selbst erneut zu vergeben<sup>949</sup>, denn dann würde sie sich die Möglichkeit nehmen, in Zukunft überhaupt neue TLDs einzuführen. Mit einer einmaligen Bestätigung alternativer TLDs würde man auch bei anderen Betreibern die Hoffnung wecken, anerkannt zu werden. Zusätzlich würde man damit vermehrt die Gründung alternativer TLDs bewirken und sich der Handlungsfreiheit völlig berauben.

Eine Lösung könnte dahin gehen, daß die Gründung alternativer TLDs völlig dem freien Markt unterstellt wird und ICANN die neuen TLDs nach dem Prinzip „first come, first served“ in den *A Root Server* mit aufnimmt. Problematisch sind jedoch die Fälle, bei denen sich schon zum jetzigen Zeitpunkt alternative TLDs überschneiden. Zum Beispiel wird die TLD *.shop* schon in vielen alternativen *Root Servern* gehostet. Es ließe sich für ICANN schwer begründen, warum sie eine solche TLD an den schnellsten Bewerber vergeben möchte, obwohl möglicherweise ein anderer Anbieter diese schon bedeutend länger nutzt. ICANN stände auch in diesem Falle vor dem Konflikt, TLDs anzuerkennen, welche schon anderweitig existieren. Eine Schaffung von TLDs außerhalb des Einflußbereiches einer kontrollierenden Instanz hätte zusätzlich zur Folge, daß nicht sichergestellt werden kann, daß notwendige Kriterien zur Stabilität der entsprechenden *Registry* von den Anbietern eingehalten werden. Das Drängen auf Einhaltung dieser Kriterien ist jedoch ein Hauptgrund für das vorsichtige Vorgehen von ICANN bei der Einführung neuer TLDs gewesen. Ein Ausweg aus dem Konflikt bestände nur

---

<sup>947</sup> So aber das Policy Paper von *New.net*, Fn. 944. Vgl. auch den Vorschlag eines sog. Virtual Inclusive Root durch *Higgs*, Alternative Roots sowie *Higgs*, Root Zone Definitions.

<sup>948</sup> *New.net* veröffentlicht jedoch nicht, wieviele SLDs sie bislang unter ihren alternativen TLDs registriert hat.

<sup>949</sup> Siehe *Ermert*, Telepolis 7812.

in einer Erweiterung des DNS auf multiple Root-Verzeichnisse. Dies hätte jedoch ein Um-schreiben sämtlicher auf dem DNS basierender Software zur Folge und ist nur auf lange Sicht zu realisieren. ICANN kann jedoch weiteren Schaden verhindern, wenn sie in kürzester Zeit eine zweite Vergaberunde von TLDs eröffnen würde. Dazu müßte sie feste Kriterien für die Bewerbungen festlegen und wie bereits festgestellt, alle Bewerber zulassen, die diese Bedin-gungen erfüllen. TLDs, für welche Mehrfachbewerbungen vorliegen, muß ICANN nach ei-nem fairen Verfahren verteilen. Nach dieser zweiten Vergaberunde sollte ICANN nach dem Prinzip „first come, first served“ an neue Bewerber weitere TLDs zuteilen. Somit kann das anstehende Risiko einer Fragmentierung des DNS bei einem Wettbewerb zwischen dem *A Root Server* der ICANN und den alternativen *Root Servern* die ICANN zu einem schnelleren und faireren Verfahren bei der Vergabe neuer TLDs zwingen. Soweit sie flexibel genug ist, dieser Gefahr zu begegnen, haben die alternativen *Root Server* aus gesamtökonomischer Sicht ihre Aufgabe erfüllt, einen besseren Service zu Gunsten der Kunden auch im TLD-Bereich zu bewirken.

### 5.2. Ausdehnung des DNS auf andere Systeme – ENUM

Die Vorteile einer Auflösung von IP-Adressen durch das DNS lassen sich auch auf andere Adressierungssysteme übertragen. Dabei kann das DNS herangezogen werden, um anstatt die zugehörigen IP-Adressen eines Domainnamens herauszufinden, andere Adreßangaben an den nachfragenden Internetnutzer zu übermitteln. Ein solches, das DNS einbeziehende System stellt das in enger Zusammenarbeit mit der ITU<sup>950</sup> durch die IETF entwickelte ENUM<sup>951</sup> dar. Die Bezeichnung ENUM steht für *Electronic Number and Telephone Number URI Mapping*, kurz *Telephone Number Mapping*. ENUM soll es ermöglichen, daß man mittels des Internets zu einer Telefonnummer korrespondierende Web-, Email- oder auch Fax-Adressen finden kann. Hierzu wird eine internationale Telefonnummer, welche dem *International Public Tele-communication Numbering Plan E.164*<sup>952</sup> entspricht, als Domainname abgebildet. ENUM ar-beitet mit Telefonnummern, die bereits einem regulären Telefonanschluß zugewiesen wurden. Für die ausschließliche Nutzung mit ENUM können keine Telefonnummern vergeben wer-den.

Der Domainname, welcher mit der Telefonnummer korrespondiert, wird in umgekehrter Rei-henfolge geschrieben und soll einer speziellen SLD zugewiesen werden. Für die Telefon-nummer der Friedrich Schiller Universität Jena (++49 3641 9300) würde der entsprechende Domainname 0.0.3.9.1.4.6.3.9.4.e164.arpa lauten. Die TLD .arpa ist eine nur für Experimente zugängliche TLD, welche hier mittels der Domain e.164.arpa einen ausführlichen Test des ENUM ermöglichen soll. Mittels dieses Domainnamens können wiederum sogenannte *Nam-*

---

<sup>950</sup> Vgl. die Homepage zu ENUM bei der ITU: <http://www.itu.int/osp/spu/enum/>.

<sup>951</sup> Die Umsetzung von Telefonnummern in das DNS wird im *RFC 2916*, Faltstrom beschrieben. Vgl. auch die Kurzbeschreibung von ENUM von *Marsan*, Network World, IETF spec could propel Internet telephony, 2. Ok-tober 2000.

<sup>952</sup> Siehe die Inhaltsübersicht unter *ITU*, [E.164] Recommendation E.164/I.331, <http://www.itu.int/itudoc/itu-t/rec/e/e164.html>.

*ing Authority Pointer*<sup>953</sup> (NAPTR) abgefragt werden, welche Verweise auf eine Vielzahl von Adressen beinhalten können. Es werden damit verschiedene Kommunikationslösungen ermöglicht, wobei Telefonnummern als einzige Identität dienen. Es wird ermöglicht, daß zum Beispiel der Email-, Fax-, Mobil-, Voicebox- oder Pager-Kontakt mittels einer einzigen Nummer, der Telefonnummer hergestellt werden kann. Mit dieser Abbildungsfunktion von Telefonnummern kann ENUM, wie das DNS selbst, für vielfältige Anwendungen genutzt werden. ENUM läßt einen Endnutzer erkennen, welche Kontaktmöglichkeiten korrespondierend zu einer Telefonnummer existieren, um diese dann auch nutzen zu können.

ENUM hat ein großes Interesse bei Telefongesellschaften und ISPs geweckt. Einer der Gründe für die Attraktivität dieses Verfahrens ist darin begründet, daß ENUM Lösungsmöglichkeiten für Voice-over-IP, Universal Messaging und Internetfax ermöglicht. ENUM kann als ein Mittel zur weiteren Verschmelzung von herkömmlichen Kommunikationsmethoden mit dem Internet betrachtet werden.

Damit sich ENUM-Anwendungen bei den Internetnutzern durchsetzen, muß es sorgfältig und durchdacht eingeführt werden, um Stabilität und Zuverlässigkeit des ENUM-Systems zu gewährleisten. Umstritten ist bislang jedoch die zukünftige Struktur zur Bereitstellung eines ENUM-Systems. Darüber hinaus ist nicht geklärt, inwieweit sich das ENUM-System dem freien Wettbewerb stellen soll und inwieweit staatliche Organisationen in die Administration involviert werden können. Wichtig ist zunächst, daß nationale Alleingänge vermieden werden, um für die Endnutzer ein Optimum an Nutzen zu erreichen.

Die ITU und die IETF haben eine Reihe von Vorgaben gesetzt, welche eine mögliche zukünftige Struktur eines auf dem ENUM beruhenden Systems beschreibt<sup>954</sup>. Die Verwaltung eines ENUM-Systems soll in drei Ebenen unterteilt werden. Die Grundebene ist die Domain, unter welcher der ENUM-Service gehostet wird. Zur Zeit hat die IANA/ICANN die Domain e164.arpa zu Testzwecken freigegeben. Es ist aber ebenfalls möglich, ein ENUM-System unter einer anderen Adresse (zum Beispiel e164.itu, e164.de, tel.com) zu etablieren. Damit stellt sich die Frage, ob einzelne ENUM-Server im Wettbewerb zueinanderstehen sollten. Es wird zunächst nicht verhindert werden können, daß verschiedene ENUM-Server unter unterschiedlichen Adressen von einander unabhängig in das Internet gestellt werden. Einige werden versuchen, für ihre ENUM-Zone einen staatlich besonders legitimierten Status zu erhalten. Einige werden in einen Wettbewerb, basierend auf Service und Preis, zueinander treten, um einen möglichst großen Kundenstamm zu akquirieren<sup>955</sup>. Schließlich wird es geschlossene ENUM-Server für Privatnutzer geben, die diese als unternehmensinterne Informationssysteme nutzen können. Die Existenz von staatlich sanktionierten ENUM-Systemen hätte den Vorteil, daß ein

---

<sup>953</sup> RFC 2915, Mealling/Daniel.

<sup>954</sup> RFC 3026, Blane.

<sup>955</sup> Bislang existieren schon zwei amerikanische Anbieter, Verisign/NSI unter enumworld.com und NetNumber mit e164.com, welche vorsehen, einen eigenen ENUM-Service aufzubauen. Auch NeuStar unter enum.org und Lucent unter e164.org haben verschiedene Tests bezüglich eines privaten ENUM-Systems unternommen. Es ist davon auszugehen, daß die Anzahl privater Anbieter in kürzerer Zeit kräftig ansteigen wird.

Nutzer von ENUM eine zentrale Anlaufstelle hätte, um die zu einer Telefonnummer korrespondierenden Adressen zu ermitteln. Im Wettbewerb stehende ENUM-Systeme hätten den Vorteil, daß diese ständig bemüht sein werden, den Endkunden einen optimalen Service anzubieten und Innovationen zügig umzusetzen. Für die nationalen Telekommunikationsbehörden stellt sich damit die Frage, in welchem Domainzweig ein ENUM-Service unterstützt werden soll. Ist den von der ITU und der IETF gesetzten Vorgaben zu folgen, die einen ENUM-Service unter e164.arpa vorsehen oder sollen mehrere ENUM-Service unter verschiedenen SLDs zugelassen werden? Für einen Endkunden wäre es sicherlich schwierig, mittels verschiedener Domainadressen, zu bestimmen, unter welcher er seine ENUM-Informationen speichern soll. Ebenso weiß der eine Telefonnummer erhaltende Internetnutzer nicht, unter welcher Domainadresse er nach gespeicherten korrespondierenden ENUM-Informationen zu suchen hat. Es müßten somit noch Spezifikationen entworfen werden, welche den Zugriff auf die einzelnen unabhängigen ENUM-Server regeln. Die Betreiber werden kein Interesse haben, auf die Konkurrenzserver zu verweisen. Vorstellbar wären aber von dritten Parteien betriebene Server, welche auf alle möglichen Adressen von ENUM-Servern verweisen und diesen Datenbestand gegenseitig austauschen würden. Dann könnte ein neuer Anbieter eines ENUM-Services sein System bei einem dieser Betreiber anmelden, um in diese Adreßliste zu gelangen. Eine das ENUM-System nutzende Software würde schließlich alle in diese Adreßliste eingetragenen ENUM-Server abfragen.

Der von der ITU und der IETF vorgesehene zentrale ENUM-Server mit einer festgelegten Adresse (wie zum Beispiel e164.arpa) soll zunächst der ITU unterstehen und für alle Internetnutzer autoritär sein. Es ist vorgesehen, daß die Verwaltung nach nationalen Zonen erfolgt, welche sich nach den Länderkennzahlen der ITU-Empfehlung E.164<sup>956</sup> (zum Beispiel für Deutschland 9.4.e164.arpa oder für die USA 1.e164.arpa) richten sollen. Die nationalen Zonen würden von der ITU an die Mitgliedsstaaten delegiert, welche jeweils selbst bestimmen müßten, wie ihre Zone zu verwalten sei<sup>957</sup>. Die einzelnen nationalen Zonen könnten so auf verschiedene Weise reguliert werden. Es sollen darüber hinaus nur nationale Gebietskörperschaften einen Platz im ENUM-Server finden können, die von der ITU ausdrücklich zur Teilnahme zugelassen worden sind. Auf dieser Ebene werden schließlich die einzelnen im nationalen Telefonnetz bestehenden Telefonnummern abgebildet und die korrespondierenden Adreßangaben für weitere Kommunikationsdienste in die NAPTR-Datensätze eingetragen. Doch auch hier ergeben sich ähnliche Probleme wie auf der untersten Ebene. Da das ENUM-System auf dem DNS basiert, muß auch hier geklärt werden, ob es einen Wettbewerb unter mehreren *Registries* und *Registrars* geben soll. Das DNS-Protokoll verlangt grundsätzlich, daß für jeden Knotenpunkt im DNS jeweils nur eine Anlaufstelle zuständig ist<sup>958</sup>. Schon aus

---

<sup>956</sup> Vgl. Fn. 952.

<sup>957</sup> Vgl. RFC 3026, Blane, Kap. 3.3. - country code zone. Für Deutschland ist bislang die Zuständigkeit für den Strang 9.4.e164.arpa nicht geklärt. In Frage käme eine Regulierung durch die Regulierungsbehörde für Telekommunikation und Post (RegTP) aber auch direkt durch das Bundesministerium für Wirtschaft und Technologie (BmWI).

<sup>958</sup> Vgl. RFC 2826, IAB.

diesen technischen Gründen, wird man auf im Wettbewerb stehende *Registries* verzichten müssen. Beim Betrieb von mehreren parallelen *Registries*, bestände wie bei alternativen Roots das Risiko einer Fragmentierung eines autoritären ENUM-Systems. Die einzelnen *Registries* würden dann jeweils nur einen Anteil der angemeldeten Telefoneinträge hosten, da nicht davon ausgegangen werden kann, daß alle Nutzer bereit sind, sich bei allen *Registries* eintragen zu lassen, um dann auch die entsprechende Gebühr bei allen Betreibern zu entrichten. Ein Endnutzer, welcher die einer Telefonnummer korrespondierenden Einträge sucht, müßte schließlich diese bei allen *Registries* nachschlagen. Der Einheitlichkeit eines globalen Nachschlagesystems wäre damit der Sinn genommen. Entsprechend den TLDs kann demzufolge für den deutschen Knotenpunkt im DNS 9.4.e164.arpa nur eine *Registry* zuständig sein, wie auch für die TLDs .com oder .net nur eine *Registry* zuständig ist. Das für diese *Registry* zuständige Unternehmen ließe sich jedoch mittels einer Ausschreibung nach wettbewerblichen Kriterien auswählen und für einen begrenzten Zeitraum einsetzen. In einem solchen Auswahlprozeß sollten neben dem finanziell günstigsten Angebot auch technische und administrative Aspekte einbezogen werden. Im Gegensatz zur *Registry* können mehrere *Registrars* an der Registrierung der Telefonnummern in das ENUM-System involviert werden. Dieses System multipler Registrare würde dann die dritte Ebene in dem von der ITU vorgeschlagenen Modell bilden und könnte sich nach dem *Shared Registry Model* der ICANN richten. Trotz staatlicher Sanktionierung des unter der Adresse von e164.arpa vorgeschlagenen Systems wäre genügend Wettbewerb garantiert, um für die Endnutzer ein auf Dauer optimales Preis-Leistungsverhältnis zu erreichen.

Das ENUM-System wirft zwei wichtige rechtliche Probleme auf. Erstens sind die NAPTR-Einträge mittels des DNS für jedermann einsichtlich. Für diese Informationen kann folglich ein Datenschutz nicht gewährt werden. Entsprechend sollten die mittels ENUM gespeicherten Informationen nur Daten enthalten, welche erforderlich sind, um entsprechende Kommunikationsverbindungen herzustellen. Persönliche Daten der Endnutzer sollten nicht gespeichert werden. Soweit eine solche Speicherung noch zum Betrieb des ENUM nötig ist, müssen Verfahren entwickelt werden, um diese vor unbefugten Zugriff zu verbergen.

Zweitens besteht auch beim ENUM die Möglichkeit, daß es zu Streitigkeiten zwischen den einzelnen beteiligten Organisationen kommt, sei es zwischen den Unternehmen, welche einen ENUM-Service anbieten oder zwischen diesen und der ITU, einer nationalen Behörde oder Endnutzern des ENUM-Services. Zur Zeit wird viel Augenmerk auf die Mechanismen zur Streitschlichtung im DNS gelegt. Entsprechend sind die ENUM-Betreiber gezwungen, basierend auf den im DNS gewonnenen Erfahrungen, eigene Verfahren zur Streitschlichtung zu entwickeln.

### 5.3. Parallel zum DNS

Auf dem DNS basierende Verfahren sind jedoch nicht die einzige Lösung, die Orientierung im Internet zu erleichtern. Im Laufe der letzten sieben Jahre hat sich eine Reihe von Methoden etabliert, die eine Alternative zum DNS darstellen. Hierzu zählen auf Keywords basierende Systeme, aber auch Suchmaschinen und Indizes. Eine Sonderrolle stellt die Verzeichnisstruktur X.500 dar, die einen theoretischen Ansatz zur Überwindung der

### 5.3. Parallel zum DNS

---

nisstruktur X.500 dar, die einen theoretischen Ansatz zur Überwindung der Nachteile des DNS bietet, sich bis jetzt aber noch nicht in der Praxis durchsetzen konnte.

Regelmäßig wird auf Objekte aus der realen Welt mittels eines allgemeinen Namens oder Ausdrucks (*Common Names*) verwiesen (zum Beispiel der Name eines Unternehmens oder Produktes, der Titel einer Publikation, usw., lateinische Bezeichnungen für Pflanzen und Tiere). Solche Bezeichnungen sind gewöhnlich leichter zu merken, als die im Internet verwendeten Domainnamen. Es wird deshalb seit einiger Zeit versucht, ein Verfahren zu finden, welches den Zugriff auf Ressourcen im Internet mittels Wörter oder Ausdrücken ermöglicht<sup>959</sup>. Inzwischen wird der Service angeboten, *Common Names* WWW-Angeboten zuzuweisen. Die hinter diesem Service stehenden Firmen richten ihr Hauptaugenmerk vor allem auf zahlungskräftige Unternehmen und bieten an, daß man deren Homepage, durch einfaches Eintippen ihres Namens oder ihrer Marke in einen Webbrowser, erreichen kann. Den bekanntesten Anbieter stellt die schon 1996 gegründete Firma *RealNames Corporation*<sup>960</sup> dar. Die sogenannte *Keyword Resolution* von *RealNames* läßt sich in viele Internet-Dienste integrieren. Seit längerer Zeit hat *Microsoft* das System in ihren *Internet Explorer* eingebaut, welches damit von einem Großteil der Internetnutzer erreichbar ist. Darüber hinaus greifen viele Internetverzeichnisse auf die bei *RealNames* reservierten Stichwörter zurück. Wie die Domainnamen können *Common Names* durch ein weltweites Netz von *Registrars* reserviert werden. Eine Beschränkung auf den englischen Zeichensatz und die arabischen Ziffern besteht beim System von *RealNames* im Gegensatz zum herkömmlichen DNS nicht, so daß Registrierungen in allen Sprachen vorgenommen werden können. Um sich selbst vor Klagen wegen Beihilfe zu Markenrechtsverletzungen zu schützen, hat *RealNames* eine sogenannte *Keyword Dispute Resolution Policy*<sup>961</sup> entwickelt. Diese ist Vertragsbestandteil des *Keyword Registration Services Agreement* und enthält Regeln, wie Markenrechtsverletzungen durch ein effizientes Onlineverfahren geltend gemacht werden können.

Die *Microsoft, Inc.* möchte in neuen Versionen ihrer Produkte (wie das Softwarepaket *Office* und den *Internet Explorer*) eine weitere Variante eines Keywordsystems integrieren, die sogenannten *Smart Tags*. Mit dieser Funktion können vornehmlich Firmennamen in einer WWW-Text mit einem Verweis auf die Webseite des Unternehmens unterlegt werden. Dazu wird der aus dem Internet mittels eines *Microsoft*-Programmes geladene Text auf Stichwörter hin untersucht und mit einer gestrichelten Linie unterlegt<sup>962</sup>. Die *Smart Tags* haben in den USA bislang jedoch eine Reihe von Protesten ausgelöst. Insbesondere sieht man in der Anwendung dieser *Smart Tags* einen Eingriff in die Urheberrechte der Autoren der betroffenen WWW-Seiten. Daneben befürchtet man, daß *Microsoft* die Möglichkeit habe, Webseiten an-

---

<sup>959</sup> Das Verfahren soll das Common Name Resolution Protocol (CNRP) darstellen, siehe *RFC 2972*, Masinter u.a.

<sup>960</sup> Siehe *RealNames*, <http://www.realnames.com>.

<sup>961</sup> Siehe *RealNames*, Keyword Dispute Resolution Policy, [http://web.realnames.com/Virtual.asp?page=Eng\\_Policy\\_DisputeResolution](http://web.realnames.com/Virtual.asp?page=Eng_Policy_DisputeResolution).

<sup>962</sup> Siehe *Heise-Newsticker*, Internet-Explorer-Beta mit Smart Tags, 26. Juni 2001.

derer zum eigenen Vorteil abzuändern<sup>963</sup>. Es muß jedoch die vollständige Umsetzung dieses neuen Features in die Softwareprodukte von *Microsoft* abgewartet werden, ehe Stellungnahmen zur Reichweite des Eingriffes in die Urheberrechte möglich sind.

Weitere Möglichkeiten, bestimmte Angebote im Internet aufzufinden, stellen die verschiedenen Suchmaschinen und Internetverzeichnisse dar. Diese zwei Servicetypen lassen sich zwar voneinander klar trennen, werden von einigen Unternehmen jedoch zusammen angeboten und bieten sogar Mischformen an, wie Suchmaschinen auf eigenst erstellte Verzeichnisse zugreifen. Suchmaschinen<sup>964</sup> greifen auf einen Datenbestand zurück, welche spezielle Programme ohne menschlichen Eingriff im Voraus erstellt haben. Dazu laden diese Programme ganze Webseiten aus dem Internet in ihren Speicher, indizieren diese nach Stichwörtern und folgen den auf der gespeicherten Webseite enthalten Hyperlinks, um die Indizierung zu wiederholen. Die indizierten Stichwörter werden in die genannte Datenbank eingetragen und verweisen auf die Seite, in der sie gefunden worden sind. Ein Endnutzer kann dann mittels eigener Stichwörter in der Suchmaschine bestimmte Webseiten suchen lassen. Einige Suchmaschinen verwenden darüber hinaus spezielle Algorithmen, um die gefundenen Webseiten nach Relevanz zu sortieren. Die zweite Variante stellen die Internetverzeichnisse<sup>965</sup> dar. Bei einem solchen Verzeichnis werden nach Kategorien und Unterkategorien Links zu Webseiten eingesortiert. Die Entscheidung, ob und wo eine Webseite in das Verzeichnis aufgenommen werden soll, wird manuell entschieden. Ein Endnutzer kann dann eine entsprechende Kategorie wählen (zum Beispiel Sport/ Fußball/ Europameisterschaft) und wird eine manuelle Aufstellung von relevanten Webseiten zu diesem Thema erhalten. Meist enthalten diese Listen noch Kurzbeschreibungen oder Ausschnitte aus den verlinkten Webseiten. All diese Orientierungshilfen im Internet kommen jedoch nicht ohne das DNS aus, da sie auch weiterhin auf den Domänennamen des entsprechenden Angebotes verweisen müssen. Sie geben jedoch dem Endnutzer ein Werkzeug in die Hand, um auch Informationen zu finden, deren Urheber und Adresse er nicht kennt.

Einen über die bisherigen Orientierungshilfen hinausgehenden Ansatz stellt das Verzeichnis-System X.500 aus dem Jahre 1998 dar<sup>966</sup>. Es wurde in Zusammenarbeit zwischen ITU-T (damals die CCITT) und ISO entwickelt. X.500 soll ein einheitliches, weltweites System zur Benennung, Beschreibung und Auffindung aller Ressourcen, die in einem Netzwerk möglich sind, bieten. Über X.500 sollen die Nutzer Computer, Drucker oder Router über logische oder symbolische Namen ansprechen, auf die Dateisysteme zugreifen, Informationen über andere Nutzer (wie Emailadresse oder Telefonnummer) erhalten oder Zugriff zu sonstigen Informati-

---

<sup>963</sup> Vgl. u.a. *Mossberg, Walter S.*, New Windows XP Feature Can Re-Edit Others' Sites, The Wall Street Journal, 7. Juni 2001, <http://public.wsj.com/sn/y/SB991862595554629527.html>.

<sup>964</sup> Zu den wichtigsten und mit dem umfangreichsten Datenbestand gehörenden Suchmaschinen von der Alta-Vista Company (<http://www.altavista.com>) und Google (<http://www.google.com>).

<sup>965</sup> Zu den wichtigsten und umfangreichsten Internetverzeichnissen zählt auf internationaler Basis die Yahoo! Inc. (<http://www.yahoo.com>), welche Verzeichnisse in vielen verschiedenen Sprachen und für viele Staaten anbieten. Auf deutscher Ebene zählt die Web.de AG (<http://www.web.de>) zu den bedeutendsten Anbietern eines Internetverzeichnisses.

### 5.3. Parallel zum DNS

---

onen erlangen können. Dazu werden einzelne Datenobjekte gebildet und Attribute zugewiesen, welche bestimmte Werte annehmen können. Diese Objekte werden in den hierarchischen *Directory Information Tree* integriert, um dann zu Objektgruppen (sogenannte Klassen) zusammengefaßt zu werden. Die Informationen der Objekte können wiederum über diese Klassen angesprochen werden. Da das Ansprechen der Objektattribute über die Klassen und Überklassen sich für einen Nutzer recht kompliziert gestaltet, sind im X.500 Verfahren integriert, die beliebige Objekte mittels Abfragen auffinden. Trotz der Ausgewogenheit eines X.500-Verzeichnisses gibt es bislang keine nennenswerten Ansätze, dieses global auf Internetebene zu etablieren. Auf X.500 basierende Verzeichnisse eignen sich vielmehr auf unternehmensinterner Ebene ein Nachschlagesystem aufzubauen. Auf Grund der festen Einteilung in Klassen und Objekte kann kein allumfassender Verzeichnisansatz erstellt werden. Auf globaler Ebene gibt es unbestimmt viele verschiedene Kategorisierungsmöglichkeiten. Darüber hinaus wird jeder Verzeichnissteller eine andere Ansicht über die Bestimmung und Einordnung eines Objektes haben.

Jede der einzeln vorgestellten Orientierungshilfen hat eigene Vor- und Nachteile gegenüber dem DNS. Auch wenn ein Unternehmen über ein Stichwort schneller zu erreichen ist, als über einen langen Domainnamen mit Vorsilbe wie www. und TLD wie .de, wird man eine bestimmte Seite innerhalb eines komplexen WWW-Angebotes eines Unternehmens schneller durch einen Domainnamen unter Zusatz von Pfad- und Dateiangaben erreichen können. Suchmaschinen und WWW-Verzeichnisse bieten die Möglichkeit auch unbekannte Informationen zu finden, benötigen jedoch zum Verweisen auf das Angebot dessen Domainnamen. Nach Kenntniserlangung über ein spezielles Angebot wird man dieses schneller über den Domainnamen erreichen können. Es ist nur im jeweiligen Einzelfall möglich, zu unterscheiden, welcher Service am vorteilhaftesten ist. Es wird sich nicht eine Variante auf Kosten einer anderen vollständig durchsetzen können, sondern eine parallele Benutzung aller Orientierungshilfen für einen Internetnutzer am einträglichsten sein. Solange man die Service-Angebote einem freien Wettbewerb aussetzt, werden sich die Angebote innovativ weiterentwickeln und ständig neue Lösungen zur Überwindung von bislang bestehenden Mängeln angeboten werden.

---

<sup>966</sup> Zum X.500-Protokoll siehe *Kuri*, c't 1996, Heft 12, 334.

*As for the future, your task is not to foresee, but to enable it.*

*– Antoine de Saint-Exupéry –*

*„Datenstau im Internet, mein Programm wird abgesetzt.  
Hauptmenü, doch keine Wahl. Warum ich bloß Gebühren zahl?  
Testsignal nur visuell, Information nicht aktuell.  
Netztransfer zu intensiv [...] doch wir sind bereit!  
Wir sind INTERAKTIV!“*

*– welle: erdball – alles ist möglich –*

## 6. Ausblick

Die Entwicklung des Internets und dessen Regulierungsstrukturen sind noch längst nicht zum Stillstand gelangt. Auch heute noch wird regelmäßig über bestehende Mißstände diskutiert und versucht, Lösungen für diese anzubieten. Dabei konnte diese Arbeit nur einen kleinen Ausschnitt der Internetregulierung darstellen. Die ICANN stellt die zentrale Organisation in Fragen der Numerierung von Protokollen und Adressierung von Computern dar, während die IETF und das W3C ihr Augenmerk auf die Standardisierung der Anwendungen des Internets gerichtet haben. Darüber hinaus existieren jedoch eine Reihe weiterer Regulierungsversuche von privater aber auch von staatlicher Seite aus. Zum Beispiel haben verschiedene Initiativen im Rahmen des Jugendschutzes Verhaltenskodizes und Selbstklassifizierungssysteme entwickelt, beziehungsweise sogenannte *Hotlines* ins Leben gerufen<sup>967</sup>. Einzelstaaten versuchen in die Kommunikation im Internet per Gesetz einzugreifen<sup>968</sup> und erstrecken dabei ihre Hoheitsgewalt auf Angebote außerhalb ihres Territoriums<sup>969</sup>. Schließlich sehen Gerichte den Anwen-

---

<sup>967</sup> Siehe ausführlich hierzu die Schriftensammlung Waltermann/Machill, Verantwortung im Internet. Vgl. auch zu PICS Fn. 208.

<sup>968</sup> Siehe zum Beispiel das deutsche Gesetzespaket zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (IuKDG, Fn. 124) in der Fassung vom 13. Juni 1997 mit den enthaltenen Gesetzen: Teledienstgesetz (TDG, Fn. 126), Gesetz über Datenschutz bei Telediensten (TDDSG, Fn. 127) oder Signaturgesetz (SigG, Fn. 128). Weiterhin wurde im Bundestag ein Gesetz über den Elektronischen Geschäftsverkehr (EGG) beraten, siehe Entwurf der Bundesregierung vom 14. Februar 2001,

<http://www.bmwi.de/Homepage/download/infogesellschaft/EGG-Entwurf.pdf>.

<sup>969</sup> Zum Beispiel führte der US-amerikanische Digital Millennium Copyright Act (DMCA) zur Verhaftung des russischen Programmierers Dmitry Sklyarov nach einem Vortrag auf der Hackerkonferenz DefCon Nine in den USA und zu einem Verfahren vor einem US-Gericht gegen diesen und dessen russischen Arbeitgeber Elcom-

---

dungsbereich nationalen Rechts auf internationale Sachverhalte aus dem Internetbereich eröffnet<sup>970</sup>.

Im Rahmen dieser Arbeit konnte festgestellt werden, daß die Selbstregulierung des Internets einer staatlichen Regulierung vorzuziehen ist. Besonders die komplizierten technischen Zusammenhänge und der internationale Hintergrund erschweren die Teilnahme staatlicher Behörden an der Verwaltung des Internets. Soweit es um die Durchsetzung verletzter Rechte Dritter geht, kann jedoch mangels eigenständiger Jurisdiktion im Internet auf ein staatliches Einschreiten nicht verzichtet werden.

Der Umfang und die Bedeutung der Internetstandards selbst sind ebenfalls weiterhin im Fluß. So wurden zum Beispiel im Jahr 2001 durch die ETSI 194 Standardisierungsvorschläge als RFCs veröffentlicht<sup>971</sup>. Das W3C publizierte ebenfalls eine Reihe von Standards, welche vor allem der Interoperabilität zwischen den verschiedenen stationären und mobilen Endgeräten dienen sollen. Insbesondere die Einbindung diverser Mobilfunkgeräte der dritten Generation, die auf den *Universal Mobile Telecommunications Systems*<sup>972</sup> basieren, stellt eine umfangreiche Herausforderung an den Standardisierungsprozeß im Internet dar. Die Verschmelzung der herkömmlichen Techniken des Mobilfunks mit dem Internet hat gleichzeitig umfassende Auswirkungen auf die Zusammenarbeit von Gremien des Internets mit traditionellen Standardisierungsorganisationen. Gegenüber diesen traditionellen Organisationen haben die im Internet beheimateten Institutionen den Vorteil, daß sie sich auf ein offenes und transparentes Verfahren berufen können. Dadurch erlangen sie eine größere Flexibilität gegenüber klassischen Gremien und eine schnellere Anerkennung der beschlossenen Standards unter den Anwendern. Die hauptsächliche Quelle für die grundlegenden Standards des Internets stellen immer noch die RFCs der IETF dar. Diese versucht deshalb die Prinzipien des offenen Standardisierungsprozesses zu wahren. Hervorzuheben ist, daß jeder an den stattfindenden Diskussionen teilnehmen und eigene Ideen oder Entwürfe für Standards einbringen kann.

Allmählich treten jedoch auch bei den Internetorganisationen Strukturprobleme zutage. Zum Beispiel hat die IETF mit der Organisation ihres inzwischen auf über 130 *Working Groups* herangewachsenen Unterbaus<sup>973</sup> und der mehreren tausend am Diskussionsprozeß teilnehmenden Wissenschaftler zu kämpfen. Ebenfalls erweist sich für die IETF eine klare Repräsentation ihrer Interessen und Rechte durch die ISOC nach außen als unverzichtbar. Zum Beispiel stehen inzwischen alle veröffentlichten RFCs unter dem Urheberrechtsschutz der ISOC. Andererseits muß auch die ISOC ihre strukturellen Probleme lösen, um ihren Aufgaben ge-

---

Soft, *Heise-Newsticker*, eBook-Hacker nach Vortrag festgenommen, 17. Juli 2001 und *Heise-Newsticker*, Verfahren gegen eBook-Hacker eröffnet, 28. August 2001.

<sup>970</sup> Vgl. die Entscheidung des *BGH* vom 12. Dezember 2000, „Auschwitzlügen“, *BGHSt* 46, 212 zur Anwendung deutschen Strafrechts auf Veröffentlichungen eines Australiers bezüglich des Völkermordes an den Juden durch die Deutschen während des Dritten Reiches.

<sup>971</sup> Siehe die Liste der RFCs unter *RFC-Editor*, RFC-Index, <http://www.rfc-editor.org/rfc-index.html>.

<sup>972</sup> UMTS - Ein Datenfunkstandard für die Bereiche des Satelliten-, des Digital- und des Mobilfunks.

<sup>973</sup> Siehe *IETF*, Active IETF Working Groups, <http://www.ietf.org/html.charters/wg-dir.html>.

recht zu werden. Insbesondere ist es notwendig, daß sie ihr Verhältnis zu ihren *Regional Chapters* klärt und eine eindeutige Verteilung der Aufgaben festlegt.

Wie festgestellt wurde, ist die zweite Säule der Internetregulierung, die Verwaltung der IP-Adressen. Diese kaum spektakuläre Aufgabe wird vorrangig von den drei *Internet Registries* ARIN, RIPE-NCC und APNIC wahrgenommen. Doch auch hier stehen wichtige Änderungen an, in dem für die bislang nicht direkt vertretenen Regionen Afrika und Südamerika neue IRs (AfriNIC und LACNIC) ins Leben gerufen wurden. Darüber hinaus werden die IRs die organisatorischen Probleme bezüglich der Einführung des neuen Ipv6-Systems zu lösen haben.

Ganz so von der Öffentlichkeit unbeachtet wie die Vergabe der IP-Nummern ist die Domainvergabe als dritte Säule der Internetregulierung jedoch nicht geblieben. Besonders auf internationaler Ebene hat die Gründung der ICANN für viel Diskussionsstoff gesorgt. Schon der ursprüngliche Versuch, die Verwaltung des DNS durch die Gründung des IAHC zu reformieren stieß zum einen auf große Anerkennung und zum anderen auf entsprechenden Widerstand. Zu einer Zwangseinigung führte erst das von der US-Regierung mit dem *White Paper* eröffnete Verfahren. An dessen Ziel stand die Gründung einer privaten *nonprofit* Organisation, welche die Schlüsselfunktionen des Internets, wie die Verwaltung und die Erweiterung des DNS, die Verwaltung der IP-Adressen und der Rootserver, oder das Festlegen von Protokollparametern und Standards, übernehmen sollte. Damit wurde klar, daß die neue Organisation nicht nur die Domainvergabe beherbergen, sondern auch eine Dachorganisation für die Vergabe der IP-Nummern und für die Standardisierung werden sollte. Entsprechend sind in der daraufhin gegründeten ICANN neben den verschiedenen an der Domainvergabe beteiligten Gremien und Unternehmen auch die IRs und die wichtigsten Standardisierungsorganisationen beteiligt.

Ob die ICANN nur als ein Gremium zur technischen Koordinierung von Internetfunktionen oder als politisches Organ einzuordnen ist, bleibt weiterhin umstritten. Es mußte allerdings festgestellt werden, daß es zunächst für jeden Entscheidungsträger schwierig ist, rein technisch-koordinierende Bestimmungen festzulegen, ohne damit selbst in das politische Tagesgeschäft einzugreifen. Gerade aber mit der Einführung der UDRP und neuer TLDs hat die ICANN offensichtlich diesen schmalen Pfad der Entscheidungsfindung in Richtung politisches Gremium verlassen. Trotz der gravierenden Vorteile welche die UDRP bietet, insbesondere der schnellen, preiswerten und vor allem grenzenlosen Lösung von Markenrechtsstreitigkeiten um Domainnamen, wurde jedoch ein weltweites System von Markenrechten geschaffen, welches bei weitem die Lösungen der nationalstaatlichen Rechtsordnungen übertragt. Die UDRP spricht neue Rechte für Markenrechtsinhaber aus, welche in dieser Stärke bislang weder in der Praxis anerkannt, noch in der rechtswissenschaftlichen Literatur erörtert wurden. Der nach der Umsetzung der UDRP rigorose Vorrang von Markenrechten gegenüber anderen Namensrechten schränkt in viel zu starkem Umfang die herkömmlichen Regeln des Ausgleiches zwischen dem Schutz von Markennamen und der Notwendigkeit, eine freie Meinungsäußerung im Internet zu sichern und eine offene Namensgebung zuzulassen, ein. An der Streitschlichtungspraxis der UDRP ist besonders problematisch, daß eine Voreingenommenheit zu Gunsten der Markenrechtsinhaber besteht und die Entscheidungen keinem internen

---

Revisionsprozeß unterworfen werden können. So scheint schon die Unparteilichkeit kaum gewährt, wenn die Organisation WIPO als weltweite Vertreterin des geistigen Eigentums selbst einen *Dispute-Resolution Service Provider* betreibt<sup>974</sup>.

Die Erweiterung der gTLDs um weitere sieben TLDs verlief ebenfalls nicht zufriedenstellender. Eine Eingrenzung der Kandidaten auf maximal sieben war nicht gerechtfertigt und blieb dem starken Einfluß der Markenrechtslobby geschuldet, welche bislang jede Einführung neuer gTLDs verhindern konnte. Die von der ICANN immer wieder hervorgebrachte Begründung, zu viele Domains würden den technischen Betrieb des DNS und damit das Internet gefährden, konnte durch entsprechende Tests nicht nachgewiesen werden. Folge dieser Selbstbeschränkung war eine intransparente Auswahl dieser sieben neuen TLDs aus einem Bewerberpool von 44 Kandidaten mit einer Vielzahl von Vorschlägen. Viele vernünftige Konzepte mußten deshalb geopfert werden, um die Bewerbungen auf das gewünschte Maß zu reduzieren.

Darüber hinaus wehrt sich die ICANN gegen jede Alternative zum derzeitigen DNS. Erweiterungen des DNS außerhalb des Einflusses der ICANN werden pauschal von ihr als schädlich für die Infrastruktur des Internets betrachtet, ohne sich aktiv an der neu entfachten Diskussion zu beteiligen. Innovative Ideen werden damit unterdrückt oder es entstehen Unternehmen wie *New.net*, welche durch spezielle Zusatzsoftware das DNS zu umgehen versuchen.

Obgleich die ICANN die Einführung einer regionalen TLD für Europa längst gebilligt hat, scheiterte bislang die Einführung der TLD .eu an den bürokratischen Hürden. Es scheint kaum möglich zu sein, die verschiedenen Ansichten von Kommission, Europäischem Rat und Parlament zu harmonisieren. Besonders die Forderung des Rates, daß jedes Land nach eigenem Belieben Einschränkungen bei der Verwendung von geographischen und politischen Adressen machen kann, schürte die Angst vor einem bürokratisch aufgeblähten Registrierverfahren. Dabei sollte vor allem ein automatisierter, möglichst einfacher Registrierprozeß unter dem Prinzip „first come, first served“ den Erfolg von .eu sichern.

Betrachtet man die Domainnamen aus rechtlicher Sicht, hat sich in Deutschland längst eine verlässliche Spruchpraxis zur Lösung von Konflikten um diese gebildet. Der in den Anfangsjahren des Internets weitverbreiteten Praxis des *Domain Grabblings* aber auch dem später einsetzenden *Reverse Domain Namen Hijacking*<sup>975</sup> konnten jeweils klare Grenzen gesetzt werden. Auch die Verantwortlichkeit der DENIC eG in Markenrechtsstreitigkeiten konnte geklärt werden. Insbesondere wurde inzwischen vom Bundesgerichtshof festgestellt, daß weder aus dem Markenrecht noch aus dem TDG ein Anspruch auf Löschung oder Übertragung eines Domainnamens gegen die DENIC eG hergeleitet werden kann<sup>976</sup>. Ebenfalls konnte festgestellt werden, daß die DENIC eG im Rahmen der Regeln des deutschen und europäischen

---

<sup>974</sup> Mueller, Rough Justice, Kap. 4. Forum Shopping and Bias.

<sup>975</sup> Vgl. Fn. 461.

<sup>976</sup> Vgl. Fn. 928.

Kartellrechts agiert. Soweit die Offenheit der Genossenschaft weiterhin gewahrt bleibt und keine ISPs benachteiligt werden, muß die DENIC eG kein Einschreiten von Kartellbehörden befürchten.

Schließlich konnten im Rahmen dieser Arbeit einige Alternativen zum DNS aufgezeigt werden. Zum einen existieren eine Reihe von Versuchen, die Beschränkung der gTLDs durch eigenständige Rootserver zu umgehen. Die Firma *New.net* erreicht durch Allianzen mit verschiedenen ISPs und Softwarefirmen inzwischen einen beträchtlichen Kundenkreis. Obgleich diese Angebote zu einer Zersplitterung des Internets führen könnten, zeigen sie auf, daß das von ICANN verwaltete DNS problemlos erweitert werden kann.

Um einen einheitlichen Zugriff auf die Vielzahl an inzwischen bestehenden Nachrichtensysteme über das Internet zu ermöglichen, wird an einem weiteren Verzeichnissystem gearbeitet, dem ENUM. Im Vergleich zur Entwicklung des DNS in den frühen Jahren des Internets, wird eine Einigung auf einen Standard für das ENUM durch die Teilnahme unterschiedlicher Interessensvertreter erschwert. Die Schwierigkeiten einer Koordination divergierender Interessen, welche dem DNS und den Reformbestrebungen um dieses erst in späteren Jahren begegneten, begleiten die Diskussion um das ENUM schon in dessen Geburtsjahren.

Wie aufgezeigt werden konnte, sind im Rahmens des Internets noch eine Reihe von Problemen und Streitfragen, sei es struktureller, politischer oder technischer Natur offen, welche in den nächsten Jahren zu lösen sind. Sicherlich werden weitere hinzukommen, ohne daß diese heute schon vorhersehbar sind. Andererseits könnten einige Probleme auch schnell gelöst werden. So mögen viele Diskussionen um neue gTLDs, *Domain Grabbing*, Monopolstellungen von Unternehmen, ICANN und UDRP erlöschen, sobald die ICANN allgemeingültige Regeln zur Einführung neuer gTLDs eingeführt hat und daraufhin viele neue gTLDs der unterschiedlichen Zielrichtung in das jetzt schon bestehende Angebot an TLDs integriert werden. Die Selbstregulierungsverfahren und die daran beteiligten Institutionen können behilflich sein, diese und die noch aufkommenden Streitfragen einer für die Allgemeinheit nützlichen Lösung zuzuführen. So können auch für die kommenden Jahre spannende Auseinandersetzungen um staatliche Regulierung und Selbstregulierung des Internets erwartet werden.