Juristische Reihe TENEA / www.jurawelt.com Bd. 20

Marco Siegert

Das Internet – Grundlagenwissen für die Polizei

Geschichte · Technik · Multimediarecht · Strafrecht · Strafprozeßrecht · Gefahrenabwehr · Kinderpornographie

Juristische Reihe TENEA / www.jurawelt.com Bd. 20

20

TENEA

jurawelt.com
Jurawelt
Referendarswelt
Studentenwelt
Anwaltswelt

TENEA

Marco Siegert, geboren 1978 in Lutherstadt Wittenberg. 1996 Abitur am Albert-Schweitzer-Gymnasium in Coswig (Anhalt). Studium an der Fachhochschule der Polizei des Landes Brandenburg. 2000 Abschluss als Diplom-Verwaltungswirt – FH (Polizei). Derzeit Studium am Hasso-Plattner-Institut für Softwaresystemtechnik der Universität Potsdam.

Seit mehr als zehn Jahren erweckt eine der bedeutendsten technischen Entwicklungen des 20. Jahrhunderts zunehmend auch das Interesse der breiten Öffentlichkeit - die Rede ist vom Internet. Das Internet ist gerade dabei, alle Lebensbereiche unserer modernen Kommunikationsgesellschaft zu durchdringen. In der Zukunft wird es in fast allen Bereichen unserer Zivilisation eine nicht unwesentliche Rolle spielen.

So leuchtend die Zukunft der multimedialen Kommunikationsgesellschaft auch erscheint, so unbestreitbar bringt die Internettechnologie auch neue Gefahren hervor. Damit das Internet nicht zu einem »rechtsfreien Raum« wird, ist es u.a. notwendig, dass nationale und internationale Strafverfolgungsbehörden angemessen im »Cyberspace« vorgehen.

Hierzu ist es erforderlich, dass Polizeibeamte, Staatsanwälte und Richter über ein gewisses Grundwissen der technischen und soziokulturellen Zusammenhänge des Internets verfügen. Die Literaturrecherche des Autors zum vorliegenden Buch hat den Mangel an Grundlagenliteratur in diesem Bereich bestätigt.

Hierbei wird nicht die Fachliteratur zu den straf-, strafprozess-, und zivilrechtlichen Problemstellungen bemängelt, denn diese ist sehr umfangreich vorhanden. Vielmehr wird die polizeispezifische Fachliteratur kritisiert, die sich vor allem mit kriminalistischen und kriminologischen Problemstellungen und Aufgabenstellungen des Gefahrenabwehrrechts auseinandersetzen muss.

Das vorliegende Buch soll sich genau an dieser Stelle einordnen und - aus polizeilicher Sicht - die Vermittlung eines ersten Gesamtüberblicks versuchen, ohne dabei einen Anspruch auf Vollständigkeit zu erheben.

TENEA

ISBN 3-936582-55-6 26 € 52,80 SFr

TENEA

Juristische Reihe TENEA / www.jurawelt.com Bd. 20

Tenea (ἡ Τενέα), Dorf im Gebiet von Korinth an einem der Wege in die → Argolis, etwas s. des h. Chiliomodi. Sehr geringe Reste. Kult des Apollon Teneates. T. galt im Alt. sprichwörtl. als glücklich, wohl wegen der Kleinheit […]

Aus: K. Ziegler, W. Sontheimer u. H. Gärtner (eds.): *Der Kleine Pauly.* Lexikon der Antike. Bd. 5, Sp. 585. München (Deutscher Taschenbuch Verlag), 1979.

MARCO SIEGERT

Das Internet – Grundlagenwissen für die Polizei

Geschichte · Technik · Multimediarecht · Strafrecht · Strafprozeßrecht · Gefahrenabwehr · Kinderpornographie

TENEA

Marco Siegert:

Das Internet – Grundlagenwissen für die Polizei

Geschichte · Technik · Multimediarecht · Strafrecht · Strafprozeßrecht · Gefahrenabwehr · Kinderpornographie

(Juristische Reihe TENEA/www.jurawelt.com; Bd. 20)

© TENEA Verlag für Medien
Berlin 2002
Alle Rechte vorbehalten. All rights reserved.
Digitaldruck und Bindung:
Digital-Print-Service · 10119 Berlin
Umschlaggestaltung: nach Roland Angst, München
TENEA-Graphik: Walter Raabe, Berlin
Printed in Germany 2002

ISBN 3-936582-55-6

1 Inhalt

1 Inhalt 5

2 Vorwort 13

3 Historische Grundlagen 17

3.1 Allgemeines 17

3.2 Vorgeschichte 18
3.2.1 Der Kalte Krieg und die Gründung der ARPA 18
3.2.2 IPTO und Neuorientierung der ARPA 20
3.2.3 Die ersten Vernetzungskonzepte unter Taylor 22
3.2.4 Grundlagenarbeit von Baran und Davies 24

3.3 Experimentierphase 27
3.3.1 Aufbau eines experimentellen Paketvermittlungsnetzwerkes unter Roberts 27
3.3.2 Die Entwicklung der IMPs bei BBN 29
3.3.3 Die Installation der ersten IMPs und TIPs 31

3.4 Skalierungsphase 37
3.4.1 Die Weiterentwicklung des ARPANet 37
3.4.2 ALOHANet, PRNet, SATNet und TCP/IP 39
3.4.3 CSNet, NSFNet und INTERNET 43
3.4.4 Außerbetriebnahme des ARPANet 45
3.4.5 Kurzer Abriß der weiteren Entwicklung 46

4 Technische Grundlagen 49

4.1 Allgemeines 49

4.2 Transmission Control Protocol (TCP) 49

4.3 Internet Protocol (IP) 50

4.4 Domain Name System (DNS) 52

4.5 Client-Server-Architektur 55

4.6 Routing und Gateways 57

4.7 Organisation des Internets 58

4.8 Zugang zum Internet 61
4.8.1 Allgemeines 61
4.8.2 Zugangsmöglichkeiten nach Alpar und Ramm 61
4.8.3 Klassifizierung nach Jofer 63
4.8.4 Die Online-Dienste 64
4.8.5 Schlußfolgerung 65

4.9 Ethernet, Btx und Mailboxnetze 66
4.9.1 Ethernet 66
4.9.2 Bildschirmtext (Btx) und T-Online 66
4.9.3 Mailboxnetze und andere Online-Dienste 69

5 Die Dienste des Internets 71

5.1 Allgemeines 71

5.2 Elektronische Post (E-Mail) 72
5.2.1 Allgemeines 72
5.2.2 E-Mail-Anhänge (Attachments) 75
5.2.3 FreeMail 77
5.2.4 Digitale IDs 78

5.3 Diskussionsgruppen (News) 80
5.3.1 Allgemeines 80
5.3.2 E-Mail-Verteilerlisten und Listserver 81
5.3.3 Usenet Newsgroups (Usenet News, NetNews) 82

5.4 Telnet: Nutzung entfernter Ressourcen 85

5.5 Dateitransfer (FTP) 86

5.6 Suchdienste 88
5.6.1 Archie 88
5.6.2 Gopher 89
5.6.3 WAIS 90

5.7 Zeitgleiche Kommunikation 92
5.7.1 Internet Relay Chat (IRC) 92
5.7.2 Internet Phone (Iphone) 93
5.7.3 Worlds Chat (Wchat) 94
5.7.4 Multiple User Dungeon (MUD) und Multiplayer-Online-Games (MOG) 95

5.8 World Wide Web 96
5.8.1 Allgemeines 96
5.8.2 HTML (Hypertext Markup Language) 98
5.8.3 HTTP (Hypertext Transfer Protocol) 99
5.8.4 Uniform Resource Locator (URL), - Identifier (URI) und – Names (URN) 101
5.8.5 WWW-Gateways und WWW-Formulare 104
5.8.6 WWW-Browser 105

6 Die Zukunft des Internets 109

6.1 Die multimediale Zukunft des Internets 109

6.2 Das „Internet Protocol – Version 6“ (IPv6) 109

6.3 Die mobile Zukunft des Internets 110

6.4 Verschmelzung von Telefon und Internet 111

6.5 Hyper-G 112

7 Pornographie im Internet 115

7.1 Grundlagen 115

7.2 Die Bundesprüfstelle für jugendgefährdende Schriften (BPS) 116

7.3 Auswirkungen von Pornographie auf unsere Gesellschaft 116

7.4 Pornographie in unserer Gesellschaft 117

7.5 Kinderpornographie als Variante der harten Pornographie 119
7.5.1 Allgemeines 119
7.5.2 Die Strategie der Täter 121

7.6 Der „klassische“ Markt 126

7.7 Der Vertrieb über das Internet 128

8 Phänomenologie netzbezogener Straftaten 131

8.1 Allgemeines 131

8.2 Computerkriminalität 131

8.3 Versuch einer Klassifizierung der Computerkriminalität.....132
8.3.1 Netzspezifische Verbreitungsdelikte.....133
8.3.2 Das Internet als Mittel zur Tatkommunikation.....134
8.3.3 Das Internet als virtuelles Tatwerkzeug.....135

8.4 Kriminologische Erkenntnisgewinnung 135

8.5 Mißbrauchsmöglichkeiten ausgewählter Internet-Dienste.....137
8.5.1 Allgemeines.....137
8.5.2 Mißbrauch ohne Dienstbezug.....137
8.5.3 E-Mail.....139
8.5.3.1 Netzspezifische Verbreitungsdelikte 139
8.5.3.2 E-Mail als Mittel der Tatkommunikation..... 140
8.5.3.3 E-Mail als virtuelles Werkzeug 140
8.5.4 News.....142
8.5.4.1 Netzspezifische Verbreitungsdelikte 142
8.5.4.2 News als Mittel der Tatkommunikation 143
8.5.4.3 News als virtuelles Werkzeug 144
8.5.5 Telnet.....145
8.5.5.1 Netzspezifische Verbreitungsdelikte 145
8.5.5.2 Telnet als Mittel zur Tatkommunikation 145
8.5.5.3 Telnet als virtuelles Werkzeug 145
8.5.6 FTP 145
8.5.6.1 Netzspezifische Verbreitungsdelikte 145
8.5.6.2 FTP als Mittel zur Tatkommunikation 146
8.5.6.3 FTP als virtuelles Tatwerkzeug 146
8.5.7 IRC.....147
8.5.7.1 Netzspezifische Verbreitungsdelikte 147
8.5.7.2 IRC als Mittel zur Tatkommunikation..... 148
8.5.7.3 IRC als virtuelles Tatwerkzeug..... 149
8.5.8 Iphone 149
8.5.8.1 Netzspezifische Verbreitungsdelikte 149
8.5.8.2 Iphone als Mittel zur Tatkommunikation 150
8.5.8.3 Iphone als virtuelles Werkzeug 150
8.5.9 WWW 150
8.5.9.1 Netzspezifische Verbreitungsdelikte 150
8.5.9.2 Das WWW als Mittel zur Tatkommunikation 153
8.5.9.3 Das WWW als virtuelles Tatmittel 153

9 Strafverfolgung im Internet.....155

9.1 Grundlagen des materiellen Strafrechts.....155
9.1.1 Allgemeines.....155
9.1.2 Territorialitäts -, Ubiquitäts -, Weltrechts – und Personalitätsprinzip.....155
9.1.3 Der Tatortbegriff nach § 9 I StGB 157
9.1.4 Art. 296 EGStGB 160
9.1.5 Rechtfertigungsgründe 160
9.1.6 Verbotsirrtum nach § 17 StGB 161

9.1.7 Eingeschränkter Verfolgungszwang der Staatsanwaltschaft nach § 153 c StPO ... 162
9.1.8 Strafbarkeit der Provider ... 162
9.1.9 Garantenstellung der Provider ... 163
9.1.10 Das IuKDG und der MDStV ... 165
9.1.11 §§ 2, 3 und 4 TDG ... 166
9.1.12 § 5 TDG ... 167
9.1.13 Sperrung von rechtswidrigen Inhalten ... 170
9.1.14 Täterschaft und Teilnahme ... 172
9.1.15 Strafbarkeit von Links zu Seiten mit strafbaren Inhalten ... 173
9.1.16 Der Begriff der „Schrift“ ... 175
9.1.17 Stop-Seiten und Exclude-Filter ... 178
9.1.18 Zusammenfassung ... 179

9.2 Ausgewählte Rechtsprobleme aus dem Bereich des StGB ... 181
9.2.1 Allgemeines ... 181
9.2.2 § 86 [Verwenden von Kennzeichen verfassungswidriger Organisationen] StGB ... 183
9.2.3 § 184 [Verbreitung pornographischer Schriften] StGB ... 185
9.2.4 Surfen im Internet und Herunterladen von rechtswidrigem Material ... 186
9.2.5 Angeben einer falschen Identität ... 187
9.2.6 Anzeigepflichten ... 188
9.2.7 Recht am eigenen Bild ... 188
9.2.8 Newsgroups ... 188
9.2.9 Chat ... 190
9.2.10 E-Mail ... 191
9.2.11 Suchmaschinen und Verzeichnisse ... 193
9.2.12 Cookies ... 194
9.2.13 Hacker-Tools ... 195

9.3 Grundlagen des Strafprozeßrechts ... 195
9.3.1 Örtliche und sachliche Zuständigkeit ... 195
9.3.2 Ermittlungen mit Auslandsbezug ... 197
9.3.3 Aktive Mitwirkungspflichten von Zeugen und Betroffenen ... 199
9.3.4 Zusammenfassung ... 202

9.4 Ausgewählte Rechtsprobleme aus dem Bereich der StPO ... 202
9.4.1 Durchsuchung von Räumlichkeiten und Computern ... 202
9.4.2 Sicherstellung/Beschlagnahme von Hardware ... 204
9.4.3 Überwachen von Mailboxen ... 206
9.4.4 Sicherstellung/Beschlagnahme von Computerdaten ... 212
9.4.5 Abruf von E-Mails ... 213
9.4.6 Zusammenfassung ... 215

10 Gefahrenabwehr im Internet 217

10.1 Allgemeines 217

10.2 Abgrenzung von TDG und MDStV 218

10.3 Zuständigkeiten 219
10.3.1 Sachliche Zuständigkeit 219
10.3.2 Örtliche Zuständigkeit 220

10.4 Materielle Voraussetzungen 221

10.5 Störerbegriffe 223

10.6 Sonderproblem – Hyperlinks 226

10.7 Störerauswahl 227

10.8 Grundsatz der Verhältnismäßigkeit 228
10.8.1 Allgemeines 228
10.8.2 Geeignetheit 228

10.9 Erforderlichkeit 229

10.10 Verhältnismäßigkeit im engeren Sinne 230

10.11 Die anlaßunabhängige Recherche im Internet durch das BKA 230

10.12 Zusammenfassung 234

11 Schluß 237

12 Anlagen 239

12.1 Anlage 1 – Liste wichtiger Institutionen für das Internet 239

12.2 Anlage 2 – Die Zukunft des mobilen Datenfunks (Stand 1999) 241

12.3 Anlage 3 – LIST Kommando des Listservers 242

12.4 Anlage 4 – Einige Smiles und Abkürzungen im IRC 243

12.5 Anlage 5 - Ausgewählte indizierungsfähige Medien der BPS 244

13 Verzeichnisse 245

13.1 Abbildungsverzeichnis 245

13.2 Tabellenverzeichnis 246

13.3 Literaturverzeichnis 247

14 Index 257

2 Vorwort

Seit mehr als zehn Jahren erweckt eine der bedeutendsten technischen Entwicklungen des 20. Jahrhunderts zunehmend auch das Interesse der breiten Öffentlichkeit und somit auch der Strafverfolgungsbehörden. Die Rede ist vom Internet. Dieses globale Computernetzwerk ist ein Zusammenschluß aus vielen kleinen (regionalen und überregionalen) Netzwerken auf der Grundlage von TCP/IP. Das Internet ist gerade dabei, alle Lebensbereiche unserer modernen Kommunikationsgesellschaft zu durchdringen. In der Zukunft wird es in fast allen Bereichen unserer Zivilisation eine nicht unwesentliche Rolle spielen.

Die Bedeutung des Internets kann mit der Nutzbarmachung des elektrischen Stroms oder der Erfindung des Automobils gleichgesetzt werden. So leuchtend die Zukunft unserer multimedialen Gesellschaft auch erscheint, so unbestreitbar birgt diese Zukunftstechnik aber auch neue Gefahren in sich. Zweifellos überwiegen die Vorteile. Dennoch darf nicht verschwiegen werden, daß neue Technik auch immer neue Mißbrauchsmöglichkeiten oder alte Mißbrauchsmöglichkeiten im „neuen Gewande“ ermöglicht. An dieser Stelle soll sich der Gegenstand des Buches einordnen. Die für Strafverfolgungsbehörden – insbesondere die Polizei – wichtigen Aspekte sollen in ihrer Komplexität dargestellt, Zusammenhänge – auch für den Laien verständlich - herausgearbeitet werden.

Die zwei ersten Hauptteile behandeln historische und technische Grundlagen des Internets. Zwei weitere Abschnitte sollen straf- und strafprozeßrechtliche Gesichtspunkte sowie Aspekte der Gefahrenabwehr berücksichtigen. Ein Punkt wird sich mit der Phänomenologie von Internetstraftaten beschäftigen. An dieser Stelle wird aufgezeigt, welche Mißbrauchshandlungen im Internet bereits vorgekommen sind und welche Möglichkeiten die Technik grundsätzlich noch bietet. Abgerundet werden die Darstellungen durch einen internetbezogenen Teil, der sich ausschließlich mit Pornographie im Allgemeinen und Kinderpornographie im Speziellen beschäftigt.

Dieses Buch richtet sich vornehmlich an Polizeibeamte. Im Bereich der Gefahrenabwehr wird zwar exemplarisch die Rechtslage im Bundesland Brandenburg behandelt, dennoch haben vor allem die Ausführungen zu den straf- und strafprozessrechtlichen Regelungen allgemeingültigen Charakter. Es wird

vorausgesetzt, daß grundlegende Kenntnisse im Umgang mit Computern vorhanden sind. Die technischen Grundlagen des Internets werden durch dieses Buch erst vermittelt.

In der Vergangenheit wurde das Thema „Polizei und Internet“ meist stiefmütterlich behandelt. Dies wird vor allem auch dadurch deutlich, daß meine Recherche zu polizeispezifischer Fachliteratur nur wenige Beiträge hervorbrachte. Es gibt noch genügend polizeibezogene Fragen, die einer ausführlichen Betrachtung bedürfen. M.E. kommt es hierbei nicht so sehr auf die Erörterung juristischer Probleme an, denn hierfür gibt es ausreichend fachspezifische Literatur. Die Polizei muß für ihren eigenen Tätigkeitsbereich - der Prävention und der Repression - forschen. Daher gilt es vor allem kriminalistische und kriminologische Fragestellungen, die sich im Zusammenhang mit den neuen Medien ergeben, zu erforschen.

Ich hoffe, durch meine Arbeit einen kleinen Beitrag für die Bewältigung der noch vor uns liegenden Entwicklung geleistet zu haben. Die Ausführungen erheben keinen Anspruch auf Vollständigkeit, dennoch werden nach meinem Empfinden die wesentlichsten Fragen, die sich durch die zunehmende Bedeutung des Mediums Internet ergeben, behandelt werden. Es bedarf sicherlich keiner weiteren Erörterung, daß einzelne Teilbereiche - die diese Arbeit nur anschneiden kann - mehrere Bände füllen könnten. Aus diesem Umstand wird auch ersichtlich, daß es mitunter sehr schwierig sein wird, das Wesentliche vom Unwesentlichen zu trennen. Ich hoffe, daß es mir gelingen wird.

Ein weiteres Problem stellen die zur Zeit noch existierenden mannigfachen juristischen Lösungsansätze im Bereich des Straf – und des Strafprozeßrechts dar. Nur zögernd wagt sich die Rechtsprechung in das juristische Neuland vor. Dementsprechend werden in der Literatur auch viele unterschiedliche Ansätze und Meinungen vertreten. Es ist daher nicht verwunderlich, daß man durchaus – bei der Betrachtung ein und derselben Fragestellung – zu unterschiedlichsten Lösungen kommen kann. Dies gilt es zu beachten. Die aktuelle Rechtsprechung wurde – soweit ersichtlich – eingearbeitet.

Beim Lesen der nachfolgenden Ausführungen ist auf folgende Besonderheiten zu achten: Zitate werden durch doppelte Anführungszeichen („“) eingeschlossen. Text in eckigen Klammern bedeutet innerhalb von Zitaten eine Ergänzung durch den Verfasser ([Ergänzung]). Außerhalb von Zitaten und inner-

halb von Paragraphenangaben enthalten sie den geläufigsten Paragraphentitel (§ 184 [Verbreitung pornographischer Schriften] StGB). Innerhalb von Zitaten bedeuten drei, durch eckige Klammern eingeschlossene Punkte ([...]), Auslassungen durch den Verfasser. Quellenangaben erscheinen in eigener Kurzschreibweise in den Fußnoten. Die genaue Quellenangabe befindet sich im Literaturverzeichnis, welches alphabetisch nach den Nachnamen der Verfasser geordnet wurde. Sofern eine Quelle übernommen wurde, findet sich ihr Nachweis direkt in der jeweiligen Fußnote. Reine Gerichtsurteile wurden teilweise nicht in das Literaturverzeichnis aufgenommen, sondern nach allgemein anerkannten juristischen Regeln direkt in den Fußnoten zitiert. Gesetzesnamen wurden in den geläufigen Abkürzungen verwendet. Es wurde weitestgehend darauf verzichtet, Internetquellen zu zitieren. Wurde eine Quelle aus dem Internet zitiert, wird hinter der URL das Abrufdatum in eckigen Klammern angegeben (http://www.tiscalinet.de[05.08.2000]). Dies ist von besonderer Bedeutung, da sich die Adresse von Internetdokumenten schnell ändern kann. Das Datum bezieht sich auf den Zeitpunkt, an dem der Inhalt in der gemeinten Form letztmalig abgerufen wurde[1].

Ich wünsche mir, daß meine Ausführungen interessierte und kritische Leser finden werden. Ferner hoffe ich, daß sie andere Autoren – die sich vielleicht mit diesem Thema auseinandersetzen möchten – inspirieren, ebenfalls ihren durchaus notwendigen Beitrag zum Thema „Polizei und Internet“ zu leisten.

Ich möchte mich an dieser Stelle bei all den Menschen bedanken, die direkt, durch fachliche und inhaltliche Unterstützung, oder indirekt, durch ihre Geduld mit meiner ruhelosen Person, zum Gelingen dieser Arbeit beigetragen haben. Insbesondere bedanke ich mich bei Herrn Grossmann, Herrn Prof. Dr. Wirth, Frau Förster, meinen Eltern, Großeltern und Geschwistern und natürlich bei meiner lieben Steffi.

Marco Siegert, Potsdam im Dezember 2002

---

[1] Das Internet gewinnt in allen Bereichen der wissenschaftlichen Arbeit zunehmend an Bedeutung. Das ist nicht verwunderlich, denn es wurde ja zu diesem Zweck entwickelt. Eine Möglichkeit, Internetquellen dauerhaft nachvollziehbar zu machen, stellt die Spiegelung (Speicherung) einer Homepage (Internetquelle) auf CD-ROM dar. Durch die Konvertierung von wissenschaftlichen Ausarbeitungen in das HTML-Format könnte eine effektive Einbeziehung der Internettechnik in die wissenschaftliche Literatur erfolgen.

3 Historische Grundlagen

3.1 Allgemeines

Nach Alpar läßt sich die Entstehung des Internets grundsätzlich in drei Phasen einteilen[2]. Er verwendet für diese drei Entwicklungsstufen die Begriffe Experimentierphase, Skalierungsphase und Kommerzialisierung des Internets[3].

Hierbei umfaßt die Experimentierphase nach seiner Ansicht das erste Entwicklungsstadium und die Einrichtung der ersten Netzwerkknoten des ARPANet. Die Skalierungsphase umfaßt das „Wachstum“ des Netzwerkes und dessen Ausbreitung über den nordamerikanischen Kontinent. Berücksichtigt werden müssen hier auch die Parallelentwicklungen außerhalb Amerikas und die Einführung neuer Techniken. Die Entwicklung des NSFNets spielt hierbei eine wesentliche Rolle. Die Kommerzialisierung des Internets setzte ein, als ab 1995 für kommerzielle Unternehmen die Möglichkeit bestand, ihre Netzwerke mit dem Internet zu verbinden oder auf sonstigen anderen Wegen Netzpräsenz zu erlangen.

Derzeit befinden wir uns in der Phase der Kommerzialisierung des Internets. Ob es noch eine weitere Entwicklungsstufe geben wird, ist noch nicht genau abzusehen. M.E. ist diese Weiterentwicklung aber sehr wahrscheinlich. Wie sie konkret aussehen wird, kann man zur Zeit noch nicht genau abschätzen, da alle naheliegenden Erweiterungsmöglichkeiten noch im Bereich der Kommerzialisierung liegen. Die zukünftige Entwicklung des Internets wird allein der technischen und gesellschaftspolitischen Entwicklung entsprechen.

M.E. ist die Gliederung in die drei beschriebenen Entwicklungsstufen durch Alpar nicht ausreichend, da das ARPANet als Vorläufer des Internet nicht „aus dem Nichts“ entstanden ist. Vor der Installation der ersten Netzwerkknoten gab es eine gewisse Vorlaufzeit, die sich vor allem in drei wesentlichen Punkten von der Experimentierphase unterscheidet.

Zuerst wäre an dieser Stelle die politische Situation zu nennen, die einen maßgeblichen Einfluß auf die Entstehung des ARPANets hatte. Zum anderen

---

[2] Alpar, Kommerzielle Nutzung des Internet, Seite 13 - 23

[3] Ein kurzer Abriß der Geschichte des Internet bei: Hartung, Internet, dp-special April 1998, Seite 2 - 15

war eine gewisse theoretische Vorleistung erforderlich, die im Grunde nicht direkt auf die Errichtung eines Netzwerkes abzielte. Abschließend ist anzumerken, daß ein Experiment nur mit einem Versuchsaufbau im klassischen Sinne beginnen kann. Daher kann man erst ab der wirklichen Installation der ersten Netzwerkknoten von einer wirklichen Experimentierphase sprechen. Als Ergebnis dieser Überlegungen wird sich der nachfolgende Abschnitt an der Gliederung nach Vorgeschichte, Experimentierphase, Skalierungsphase und Kommerzialisierung ausrichten.

3.2 Vorgeschichte

3.2.1 Der Kalte Krieg und die Gründung der ARPA

In der Literatur wird häufig die Ansicht vertreten, daß das ARPANet - als Vorläufer des Internets - entwickelt wurde, um einem Atomwaffenangriff auf das Territorium der USA, durch die zu der Zeit noch bestehende UdSSR, begegnen zu können[4]. Grundlage dieser Meinung ist eine Annahme aus den Anfangszeiten des Kalten Krieges. Dabei ging man von der Hypothese aus, daß die Zerstörung der feindlichen Kommunikationswege die erste Hürde beim angestrebten Sieg über den Feind sei. Durch die Schaffung einer netzähnlichen Kommunikationsstruktur wollte man dieser Gefahr begegnen. Bei der Ausschaltung eines Vermittlungspunktes würde eine Nachricht eben einen anderen Weg nehmen und so auf jeden Fall ihr Ziel erreichen. Diese vorangestellte Aussage wird hartnäckig in der Literatur vertreten. Sie verwehrt aber den Blick auf die wahren Hintergründe, die zur Entwicklung des Netzwerkes führten[5]. Aus diesem Grund soll nun an dieser Stelle eine etwas ausführlichere Darstellung der geschichtlichen Abläufe erfolgen.

Nach dem Ende des 2. Weltkrieges begann bekanntlich die Phase des „Kalten Krieges“, in der sich vor allem die USA und die UdSSR als imaginäre Gegner gegenüberstanden. Diese Zeit war auf beiden Seiten nicht nur durch einen Wirtschaftsboom, sondern auch durch Wettrüsten und den Kampf um die Hegemonie im Weltall geprägt. Im Oktober 1957 schickten die Russen ihren

---

[4] Fink, Die Welt von T-Online, Seite 153

[5] Hafner/Lyon, Arpa Kadabra oder die Geschichte des Internet, Seite 10

Satelliten „Sputnik I“ in den Kosmos und demonstrierten auf diese Weise ihren erheblichen Forschungs – und Technologievorsprung vor den USA. In den Vereinigten Staaten, derzeit unter der Präsidentschaft Eisenhowers, löste der russische Satellitenstart eine nationale Krise aus. „Plötzlich saß, wie es der Präsident ausdrückte, der amerikanischen Psyche ´das Gespenst der umfassenden Vernichtung´ im Nacken“[6], da man die eigene nationale Sicherheit durch die neuen sowjetischen Erfolge in der Raumfahrt bedroht sah.

Da Eisenhower erkannte, daß die USA Gefahr liefen, ihren technologischen Vorsprung einzubüßen, strebte er die Mobilisierung der amerikanischen Wissenschaft und Forschung an. Als erstes setzte er sich mit einem Beraterkomitee - bestehend aus einer umfänglichen Abordnung der bedeutendsten amerikanischen Wissenschaftler – zusammen, um die Situation zu erörtern. Das Komitee kam zu dem Ergebnis, daß Eisenhower als erstes einen unabhängigen Berater für Wissenschaftsfragen einsetzen sollte. Weiterhin stellte das Gremium fest, daß die wissenschaftliche Forschung auf dem Militärsektor durch eine unabhängige Behörde koordiniert werden sollte. Der Start von „Sputnik II“, nur einen Monat nach „Sputnik I“, verstärkte den Druck auf den Präsidenten nochmals. Im November 1957 gab Eisenhower dann seine Entscheidung bekannt. Zum ersten Sonderberater für Wissenschaftsfragen wurde der Präsident des Massachusetts Institute of Technology, Killian, ernannt.

Zusammen mit Killian, und nach mehreren Beratungen mit dem wissenschaftlichen Ausschuß, schlug der Verteidigungsminister McElroy die Einrichtung einer unabhängigen Behörde für Entwicklung und Forschung vor. Sie sollte dem Verteidigungsminister direkt unterstellt werden. Die originäre Aufgabe dieser Behörde sollte darin bestehen, Forschungsmittel zentral zu verwalten und erfolgversprechende Forschungsprojekte zu initiieren und zu unterstützen.

Durch diese geplante Konzentration wollte man alle Forschungsprojekte, die vorher den einzelnen Teileinheiten der amerikanischen Streitkräfte zugeordnet waren, einer Behörde unterstellen. Sie allein sollte die Koordination übernehmen und die Aufsicht führen. Zudem war McElroy davon überzeugt, „daß eine Zentralstelle für die Organisation wissenschaftlicher Forschungsprojekte die Rivalität zwischen den Waffengattungen weitgehend beseitigen wür-

[6] ebd., Seite 15

de, weil damit die staatlichen Forschungsgelder im wesentlichen seiner direkten Aufsicht unterstellt würden.“[7]

Obwohl die Regierung noch größere Zukunftspläne hatte, die insbesondere die Schaffung einer Raumfahrtbehörde - der „National Aeronautics and Space Administration“ (NASA) - vorsahen, unterstützte der Präsident das Vorhaben. Am 20. November verkündete McElroy vor dem Kongreß seine Pläne, die militärische Forschung einer zentralen Behörde zu unterstellen. Es konnten nun konkrete Dienstanweisungen für die neue Behörde ausgearbeitet werden. Wie erwartet, stießen die Entwürfe in den Stäben der Army, Navy und Air Force auf heftige Kritik, da diese ihre Forschungsgelder schwinden sahen. Ungeachtet entgegenlaufender Bestrebungen, konnten die Entwürfe grundsätzlich umgesetzt werden. Am 7. Januar 1958 beantragte Eisenhower für die neue Behörde mit dem Namen „Advanced Research Projects Agency“ (ARPA) die notwendigen Mittel beim Kongreß, der diese dann auch bewilligte. Der erste Leiter der ARPA wurde Johnson, Vorstandsmitglied von General Electric. Als wissenschaftlicher Leiter wurde York vom Lawrence Livermore Laboratory ausgewählt.

Die ARPA nahm mit einer finanziellen Erstausstattung von 520 Millionen Dollar und einem Budget von 2 Milliarden Dollar ihren Dienst im Pentagon auf. „Sie erhielt die Oberaufsicht über alle US-amerikanischen Raumfahrtprogramme und alle strategischen Raketenprojekte. 1959 zählte der Stab etwa 70 Leute. [...] Dabei handelte es sich vor allem um wissenschaftliche Projektleiter, die Anträge für Forschungs – und Entwicklungsprojekte analysierten und begutachteten und die Arbeit hunderter Vertragspartner überwachten.“[8]

3.2.2 IPTO und Neuorientierung der ARPA

Als im Spätsommer 1958 das Gesetz zur Gründung der NASA in Kraft trat, kamen die ersten gravierenden Änderungen auf die ARPA zu. Die Raumfahrt- und die Raketenprogramme wurden der NASA unterstellt. In der Folge sank das Budget der ARPA auf 150 Millionen Dollar. Praktisch jeglicher Legitimation beraubt, suchte die ARPA nach einem neuen Tätigkeitsbereich. In dieser Pha-

[7] ebd., Seite 20

[8] Hafner/Lyon, Arpa Kadabra oder die Geschichte des Internet, Seite 22

se der Aufgabenneuverteilung erkannte man, daß der Behörde der Bereich der wissenschaftlichen Grundlagenforschung übertragen werden konnte. In diesem Sinne wurde die ARPA umstrukturiert und eine Fördereinrichtung für Forschungsprojekte mit relativ ungewissen Erfolgsaussichten - aber auch potentiellem Nutzen.

Unter der Präsidentschaft Kennedys und der Aufsicht des Verteidigungsministers McNamara konnte sich die ARPA wieder etablieren. Unter Kennedy wandelte sich die amerikanische Verteidigungsstrategie. Aus einer Politik der massiven Vergeltung wurde eine Strategie der flexiblen Reaktion. Der wissenschaftliche Sektor des Verteidigungsministeriums gewann zunehmend an Bedeutung. Zu Beginn des Jahres 1961 wurde in der ARPA die Position des Vizedirektors neu besetzt. Ruina löste Betts ab. Unter Ruina wurde der Jahresetat der Behörde auf 250 Millionen US Dollar erhöht. Zu der Zeit beschäftigte sich die ARPA vor allem mit Grundlagenforschung zur Raketenabwehr oder mit Nachweismethoden für Atomwaffenversuche sowie Verhaltensforschung im Bereich der militärischen Kommando- und Kontrollstrukturen.

Im selben Jahr erhielt die ARPA von der Air Force einen Großcomputer, den Q-32. Dieser war zuvor zur Unterstützung eines Frühwarnsystems der Luftabwehr eingesetzt worden. Innerhalb der ARPA wurde der Computer einem Projekt zugeordnet, das sich ab 1962 unter der Leitung Lickliders mit militärischen Kommando– und Kontrollstrukturen beschäftigte. Dieses Projekt sollte erforschen, inwieweit Computer (und hier vor allem Time-Sharing-Systeme[9]) militärische Entscheidungsprozesse beeinflussen könnten. Unter Licklider konnte die Forschung im Bereich der künstlichen Intelligenz und der gesamten Computerwissenschaft vorangetrieben werden.

In diesem Zusammenhang wurden auch erstmals Probleme einer Vernetzung von verschiedensten Computern erörtert und erforscht, wodurch sich grundsätzlich die Hauptzielrichtung der Forschungsabteilung änderte. Über seine Computervisionen verfaßte Licklider 1960 den wegweisenden Artikel „Man-Computer-Symbiosis“. Licklider zeigte mögliche Beziehungen zwischen Mensch und Maschine auf. Als er 1964 die ARPA verließ, „war es ihm gelungen, die Forschungs – und Entwicklungstätigkeit der Computerforschungsabtei-

lung in eine neue Richtung zu lenken: weg von der Beschäftigung mit Command – and Control-Systemen [...], hin zu Arbeiten an Time-Sharing-Systemen, Computergrafik und verbesserten Computersprachen“[10]. Dementsprechend wurde die Abteilung „Command and Control Research“ in „Information Processing Techniques Office“ (IPTO[11]) umbenannt. Nachfolger Lickliders wurde Sutherland.

3.2.3 Die ersten Vernetzungskonzepte unter Taylor

1965 wurde Taylor Assistent Sutherlands, später 3. Direktor der IPTO. Er betreute die verschiedenen Computerforschungsprojekte der Abteilung. Zu dieser Zeit konzentrierte sich die Computerforschung vor allem in räumlich weit auseinander-gelegenen Universitäten und ähnlichen Forschungseinrichtungen. Die Institutionen wurden zu diesem Zweck durch die ARPA mit Computern und Forschungsgeldern ausgestattet. Taylor hatte in einem Terminalraum drei Terminals stehen, mit denen er getrennten Zugriff zu drei solcher Computer[12] herstellen konnte. Diese Rechner hatten alle ein anderes Betriebssystem, verlangten eine unterschiedliche Anmeldeprozedur und arbeiteten mit verschiedenen Befehlssätzen. Anhand dieser Problematik erkannte Taylor die revolutionären Möglichkeiten, die Lickliders Computervisionen boten.

Ergänzend kamen weitere Aspekte hinzu. Im steigenden Maße forderten die Universitäten für ihre Forschungsarbeiten immer mehr Computerressourcen.

Da es sich hierbei ausschließlich um Großrechner handelte, stiegen die Kosten natürlich an. Desweiteren bestand zunehmend die Gefahr, daß in den verschiedenen Institutionen vermehrt Doppelarbeit geleistet wurde, da die Wissenschaftler ja nicht direkt miteinander kommunizieren und so ihre Forschungsergebnisse nicht austauschen konnten. Auch hier bot sich ein Computernetzwerk im Sinne Taylors an, da so Ressourcen gemeinsam genutzt und Rechenleistung verteilt werden konnte. Zusätzlich eröffnete sich dadurch auch

---

[9] Unter Time-Sharing-Systemen versteht man Computer, an denen mehrere Terminals angeschlossen werden und die somit mehreren Nutzern Zugriff auf die Rechenleistung eines Computers ermöglichen

[10] Hafner/Lyon, Arpa Kadabra oder die Geschichte des Internet, Seite 45

[11] Büro für Grundlagen der Datenverarbeitung, IPTO

die Möglichkeit, finanzielle Ausgaben zu senken, da nur wenige leistungsstarke und teure Rechner benötigt wurden. Das Netzwerk konnte einen gemeinsamen Zugriff auf die Rechner gewährleisten.

Am Ende dieses Erkenntnisprozesses beantragte Taylor beim damaligen Leiter der ARPA, Herzfeld, die Genehmigung für die Einrichtung eines erweiterbaren experimentellen Computernetzwerkes[13]. Das Netzwerk sollte allein aus dem Grund eingerichtet werden, räumlich verteilte Forschungsstätten miteinander zu verbinden und Wissenschaftlern einen Zugang zu gemeinschaftlich nutzbaren Ressourcen zu ermöglichen[14].

Unmittelbar nach der Bewilligung der finanziellen Mittel begann Taylor mit dem Aufbau und der Organisation des Netzwerkprojekts. 1966 übernahm er die Leitung der IPTO. Die Projektleitung wurde an Roberts vergeben, der vom Lincoln Laboratory zur ARPA kam. Dort hatte er bereits ein Experiment überwacht, bei dem der Computer des Lincoln Laboratory mit dem Computer vom SDC in Santa Monica , über eine eigens dafür verlegte Vollduplexleitung[15], verbunden wurde. Er begann unmittelbar mit der Konzeptionierung des Netzwerkes.

„Zu dieser Zeit verfügte man bereits über umfangreiches Wissen zum Bau komplizierter Übertragungsnetze für Stimm-, Geräusch– und andere einfachere Signale.“[16] Mit Erfindung des Telefons und der Telegrafie hatte die Menschheit den Grundstein für überregionale Kommunikation gelegt. Nun begab sie sich mit einer weiteren Möglichkeit - der netzwerkfähigen Datenübertragung – auf den Weg in ein neues Kommunikationszeitalter.

Die Firma AT&T besaß zu der Zeit nahezu das Monopol im amerikanischen Telefonmarkt. Bereits in der Vergangenheit hatte sie mehrmals ihre Vorherrschaft ausgenutzt, Neuentwicklungen im Telefonbereich zu unterbinden. Dadurch war es ihr immer wieder gelungen, die eigene Vormachtstellung auf-

---

[12] Bei den drei Computern handelte es sich um Rechner an den Standorten: Cambridge („Massachusetts Institute of Technology“ (MIT)), Berkley (Universität von Kalifornien) und der Santa Monica

[13] Hafner/Lyon, Arpa Kadabra oder die Geschichte des Internet, Seite 48 und 49

[14] ebd., Seite 10

[15] Eine Vollduplexleitung erlaubt eine simultane Datenübertragung in beide Richtungen zwischen zwei Punkten.

[16] Hafner/Lyon, Arpa Kadabra oder die Geschichte des Internet, Seite 59

recht zu erhalten[17]. Es war also zu erwarten, daß AT&T auch dieses Projekt blockieren würde[18]. Es stand fest, daß für die Übertragung von Computerdaten das bestehende Telefonnetz ungeeignet war. Den Telefonnetzen liegen sogenannte zentralisierte Netzmodelle zugrunde, d.h. daß von einem zentralen Punkt („Nervenzentrum“) die entsprechenden Verbindungen zu den anderen Punkten sternförmig abgehen. Eine weitere Netzwerkstruktur stellte das dezentralisierte Netzmodell dar. Hier sind mehrere „Nervenzentren“ durch Fernleitungen miteinander verbunden. Übertragen wurden die Signale analog. Das hatte zur Folge, daß mit zunehmender Länge der Übertragungswege die Stärke der Signale abnahm und so Informationen verloren gehen konnten. Für den Aufbau eines Computernetzwerks war die herkömmliche Netzwerktechnik also nicht nutzbar. Es bedurfte neuer Netzwerkstrukturen, neuer Vermittlungstechnik und einer neuen Übertragungsart für Daten.

3.2.4 Grundlagenarbeit von Baran und Davies

Noch bevor Roberts mit der Arbeit an dem Netzwerkprojekt begann, „gelangten zwei Forscher, Paul Baran und Donald Davies – die einander nicht kannten und auf verschiedenen Kontinenten auf verschiedene Ziele hinarbeiteten - zu praktisch derselben revolutionären Idee für ein neuartiges Kommunikationsnetz“[19]. Die wesentlichsten Eigenschaften dieses neuartigen Kommunikationsnetzes kann man wie folgt zusammenfassen: Bei der Netzwerkstruktur sollte es sich um ein sogenanntes verteiltes Netzwerk handeln. Bildlich kann man sich diese Form Netzwerk wie eine Art Fischernetz vorstellen.

Die einzelnen Netzwerkknoten sind grundsätzlich nicht nur mit einem Zentrum, sondern auch mit ihren Nachbarknoten verbunden. Diese Knoten sind abermals mit ihren Nachbarknoten verbunden[20]. Desweiteren sollte die Daten-

---

[17] Ein Beispiel für eine solche Vorgehensweise stellt das durch AT&T angeregte Verbot des „Hush-A-Phone“ (Telefon mit Kunststoffabdeckung über der Sprechmuschel, damit man nicht mithören konnte, was der Sprecher sagt) durch die Federal Communications Commission.

[18] Hafner/Lyon, Arpa Kadabra oder die Geschichte des Internet, Seite 60

[19] ebd., Seite 61

[20] Den Grad der Vernetzung zwischen den Knoten eines Netzwerkes nennt man Redundanzniveau; ein Netz mit der absoluten Mindestzahl an Verbindungen zwischen den Knoten hat das Redundanzniveau I.

übertragung nicht mehr analog, sondern digital erfolgen[21]. Letztendlich erfolgte die Nachrichtenübertragung nicht mehr in einem ganzen Stück, sondern in einzelnen Paketen. Das bedeutet, daß eine Nachricht in mehrere gleich große Teile zerlegt wird und diese - mit der Zieladresse der Nachricht versehenen Pakete - auf unterschiedlichen Wegen zu ihrem Ziel gelangen. Am Bestimmungsort sollten die einzelnen Nachrichtenblöcke dann wieder in der richtigen Reihenfolge zusammengesetzt werden.

Baran entwickelte seine Idee im militärischen Bereich auf dem Gebiet der Kommunikationsstrukturforschung[22]. Da man erkannt hatte, daß die Überlebenschance bei und nach einem atomaren Angriff maßgeblich von der Funktionstüchtigkeit des Kommunikationsnetzes abhing, suchte man nach entsprechenden Verbesserungsmöglichkeiten. Allein aus diesem Grund entwickelte Baran die vorangestellte Netzwerktheorie. Nach seiner Ansicht würde ein solches Netzwerk eine sichere Kommunikation über weite Entfernungen bieten, weil bei der Zerstörung eines Netzwerkknotens ein Paket eben einen anderen Weg nehmen würde[23].

Nach Barans Vorstellungen sollten die einzelnen Knoten des Netzwerks spezielle Computer sein. In diesem „Modell enthielt jeder Knoten eine Verkehrslenkungstabelle, die als Art Transportkoordinator oder Verteiler fungierte. [...] Die Tabelle gab auch den jeweils besten Leitweg an und wurde durch Informationen über benachbarte Knoten, Entfernungen und Verzögerungen ständig auf den neusten Stand gebracht“[24]. Damit dieses System auch effektiv arbeiten konnte, sollten die Tabellen[25] ständig aktualisiert werden.

Als Baran sein Modell bei AT&T vorstellte, stieß er wie bereits angedeutet auf heftigen Widerstand. Es dauerte 4 Jahre, bis er alle Einwände gegen sein Modell entkräften konnte, dennoch verweigerte AT&T die Einrichtung eines ex-

---

[21] In der Computerwelt werden Daten digital verarbeitet, der Computer kennt nur die Zustände ein und aus (viel Strom und wenig Strom, 0 und 1); digitale Daten sind einfacher speicher – und reproduzierbar.

[22] Baran arbeitet zu der Zeit für die private Firma RAND, die von der Air Force finanziert wurde und sich u.a. mit der Überlebensfähigkeit von Kommunikationssystemen beschäftigte.

[23] Die Wahrscheinlichkeit, daß ein Paket sein Ziel erreicht, steigt mit zunehmendem Redundanzniveau; bereits bei einem Redundanzniveau von III oder IV ging man von einer optimalen Leistungsfähigkeit des Netzes aus.

[24] Hafner/Lyon, Arpa Kadabra oder die Geschichte des Internet, Seite 71

[25] In diesem Zusammenhang spricht man auch von Routing-Tabellen; die dazugehörigen Computer nennt man Router, da sie ausschließlich für die "Verkehrslenkung" zuständig sein sollten.

perimentellen Netzwerks. Als man Baran vorschlug, ein solches Netzwerk durch die Defense Communications Agency (DCA) aufbauen zu lassen, lehnte dieser ab, und das Projekt verschwand vorerst in der Versenkung[26].

„Im Herbst 1965, kurz nachdem Baran die Arbeit an seinem Vorhaben eingestellt hatte, machte sich Donald Watts Davies [...] die ersten persönlichen Notizen, in denen er einige Ideen zu einem neuen Computernetzwerk entwikkelte.“ [27] [28] Nach Abschluß eines Vortrages über seine Idee eines digitalen Speichervermittlungsnetzwerkes trat ein Mitarbeiter des amerikanischen Verteidigungsministeriums an Davies heran und informierte ihn über das gescheiterte Vorhaben Barans. Als man das Potential erkannte, welches in der Theorie Davies steckte, wurde er zum Leiter der Informatikabteilung am NPL ernannt.

Die Modelle von Baran und Davies ähnelten sich sehr stark. Unterschiede gab es nur in wenigen Punkten. Beide Theorien bauten auf einer digitalen Paketvermittlung[29] mit einer adaptiven Verkehrslenkung[30] auf.

Der größte Unterschied zwischen Baran und Davies bestand in den Zielen, die die beiden Forscher mit ihren Projekten verfolgten. Während Baran ein überlebensfähiges Netzwerk einrichten wollte, bemühte sich Davies, eine bessere Kommunikationsgrundlage für vernetzte Computer zu schaffen.

---

[26] Baran lehnte die DCA ab, weil er diese staatliche Organisation noch für inkompetenter hielt als AT&T.

[27] Davies arbeitete zu der Zeit als Physiker am britischen National Physical Laboratory (NPL) in London.

[28] Hafner/Lyon, Arpa Kadabra oder die Geschichte des Internet, Seite 75

[29] Baran sprach in diesem Zusammenhang von „distributed adaptive message block switching“ (dt.: verteilte adaptive Nachrichtenblockvermittlung), Davies prägte den später anerkannten Begriff „Paket-Switching“ (dt.: Paketvermittlung).

[30] Unter adaptiver Verkehrslenkung versteht man die ständige Aktualisierung der Routing-Tabellen und die Anpassung des Routing an die verschiedene Netzwerkbelastung.

3.3 Experimentierphase

3.3.1 Aufbau eines experimentellen Paketvermittlungsnetzwerkes unter Roberts

Als Roberts im Dezember 1966 im Pentagon anfing, kannte er weder das Projekt Barans noch das von Davies in London. Als erstes gewann er Kleinrock für sein Projekt. Dieser kam vom UCLA und sollte dort das offizielle Network Measurement Center[31] einrichten. Nachdem dann das Projekt angelaufen und die ersten Besprechungen abgehalten worden waren, nahm das Projekt langsam Form an. Als erstes einigte man sich auf die folgenden grundlegenden Eigenschaften, die das experimentelle Netzwerk auf jeden Fall besitzen sollte: Die Antwortzeiten sollten unter 1 Sekunde liegen, und das Netzwerk sollte zuverlässig und effektiv arbeiten. Vorerst offen blieben die Fragen, welche Struktur das Netzwerk haben sollte und ob die Verbindungen normale Wählleitungen für Telefone oder Vollduplexleitungen sein sollten. Unbeantwortet blieb auch die Frage, ob die Großrechner an den Universitäten selbst die Knoten des Netzwerkes bilden sollten oder ob dafür andere Rechner in Frage kämen.

Eine Computerkonferenz aus Vertretern der Universitäten und den verschiedenen Führungskräften der ARPA, in Ann Arbor Anfang 1967, brachte weitere Probleme zum Vorschein. Auf der einen Seite wollten die Wissenschaftler an den Universitäten Teile der Rechenleistung ihrer Computer nicht für ein Netzwerk hergeben, in dem sie noch keinen Sinn sahen. Auf der anderen Seite stellte sich die Frage, wie man die verschiedenen Betriebssysteme der Institutsrechner zur Kommunikation bewegen könnte und vor allem über welche Leitungen die Kommunikation ablaufen sollte.

Clark von der Washington-Universität in St. Louis hatte für diese Probleme die passende Antwort. Er schlug vor, die Großrechner auszuklammern und statt dessen ein Subnetz einzurichten, dessen Knoten aus baugleichen Computern bestehen konnte. Die Großrechner konnten ja dann mit diesen Computern verbunden werden.

---

[31] Das Network Measurement Center sollte vor allem die Netzwerkleistung testen.

Später prägte Roberts für diese Schnittstellen den Begriff „Interface Message Processors“ (IMPs)[32]. Durch die Umsetzung dieser Idee brauchte man nicht auf die wertvollen Rechnerkapazitäten der Institute zurückzugreifen und außerdem sprachen so alle Knotenrechner die „gleiche Sprache“. „Zufällig war Davies in England unabhängig davon zu genau diesem Konzept gelangt.“[33] Als Clarks Idee bekannt wurde, verschwanden die Einwände gegen das Vorhaben nach und nach. Übrig blieb das Problem der Verbindungsleitungen.

Auf einer weiteren Konferenz Ende 1967 in Gatlinburg stellte Roberts das Projekt einem größeren Fachpublikum vor. Durch einen Vortrag Scantleburys erfuhr Roberts erstmals von den Arbeiten Barans und den Forschungen des Teams von Davies am NPL. Scantlebury diskutierte mit Roberts auch das Leitungsproblem. Er schlug in diesem Zusammenhang eine ähnliche Verfahrensweise wie die von Davies geplante vor. Dieser wollte weniger Leitungen benutzen, die aber dafür mit höherer Geschwindigkeit arbeiten sollten. Roberts ging auf den Vorschlag ein.

„Bei der Konstruktion des experimentellen Netzwerks ging es Roberts nicht vorrangig – nicht einmal in zweiter Linie – um dessen Überlebensfähigkeit. [...] Barans Erkenntnisse zur Datenübertragung weckten trotzdem seine Neugier, und Anfang 1968 suchte Roberts Baran auf.“[34] Da sich Roberts nun auf die Arbeiten von Davies und Baran stützen konnte, entwickelte sich das Projekt weiter.

Das erste Konzept sah vor, IMPs an 4 Standorten - UCLA, SRI, Universität von Utah und Universität von Kalifornien in Santa Barbara - zu installieren. Erster Standort sollte die UCLA sein, da hier das Network Measurement Center von Kleinrock aufgebaut wurde, später sollten 15 Knoten hinzukommen. Roberts plante von Anfang an ein transkontinentales Netzwerk mit langen Datenleitungen. Im Gegensatz dazu baute Davies am NPL ein lokales Netzwerk mit Datenleitungen um die 100 Meter.

---

[32] Die IMPs (ausgesprochen: „Imps“) sollten die eigentliche Netzwerkverbindung herstellen, Daten senden und empfangen, Fehler suchen und beim Auftreten von Fehlern Daten nochmals senden, den Datenverkehr lenken und nachprüfen, ob die Nachrichten an den vorgegebenen Zielen angekommen waren.

[33] Hafner/Lyon, Arpa Kadabra oder die Geschichte des Internet, Seite 85

[34] ebd., Seite 90

Als Standort des Network Information Center (NIC), unter der Leitung von Engelbart, wurde das SRI gewählt. Da die Idee ausgereift und alle Probleme geklärt waren, wurde im Juli 1968 der Auftrag zum Bau der IMPs ausgeschrieben, den Zuschlag erhielt eine kleine Consultingfirma in Cambridge – Bolt Beranek and Newman (BBN).

3.3.2 Die Entwicklung der IMPs bei BBN

Unter der Projektleitung von Heart, der vom Lincoln Lab zu BBN gekommen war, sollten vier IMPs entwickelt werden. Das Auftragsvolumen durch die ARPA betrug mehr als 1 Millionen Dollar. Zur Realisierung des Projektes zog Heart verschiedene Fachleute heran. Vom Lincoln Lab kamen als Spezialisten für Echtzeitsysteme Walden und Crowther und als Hardware-Spezialist Ornstein. Als Debugging-Experte stieß Bernie Cosell aus der Computerabteilung von BBN zu der Projektgruppe. Vom MIT kamen Kahn, Professor für Elektrotechnik, und Rising als Elektroingenieur. Als Ergänzung sollte ein junger Hardwareingenieur – Barker – die ersten IMPs installieren und testen. Jedes Mitglied der Gruppe hatte seinen festen Aufgabenkreis.

„Crowther befaßte sich mit dem Dialog zwischen IMP und IMP, Walden konzentrierte sich auf die IMP-Host-Probleme, während Cosell für die Werkzeuge zur Programmentwicklung und Fehlersuche zuständig war.“[35] Kahn beschäftigte sich mit der Spezifikation der Schnittstelle Host-IMP. Als Ausgangsmodell für den ersten IMP sollte ein Honeywell-516-Computer dienen. Diesen wollte man durch eine speziell dafür hergestellte Ein– und Ausgabeeinheit ergänzen, und durch Honeywell - nach den Vorgaben von BBN – umbauen lassen. Ornstein war für die Konstruktion des Aus- und Eingabegerätes zuständig.

Während sich BBN mit der Konstruktion der IMPs beschäftigte, kümmerte sich Roberts um AT&T, welche die Leitungen für die ersten 4 Standorte legen sollten. Hierbei handelte es sich um 50-Kilobit-Leitungen, wie sie von Scantlebury vorgeschlagen worden waren. Ferner mußte sich Roberts auch um die Modems und die jeweiligen Verbindungen von den Instituten (IMPs) zu den örtlichen Telefonämtern kümmern. Zusehens konkretisierte sich der Netzwerkplan.

---

[35] ebd., Seite 125

Es wurde deutlich, daß das ARPANet eine Mischung aus den Modellen von Baran und Davies werden sollte. Allerdings konnte in der ersten Ausbaustufe nicht die von Baran vorgeschlagene Redundanz erreicht werden. Im BBN-Plan war grundsätzlich jeder Knoten mit 2 Nachbarknoten verbunden, manchmal nur mit einem, manchmal aber auch mit dreien. Die Projektgruppe um Heart setzte nicht nur die von Roberts ausgegebene Spezifikation um, sondern brachte in diesem Zusammenhang auch Neuentwicklungen hervor, die nicht in der Ausschreibung zu finden waren. Hierzu gehörte beispielsweise die Implementierung einer zentralisierten Fernüberwachung und -steuerung der IMPs.

Parallel zu den Entwicklungsarbeiten bei BBN wurde in jedem der ersten IMP-Standorte eine separate Projektgruppe eingerichtet. Diese Projektgruppen sollten sich mit der von Kahn spezifizierten Schnittstelle zwischen dem jeweiligen Host und dem IMP befassen. Aus deren Mitte wurde dann auch im Februar 1969, innerhalb eines gemeinsamen Meetings bei BBN, der Vorschlag eingebracht, mehr als nur einen Host mit einem IMP zu verbinden[36]. Als Kahn im April 1969 die Spezifikation der Host-IMP-Schnittstelle fertiggestellt hatte, konnte ein Gremium aus Wissenschaftlern der Host-Standorte mit der Entwicklung des Host-zu-Host-Protokolls beginnen[37].

Ab Herbst 1968 begann Kleinrock mit einer Gruppe von ca. 40 Mitarbeitern das Network Measurement Center am UCLA aufzubauen. Zu den Mitarbeitern dieser Gruppe zählten auch Cerf, Crocker und Postel. „Im Sommer 1968 traf sich eine kleine Gruppe graduierter Studenten von den ersten vier Host-Standorten – UCLA, SRI, UC Santa Barbara und Universität von Utha – in Santa Barbara.“[38] [39] Erste Ideen und Vorschläge hinsichtlich des Host-zu-Host-Protokolls wurden erarbeitet.

---

[36] Die Spezifikation von Roberts sah vor, daß an jedem Standort nur ein Host mit dem IMP verbunden werden sollte; da aber an den Standorten teilweise mehrere Rechner zur Verfügung standen, äußerten die Institute den Wunsch, mehrere Hosts an einen IMP anschließen zu können; die Spezifikation wurde verändert, so daß bis zu vier Hosts mit dem IMP verbunden werden konnten.

[37] Dies war nötig, da es sich bei den Hosts um grundverschiedene Rechner mit grundverschiedenen Betriebssystemen handelte; ein Protokoll ist notwendig, damit sich in einem Netzwerk unterschiedliche Computersysteme miteinander verständigen können.

[38] Hafner/Lyon, Arpa Kadabra oder die Geschichte des Internet, Seite 125

[39] Die Gruppe, die sich mit den Protokollen beschäftigte, gab sich später selbst den Namen „Network Working Group“ (NWG; dt.: Arbeitsgruppe Netzwerk).

Anwendungsbereiche für das Netzwerk sah man beispielsweise in interaktiver Grafik, verteilten Prozessen, automatischen Datenbankabfragen oder elektronischer Post. Die Gruppe erarbeitete erste Spezifikationen. Als erste Anwendungen sollten die Protokolle den Fernlogin[40] und den Dateitransfer[41] beherrschen. Für die Grundlagendokumente prägte Crocker den Namen „Request for Comments“ (RFCs)[42]. „Viele Jahre danach blieben RFCs das wichtigste Medium der Kommunikation in der Netzwerkgemeinschaft, der allgemein akzeptierte Weg, um neue technische Standards zu empfehlen, zu prüfen und zu akzeptieren (und sie sind es bis heute).“[43]

3.3.3 Die Installation der ersten IMPs und TIPs

Am 30. August 1969 wurde der erste IMP am UCLA installiert, am 1. Oktober der zweite am SRI. Nunmehr war es möglich, das erste Mal zwei räumlich getrennte Computer über ein Netz - an dieser Stelle erst aus 2 Knoten bestehend - miteinander zu verbinden. Die erste Verbindungsaufnahme des Hosts „Sigma-7“ am UCLA mit dem „SDS-940“ am SRI schlug fehl, der zweite Versuch gelang. Als nächstes wurde am 1. November ein IMP an der Universität von Kalifornien und im Dezember ein IMP an der Universität von Utha installiert.

Das erste Netzwerk (4 IMPs) erreichte nur eine geringe Redundanz. Zwischen UCSB, UCLA und SRI bestanden jeweils Verbindungen, die in ihrer Gesamtheit eine Dreiecksstruktur bildeten. Nach Utha hingegen hatte nur der IMP vom SRI eine Verbindung. Fiel dieser aus, teilte sich das Netzwerk in 2 Teile. Demnach mußten weitere Knotenrechner eingebunden werden. Das erste Host-zu-Host-Protokoll, daß die NWG entwickelte, war das kleine Protokoll Telnet. Es wurde im Dezember 1999 in einer Präsentation Roberts vorgestellt.

---

[40] Unter einem Login versteht man die Anmeldung eines Benutzers an einen Computer; ein Fern-Login ist hierbei ein Login eines räumlich weit entfernten Benutzers in einen Rechner über ein Netzwerk.

[41] Unter einem Datei-Transfer versteht man den Austausch von Dateien zwischen zwei Computern; der Übertragungsweg und die Übertragungsart spielten hierbei eine untergeordnete Rolle.

[42] Request for Comments (RFCs) steht für dt.: Ersuchen um Stellungnahme; die entsprechenden Dokumente wurden ausgearbeitet und zirkulierten dann zwischen den verschiedenen Host-Standorten, wo sie dann diskutiert wurden; RFC I beschäftigte sich z.B. mit der Verbindungsaufnahme (engl.: Handshake) zweier Hosts.

[43] Hafner/Lyon, Arpa Kadabra oder die Geschichte des Internet, Seite 167

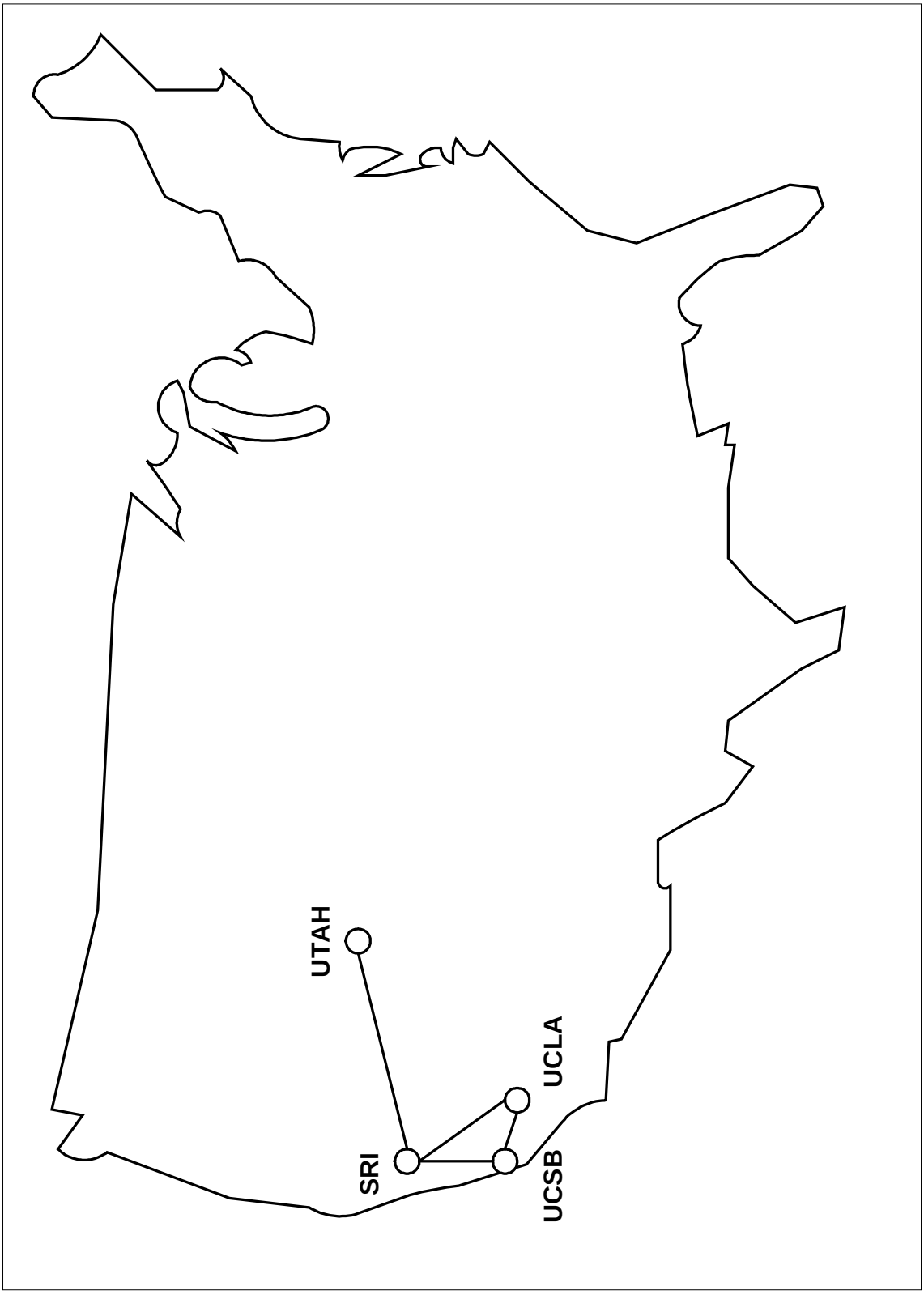

Abbildung 1: Das ARPANet im Dezember 1969[44]

[44] Quelle: http://som.csudh.edu/cis/lpress/history/arpamaps/[01.12.2002] (durch Autor nachbearbeitet)

Mit Hilfe dieses Protokolls konnte man sich von jedem beliebigen Terminal, welches mit einem Host an einem ARPA-Standort verbunden war, in einen anderen ARPA-Host[45] einloggen. Es handelte sich also hierbei um ein Protokoll für den Fernlogin. 1970 konnte die NWG ein weiteres Protokoll vorstellen, das unter dem Namen Network Control Protokol[46] (NCP) bekannt wurde.

„Das Netzwerk war nun Realität, doch mit nur vier Knoten, die sich alle an der Westküste befanden, war seine Topologie simpel, das Experiment klein. Computerhochburgen wie das MIT und das Lincoln Laboratory [...] hatten keinen Zugang. Nicht einmal [...] der Terminalraum der ARPA im Pentagon war bislang vernetzt. Auch nicht BBN selbst.“[47] Ende März 1970 wurde die erste Verbindung des experimentellen ARPA-Netzwerkes von der West- zur Ostküste installiert. Eine 50-Kilobit-Leitung verband nun das Rechenzentrum der UCLA mit dem Netzwerkknoten Nr. 5 - BBN. Durch die Einrichtung dieser Verbindung war es nun möglich, direkt von BBN aus das Netzwerk zu überwachen, zu warten und zu entstören[48]. Durch die Entwicklung spezieller Testprogramme und -prozeduren war es möglich, genaue Fehlerdiagnosen durchzuführen. Die Problemstellen konnten genau eingegrenzt werden[49]. Die IMPs wurden so programmiert, daß sie in bestimmten Abständen einen Bericht über ihren Status zu BBN sendeten. Zur Verarbeitung und Auswertung dieser Meldungen wurde bei BBN eigens dafür das Network Control Center[50] (NCC) eingerichtet. Eigentlich war die Netzwerküberwachung nicht formell geregelt worden.

Im Sommer 1970 wurden die Netzwerkknoten 6 bis 9 installiert. Weitere IMP-Standorte gab es jetzt am MIT, bei RAND, bei System Development Corp. und in Harvard. Eine zweite Transkontinentalleitung wurde zwischen Utah und dem MIT eingerichtet. Die Fernleitung zwischen UCLA und BBN wurde ersetzt und ging nun über RAND.

---

[45] Der Begriff Host ist streng vom Begriff IMP abzugrenzen, demnach ist ein Login zwischen IMPs etwas anderes als ein Login zwischen Hosts.

[46] Network Control Protocol (NCP); dt.: Netzwerk-Kontroll-Protokoll

[47] Hafner/Lyon, Arpa Kadabra oder die Geschichte des Internet, Seite 167

[48] Unbewußt hatte man die neue Technik der Fernwartung und -diagnostik erfunden; das Netzwerk war so konstruiert, daß es sich von einem weit entfernten Ort aus steuern ließ.

[49] So war es möglich, genau zu bestimmen, ob der Fehler in der Fernleitung, im Modem oder im IMP/Host selber lag.

[50] Network Control Center (NCC), dt.: Netzwerk Kontroll Zentrum

Ab November 1970 wurde das NCC bei BBN unter der Leitung von McKenzie ausgebaut. Langsam wurde das Netzwerk vom Experimentalbetrieb in den Normalzustand überführt. Das NCC zog in ein neues Gebäude um, die Mitarbeiterzahl betrug nunmehr 30 Personen. Es wurde eine logische Karte installiert, die alle IMPs, Host-Rechner und Verbindungen und den jeweiligen Status anzeigte. Zu einem wöchentlichen Termin stand BBN das komplette Netzwerk zur Verfügung. Dann konnte neue Software auf den IMPs installiert, die IMPs gewartet oder Netzwerktests durchgeführt werden. Weitere Netzwerkknoten wurden in Betrieb genommen: Universität von Illinois in Urbana-Champaign (IMP Nr. 12), Burroughs Corporation in Paoli in Pennsylvania (IMP Nr. 15).

Ende des Jahres 1970 wurde der letzte IMP der Klasse Honeywell 516 installiert. Danach sollte die leichtere und kostengünstigere Honeywell 316 in weiteren IMP-Standorten eingesetzt werden. „Der Übergang zum leichteren 316er IMP bildete aber nur einen Teil einer strukturellen Veränderung des ARPA-Netzwerkes [...].“[51] Hearts Team und Roberts machten sich Gedanken darüber, wie man vielen Benutzern den Zugang zum ARPA-Netzwerk ermöglichen könnte, ohne daß dafür ein eigener Host notwendig war. Die Lösung des Problems bestand einfach darin, eine größere Anzahl Terminals an einen IMP anzuschließen. Über diesen sollte dann der Zugriff über das Netzwerk auf regional entfernte Hosts, die ja die eigentlichen Anwenderdaten enthielten, erfolgen. Die alten 516´er und 316´er IMPs unterstützten aber nur 4 Hosts. Aus diesem Anlaß entwickelte BBN einen sogenannten Terminalcontroller, der den Anschluß von bis zu 63 Terminals ermöglichte. Die Terminals wurden über Stand- oder Wählleitungen (Telefonleitungen) mit dem Terminalcontroller verbunden. Er erhielt den Namen Terminal-IMP (TIP). An diesen TIP konnten nun die verschiedensten Endgeräte wie Grafikbildschirme, Drucker oder Fernschreibterminals angeschlossen werden. Aufgrund dieser Entwicklung wuchs das Netzwerk und damit auch das NCC.

Bis Ende 1971 wurden 3 TIPs in Betrieb genommen – zuerst bei MITRE, dann am Ames Research Center der NASA und am National Bureau of Stan-

[51] Hafner/Lyon, Arpa Kadabra oder die Geschichte des Internet, Seite 204

dards. Ein weiterer wurde direkt bei BBN installiert. Zu diesem Zeitpunkt bestand das Netzwerk aus 19 Knoten.

Ab Mitte 1971 arbeitet BBN verstärkt in der Network Working Group mit, um diese bei der Entwicklung des „file-transfer-protocol“ (FTP)[52] zu unterstützen. „Anfang Juli 1972 legten sie [die NWG] letzte Hand an FTP an, und Jon Postel, jetzt Herausgeber und Verteiler der RFC´s, veröffentlichte das Protokoll als RFC 354.“[53]

Das ARPANet war bisher nur einer relativ kleinen Zahl von Computerwissenschaftlern bekannt. Daher beschloß Roberts, das Netzwerk im Oktober 1972 auf der ersten internationalen Konferenz über Computerkommunikation (ICCC) in Washington, anhand einer Vorführung, einem breiten Fachpublikum vorzustellen. Vorbereitet wurde diese Präsentation, die im Washingtoner Hilton stattfinden sollte, durch Bob Kahn. Im Hotel wurde ein TIP installiert, AT&T legte zwei 50-Kilobit-Leitungen. Die Präsentation wurde zu einem riesigen Erfolg[54]. Bereits kurz nach der ICCC gründeten die Leiter mehrerer Vernetzungsprojekte aus verschiedenen Staaten die „International Network Working Group“ (INWG), ihr Leiter wurde Cerf. Zu der Zeit bestand das ARPANet aus 29 Knoten. Zwischen 1973 und 1975 wuchs das Netzwerk durchschnittlich um einen Knoten im Monat. Bereits vor der Präsentation liefen verschiedene Projekte an, die sich mit dem Netzwerk befaßten.

---

[52] File transfer protocol (FTP), dt.: Datei-Übertragungs-Protokoll; hierbei handelt es sich um ein Protokoll zum Verschicken und Empfangen von Dateien zwischen zwei Host-Computern über ein verbindendes Netzwerk.

[53] Hafner/Lyon, Arpa Kadabra oder die Geschichte des Internet, Seite 209

[54] Über die vielfältigsten Beispiele der angebotenen Präsentationen vgl. auch: Hafner/Lyon, Arpa Kadabra oder die Geschichte des Internet, Seite 215 ff.

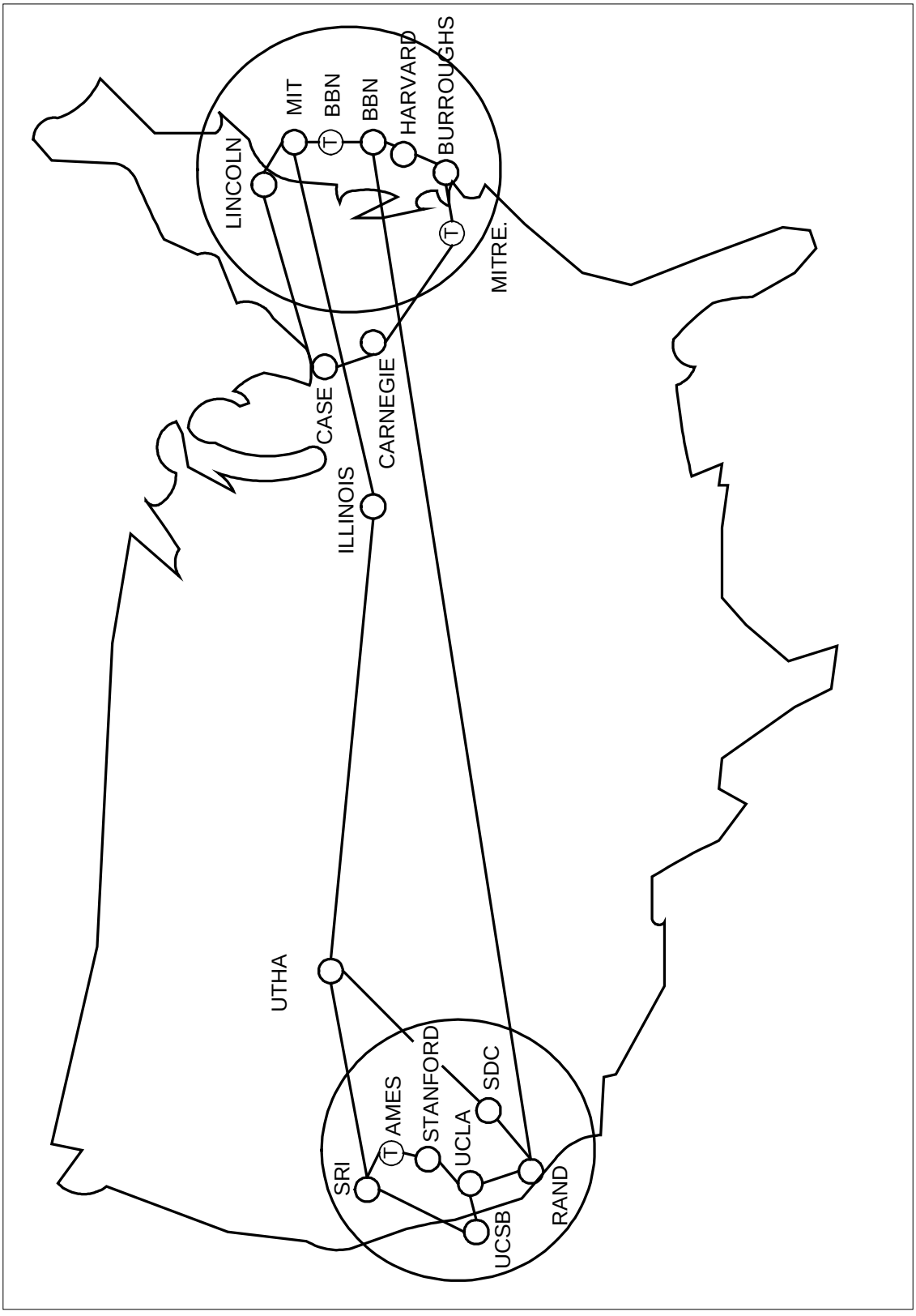

Abbildung 2: Das ARPANet im September 1971[55]

[55] Quelle: http://som.csudh.edu/cis/lpress/history/arpamaps/[01.12.2002] (durch Autor nachbearbeitet)

3.4 Skalierungsphase

3.4.1 Die Weiterentwicklung des ARPANet

Eine der nächsten wichtigen Entwicklungen für das ARPANet stellte E-Mail[56] dar. „Die erste elektronische Postzustellung zwischen zwei Rechnern fand im Jahre 1972 statt. In die Wege geleitet hatte sie Ray Tomlinson, ein ruhiger, zurückhaltender Ingenieur bei BBN.“[57] In den Anfängen wurde E-Mail über das FTP-Protokoll realisiert. Später erhielt E-Mail ein eigenes Protokoll. E-Mail wurde die beliebteste Anwendung für das ARPANet.

Aus einer Studie aus dem Jahre 1973 ging hervor, daß drei Viertel des gesamten Netzverkehrs durch E-Mails verursacht wurden. Den ersten E-Mail-Manager programmierte Roberts. Nach Veröffentlichung des Programms wurde die Idee aufgegriffen, das ursprüngliche Programm „RD“ (für engl.: read) modifiziert und neue Programme entwickelt.

Ab 1973 befaßte sich eine Gruppe unter der Leitung von Bhushan mit der Implementierung eines E-Mail-Übertragungs-Protokolls. Durch RFC 680 „Message Transmission Protocol“ wurde 1975 ein Vorschlag für einheitliche Headerfelder veröffentlicht[58]. 1977 erschien RFC 724 als Vorschlag eines offiziellen Standards für das Format von ARPA-Netzwerk-Nachrichten. RFC 733 brachte eine Endfassung, nach der dann viele E-Mail-Programme modifiziert wurden. Dennoch konnte sich der Standard nicht durchsetzen. Das Programm MSG von Vittal hielt sich nicht an RFC 733, dennoch war es so komfortabel, daß es sich in der Netzwerkgemeinschaft stark verbreitete und so ein Quasi-Standard wurde.

Eine weitere Neuerung stellte die Entwicklung der MsgGroup (engl.: Message Service Group) dar, die durch Walker im Juni 1975 initiiert wurde[59]. Die MsgGroup stellte in diesem Sinne die erste Mailingliste dar[60]. In ihr wurde vor

---

[56] E-Mail = Electronic Mail, dt.: Elektronische Post

[57] Hafner/Lyon, Arpa Kadabra oder die Geschichte des Internet, Seite 226

[58] Headerfelder bei E-Mails enthalten bestimmte Informationen, wie z.B.: Absender, Absendedatum, Betreff etc.

[59] MsgGroup = Message Service Group, dt.: eine Art elektronische Diskussionsgruppe

[60] Wer Mitglied einer Mailingliste ist, kann Nachrichten für ein bestimmtes Thema an die Liste senden; diese Nachricht wird dann an alle Mitglieder übermittelt.

allem die Diskussion über die Standardisierung von E-Mails geführt. Die Verwaltung der MsgGroup hatten Farber und Stefferud übernommen.

Ab 1972 übernahm McQuillan bei BBN die Pflege, Verbreitung und Verbesserung der IMP-Software. Da das Netzwerk kontinuierlich wuchs und langsam eine Knotenzahl von 50 bis 60 Rechnern erreichte, machten sich erste Fehler in der Routingsoftware, die Crowther und Walden geschrieben hatten, bemerkbar. Vereinzelt kam es durch diese Fehler zum vollständigen Absturz des ARPANet[61].

„Innerhalb von zwei Jahren und mit zahlreichen neuen Versionen ersetzte McQuillan nach und nach die Routing-Algorithmen, das Bestätigungsverfahren und schließlich das gesamte Betriebsprogramm der IMPs. Er entwickelte einen völlig anderen Algorithmus, der Informationen über Veränderungen im Netzwerk blitzschnell an alle IMPs verteilte, damit sie keine falsche Routing-Entscheidungen trafen.“[62] 1974 waren fast 50 IMPs im ARPANet miteinander verknüpft.

Das Netzwerk wuchs und wurde zur Grundlage mannigfaltigster Kommunikation. Es avancierte im Wandel der Zeit nicht nur zur Plattform für technische Diskussionen und Innovationen, sondern ermöglichte auch neuartige Nutzungsformen. Das erste Spiel, das im Netzwerk gespielt wurde, war die Computerfassung des raffinierten Fantasyspiels „Dungeons und Dragons“. Das Spiel war von Crowther geschrieben und dann von Woods erweitert worden. Während der Watergate-Krise forderte ein Student im Netz ein offizielles Amtsenthebungsverfahren Nixons. 1977 wurde in der MsgGroup das private Roboterprojekt „Quasar“ heiß diskutiert, bei dem man von einer Fälschung ausging. „Dieses Ereignis markierte den Beginn der ersten Debatte über die freie Meinungsäußerung im Cyberspace.“[63] Später stellte sich heraus, daß es sich bei dem Roboter wirklich um eine Fälschung gehandelt hatte. Das Problem bestand vor allem in der Tatsache, daß das ARPANet Eigentum der US-Regierung war und die Netzwerkgemeinschaft das staatlich initiierte und vor

---

[61] Ein Beispiel hierfür war der Fehler in der Routingsoftware des IMP von Harvard, im Dezember des Jahres 1973; dieser Fehler, bei dem in den Routingtabellen überall Nullen eingetragen wurden, hatte zur Folge, daß das gesammte Netzwerk versuchte, die Daten über Harvard zu routen; der IMP brach natürlich unter der Datenlast zusammen und mit ihm das gesamte Netzwerk.

[62] Hafner/Lyon, Arpa Kadabra oder die Geschichte des Internet, Seite 233

[63] ebd., Seite 246

allem finanzierte Netz nutzte, um ein privates Unternehmen zu verunglimpfen. Nicht alle stimmten dieser Ansicht zu, woraus sich eine Grundsatzdiskussion entwickelte, die noch Jahre später immer wieder aufflammte. Eine ähnliche Debatte löste im Jahre 1979 die Einführung des Finger-Befehls an der Carnegie-Mellon-Universität aus[64]. Mit Hilfe dieses Befehls ließen sich die Online-Geflogenheiten von Benutzern ermitteln. Nach Bekanntwerden gab es erste Proteste. Als Reaktion auf den Widerstand wurde der Befehl so abgeändert, daß jeder Benutzer selbst entscheiden konnte, welche Informationen er von sich preisgeben wollte. Kritisiert wurden danach vor allem die Bestrebungen, an der Offenheit des Netzwerkes zu manipulieren.

3.4.2 ALOHANet, PRNet, SATNet und TCP/IP

Nachdem weitestgehend alle praktischen Probleme beim Betrieb des ARPANet[65] gelöst worden waren, wandte man sich neuen Techniken zu. Bisher wurde das Netz ausschließlich mittels Standleitungen von AT&T betrieben. Erklärtes Ziel war nun die drahtlose Datenübertragung durch Funk. Erste Forschungen und Entwürfe lieferten Abramson und mehrerer seiner Kollegen. Noch unter der Federführung von Taylor wurden die Mittel für ein Funknetzwerk an der Universität von Hawaii genehmigt. Das Projekt erhielt den Namen ALOHA. Hierbei wurden „per Funk Daten zwischen sieben, über vier Inseln verteilten Computern“[66] übertragen.

Ein weiteres Nutzungskonzept, das auf dem ALOHANet aufbaute, skizzierten Roberts und Kahn 1972. Dabei handelte es sich um ein Paketvermittlungsnetzwerk mit kleinen tragbaren Computern. Durch Roberts wurde das SRI mit der Ausarbeitung des Konzepts beauftragt. Das digitale Funknetzwerk (Packet Radio Network) - als drahtlose Variante des ARPANet - kam aus dem Versuchsstadium nie heraus und wurde aufgrund technischer Schwierigkeiten später eingestellt.

---

[64] Der Befehl wurde in den 70er Jahren durch Les Earnest in der KI-Abteilung von Stanford erfunden und 1979 erstmals an der CMU angewendet.

[65] Die ARPA (Advanced Research Projects Agency) wurde in DARPA (Defense Advanced Research Projects Agency) umbenannte, die Bezeichnung ARPANet wurde beibehalten.

[66] Hafner/Lyon, Arpa Kadabra oder die Geschichte des Internet, Seite 261

Die nächste Entwicklungsstufe stellte das SATNet dar. Hierbei handelte es sich um ein satellitengestütztes Netzwerk. Die Host-zu-Host-Kommunikation erfolgte nicht über eine Standleitung, sondern über einen Satelliten. Der Nachteil dieses Systems bestand zu der Zeit aber noch in der Langsamkeit der Datenübertragung. Da die damaligen Transatlantikleitungen sehr störanfällig waren, wurden die ersten Verbindungen nach England, Norwegen, Italien und Deutschland eben über das SATNet eingerichtet. Nach und nach wurden die Seeleitungen aber durch moderne Glasfaserleitungen ersetzt, das SATNet wurde entbehrlich.

Schon im Jahre 1972 hatte sich Kahn weitreichendere Gedanken über Vernetzung gemacht. „Mehrere Staaten außerhalb der Vereinigten Staaten bauten Datensysteme auf, und eine wachsende Zahl großer Unternehmen begann, eigene Vernetzungskonzepte zu entwickeln.“[67] Kahns Idee bezog sich vor allem auf die Verknüpfung, dieser in der Entstehung begriffenen kleineren Netzwerke.

In England wurde die Entwicklung durch Davies am NPL vorangetrieben. In Frankreich wurde durch Pouzine die französische Version des ARPANet - unter dem Namen „Cyclades“ - entwickelt. Mit der Verbindung dieser teilweise sehr unterschiedlichen Netzwerke mit unterschiedlichsten Topologien und Geschwindigkeiten beschäftigte sich die INWG. Ihr Konzept hieß „Concatenated Network“ (dt.: Verbundnetzwerk) oder kurz CATENet.

Bereits 1973 hatten Cerf und Kahn die Idee, das PRNet, das ARPANet und das SATNet miteinander zu verbinden. Die Kopplung der einzelnen Netzwerke sollte über „Gateways“ (dt.: Übergänge, Netzkoppler) erfolgen. Diese wollte man durch spezielle Router realisieren, die Nachrichten zwischen den einzelnen Netzwerken vermitteln konnten. Das Problem, das sich auftat, bestand ein weiteres Mal in der Entwicklung von Protokollen. Nur spezifische Protokolle konnten alle Hosts der verschiedenen Netzwerke dazu bringen, miteinander zu kommunizieren.

Kahn und Cerf erarbeiteten innerhalb der INWG, unter engem Kontakt zu Davies und Pouzine, ein Konzept, welches 1974 der Öffentlichkeit vorgestellt

---

[67] ebd., Seite 263

wurde. Die Spezifikation wurde „Transmission Control Protocol“ (TCP)[68] genannt und stellte ein Host-zu-Host-Protokoll dar, durch welches ein Hauptteil der Verantwortlichkeit auf die Hosts übertragen wurde. Durch die Entwicklung des TCP wurde es nunmehr möglich, die verschiedenartigsten Netzwerke miteinander zu verbinden. Benötigt wurde nur ein Gateway und die Installation von TCP auf allen Hosts des einzubindenden Netzwerks.

[68] Transmission Control Protocol (TCP), dt.: Datenübertragungs – und Steuerungsprotokoll

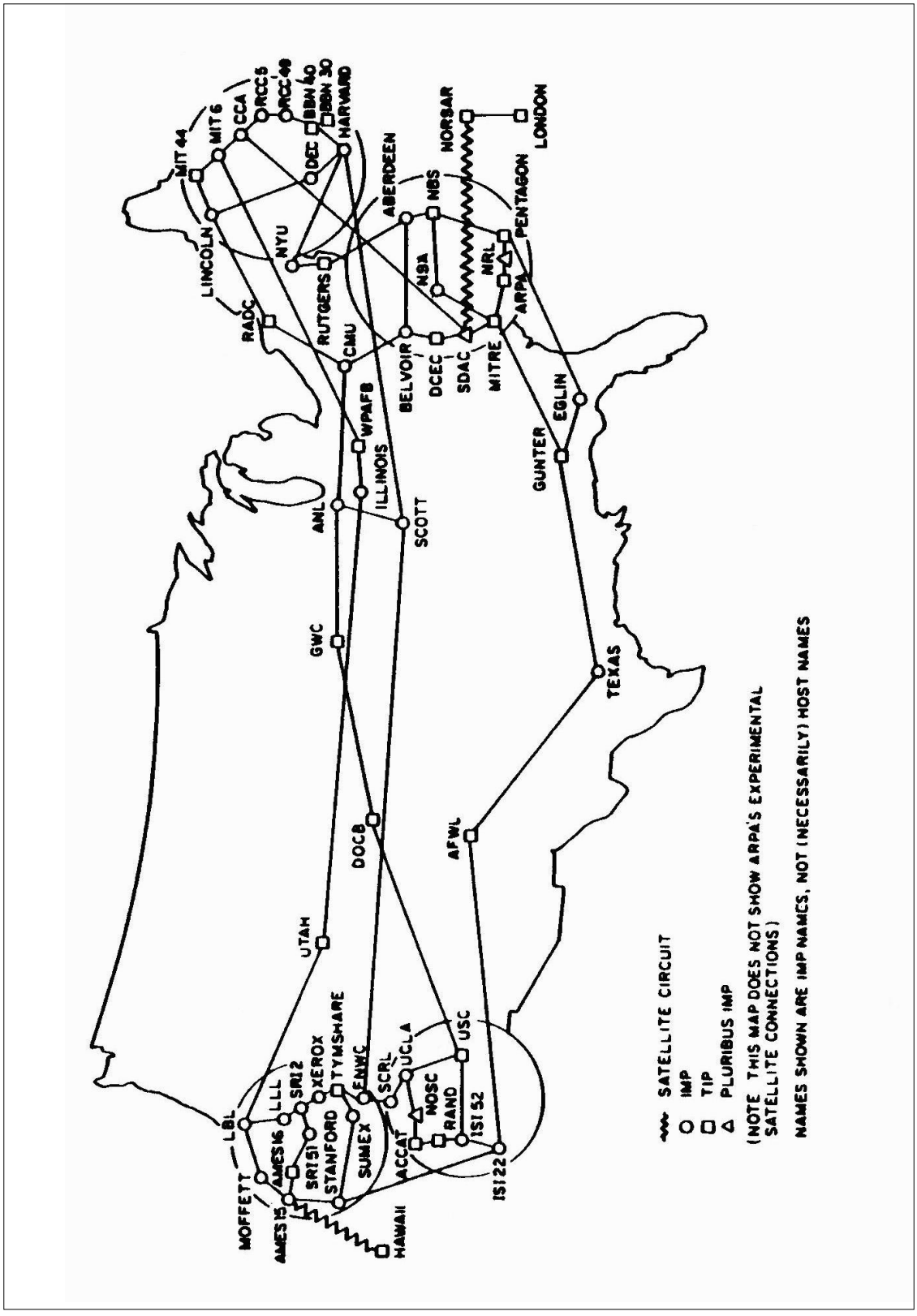

Abbildung 3: Das ARPANet im Juli 1977[69]

[69] Quelle: http://som.csudh.edu/cis/lpress/history/arpamaps/[01.12.2002]

Bereits ab 1971 hatte es erste Diskussionen über die Abgabe des ARPA-Net an private Betreiber gegeben. AT&T lehnte eine Übernahme ab, da man hier immer noch der Meinung war, daß das ARPANet mit dem AT&T-Netz inkompatibel sei. Eine weitere Möglichkeit der Übernahme bestand durch BBN. 1973 gewann BBN Roberts für die Leitung ihres Tochterunternehmens TELENET, das einen privaten Paketvermittlungsdienst anbieten sollte. Demnach konnte Roberts das ARPANet nicht an BBN verkaufen, sondern veranlaßte im Sommer 1975 die Übernahme des Netzwerkes durch die DCA. Nachdem Roberts die DARPA verlassen hatte, wurde Licklider neuer Leiter der IPTO. Als er den Übergang des ARPANet zur DCA abgewickelt hatte, verließ er die DARPA ebenfalls.

Da die DARPA nun von der täglichen Last der Netzwerkverwaltung befreit war, konnte sie sich intensiv mit der Entwicklung der CATENet-Protokolle beschäftigen. Ab 1975 kam Cerf als Programmanager zur DARPA und entwickelte das TCP weiter. Im Oktober 1977 konnten Cerf und Kahn das erste funktionierende Drei-Netzwerke-System aus ARPANet, SATNet und Packet Radio Network - auf der Grundlage von TCP - vorstellen. Dieses Netzwerk erhielt den Namen ARPA-Internet.

1978 wurde der Teil des TCP abgetrennt, der für das Routing zuständig war. Er wurde durch ein eigenes Protokoll realisiert – das Internet Protocol (IP). Danach war das TCP nur noch für das Zerlegen und Zusammensetzen der Nachrichten, die Fehlersuche und das erneute Senden verlorengegangener Pakete zuständig. Das IP war ausschließlich für das Routing der einzelnen Pakete verantwortlich.

3.4.3 CSNet, NSFNet und INTERNET

Nicht nur die ARPA (später umbenannt in DARPA) förderte Forschungsprojekte auf den verschiedensten Sektoren. Auch die „National Science Foundation“ (NSF)[70] unterstützte und finanzierte Grundlagenforschung. Bereits 1974 hatte die NSF Ideen für ein neues Netzwerk, das ausschließlich für Computerwissenschaftler gedacht war.

[70] National Science Foundation (NSF), dt.: Nationale Stiftung für die Wissenschaft

Da sich die Computerwissenschaften etablierten, entstanden viele neue Informatikfakultäten in den Bildungsinstituten der USA. Aber nur die wenigsten Einrichtungen hatten Zugang zum ARPANet. 1979 konnten von 120 Informatikfakultäten 15 auf das ARPANet zugreifen. Die Möglichkeit einen Knotenrechner zu bekommen, bestand für die meisten Fakultäten nicht, da nur Institute angeschlossen wurden, an denen im gewissen Grad staatlich finanzierte Forschung betrieben wurde.

Anfang 1975 wurde durch die NSF beschlossen, das „Computer Science Research Network“ (CSNet)[71] aufzubauen. Der Entwurf sah ein offenes Netzwerk vor, an das sich beliebige Einrichtungen – die allerdings auf dem Gebiet der Informatik tätig sein mußten - anschließen konnten. Das Netzwerk sollte sich auf Leitungen eines kommerziellen Providers - wie beispielsweise TELENET - stützen. Finanzieren mußte sich das Projekt durch Beiträge und Verbindungsgebühren der angeschlossenen Institutionen. Ab 1980 wurde mit dem Aufbau des Netzwerkes begonnen. Unterstützt werden sollte es 5 Jahre lang durch die NSF. Die Verantwortung für den Betrieb wurde später von der NSF an die „University Corporation for Atmospheric Research“ (UCAR) übertragen. Bereits im Juni 1983 waren mehr als 70 Standorte an das Netzwerk angeschlossen.

„Mitte der 80er Jahre entstanden auf den Erfolg des CSNet hin weitere Netzwerke. Eines davon, das BITNet (Because It´s Time Network), war ein kooperatives Netz von IBM-Systemen, doch ohne Mitgliedschaftsbeschränkung. Ein anderes mit der Bezeichnung UUCP hatten die Bell Laboratories für den Dateitransfer und die Ausführung von Befehlen auf entfernten Rechnern aufgebaut. USENet, das 1980 als Kommunikationsmittel zwischen zwei Maschinen […] begann, entwickelte sich zu einem verteilten Nachrichtennetz, das UUCP nutzte. Die NASA hatte ihr eigenes Netzwerk mit der Bezeichnung Space Physics Analysis Network oder SPAN.

Da dieses wachsende Konglomerat von Netzwerken mit Hilfe der TCP/IP-Protokolle [und Gateways] miteinander kommunizieren konnte, wuchsen […] [die Netzwerke] allmählich zu dem zusammen, was dann – nach dem ersten

[71] Computer Science Research Network (CSNet), dt.: Forschungsnetzwerk für Computerwissenschaften

Wort von ´Internet Protocol´ - ´Internet´ heißen sollte“[72]. In Europa entstanden mehrere TCP/IP-Netzwerke, in Kanada das CDNet.

Um auch anderen Fakultäten - außer denen der Informatik - Vernetzungsmöglichkeiten zu bieten, wurden ab 1985 fünf Computerzentren als sogenanntes NSFNet miteinander verbunden. Finanziert wurde das Projekt durch die NSF. Dieses Netzwerk sollte nur als Backbone (dt.: Rückgrat) für andere regionale Netzwerke dienen. Die Benutzung sollte kostenfrei sein. Auf dieser Grundlage wurden regionale Netzwerke installiert und dann über Gateways mit dem NSF-Backbone verbunden[73]. Über das NSFNet bestand dann die Möglichkeit, Verbindungen zu anderen angeschlossenen Netzwerken herzustellen.

3.4.4 Außerbetriebnahme des ARPANet

Am 01.01.1983 wurde das ARPANet von NCP auf TCP/IP umgestellt. 1983 wurde es in zwei Teile geteilt, der eine Teil – das ARPANet – blieb der Computergemeinschaft erhalten, der andere Teil – das MILNet – wurde weiter durch das Militär genutzt.

Zu der Zeit sah die Struktur des Internet sternförmig aus, mit dem ARPANet als Zentrum und den anderen Netzwerken in kreisförmiger Anordnung darum. Zudem bestanden weitere Verbindungen nach Übersee. Die Verbindung zwischen den verschiedenen Netzwerken, auf der Grundlage von TCP/IP, nahm zu. Die Entwicklung der Ethernet-Technik[74] verstärkte den Prozeß nochmals. Eine Vereinfachung in der Adressierung brachte die Einführung des „Domain Name System“ (DNS)[75], unter der Federführung von Postel, Mockapetris und Partridge. Ab 1985 drängte die DARPA auf die Benutzung des DNS-Systems.

Im Jahre 1986 wurde das DNS-Konzept von den Vertretern der größten Netzwerke anerkannt. Die Strukturen veränderten sich. Das NSFNet entwickel-

---

[72] Hafner/Lyon, Arpa Kadabra oder die Geschichte des Internet, Seite 289

[73] Beispiele für regionale Netzwerke sind das NYSERNet (New York State Educational Research Network) im Staat New York und das CERFNet (California Educational Research Network) in San Diego.

[74] Bei der Ethernet-Technik handelt es sich um ein Vernetzungskonzept für enge räumliche Netzwerke (LANs – Local Area Networks), z.B. in Universitätsgebäuden etc.; die Technik wurde 1973 durch eine Entwicklergruppe unter Leitung Metcalfs am XEROX-PARC entwickelt.

[75] Domain Name System (DNS), dt.: Domain-Namen-System; durch DNS wird jedem Host eine eindeutige - hierarchisch gegliederte - Adresse zugewiesen.

te sich zum Backbone für das Internet, da seine Leitungen 25mal schneller waren als die des ARPANet. Die an das NSFNet angeschlossenen Hosts übertrafen bald die Anzahl der an das ARPANet angeschlossenen Rechner.

Ab 1985 beschloß die Führungsetage der DARPA, das Netzwerk außer Betrieb zu nehmen, da die Knotenrechner veraltet und die Verbindungen zu langsam waren. Bis 1989 wurden sukzessive alle IMPs und TIPs vom Netz genommen, den Hauptverkehr bewältigte bereits der NSF-Backbone.

Auch der Betrieb des SATNet wurde eingestellt. Die Knotenrechner des ARPANet wurden abgebaut, gingen in den Bereich des MILNet oder des NSFNet über oder wurden zu regionalen Gruppen zusammengefaßt. Einige Rechner wurden durch die neuen Betreiber saniert und in regionale Netze umgewandelt. Ende 1989 gab es kein ARPANet mehr.

3.4.5 Kurzer Abriß der weiteren Entwicklung

Im zivilen Teil des Netzes nahm die Anzahl der angeschlossenen Rechner im Laufe der 80er Jahre sprunghaft zu. Einzelne Universitätsrechner oder kleinere Rechnernetze konnten mit einem Rechenzentrum verbunden werden, welches dann den Zugriff auf andere Netze ermöglichte. So wurden immer mehr kleinere Netze mit dem Internet verbunden.

In Europa gab es zeitgleich ähnliche Entwicklungen. Hier „begann der Aufbau von nationalen Netzwerken Anfang der 80er Jahre“.[76] Zuerst setzte man jedoch auf andere Protokolle als TCP/IP, nämlich auf den ISO-Standard. Diese Norm unterschied sich in wesentlichen Teilen von dem amerikanischen TCP/IP-Modell, das nicht ISO-normiert war.

Europas nationale Forschungsnetze (z.B.: EUNet, EARN oder der europäische Teil des CSNet) mußten über einen Gateway mit dem amerikanischen Backbone verbunden werden. Ein europäischer Backbone existierte noch nicht. 1986 wurde die Organisation „Réseaux Associés pour la Recherche Européenne“ (RARE) gegründet.

Die Aufgabe dieser Organisation bestand darin, alle Initiativen zur systemübergreifenden Rechnervernetzung europaweit zu koordinieren. Zu die-

[76] Alpar, Kommerzielle Nutzung des Internet, Seite 18

sem Zweck rief die RARE ein Projekt namens „Cooperation for an Open Systems Interconnection Networking in Europe“ (COSINE) ins Leben.

Trotz ernsthafter Bemühungen konnte sich der ISO-Standard nicht durchsetzen. Unter dem amerikanischen Erfolgsdruck entstand schließlich ein europäisches Datennetz, das multiprotokollfähig war und TCP/IP unterstützte. Dieses Netz lief zunächst unter der Bezeichnung „EuropaNET“. Verschiedene nationale wissenschaftliche Netzwerke, etwa das „Deutsche Forschungsnetz“ (DFN), wurden daran angeschlossen. Durch eine Transatlantikleitung wurde die Anbindung Europas an den amerikanischen Backbone sichergestellt. Die Koordination des Internet-Verkehrs innerhalb Europas obliegt der Organisation „Réseaux IP Européens“ (RIPE). In Europa gibt es seit 1992 ein Leitungs-Verbundsystem: dieses System nennt sich „Europäischer Internet-Backbone“ (Ebone). Auf anderen Kontinenten gab und gibt es vergleichbare Entwicklungen.

Wie bereits beschrieben, hatten zwei Wissenschaftler zeitgleich die Paketvermittlungstechnik erfunden, Baran in den USA und Davies am NPL in London. Während in den USA das ARPANet aufgebaut wurde, kam es zu Parallelentwicklungen in Europa, und hier vor allem in England und Frankreich. Durch den Informatiker Pouzine wurde das französische Gegenstück des ARPANet – „Cyclades“ – entwickelt. Davies arbeitete weiter am NPL und baute dort ein eigenständiges Paketvermittlungsnetzwerk auf.

„In Deutschland begann die Entwicklung 1984 mit der Gründung eines nationalen Forschungsnetzes durch den `Verein zur Förderung eines Deutschen Forschungsnetzes´ (DFN). In Kooperation mit der damaligen Deutschen Bundespost wurde das `Wissenschaftsnetz´ (WIN) aufgebaut. Bis 1992 war der Zugang zu diesem Netzwerk nur Universitäten und Forschungseinrichtungen erlaubt.“[77] Was man also heute unter "Internet" versteht, ist nicht ein einziges homogenes Netz, sondern ein Verbund aus vielen kleinen, territorial oder organisatorisch begrenzten Netzen. Diese Netzwerke besitzen eine Anbindung an die Backbones und damit an das Gesamtnetz. Heute wird das Internet zu einem großen Teil durch kommerzielle Unternehmen betrieben.

---

[77] ebd., Seite 18

4 Technische Grundlagen

4.1 Allgemeines

Wie bereits aus den Ausführungen zur Geschichte des Internets ersichtlich wurde, unterliegt das Internet bestimmten Grundprinzipien. Ein fester Kern bestimmter Eigenschaften bildet hierbei einen existentiellen Mindeststandard. Das wird deutlich, wenn man die inhomogene Landschaft der verschiedenen Netzwerke betrachtet, die miteinander verbunden sind. Jedes Netzwerk unterliegt seinen eigenen Regeln und hat eigene Besonderheiten. Dennoch müssen diese vielen verschiedenen Netzwerke über eine Gemeinsamkeit verfügen, die es ihnen ermöglicht, miteinander zu kommunizieren[78].

4.2 Transmission Control Protocol (TCP)

Das „Internet Protocol“ (IP) bildet zusammen mit dem „Transmission Control Protocol[79]“ den angesprochenen Mindeststandard. Diese beiden Protokolle bieten zusammen die Möglichkeit, verschiedenste Netzwerke miteinander zu verbinden. Wenn durch die verschiedenen Dienste das Internet[80] benutzt wird, bildet TCP/IP sozusagen immer das Basisprotokoll, auf das die speziellen Protokolle der jeweiligen Dienste aufsetzen.

Wenn Daten über das Netz transportiert werden sollen, zerlegt TCP im Vorfeld den Datenstrom in kleine Pakete. Die Paketgröße ist genormt. Jedes Paket enthält eine Angabe dazu, an welche Adresse es geschickt werden soll und das wievielte Paket innerhalb der Sendung es ist. TCP arbeitet also auf der Absender- und auf der Empfängerseite und sorgt für das Zerlegen und das Wiederzusammensetzen der einzelnen Pakete. Es gehört zu den Grundprinzipien des Internets, daß der Weg eines Pakets nicht festgelegt wird. Daher ist es die Regel, daß die Pakete in einer anderen Reihenfolge beim Empfänger ankommen, als sie beim Sender abgeschickt wurden.

---

[78] Einen kurzen Überblick über die Internet-Technik bei: Hartung, Internet, dp-special April 1998, Seite 2 – 15; Berger-Zehnpfund, Kinderpornographie im Internet, Kriminalistik 10/1996, Seite 635 bis 639; ausführlicher Heinzmann/Ochsenbein, Strafrechtliche Aspekte des Internet, Kriminalistik 7/1998, Seite 513 bis 520, Kriminalistik 8-9/1998, Seite 599 bis 606

[79] Transmission Control Protocol (TCP), dt.: Protokoll für die Übertragungskontrolle

[80] Die Dienste FTP, Gopher, Archie, E-Mail, Chat, News, WWW und Usenet werden nachfolgend behandelt.

Erst wenn alle Pakete einer Sendung vollständig beim Empfänger angekommen sind, gilt die Übertragung der Daten als abgeschlossen. Da die Pakete numeriert sind, können sie durch das TCP wieder in der richtigen Reihenfolge zusammengesetzt werden.

4.3 Internet Protocol (IP)

Damit die Pakete auch ihren Empfänger erreichen, werden sie mit einer eindeutigen Adresse versehen - der IP-Adresse[81]. Jeder Rechner, der am Internetverkehr teilnimmt, ist mit einer IP-Adresse im Netz angemeldet. Einen in der Art im Internet angemeldeten Rechner nennt man Hostrechner oder Host. In diesem Sinne bekommt auch der Benutzer, der sich beispielsweise über das Telefonnetz der Telekom in das Internet einwählt eine IP-Adresse. Sein Rechner ist dann online und wird zum Host.

Wie erfolgt nun die Adressierung im Internet? Eine IP-Adresse ist eine maximal 12stellige Dezimalzahl, bei der jeweils 3 Ziffern durch einen Punkt getrennt werden[82]. Eine Möglichkeit für eine IP-Adresse wäre z.B. 126.174.201.98. Die Punkte haben die Aufgabe, über- und untergeordnete Netze zu trennen. Eine Zahl in der Quadrupel kann höchstens den Wert 255 annehmen. So wie zu einer Telefonnummer im weltweiten Telefonnetz eine Landeskennzahl, eine Ortsnetzkennzahl, eine Teilnehmerrufnummer und manchmal auch noch eine Durchwahlnummer gehört, gibt es auch im Internet eine Vorwahl - die Netzwerknummer - und eine Durchwahl - die Hostnummer.

Der erste Teil einer IP-Adresse ist stets die Netzwerknummer, der zweite Teil die Hostnummer. Wo die Grenze zwischen Netzwerknummer und Hostnummer verläuft, bestimmt ein Klassifizierungsschema für Netztypen. Die folgende Tabelle verdeutlicht diese Klassifizierung. In der Spalten für die IP-Adressierung steht für jede Klasse das allgemeine Schema. Ein typisches Beispiel verdeutlicht die Zusammenhänge. Die Netzwerknummer (der Vorwahlteil) ist fett dargestellt, der Rest der IP-Adresse ist die Hostnummer eines Rechners innerhalb dieses Netzes.

---

[81] Internet Protocol (IP), dt.: Internet Protokoll

[82] Der Fachbegriff für dieses Zahlengebilde ist Quadrupel.

Klassifizierung	Adressierung	Beispiel
Klasse-A-Netz	**xxx**.xxx.xxx.xxx	**103**.234.123.87
Klasse-B-Netz	**xxx.xxx**.xxx.xxx	**151.170**.102.15
Klasse-C-Netz	**xxx.xxx.xxx**.xxx	**196.23.155**.113

Tabelle 1: Klassifizierungsschema für Netztypen

Die oberste Hierarchiestufe bilden die sogenannten Klasse-A-Netze. Hier ist nur die erste Zahl einer IP-Adresse die Netzwerknummer, alle anderen Zahlen sind Hostnummern innerhalb dieses Netzwerks. Theoretisch ist bei einer dreistelligen Zahl die Möglichkeit der Existenz von 255 Klasse-A-Netzen denkbar, bei Netzwerknummern solcher Netze sind allerdings nur Zahlen zwischen 1 und 126 möglich, d.h. es kann weltweit nur 126 Klasse-A-Netze geben. Eine IP-Adresse, die zu einem Klasse-A-Netz gehört, ist also daran erkennbar, daß die erste Zahl zwischen 1 und 126 liegt. Das amerikanische Militärnetz oder T-Online ist beispielsweise so ein Klasse-A-Netz. Innerhalb eines Klasse-A-Netzes kann der Netzbetreiber die zweite, dritte und vierte Zahl als IP-Adressen an andere Hostrechner vergeben. Da alle drei Zahlen Werte von 0 bis 255 haben können, kann ein Klasse-A-Netzbetreiber also bis zu 16,7 Millionen IP-Adressen an Host-Rechner innerhalb seines Netzes vergeben.

Die nächste Hierarchiestufe bilden die Klasse-B-Netze. Die Netzwerknummer solcher Netze erstreckt sich über die beiden ersten Zahlen der IP-Adresse. Bei der ersten Zahl können Klasse-B-Netze Werte zwischen 128 und 192 haben. Eine IP-Adresse die zu einem Klasse-B-Netz gehört ist also daran erkennbar, daß die erste Zahl zwischen 128 und 192 liegt. Bei der zweiten Zahl sind Werte zwischen 0 und 255 erlaubt. Dadurch sind etwa 16.000 solcher Netze möglich. Da die Zahlen drei und vier ebenfalls Werte zwischen 0 und 255 annehmen können, sind in jedem Klasse-B-Netz bis zu ca. 65.000 Hostrechner adressierbar. Klasse-B-Netze werden vor allem an große Firmen, Universitäten und Online-Dienste vergeben.

Die unterste Hierarchiestufe stellen die Klasse-C-Netze dar. Die erste Zahl der IP-Adresse eines Klasse-C-Netzes liegt zwischen 192 und 223. Die Zahlen zwei und drei gehören ebenfalls noch zur Netzwerknummer. Über zwei Millionen solcher Netze sind dadurch möglich. Vor allem an kleine und mittlere

Unternehmen mit direkter Internet-Verbindung, auch an kleinere Internet-Provider, werden solche Adressen vergeben. Da nur noch eine Zahl mit Werten zwischen 0 und 255 übrig bleibt, können in einem Klasse-C-Netz maximal 255 Host-Rechner angesprochen werden.

Ob dieses Adressierungsschema den Anforderungen der Zukunft weiterhin gerecht werden wird, darf bezweifelt werden. Es gibt bereits Ideen für eine Neustrukturierung der Adressierung von Netzen und Hostrechnern. Diese Neustrukturierung soll dahingehend erfolgen, daß die IP-Adresse einfach verlängert wird[83].

4.4 Domain Name System (DNS)

Wie bereits erläutert, erfolgt die Adressierung der Datenpakete im Internet mit Hilfe der IP-Adressen, bei denen es sich um einen Zahlencode handelt. Da sich der Mensch, als ausschließlicher Nutzer des Internets, diesen Zahlencode nur schwer merken kann, wurde ein weiteres Adressierungssystem – das DNS[84] - entwickelt, welches auf Zeichenfolgen aufbaut. D.h. anstatt der Eingabe von einer Zahlenfolge ist es grundsätzlich auch möglich, eine Kombination aus verschiedenen Wörtern (Domain-Namen) zu verwenden.

„Die Zuordnung der eindeutigen Namen erfolgt [...] nicht aufgrund der Größe der Netzwerktopologie, sondern ist ein System von logisch und inhaltlich zusammengehörigen Rechnergruppen. Aber auch dieses Namenssystem ist hierarchisch geordnet. Die logisch zusammengehörenden Bereiche werden Domain genannt [...]. [...] Der hinterste Teil eines solchen Aliasnamens stellt die gröbste logische beziehungsweise inhaltliche Einteilung dar (der sogenannte Top Level Domain) [...], der vorderste Teil bezeichnet direkt den einzelnen Rechner.“[85]

Besteht die Domain-Adresse aus mindestens drei Teilen, wird die erste Domain nach dem Top-Level-Domain als Second-Level-Domain und jede weitere Domain als Local-Level-Domain bezeichnet. Die Anzahl der Local-Level-Domains ist dabei beliebig. Die einzelnen Domain-Angaben solcher Namens-

---

[83] Näheres hierzu unter „Die Zukunft des Internets“

[84] Domain Name System (DNS), dt.: Domain Namen System

[85] Steyer, HTML 4, Seite 63

adressen sind, wie bei IP-Adressen, durch Punkte voneinander getrennt. Eine solche Namensadresse könnte beispielsweise tiscalinet.de sein[86].

Top-Level-Domains stehen in einer Domain-Adresse an letzter Stelle. Es handelt sich um einigermaßen sprechende Abkürzungen. Daher wird die Domain-Adresse im Gegensatz zu den IP-Adressen von rechts nach links gelesen[87]. Der vorderste Teil spricht immer direkt den Host an. Den systematischen Aufbau einer Domain-Adresse zeigt die folgende Abbildung:

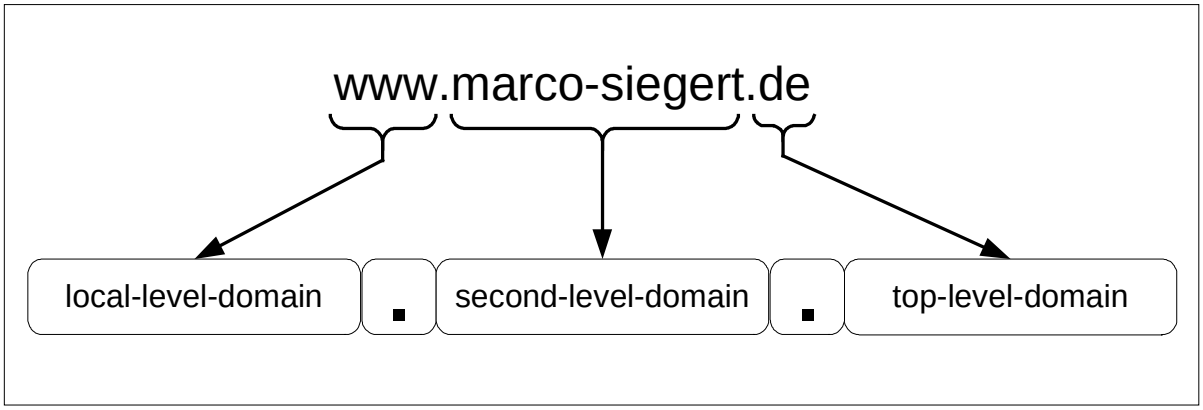

Abbildung 4: Systematischer Aufbau einer Domain-Adresse

Innerhalb der TLDs unterscheidet man zwischen sogenannten „generic Top Level Domains“ (gTLDs) und „country code Top Level Domains“ (ccTLDs). „Der Bereich der gTLDs umfaßt derzeit drei offene Top-Level-Domains (com; org; net), die weltweit allen Internetnutzern zur Registrierung offen stehen, und vier Top-Level-Domains, die nur Organisationen und Einrichtungen in den USA (edu; mil; gov) bzw. internationalen Organisationen (int) vorbehalten sind.“[88] Ob eine ccTLD[89] nur durch Staatsangehörige registriert werden kann, oder für jeden beliebigen Nutzer, entscheidet die Registrierungsstelle, die für die entsprechende ccTLD verantwortlich ist. Eine Auswahl der geläufigsten TLDs zeigt die folgende Tabelle:

---

[86] Ramm, Recherchieren und Publizieren im World Wide Web, Seite 16 und 17, spricht im Zusammenhang mit einer vollständigen Domainadresse von „Fully Qualified Domain Name“.

[87] Diese Aussage gilt nur für die reine Domainadressierung, da noch weitere Angaben zur Adresse hinzukommen können, andere Angaben hingegen werden wieder von links nach rechts gelesen.

[88] Bettinger, Abschlußbericht der WIPO zum Internet Domain Name Process, CR 7/1999, Seite 445, Fn. 4

[89] Die Landeskennungen werden durch die ISO-3166-Norm festgelegt.

Domain	Erläuterung
Typenkennung (vollständig)	
com	(commercial) Kommerziell orientierter Namensinhaber
org	(organisation) Organisation
net	(network) Allgemeines Netz
edu	(educational) amerikanische Hochschulen
gov	(governement) amerikanische Behörden
mil	(military) amerikanische Militäreinrichtungen
arpa	(Advanced Research Projects Agency) Gründungsorganisation des Internet
Landeskennung (Auszug)	
de	Deutschland
ar	Österreich
ch	Schweiz
it	Italien
fr	Frankreich
uk	Großbritannien
my	Malaysia

Tabelle 2: Beispiele für TLDs

Jede dieser Top-Level-Domains stellt einen Verwaltungsbereich dar, für den es auch eine "Verwaltungsbehörde" gibt. Diese Stelle ist für die Namensvergabe von Sub-Level-Domains innerhalb ihres Verwaltungsbereichs zuständig. Wenn man beispielsweise einen Domain-Namen im Bereich des ccTLD „de“ beantragen will, muß der Antrag an die DE-NIC (Deutsches Network Information Center[90]) gestellt werden.

[90] http://www.denic.de/[06.08.2000]

Eine Anmeldung hat aber nur dann Erfolg, wenn die Namensadresse noch nicht anderweitig vergeben wurde. Das ergibt sich aus der logischen Konsequenz, daß eine Adressierung eindeutig sein muß.

Die Notwendigkeit einer Registrierung hatte zur Folge, daß Namen großer Firmen, die noch keine eigene Domain beantragt hatten, durch „geschäftstüchtige“ Personen registriert wurden. Erkannte die Firma dann irgendwann die Zeichen der Zeit und wollte sie dann eine Domain mit ihrem Firmennamen registrieren, mußte sie diese oft teuer zurückkaufen. Diese Vorgehensweise nennt man Domain-Grabbing. Mittlerweile hat die Rechtsprechung diesen Machenschaften einen Riegel vorgeschoben. Dennoch kommt es im Zusammenhang mit attraktiven Domain-Namen immer wieder zu Rechtsstreitigkeiten. Wenn etwa zwei zufällig gleichnamige Firmen, die sonst nichts miteinander zu tun haben, den gleichen Domain-Namen reservieren lassen wollen, kann nur eine der Firmen den Zuschlag erhalten. Um Streitigkeiten dieser Art zu reduzieren, gibt es mittlerweile auch Bestrebungen, neue TLDs einzuführen[91].

Inhaber von zweiteiligen Domain-Namen können nochmals Sub-Level-Domains vergeben. So ist es keine Seltenheit, daß beispielsweise Zugangsanbieter unterhalb ihres Domain-Namen (z.B. name-zugangsanbieter.de) weitere Sub-Domains einrichten (z.B. home.name-zugangsanbieter.de oder news.name-zugangsanbieter.de).

4.5 Client-Server-Architektur

Das Internet baut auf der Grundlage der Client-Server-Architektur auf. Wie bereits angesprochen bietet das Internet verschiedene Dienste an (z.B. E-Mail, FTP, WWW etc.). Wie bei einer Mailbox handelt es sich bei E-Mail um ein Programm, das auf einen bestimmten Computer installiert ist und auf Anfragen wartet. Den Computer nennt man Server (dt.: Diener), da er das Programm zur Verfügung stellt. Ähnlich verhält es sich mit den anderen Diensten des Internets. Grundsätzlich erfordert jeder Dienst ein eigenes Programm (Server-Software). Aber nicht jedes Programm fordert einen eigenen Server. Über das Netzwerk erhält man Zugang zu solch einen Server. Er wartet ständig auf Anfragen von Clients.

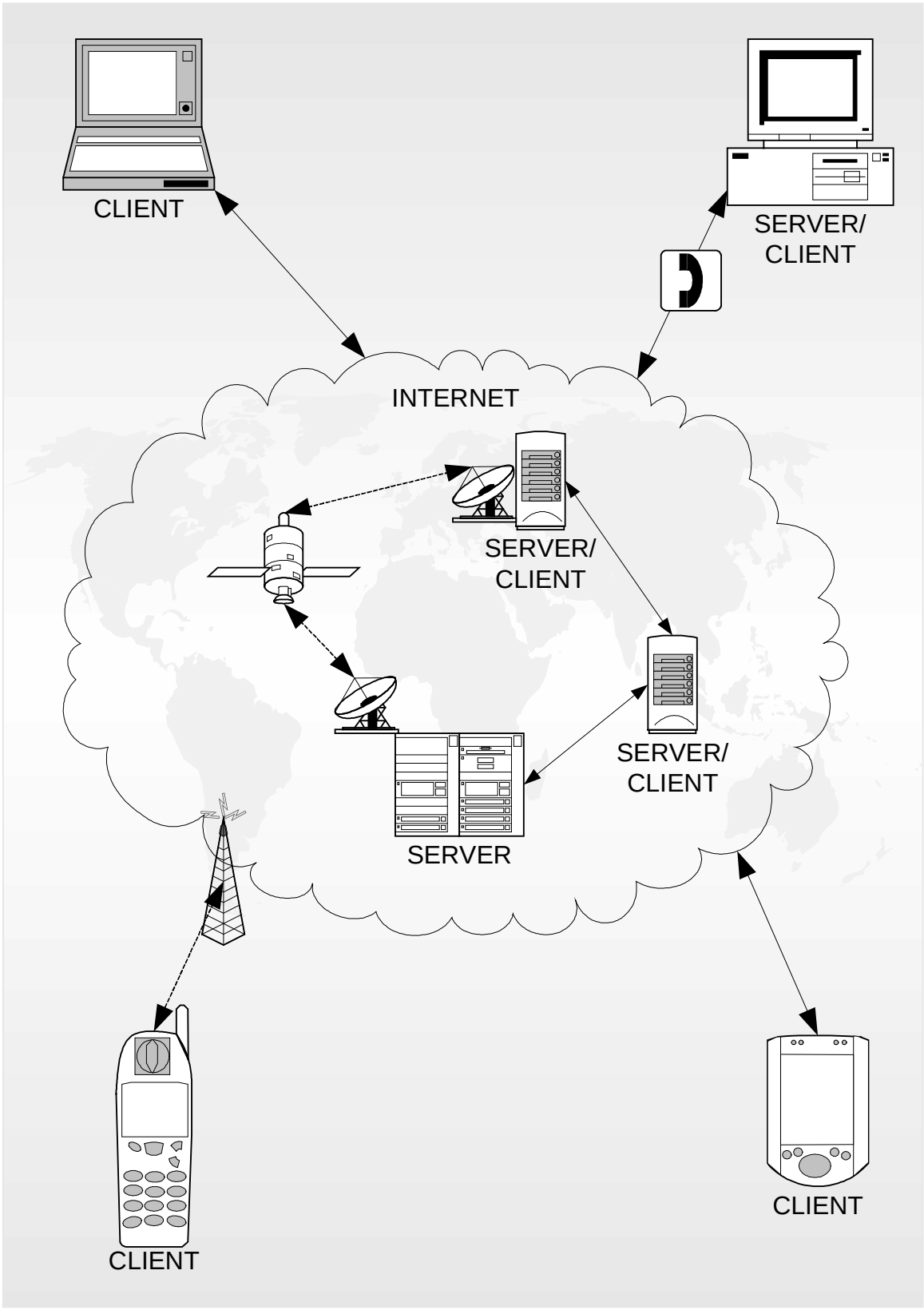

Abbildung 5: Vielfalt einer Client-Server-Architektur

---

[91] Über den Stand der Dinge: Bettinger, Abschlußbericht der WIPO zum Internet Domain Name Process, CR 7/1999, Seite 445 bis 448

Auf den Clients hingegen muß eine entsprechende Client-Software arbeiten, die die Anfragen an den Server stellt. Somit sind Server Hosts, auf denen eine Server-Software läuft. Clients sind Hosts, auf denen eine Client-Software läuft.

Um die Kommunikation zwischen den verschiedenen Clients und ihren korrs-pondierenden Servern zu regeln, gibt es entsprechende Protokolle. Client-Server-Kommunikation, im WWW etwa regelt das HTTP-Protokoll. Ein solches Protokoll läuft oberhalb des TCP/IP-Protokolls ab.

Daß ein Client Daten anfordert und ein Server die Daten sendet, ist der Normalfall. Es gibt jedoch auch "Ausnahmen". So kann ein Client nicht nur Daten anfordern, sondern auch Daten an einen Server schicken: zum Beispiel, wenn man per FTP eine Datei auf den Server-Rechner hochladen möchte oder wenn man eine E-Mail versenden will. In diesen Fällen spricht man auch von Client-Push ("Client drängt dem Server Daten auf").

Ein anderer Ausnahmefall ist es, wenn der Server zuerst aktiv wird und dem Client etwas ohne dessen Anforderung zuschickt. In diesem Zusammenhang spricht man von Server-Push ("Server drängt dem Clienten Daten auf"). Neue Technologien wollen diesen Ausnahmefall zu einer Regel machen: Diese Technologien sollen es ermöglichen, daß ein Client regelmäßig Daten empfangen kann, ohne diese explizit anzufordern. Dadurch sind Broadcasting-Dienste - wie beispielsweise Newsletter - realisierbar. Der Netscape Navigator und der Microsoft Internet Explorer (beide ab Version 4.0) haben entsprechende Schnittstellen, um solche Dienste in Anspruch zu nehmen.

4.6 Routing und Gateways

Im Internet ist es grundsätzlich nur innerhalb des eigenen Sub-Netzes möglich, Daten direkt von einer IP-Adresse zu einer anderen zu schicken. Das DNS spielt hierbei keine Rolle, entscheidend sind allein die IP-Adressen. In allen anderen Fällen, in denen die Daten an eine Adresse eines anderen Netzes geschickt werden sollen, werden Rechner benötigt, die den Verkehr zwischen den einzelnen Netzwerken koordinieren. „In der Internetarchitektur wird zwischen Router und Gateways unterschieden.

Ein Router stellt eine protokollgebundene Verbindung zwischen zwei oder mehreren Netzwerken her. Voraussetzung für den Datenverkehr über einen

Router ist die Verwendung desselben Protokolls durch die angeschlossenen Netzwerke. [...] Ein Gateway hingegen ermöglicht eine Verbindung über Protokollgrenzen hinweg.“[92] Damit sind die Gateways grundlegender Baustein für das weltumspannende Internet.

Das Weiterleiten der Daten zwischen Sub-Netzen wird als Routing bezeichnet. Die Beschreibungen der möglichen Routen, vom eigenen Netzwerk zu anderen Netzwerken, werden auf den Gateway-Rechnern und den Routern in sogenannten Routing-Tabellen vorgehalten.

Zu den Aufgaben eines Gateways/Routers gehört auch die Ermittlung einer Alternativ-Route, wenn die übliche Route nicht funktioniert. Dies passiert etwa, weil bei der entsprechenden Leitung eine Störung oder ein Datenstau aufgetreten ist. Gateways/Router senden sich ständig Testpakete zu, um das Funktionieren der Verbindung sicherzustellen und für Datentransfers "verkehrsarme" Wege zu finden.

Wenn also im Internet ein Datentransfer stattfindet, ist keinesfalls von vornherein klar, welchen Weg die Daten nehmen. Sogar einzelne Pakete einer einzigen Sendung können völlig unterschiedliche Wege nehmen. Wenn man beispielsweise von Deutschland aus eine WWW-Seite von einem amerikanischen Rechner aufruft, kann es passieren, daß die Hälfte der Seite über den Atlantik kommt und die andere Hälfte über den Pazifik. Nun wird auch klar, warum das TCP/IP in der beschriebenen Weise arbeiten muß.

4.7 Organisation des Internets

Angesichts der komplexen Technik, die das Internet zweifelsfrei darstellt, ergibt sich zwangsläufig die Frage, wer das Internet organisiert oder wie es sich organisiert. Wer verwaltet das Netzwerk, wem gehört es?

Angesichts der Nutzerzahlen ist der Verwaltungsaufwand im Netz vergleichsweise gering. Die meisten Endanwender wissen nicht einmal, daß es Verwaltungsstellen überhaupt gibt.

Fest steht, daß sich das Internet aus vielen kleinen Netzen zusammensetzt. Grundsätzlich unterliegen diese Einzelnetzwerke der Herrschaftsgewalt ihres jeweiligen Betreibers. „Demzufolge ist jeder mit dem Internet verbundene

---

[92] Alpar, Kommerzielle Nutzung des Internet, Seite 27 und 28

Teilnehmer ein Teileigentümer, nämlich als Eigner seines Gerätes oder Teilnetzes. Es existiert daher weder ein zentraler Eigentümer noch eine zentrale Leitung bzw. Verwaltung."[93] Da sich aber die Netze zu einem Verbund zusammengeschlossen haben, einheitliche Standards benutzen und faktisch jeder einzelne Betreiber auf seine „Nachbarn" angewiesen ist, muß es gewisse Regeln geben. Ohne dieses „ungeschriebene Gesetz" könnte das Internet nicht existieren.

Viele Bereiche des Internets beruhen faktisch auf Selbstorganisation. Bei Diensten wie E-Mail gilt beispielsweise das stille Abkommen, daß jeder beteiligte Gateway alle Mails weiterleitet, auch wenn weder Sender noch Empfänger dem eigenen Subnetz angehören. Die Kosten trägt zwar der Netzbetreiber, aber da alle ein Interesse am weltweiten Funktionieren des Netzes haben, ist jeder bereit, die anfallenden Mehrkosten zu tragen.

Die Funktionsfähigkeit des Internets basiert also auf einer Bereitschaft der Beteiligten, keine Pfennigfuchserei zu betreiben! Großzügigkeit hat das Internet geschaffen, und Kleingeisterei ist der größte Feind der Internet-Idee. Nicht zu vergessen ist auch die staatliche Subventionierung des Netzwerkes.

Offizielle Anlaufstellen gibt es für die Vergabe von Netzwerkadressen (IP-Adressen) und für Namensadressen (DNS). Für die Vergabe von IP-Adressen innerhalb eines Netzwerks ist der jeweilige Netzbetreiber verantwortlich, da er aus seinem ihm zugewiesenen Adreßbereich wiederum einen weiteren Adreßbereich kapseln kann. Will also ein kommerzielles Unternehmen eine Standverbindung zum Internet und gleichzeitig Zugangsanbieter für Endanwender werden, muß es sich ein Klasse-A-, -B- oder –C-Netz zuweisen lassen. Ferner kann er durch einen Vertrag mit einem anderen Netzbetreiber, der bereits „online" ist, einen Teil von dessen Adreßbereich erwerben.

Neben den Netzwerkbetreibern gibt es noch verschiedene Organisationen, die sich um Standards innerhalb des Internets kümmern[94] [95] [96].

---

[93] ebd., Seite 35

[94] Eine Auswahl der wichtigsten Organisationen findet sich in der Anlage 1.

[95] Zur Organisation der „Internet Society" (ISOC) vgl. auch: Alpar, Kommerzielle Nutzung des Internet, Seite 38.

[96] Zur Bildung von Internet-Standards durch die „Request for Comments" (RFC) vgl. Alpar, Kommerzielle Nutzung des Internet, Seite 39 – 41.

Die Kosten für die Datenübertragungen im Internet tragen die Betreiber der Sub-Netze. Diese Kosten pflanzen sich nach unten fort, zu Providern innerhalb der Sub-Netze und zu den Endanwendern, die über Provider Zugang zum Internet haben oder Internet-Services nutzen.

Für die internationale zentrale Adreßverwaltung war ursprünglich das amerikanische „Internet Network Information Center“ (InterNIC)[97] verantwortlich. Diese Aufgabe soll für InterNIC bis September 2000 befristet sein und dann durch eine neue Organisation für die Registrierung und Verwaltung der Adressen, der „Internet Corporation for Assigned Numbers and Names“ (ICANN), abgelöst werden[98] [99]. Seit März 1999 erfolgt die Übernahme der technischen Kontrolle durch ICANN.

Durch das gTLD-MoU (generic Top Level Domains – Memorandum of Understanding) wurde im Vorfeld ein Vorschlag unterbreitet, der als zukünftige Oberaufsicht über die Vergabe und Verwaltung der Internetadressen die UNO beziehungsweise ihre Unterorganisation „International Telecommunications Union“ (ITU) vorsah. Die US-Regierung hingegen verfolgte einen anderen Plan, nach dem die zukünftige Verwaltung privatwirtschaftlich organisiert werden sollte. Der Kompromiß ist ICANN.

Das InterNIC wird von Network Solutions Inc. im Auftrag der „National Science Foundation“ (NSF) geleitet. Hier werden Domain - und Netzwerkadressen registriert. Die Aufgaben der Adreßregistrierung wird durch die InterNIC zum größten Teil an regionale Institutionen vergeben. In Europa ist hierfür die „Réseaux IP Européans“ (RIPE)[100] in Amsterdam zuständig. In Deutschland übernimmt diese Aufgabe das „Deutsche Network Information Center“ (DE-NIC)[101] an der Universität Karlsruhe. Das DENIC koordiniert die Vergabe von Domain - und Netzwerkadressen.

---

[97] http://www.internic.net/[06.08.2000]

[98] Für nähere Informationen vgl.: Ermert, Namenspatron, Seite 48.

[99] Vgl. auch: Kuri, Canned Heat, Seite 32.

[100] http://www.ripe.net/[06.08.2000]

[101] http://www.denic.de/[06.08.2000] und http://www.nic.de/[06.08.2000]

4.8 Zugang zum Internet

4.8.1 Allgemeines

So vielseitig das Internet ist, so unterschiedlich sind auch die technischen Möglichkeiten, am Internet teilzuhaben. Im Grunde kann man nur zwei wesentliche Arten der Zugangserlangung unterscheiden. Zum einen besteht die Möglichkeit, selbst Provider im weitesten Sinne zu sein. Provider sind über sogenannte Standleitungen mit dem Internet verbunden. Das Unterhalten einer Standleitung bedeutet, daß der angeschlossene Rechner 24 Stunden am Tag von jedem Punkt der Welt erreichbar ist. Diese Möglichkeit kommt für größere Unternehmen, Behörden, staatliche Einrichtungen etc. in Betracht, da diese permanenten Verbindungen sehr kostenintensiv sind.

Für einen normalen Benutzer kommt diese Variante nicht in Frage, da sie seine finanziellen Mittel übersteigen würde. Wenn also ein normaler Benutzer Zugang zum Internet haben möchte, muß er sich eines Providers bedienen[102]. Ein Provider ist beispielsweise ein Unternehmen, eine Behörde oder eine staatliche Einrichtung, die eine Standleitung zum Internet unterhält und die es privaten Benutzern ermöglicht, sich über ihren Host in das Internet einzuwählen. Ob diese Benutzung entgeltlich erfolgt oder nicht, soll an dieser Stelle nicht erläutert werden, da sich an den technischen Grundlagen nichts ändert.

4.8.2 Zugangsmöglichkeiten nach Alpar und Ramm

Nach Alpar kann man grundsätzlich vier unterschiedliche Zugangsmöglichkeiten (eine der vier Möglichkeiten ist die Standleitung, die bereits angesprochen wurde) zum Internet unterscheiden[103]. Ramm zählt drei wesentliche Möglichkeiten auf, die Standleitung erwähnt er nicht explizit[104].

Bei den vorhandenen Möglichkeiten unterscheidet Alpar maßgeblich zwischen vollwertigen Internet-Online-Zugängen und eingeschränkten Internet-Offline-Zugängen. Das besondere an den Internet-Offline-Zugängen besteht darin, daß ein Server bestimmte Aufgaben für einen Clienten erledigt.

---

[102] Die Unterscheidung nach Internet Access-Provider, Serviceprovider und Contentprovider spielt an dieser Stelle noch keine Rolle, da sie ausschließlich für rechtliche Betrachtungen verwendet wird.
[103] Alpar, Kommerzielle Nutzung des Internet, Seite 32 – 34

Durch den Clienten wird dann nur eine Verbindung mit dem jeweiligen Server aufgebaut und die Ergebnisse der gestellten Aufgaben heruntergeladen. Der Client kommuniziert also nur mit einem einzigen Server, der quasi zu einem Clienten „umfunktioniert“ wird.

Einer der wichtigsten Internet-Offline-Zugänge ist die UUCP-Verbindung[105]. Die Datenübertragungsmethode basiert auf dem Unix-to-Unix-Copy-Protocol, welches ursprünglich für den Datenaustausch zwischen Unix-Rechnern gedacht war. Allerdings stehen mittlerweile auch für andere Betriebssysteme entsprechende Implementierungen zur Verfügung. Das Protokoll ermöglicht das Downloaden von einem Server, der für den Benutzer eingehende Nachrichten sammelt. Diese Daten können dann nach Abbruch der Verbindung (also offline) bearbeitet werden. Leider beschränkt sich diese Methode nur auf das Abrufen von Mails oder News. Andere Dienste des Internets sind über dieses Protokoll nur schwer zu realisieren. „Diese Verfahrensweise ist im Prinzip die gleiche wie bei Hobby-Mailboxnetzen [...]. Man nennt sie auch `store-and-forward-Prinzip´.“[106]

Ein klassischer Internet-Online-Zugang ist die Terminalverbindung. Hierbei greift der Benutzer über ein Terminalprogramm auf einen Host zu. Er bedient dann die Programme, die auf diesem Host laufen. Es erfolgt also eine Art Fernsteuerung der Host-Software. Parallel zu dieser Verbindung kann man dann noch eine UUCP-Verbindung aufbauen, um die gewonnenen Daten auf den eigenen Computer zu übertragen. Der Rechner kann direkt an den Host angeschlossen sein oder seine Verbindung über ein Modem und die Telefonleitung herstellen. Ramm spricht in diesem Zusammenhang von „Online-Accounts“[107]. Der Benutzer kann alle Internetdienste benutzen, sofern auf dem Host das entsprechende Clientprogramm für den jeweiligen Dienst installiert ist. Da sich eine Terminalverbindung so verhält, als ob man selbst vor dem Host sitzen würde, muß man natürlich auch das Betriebssystem des Hosts beherrschen.

---

[104] Ramm, Recherchieren und Publizieren im World Wide Web, Seite 31 - 40
[105] Unix-to-Unix-Copy (UUCP)
[106] Ramm, Recherchieren und Publizieren im World Wide Web, Seite 32
[107] ebd., Seite 31 - 32

Ein weiterer Internet-Online-Zugang ist die SLIP- oder PPP-Verbindung. Hierbei handelt es sich um eine direkte TCP/IP-Verbindung. Die Telefonleitung erlaubt kein paketorientiertes Empfangen und Senden von Daten. SLIP und PPP sind für die Wandlung von serieller in paketorientierte Übertragung und umgekehrt verantwortlich. PPP ist hierbei die neuere Variante.

Über die Telefonleitung (Modem oder ISDN) wird mittels SLIP/PPP eine Verbindung zum Provider aufgebaut, der online ist und dem Benutzer den Zugriff auf die verschiedenen Internetdienste erlaubt. Der Benutzer erhält dabei eine eigene IP-Adresse. Diese kann vom Provider fest vergeben werden oder sich bei jeder Einwahl ändern. In diesem Zusammenhang spricht man auch von statischer oder dynamischer Adressvergabe. Die IP-Adresse wird vom Provider zugeteilt und gehört zu seinem Adressbereich. Da der Benutzer eine eigene IP-Adresse erhält, ist er nach der Einwahl ein vollwertiger Host im Internet, d.h. er kann jeden Rechner über dessen IP-Adresse erreichen. Allerdings kann der Host auch von jedem anderen Rechner erreicht werden, der „online“ ist. Der Benutzer kann alle Dienste des Internets nutzen, wenn er die entsprechenden Client-Programme auf seinem Rechner installiert hat.

4.8.3 Klassifizierung nach Jofer

Wie bereits ausgeführt, kann sich eine Organisation, aber auch jede Privatperson eine permanente Verbindung zum Internet einrichten, indem sie beispielsweise eine Standleitung zu einem Netzbetreiber herstellt. Diese Möglichkeit besteht, ist aber sehr kostenintensiv und daher für einen Normalverbraucher nicht erschwinglich. Jofer bezeichnet diese Art des Netzzugangs als dezidierten Zugang. Zu dieser Zugangsmöglichkeit muß also auch ein Terminal[108] eines Hochschulrechenzentrums zählen, da es eine dauerhafte Verbindung zum Server der Einrichtung besitzt.

Neben den dauerhaften Verbindungen gibt es auch noch temporäre Verbindungen zum Internet, also zeitlich beschränkte Verbindungen. Jofer unter-

[108] Ramm, Recherchieren und Publizieren im World Wide Web, Seite 31, spricht in diesem Zusammenhang von einem Online-Account.

scheidet hierbei zwischen temporärer direkter und temporärer indirekter Internetverbindung[109].

Die klassischste Form der temporären direkten Internetverbindung ist die Anwahl eines permanent mit dem Internet verbundenen Rechners mittels Modem/ISDN/ADSL[110] über die Telefonleitung. Beim Verbindungsaufbau mittels Modem wird die Telefonnummer des Host-Modems des jeweiligen Zugangsanbieters angewählt. Zwischen den Modems wird dann die Verbindung hergestellt.

Im Gegensatz dazu wird bei der temporären indirekten Internetverbindung ein sogenannter Online-Dienst angewählt. Die Besonderheit dieses Zugangs besteht darin, daß die Online-Dienste eine eigene Zugangssoftware benötigen, die spezielle Protokolle benutzt. Innerhalb des Online-Dienstes besteht dann auch die Möglichkeit, daß Dienste angeboten werden, die das Standardangebot des Internets übersteigen. D.h. es ist durchaus normal, daß ein Online-Dienst zusätzliche Dienste anbietet, die dann aber nur von Mitgliedern gerade dieses Online-Dienstes genutzt werden können[111].

4.8.4 Die Online-Dienste

Eine besondere Zugangsmöglichkeit zum Internet bieten die verschiedenen Online-Dienste. Sie erfreuen sich unter den Internetnutzern zunehmender Beliebtheit. Zu den Online-Diensten gehören u.a. T-Online, AOL und CompuServe. Was unterscheidet nun diese Online-Dienste von den „normalen“ Providern? Um den Unterschied verstehen zu können, muß man die Grundidee und die Leitgedanken des Internets heranziehen. Das Internet ist ein Zusammenschluß von kleineren und größeren Computernetzen zu einem weltumspannenden Netzwerk. Um miteinander kommunizieren zu können, verwenden die angeschlossenen Computer ein einheitliches Protokollsystem für die Adressierung (IP) und die Datenübermittlung (TCP). Ferner wurden mehrere Dienste entwickelt (Client-Server-Programme), die auf dem TCP/IP aufbauen, also In-

---

[109] Jofer, Strafverfolgung im Internet, Seite 19 ff.

[110] An dieser Stelle nur das Modem zu erwähnen wäre falsch, da der Verbindungsaufbau über ISDN und ADSL nicht mit der Modulation und Demodulation eines Modems gleichzusetzen ist; ferner werden die enstsprechenden Geräte auch nicht Modem genannt, sondern ISDN- bzw. ADSL-Adapter.

[111] Das beste Beispiel ist hier das btx-Angebot von T-Online (so funktioniert Homebanking meistens nur über T-Online, wenn die entsprechende Bank an das Datex-P-Netz angeschlossen ist).

ternet-Standards darstellen. Nun ist es keineswegs so, daß ein kleines – an das Internet angeschlossenes Netzwerk – alle Dienste unterstützen muß.

So kann es also durchaus passieren, daß der Nutzer eines bestimmten Netzwerkes nicht alle Internet-Dienste nutzen kann. Auf der anderen Seite besteht aber auch die Möglichkeit, daß in einem Netzwerk - neben dem Internet-Standard - noch andere Anwendungen möglich sind, die nicht auf TCP/IP laufen oder die zwar auf TCP/IP laufen, aber kein Internet-Standard sind. In beiden Fällen ist ein solcher Dienst eben nur in dem lokalen Netzwerk nutzbar. Die Internet-Dienste bleiben natürlich auch nutzbar. Die Schlußfolgerung aus diesen Ausführungen ist, daß es durchaus Netzwerke geben kann, in denen neben dem Internet-Standard noch weitere Angebote bestehen. Das beste Beispiel ist Btx von T-Online. Btx ist nur für T-Online-Kunden nutzbar. Daß es kein Internet-Standard ist, erkennt man an der Notwendigkeit einer speziellen Software (KIT-Decoder) für die Benutzung.

Provider, die neben ihren eigenen Netzwerkdiensten auch die Dienste des Internets anbieten, nennt man Online-Dienste. Das Besondere an diesen Diensten ist, daß die Benutzer oft denken, das Internet zu benutzen, obwohl sie eigentlich beispielsweise den netzwerkeigenen Chat benutzen und keinen „Internet Relay Chat“ (IRC). Daß sie Teil des Internets sind, kann nicht bestritten werden, da sie eine physikalische Verbindung zu den Backbones besitzen.

Zur Zeit verschwimmen die Grenzen zwischen den Online-Diensten und den „normalen“ Providern, da sich der Betreiber des Online-Dienstes gegenüber einem Benutzer auch als „normaler“ Provider verhalten kann. D.h. daß z.B. T-Online auch die Einwahl über das DFÜ-Netzwerk ermöglicht und nicht unbedingt die spezifische Zugangssoftware benötigt wird. Dann steht allerdings nur der Internet-Standard zur Verfügung. Die Nutzung von Btx wäre nicht möglich.

4.8.5 Schlußfolgerung

Die Möglichkeiten eines Benutzers hängen grundsätzlich von der Art des Netzzuganges ab. Die Angebotspalette kann von Anbieter zu Anbieter verschieden sein. Die Zugangsmöglichkeiten sind vielfältig und durch die ständige Neuentwicklung einem steten Wandel unterworfen.

Grundsätzlich sind die Klassifizierungen von Alpar/Ramm und Jofer brauchbar. Sie entsprechen der jeweiligen Zeit, in der sie erarbeitet wurden, und dem jeweiligen Stand der Technik.

Doch gerade die Technik im Computerbereich ist einer ständigen Veränderung und Erneuerung unterworfen, so daß eine Klassifizierung schnell überholt sein kann.

Eine Gliederung ergibt nur dann einen Sinn, wenn sich jeder denkbare Fall in das Schema einordnen läßt. In diesem Sinne kann es sich bei den vorgestellten Zugangsmöglichkeiten nach Alpar/Ramm nicht um eine Klassifizierung handeln. Die Klassifizierung nach Jofer vermag m.E. nicht zu überzeugen, da sie die technischen Hintergründe nicht klar trennt.

4.9 Ethernet, Btx und Mailboxnetze

4.9.1 Ethernet

Im Laufe der Entwicklung wurden mehr und mehr regionale Netzwerke mit den grundlegenden Eigenschaften des ARPA – und später des CS- und NSFNet - geschaffen. Die Netzwerke wurden entweder durch private Investoren oder durch staatliche Organisationen oder Behörden finanziert. Die Erfindung der Ethernet-Technik[112] durch Metcalf verhalf der Netzwerktechnik zum Durchbruch, da sie kostengünstig umsetzbar und somit für kleinere Institutionen erschwinglich war. Später konnten diese Netzwerke über Gateways auch mit dem Internet verbunden werden.

4.9.2 Bildschirmtext (Btx) und T-Online

Durch den Engländer Fedida wurde Mitte der Siebziger Jahre der Videotex erfunden[113]. In Deutschland erhielt das System den Namen „Bildschirmtext“. 1979 wurde „Bildschirmtext“ als Btx erstmals auf der Internationalen Funkausstellung in Berlin vorgeführt. Entscheidend für die Entwicklung in Deutschland

[112] Bei der Ethernet-Technik handelt es sich um eine grundlegend andere Netzwerktechnik als TCP/IP, aufgebaut wird ein sogenanntes LAN (eng.: local area network), welches auf einem eng begrenzten Raum installiert wird (z.B. Vernetzung eines Gebäudes).

[113] Videotex ist nicht mit Videotext zu verwechseln, der von vielen Fernsehanstalten parallel zum Fernsehprogramm ausgestrahlt wird.

war die Einführung von Btx durch die Deutsche Bundespost im Jahre 1983. Nach Abschluß eines Feldversuches wurde 1984 der bundesweite Aufbau von Btx abgeschlossen.

Bis 1989 konnte man Btx nur mit Hardware-Decodern in Verbindung mit Fernsehgeräten nutzen, danach wurden durch die Bundespost Software-Decoder zugelassen. Damit öffnete sich Btx dem PC. Im Jahre 1991 gab es weltweit mehrere Videotex-Systeme, u.a. auch in den USA und in Frankreich.

„Am 1.1.1993 führte die Telekom das neue Konzept Datex-J/Btx ein.“[114] Dieses Konzept beinhaltet die Trennung von Inhalt (Btx) und Datennetzwerk (Datex-J). 1995 erhielt der Dienst nochmals einen neuen Namen - unter dem er noch heute existiert – T-Online. Im T-Online-Netz wird ein spezieller Übertragungsstandard verwendet. Deshalb ist für den Zugang auch eine spezielle Decoder-Software notwendig. Die Verbindung zum Datex-J-Netz erhält der Benutzer über das Telefonnetz. Über das Netzwerk stehen die verschiedenen Dienste von T-Online (Btx, Btx Plus, E-Mail oder Internet) zur Verfügung. Wer die Dienste des Internets über T-Online nutzen möchte, muß dafür einen speziellen Decoder benutzen, der TCP/IP unterstützt.

T-Online bietet verschiedene Netzübergänge (Gateways). Zum einen gibt es einen Gateway zum Internet und zum Datex-P-Netz[115] sowie Übergänge zu vergleichbaren Videotex-Systemen weltweit wie z.B.: Teletel (Frankreich), Prestel (Großbritannien), Videotex (Schweiz), Ibertex (Spanien), Videotexnet (Niederlande), Videotel (Italien), PAN (engl. Public Access Network in Österreich) oder Luxtel (Luxemburg). Andere Online-Dienste wie z.B. CompuServe sind auch über T-Online erreichbar. Auch auf einige Mailboxen (z.B. CyberCity) kann über T-Online zugegriffen werden, das Netzwerk dient somit als Gateway zu den verschiedensten Diensten und Netzwerken.

„T-Online besteht aus einer Leitzentrale sowie vielen verteilten Netzknoten. Die Leitzentrale befindet sich in Ulm. Von dort aus wird das gesamte System verwaltet und gesteuert. In der Leitzentrale sind alle Teilnehmerdaten und die Programme der Anbieter im Original abgespeichert. Die regionalen Netz-

---

[114] Fink, Die Welt von T-Online, Seite 9

[115] Anbieter können ihre Seiten nicht nur direkt im T-Online Netz speichern, sondern auch auf externen Rechnern, diese sind dann an das Datex-P-Netz angeschlossen, welches die Verbindung zu T-Online darstellt.

knoten übermitteln alle Daten an die Leitzentrale. In den regionalen Netzknoten werden nur häufig aufgerufene Seiten und häufig benötigte Teilnehmerdaten als Kopie der Originaldaten gespeichert. Sind Daten nicht regional vorhanden, werden sie aus der Leitzentrale übermittelt.

Es gibt also keine direkte Verbindung vom Teilnehmer zur Leitzentrale. Externe Rechner sind über die regionalen Netzknoten an T-Online angeschlossen."[116]

Der Abruf von Seiten eines Anbieters durch Benutzer kann kostenfrei oder unter Zahlung einer Gebühr erfolgen. Die Gebühren werden dem Anbieter monatlich durch T-Online überwiesen. Der Nutzer erhält eine Rechnung.

Informationen im T-Online-Netz liegen in Form von Seiten vor. Die Seiten eines Anbieters bilden dabei eine Art Baumstruktur. Ausgehend von einer Leitseite lassen sich weitere Seiten erreichen. Die Seiten wurden Anfangs nach dem CEPT-Standard erstellt, später nach dem KIT-Standard, der erweiterte Multimediaelemente unterstützt.

T-Online bietet verschiedene eigene Dienste. Dazu gehören u.a. Online-Banking (Bankgeschäfte), Online-Broking (Börsengeschäfte), Mitteilungsdienst und E-Mail, Telefax, Telex[117] und Telebrief[118], Absenden von Cityruf-Nachrichten[119], Telebox-400[120], Teledialoge[121] und Foren[122].

---

[116] Fink, Die Welt von T-Online, Seite 37

[117] Bei Telex handelt es sich um einen Dienst zur Übertragung von Mitteilungen, er umfaßt einen Zeichensatz von nur 32 Zeichen.

[118] Bei Telebrief handelt es sich um einen Dienst zur Übertragung von Mitteilungen, hierbei wird eine Mitteilung auf elektronischem Weg zu einem Postamt befördert und dann von dort auf herkömmlichem Wege zugestellt.

[119] Bei Cityruf handelt es sich um einen Funkrufdienst der Telekom, der mit einem speziellen Cityruf-Empfänger realisiert wird; man unterscheidet Cityruf Ton, Cityruf Numerik und Cityruf Text.

[120] Bei Telebox-400 handelt es sich um ein Mailboxsystem der Deutschen Telekom, es dient zum individuellen Mitteilungs -, Daten – und Grafikaustausch in über 50 Länder.

[121] Ein Teledialog ermöglicht die direkte Kommunikation zwischen mehreren Teilnehmern.

[122] Ein Forum ist eine Art „Schwarzes Brett“ oder Pinnwand, an der man eine Nachricht hinterläßt und dann nach einiger Zeit nachschaut, ob jemand eine Antwort in Form einer anderen Nachricht hinterlassen hat.

4.9.3 Mailboxnetze und andere Online-Dienste

Ein weiterer Online-Dienst ist CompuServe, der weltweit, und nicht wie T-Online nur in Deutschland, verfügbar ist. Die Palette der Dienste ist ähnlich umfangreich wie das Angebot von T-Online. Unterstützt wird insbesondere Internet, Telebox-400, Telex und Fax.

Eine andere netzähnliche Kommunikationsstruktur stellen die verschiedenen regionalen und internationalen Mailboxsysteme dar. Bei Mailboxen unterscheidet man Einport- und Mehrport-Mailboxen und Mailboxnetze. Auf die verschiedenen Mailboxen kann man auf unterschiedlichste Weise zugreifen. Unter Einsatz eines Modems ist die Nutzung des Telefonnetzes möglich. Nach der Digitalisierung des deutschen Telefonnetzes durch die Deutsche Telekom werden Sprache und Daten nunmehr digital und nicht mehr analog übertragen. Eine digitale End-to-End Verbindung bietet ISDN. Eine weitere Möglichkeit stellt die Verbindungsaufnahme über ein GSM-Netz (Mobilfunk) dar. Genau wie bei Btx kann der Zugang zu manchen Mailboxen oder anderen Informationsdiensten auch über Datex-P oder Datex-J erfolgen. Die Verbindung zu Datex-P wird entweder über Telefon oder einen speziellen X.25-Anschluß hergestellt.

Mailboxen sind nichts anderes als spezielle Mailbox-Programme, die auf einem Computer laufen, der mit einem Netzwerk (Telefon, ISDN etc.) verbunden ist. „Einport-Mailboxen werden in den meisten Fällen von Hobbyisten betrieben. Dazu sind ein Computer, ein Modem und ein Telefonanschluß notwendig.“[123] Auf einem Host muß ein Mailbox-Programm laufen. Über ein Terminalprogramm kann sich dann ein Benutzer in die Mailbox einwählen.

Bei Einport-Mailboxen kann sich immer nur ein Benutzer einwählen. Im Unterschied dazu ist bei Mehrport-Mailboxen die parallele Benutzung durch mehrere Benutzer möglich. Die Mehrport-Mailboxen sind oft gebührenpflichtig, da für den Betrieb mehrere parallele Telefonleitungen und dementsprechend auch mehrere Telefonnummern notwendig sind. Allerdings eröffnet eine Mailbox auch besondere Echtzeit-Interaktionsformen zwischen Menschen wie z.B. Chat oder Mehrbenutzer-Spiele. Fink teilt die Mailboxen nach ihrer Art in geschlossene Mailboxen (von Firmen oder Organisationen für interne – nichtöf-

[123] Fink, Mailboxen optimal nutzen, Seite 78

fentliche – Kommunikation), öffentliche Mailboxen (von Computervereinen, Hobbyisten oder Vereinen zur öffentlichen Kommunikation), Support-Mailboxen (von Firmen für z.B. Treiber – oder Softwareupdates) und kommerzielle Mailboxen (aus Eigenzweck) ein.

Die nächste Steigerungsstufe stellen die Mailboxnetze dar[124]. Hierbei handelt es sich um ein Verbund von Systemen Gleichgesinnter. „Bekannte Hobby-Mailboxnetze in Deutschland sind Fido, Z-Net und Maus.“[125] Fink zählt das Internet auch zu den Computer – und Mailboxnetzen[126]. Realisiert werden diese Netze durch spezielle Programme, die eine einheitliche Schnittstelle besitzen, über die die Kommunikation abgewickelt wird. Ferner ist eine bestimmte Adressierungsform notwendig, um jeden Teilnehmer eindeutig identifizieren zu können[127]. Indirekt stellen somit Datex-J/Btx oder CompuServe Mailboxnetze dar. Die Mailbox-Technik kann aber nicht mit dem Internet (TCP/IP) verglichen werden, da in normalen Mailboxnetzen keine Standleitungen[128] existieren.

[124] Für eine Übersicht über diverse Computer – und Mailboxnetze vgl. Fink, Mailboxen optimal nutzen, Seite 82 ff.

[125] Fink, Mailboxen optimal nutzen, Seite 80

[126] ebd., Seite 87

[127] Für nähere Informationen zu den verschiedenen Adressierungsformen im Fido-Netz, Z-Netz oder MausNet vgl. Fink, Mailboxen optimal nutzen, Seite 82 ff.

[128] Eine Standleitung ist die permanente Verbindung zwischen zwei Computern; im Gegensatz dazu stellt ein gewöhlicher Benutzer eine zeitlich begrenzte Wählverbindung zu einem Computer her.

5 Die Dienste des Internets

5.1 Allgemeines

Bei den Diensten des Internets[129] handelt es sich um sogenannte Server-Software, die auf einem Rechner läuft, der ständig mit dem Internet verbunden ist. Wie bereits dargestellt, arbeitet im Grunde jeder Internetdienst mit einem eigenen Protokoll. Diese einzelnen Protokolle setzen dabei auf das TCP auf. Grundsätzlich besteht die Möglichkeit, für jede Software einen eigenen Rechner zu verwenden. Aus Kostengründen werden aber häufig mehrere Dienste auf einem Server installiert. Wenn jetzt ein Paket einen solchen Rechner erreicht, würden die installierten Dienste nicht wissen, für welchen von ihnen das Paket nun eigentlich bestimmt ist. Zu diesem Zwecke wurde in das TCP die sogenannten TCP-Ports eingebaut. Diese TCP-Ports haben die Aufgabe, nur die Anfragen aufzunehmen, die auch für sie bestimmt sind. Die Ports werden durch numerische Werte zwischen 0 und 1023 adressiert. Für die Portbelegung gibt es festgelegte Standards, so daß jedem Dienst ein oder zwei Portnummern eindeutig zugeordnet sind. Wenn also ein Client eine Anfrage stellt, versieht er diese mit einer Portnummer. Der Server leitet dann die Pakete an den entsprechenden Port weiter. Die nachfolgende Tabelle gibt einen Überblick über die wichtigsten Portnummern.

[129] Die nachfolgende Gliederung entspricht ihren Grundzügen nach der von Alpar (Alpar, Kommerzielle Nutzung des Internet, Seite 49 –113).

Dienst	Portnummer
FTP	21 (Kontrollverbindung) 20 (Datenverbindung)
Gopher	70
Telnet	23
E-Mail	25
WWW	80
News	119

Tabelle 3: Internetdienste und ihre TCP-Portnummern

Um nun der angegebenen Adresse explizit eine Portnummer zuzuweisen, wird sie – durch Doppelpunkt abgetrennt – hinter der IP-Adresse oder der Domain-Adresse angegeben. Folgende Varianten wären also beispielsweise denkbar: 120.200.143.98:23 (eine Telnetverbindung) oder ftp.tripod.de:21 (eine FTP-Verbindung). Wenn ein spezieller Client genutzt wird, sind die Standardports meist voreingestellt, so daß die explizite Angabe einer Portnummer nur bei einem fehlgeschlagenen Verbindungsaufbau angegeben werden sollte. Mit einem sogenannten Portscann (die Software dazu nennt man Portscanner) kann man eine bestimmte Rechneradresse abfragen. Als Antwort erfolgt dann die Rückgabe aller aktiven TCP-Ports des Hosts.

5.2 Elektronische Post (E-Mail)

5.2.1 Allgemeines

E-Mail steht für „electronic mail“ (dt.: Elektronische Post) und ist der am meisten genutzte Dienst des Internets[130]. Die E-Mail dient dem Versenden von Nachrichten und Dateien. Die Funktionsweise ist mit der herkömmlichen Post vergleichbar[131]. Durch den Absender wird mittels eines Mail-Clienten eine

[130] Vgl. auch: Alpar, Kommerzielle Nutzung des Internet, Seite 74 – 77.

[131] Von überzeugten E-Mail-Benutzern wird die herkömmliche Post oft als „snail mail“ (dt.: Schneckenpost) bezeichnet.

Nachricht abgefaßt. Diese Nachricht wird dann mit der Empfängeradresse (E-Mail-Adresse) versehen und abgesendet. Jede ausgehende Nachricht wird auch automatisch mit der Absenderadresse versehen. So kann der Empfänger erkennen, von wem er die Nachricht erhalten hat und entsprechend antworten.

Um den Dienst E-Mail nutzen zu können, müssen also Absender und Empfänger über eine gültige E-Mail-Adresse verfügen[132], also in einem Mail-Server eingetragen sein. Die E-Mail-Adresse ist durch ein Paßwort geschützt, so daß ein unbefugtes Senden unter falschem Namen oder unberechtigtes Empfangen von E-Mails ausgeschlossen ist. Die allgemeine Form einer E-Mail-Adresse ist „benutzername@subdomain.top-level-domain“.

Das „@“ (eng.: at, dt.: bei) dient als Trennzeichen zwischen der Domain-Adresse und dem Benutzernamen des Inhabers. Der persönliche Benutzername ist oftmals der Name oder ein Namenskürzel (z.B.: m.siegert@nikocity.de), er kann aber auch frei erfunden werden (z.B.: fredchen@nikocity.de). Auf jeden Fall darf er nur einmal existieren.

Wie bei einem normalen Brief, besteht eine E-Mail grundsätzlich aus zwei Teilen, dem Nachrichtenteil (body) und dem Adreßteil (header). Im Nachrichtenteil steht die eigentliche Nachricht im ASCII-Code (American Standard Code of Information Interchange)133. Der Header besteht aus verschiedenen Headerfeldern, in denen der Benutzer verschiedene Informationen eintragen kann.

Bei der Arbeit mit E-Mail werden die Protokolle „Simple Mail Transfer Protocol“ (SMTP), „Post Office Protocol“ (POP) und das „Interactive Mail Access Protocol“ (IMAP) verwendet. „Das 1982 durch J.B.Postel vorgeschlagene Simple Mail Transfer Protocol (SMTP) regelt als zugrundeliegender Transportmechanismus den Versand (fast) aller via Internet übermittelter E-Mail (RFC 821).“[134] Das Versenden einer E-Mail erfolgt in der Weise, daß die Nachricht immer von Server zu Server weitergereicht wird, bis sie ihr Ziel erreicht hat. Die Kommunikation der Server erfolgt dabei über TCP Port 25. Im Gegensatz dazu regelt das POP die Kommunikation zwischen dem E-Mail-Clienten und dem Host, sowohl beim Empfang, als auch beim Senden. Voraussetzung dafür ist allerdings eine bestehende SLIP- oder PPP-Verbindung. Das IMAP ist für

---

[132] Zur Ermittlung von E-Mail-Adressen: Hartung, Internet, dp-special April 1998, Seite 11 und 12.

[133] Dieser Code kann u.a. nicht die Zeichen ü,ö,ä,ß darstellen, was ein erhebliches Problem ist.

die Fälle gedacht, bei denen durch mehrere Clienten auf den gleichen Account zugegriffen wird. Die nachfolgende Tabelle gibt eine Übersicht über Headerfelder (teilweise werden die Headerfelder durch die E-Mail-Clienten automatisch ausgefüllt):

[134] Alpar, Kommerzielle Nutzung des Internet, Seite 51

Headerfeld	Erläuterung
to	enthält die E-Mail-Adresse des Empfängers
cc	(carbon copy); Kopie der E-Mail geht an die eingetragene E-Mail-Adresse (beim Empfänger werden die Einträge dieses Feldes angezeigt)
bcc	(back carbon copy); Kopie der E-Mail geht an die eingetragene E-Mail-Adresse (beim Empfänger werden die Einträge dieses Feldes nicht angezeigt)
from	E-Mail-Adresse und Name/Pseudonym des Absenders
subject	Betreff der E-Mail
date	enthält das Datum und die Zeit des Absenders in der lokalen Zeit des Absenders (zumeist ist die Zeitzone mittels eines Kürzels oder als Abweichung von der Weltzeit=UTC angegeben
message-id	eindeutig Identifikationsnummer
recieved	enthält die Mail-Gateways, die die E-Mail auf dem Weg durch das Netz durchlaufen hat
reply-to	enthält eine E-Mail-Adresse, an die eine Rückantwort gehen soll, wenn auf die E-Mail geantwortet wird

Tabelle 4: Ausgewählte Bestandteile eines E-Mail Headers[135]

5.2.2 E-Mail-Anhänge (Attachments)

Attachment ist heute der im E-Mail-Verkehr übliche Begriff für Anhang. Dies beschreibt eine Technik, bei der mit der E-Mail z.B. eine Datei versendet werden kann[136]. Wie bereits angesprochen, kann eine E-Mail eigentlich nur reinen Text enthalten (ASCII-Zeichen). Was passiert nun, wenn man eine Binärdatei größeren Umfangs an eine E-Mail „anhängen“ will?

[135] Übernommen aus: Alpar, Kommerzielle Nutzung des Internet, Seite 50 (Tabelle 3.1).

[136] Diese angehängten Dateinen können von der unterschiedlichsten Sorte sein, so können Bild – oder Tondateien verschickt werden, einfache Textdateien aber auch ausführbare Programme.

„Eine [...] standardisierte Lösung wird durch das MIME Protokoll (Multipurpose Internet Mail Extension, RFC 1521) in Form einer Ausweitung des ursprünglichen E-Mail-Standards auf die Übermittlung von Audio-, Video- oder Bilddaten sowie Applikationen vorgeschlagen. MIME zerlegt dazu unter Umständen den Body einer E-Mail in mehrere Parts (multipart messages), die wiederum die eigentlichen Daten enthalten, und erweitert unter Wahrung des RFC 822 Standards den ursprünglichen Header einer E-Mail um [...] zusätzliche Felder."[137] [138] (siehe nachfolgende Tabelle)

Headerfeld	Erläuterung
mime-version	Versionsnummer
content-type	Art der Daten, die in der E-Mail übertragen werden
content-transfer-encoding	Art der verwendeten Konvertierung nach ASCII
content-id	ID zur Beschreibung des Inhalts
content-description	textuelle Beschreibung des Inhalts

Tabelle 5: MIME-Headerfelder[139]

Somit wird durch das MIME-Verfahren eine Binärdatei in ASCII-Text umgewandelt und dann versendet. Von besonderer Bedeutung sind hierbei die Headerfelder „content-type" und „content-transfer-encoding". Sie beschreiben die Art, der in der E-Mail enthaltenen Daten und das Konvertierungsverfahren. Welche Einträge im Headerfeld „content-type" möglich sind, verdeutlicht die nachfolgende Tabelle:

[137] Alpar, Kommerzielle Nutzung des Internet, Seite 53 und 54

[138] Eine weitere Möglichkeit, die an dieser Stelle jedoch nicht behandelt wird, bieten sogenannte Binär-ASCII-Konverter (z.B.: UUENCODE und UUDECODE). Hierbei wird die entsprechende Binärdatei z.B. durch UUENCODE in ASCII konvertiert, als E-Mail versandt und dann beim Empfänger wieder durch UUDECODE „entschlüsselt". Da durch einige E-Mail-Server die maximale Gößе einer E-Mail auf 64 kByte festgelegt ist, kann eine „übergroße" Datei auch auf mehrere E-Mails aufgeteilt werden.

[139] Übernommen aus: Alpar, Kommerzielle Nutzung des Internet, Seite 54 (Tabelle 3.2).

Bezeichnung	Erläuterung
Application	für alle Arten nicht näher spezifizierter binärer Daten
Image	z.B. GIF oder JPEG
Message	für eine in einer MIME E-Mail eingeschlossenen Nachricht (z.B. RFC 822)
Multipart	zur Kennzeichnung der Art, der in der MIME E-Mail enthaltenen Teile (z.B. MIXED)
Text	z.B. PLAIN, RICHTEXT
Video	z.B. MPEG

Tabelle 6: Mögliche Einträge für das Headerfeld „content-type“[140]

5.2.3 FreeMail

Heute ist es normal, daß man von einem Provider, bei dem man registriert ist, automatisch eine E-Mail-Adresse zugewiesen bekommt. Allerdings besteht auch die Möglichkeit, eine sogenannte FreeMail-Adresse zu bekommen. Dies bietet sich vor allem für Internet-Benutzer an, die über keinen eigenen Internetzugang verfügen. Die Post wird dann nicht vom Mailserver mittels E-Mail-Client abgeholt, sondern online gelesen. D.h. der Benutzer geht z.B. in ein Internet-Cafe und gibt die Adresse seines FreeMail-Anbieters ein (z.B.: www.hotmail.com[06.08.2000]). Dort kann er sich dann registrieren lassen. Nach der Eingabe von persönlichen Daten - die aber sehr leicht zu fälschen sind, indem man einfach Phantasiedaten eingibt – erhält man eine E-Mail-Adresse und ein persönliches Kennwort. Wenn man nun eine E-Mail schreiben will oder erhaltene E-Mails lesen möchte, muß man sich durch Eingabe des Benutzernamens und des persönlichen Paßwortes auf der Website des Free-Mail-Anbieters authentifizieren. Dann kann man online E-Mails lesen und schreiben. Die FreeMail-Anbieter (FreeMailer) haben bestimmte Optionen, wie ein E-Mail-Account (E-Mail-Konto) behandelt wird.

[140] Vgl. auch: Alpar, Kommerzielle Nutzung des Internet, Seite 54.

Werden eingegangene Nachrichten eine Zeitlang nicht gelesen oder wird die Kapazität des Accounts überschritten, werden die E-Mails gelöscht. Das hat den Nachteil, daß sie nicht mehr zur Verfügung stehen. Wählt man hingegen die Möglichkeit, einen E-Mail-Clienten zu benutzen, holt man einfach die Nachrichten vom Server und speichert sie auf der eigenen Festplatte ab. Dann gibt es auch keine Probleme mit den MIME E-Mails. Wenn man nämlich eine solche E-Mail direkt auf dem Server betrachtet, der den MIME-Standard nicht unterstützt, erhält man folglich nur ein Durcheinander von Zeichen. Daher bietet es sich an, wenn nötig auf HTML-E-Mails etc. zu verzichten und reine ASCII-Mails zu schreiben[141].

5.2.4 Digitale IDs

Das heutige E-Mail-System hat aber auch noch mit einigen anderen Problemen zu kämpfen. Eine normale E-Mail ist auf dem Weg vom Sender zum Empfänger etwa so geheim wie eine Ansichtskarte. Für vertrauliche Mitteilungen oder sensible Daten ist sie ungeeignet. Ferner läßt sich eine E-Mail-Adresse leicht fälschen, da ja der Name bei der Registrierung frei wählbar ist (z.B.: Hans Müller läßt sich eine E-Mail-Adresse „Franz.Maier@nikocity.de registrieren und schreibt eine E-Mail an Horst Maier, der davon überzeugt ist, eine Nachricht seines Sohnes zu bekommen). Je mehr Menschen vertrauliche Informationen per E-Mail senden, desto stärker muß gewährleistet werden, daß in E-Mail versandte Dokumente nicht gefälscht und gesendete Nachrichten von anderen Personen, als dem beabsichtigten Empfänger, nicht abgefangen und gelesen werden können. Zu diesem Zweck wurden zwei Mechanismen eingeführt, Zertifizierung und Verschlüsselung, die die Sicherheit und Vertraulichkeit von E-Mails weitestgehend sicherstellen können.

Durch den Einsatz digitaler IDs kann man die eigene Identität bei elektronischen Transaktionen auf ähnliche Art nachweisen, als würde man beim Einlösen eines Schecks den Personalausweis vorzeigen. Die digitale ID kann man

[141] Neuere E-Mail-Clients bieten auch die Möglichkeit, eine E-Mail im HTML-Format zu verfassen. Somit sind auch die vielfältigen Gestaltungsmöglichkeiten von HTML (wie z.B. Farben oder Hintergrundbilder) möglich. Natürlich wird diese E-Mail dann auch gemäß MIME konvertiert und ist daher beim Empfänger nur lesbar, wenn der Client MIME unterstützt.

auch zur Verschlüsselung von Nachrichten verwenden. Digitale IDs beinhalten die S/MIME-Spezifikation für sichere elektronische Post.

Hierbei handelt es sich um eine Verschlüsselungsmethode. Eine weitere Methode ist „Pretty Good Privacy“ (PGP). Hierbei handelt es sich um sogenannte Freie Software, die es für verschiedene Betriebssysteme gibt und die jeder unentgeltlich nutzen kann.

Eine digitale ID besteht aus einem "öffentlichen Schlüssel", einem "privaten Schlüssel" und einer "digitalen Signatur". Wenn man eine Nachricht digital signiert, fügt man einfach die digitale Signatur und den öffentlichen Schlüssel hinzu. Die Kombination aus digitaler Signatur und öffentlichem Schlüssel wird als "Zertifikat" bezeichnet.

Der Empfänger kann dann die digitale Signatur zur Überprüfung der Identität des Absenders verwenden. Mit Hilfe des öffentlichen Schlüssels kann er verschlüsselte Nachrichten an den ursprünglichen Absender zurückschicken. Dieser kann die verschlüsselten Nachrichten nur mit dem privaten Schlüssel lesen. Bevor man in der Lage ist, digital signierte Nachrichten zu senden, muß man eine digitale ID erwerben und das E-Mail-Konto für deren Einsatz einrichten.

Digitale IDs werden von unabhängigen Zertifizierungsstellen ausgegeben. Wenn man eine digitale ID auf der Website einer Zertifizierungsstelle beantragt, wird vor der Ausgabe die Identität des Antragstellers geprüft. Es existieren unterschiedliche Klassen digitaler IDs, die unterschiedlichen Stufen der Vertrauenswürdigkeit entsprechen. Weitere Informationen erhält man meist im Hilfesystem, auf der Website der Zertifizierungsstelle.

Wenn man die digitale ID einer anderen Person erhalten möchten, kann man die Person auffordern, eine digital signierte E-Mail zu senden. Ferner kann man auch auf der Website einer Zertifizierungsstelle die Datenbank für digitale IDs durchsuchen. Es gibt auch Internetverzeichnisdienste, die digitale IDs zusammen mit anderen Informationen speichern.

Durch die "Gültigkeitsprüfung" kann man die Gültigkeit einer digital signierten Nachricht feststellen. Wenn man eine solche Überprüfung vornimmt, fordert der E-Mail-Client - von der entsprechenden Zertifizierungsstelle - Informationen zu der digitalen ID an.

Die Zertifizierungsstelle sendet Informationen über den Status der digitalen ID. Dazu gehört auch, ob die digitale ID entzogen wurde. Zertifizierungsstellen speichern Daten zu Zertifikaten, die aufgrund von Verlust oder Kündigung entzogen wurden.

5.3 Diskussionsgruppen (News)

5.3.1 Allgemeines

„Um gezielt an Informationen einer speziellen Thematik zu gelangen, ist es sinnvoll mit Personen zu kommunizieren, die sich mit dieser Thematik auseinandersetzen. Das große Problem besteht meist darin, herauszufinden, wer sich mit diesem Thema beschäftigt. Eine Lösung des Problems wird im Internet in Form der Diskussionsgruppen angeboten, in denen Informationen zu zahlreichen Themengebieten wie Forschung, Lehre, Freizeit, Recht, Wirtschaft, Soziales usw. ausgetauscht werden.“[142]

Eine Newsgroup ist mit einem schwarzes Brett vergleichbar, an dem man Nachrichten hinterlassen kann, die alle Benutzer lesen können[143]. Jede Newsgroup behandelt einen Themenbereich. Mittlerweile sind mehr als 20.000 Newsgroups im Internet verfügbar. „Es gibt über 8.000 nach Themen geordnete internationale „Newsgroups“, in denen jeder Internet-Teilnehmer (auf englisch) eigene Diskussionsbeiträge veröffentlichen, auf Beiträge anderer Teilnehmer antworten oder Beiträge kommentieren kann. Hinzu kommen hierzulande rund 500 nationale Newsgroups in deutscher Sprache, und in vielen Regionen sind darüber hinaus lokale Gruppen verfügbar.“[144]

Das System der Newsgroups ist auf verschiedene Netze verteilt. Grundsätzlich kann man drei verschiedene Möglichkeiten, an den Newsgroups teilzunehmen, unterscheiden. Alpar differenziert E-Mail-Verteilerlisten, Listserver und Usenet-Newsgroups[145].

Vor allem der Begriff „Usenet“ wird verschieden gebraucht und führt dadurch oft zu Mißverständnissen und falschen Ansichten über die Newsgroups.

---

[142] Alpar, Kommerzielle Nutzung des Internet, Seite 56 und 57

[143] Wenn man eine Nachricht hinterläßt, spricht man von „die Nachricht posten“.

[144] Ramm, Recherchieren und Publizieren im World Wide Web, Seite 21

[145] Alpar, Kommerzielle Nutzung des Internet, Seite 56 bis 69

Alle drei Möglichkeiten haben eine Gemeinsamkeit, die Kommunikation erfolgt über eine modifizierte Form von E-Mail.

5.3.2 E-Mail-Verteilerlisten und Listserver

Die Funktionsweise von E-Mail-Verteilerlisten ist sehr einfach. Als erstes wird eine bestimmte E-Mail-Adresse als Newsgroup auf einem Server eingerichtet. D.h. es wird ein Account in der Form „newsgroup_name@subdomain.toplevel_domain“ angelegt. Weiterhin wird manuell eine sogenannte Verteilerliste erstellt, in die alle Abonnenten der Newsgroup eingetragen werden müssen. Wenn jemand eine Nachricht posten will, sendet er sie als E-Mail mittels seines E-Mail-Client einfach an die eingerichtete E-Mail-Adresse. Das Serverprogramm enthält eine sogenannte Weiterleitungsfunktion. Alle eingehenden E-Mails werden automatisch an alle Abonnenten versandt. Da diese Möglichkeit auch ohne Server-Software realisierbar ist, könnte sie dem Grunde nach auch zum E-Mail-Dienst gerechnet werden, da sie allein auf den E-Mail-Protokollen aufbaut. So kann auch eine Privatperson seinen E-Mail-Clienten so gestalten, daß er genau diese Weiterleitungsfunktion durchführt. Die Nachteile der E-Mail-Verteilerlisten liegen klar auf der Hand. Zum einen müssen die Verteilerlisten verwaltet werden. Abonnenten müssen manuell aus- und eingetragen werden. Zum anderen sind die Nachrichten „unmoderiert“, d.h. sie werden ohne Inhaltsprüfung an alle Teilnehmer versandt.

Eine Erweiterung dieser Methode stellen die Listserver-Diskussionsgruppen dar. Wie auch die Mailing-Listen, basiert das Listserver-System auf dem Transportmittel E-Mail. Allerdings wird der Dienst durch spezielle Softwarepakete abgewickelt. Im Sinne der Client-Server-Architektur wird der Server durch LISTSERV (= list server) und der Client durch LISTPROC (= list processor) realisiert. Der Unterschied zu normalen Verteilerlisten besteht in der weitestgehenden Automation der An- und Abmeldung von Benutzern, einer Online-Hilfe, einer Kommunikation über mehrere Listserver hinweg sowie einer Abrufmöglichkeit für archivierte Beiträge. „Die Nutzung der Funktion eines Listserver erfolgt durch Kommandos, die in standardisierten E-Mail-Nachrichten an eine spezielle Listserver-E-Mail-Adresse, die in der Regel dem Schema

Listserv@Domain entspricht, verschickt werden."[146] [147] Die Listserver enthalten Listen aller erreichbaren Newsgroups. Diese Liste kann man sich durch spezielle Kommandos anzeigen lassen.[148] Sie enthält dann die Adressen der Newsgroups nebst Kurzbeschreibung. Will man einer Gruppe beitreten, muß man sich an den entsprechenden Listserver (nicht die Adresse der Gruppe) wenden. Wird eine Newsgroup durch einen Listserver nicht verwaltet, reicht er die Anmeldung an den nächsten Listserver weiter.[149]

5.3.3 Usenet Newsgroups (Usenet News, NetNews)

Nach Ramm ist das Usenet die „Menge aller Rechner, die am Austausch von News teilnehmen"[150]. Alpar hingegen sieht das Usenet nur als einen Teil der Newsgroups. Beiden Ansichten kann man folgen, da die E-Mail-Verteilerliste und die Listserver eigentlich E-Mail-Anwendungen sind, die auch mit „normalen" E-Mail-Clienten betrieben werden können. Das Usenet hingegen bietet eine andere Art und Weise des Nachrichtenzugriffs. Auch haben die Beiträge eine andere Form. Ferner ist zu beachten, daß nicht „nicht alle Internet-Rechner an den News teilnehmen und andererseits (z.B. über UUCP, s.u.) auch Rechner News austauschen können, die gar nicht über TCP/IP mit dem Internet verbunden sind [...] [,somit] ist das Usenet weder eine Teilmenge des Internet noch umgekehrt."[151]

Ein grundlegender Unterschied zu den zwei vorgenannten Varianten besteht darin, daß die Nachrichten nicht automatisch zugesandt werden, sondern vom Benutzer - von einem sogenannten News-Server - abgerufen werden müssen. Hierzu benötigt er dann auch ein spezielles Programm, einen Newsreader. Mittels dieses Clienten kann der Benutzer auch Artikel posten. Die News-Server sind untereinander verbunden und gleichen ihren Datenbestand in periodischen Abständen mit ihren „Nachbarn" ab.

---

[146] Alpar, Kommerzielle Nutzung des Internet, Seite 59 (hier auch nähere Informationen zu Listserver-Kommandos etc.)

[147] Eine Übersicht über aktive Listserver-Diskussionsgruppen unter: http://www.tile.net/lists/[06.08.2000].

[148] Eine Übersicht über Kommandos von Listservern bietet Anlage 3.

[149] Für nähere Informationen zu Listserver-Kommandos vgl. Alpar, Kommerzielle Nutzung des Internet, Seite 58.

[150] Ramm, Recherchieren und Publizieren im World Wide Web, Seite 21

Grundlage dafür ist das „Network News Transport Protocol“ (NNTP). So wird gewährleistet, daß jeder Server auf dem aktuellsten Stand ist und eine gepostete Nachricht auf allen News-Servern präsent ist. „Ende 1995 existierten weltweit etwa 12.000 bis 14.000 Newsgroups.“[152] Angesichts dieser Größenordnungen ist es nicht verwunderlich, daß ein Server nicht alle Newsgroups anbieten kann, sondern nur eine eingeschränkte Auswahl. Desweiteren sind viele News-Server nicht öffentlich, d.h. daß nur innerhalb einer Domain auf diesen Server zugegriffen werden kann. Durch diese Vorkehrung wird einer Serverüberlastung vorgebeugt.

Die Newsgroups des Usenet unterliegen einem Klassifizierungssystem. Dieses System ist kein offizieller Standard, sondern hat sich so im Laufe der Jahre herauskristallisiert. Die Newsgroups sind hierarchisch in Haupt- und Subthemen angeordnet. Es existieren auch die Begrifflichkeiten Toplevel-Hierarchie und Sublevel-Hierarchie. Bei den Toplevel-Hierarchien kann man grundsätzlich zwischen themenorientierten und länder- bzw. regionalorientierten Bezeichnungen unterscheiden. Eine Newsgroup-Bezeichnung wird von links nach rechts gelesen, die einzelnen Themen werden durch Punkte voneinander getrennt[153]. Eine Auswahl der Hauptthemen zeigt die nachfolgende Tabelle:

---

[151] ebd., Seite 21

[152] Alpar, Kommerzielle Nutzung des Internet, Seite 66

[153] So würde die Newsgroup „comp.os.ms-windows.apps“ folgendermaßen zu lesen sein: Computer (comp=computer), Betriebssysteme (op=operating system), Microsoft Windows (ms-windows), Programme (apps=applications).

Hauptthema	Inhalt
comp	Computer
alt / misc	Sonstiges (alternative / miscellaneous)
sci	Wissenschaft mit Schwerpunkt Naturwissenschaften (scientific)
soc	Soziales (social)
talk	Diskussion aller Art
news	im Zusammenhang mit Usenet News (neue Gruppen, Newsreader)
rec	Freizeitaktivitäten / Hobbys (recreational)
biz	Wirtschaft (business)
bit	Beiträge aus Listserver-Diskussionslisten (bitnet)
bionet	Biologie
de	deutschsprachige Newsgroups
fido	Diskussionsgruppen des Fidonet (Mailbox-Netz)
maus	Diskussionsgruppen des Maus-Net (Mailbox-Netz)

Tabelle 7: Hauptthemen der Usenet Newsgroups[154]

Wenn jemand eine Nachricht mit einem neuen Subject (Thema) postet, kann ein anderer auf die Nachricht antworten und bezieht sich somit auf das gleiche Thema. Ein Dritter antwortet ebenfalls, und ein Vierter antwortet dem Dritten. Auf diese Weise entsteht eine Baumstruktur von Nachrichten zu einem bestimmten Thema. Diese Baumstruktur wird auch als Thread bezeichnet. Man kann selbst einen neuen Thread beginnen oder auf eine Nachricht antworten und sich dadurch in den betreffenden Thread einschalten.

Ein Newsgroup-Artikel ähnelt sehr stark einer E-Mail, er ist Internet-Standard und besteht aus Header und Body. Allerdings wurden zusätzliche

[154] Vgl. auch: Alpar, Kommerzielle Nutzung des Internet, Seite 68, Tabelle 3.6 Auswahl von Usenet Newsgroups Hauptthemen.

Headerfelder eingefügt. Die wichtigsten Headerfelder zeigt die folgende Tabelle:

Headerfeld	Erläuterung
newsgroup	enthält die Newsgroup(s), an die der Artikel verschickt werden soll
lines	Anzahl der Zeilen, die der Artikel enthält
summary	Kurzbeschreibung des Artikelinhalts
keywords	dient dazu, den Artikel mittels Schlagworte zu kennzeichnen
distribution	begrenzt den Bereich, innerhalb dessen der Artikel veröffentlicht wird (z.B. de, für Deutschland und Frankreich)

Tabelle 8: Zusätzliche E-Mail-Headerfelder eines Usenet Newsgroup Artikels[155]

5.4 Telnet: Nutzung entfernter Ressourcen

Telnet ist einer der ältesten Dienste des Internets und wird dazu verwendet, einen räumlich getrennten Rechner so zu bedienen, als säße man direkt davor[156]. Nach Ramm ist „Telnet [...] kein `Dienst´ an sich, sondern lediglich eine Terminalemulation“[157]. Da aber auf dem Host ein Programm läuft, das auf Telnet-Anfragen wartet und mit einem Client-Programm eine entsprechende Verbindung aufbauen kann, unterscheidet sich Telnet den Grundsätzen nach nicht von anderen Diensten. Telnet ist damit eine einfache Lösung für Systemadministratoren, also Netzwerkbetreuer, die z.B. für Störfälle auch von zu Hause Zugriff auf ihren Server herstellen wollen.

Telnet ist vor allem für Unix-Systeme gedacht. Es erlaubt das betriebssystemeigene Login (Anmelden) eines Benutzers an einem ans Internet angeschlossenen Host-Rechner. Das Protokoll, welches für eine Telnet-Sitzung verwendet wird, heißt „Network Virtual Terminal“ (NVT). Programme, mit denen

---

[155] Vgl. auch: Alpar, Kommerzielle Nutzung des Internet, Seite 68, Tabelle 3.7 Zusätzliche E-Mail Headerfelder eines Usenet Newsgroup Artikels.

[156] Vgl. auch: Alpar, Kommerzielle Nutzung des Internet, Seite 74 – 77.

[157] Ramm, Recherchieren und Publizieren im World Wide Web, Seite 20

man eine Telnetverbindung aufbauen kann, nennt man Telnet-Client. Die Verbindung wird über die IP-Adresse oder die Domain-Adresse aufgebaut. Zusätzlich kann eine TCP-Portnummer angegeben werden. Der Standardport ist 23.

Den Zugriff auf den entfernten Rechner wird als remote-login (rlogin) bezeichnet. Grundsätzlich werden zwei Möglichkeiten eines Telnet-Login unterschieden. Beim persönlichen rlogin ist die Benutzeranzahl des jeweiligen Host-Betriebssystems genau festgelegt. D.h. jeder Benutzer, der ein rlogin durchführt, erhält erst Zugriff zum Rechner, wenn er sich durch einen Benutzernamen (UserID) und ein geheimes Paßwort authentifiziert hat (normal Telnet). Wer solche Zugriffsrechte erhält, entscheidet der Systemadministrator des jeweiligen Host-Rechners. Er kann beliebig viele UserIDs und Paßwörter vergeben und auch jeder Zeit wieder löschen. Die zweite Möglichkeit ist der öffentliche oder anonyme Login (anonymous Telnet). Bei dieser Variante besteht für jedermann die Möglichkeit, einen rlogin durchzuführen.

Nach dem Einwählen erhält man meist eine allgemeine Information über den Host, sein Betriebssystem und eine sogenannte Eingabeaufforderung, wie sie z.B. noch unter DOS oder Unix gebräuchlich ist. Dementsprechend kann man dann auf dem entfernten Rechner Betriebssystembefehle eingeben, Programme starten etc. Sollte es sich um ein anonymous rlogin handeln, wird oft noch eine Information zur rlogin-Prozedur ausgegeben.

Normale Computeranwender, die nicht unmittelbar mit der administrativen Betreuung von Servern betraut sind, werden für Telnet kaum Verwendung finden. Allerdings gibt es nicht nur für die gängigen Unix-Versionen oder ihre Derivate, sondern auch für MS Windows oder vergleichbare Betriebssysteme Telnet-Clients. Wenn man mit einem rlogin auf einen fremden Rechner Zugriff erhält, kann man diese Möglichkeit nur ausnutzen, wenn man auch die Betriebssystembefehle des Hostrechner-Betriebssystems kennt.

5.5 Dateitransfer (FTP)

„Ebenso wie Telnet wird auch FTP benutzt, um Verbindungen zu anderen Rechnern herzustellen. Während Telnet-Verbindungen jedoch zum Aufruf von Programmen dienen, sind FTP-Verbindungen auf das [wechselseitige] Übertra-

gen von Dateien spezialisiert.“[158] [159] FTP steht hierbei für „File Transfer Protocol“ (FTP). Der Anwendungsbereich von FTP ist vielseitig. So besteht zum einen die Möglichkeit, Dateien vom eigenen Rechner auf den FTP-Server zu übertragen (uploaden, upload) oder umgekehrt, Dateien aus dem Netz zu laden (downloaden, download). Ferner bietet das FTP-Protokoll Befehle an, um auf dem entfernten Rechner Operationen durchzuführen wie: Verzeichnisinhalte anzeigen, Verzeichnisse wechseln, Verzeichnisse anlegen oder Dateien löschen.

Programme, die für den Verbindungsaufbau zu einem FTP-Server verwendet werden, nennt man FTP-Client. Ein FTP-Server arbeitet mit zwei TCP-Portnummern. „Die bei FTP verwendete Architektur entspricht dem Client/Serverprinzip und beinhaltet als wesentliches Merkmal die Trennung von Kontroll – und Datenverbindung [...]. Während einer FTP-Sitzung wird die durch den Client eröffnete Kontrollverbindung (Standard: TCP Port 21) zum Austausch von Kommandos genutzt [...]. Wird eine Datenübertragung ausgelöst, so findet diese über die Datenverbindung statt (Standard: TCP Port 20).“

Ähnlich wie bei einer Telnet-Sitzung gibt es zwei Möglichkeiten, eine Verbindung zu einem FTP-Server herzustellen. Auf der einen Seite gibt es die Möglichkeit, sich durch eine bestimmte UserID nebst Paßwort zu authentifizieren (normal FTP). Auf der anderen Seite kann man auch eine anonyme FTP-Sitzung durchführen (anonymous FTP). Es gibt sowohl reine „normal FTP-Server“ als auch reine „anonymous FTP-Server“. Ähnlich wie bei „normal Telnet“ kann ein Zugriff über „normal FTP“ nur erfolgen, wenn der Benutzer durch den Systemadministrator im Hostrechner mit einer UserID und einem Paßwort eingetragen ist. Bei „anonymous FTP“ handelt es sich um öffentlich zugängliche Bereiche auf Servern. Dazu braucht man keine Zugangsberechtigung. Es ist eine ungeschriebene Regel, daß man für die UserID „anonymous“ und als Paßwort die eigene E-Mail-Adresse angibt.

Zu beachten ist, daß es auch die Möglichkeit des FTP per E-Mail gibt. Diese Variante funktioniert allerdings nur, wenn der benutzte E-Mail-Server eine entsprechende Funktion hat. Man spricht dann von einem FTPMailer. Die

---

[158] Ramm, Recherchieren und Publizieren im World Wide Web, Seite 20

[159] Vgl. auch: Alpar, Kommerzielle Nutzung des Internet, Seite 74 – 77.

Funktionsweise ist von FTPMailer zu FTPMailer verschieden. „Den Ablauf und einzelne Kommandos erhält man aber, indem man eine E-Mail mit der Kommandozeile HELP im Body an die E-Mail-Adresse eines FTPMailers sendet (z.B. an ftpmail@info2.rus.uni-stuttgart.de).“[160]

5.6 Suchdienste

5.6.1 Archie

„Archie ist ein Suchdienst zum Lokalisieren von Dateien und Verzeichnissen auf entfernten anonymen FTP-Servern. Archie enthält dazu zwei Datenbestände, die Filenames-Database und die Software-Description- oder Whatis-Database. Während in der Filenames-Database Informationen aus den Inhaltsverzeichnissen von FTP-Servern archiviert sind, enthält die Whatis-Database Namen und Kurzbeschreibungen zu einer Reihe von Softwarepaketen und Dateien.“[161] Somit kann Archie zu einem bestimmten Stichwort die genaue Bezeichnung einer Software liefern und den FTP-Server angeben, von dem die Software heruntergeladen werden kann. Die Informationen in der Whatis-Database werden manuell erstellt, wobei z.B. die Newsgroups und Autoreninformationen hinzugezogen werden. Die File-Database hingegen wird automatisch generiert. In regelmäßigen Abständen werden die FTP-Server abgefragt und die erhaltenen Informationen an den Archie-Server übergeben. Die Informationen über den Dateibestand der FTP-Server werden aufbereitet und in einer speziellen abfragbaren Datenbank bereitgehalten. Auf die Datenbank kann dann mittels eines Archie-Clienten zugegriffen werden. Dabei unterstützen die Archie-Clienten mehrere Suchmodi, welche die nachfolgende Tabelle zeigt:

[160] Alpar, Kommerzielle Nutzung des Internet, Seite 71
[161] Alpar, Kommerzielle Nutzung des Internet, Seite 78

Modus	Erläuterung
exact	zeigt alle Daten, die genau dem Suchbegriff entsprechen
sub	zeigt alle Daten, die den Suchbegriff als Teilzeichenkette enthalten
subcase	zeigt alle Daten, die den Suchbegriff unter Beachtung von Groß - und Kleinschreibung als Teilzeichenkette enthalten
regex	zeigt alle Daten, die den mit Platzhaltern versehenen Suchbegriff als Muster enthalten

Tabelle 9: Suchmodi in Archie

Eine weitere Einengung des Suchbereiches kann durch die Angabe eines bestimmten Domain-Bereichs erfolgen. Zu beachten ist, daß der größte Teil der Archie-Clients nur den Zugriff auf die Filenames-Database ermöglichen. Für die Abfrage der Whatis-Database ist dann oft ein rlogin mittels Telnet oder eine Anfrage mittels E-Mail erforderlich[162].

5.6.2 Gopher

Gopher gilt heute als der Vorläufer des World Wide Web, wobei Gopher durch das WWW zusehends verdrängt wird. Der Name Gopher kann auf zwei mögliche Ursprünge zurückgeführt werden. Zum einen könnte der Ausdruck für „Go for it !“ stehen, mit welchem amerikanische Botenjungen aufgefordert wurden, bestimmte Sachen oder Informationen zu besorgen. Zum anderen könnte es auch von der amerikanischen Bezeichnung für Beutelratte oder Erdhörnchen abgeleitet werden. Das Tier Gopher ist das Maskottchen der Universität Minnesota, an der Gopher als campusweites Informationssystem 1991 entwikkelt wurde. Die Aufgabe von Gopher ist es, große Informationsbestände leichter durchsuchbar zu machen und sie unter einer einheitlichen Schnittstelle zur Verfügung zu stellen. Hierzu werden die Inhalte der weltweiten Gopher-Server miteinander verlinkt, so daß sich der Benutzer über sogenannte „Hypermenüs“ durch den Gopherspace bewegen kann.

[162] Näheres siehe: Alpar, Kommerzielle Nutzung des Internet, Seite 80 und 81.

Gopher ist eine menübasierte Bedienoberfläche zum Auffinden von Informationen, aber auch zum Nutzen anderer Internet-Dienste wie FTP oder Telnet. Einem Eintrag in einem Gopher-Menü ist nicht anzusehen, wo sich die damit verbundenen Dateien oder Programme befinden. Anwender mit text- und tastaturorientierten Rechnern können aus den Menüs, die das Gophersystem am Bildschirm anzeigt, mit Buchstaben- oder Zifferntasten Einträge auswählen. Bei grafischen Benutzeroberflächen sind die Menüs mit der Maus anklickbar. In dieser Hinsicht gleicht Gopher dem World Wide Web, denn auch bei diesem Dienst muß man keine Insider-Befehle kennen, um im Informationsbestand zu navigieren. Gopher bietet eine Suche an, mit deren Hilfe die Gopher-Server nach Stichworten durchsucht werden können.

Der Nachteil von Gopher gegenüber dem WWW ist, daß es keine Standards wie HTML gibt. Es gibt lediglich die Gopher-Menüs und die damit verknüpften Dateiaufrufe oder Befehle. Ein guter Gopher-Client kann zwar diverse Dateiformate anzeigen, doch es gibt keine Mittel zur Gestaltung eigener Bildschirmseiten um dadurch eigenständige Präsentationen von Information zu schaffen.

5.6.3 WAIS

WAIS ist die Abkürzung für „Wide Area Information Server“ und beschreibt eine sogenannte Volltextsuche in weltweit verteilten Datenbanken. WAIS wurde ab 1989 in einem Gemeinschaftsprojekt von Thinking Machines Corporation, Apple Computer und Dow Jones & Co. entwickelt und im Frühjahr 1991 zum Internetstandard erklärt. 1992 wurde die Aufsicht über WAIS an eine unabhängige Organisation – WAIS Inc. – übergeben. „Für die Weiterentwicklung von WAIS im frei zugänglichen Bereich (Public Domain) zeichnet seit 1992 die von der NSF gegründete CNIDR (Clearinghouse for Networked Information Discovery and Retrieval) verantwortlich. Zur Unterscheidung wird WAIS in der Public Domain unter dem Namen freeWAIS geführt.

Die Datenbanken enthalten Textdokumente in den unterschiedlichsten Formaten, zunehmend aber auch Ton-, Bild- und Videodateien. Die Datenbanken decken den gesamten Informationsbedarf unserer heutigen Gesellschaft ab.

So finden sich u.a. Dokumente aus den Bereichen Wissenschaft, Politik, Gesellschaft, Literatur oder Informatik. Volltextsuche heißt, daß nicht nach Stichwörtern oder nur in Kurzbeschreibungen oder in Überschriften gesucht wird, sondern in einem kompletten Text. Das Durchsuchen der Datenbanken erfolgt mit einem WAIS-Clienten. Das Suchergebnis wird in einem sogenannten Ranking (Rangfolge) dargestellt. D.h. daß ein Dokument um so weiter zur Spitze der Trefferliste vorrückt, je häufiger der Suchbegriff in seinem Inhalt gefunden wurde. Das Dokument an der Spitze der Ranking-Liste erhält den Wert 1.000. Grundsätzlich unterstützt ein Server auch Anfragen, die mehrere Suchbegriffe enthalten. Diese Suchbegriffe werden dann mit dem boolschen Operator „und“ verknüpft. Andere Verknüpfungen sind grundsätzlich nicht vorgesehen, hängen aber von den jeweiligen Servereinstellungen ab. Die fehlende Abfragesprache stellt somit einen großen Nachteil von WAIS in Bezug auf andere Recherchemöglichkeiten dar. Von Vorteil ist die nicht bedeutungslose Schnelligkeit, mit der eine WAIS-Abfrage durchgeführt wird.

Wenn ein Benutzer eine WAIS-Abfrage machen will, muß er zuerst die Datenbanken wählen, die bei der Suche einbezogen werden sollen. Als Hilfsmittel existiert eine Liste, in der alle Datenbanken aufgeführt werden (Directory-of-Servers)[163]. Als nächstes muß eine Suchanfrage formuliert werden. Dann wird die Suche gestartet, nach Abschluß wird die Ranking-Liste angezeigt. Der Benutzer kann nun Dokumente auswählen, welche dann durch den Clienten heruntergeladen und angezeigt werden.

Die WAIS-Abfrage ist eine mächtige Dienstleistung, gerät aber immer mehr ins Hintertreffen. Zur Zeit erfolgt eine Verlagerung der Abfragen vom WAIS-Clienten, hin zu WWW-Seiten, die ein Abfrageformular bereitstellen. Eine weitere Möglichkeit besteht in der Nutzung eines öffentlichen WAIS-Clienten über Telnet[164].

---

[163] Die Datei Directory-of-Servers ist mittels anonymous FTP unter ftp.wais.com/pub/directory-of-servers/wais-sources.tar.Z downloadbar.

[164] Für nähere Informationen zur Nutzung einer Telnet-WAIS-Abfrage vgl.: Alpar, Kommerzielle Nutzung des Internet, Seite 87 und 88.

5.7 Zeitgleiche Kommunikation

5.7.1 Internet Relay Chat (IRC)

„IRC wurde im Jahre 1988 ursprünglich als Ersatz für das UNIX-Programm TALK konzipiert, mittels dessen zwei Benutzer zeitgleich miteinander in Kontakt treten können. IRC ist heute ein Mehrbenutzerdialog-System, in dem sich Menschen [virtuell] treffen, um miteinander zu kommunizieren.“[165] Mit Hilfe eines IRC-Clienten kann man Zugang zu einem IRC-Server erhalten[166]. Hier wählt der Benutzer einen sogenannten „Nickname“ (richtiger Name oder Pseudonym) aus. Danach bestimmt er den „Channel“, in dem er chatten möchte oder eröffnet einen neuen Channel. Dann kann er aktiv am Gespräch teilnehmen. Der IRC-Client läßt sich durch verschiedene Befehle steuern. Hierdurch sind verschiedene Kommunikationsmöglichkeiten mit anderen Teilnehmern möglich. Die bekanntesten Varianten sind das Anflüstern[167] und das Separée[168].

Derjenige, der einen Channel eröffnet hat, wird als sogenannter Operator bezeichnet. Der Operator ist an einem @-Zeichen vor dem Nicknamen erkennbar und besitzt erweiterte Rechte, sogenannte Operatorrechte. Er hat die Aufsicht über seinen Channel und kann so z.B. auch Benutzer, die den Chat gröblichst stören, aus dem Channel ausschließen. Den Begriff „chatten“ kann man mit Tratschen oder Quatschen übersetzen.

IRC bietet nicht nur die Möglichkeit, miteinander zu kommunizieren. Über eine Zusatzfunktion ist es möglich, einem anderen Benutzer eine Datei zu senden oder von einem anderen Benutzer eine Datei zu erhalten. Einige Besonderheiten sind bei der Benutzung des IRC zu beachten. Zum einen werden oft kryptische Abkürzungen für vielverwendete geläufige Wortgruppen oder ganze Sätze verwendet.

---

[165] Alpar, Kommerzielle Nutzung des Internet, Seite 89

[166] Weitere Informationen zu IRC findet man unter: ftp://rtfm.mit.edu/pub/usenet/alt.irc/ oder ftp://cs.ftp.bu.edu/irc/support/ und in der Usenet Newsgroup alt.irc.questions.

[167] Beim Anflüstern wird einem anderen Benutzer eine Nachricht zugesandt, die nur er alleine auf seinem Bildschirm sehen kann.

[168] Jeder Benutzer kann ein Separée eröffnen, in das er einen anderen Benutzer einlädt. Nimmt der eingeladene Benutzer diese Einladung an, d.h. er wechselt in das Separée, können sich die beiden Chatter nun ungestört unterhalten.

Zum anderen besteht die Möglichkeit, Emotionen und Gefühle durch sogenannte Smiles auszudrücken. Im Chat wird von diesen zwei Möglichkeiten ausreichend Gebrauch gemacht, daher ist es für jeden Chatter zwingend erforderlich, die grundlegenden Abkürzungen und Smiles zu beherrschen[169]. Es ist zu beachten, daß diese Smiles und Abkürzungen auch bei E-Mails oder den Newsgroups verwendet werden.

IRC ist einer der Internet-Dienste, der schnell hohe Kosten verursachen kann. Denn während der ganzen Teilnahmedauer muß man online sein, und viele merken beim Chatten nicht, wie die Zeit vergeht. Es gibt nur wenige, die eine ganze Nacht lang im WWW surfen, aber viele, die eine ganze Nacht lang chatten. Eine Vielzahl der hochgradig Internetsüchtigen, sind vor allem in den Chat-Bereichen zu finden.

5.7.2 Internet Phone (Iphone)

Iphone ermöglicht das Telefonieren über das Internet[170] [171]. Die Technik, die dieser Möglichkeit zugrunde liegt, heiß „Voice over IP“ (VoIP). Voraussetzung hierfür ist natürlich die Fähigkeit des eigenen Rechners, Töne aufzunehmen und wiederzugeben. Die Ausstattung mit einer Soundkarte ist daher zwingend erforderlich. Grundsätzlich funktioniert Iphone nach dem gleichen Prinzip wie IRC. D.h. der Benutzer loggt sich mit einem Iphone-Clienten in einen Iphone-Server ein. Dort halten sich weitere Benutzer auf, die man sich anzeigen lassen kann. Dann kann man sich einen Benutzer auswählen und mit diesem dann Gespräche führen.

Das Besondere ist, daß die Gespräche nicht zu den Preisen der Telekom geführt werden, da sie ja nicht über das Telefonnetz der Telekom im herkömmlichen Sinne vermittelt werden, sondern zu den jeweiligen Konditionen des eigenen Zugangsanbieters.

Berechnet der Provider z.B. 2,5 Pfennige/Minute für Online-Zeiten, bezahlt man natürlich auch den gleichen Preis für Iphone. Damit ist z.B. kostengünsti-

---

[169] Einen Überblick über geläufige Abkürzungen und Smiles bietet Anlage 4.
[170] Vgl. auch: Kuri, Sprache im Päckchen, Seite 220.
[171] Vgl. auch: Kossel, Netzgespräche, Seite 230.

ges Telefonieren ins Ausland möglich (vorausgesetzt natürlich, daß der Gesprächspartner auch online und in einen Iphone-Server eingeloggt ist[172]).

Iphone ist zwar kostengünstig, belastet aber den Netzverkehr sehr stark, da die Sprache digitalisiert werden muß. Zur Zeit reichen die gebräuchlichen Übertragungsstandards noch nicht aus, eine Sprachqualität wie über Telefonnetz zu erreichen. So kann es durchaus vorkommen, daß das Gespräch kurz stockt oder es zu anderen Störungen kommt.

5.7.3 Worlds Chat (Wchat)

Wchat[173] ist eine modifizierte Form des IRC. Während im IRC nur die reine Kommunikation möglich ist und man von einem virtuellen Chatraum spricht, werden im Wchat der komplette Chat und seine Channel visualisiert. Das bedeutet, daß sich der Benutzer wie in einem sogenannten Adventure-Spiel durch eine vorgegebene Räumlichkeit bewegt. Diese Räumlichkeit stellt in ihrer Gesamtheit den Wchat-Server dar. Einzelne Räume oder Areale verdeutlichen die einzelnen Channel. Der Benutzer wählt nach dem Login eine Figur (Avatar) aus, die seinen Nicknamen erhält. Mittels dieser Figur kann er sich durch die virtuelle Realität bewegen. In den einzelnen Räumen kann er sich mit den dort ebenfalls anwesenden Personen unterhalten. Die Gespräche werden in einem separaten Fenster angezeigt. Das Wechseln in einen anderen Raum des Wchat ist somit mit dem Wechseln eines Channel im IRC vergleichbar. Die Kommunikation zwischen den einzelnen Teilnehmern erfolgt über Tastatureingabe.

Die Technik, die sich hinter dem Wchat verbirgt, ist eine Erweiterung der „Virtual Reality Modeling Language“ (VRML), nämlich VRML+. Hierbei handelt es sich um eine standardisierte Beschreibungssprache für dreidimensionale Modelle. VRML+ ermöglicht hierbei die Visualisierung mehrerer Benutzer.

„Der VRML+ World Server liefert dazu dem Client die notwendigen Informationen über die [virtuelle] Welt (Aussehen und mögliche Aktionen), die Posi-

---

[172] Das sind zugleich auch die entscheidenden Nachteile, die VoIP zur Zeit noch hat, d.h. daß beide Teilnehmer online sein müssen, also für beide Teilnehmer auch Gebühren anfallen, daß beide Teilnehmer wissen müssen, auf welchem Server sich der gewünschte Gesprächspartner befindet (ein Anklingeln des gewünschten Gesprächspartners ist nicht mgl.), und daß die hergestellten Verbindungen noch sehr schlecht sind.

[173] Nähere Informationen unter: http://www.worlds.com[06.08.2000].

tion des eigenen und anderer Avatare und verarbeitet die durch den Client initiierten Aktionen wie Bewegen und Kommunizieren.“[174]

5.7.4 Multiple User Dungeon (MUD) und Multiplayer-Online-Games (MOG)

„MUD, dessen Abkürzung auch für Multiple User Dimension oder Multiple User Dialog stehen kann, ist ein Dienst mittels dessen sich Benutzer in eine auf dem MUD-Server existierende Fantasiespielwelt begeben können. Innerhalb dieser [virtuellen] Welt erhält jeder Spieler die Kontrolle über einen virtuellen Charakter, mittels dessen er sich umherbewegen, gegen Unholde kämpfen, Rätsel lösen sowie mit anderen kommunizieren kann. In der Regel geht es dabei um das Lösen von Rätseln.“[175]

Die Varianten, in denen MUD existiert, sind sehr verschieden. Es wird in Kategorien aufgeteilt. Somit unterscheiden sich auch die dargestellten virtuellen Welten und die Formen, wie in ihnen agiert wird. Man unterscheidet zwei Grundkategorien: TinyMUD oder auch TeenyMUD und LPMUD, DikuMUD oder auch AberMUD.

Dem Wesen nach lehnt sich MUD an ein Fantasyspiel namens „Dungeons and Dragons“ an, welches ursprünglich auf Papier gespielt wurde. „Dabei gestaltet ein Spieler einen bestimmten Schauplatz, den er mit Ungeheuern bevölkert und mit Rätselaufgaben spickt. Die anderen Spieler müssen sich dann einen Weg durch diese Phantasiewelt bahnen. Das ganze Spiel existiert nur auf dem Papier und in den Köpfen der Spieler.“[176] Crowther (ein Mitarbeiter bei BBN und Beteiligter im IMP-Projekt) setzte dieses Spiel in ein Computerprogramm um und nannte es „Adventure“. Durch Woods wurde Adventure verbessert, erweitert und erstmals auf dem Rechner der KI-Abteilung von Stanford installiert. Dort konnte man sich über das Netzwerk einloggen und mitspielen.

Ob es sinnvoll ist, den MUD als eigenständigen Internet-Dienst zu klassifizieren, ist fragwürdig. Es handelt sich vornehmlich um ein sogenanntes Multiuser-Spiel, bei dem mehrere Spieler auf einem Server miteinander spielen.

---

[174] Alpar, Kommerzielle Nutzung des Internet, Seite 93
[175] ebd., Seite 94
[176] Hafner/Lyon, Arpa Kadabra oder die Geschichte des Internet, Seite 244

Im Laufe der Zeit haben sich noch weitere Netzwerkspiele entwickelt[177]. Hier etablieren sich in der letzten Zeit vor allem sogenannte 3D-Shooter-Games. Bei diesen 3D-Shootern, zu denen z.B. Quake III Arena oder Half-Life zählen, ist es erklärtes Ziel, einen Mitspieler, der sich ebenfalls in der virtuellen Welt befindet, zu töten[178]. Jedes einzelne Online-Spiel als eigenständigen Dienst zu qualifizieren, würde der Übersichtlichkeit und der notwendigen abstrakten Gliederung abträglich sein. Demnach lassen sich alle Netzwerkspiele unter dem einheitlichen Begriff Multiplayer-Online-Games (MOG) zusammenfassen. Somit ist MOG der Überbegriff für alle im Internet existenten Spiele mit mindestens zwei Benutzern.

5.8 World Wide Web

5.8.1 Allgemeines

Das World Wide Web (WWW) ist der jüngste Dienst des Internets. Das Web zeichnet sich dadurch aus, daß es auch ungeübteren Anwendern erlaubt, sich im globalen Informationsangebot zu bewegen. Das Konzept des WWW wurde am Kernforschungsinstitut CERN in der Schweiz (Genf) unter der Leitung von Tim Berners-Lee entwickelt. Durch das WWW wollte Berners-Lee eine elektronische Publikationsplattform für Forscher schaffen, die es allen ermöglichen sollte, auf Forschungsergebnisse zuzugreifen. Es ging darum, wissenschaftliche Dokumente online sichtbar zu machen, wobei einfache Textformatierung und das Einbinden von Grafik möglich sein sollte. Ganz entscheidend war aber auch die Idee, Hypertextfunktionalität einzubauen, so daß Dokumente Verweise auf beliebige andere Dokumente enthalten konnten - auch, wenn diese auf ganz anderen Internet-Servern liegen.

Dies war notwendig, da die Mitarbeiter des CERN an vielen unterschiedlichen Projekten beteiligt waren, die zudem über die ganze Welt verteilt waren. Vorerst sollte das Projekt nur im CERN realisiert werden. „Die anfänglichen Arbeiten im Jahre 1989 zielten auf die Definition eines neuen Kommunikationsprotokolls, den Aufbau eines Testservers und die Erstellung einer Programmbi-

---

[177] Vgl. auch: Kuri / Wiedenhoff / Gieselmann, Virtuelle Zockerrunden, c´t 2/00, Seite 100 ff.
[178] Für 3D-Shooter gibt es auch die Bezeichnung „First-Person-Shooter“.

bliothek (wwwlib) ab.“[179] Nach erfolgreichem Abschluß der Testphase wurde die Programmbibliothek 1992 der Internet-Community als Public Domain übergeben. Im September 1992 waren weltweit ca. 20 WWW-Server im Einsatz. „Im Juni 1993 schätzte man 130 WWW-Server, ein Jahr später waren es fast 1.300. Im Dezember 1994 zählt der `Web Wanderer´ [...] bereits 11.576 WWW-Server.“[180] In der zweiten Jahreshälfte 1993 brachten einflußreiche Blätter wie die New York Times erste Artikel über den neuen Internet-Dienst. Hunderttausende Menschen mit Internet-Zugang und Zugang zu Servern begannen, HTML fürs WWW zu schreiben, Wissenschaftliches - aber auch Persönliches, Abstruses, Verrücktes.

Bill Gates beispielsweise, Chef des mächtigen Softwarekonzerns Microsoft, nahm die Entwicklung des Internets, das es durch das WWW erfuhr, nicht ernst. Auch traditionelle Online-Dienstanbieter wie CompuServe oder die Telekom schotteten sich zunächst gegen das „Chaos Internet“ ab. Die Lawine war jedoch nicht mehr aufzuhalten. Das Internet wurde so mächtig, daß die anfänglichen Gegner später, als der Boom bereits in vollem Gange war und Anwender entsprechende Software und Internet-Zugänge verlangten, Hals über Kopf den Kurs wechselten und fieberhaft in das neue Medium investierten. Heute sind Internet-Provider in erster Linie Online-Dienste. Microsoft beschäftigt Heerscharen von Entwicklern, die nichts anderes im Sinn haben, als das Versäumte nachzuholen, um auch im Internet-Bereich zum Softwareanbieter mit dem größten Umsatz zu werden.

Die Anzahl von Technologien und Softwarelösungen im WWW-Bereich ist heute kaum noch überschaubar. Doch je bunter und unübersichtlicher der Markt, desto wichtiger werden allgemein anerkannte Standards wie HTML und andere Sprachen, die vom W3-Konsortium normiert werden. Denn letztendlich sind die Daten das entscheidende, nicht die Software. Immer mehr Endanwender und Entscheidungsträger beginnen, die Probleme zu begreifen. Und dementsprechend wächst der Druck auf Softwarehersteller, sich an den Standards zu orientieren. Das gilt für einfache Dokumentenformate wie HTML, genauso wie etwa für Ansätze zu elektronischem Business.

---

[179] Alpar, Kommerzielle Nutzung des Internet, Seite 95

[180] Ramm, Recherchieren und Publizieren im World Wide Web, Seite 9

Seit der Freigabe der wwwlib sind fast 10 Jahre vergangen, in denen das Web zu einem der beliebtesten Internet-Dienste geworden ist. Warum es so erfolgreich geworden ist, soll noch an anderer Stelle geklärt werden. Grundsätzlich beruht das Konzept WWW auf vier tragenden Säulen. Diese Säulen werden durch HTTP, HTML, URL/URI - und die dadurch mögliche Integration anderer Dienste - gebildet. Was es mit den einzelnen Komponenten auf sich hat, wird nachfolgend erläutert.

5.8.2 HTML (Hypertext Markup Language)

Das WWW besteht aus sogenannten WWW-Seiten. Diese WWW-Seiten bezeichnet man auch als Webseiten oder Websites. Grundsätzlich werden sie durch die Dokumentbeschreibungssprache „Hypertext Markup Language“ (HTML) umschrieben. „Bei HTML [...] handelt es sich um eine Weiterentwicklung der in der ISO-Norm 8779:1986 festgeschriebenen Sprache SGML (Structured Generalized Markup Language).“[181] Dieser Standard wurde 1988 von Charles F. Goldfarb entwickelt.

HTML ist keine Programmiersprache wie z.B. C, C++ oder Turbo PASCAL, da ihr die dafür notwendigen Kontrollstrukturen (Schleifen, Alternativen etc.) fehlen. Vielmehr umschreibt HTML ein Dokument, „sagt“ also dem Browser, an welcher Stelle der Seite z.B. ein Textabschnitt steht, welche Ausmaße er hat und wie er formatiert ist. Dieses Umschreiben geschieht mit sogenannten Markup-Tags. Hierbei handelt es sich um Befehle, die ein bestimmtes Element des Dokuments einschließen und das Dokument dadurch strukturieren und formatieren.

Das Besondere an HTML ist, daß die Webseiten im ASCII-Textformat erstellt werden und so auch vom Browser empfangen werden. Demnach kann zum Schreiben einer HTML-Seite jeder beliebige Texteditor verwendet werden. Der Browser interpretiert dann die Tags und stellt die Webseite dar. Früher wurden Webseiten ausschließlich in HTML geschrieben, mittlerweile gibt es viele Ergänzungen zu HTML. Die wichtigsten sind JavaScript, Java, XML/XSL, VRML, Flash, CGI etc.[182]

---

[181] Steyer, HTML 4, Seite 27

[182] Für weiterführende Informationen vgl. u.a.: Steyer, HTML 4, Seite 33 ff.

HTML ist Hypertext. Unter Hypertext versteht man eine Erweiterung der Eigenschaften eines normalen Textes. D.h. in einem Hypertext sind bestimmte Elemente (z.B. Text oder ein Bild) aktiv (hot). Wenn man solch ein Element mit der Maus anklickt, wird ein anderes Dokument geöffnet, eine bestimmte Aktion ausgeführt oder der Browser springt im gleichen Dokument an eine andere Stelle. Diese aktiven Elemente nennt man Links. Webseiten können beliebig miteinander verlinkt werden. Die Seiten, die sich hinter einem Link verbergen, müssen dabei nicht auf dem gleichen Rechner abgespeichert sein, wie die Seite, die den Link enthält. Da sich ein Benutzer auf die Art und Weise sehr schnell durch das WWW bewegen kann, spricht man auch umgangssprachlich vom: „im Web surfen“. Da die Seiten weltweit miteinander verlinkt sind, wurde für das Projekt auch der Name World Wide Web gewählt. Fälschlicher Weise sprechen Anfänger, wenn sie eigentlich das Internet meinen, oft vom WWW. Das WWW bildet weiterhin nur einen Teil des Internets.

5.8.3 HTTP (Hypertext Transfer Protocol)

Das WWW benutzt das „Hypertext Transfer Protocol“ (HTTP)[183]. Dieses Protokoll ähnelt sehr stark dem Gopher-Protokoll. Daher ist auch nachvollziehbar, daß das WWW zunehmend Gopher verdrängt. Mittels HTTP werden Browser-Anfragen an WWW-Server gestellt und Webseiten vom Server an den Clienten übertragen. Wie die Protokolle der anderen Dienste, setzt HTTP auch auf TCP/IP auf. Die Browser benutzen als Standard den TCP Port 80. Ab HTTP 1.0 wird die Verhandlung von Datentypen zwischen Browser und Server unterstützt. Dazu wurden dem Protokoll MIME-Typ-Informationen hinzugefügt. Der Server sendet zusätzlich zu den einzelnen Elementen einer Webseite diese Informationen zum Browser. Mit Hilfe dieser Angaben kann der Browser dann das entsprechende Element darstellen oder reicht sie an eine andere Anwendung weiter. Die nachfolgende Tabelle zeigt schematisch den Ablauf einer HTTP-Sitzung:

[183] Für die Ermittlung einer Web-Adresse vgl. auch: Hartung, Internet, dp-special April 1998, Seite 2 – 15.

Schritt	Funktion
Verbindungsaufbau	Der WWW-Client stellt eine TCP/IP-Verbindung zum Server her
Anfrage (Request)	Der Client sendet seine Anfrage über die hergestellte Verbindung. Dies kann entweder die Aufforderung zur Übermittlung z.B. eines bestimmten Dokumentes sein (GET-Request), oder der Client überträgt mittels der Requestmethoden POST oder PUT selbst Daten zum Server. Des weiteren werden hier die MIME-Typen verhandelt, die sowohl Server als auch Browser verarbeiten können.
Antwort (Response)	Hier reagiert der Server auf die Anfrage, sendet also z.B. das angeforderte Dokument. Mittels eines Statuscodes teilt er mit, ob er die Anfrage bearbeiten konnte oder ob Fehler aufgetreten sind.
Verbindungsabbau	Ist die Übertragung von Anfrage und Antwort abgeschlossen, wird die Verbindung wieder geschlossen.

Tabelle 10: Ablauf einer HTTP-Operation[184]

Die Tabelle veranschaulicht gut, daß eine Verbindung zu einem WWW-Server nicht dauerhaft ist, sondern nur so lange aufrechterhalten wird, bis ein angefordertes Dokument beim Clienten eingetroffen ist. Hierdurch werden vor allem Netzwerkressourcen geschont.

[184] Alpar, Kommerzielle Nutzung des Internet, Seite 98, Tabelle 3.13: Ablauf einer HTTP-Operation

5.8.4 Uniform Resource Locator (URL), - Identifier (URI) und – Names (URN)

Die URL[185] stellt eine einheitliche Adressierungsform für die verschiedenen Dienste des Internets zur Verfügung. Die Art bestimmt sich dabei jeweils nach dem entsprechenden Internet-Dienst, dem die Ressource zugeordnet ist. So wird dem WWW eine Website, dem FTP eine Datei, WAIS eine Datenbank und dem Usenet eine News zugeordnet. Durch die URL kann dann das Objekt im Netz eindeutig angesprochen werden.

Alle Dienste, die bisher behandelt wurden, unterscheiden sich in wesentlichen Punkten. Sie haben verschiedene Protokolle und benötigen daher für die Nutzung der entsprechenden Dienstleistung jeweils einen eigenen Clienten. So kann ein Benutzer beispielsweise eine E-Mail nicht mit einem WAIS-Clienten empfangen oder verschicken. Durch die URL werden alle Dienste in das WWW integriert, d.h. daß man mit einem Browser alle anderen Protokolle und Datentypen des Internets (z.B.: FTP oder Gopher) nutzen kann. In diesem Zusammenhang spricht man von einer Integration der „klassischen“ Internet-Dienste in das WWW. Der Browser wird durch die sogenannten „Helper Applications“ dazu befähigt, auch andere Dienste des Internets zu nutzen. Daher ist es stark vom Hersteller des Browsers abhängig, also von der Art und Anzahl der „Helper Applications“, welche Dienste der Browser neben dem WWW zusätzlich unterstützt.[186]

Hinter jedem externen Link einer Webseite verbirgt sich letzten Endes ein Verweis auf ein Objekt, was sich außerhalb des eigenen Rechners befindet. Diese Verweise sind URL und sprechen somit verschiedene Ressourcen an. Demnach kann sich hinter einem Link z.B. eine E-Mail-Adresse oder eine downloadbare Datei (FTP) verbergen. Den grundlegenden Aufbau einer URL zeigt die nachfolgende Abbildung:

---

[185] „Uniform Resource Locator“ (URL), dt.: Einheitliche Ressourcenidentifikation

[186] Vgl. auch: Alpar, Kommerzielle Nutzung des Internet, Seite 99, Abb. 3.26: Integration „klassischer“ Internetdienste in das WWW.

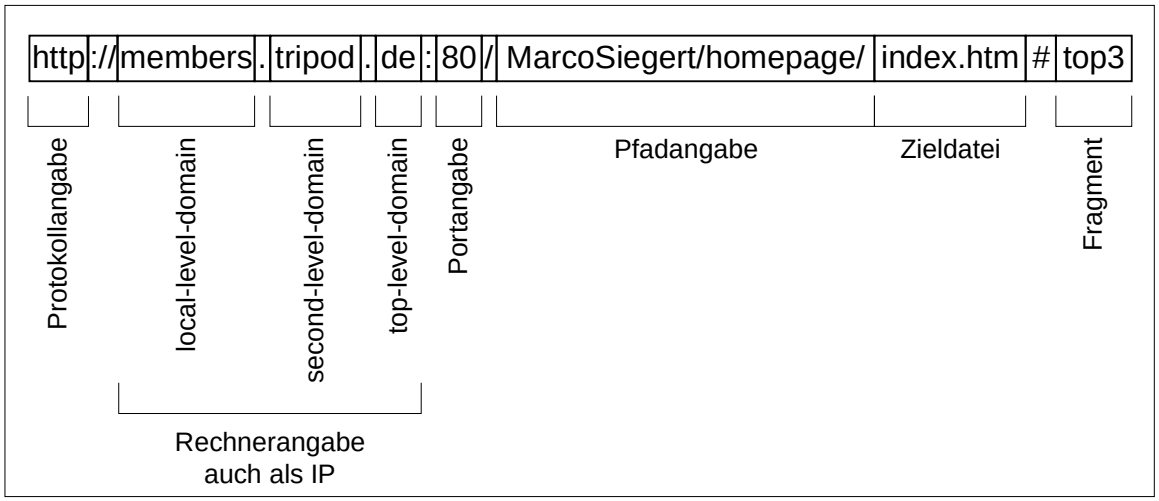

Abbildung 6: Der Uniform Resource Locator (URL)

Grundsätzlich ist die IP-Adresse oder die Domain-Adresse, nebst Angabe der TCP-Portnummer, Bestandteil der URL. Ergänzt wird diese Adressenangabe durch die Protokollangabe, mit der die Ressource angesprochen werden soll. Welche Angaben für die verschiedenen Dienste notwendig sind, zeigt die nachfolgende Tabelle:

Dienst	Protokoll	Erläuterung
FTP	ftp ftps file	• Verweis auf Daten von einem FTP-Server • es wird kein Datentyp übermittelt, aber manche Browser versuchen anhand der Daten oder des Dateinamens zu erkennen, wie die Daten zu behandeln sind • „ftps“ ist die sichere Variante für Netscape-Betrieb • Anwendung für anonymous FTP-Server: ftp://rechner/pfad/dateiname • wenn nur ftp://rechner/pfad verwendet wird, zeigt der Browser den Inhalt des genannten Verzeichnisses an • für nichtöffentliche FTP-Server können Benutzername und Paßwort mit angegeben werden: ftp://user:password@rechner
Gopher	gopher	• Zugang zu einem Gopher-Server (Vorgänger des WWW): • gopher://rechner • gopher://rechner/ressourcenname

WWW	http https	• Verweis auf Daten von einem WWW-Server • der Datentyp wird den Daten voran übermittelt • „https“ ist ein spezielles Protokoll für die verschlüsselte Datenübertragung zwischen Client und Server • Anwendung: http://rechner/pfad/dateiname#sprungziel • wenn nur http://rechner/pfad angegeben wird, wird eine serverseitig voreingestellte Seite (oft index.htm) angezeigt • „https“ wird genau wie „http“ verwendet
E-Mail	mailto	• automatisches Absenden einer E-Mail an die angegebene Adresse • funktioniert nur, wenn in der Browser-Konfiguration ein SMTP-Server angegeben ist, bei dem der Browser die Mail einliefert • Anwendung: mailto:benutzername@rechner
Usenet	news snews nntp	• Verweis auf einen bestimmten News-Artikel oder eine ganze Newsgroup • nicht von allen Browsern unterstützt • „snews“ ermöglicht die verschlüsselte Übertragung der News • um einen bestimmten Artikel oder alle Artikel einer Gruppe anzuzeigen (Verbindung wird zum lokal beim Browser eingestellten News-Server hergestellt): • news:gruppenname • news:artikelkennung • Verbindung mit Angabe des News-Servers, auf dem die Artikel / Gruppen abzuholen sind (muß öffentlich zugänglich sein): • news://rechner/gruppenname • news://rechner/artikelkennung
Telnet	telnet	• der Browser soll eine Telnetverbindung zum angegebenen Rechner öffnen • Verbindung wird über eine „Helper Application“ hergestellt • Anwendung: telnet://rechner
WAIS	wais	• Zugang zu einem WAIS-Server, nur wenig unterstützt • Anwendung: wais://rechner

Tabelle 11: URL-Aufbau der wichtigsten Dienste des Internets[187]

Die Bedeutung der URL für die Funktionsfähigkeit des WWW ist unbestritten. Dennoch bringt diese Form der Adressierung auch den Nachteil mit sich, daß eine URL statisch auf eine Ressource verweist. Da das Internet aber ei-

[187] Ramm, Recherchieren und Publizieren im Internet, Seite 318, Anhang D.3: Im URL zulässige Protokolle

nem ständigen Wandel unterzogen ist, kann es durchaus vorkommen, daß eine URL in die Leere führt. So kann ein Link weiterhin auf eine E-Mail-Adresse verweisen, obwohl der dazugehörige Account bereits gelöscht wurde. Es gibt Schätzungen, daß hinter 15 bis 20 % der WWW-Links keine Ressourcen mehr existieren.

Ein weiterer Nachteil ist, daß es bei besonders oft abgefragten Dokumenten zu einer Überlastung des dokumentführenden Servers kommen kann, da alle Verweise eben auf diesen Server gerichtet sind. Das URN/URI-Konzept versucht diese Mängel dadurch auszugleichen, daß nicht die physische Lage des Objektes beschrieben wird, sondern das Objekt selbst. Damit ist die URN/URI nicht mehr orts- , sondern namenbezogen. So kann man ein bestimmtes Dokument durch Eingabe des Namens ermitteln. Diese neue Adressierungsform erfordert aber die Verwaltung bestimmter Dokumente in Datenbanken (zentrales URN-Verzeichnis) und die automatisierte Verteilung der ausgewählten Dokumente auf mehrere Server. Ein Browser müßte demnach seine Anfrage erst einmal an einen URN-Server stellen und dieser leitet ihn dann auf einen der vielen dokumentführenden Server weiter. Das Besondere am URN-Konzept ist, daß es nur für stark frequentierte Webseiten benutzt werden soll, so daß grundsätzlich URL- und URN-Konzept nebeneinander existieren können.

5.8.5 WWW-Gateways und WWW-Formulare

„Betrachtet man das Spektrum der verschiedenen Dienste, so fällt auf, daß z.B. für IRC keine direkte Schnittstelle vorgesehen ist. Weiterhin ist es nicht möglich, direkt auf lokale Informationsressourcen, wie z.B. ORACLE-Datenbanken, zuzugreifen. Das liegt daran, daß diese Informationen nicht wie es sonst im WWW üblich als statische Files vorliegen. Um den vollen Nutzen des WWW, gerade auch in kommerzieller Hinsicht, zu realisieren, muß aber auch die Integration solcher Informationsressourcen gewährleistet sein.“[188] Gateways und Formulare bieten eine Möglichkeit, diese Ressourcen zu nutzen.

Gateways sind Programme, die zwischen einem WWW-Server und einer externen Anwendung vermitteln. Bei einer solchen externen Anwendung kann

[188] Alpar, Kommerzielle Nutzung des Internet, Seite 106 und 107

es sich u.a. um ein IRC- oder um einen Archie-Clienten handeln. So ist auch der Zugriff auf statische Datenbanken möglich. Diese Gateway-Programme können in jeder beliebigen Programmiersprache erstellt werden. Beliebt ist hierbei u.a. die Scriptsprache Perl. Das Gateway-Programm stellt eine Anfrage an ein externes Programm, welches dann dem Gateway die entsprechenden Informationen zurückgibt. Das Gateway-Programm erstellt aus den gewonnenen Informationen eine WWW-fähige Seite, die der Browser interpretieren kann.

Die Informationen, die einem Gateway-Programm übergeben werden (z.B. eine Suchanfrage an eine Datenbank oder an einen Archie-Clienten), können in ein sogenanntes WWW-Formular eingegeben werden. Dadurch ermöglicht das Formularkonzept eine echte Interaktion des Benutzers mit dem WWW-Server. Mittels CGI werden die Daten aus den Formularfeldern an ein Skript übergeben, das diese Daten dann entsprechend weiterverarbeitet.

5.8.6 WWW-Browser

Das WWW beruht, ähnlich der anderen beschriebenen Dienste, ebenfalls auf der Client-Server-Architektur. Folglich spricht man von WWW-Server und WWW-Clienten. Für die Bezeichnung des WWW-Client hat sich der Begriff Browser eingebürgert. Der erste Browser war ein sogenannter „Line-Mode-Browser“, d.h. daß der Text seitenweise angezeigt wurde und hinter den Hyperlinks Zahlen standen, durch deren Eingabe man zu den Verweisen sprang. Doch bald schon wurden Browser mit grafischer Benutzeroberfläche entwickelt. Marc Andreessen entwickelte den ersten WWW-Browser für grafische Benutzeroberflächen, den Mosaic-Browser. Die Programmierer von Mosaic erfanden auch neue Features, die sie in ihren WWW-Browser implementierten, ohne daß diese Features standardisiert waren. Doch andererseits wurde hauptsächlich dadurch jene Lawine ins Rollen gebracht, die wir heute erleben. Marc Andreessen, der den Boom frühzeitig erkannte, stieg schließlich aus dem Mosaic-Projekt aus und wurde Mitbegründer einer neuen Firma für WWW-Software: Netscape. Die wohl gängigsten Browser sind der Netscape Navigator, der

Microsoft Internet Explorer und der Browser von Opera. Diese Clients sind mittlerweile für alle gängigen Betriebssysteme erhältlich.[189]

Wie bereits vorstehend beschrieben, integriert das WWW die „klassischen“ Internet-Dienste. Demnach muß der Browser auch mit den verschiedenen Funktionen und Besonderheiten der jeweiligen Dienste umgehen können. Obwohl die üblichen Browser die Standardfunktionen der verschiedenen Dienste grundsätzlich beherrschen, können sie nicht ein spezielles Client-Programm ersetzen. Wer also die volle Funktionalität von E-Mail, FTP und Co. nutzen möchte, sollte weiterhin auch die dafür entwickelten Clients nutzen. Vor allem den gehobenen Sicherheitsstandards werden die speziellen Clients besser gerecht als die Browser.

[189] Einen Überblick über verschiedene Browser bietet: Ramm, Recherchieren und Publizieren im World Wide Web, Seite 41 ff.

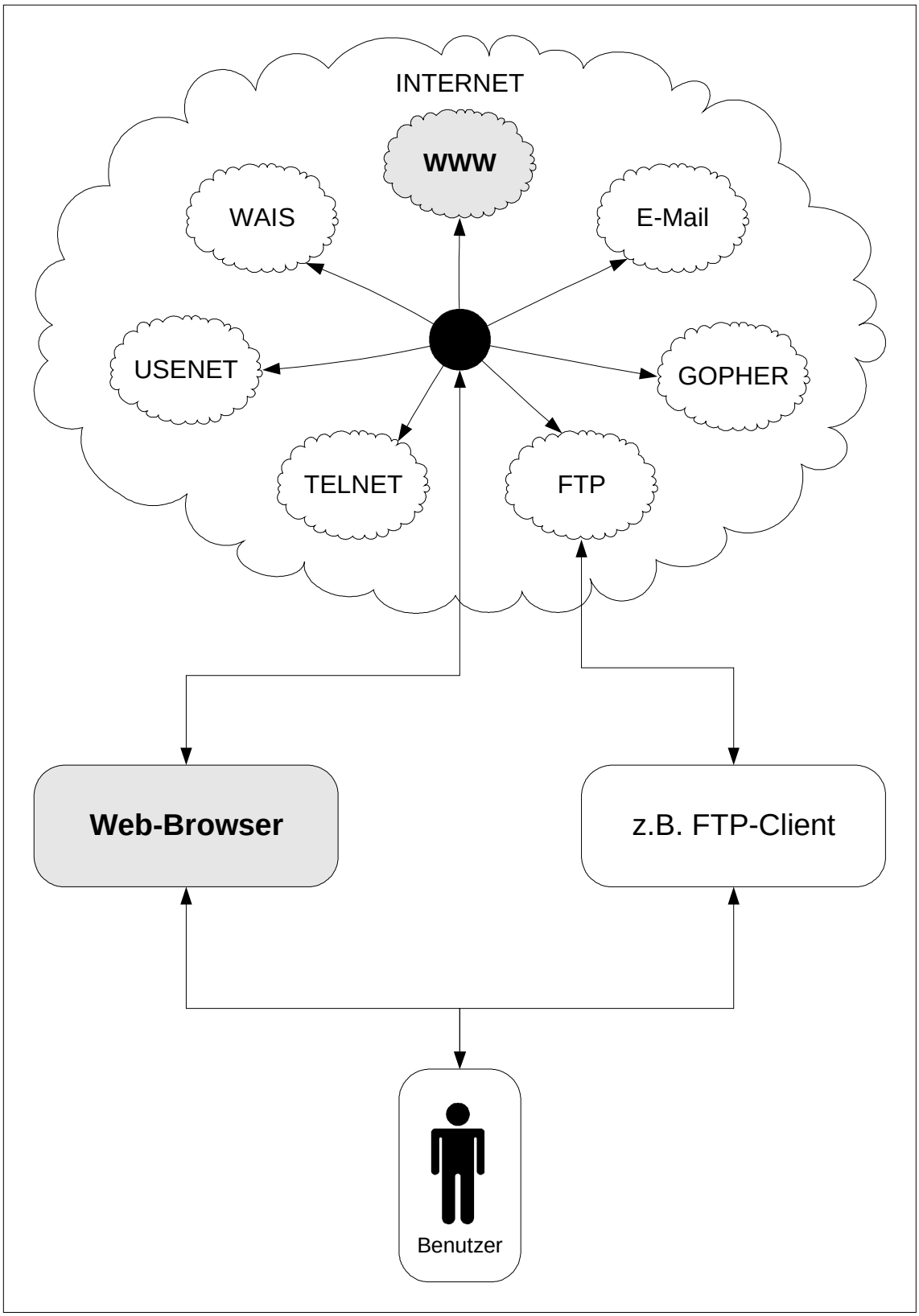

Abbildung 7: Zusammenhang „Browser – WWW – Internet“

6 Die Zukunft des Internets

6.1 Die multimediale Zukunft des Internets

Sowohl gesellschaftlich auch als technisch hat das Internet eine enorme Entwicklung erlebt. Wie es die aktuellen Trends bestätigen, wird das Internet auch in der Zukunft ständigen Erneuerungen ausgesetzt sein. Dies ist erforderlich, da es sich zu einem wichtigen Teil des menschlichen Lebens entwickelt hat. Welche Auswirkungen es weiter auf die Menschheit haben wird, soll an dieser Stelle nicht behandelt werden. Es erscheint wichtiger, einen Blick auf die zukünftigen technischen Entwicklungen zu werfen.

Zur Zeit existiert das Internet neben Fernsehen, Radio und Presse[190]. Durch seine multimediale Fähigkeit und seinem globalen Charakter wird das Internet zunehmend mit unserer altehrwürdigen Medienlandschaft verschmelzen. Das Internet wird Videokonferenzen, flimmerfreie Bilder und HiFi-Ton, Fernsehen über IP und weitere Formen des E-Commerce bringen.

6.2 Das „Internet Protocol – Version 6“ (IPv6)

Die Konsequenz daraus ist, daß auch in Zukunft immer mehr Nutzer das Internet für sich entdecken werden. Die Folge wird sein, daß immer mehr Endbenutzer, aber auch immer mehr Institutionen und Firmen, dauerhaft im Internet präsent sein wollen und daher die IP-Adressen nicht mehr ausreichen. Ergänzend dazu gibt es bereits Forschungsprojekte, deren Ziel es ist, z.B. auch Kühlschränke, Mikrowellen oder sogar Glühlampen mit einem eigenen Netzanschluß zu versehen. Diese umfassende Vernetzung greift in den Bereich der Heimautomation[191] ein und würde es einem Benutzer beispielsweise ermöglichen, technische Geräte in seiner Wohnung von jedem beliebigen Platz der Erde aus zu steuern. Dieser Mangel an Adressen, der u.a. durch eine dynamische Adressvergabe bei den Providern kaschiert wird, soll durch die Einführung des „Internet Protocol Version 6“ (IPv6) beglichen werden, das IPv4 ablöst[192].

---

[190] Vgl. auch: Neuberger/Tonnemacher, Online – Die Zukunft der Zeitung?

[191] Näheres siehe: Kuri, Das vernetzte Haus, Seite 178 ff.

[192] Vgl. auch: Krempel, Generalüberholung für das Internet, Seite 212.

Ende Juli 1999 ging IPv6 offiziell in Betrieb. IPv6 arbeitet mit einer Bitlänge von 128 bit und stellt dadurch gegenüber dem IPv4 (32 bit) einen wesentlich größeren Adressraum zur Verfügung. Eine weitere Neuerung des IPv6 ist der Einbau der sogenannten MAC-Adresse[193]. Durch diese Adresse ist es möglich einen Rechner eindeutig zu identifizieren.

6.3 Die mobile Zukunft des Internets

Das Internet wird mobil[194] [195]. Immer mehr Menschen schaffen sich ein Mobiltelefon an. Grundsätzlich ist es auch mit diesen Mobiltelefonen möglich, die Dienste des Internets zu nutzen. In der Kombination mit einem Laptop oder einem Taschencomputer (z.B. Palmtop) dient ein Handy mit integriertem Modem als Verbindung zum Netzwerk. Die heutigen Übertragungsgeschwindigkeiten sind noch zu gering, die Online-Gebühren zu hoch. Doch neue Übertragungsstandards wie z.B. HSCSD[196], GPRS[197] und UTMS[198] werden den Durchbruch bringen[199]. Obwohl zur Zeit diese Möglichkeit nur von wenigen genutzt wird, gehört den mobilen Geräten die Zukunft. Es wird nur eine gewisse Zeit brauchen, bis sich ein Markt gebildet hat und die Preise sinken. Die Zahl der mobilen Hosts wird sich erhöhen. Mobilfunkanbieter werden dann zu Internet-Provider. „Nach einer IDC-Studie gehen in 3 Jahren [also 2002] nur noch 65 Prozent des Internet Traffic von PCs aus – der Rest stammt von Handys, PDAs, Set-Top-Boxen, Terminals, die in ein Telefon eingebaut sind und so weiter.“[200]

Doch nicht nur in Verbindung mit einem Taschencomputer ist das Handy internettauglich. Sogenannte WAP-Handys ermöglichen den Abruf spezieller Internetseiten, die mit der „Wireless Markup Language“ erstellt und über das

---

[193] Die MAC-Adresse ist eine 48 bit lange Zahlenfolge, die eine Ethernet-Adapter-Karte eindeutig identifiziert.

[194] Für einen weitreichenden Überblick über die neuen Mobilfunkstandards vgl.: Zivadinovic, Drahtlos anknüpfen, Seite 186.

[195] Vgl. auch: Zivadinovic, Drahtloses Internet, Seite 30.

[196] High Speed Circuit Switched Data (HSCSD), diese Technik arbeitet mit Kanalbündelung von je 9,6 oder 14,4 KBit/s.

[197] General Packet Radio Services (GPRS), diese Technik ermöglicht paketvermittelnde Datenübertragung in GSM-Netzen (Mobilfunknetze) mit Transferraten bis zu 115,2 KBit/s.

[198] Universal Mobile Telecommunications System (UMTS), diese Technik ist die dritte Generation von Mobilfunkstandards mit Transferraten bis zu 2 MBit/s auf Paketvermittlungsbasis.

[199] Einen Überblick über die kommenden Mobilfunkstandards bietet Anlage 2.

„Wireless Application Protokoll“ (WAP) empfangen werden. Das Senden und Verschicken von E-Mails über das Mobiltelefon ist ebenfalls kein Problem mehr.

Die herkömmliche Wählverbindung über das Telefonnetz mittels Modem wird durch neue digitale Übertragungsstandards abgelöst[201]. So ist mittlerweile das gesamte Telekomnetz digitalisiert. ISDN ist schon lange kein unbekannter Begriff mehr und langsam hält auch die ADSL-Technik[202] [203] in den Großstädten Einzug. Doch wie auch bei den Handys geht der Trend zur drahtlosen Internetverbindung. Erstmals werden sogar Satellitenverbindungen oder Funkverbindungen für den Privatanwender erschwinglich, Internet aus dem fahrenden Auto ist keine Utopie mehr. Auch im Bereich der Standleitungen und der Backbones gibt es neue Entwicklungen, die eine weitere Erhöhung der Durchsatzraten ermöglichen. An dieser Stelle sind vor allem die optischen Netzwerktechniken auf Glasfaserbasis zu nennen, die Bandbreiten im GBit/s-Bereich liefern[204].

6.4 Verschmelzung von Telefon und Internet

Grundsätzlich existiert das Internet eigenständig neben dem eigentlichen Telefonnetz. In Deutschland ist das Telefonnetz überwiegend in den Händen der Deutschen Telekom. Die Deutsche Telekom ist aus der Bundespost hervorgegangen und wurde privatisiert. Obwohl die Telekom ein privatwirtschaftliches Unternehmen ist, unterliegt sie der Aufsicht der Regulierungsbehörde für Telekommunikation.

Durch VoIP wurde es erstmals möglich, für eine Sprachübertragung ein anderes Medium / Netzwerk zu nutzen als das Telefonnetz, nämlich das Internet. Am Anfang der Internet-Telefonie waren Gespräche nur im sogenannten Halb-Duplex-Modus möglich, d.h. daß nur jeweils ein Gesprächsteilnehmer sprechen konnte. Die Technik hat sich weiterentwickelt und so sind heute auch Gespräche im Voll-Duplex-Modus möglich.

---

[200] Luckhardt, Das Netz ist immer und überall, Seite 98

[201] Vgl. auch: Zivadinovic, Schneller Surfen, Seite 44.

[202] Asymetric Digital Subscriber Line (ADSL), Technik für die digitale Datenübertragung

[203] Vgl. auch: Endres, DSL – Die schnelle Leitung, Seite 126.

[204] Vgl. auch: Kuri, Das globale Netz, Seite 51.

Da VoIP auf der Paketvermittlung aufbaut, ist die Qualität der Verbindung und die mögliche Entfernung zwischen den beiden Gesprächspartnern maßgeblich von der Höhe des möglichen Datendurchsatzes an der schwächsten Stelle des Netzwerkes abhängig. Da die Netzwerktechnik einem ständigen Wandel unterliegt und die Leistungen - sowohl der Backbones, als auch der Zugänge der Benutzer zu ihren Providern - ständig zunehmen, werden auch vermehrt Anwendungen möglich, die einen großen Datendurchsatz benötigen. Allgemein geht man davon aus, daß es grundsätzlich möglich ist, den gesamten Telefonverkehr über das Internet abzuwickeln[205]. Dies kann aber nicht über die bisherige Technik (Computer) erfolgen, sondern nur über spezielle Stand-Alone-Endgeräte (Internet-Telefone oder –Faxgeräte). Die Entwicklung solcher Konzepte und Geräte hat bereits begonnen. Es gibt längst Lösungen für Endverbraucher, die es ermöglichen, den gesamten internen Telefonverkehr einer Firma über ein Ethernet abzuwickeln.

Ob sich diese Perspektiven weltweit durchsetzen werden, bleibt abzuwarten. Durch die ITU wurde bereits ein Standard erarbeitet, der eine Übertragung von Daten und Sprache über ein Netz ermöglicht. Sowohl für den Verbraucher, als auch für die Telefonbetreiber würde sich durch die Sprachübertragung über die Datennetzwerke eine erhebliche Kostenersparnis ergeben, da der Verwaltungs- und Wartungsaufwand für ein Netzwerk entfallen würde. Da die Deutsche Telekom sowieso einen Großteil der Infrastruktur des deutschen Internets trägt, würden sich auch hier keine Verluste ergeben, da die Telefonkunden ja nicht zur Konkurrenz „abwandern“ können.

6.5 Hyper-G

Wie bereits das URN-Konzept verdeutlicht, bringt die URL des WWW überwiegend Vorteile aber auch einige Nachteile. Ein Konzept, daß noch weiter als URN geht, ist Hyper-G. Hyper-G wurde als Hypermedia-System an der technischen Universität Graz entwickelt und baut auf einem strukturierten Hypertextsystem auf. Durch Hyper-G sollen die wesentlichsten Nachteile der URL aufgehoben werden, indem das WWW systematisch geordnet und katalogisiert wird. So soll die Suche nach Dokumenten ermöglicht werden, denn im jetzigen

[205] Vgl. auch: Kuri, Sprache im Päckchen, c´t 10/99, Seite 220 ff.

Zustand ist das WWW nahezu anarchistisch und chaotisch - und das Suchen bestimmter Informationen gleicht der sprichwörtlichen Suche nach der „Nadel im Heuhaufen“. Die nachfolgende Tabelle verdeutlicht die wesentlichsten Unterschiede von Hyper-G zum WWW:

WWW	Hyper-G
Client baut nacheinander Verbindungen zu verschiedenen WWW-Servern auf	Client ist die ganze Zeit mit einem Hyper-G-Server verbunden, dieser besorgt die Informationen aus aller Welt
Hyperlinks sind fest in die Dokumente eingebaut und nur im Text (beschränkt auch im Bild) möglich	Hyperlinks werden zu jedem „Objekt“ in einer eigenen Datei gespeichert, und sind so z.B. in Animationen denkbar
Hyperlinks sind unidirektional – keine Möglichkeit festzustellen, welche anderen Dokumente auf ein bestimmtes Dokument verweisen	Bidirektionale Hyperlinks ermöglichen es, jederzeit festzustellen, welche anderen Dokumente auf ein bestimmtes Dokument zeigen
Alle Benutzer sind „anonym“, Authentifizierung ist die Ausnahme	Anonyme Nutzung möglich, aber Authentifizierung üblich
Eine bestimmte Information (WWW-Seite) ist in der Regel nur auf einem bestimmten WWW-Server erhältlich; Überlastung möglich	Flood-Algorithmus verteilt Seiten nach „Bedarf“ in der ganzen Welt, so daß sie dezentral abgerufen werden können
Anlegen von Suchindizes nur durch externe Systeme (Robots [...])	Automatische Indizierung der Seiten bei Einfügen in die Datenbank
Keine Veränderung der Seiten mit dem WWW-Browser möglich	Veränderung von Seiten möglich, soweit Rechte eingeräumt werden

Tabelle 12: Hyper-G und WWW im Vergleich[206]

[206] Ramm, Recherchieren und Publizieren im Internet, Seite 11, Tabelle 1.1: Hyper-G und WWW

Durch die automatische Indizierung der Seiten beim Eintragen in die Datenbank ist eine detaillierte und vor allem lückenlose Suche nach bestimmten Dokumenten möglich, was wohl eher den wissenschaftlichen Anforderungen an das Hypermedia-System entspricht als die Verwendung von Internet-Verzeichnissen und Suchmaschinen. Durch die gleichzeitige Verteilung stark frequentierter Seiten auf mehrere Server wird einer Überlastung einzelner Server vorgebeugt, insofern tritt der gleiche Effekt wie bei URN ein.

Trotz der ersichtlichen Vorteile hat das Hyper-G-Konzept auch noch mit einigen Problemen zu kämpfen. Hyper-G ist derzeit vor allem im deutschsprachigen Raum verbreitet. Allerdings beschränkt sich die Anwendung zur Zeit noch auf experimentelle Testsysteme im akademischen Bereich. Das größte Problem von Hyper-G ist dessen Erweiterbarkeit - und hier vor allem die Belastung der Hyper-G-Server durch die anfallenden Datenmengen, die durch die Spiegelungen entstehen. Demnach konnte sich das System bisher nur im reinen wissenschaftlichen Sektor etablieren. Ein weiterer Grund ist auch die bisher fehlende Freigabe der Quelltexte der Hyper-G-Server oder die Unmöglichkeit eines kostenlosen Erwerbs von vorkompilierter Serversoftware. Als Clients für Hyper-G sind für Unix der „Harmony“ und für Windows der „Amadeus“ erhältlich. Hyper-G ist doppelt kompatibel, d.h. daß man mit einem WWW-Clienten Hyper-G nutzen kann und mit einem Hyper-G-Clienten auch das WWW.

7 Pornographie im Internet

7.1 Grundlagen

Pornographie ist ein Begriff, der sicherlich schon genauso alt ist, wie die menschliche Zivilisation. „Die rein sprachliche Erklärung des Wortes Pornographie ist eine sehr einfache: der Begriff `Pornographie´ kommt aus dem Griechischen. Porne bedeutet Hure und graphein heißt schreiben, darstellen. Pornographie ist also die Darstellung von Huren.“[207]

Unsere Gesellschaft kennt verschiedene Definitionen dieses unbestimmten Begriffes. Diese Definitionen unterscheiden sich sehr stark voneinander. Die Begriffsbestimmungen können sich sowohl von Land zu Land unterscheiden, als auch innerhalb des jeweiligen Landes. Für die verschiedenen Ansätze spielen vor allem historische und gesellschaftspolitische Faktoren eine wichtige Rolle.

In Deutschland war Pornographie in seiner umfassenden Form bis 1975 verboten. 1975 wurde die sogenannte leichte Pornographie für Erwachsene - und eingeschränkt auch für Jugendliche - freigegeben. An dieser Stelle wird deutlich, daß das deutsche Strafrecht eine Unterteilung der Pornographie vornimmt. Es unterscheidet einfache und harte Pornographie. Den Bereich der einfachen und harten Pornographie trennt Sohne wie folgt: „Unter harter Pornographie werden Medien verstanden, die sexuellen Mißbrauch an Kindern, sexuelle Handlungen zwischen Menschen und Tieren sowie Gewalttätigkeiten (sado-masochistische Darstellungen, Vergewaltigungen) beinhalten. Unter einfacher Pornographie werden aus juristischer Sicht Darstellungen gesehen, `die ihrer Gesamttendenz nach ausschließlich oder überwiegend auf das lüsterne Interesse an sexuellen Dingen beim Betrachter abzielen, dabei sexuelle Handlungen (Geschlechtsverkehr, Manipulationen am Geschlechtsteil) in grober aufdringlicher, aufreißerischer Weise anbieten, wobei die betont hervorgehobenen Geschlechtsorgane den wesentlichen Bildinhalt darstellen.“[208]

---

[207] Sohne, Pornographie, Seite 11

[208] ebd., Seite 11; mit Nachweisführung bei: Bremme, Bettina „Sexualität im Zerrspiegel. Die Debatte um Pornographie.“, Münster/New York, Waxmann Verlag, 1990

Desweiteren zeigt Sohne noch eine feministische Definitionsvariante und eine Definitionsvariante nach Lexika auf. An dieser Stelle ist es für die vorliegende Arbeit nur von Bedeutung, wie das (deutsche) Strafrecht den Begriff Pornographie definiert. Daher wird auf die Darstellung der verschiedenen anderen Sichtweisen verzichtet. Für die juristische Betrachtung der Problematik sind für die Ermittlungsbehörden und die Gerichte vor allem die Vorschriften der §§ 11 [Personen und Sachbegriffe] III, 184 [Verbreitung pornographischer Schriften] und 131 [Gewaltdarstellung] StGB und das Gesetz über die Verbreitung jugendgefährdender Schriften (GjSM) erstrangig.

7.2 Die Bundesprüfstelle für jugendgefährdende Schriften (BPS)

Eine besondere Rolle - in der Praxis der Strafrechtspflege für den Bereich der Pornographie - nimmt die Bundesprüfstelle für jugendgefährdende Schriften (BPS) ein. Diese, seit 1953 bestehende Behörde, unterstützt die Gerichte und führt eine Liste jugendgefährdender Medien. Die Liste enthält indizierte Schriften (siehe auch Begriffsbestimmung gem. § 11 III StGB), woraus die Begrifflichkeit „Index jugendgefährdender Schriften“ abgeleitet wurde[209]. Weiterhin umfaßt der Tätigkeitsbereich der BPS gewisse Präventionsmaßnahmen, da eines ihrer Aufgabengebiete die Zusammenarbeit mit Politik, Massenmedien, Schule und Eltern ist.

An dieser Stelle sei nur angemerkt, daß die Praxis der Indizierung im pornographischen Bereich (die Aufgabe der Indizierung bezieht sich nur zu einem Teil auf pornographische Schriften, ihr Aufgabenbereich ist breiter) sicherlich lückenhaft ist. Dies liegt zum größten Teil an den unbestimmten Rechtsbegriffen des Sexualstrafrechts. Diese unterliegen nicht nur der objektiven Bewertung durch den Richter, sondern auch einer nicht zu unterschätzenden gesellschaftlichen Ansicht.

7.3 Auswirkungen von Pornographie auf unsere Gesellschaft

Eine Frage, die sich vor allem Sexualwissenschaftler stellen, ist, welche Auswirkungen Pornographie auf unsere Gesellschaft hat. Zu diesem Themenkomplex gibt es weitreichende Untersuchungen, die aber teilweise zu unter-

[209] Eine Aufzählung der wichtigsten indizierungsfähiger Medien enthält Anlage 5.

schiedlichen Ergebnissen kommen. Auf der einen Seite gibt es Untersuchungen, in deren Ergebnis Pornographie beispielsweise zu erhöhter Aggression führt. Auf der anderen Seite gibt es aber auch Studien, die genau das Gegenteil beweisen wollen[210]. Sohne kommt zu dem Ergebnis, daß Pornographie bestimmte Auswirkungen nach sich zieht. Hauptkonsument von Pornographie sind Männer in einem Alter zwischen 18 und 29 Jahren. Es ist sicherlich nicht ohne Bedeutung, daß der durchschnittliche Internetnutzer auch männlichen Geschlechts und zwischen 18 und 29 Jahren alt ist. Die möglichen Auswirkungen, die der (mehr oder weniger regelmäßige) Konsum von einfacher und harter Pornographie haben kann, zeigt die folgende Übersicht:

- Zunahme der Anzahl Sexualpartner / Sexualpartnerinnen
- Förderung sexistischer Sexualphantasien (Streben nach Dominanz, Kontrolle, Zwang und Gewalt)
- Steigerung des Bezugs der Realität zu den pornographischen Phantasien (Gefahr des Auslebens sexistischer Phantasien)
- Zunahme der Masturbations-, Orgasmus- und Koitushäufigkeit; Abnahme der Koitusdauer
- Weckung verschiedener pornographischer Wünsche
- Zunahme von Gewaltanwendungen beim Sex und zur Sexerlangung (Pornographie fördert sexuelle Gewalt)
- Erzeugung von Minderwertigkeitsgefühlen oder Leistungsdruck

Tabelle 13: Mögliche Auswirkungen von Pornographie-Konsum[211]

7.4 Pornographie in unserer Gesellschaft

Pornographie ist in der vielfältigsten Weise in unserer heutigen Gesellschaft zu finden. Man erlebt Pornographie im Fernsehen, im Kino, auf Videos, in Zeitschriften, in speziellen Pornoshops, auf einem eigenen Schwarzmarkt oder auch in der Kunst. Dies sind die klassischen Möglichkeiten, um zumindest an einfache Pornographie zu gelangen. Einige der aufgeführten Varianten bie-

[210] Beispiele für beide Varianten führt Sohne, Pornographie, Seite 101 mit Quellennachweis auf.

ten auch die Möglichkeit, an illegale (harte) Pornographie zu kommen. Hier muß besonders auf den Schwarzmarkt hingewiesen werden und auf die diversen Pornoshops und Kioske. Hier hat sich oft, abgeschottet von der Öffentlichkeit, ein Handel „unter dem Ladentisch“ herausgebildet.

Neben den klassischen Vertriebsmethoden hat sich - mit dem Aufkommen des PCs in der breiten Bevölkerung - auch der Computer als mögliche Vertriebsmethode herauskristallisiert. „Zur Zeit gibt es nur Vermutungen über das Ausmaß der Verbreitung pornographischer Erzeugnisse in diesem Bereich. Die Organe des Jugendschutz werden erst dann mit den Auswüchsen der betreffenden Medien konfrontiert, wenn sie bereits vorhanden sind. Von daher kann aus den Materialien, die den Jugendämtern zugehen, nicht auf den ganzen Markt geschlossen werden. Dennoch kann eine steigende Tendenz beobachtet werden.“[212]

Am Anfang wurde die computergestützte Verbreitung von Pornographie vor allem über Disketten abgewickelt. Hierbei wurden Bilder oder Videos mit entsprechender Technik digitalisiert, vervielfältigt und dann weitergegeben, getauscht oder verkauft. Aus diesen Anfangszeiten stammen auch die ersten pornographischen Computerspiele. Durch die einfache Möglichkeit, Disketten zu kopieren, wurden der BPS nur wenige einschlägige Beispiele bekannt.

Nach dem Zeitalter des Stand-Alone-Computers brach das Zeitalter der Vernetzung an. Die Entwicklung des Internets war schon in vollem Gange. Da aber der Zugang zum Internet nur Behörden und Bildungseinrichtungen möglich war, nutzten die Straftäter, ebenso wie der Rest der (normalen) Bevölkerung, die Mailbox-Technik und die deutsche Version des Videotex (Btx).

In den Mailboxen konnten nun die entsprechenden Bilder oder Spiele abgelegt werden, so daß die aufwendige Verbreitung mittels Disketten nicht mehr notwendig war[213]. Btx, als eine höherwertige Variante der Vernetzung, bot für die Verbreitung pornographischer Schriften ebenfalls eine gute Grundlage. Vor allem, nachdem die Möglichkeit Btx zu nutzen mittels PC möglich wurde, konnte Btx an Attraktivität gewinnen. Als Beweis liefert Sohne Beispiele für illegalen

---

[211] Für nähere Informationen vgl. auch: Sohne, Pornographie, Seite 101 bis 128.

[212] Sohne, Pornographie, Seite 53

[213] Daß sich die Mailbox-Technik auch für andere Straftaten nutzen läßt, wird die Arbeit in ihrem weiteren Verlauf noch zeigen

Handel mit Kinderpornographie über Btx[214]. Das Zeitalter des Internets brachte dann den wahren Fortschritt. Nunmehr war es möglich, weltweit miteinander in Kontakt zu treten. Das Internet hat es den Tätern leicht gemacht, ihre Materialien miteinander auszutauschen und untereinander zu kommunizieren. Der potentiell Interessierte findet schnell das, was er sucht. Er braucht sich dabei nicht einmal aus der Anonymität seines Heimes herausbewegen.

7.5 Kinderpornographie als Variante der harten Pornographie

7.5.1 Allgemeines

Kinderpornographie – als Variante der harten Pornographie – macht ca. 1-2% der Gesamtkriminalität aus[215]. Traurigstes Beispiel für die Ausmaße, die diese Kriminalität teilweise annehmen kann, ist die Ermittlung eines international agierenden Kinderpornorings im August 1998. Bei der polizeilichen Aktion, die unter dem Namen „Wonderland“ durch die Medien geisterte, wurden über 100 Tatverdächtige (Konsumenten, Händler und Produzenten) aus 21 Staaten festgestellt. Dieses Beispiel zeigt in erschreckender Weise, daß Pornographie mehr ist als das Verbreiten pornographischer Schriften. Oftmals wird verkannt, daß hinter fast jedem Bild auch ein realer Mißbrauch eines Kindes steckt, der zudem meist ungesühnt bleibt. Pornographie ist nicht nur ein Problem unserer Gesellschaft, sondern auch ein nicht zu unterschätzender Wirtschaftsfaktor.

„Weltweit, so will das UNO-Kinderhilfswerk errechnet haben, werden mit kinderpornographischen Materialien aller Art 500 Milliarden Mark Umsatz im Jahr erzielt. Allein in der Bundesrepublik seien es 1,5 Milliarden Mark alle zwölf Monate.“[216]

Weiterhin stellt sich die Pornographie nicht als alleiniges Problem unserer Gesellschaft dar. Vielmehr ist sie ein Teilbereich einer Vielzahl von Abartigkeiten. „Wir haben nach Schätzungen von Fachleuten und Studien vermutlich bis zu 50.000 Konsumenten von Kinderpornographie in Deutschland, wir haben mehrere 10.000 Sextouristen, die sich jedes Jahr von Deutschland aus in die speziellen Traumziele in aller Welt aufmachen. Die Philippinen, Thailand, Bra-

---

[214] Sohne, Pornographie, Seite 55 und 56

[215] Gallwitz, Kinderpornographie ist sexueller Übergriff und Mißbrauch in der Praxis, Seite 1

[216] Drewes, Die Kindersexmafia und ihre unsichtbaren Kanäle, Seite 88

silien, Kenia, die Dominikanische Republik, Indien, Sri Lanka, Birma, Laos, Ungarn, Tschechien oder GUS Staaten sind hier zu nennen. Und im Durchschnitt verbraucht dabei jeder Kindersex-Tourist nach Untersuchungen 8 Kinder je 22 Tage, im Vergleich zu normalen Sex-Touristen, die es nur auf 5 Frauen je 22 Tage bringen.“[217]

Das Geschäft mit der Sexualität hat sich quantitativ und qualitativ ausgeweitet, neue Formen sind entstanden, so daß es nicht verwunderlich ist, daß die Kinderpornographie – als Teil der sexuell motivierten Kriminalität – ebenfalls zunimmt. Dies verdeutlicht auch die Zahl der in Deutschland existierenden 50.000 Prostituierten, die etwa 80 Millionen Freierkontakte mit ca. 3,2 Millionen Freiern haben. Rein rechnerisch gesehen handelt es sich hierbei um 18% der Männer im geschlechtsfähigen Alter, also fast jeder fünfte. Nach Expertenmeinungen wird der Markt für Kindersex und Kinderpornographie in Deutschland unterschätzt. Erhebungen gehen davon aus, daß es in Deutschland ca. 50.000 ständige Konsumenten von Kinderpornographie gibt.

Allgemein hat die Anwendung von Gewalt und die Gewaltbereitschaft in unserer Gesellschaft zugenommen. Vor allem die Gewalt in den Familien steigt stetig. Bis zu 75% der Streifenwageneinsätze in deutschen Großstädten wurden nach einer Studie wegen Familienstreitigkeiten gefahren[218]. Dabei existieren genug Studien, die den Zusammenhang zwischen allgemeiner Gewalt und sexueller Gewalt eindeutig belegen können.

Die entstehende sexuelle Gewalt bringt dann auch den sexuellen Mißbrauch von Kindern mit sich, deren Dokumentation dann die Kinderpornographie ist. An dieser Stelle schließt sich dann der Kreis, der vor allem auch durch das lukrative Geschäft mit eben dieser Pornographie ständig erneuert wird.

„Der Konsum von Kinderpornographie erhöht die Wahrscheinlichkeit von Übergriffen auf Kinder. So erweisen sich die sogenannten FKK-Hefte als Einstiegsmedium, da sie eine Legitimierung und Bagatellisierung sexualisierter Betrachtung von Jungen und Mädchen enthalten [...].“[219] Es muß also festgehalten werden, daß ein unmittelbarer Zusammenhang zwischen dem realen

---

[217] Gallwitz, Kinderpornographie ist sexueller Übergriff und Mißbrauch in der Praxis, Seite 3
[218] ebd., Seite 4
[219] Manske-Herlyn, Gegenstrategien gegen Pornographie mit Jungen und Mädchen, Seite 9

sexuellen Mißbrauch eines Kindes und Kinderpornographie und umgekehrt bestehen muß.

Das Dunkelfeld, mit dem wir es bei dem Mißbrauch von Kindern zu tun haben, ist enorm hoch und beträgt zwischen 1:10 bis 1:30. D.h. daß auf eine bekanntgewordene Straftat in diesem Zusammenhang im Schnitt 20 unbekannte Straftaten kommen. Durchschnittlich gibt es 800 sogenannte langzeitvermißte Kinder in Deutschland, deren Schicksal ungewiß ist. Die Folgen, die der sexuelle Mißbrauch für diese Opfer haben kann, sind katastrophal und hängen von vielen Faktoren ab[220]. Für das Opfer ist es nur sehr schwer möglich, seiner Opferrolle zu entkommen. Dokumentierter Mißbrauch (Kinderpornographie) kann die Opfer ein Leben lang verfolgen. Die Globalität des Internets trägt zu einer schnellen Verbreitung neuer Kinderpornographie bei. Inzwischen steht fest, daß in das Internet eingespeiste Pornographie nie mehr gelöscht werden kann.

7.5.2 Die Strategie der Täter

Grundsätzlich kann man im Bereich der Kinderpornographie zwischen zwei Tätergruppen unterscheiden. In der Hauptüberschrift wurde ebenfalls der Begriff Kindesmißbrauch verwendet, da Kinderpornographie dokumentierter Kindesmißbrauch ist. Dabei ist allerdings zu beachten, daß nicht jeder Kindesmißbrauch dokumentiert wird.

„Sexuelle Ausbeutung von Mädchen und Jungen im Rahmen von Pornoproduktionen wird sowohl durch dem Opfer vertraute Personen aus dem sozialen Nahbereich verübt, die Videos für den `Privatgebrauch´ produzieren (home videos), als auch durch professionelle Pornoproduzenten, die pornographisches Material für den illegalen Handel herstellen. Im zweiten Fall sind nicht unbedingt die familiären Bezugspersonen des Kindes in das Verbrechen verstrickt. Mütter und Väter sind in einigen Fällen beispielsweise nicht darüber informiert, daß ihre Töchter und Söhne von Mitarbeitern aus Institutionen sexuell mißbraucht und dabei gefilmt oder fotografiert werden. Immer wieder nehmen

[220] Eine Übersicht zu diesen Faktoren bietet: Gallwitz, Kinderpornographie ist sexueller Übergriff und Mißbrauch in der Praxis, Seite 7.

professionelle Täter auch über Dritte Kontakt zu potentiellen Opfern auf und setzen z.B. andere Kinder als `Schlepper´ ein.“[221]

Der Mißbrauch der Opfer läuft in der Regel über einen längeren Zeitraum ab. Es sind nur wenige Fälle bekannt, bei denen Opfer von professionellen Pornoproduzenten im öffentlichen Raum abgefangen wurden, um mit ihnen einen Porno zu drehen. Einen Überblick über die Täter und ihr Vorgehen im Bereich des Kindesmißbrauchs und der Kinderpornographie bietet die folgende Übersicht:

- der überwiegende Teil der Opfer kennt die Täter bereits vor dem sexuellen Mißbrauch
- Mädchen werden zu etwa einem Drittel von Tätern aus der Familie mißbraucht (Väter, Stiefväter, Brüder, Mütter, Großväter, Verwandte, Pädagogen, Babysitter)
- männliche Opfer werden meist von Bezugspersonen aus dem außerfamiliären Nahraum (Bekannte, Pädagogen, Trainer) und von Fremden sexuell ausgebeutet; die Täter kommen mit 10-20 % etwas seltener aus der Familie
- der Anteil weiblicher Täter liegt zwischen 10 und 20 %
- 1/3 der Täter ist selbst noch im Kindes – und Jugendalter
- einzelne Täter mißbrauchen viele Kinder
- etwa 2/3 der Täter, die innerhalb der Familie mißbrauchen, haben auch Opfer außerhalb der Familie
- die Täter kommen aus allen gesellschaftlichen Schichten
- die Täter suchen oft durch die Wahl ihres Berufes die Nähe zu Kindern (Kinderärzte, Pädagogen, Pfarrer, Erzieher, Hausmeister, Zauberer, Koch in einer Kindertagesstätte etc.)
- die Täter suchen oft durch ehrenamtliches Engagement die Nähe zu Kindern (Jugendgruppenleiter, Sporttrainer, Betreuer im Ferienlager etc.)
- gezielte Kontaktaufnahme mit alleinerziehenden Müttern, um an die Kinder zu kommen
- Aufsuchen von Orten, an denen sich Mädchen und Jungen aufhalten (Schwimmbad, Spielplatz, Spielwarenabteilung im Kaufhaus etc.)
- Aufbau und Angebot von Schulaufgabenhilfen, Freizeitangeboten und Babysitterdiensten besonders in sozialen Brennpunkten oder in Nachbarschaftsbezügen
- Täter bieten sich als Freunde der Familie an
- Mädchen und Jungen werden durch Zahlung von Geld dazu eingesetzt, ihre Freunde

[221] Enders, Die Strategie der Täter – Pornographie mit Mädchen und Jungen – Mißbrauch in Institutionen, Seite 46

zum Täter zu bringen („Schlepper“)
- Kontaktaufnahme über neue Medien (z.B. Internet via IRC)
- Sextourismus (u.a. richtete die Pädophilenszene eigene Hotels in 3.Welt-Ländern ein, in denen dann geschäftsmäßig durchorganisiert der bezahlte Mißbrauch von Kindern abläuft)
- potentielle Opfer werden durch verschiedene Tricks verführt (Überredung, emotionale Zuwendung, Geschenke, Bevorzugung, Hofieren[222], kindliches Mitgefühl wecken, heterosexuelles Interesse bei Jugendlichen wecken etc.)
- der Mißbrauch wird zu einem gemeinsamen „Geheimnis“ erklärt oder dem Opfer wird eine aktive Beteiligung eingeredet
- das Opfer wird erpreßt (angebliches Fehlverhalten, Liebe des Kindes zu der Vertrauensperson, Spielzeug, Vergünstigungen und Erfüllung grundlegender Bedürfnisse)
- dem Opfer wird gedroht (mit Folgen für den Täter oder das Opfer, für die Familie, Haustiere, Vertrauenspersonen)
- das Opfer wird psychiatrisiert
- das Schamgefühl des Opfers wird ausgenutzt oder kindliche Opfer gegeneinander ausgespielt

Tabelle 14: Die Täter/Täterinnen im Bereich des Kindesmißbrauchs und der Kinderpornographie und ihre Vorgehensweisen[223]

In der gleichen Weise, wie es beim Mißbrauch von Kindern ohne Dokumentation geschieht, werden die Opfer nach bestimmten Kriterien ausgewählt. Dabei werden vor allem Mädchen und Jungen ausgewählt, die offensichtlich über eine geringe Widerstandsfähigkeit verfügen.

Es ist bekannt, daß vor allem professionelle Pornoproduzenten Opferkontakte an sozialen Brennpunkten suchen. Einen Überblick über allgemein anerkannte Erkenntnisse zu potentiellen Opfern bietet die folgende Übersicht:

[222] Hierbei wird das Kind wie ein Erwachsener behandelt.

[223] Für weiterführende Informationen vgl. auch: Enders, Die Strategie der Täter – Pornographie mit Mädchen und Jungen – Mißbrauch in Institutionen, Seite 33 bis 45.

- die Opfer haben oft eine unvollständige oder autoritäre Sexualerziehung erfahren
- die Opfer wurden oftmals „traditionell“ erzogen (z.B. ist Erwachsenen nicht zu widersprechen)
- Opfer sind oft noch im Vorschulalter, da die Glaubwürdigkeit als Zeuge dadurch gemindert wird
- Opfer sind oft behinderte Mädchen oder Jungen
- Opfer sind oft emotional vernachlässigt und sehnen sich förmlich nach Zärtlichkeiten und Aufmerksamkeit
- etwa 2/3 der Opfer haben direkte körperliche Gewalt durch Eltern erlebt (Ohrfeigen, Schläge oder körperliche Folter) oder miterlebt, wie körperliche Gewalt gegen andere Familienangehörige eingesetzt wurde
- Opfer sind oft Kinder alleinerziehender Mütter oder Väter
- Opfer wurden oftmals schon im Vorfeld sexuell ausgebeutet und haben daher oft keine entsprechende Widerstandskraft (Spiralwirkung des sexuellen Mißbrauchs)
- besonders gefährdet sind auch Jugendliche und Kinder, die gewerbsmäßig der Prostitution nachgehen

Tabelle 15: Erkenntnisse über Opfer von Kinderpornographie und Kindesmißbrauch[224]

Im Bereich der Kinderpornographie kommt es im Gegensatz zum Kindesmißbrauch noch zu weiterem speziellen Täterverhalten. Die Opfer sollen zu einem bestimmten Verhalten gezwungen werden, um sicherzustellen, daß sie auch über die Taten schweigen.

Es ist bekannt, daß vor allem professionelle Pornoproduzenten ihre kindlichen Opfer an sozialen Brennpunkten ansprechen (Bahnhofszene oder Babystrich), da hier für sie die Wahrscheinlichkeit sehr hoch ist, finanziell bedürftige Kinder anzutreffen. Es ist dann ein Leichtes, diese in Not geratenen Kinder für

eine - anscheinend „lukrative“ - Filmrolle zu gewinnen. Haben sich die Kinder dann erst einmal in die Hände eines solchen Produzenten begeben, können sie die Geschehnisse nicht mehr beeinflussen.

Oftmals werden den Kindern vor den ersten „Dreharbeiten“ pornographische Filme mit Erwachsenen aber auch mit Kindern gezeigt. Damit wird bezweckt, daß die Kinder an das Thema herangeführt werden, daß ihnen gezeigt wird, wie sie es dann „machen“ sollen und das ihnen verdeutlicht wird, daß es normal ist, wenn Erwachsene Sex mit Kindern haben. Teilweise wird dabei der Umstand ausgenutzt, daß Jungs auch schon im vorpubertären Alter Interesse an pornographischen Medien entwickeln.

Wenn es dann zum eigentlichen Mißbrauch vor der Kamera kommt, ist es nicht selten, daß die Kinder im Vorfeld bereits mit Medikamenten, Drogen oder Alkohol „betäubt“ wurden. Das hat zur Folge, daß sie die Handlungen einfach über sich ergehen lassen. Oftmals werden die Handlungen auch in Spielsituationen eingebettet. Die Anwendung von Gewalt gegen die Kinder ist üblich. Dabei dienen auch gewalttätige Pornos zur Einschüchterung der kindlichen Darsteller.

„In den letzten zehn Jahren berichteten wiederholt Mädchen und Jungen aus unterschiedlichen Städten gegenüber Zartbitter Köln von der sexuellen Ausbeutung im Rahmen satanischer Rituale und der Produktion von `snuff-pornos´ (Pornos mit Tötungsdelikten). Mehrere Kinder und Jugendliche berichteten, daß sie miterlebten, wie andere Kinder zu Tode vergewaltigt wurden und/oder sie selbst Tiere und auch Babys töten und anschließend deren Blut trinken und verzehren mußten. [...] Nach glaubhaften Aussagen von Betroffenen werden die Morde und Praktiken der sexuellen Folter z.T. auf für den Verkauf bestimmten Videos festgehalten und die Kinder und Jugendlichen anschließend mit ihren `eigenen Taten´ erpreßt [...].

Ein in Holland festgenommener Schweizer Pornoproduzent kaufte Kinder in Rumänien, tötete sie auf bestialische Art und Weise im Rahmen seiner Pro-

---

[224] Für weiterführende Informationen vgl. auch: ebd., Seite 33 bis 45

duktionen und vernichtete die Überreste der Opfer nicht mehr nachweisbar in Salzsäurefässern."[225]

Vielfach werden den Jungen und Mädchen die Filme dann vorgespielt, um ihnen zu „beweisen", daß es ihnen doch eigentlich Spaß gemacht hat. In den Filmen sieht es auch tatsächlich so aus. An dieser Stelle sollte man dann aber bedenken, daß Schmerzenslaute mit Musik überspielt oder Wunden durch Schminke verdeckt werden können.

Sowohl die professionellen Filme, als auch die Home Videos werden z.T. über das Internet zum Verkauf angeboten. Gelangt ein pornographisches Video oder ein pornographisches Bild erst einmal in das Internet, besteht keine reale Chance mehr, dieses Bildmaterial jemals wieder aus dem Netzwerk zu entfernen. In diesem Zusammenhang spricht man von „der ewigen Zeugenschaft der Bilder". Die polizeilichen Ermittlungen zeigen regelmäßig, daß z.T. bis zu 20 Jahre alte Bilder immer wieder im Internet auftauchen. Die Betroffenen müssen also auch noch lange nach dem realen Mißbrauch damit rechnen, daß sie eines Tages in einem Video oder auf einem Bild erkannt werden. Welche psychologischen Auswirkungen das auf die Betroffenen haben kann, kann sich wohl jeder denken.

7.6 Der „klassische" Markt

Die Strukturen und Vertriebswege des professionellen Handels mit Kinderpornographie sind straff organisiert. An dieser Stelle können daher Parallelen z.B. zum professionellen Btm-Handel gezogen werden. Die Kinderpornoszene ist von konspirativem Verhalten geprägt, die Täter agieren international unter einem geringen Entdeckungsrisiko.

„Während in den 80er Jahren die gefilmten Tathandlungen und Tatorte sowie die Heimat der betroffenen Kinder sehr häufig in Südostasien, in der Karibik oder in Südamerika zu vermuten waren, lächeln nun mehr gequälte Kindergesichter von den Videos, deren Herkunft Tschechien, Polen, Rumänien, ein Land der ehemaligen Sowjetunion oder des ehemaligen Jugoslawien sein

[225] Enders, Die Strategie der Täter – Pornographie mit Mädchen und Jungen – Mißbrauch in Institutionen, Seite 49

dürfte. Die Wege sind kürzer, die Produktionen preiswerter, die Risiken geringer geworden.“[226]

Der Verkaufspreis eines Videos richtet sich vornehmlich nach dem Alter des dargestellten Kindes und der sadistischen Ausprägung der Handlungen, die an ihm vorgenommen werden. Der Marktpreis liegt nach Expertenangaben bei einem 30-minütigem Video zwischen 300 und 500 DM. Für besondere „Raritäten“ (zu denen vor allem auch die Snuff-Videos zählen) kann der Kaufpreis das Vielfache der angegebenen Preisspanne übersteigen.

Zunehmend werden die Verhaltensweisen privater „Hobbyfilmer“ auch professioneller. „Zimmereinrichtungen werden verändert, Kinder durch Masken unkenntlich gemacht, der Orginalton wird durch Musik ersetzt, um eine mögliche Identifizierung zu verhindern. Das Medium Video ermöglicht es. daß die Herstellung ohne Beteiligung Außenstehender erfolgt, also im geheimen bleibt.“[227] Polizeiliche Erkenntnisse belegen, daß die Pädophilen-Szene vor allem die Hobby-Filme schätzt, da diese ungekünstelt das „wahre Leben“ zeigen.

Nach polizeilichen Prognosen wird sich der größte Teil der Verbreiterszene ins Internet verlagern, da hier vor allem die Knüpfung anonymer Kontakte möglich ist. Dabei müssen aber aus polizeilicher Sicht vor allem auch die Möglichkeiten der Mailbox-Technik und der verschiedenen Online-Dienste beachtet werden, die insofern nicht zwangsweise einen Teil des Internets bilden. Kommunikation und Kontaktaufnahme zwischen Anbieter und Käufer finden fast ausschließlich anonym und konspirativ statt.

Zur Zeit herrscht noch die Kontaktaufnahme über sogenannte Chiffreanzeigen vor. Diese Anzeigen sind sowohl in eindeutig sexistischen Magazinen, aber auch in seriösen Magazinen oder in Tageszeitungen zu finden.

Der Anzeigentext enthält für einen unbedarften Betrachter oftmals keine Anzeichen für den Vertrieb von Kinderpornographie, Pädophile hingegen lesen „zwischen den Zeilen“ und können so auf die Angebote eingehen. In diesen Anzeigen finden sich dann Formulierungen wie: „Videos von privat“, „Löse meine private Videosammlung auf“ oder „Orginale Privataufnahmen, nur für seriöse Kenner“. Offensichtliche Wörter wie „Teen“, „Kind“ oder „Lolita“ erscheinen

---

[226] Paulus, Sexuelle Gewalt gegen Kinder und Kinderpornographie, Seite 76

nicht in diesen Anzeigen. Der Austausch von Materialien erfolgt dann weitestgehend über Postadressen, unter Vorausbezahlung.

7.7 Der Vertrieb über das Internet

„Der Pornomarkt ist - wie andere Wirtschaftsbereiche auch - ständigen Veränderungen unterworfen. Blickt man zurück in die 70er Jahre, dann wird deutlich, daß sich inhaltlich nicht nur Angebot und Nachfrage, sondern auch die Vertriebswege und -strukturen, die Größenordnung und die Akzeptanz von (kinder-)pornographischen Darstellungen enorm verändert haben.“[228]

Das Internet wird nach polizeilichen Erkenntnissen für die Verbreitung von Kinderpornographie vor allem mittels der Dienste Usenet und IRC mißbraucht. Diese Dienste bieten den Tätern die notwendige Anonymität und Konspirativität. Technik, Struktur und Nutzungsabläufe dieser Dienste erschweren erheblich die polizeilichen Ermittlungen. Die Entwicklung der Videotechnik und der digitalen Fotografie machen die Täter von der Außenwelt unabhängig, da beispielsweise für die Entwicklung von Fotos kein Labor mehr benötigt wird. Das Internet bietet die Möglichkeit, schnell, risikolos und international und ohne Kontrollen, jede Form digitalisierter Daten innerhalb von Sekunden an das andere Ende der Welt zu versenden.

Die Sprache, die in der netzspezifischen Szene gesprochen wird, ist typisch für den Bereich der Kinderpornographie und ähnelt nach polizeilichen Erkenntnissen der Sprache der „klassischen“ Kinderporno-Szene. Beispiele des Szenejargons zählt die folgende Übersicht auf:

---

[227] Laschet, Kinderpornographie – Entstehung, Vertrieb und Bekämpfungsstrategien. Eine aktuelle Bestandsaufnahme aus kriminalpolizeilicher Sicht., Seite 66

[228] Paulus, Sexuelle Gewalt gegen Kinder und Kinderpornographie, Seite 75

Begriff	Bedeutung
Junge Welpen	gemeint sind Knaben unter 14 Jahren
Lo oder Lolita	gemeint sind Mädchen unter 14 Jahren
SM	SM für Sadistisch und Masochistisch – Quälen und quälen lassen
Trash	kommt aus dem amerikanischen und bedeutet Dreck, Abfall; gemeint sind Videos, die Zusammenschnitte besonders grausamer Szenen aus mehreren anderen Videos enthalten
Snuff	bedeutet soviel wie Auslöschen, Ersticken; gemeint sind Videos, mit sexuellen Folterungen bis hin zum langsamen, qualvollen Tod des Opfers

Tabelle 16: Jargon der Kinderporno-Szene

Die Produkte, die aus dem Bereich der Pornographie im Internet angeboten werden, sind vielfältig. Polizeiliche Ermittlungen brachten Bilder und Videos mit folgenden Inhalten ans Licht: Kinderpornographie in jeder Form, Folterungen, Auspeitschungen, Verstümmelungen, Vergewaltigungen, Verzehrung von Fäkalien etc.

8 Phänomenologie netzbezogener Straftaten

8.1 Allgemeines

Dieser Abschnitt soll sich mit der Phänomenologie, also den Erscheinungsformen, der netzbezogenen Straftaten befassen[229]. Hierbei soll versucht werden, eine Klassifizierungsvariante zu erarbeiten, die auf den Betrachtungen von Jofer aufbauen[230]. Eine Klassifizierung hat für die Polizei vor allem die Bedeutung, daß sich das Meldewesen für Computerkriminalität und der Aufbau einer speziellen Abteilung, die sich mit der Computerkriminalität in summa befassen sollte, an solch einer Klassifizierung ausrichten können. Abschließend sollen dann Beispiele für mögliche und typische Kriminalitätsformen im Internet vorgestellt werden, wobei die jeweiligen Erscheinungsformen dem entsprechenden Diensten zugeordnet werden. Ein Anspruch auf Vollständigkeit wird nicht erhoben.

8.2 Computerkriminalität

Eine Straftat ist eine rechtswidrige und schuldhaft begangene Handlung im weitesten Sinne, die den Tatbestand einer Strafrechtsnorm des Strafgesetzbuches oder eines Strafnebengesetzes erfüllt. Die Polizei faßt alle Straftaten, bei denen ein Computer (im weiteren und engeren Sinne) eine Rolle spielt, unter dem Begriff Computerkriminalität zusammen. Jofer definiert Computerkriminalität wie folgt[231]:

„Computerkriminalität umfaßt alle Straftaten, bei denen die EDV [Elektronische Datenverarbeitung] in den Tatbestandsmerkmalen enthalten ist, alle Straftaten, bei denen die besonderen technischen Möglichkeiten der DV die Begehung und/oder Durchführung unterstützt haben und zu deren Aufklärung eine besondere Sachkenntnis notwendig ist.“[232]

Durch das BKA wurde diese Definition erweitert und dabei besonders auf die Straftaten im Zusammenhang mit Datennetzen und die Bedrohung der In-

---

[229] Einen kurzen Überblick über Mißbrauchsmöglichkeiten im Internet auch bei: Hartung, Internet, dp-special April 1998, Seite 2 – 15.

[230] Jofer, Strafverfolgung im Internet, Seite 34 und 35

[231] Für weitere Definitionsansätze vgl. auch: Goldmann, Computerkriminalität und ihre Bekämpfung, Kriminalistik 8-9/1989, Seite 442 bis 451.

formationstechnik abgestellt[233]. Ob diese Definition sinnvoll ist und eine wesentliche Neuerung darstellt, kann bezweifelt werden, da die Definition nach Jofer vollkommen ausreicht und grundsätzlich jede Form der Computerkriminalität unter diese Definition subsumiert werden kann.

Eine Schwäche beider Definitionen ist, daß z.B. Straftaten im Zusammenhang mit Telefon – oder TV-Netzen nicht unter die Computerkriminalität fallen. In der Praxis ist es aber oft so, daß Computerkriminalität teilweise mit Manipulationen der Telefonnetze einhergehen und von Computerkriminellen vorgenommen werden. Daher ist m.E. folgende Definition des Oberbegriffes Computerkriminalität zutreffender und wird den praktischen Anforderungen besser gerecht:

Die Computerkriminalität umfaßt alle Straftaten, bei denen die EDV (im weiteren Sinne) explizit im Tatbestand genannt wird, bei denen die Möglichkeiten der EDV die Begehung oder die Durchführung unterstützt haben oder die im Zusammenhang mit elektronischen Netzwerken begangen wurden und zu deren Aufklärung eine besondere Sachkenntnis erforderlich ist.

8.3 Versuch einer Klassifizierung der Computerkriminalität

Grundsätzlich ist die Computerkriminalität in sich weiter klassifizierbar. Bei einer netzbezogenen Straftat kommt ein weiteres Kriterium hinzu, das sonst für die strafrechtliche Betrachtung an sich ohne Bedeutung ist, für die Ermittlungsbehörden aber ein wesentliches Klassifizierungsmerkmal darstellen sollte. Eine Straftat ist netzbezogen, wenn im konkreten Einzelfall ein Computernetzwerk eine nicht unwesentliche Rolle für oder während der Tat spielte, d.h. wenn die Tat mittels eines Computers begangen wurde, der mindestens zeitweise mit einem Computernetzwerk verbunden war oder ein Computernetzwerk während der Tat genutzt wurde. In diesem Zusammenhang muß man unter einem Computernetzwerk eine Verbindung mehrerer Computer über ein Datenträger-Medium verstehen.

Das Internet ist ein Zusammenschluß vieler kleiner Netzwerke, die sich auf ein gemeinsames Protokoll geeinigt haben. Allerdings gibt es auch Netz-

---

[232] Jofer, Strafverfolgung im Internet, Seite 33

[233] Vgl. auch: Jofer, Strafverfolgung im Internet, Seite 33.

werke, die nicht mit dem Internet verbunden sind oder Telefonnetzwerke. Ferner gibt es aber auch Netzwerke, die zwar mit dem Internet verbunden sind aber darüber hinaus ihrem Benutzerkreis eigene Dienste zur Verfügung stellen. Die Straftaten im Internet bilden m.E. eine Teilmenge der netzbezogenen Kriminalität, welche wiederum einen Teilbereich der Computerkriminalität darstellt. Die reine Internet-Kriminalität umfaßt somit alle Straftaten, die im Zusammenhang mit den standardisierten Internet-Diensten begangen werden.

Im Bereich der Netzkriminalität nimmt Jofer noch eine weitere Untergliederung vor. Er unterscheidet desweiteren netzspezifische Verbreitungsdelikte, das Internet als Mittel zur Tatkommunikation und das Internet als virtuelles Tatwerkzeug[234]. Jofer differenziert hierbei nicht nach allgemeiner Netzkriminalität und reiner Internet-Kriminalität. Da die Grenzen zunehmend unscharf werden, hat das keine nachteiligen Auswirkungen. Dennoch sollte man sich dem allgemeinen Verständnis nach immer nach den technischen Zusammenhängen richten. Auf dieser Gliederung sollen die nachfolgenden Ausführungen aufbauen[235].

8.3.1 Netzspezifische Verbreitungsdelikte

Eine legale Hauptfunktion des Internet besteht in der - mehr oder weniger - kontrollierten Verteilung und dem Zugänglichmachen von unterschiedlichsten Informationen. Der Begriff Information ist dabei weitreichend zu verstehen. Synonym könnte auch der Begriff „Daten“ verwendet werden. Jeder Internet-Dienst liefert einem Benutzer grundsätzlich Daten. Diese Eigenschaft des Internets, dem Menschen Informationen zugänglich zu machen, erfährt auch die erste Mißbrauchsmöglichkeit.

Gemeint ist die Verbreitung strafbarer Informationen und die strafbare Verbreitung an und für sich legaler Daten. Die Verbreitung strafbarer Informa-

---

[234] Jofer, Strafverfolgung im Internet, Seite 34 bis 36

[235] Zu beachten ist, daß die Computerkriminalität ursprünglich der Wirtschaftskriminalität zugeordnet wurde. M.E. bildet sie aber heute eine eigenständige Kriminalitätsform, mit eigener Charakteristik. Allerdings bedient sich die Wirtschaftskriminalität sehr stark der EDV, weshalb eine koordinierte und partnerschaftliche Zusammenarbeit der beiden Bereiche angestrebt werden sollte. Erforderlich ist eine gesonderte und vor allem spezialisierte kriminalpolizeiliche Bearbeitung der als Computerkriminalität klassifizierten Delikte. Das Klassifizierungsmodell bietet eine Möglichkeit der Strukturierung einer solchen spezialisierten polizeilichen Einheit. Ob dieses Modell den weiteren technischen und gesellschaftlichen Entwicklungen standhalten wird, kann nur die Zukunft zeigen.

tionen und die strafbare Bereitstellung an sich legaler Daten wird nicht erst durch das Internet ermöglicht. Die Straftaten sind auch ohne die Einbeziehung des Internets grundsätzlich möglich. Allerdings bietet das Internet vor allem eine quantitative und auch qualitative Steigerungsmöglichkeit der Mißbrauchsvarianten.

8.3.2 Das Internet als Mittel zur Tatkommunikation

Das Internet dient dem Austausch von Informationen. Die Kommunikation zwischen zwei oder mehreren Menschen ist eine Form des Informationsaustausches. Unerheblich für die Klassifizierung ist, ob die Kommunikation an sich bereits eine strafbare Vorbereitungshandlung darstellt. Wichtig ist, daß eine strafbare Handlung ausgeführt wird, für die eine gewisse Kommunikation erforderlich ist. Alle klassischen Formen der Täterkommunikation, wie z.B. Verabredungen zu Straftaten oder Anbieten von Hehlerware sind auf das Internet übertragbar. Dies stellt auch die Besonderheit dieser Kategorie dar. Das Internet selbst ist nur Tatwerkzeug und „ersetzt“ in diesem Falle u.a. das herkömmliche Telefon, eine konspirative Örtlichkeit oder die konventionelle Briefpost. Im Internet selbst werden keine Straftaten begangen.

Inwiefern das Internet heute schon zur Tatkommunikation genutzt wird, kann nicht gesagt werden, da hierfür ausreichende kriminologische Untersuchungen fehlen. Von daher muß sich eine Betrachtung auf theoretische Überlegungen stützen. Mit Sicherheit kann aber gesagt werden, daß das Internet für Straftäter eine gute Alternative für eine funktionierende Kommunikation darstellt. Denn unsere heutige Gesellschaft – und damit sind die Straftäter inbegriffen – ist maßgeblich von einer funktionierenden Kommunikationstechnik abhängig. In dem Sinne bietet das Internet vor allem für die Organisierte Kriminalität die erforderlichen Verschlüsselungstechniken und eine konspirative Umgebung.

8.3.3 Das Internet als virtuelles Tatwerkzeug

„Die dritte Kategorie geht über die bloße Verbreitung oder den Austausch von Informationen hinaus: In diesem Fall wird das Internet als virtuelles Tatwerkzeug genutzt, mit dessen Hilfe in der Realität Straftaten begangen werden können. Über das Netz vermag ein Täter in besonders gelagerten Fällen, die Reaktion eines Menschen oder einer Maschine auszulösen: Das Netz wird als atypisches Tatwerkzeug mißbraucht. Die per se unschädliche Information kann durch den Umsetzungsakt aus ihrem virtuellen Dasein quasi heraustreten und realen Schaden verursachen.“[236]

Es ist zu beachten, daß die drei vorgestellten Kategorien nicht streng voneinander getrennt werden können. Die Übergänge zwischen den drei Formen sind fließend. Insofern kann auch eine Handlungsweise Gesichtspunkte zweier oder sogar aller drei Kategorien enthalten. Allerdings wird eine Form immer das Übergewicht haben, weshalb die Zuordnung einer Handlungsweise zu nur einer Kategorie grundsätzlich möglich sein sollte.

8.4 Kriminologische Erkenntnisgewinnung

Im allgemeinen liegen keine sicheren Daten über netzspezifische Kriminalität vor. Ein Grund dafür ist, daß das Phänomen der Kriminalität in Computernetzen aus kriminologischer Sicht noch wenig erforscht ist. Als mögliche Erkenntnisquellen nennt Jofer die Polizeiliche Kriminalstatistik (PKS), repräsentative Befragungen eines Bevölkerungsquerschnitts und die einzelfallorientierte Auswertung signifikanter Delikte[237].

Neuste Erhebungen, wieviel Kommunikation im Internet mit kriminellen Inhalten oder zu kriminellen Zwecken stattfindet, gehen weit auseinander. „Die Schätzungen reichten von 40.000-80.000 kinderpornographischen Bildern über 1% der Gesamtkommunikation zu 1/60 aller Angebote und news-Artikel (letztere beiden Zahlen auf alle Delikte bezogen).

Eine Domumentation der Hannoveraner Stelle des Kinderschutzbundes wurde kurz erwähnt, die auf noch erheblich höhere Zahlen kommt (10-15 kin-

---

[236] Jofer, Strafverfolgung im Internet, Seite 36

[237] ebd., Seite 37

derpornographische Kanäle im IRC mit mindestens 300 Tauschvorgängen am Tag) [...]."[238] Mithin muß man davon ausgehen, daß derzeit keine gesicherten Erkenntnisse vorliegen.

Die PKS macht grundsätzlich kriminologische Betrachtungen des Gebietes Computerkriminalität möglich. Allerdings geht die PKS von einer Definition der Computerkriminalität aus, die den praktischen Anforderungen nicht mehr gerecht wird und die demzufolge eine Verzerrung des Bildes bewirkt. Allgemein kann man aus der Entwicklung der Computerdelikte nur indirekt auf netzbezogene Kriminalität in den drei vorgestellten Formen schließen. D.h. daß mit zunehmendem Einsatz von Computern für die Begehung von Straftaten (Computerkriminalität im engeren Sinne) auch auf zunehmende Netzwerkkriminalität geschlossen werden kann. Aber im welchem Verhältnis sich die Netzwerkkriminalität zur restlichen Computerkriminalität entwickelt, kann nicht gesagt werden. Aus den genannten Gründen wurde es an dieser Stelle auch unterlassen, Zahlen der PKS darzustellen.

Eine repräsentative Befragung eines Bevölkerungsquerschnitts muß sich auf eine gewisse Grundgesamtheit stützen, innerhalb derer die Befragung durchgeführt werden müßte. Somit wäre eine herkömmliche Befragung der Bevölkerung auf der Straße wenig sinnvoll und nicht repräsentativ. Vielmehr müßte die Befragung direkt im Internet erfolgen. Um hier eine repräsentative Umfrage für Deutschland zu erreichen, müßte der deutsche Teil der Internetkultur genaustens analysiert werden. Dies ist unmöglich, da das Internet einen länderübergreifenden Charakter besitzt und sich nicht in Länderbereiche teilen läßt. So ist es möglich, daß sich ein Amerikaner eine E-Mail-Adresse auf einem Rechner registrieren läßt, der unter einer deutschen Domain läuft. Ferner wird in anderen Ländern durchaus anders mit der Thematik „Kriminalität im Internet" umgegangen, so daß andere Einstellungen wahrscheinlich sind. Diese Probleme verdeutlichen die Notwendigkeit einer international repräsentativen Befragung, die sich auf das gesamte Internet erstrecken müßte.

Die Ausführungen zeigen, daß eine statistische Betrachtung der netzbezogenen Kriminalität kaum möglich ist. Erst durch die Modifizierung der PKS

---

[238] Eichler, Bekämpfung der Kriminalität im Internet : Tagung beim BKA am 14./15.12.1998 mit Anmerkungen, CR 3/1999, Seite 200

könnte ein besseres Bild gewonnen werden. Bekanntlich ermöglichen die so gewonnenen Erkenntnisse nur den Blick auf das Hellfeld. Das Dunkelfeld wird durch Statistiken regelmäßig nicht erfaßt.

Da es sich bei der netzbezogenen Kriminalität um eine sehr junge Kriminalitätsform handelt, ist davon auszugehen, daß ein sehr großes Dunkelfeld existiert. Ferner werden die nachfolgenden Ausführungen zeigen, daß es sich bei dem überwiegenden Teil der Delikte um Kontrolldelikte handelt. D.h. daß die statistischen Zahlen weitestgehend von den quantitativen und qualitativen polizeilichen Ermittlungsmaßnahmen abhängen. Das bedeutet nichts anderes, als das Fallzahlen in dem Maße steigen und sinken, wie sich die Polizei im Internet engagiert. Desweiteren soll nun eine beispielhafte Darstellung möglicher Mißbrauchsmöglichkeiten des Internets erfolgen.

8.5 Mißbrauchsmöglichkeiten ausgewählter Internet-Dienste

8.5.1 Allgemeines

Von Grund auf gibt es für jeden Internet-Dienst typische Mißbrauchsvarianten, die sich aus seiner Funktionsweise und seiner Hauptaufgabe ableiten lassen[239]. Diese Mißbrauchsvarianten sollen nachfolgend exemplarisch dargestellt werden. Dabei wird kein Anspruch auf Vollständigkeit erhoben, da es sicherlich noch einige Varianten geben wird, die den Ermittlungsbehörden noch nicht bekannt sind. Bei den Mißbrauchsmöglichkeiten muß man auf der einen Seite die Möglichkeiten sehen, die auch strafrechtlich sanktioniert werden, und auf der anderen Seite Möglichkeiten, die lediglich zivilrechtlichen Charakter haben oder sich im Ordnungswidrigkeitenbereich abspielen. Bei den nachfolgenden Varianten wird insofern keine weitere Trennung vorgenommen.

8.5.2 Mißbrauch ohne Dienstbezug

Die Mißbrauchsmöglichkeiten im Internet sind vielfältig. Ein Stichwort, wenn man an Netzwerkkriminalität denkt, ist sicherlich das „Hacken“. Die Per-

---

[239] Harbort, Verbrechen im Cyberspace, Kriminalistik 3/1996, Seite 194 bis 196, bezeichnet diese Delikte als „Erscheinungsformen zeitspezifischer Computerkriminalität“; einen kurzen Abriß der Mißbrauchsmöglichkeiten auch bei: Weitemeier, Internet – Medium der Zukunft, Kriminalistik 6/1996, Seite 401 bis 405, ferner Kube, Technische Entwicklung und neue Kriminalitätsformen, Kriminalistik 10/1996, Seite 618 ff.; Janovsky, Internet und Verbrechen, Kriminalistik 7/1998, Seite 500 bis 504

sonen, die hinter dem Hacking stecken, werden oft als Hacker bezeichnet. Ursprünglich wurden als Hacker Spezialisten bezeichnet, die schwierige technische Probleme im Umgang mit Computern lösen konnten. In den letzten Jahren wird der Begriff Hacker aber zunehmend als Synonym für Internetkriminelle gebraucht, die sich darauf spezialisiert haben, in fremde Computer einzubrechen. Die Hacker selbst nennen Leute, die durch ihren Einbruch Schaden anrichten, Cracker. Der Einfachheit halber soll der Begriff Hacker an dieser Stelle aber negativ belegt bleiben[240]. An dieser Stelle müßten nun eigentlich die verschiedensten Hacking-Methoden aufgezeigt werden. Der Übersichtlichkeit wegen sollen sich die Ausführungen aber auf wenige Beispiele beschränken.

Das Internet wurde als offener Standard entworfen. Grundsätzlich werden Daten unverschlüsselt durch das Netzwerk geleitet. Dabei durchqueren sie eine Vielzahl von Rechnern, die die Daten weiterleiten (routen). Es ist also nicht verwunderlich, daß es Möglichkeiten gibt, bestimmte Datenpakete anhand ihrer Adressierung aus dem Datenstrom herauszufiltern. In diesem Zusammenhang spricht man von Monitoring oder Paket-Sniffing. Die Informationen können dann einer nicht berechtigten Person zur Kenntnis gelangen. Die Daten können verändert und dann dem Netzwerk wieder übergeben werden, allerdings liegt auch schon eine Schädigung vor, wenn die Daten nur gelesen werden (Vertraulichkeitsverlust). Aus diesen Möglichkeiten ergeben sich dann wieder neue Ansätze für kriminelle Handlungen. So kann ein Mensch systematisch erforscht werden („Der gläserne Mensch“). Erlangte Passwörter können mißbraucht werden.

„In letzter Zeit ist es für einen durchschnittlich begabten Surfer kein Problem mehr, an Programme heranzukommen, die in einfachster Weise Computer sabotieren, einen Paßwortschutz knacken oder auf einfachste Weise Daten ausspionieren. Früher war das Wissen um diese Möglichkeiten in den Händen weniger Eingeweihter.

[240] Nähere Informationen über die Subkultur der Hacker finden sich u.a. auf den Webseiten des Caos Computer Clubs: http://www.ccc.de/[06.08.2000].

Heute kann man diese Tools vom Internet laden. Selbst für die, die diese Seiten nicht finden, gibt es mittlerweile CD-ROMs auf dem Markt zu kaufen, die eine ordentliche Sammlung dieser Tools enthalten.“[241]

Immer häufiger werden Systeme auf intelligente Weise betäubt. Dies kann man erreichen, indem man z.B. unsinnige Verbindungsanfragen an einen Dienst stellt. Das hat zur Folge, daß der Server versucht, die Anfrage zu bearbeiten, was er natürlich nicht schaffen kann. Das Ergebnis ist, daß sich der Computer selbst außer Gefecht setzt, da er mit dem Rechnen beschäftigt ist. Demnach verfällt er in einen „Zustand der Bewußtlosigkeit“. In diesem Zusammenhang spricht man auch von Dazing.

Eine weitere Möglichkeit, einen Server außer Betrieb zu setzen, stellen die sogenannten Denial-of-Service-Attacks (DoS) dar[242]. Bei diesen Angriffen, die sich gegen die verschiedensten Server richten können, wird ein Rechner mit sovielen Informationen überflutet, daß er unter der Rechenlast zusammenbricht. Eine besondere Spielart des DoS wurde in der letzten Zeit angewendet, um E-Mail-Server oder IRC-Server zu sabotieren.

8.5.3 E-Mail

8.5.3.1 Netzspezifische Verbreitungsdelikte

E-Mail ist gut geeignet, bestimmte Informationen zu verbreiten. So bietet die Attachment-Funktion die Möglichkeit, an einen beliebigen Empfängerkreis Dateien zu versenden. Diese Daten können nun Töne, Bilder, Videos, Programme oder sonstige binäre Daten oder Text sein. So können pornographische Bilder oder Videos verschickt werden oder rechts- bzw. linksextremistisches Propagandamaterial. Auch eignet sich E-Mail gut zum Austausch kleinerer raubkopierter Programme, illegaler MP3-Dateien oder diverser Hacker-Tools[243].

---

[241] Jaeger, Computerkriminalität, Seite 160

[242] Einen älteren Überblick über Formen von Computermanipulationen bei: Kreitzberg, Kunstgriffe und Machenschaften, Kriminalistik 8-9/1989, S. 453 bis 458; Goldmann/Stenger, Die ganze Welt als Tatort, Kriminalistik 8-9/1989, Seite 464 bis 478.

[243] Für nähere Informationen zur Ermittlung der E-Mail-Adresse vgl. auch: Hartung, Internet, dp-special April 1998, Seite 11 und 12.

8.5.3.2 E-Mail als Mittel der Tatkommunikation

Das legale Hauptanliegen von E-Mail ist die Kommunikation mit einer anderen Person. Allerdings kann E-Mail auch zum Verabreden von Straftaten, zur Kontaktaufnahme mit potentiellen Mittätern oder zur allgemeinen Kommunikation zwischen Straftätern verwendet werden. Die Kommunikation mittels E-Mail kann durch Free-Mailer weitestgehend anonymisiert und durch den Einsatz von Verschlüsselungssoftware abgesichert werden. Der Täter ist nicht, wie bei der herkömmlichen Post, auf seinen Briefkasten oder sein Postfach angewiesen, sondern kann von jedem Internet-Café aus seine E-Mails online lesen und verfassen. Somit ist der Täter, theoretisch gesehen, vom Telefonnetz unabhängig, so daß für ihn eine Telefonüberwachung ausgeschlossen ist.

E-Mail kann u.a. zu Absprachen im Bereich der Hehlerei oder des illegalen BtM-Handels eingesetzt werden. So können über E-Mail Bestellungen aufgegeben und Übergabeorte vereinbart werden.

8.5.3.3 E-Mail als virtuelles Werkzeug

Eine besondere Bedeutung hat die E-Mail in letzter Zeit als Überträger von Computerviren und -würmern erlangt[244]. Möglich ist auch die Übertragung eines Trojanischen Pferdes auf einen fremden Computer. Diese Gelegenheit wird den Tätern ebenfalls durch die Attachments eröffnet. Mit einer E-Mail wird einfach ein ausführbares Programm versendet, daß bei leichtsinniger Ausführung durch das Opfer seine programmierten Funktionen ausführt. Je nach dem, um was für eine Art Programm es sich handelt, kommt es dann zu verschiedenen Schäden.

In der letzten Zeit hat vor allem der „I Love You“-Virus Schlagzeilen gemacht. Dieser Virus wurde als Attachment einer E-Mail versandt. Wenn ein Benutzer dieses Attachment öffnete, wurden durch den Virus einige Datei-Typen gelöscht und bestimmte Informationen an die E-Mail-Adresse des Empfängers versandt. Ferner verschickte sich der Virus selbst an 50 weitere E-Mail-Adressen des Adressbuches.

---

[244] Einen etwas älteren Beitrag, der sich mit der grundsätzlichen Funktionsweise von Viren beschäftigt, bietet: Dierstein, Gefahren für die Datenverarbeitung, Kriminalistik 8-9/1989, Seite 489 bis 516.

Dadurch kam es zu einem enormen Anstieg des E-Mail-Verkehrs in einigen Netzwerken, was zur Folge hatte, daß einige E-Mail-Server überlastet wurden und abstürzten.

Indirekt kann E-Mail somit auch zur Beeinträchtigung des Netzwerkverkehrs genutzt werden. Wird ein Server durch eine Überflutung von E-Mails gezielt außer Betrieb gesetzt, spricht man von Mail-Bombing.

E-Mail wird auch als virtuelles Werkzeug benutzt, wenn es für die Erfüllung eines Straftatbestandes zwingend erforderlich ist, daß es zu einer Kommunikation zwischen dem Täter und dem Opfer kommt. Hier ist vor allem an die Verleumdungs-, Beleidigungs- und Erpressungsdelikte zu denken, die auch mittels E-Mail begangen werden können. So ist z.B. ein Erpresserschreiben oder eine Beleidigung einer Person durch Versenden einer E-Mail möglich.

Eine E-Mail-Adresse ist eindeutig und einmalig. Allerdings ist es keine große Hürde, eine Absenderadresse einer E-Mail so zu fälschen, daß der Empfänger glaubt, von einer vertrauenswürdigen Person eine Nachricht zu erhalten. Verschlüsselung und digitale Signaturen schieben diesem kriminellen Vorgehen einen Riegel vor. Bei der Registrierung einer E-Mail werden grundsätzlich verschiedene persönliche Daten des entsprechenden Benutzers abgefragt. Bei Free-Mailern besteht die Möglichkeit, beliebige Angaben bei den persönlichen Daten zu machen. Dieses Vorgehen, welches an und für sich nicht bedenklich ist, kann allerdings für Betrugsdelikte – vor allem im Privatbereich – verwendet werden.

Ein weiteres Phänomen ist das sogenannte E-Mail-Spamming. Hierunter versteht man eine Vorgehensweise von Werbefirmen, bei der automatisch generierte Werbe-E-Mails an einen E-Mail-Server verschickt werden. Die automatische Generierung der Benutzernamen übernimmt ein Computerprogramm, welches nach bestimmten Regeln arbeitet. Die Wahrscheinlichkeit, daß eine generierte Adresse auf dem Server wirklich existiert, ist sehr hoch. Ist eine Adresse nicht vorhanden, wird die E-Mail einfach an den Empfänger (Spammer) zurückgeschickt, der diese dann automatisch löscht. Zu vergleichen ist Spamming mit einer Postwurfsendung, die beispielsweise in einer Straße an jeden Haushalt zugestellt wird. Die Folge einer Spamm-Aktion kann die Überlastung eines E-Mail-Servers sein, der dann seinen ordnungsgemäßen Betrieb nicht mehr fortsetzen kann.

Spamming ist keine Form des E-Mail-Bombing, da das Ziel des Spammers Werbung ist und nicht die Sabotage eines E-Mail-Servers.

Im Gegensatz zum Spamming, das vor allem den Systembetreiber schädigt, richten sich Junk-E-Mails direkt an den Benutzer, der mit den Werbe-E-Mails eingedeckt wird. Eine Junk-E-Mail kann Folge eines Spammings sein, sich aber gezielt auch nur an einen Benutzer richten. Junk-E-Mail kann beispielsweise die Folge eines illegalen Austauschs von Kundendaten zwischen Firmen – natürlich gegen ein Entgeld – sein.

8.5.4 News

8.5.4.1 Netzspezifische Verbreitungsdelikte

Das Usenet bietet eine Plattform für die unterschiedlichsten extremistischen Gruppierungen. Die Betonung liegt hierbei auf Gruppierungen, da die Kommunikation zwischen zwei einzelnen Menschen innerhalb einer Newsgroup recht unbequem ist. Die Newsgroups sind gerade für Gruppendiskussionen ausgelegt[245]. Hierbei kann es sich vor allem um recht- und linksextremistische Gruppen, aber auch religiöse Vereinigungen handeln. Auch für die verschiedensten Sekten kann das Usenet interessant sein. Eine besondere Bedeutung genießt hierbei die Top-Level-Hierarchie „alt“, in der alternative Newsgroups angeboten werden. Unter diesem Top-Level finden sich oft Gemeinschaften aus Extremisten und Pädophilen.

„Heute gibt es rund 35.000 [...] Newsgroups [...], von denen rund 27.000 sich um das Thema Sex drehen. Ein Großteil davon dient als Kontakt und Tauschbörse für perverse Sadisten und Pädophile. Da werden Bilder gepfählter Körper und Tips für Mißbraucher ausgetauscht oder [...] ungeschminkt Kontakte zu Kindern oder solchen Kriminellen gesucht, die Kontakt zu Minderjährigen herstellen können.“[246] Wer nicht selbst nach einer „speziellen“ Newsgroup suchen will, kann auch einen besonderen Dienst nutzen, der diese Arbeit übernimmt.

---

[245] Für nähere Informationen über die Ermittlung von Newsgroups vgl. auch: Hartung, Internet, dp-special April 1998, Seite 12.

[246] Drewes, Die Kindersexmafia und ihre unsichtbaren Kanäle, Seite 88

„Wer diese Art von Service in Anspruch nimmt (einer davon wirbt mit dem Hinweis, aus 435 verbotenen Newsgroups täglich eine halbe Millionen Fotos herauszukramen und sortiert bereitzustellen), bekommt in einer Bilder-Galerie fein säuberlich aufgelistet, was die perverse Welt so täglich alles hergibt: Fäkalien-Sex, Folterungen, Qualen, schreiende und verzerrte Gesichter, geschundene Körper.“[247]

Eine Besonderheit der Usenet Newsgroups besteht in der Möglichkeit, eine Datei an eine Nachricht anzuhängen. Da hierbei die gleichen Regelungen wie bei der E-Mail gelten, ergeben sich auch die gleichen Mißbrauchsmöglichkeiten. So ist es nicht selten, daß in Newsgroups mit kinderpornographischem Hintergrund entsprechendes Bildmaterial an die News angehängt wird.

Das wohl bekannteste Beispiel in diesem Bereich stellte das Verfahren gegen den deutschen CompuServe-Chef Felix Somm dar. Diesem wurde vorgeworfen, pornographische Schriften gemäß § 184 III StGB verbreitet zu haben. In erster Instanz wurde Somm verurteilt, obwohl sowohl die Staatsanwaltschaft als auch die Verteidigung für eine Freisprechung plädiert hatten. In zweiter Instanz wurde Somm freigesprochen. Anstoßpunkt der Ermittlungen war die Existenz von ca. 200 Newsgroups auf dem Zentralrechner der amerikanischen CompuServe Inc mit kinder-, gewalt- und tierpornographischen Inhalten. Die Anklage richtete sich gegen den Geschäftsführer der deutschen CompuServe GmbH – Felix Somm. Ihm wurde vorgeworfen, deutschen CompuServ-Kunden den Zugang zu den amerikanischen Newsgroups ermöglicht zu haben. Da CompuServe Deutschland aber keine objektiven Einwirkungsmöglichkeiten auf die Inhalte der amerikanischen Server hatte, lehnte das Gericht eine Mittäterschaft und eine Garantenpflicht ab. Dem Angeklagten konnte kein Vorsatz nachgewiesen werden[248].

8.5.4.2 News als Mittel der Tatkommunikation

Betrachtet man das Usenet als Plattform für bestimmte Gruppierungen, sieht man sehr deutlich, wie die Grenzen zwischen Informationsverbreitung und Kommunikation verlaufen. Zum einen wird das Usenet als Informationspool für

---

[247] ebd., Seite 93

[248] nähere Ausführungen zu den rechtlichen Fragestellungen erfolgen an anderer Stelle

potentielle Einsteiger genutzt, aber auch zur Kommunikation innerhalb der Gruppe. Das Usenet ist auch ein beliebter Anlaufpunkt für Hacker und Softwarepiraten[249]. Hier werden Tips und Tricks ausgetauscht und illegale Informationen angeboten.

In Newsgroups werden nicht nur pornographische Schriften verbreitet, sondern auch entsprechende Tips gegeben (u.a. auch Reisetips für Sextouristen) und Taten verabredet bzw. geplant. So berichtet Jaeger von folgendem Fall: „Vor einiger Zeit erregte der Fall eines Ehepaares Aufsehen, das über elektronische Anzeigen Kinder zum Mißbrauch anbot. Man könne, so das Ehepaar, gegen einen Aufpreis auch für die Beseitigung der Leichen sorgen.“[250]

Drewes berichtet u.a. von folgenden Fällen: „Die Newsgroups haben sich längst zu einer Drehscheibe für alle Perversitäten dieser Welt entwickelt. Auch wenn längst nicht jede Mitteilung dort ernstzunehmen ist, weil sich offenbar einige verquere Hirne einen besonderen Spaß daraus machen, Usern mit ausgefallenen Anfragen ein[zu]heizen (`Suche Kannibale, der Lust auf männliches Fleisch hat. Biete weibliches Fleisch zum Nachtisch´), offenbaren doch eine Vielzahl der dort veröffentlichten Nachfragen die wachsende Gewaltbereitschaft nicht zuletzt der Deutschen. So suchte Anfang 1998 ein `Mann, 30, aus Frankfurt/Main einen Sadisten, um mit ihm am Wochenende auf Rape-(Vergewaltigungs-)Tour zu gehen´.“[251]

8.5.4.3 News als virtuelles Werkzeug

Eine Mißbrauchsmöglichkeit der News als virtuelles Tatwerkzeug ist bisher nicht bekannt und aufgrund der technischen Gestaltung des Dienstes auch nicht wahrscheinlich.

---

[249] Allerdings darf die illegale Mailboxszene nicht vergessen werden.
[250] Jaeger, Computerkriminalität, Seite 170
[251] Drewes, Die Kindersexmafia und ihre unsichtbaren Kanäle, Seite 89

8.5.5 Telnet

8.5.5.1 Netzspezifische Verbreitungsdelikte

Grundsätzlich ist Telnet dazu geeignet, Clientprogramme auf einem Host fernzusteuern. Dadurch ist es möglich, mittels Telnet alle netzspezifischen Verbreitungsdelikte durchzuführen, die mit allen anderen Clients auch möglich sind.

8.5.5.2 Telnet als Mittel zur Tatkommunikation

Telnet kann für die Tatkommunikation genutzt werden. So ist es möglich, daß ein Täter mit einem Telnet-Programm auf den Host eines anderen Täters zugreift und sich die beiden Personen auf dem entsprechenden Rechner per Tastatur „unterhalten“ können.

8.5.5.3 Telnet als virtuelles Werkzeug

Telnet ist im besonderen Maße als virtuelles Tatwerkzeug geeignet, da seine Hauptfunktion in der Fernbedienung eines Hosts liegt. Erlangt ein Täter mittels Telnet Zugriff auf einen Host, kann er alle Funktionen ausführen, die auch der Berechtigte ausführen könnte. So kann er z.B. Informationen aus vertraulichen Datenbeständen wahrnehmen, verändern, löschen oder stehlen.

8.5.6 FTP

8.5.6.1 Netzspezifische Verbreitungsdelikte

Die Hauptfunktion von FTP besteht im Austausch von Daten. Diese Daten können beliebigen Charakters sein. Extremistische Gruppierungen, die einen FTP-Server unterhalten, ermöglichen Gleichgesinnten den Download von Propagandamaterial etc. So existieren FTP-Adressen, von denen beispielsweise Anleitungen zum Bau von Bomben, zum Hacken von Rechnern oder zum Herstellen von Drogen herunterzuladen sind. FTP ermöglicht auch die Verbreitung

pornographischer Bilder oder Videos[252]. Nicht zu vergessen ist die Szene der Raubkopierer, der Virenprogrammierer oder der Hacker, die FTP zum Vertrieb ihrer „Produkte“ ebenfalls nutzen können.

So wird eine Vielzahl der raubkopierten Software auf FTP-Servern zum Download angeboten. Teilweise muß ein Benutzer vor dem Download erst den Upload eigener illegaler Software durchführen. Diese Vorgehensweise wurde von den Softwarepiraten der Mailboxszene übernommen.

8.5.6.2 FTP als Mittel zur Tatkommunikation

Wenn ein FTP-Server betrieben wird, kann er im Grunde die gleichen Funktionen wie ein News-Server übernehmen. So wäre es möglich, daß z.B. eine extremistische Gruppierung einen eigenen FTP-Server unterhält. Dieser FTP-Server kann dann in mehrere Bereiche aufgeteilt werden. So könnte sich ein Bereich mit allgemeinen Informationen zur Gruppe befassen, ein anderer Bereich könnte indizierte Spiele zum Download anbieten und in einem weiteren Bereich könnten die einzelnen Berechtigten Nachrichten in Form von Dateien ablegen. Jeder Berechtigte kann somit Nachrichten hinterlassen und Nachrichten abrufen. Ferner besteht auch die Möglichkeit, für jeden Berechtigten ein eigenes Verzeichnis anzulegen. In dem Sinne könnte der FTP-Server als Art virtuelles Postfach umfunktioniert werden. Der Zugriff auf diesen Server kann dann mittels personal FTP beschränkt werden.

8.5.6.3 FTP als virtuelles Tatwerkzeug

Als virtuelles Tatwerkzeug kann FTP z.B. dazu eingesetzt werden, Datenbestände auf einem Server zu manipulieren. Hierzu muß der Täter natürlich die entsprechenden Rechte zum Löschen oder Verändern von Dateien besitzen. Hat er diese Rechte - z.B. durch erfolgreiche Manipulationen - erlangt, sind seinem Handeln natürlich keine Grenzen gesetzt.

Eine Besonderheit ergibt sich aus der Verbindung von FTP und WWW. Meist werden die Websites offline erstellt und dann mittels FTP auf einen FTP-Server des jeweiligen Anbieters geladen. Von dort werden sie dann in regel-

[252] An dieser Stelle sollte immer bedacht werden, daß das Internet wie eine „zweite Festplatte“ benutzt werden kann.

mäßigen Abständen auf den WWW-Server geladen, der die Websites dann der Öffentlichkeit zugänglich macht. Wenn ein Täter Zugriff auf den FTP-Account eines Anbieters hat, kann er diesen erheblich schädigen, indem er dessen Websites verändert. In diesem Zusammenhang spricht man von Website-Hacking[253].

8.5.7 IRC

8.5.7.1 Netzspezifische Verbreitungsdelikte

Eine besondere Funktion des IRC ermöglicht den Austausch von Daten zwischen zwei Benutzern, die sich in einem Channel befinden. Diese Funktion baut auf der E-Mail-Kommunikation auf, so daß sich die gleichen Mißbrauchsmöglichkeiten wie bei E-Mail ergeben. So sind unter anderem Fälle bekannt, in denen junge Mädchen in diversen Chats in der Form belästigt wurden, daß ihnen unaufgefordert kinderpornographische Bilder zugeschickt wurden. Über eine besondere Funktion des IRC – DCC (direct client to client) – können beliebige Daten, also Bilder, Videos oder illegale Software, direkt zwischen zwei Benutzern ausgetauscht werden.

Jofer berichtet von folgendem Fall: „Diese Erfahrung [im Chat] machte beispielsweise Barry F. Crimmins, ein amerikanischer Autor, der sich unter einem Pseudonym in virtuellen Chat-Rooms des Serviceproviders AOL aufgehalten hatte.

Crimmins gab vor, ein 12jähriges Mädchen zu sein und hielt sich in den Member-Rooms von AOL auf. In den Member-Rooms mit den Bezeichnungen wie `DadsNDoughters´ oder `lilboypix´ wurden Bilder mit Kinderpornographie und allen erdenklichen Formen von Pornographie (von Sex mit Teens bis hin zu Kleinkindern) getauscht. In der Folgezeit wurden ihm Tausende von Bildern unaufgefordert zugesandt […].“[254]

---

[253] Im Internet gibt es verschiedene Homepages, die solche gehackten Websites zeigen; der Imageverlust für das betroffene Unternehmen kann sehr groß sein.

[254] Jofer, Straftaten im Internet, Seite 57 und 58

8.5.7.2 IRC als Mittel zur Tatkommunikation

Die Hauptfunktion des IRC besteht in der Zurverfügungstellung einer Kommunikationsplattform. Daher kann es von Straftätern umfassend für deren Zwecke genutzt werden. So kann man im IRC Straftaten verabreden oder tatrelevante Informationen austauschen. Ferner besteht auch die Möglichkeit, weitere Gesinnungsgenossen zu treffen. Dies gilt insbesondere auch für die extremistischen Gruppierungen, die Pädophilen- oder die Hackerszene, obwohl sich die Hacker meistens auf das Usenet oder eigene Mailboxen beschränken.

Das IRC ist im besonderen Maße für die Tatkommunikation geeignet, da es verschiedene Arten der Anonymisierung unterstützt und auch verdeckte Kommunikation (z.B. durch Anflüstern oder die Benutzung eines Separées) ermöglicht. Den vollen Zugriff zu einem Channel kann nur der Systembetreiber erlangen. Ferner besteht auch die Möglichkeit, daß eine Gruppierung einen eigenen IRC-Server betreibt, der dann nur für einen bestimmten Benutzerkreis geöffnet wird, der sich mit Benutzernamen und Paßwort authentifizieren muß. Auf einem solchen Server kann dann die volle Breite der Tat- und Täterkommunikation ablaufen.

Drewes führt folgendes Beispiel für typische IRC-Dialoge aus dem sexistisch-pornographischen Bereich an: „[...] die meisten der auch besonders perversen Dialoge [verlaufen] stets gleich. Nach spätestens 10, 15 Minuten wird nach realen Kontakten gefragt und dann werden Adressen, Telefonnummern, Tips ausgetauscht: [beispielsweise] vom Bordell nahe der tschechischen Grenze, das von Russen betrieben werde, die dort junge und sehr junge behinderte tschechische Frauen für extremste Folterspiele offerieren (`Ich habe der Blinden Rasierschaum in die Augenhöhlen gespritzt.

Die hat geschrieen wie am Spieß!´) bis hin zu realen Vermittlungen von Kindern aus dem Ostblock oder Asien“[255].

Das IRC wird auch von der Raubkopiererszene genutzt. So werden im Chat Download-Adressen für raubkopierte Software ausgetauscht und entsprechende Zugriffspasswörter bekanntgegeben.

---

[255] Drewes, Die Kindersexmafia und ihre unsichtbaren Kanäle, Seite 91

8.5.7.3 IRC als virtuelles Tatwerkzeug

Das IRC bietet für einen Straftäter die Möglichkeit, direkt mit neuen potentiellen Opfern in Kontakt zu treten. So werden z.B. Kinder gezielt von Pädophilen angesprochen. Oft sind auch die verschiedenen extremistischen Gruppierungen im IRC vertreten. Der Umgangston auf einem IRC-Server kann von Channel zu Channel sehr unterschiedlich sein. Es ist keine Seltenheit, daß ein Benutzer durch einen anderen gröblichst beleidigt wird. Der IRC reguliert sich zwar weitestgehend selbst, indem der Störenfried z.B. durch den Operator aus dem Channel verwiesen wird, dennoch kommt es oft zu ausufernden verbalen Attacken gegen Chatter. Einem ausgeschlossenen Benutzer ist es durch verschiedene Tricks möglich, erneut Zugang zu einem Channel zu erlangen, aus dem er zuvor ausgeschlossen wurde.

Daß die Benutzung des IRC auch reale Bedrohungen nach sich ziehen können, veranschaulicht Jofer[256]. Er berichtet von einem Fall, bei dem ein 15jähriges Mädchen von einem männlichen Täter durch einen Trick dazu gebracht wurde ihren Namen preiszugeben. In der Folge wurde das Mädchen wiederholt verbal durch den Täter belästigt und sogar zu Hause aufgesucht.

Eine weitere beliebte Variante, das IRC als virtuelles Tatwerkzeug zu mißbrauchen, stellen die sogenannten „WARBOTS“ dar. Hierbei nutzen die Täter eine Skripting-Funktion des IRC-Clienten, mittels dessen immer wieder auftretende Eingaben automatisiert werden können. Durch die Anwendung dieser Robots (BOTS) ist es möglich, einen IRC-Server dermaßen zu belasten, daß seine Funktionsweise stark eingeschränkt wird. Dies hat zur Folge, daß ein IRC-Server wertvolle Rechenkapazität aufwenden muß und dadurch die Gesamtperformance des Systems leidet.

8.5.8 Iphone

8.5.8.1 Netzspezifische Verbreitungsdelikte

Grundsätzlich ist Iphone nicht dazu geeignet, bestimmte Informationen (die ja in einer gewissen nichtflüchtigen Form vorliegen müssen) im Internet zu

---

[256] Jofer, Strafverfolgung im Internet, Seite 58

verbreiten. Das wird deutlich, wenn man das Iphone mit einem realen Telefon vergleicht. Ausschließlicher Zweck des Dienstes ist die Übertragung von flüchtigen Daten – der menschlichen Sprache.

8.5.8.2 Iphone als Mittel zur Tatkommunikation

Iphone hat zur Zeit ausschließlich für den Bereich der Tatkommunikation eine praktische Relevanz. Die Technik ist im besonderen Maße geeignet, da die analoge Sprache in digitale Daten umgewandelt wird. Diese Daten, die als Pakete durch das Netzwerk verschickt werden, können verschlüsselt werden, so daß Iphone eine abhörsichere Kommunikationsmöglichkeit eröffnet. Die Anwendung ist zwar noch nicht so komfortabel wie die Benutzung des herkömmlichen Telefons, dennoch stellt sie für Täter, die über eine entsprechende gute Internetanbindung verfügen, eine preisgünstige und vor allem sichere Variante dar. Da die Iphone-Technik noch in den Kinderschuhen steckt, bleibt abzuwarten, welche weitere praktische Relevanz sie für die Zukunft haben wird.

8.5.8.3 Iphone als virtuelles Werkzeug

Eine Mißbrauchsvariante der Iphone-Technik als virtuelles Werkzeug ist nach dem heutigen Stand der Technik noch nicht ersichtlich. Eine mögliche Variante wäre sicherlich – wie auch beim herkömmlichen Telefonnetz - das Bestreben bestimmter Personen, kostenlos zu telefonieren. Da aber Iphone nicht an das Telefonnetz gebunden ist, reicht für das kostenlose Telefonieren über VoIP auch ein kostenloser Internetzugang aus, den man z.B. auch durch die illegale Benutzung fremder Zugangsdaten (Accounts) erlangen kann.

8.5.9 WWW

8.5.9.1 Netzspezifische Verbreitungsdelikte

Wie bereits im technischen Teil der Arbeit dargestellt wurde, stellt das WWW im Grunde eine graphische Benutzeroberfläche dar, die einen eigenen neuen Dienst (WWW) mit den konventionellen Diensten des Internets verknüpft. Im Grunde bietet das WWW durch seine Hypertext-Eigenschaft die Möglichkeit auf die unterschiedlichsten Dienste zuzugreifen. Somit werden

auch die kriminellen Mißbrauchsmöglichkeiten, die sich innerhalb der einzelnen Dienste ergeben, auf das WWW übertragen. So kann ein Link z.B. auf eine Newsgroup verweisen, in der mit pornographischen Bildern gehandelt wird oder in der extremistische Gruppierungen ihre Gesinnungen verbreiten. Allerdings kann ein Link auch auf eine FTP-URL verweisen, unter der ein Hackertool oder ein Virus erhältlich ist. Die Möglichkeiten sind also vielfältig.

Im WWW sind eine Vielzahl von „Sexshops“ zu finden. Hier kann der potentielle Kunde häufig erst einen Zugang erlangen, wenn er durch die Angabe seiner Kreditkartennummer einen bestimmten Betrag auf das Konto des Betreibers überwiesen hat. Dann erhält er ein ZugangsPaßwort, welches ihm den Zugriff auf das Angebot ermöglicht. „Zwar sind die Passwörter gegen Kreditkarte durchaus ein Mittel, sich ungebetene Gäste fernzuhalten. Wer kann es sich schon leisten, Monat für Monat mehrere Sexshops für je 100 Dollar zu besuchen? So hat sich denn auch längst ein Schwarz – und Tauschmarkt rund um Passwörter gebildet: [...] An anderen Stellen lagern seitenweise Listen mit Passwörter für die besonders perversen Ecken, in denen gepeitscht, gestochen, mit Fäkalien beschmiert und verstümmelt wird. Auch deutsche Anbieter mischen da längst fleißig mit. Einige werben gar außerhalb dieser Republik mit dem vielsagenden Hinweis `In Deutschland indiziert´“[257]. Trotz dieser Möglichkeiten gibt es im WWW nur verhältnismäßig wenig strafbare Inhalte, da die ständig abrufbereiten Seiten ein gewisses Entdeckungsrisiko bedeuten[258]. Auch neue WWW-Techniken machen sich Straftäter sehr schnell zunutze.

Ein Beispiel dafür ist die Entwicklung der Web-Cam-Technik. Hierbei wird eine sogenannte Web-Cam[259] installiert, die dann Bilder ins Internet sendet. Diese Bilder können dann in einem einstellbaren Zeittakt auf einer Website angezeigt werden. „Die vergleichsweise harmlose Variante dabei ist die Internet-Peep-Show. Dabei rekelt sich eine junge Frau vor einer solchen Live-Kamera, die über ihrem Computer montiert ist. Der User bekommt das Bild über eine Internet-Adresse auf seinen Monitor und kann nun der Frau per Tastatur Anweisungen geben, was sie tun soll. Daß diese Technik auch für den Kindes-

---

[257] Drewes, Die Kindersexmafia und ihre unsichtbaren Kanäle, Seite 88

[258] Für nähere Informationen über die Ermittlung von WWW-Adressen vgl. auch: Hartung, Internet, dp-special April 1998, Seite 12.

[259] Hierbei handelt es sich um eine Kamera, die direkt mit dem PC verbunden wird und aufgenommene Bilder an diesen sendet.

mißbrauch genutzt wird, wurde lange vermutet, aber nie bewiesen. Bis die amerikanische Bundespolizei einen solchen Fall aufdeckte. Der User saß auf einem Kontinent und konnte über Internet-Leitung (also anonym) mitverfolgen, wie ein Mißbraucher in einem anderen Kontinent vor der Live-Kamera ein Kind nach den Anweisungen per Bildschirm vergewaltigte.“[260]

Das Erstellen von Webseiten mittels HTML eröffnet für die verschiedenen Gruppierungen auch die Möglichkeit, sich im Internet zu präsentieren. So enthalten extremistische Homepages oft strafbare Äußerungen etc. Ferner besteht die Möglichkeit, Links auf solche Webseiten zu setzen, die strafbare Inhalte anbieten. Da in Deutschland sehr restriktiv mit rechts- und linksextremistischer Propaganda umgegangen wird, werden die Inhalte oft auf Server ausländischer Staaten gespiegelt. Auf den extremistischen Websites wird aber nicht nur Propaganda betrieben, u.a. findet sich im Thule-Netz eine Übersicht von Antifa-Organisationen[261] nebst Namen, Adressen und Telefonnummern.

Ein gutes Beispiel für den Mißbrauch des WWW für linksextremistische Propaganda, ist der XS4ALL (Access for All)-Fall. Hierbei wird unter der niederländischen Internetadresse http://www.xs4all.nl/[06.08.2000] die in Deutschland verbotene Zeitschrift „Radikal“ angeboten. Durch diese Zeitschrift wurde u.a. ein Leitfaden zur Behinderung von Bahntransporten herausgegeben. In diesem Zusammenhang wurden auch bereits erfolgreiche Sabotageakte beschrieben[262].

Ein Beispiel für rechtsextremistische Aktivitäten ist der Zündel-Fall. Ernst Zündel ist ein Deutschkanadier und ein führender Verleugner des Holocausts. 1995/96 wurde im amerikanischen WWW eine Website – Zuendelsite – eingerichtet. Leider konnten die deutschen Behörden nicht an den amerikanischen Server heran, um einen weiteren Zugriff auf die Zuendelsite zu unterbinden[263].

Auch Scientology oder radikale islamistische Vereinigungen sind im Internet vertreten. Allerdings sind die frei zugänglichen Bereiche der Websites oft strafrechtlich nicht zu beanstanden. Auch die offiziellen Auftritte der rechts-

---

[260] Drewes, Die Kindersexmafia und ihre unsichtbaren Kanäle, Seite 94
[261] http://www.thulenet.com/texte/adressen/text0004.htm[06.08.2000]
[262] Für nähere Informationen vgl.: Jofer, Straftaten im Internet, Seite 61 und 62.
[263] Für nähere Informationen vgl.: ebd., Seite 62 und 63.

und linksextremistischen Organisationen sind weitestgehend beanstandungsfrei.

Es besteht im WWW nicht nur die Möglichkeit, an Anleitungen zum Bau von Bomben oder für Sabotageakte zu gelangen. Das WWW bietet weiterhin detaillierte Informationen über Genexperimente oder die Herstellung von Drogen. Unter Verwendung des WWW läßt sich sogar ein gut funktionierendes Netzwerk für den illegalen Handel mit Betäubungsmitteln aufbauen.

Eine weitere Möglichkeit, das WWW zu mißbrauchen, stellen die verschiedenen ehrverletzenden Delikte dar. So gibt es Fälle, in denen auf Websites Nacktaufnahmen oder entstellte Fotos von Personen der Zeitgeschichte zu sehen sind. Ferner gehen die Täter sogar so weit, daß gefälschte Pressemitteilungen in Umlauf gebracht werden. Einen Fall, bei dem der Tod des griechischen Premierministers Andreas Papandreou behauptet wurde, führt Jofer an[264]. Ferner sind Websites bekannt, auf denen beispielsweise über unliebsame Vorgesetzte berichtet wird und diese auf das gröblichste beleidigt werden. Auch gibt es Homepages auf denen sogenannte „Spannerfotos“ zu sehen sind.

8.5.9.2 Das WWW als Mittel zur Tatkommunikation

An dieser Stelle ist vor allem auf die Einbindung von E-Mail, IRC und Usenet in das WWW zu achten. Demnach ergeben sich die gleichen Mißbrauchsvarianten wie bei den speziellen Diensten. Besonders ist auf das Gateway- und Formularkonzept des WWW hinzuweisen, was in der Verbindung mit CGI neue Mißbrauchsmöglichkeiten eröffnet, da hierdurch auch der Zugriff auf Dienste oder Anwendungen möglich ist, die nicht dem Internetstandard zugerechnet werden.

Das WWW eignet sich gut dazu, in Verbindung mit E-Mail und IRC, z.B. Verteilernetze für Hehlereigut und illegale Betäubungsmittel aufzubauen.

8.5.9.3 Das WWW als virtuelles Tatmittel

Da das WWW Zugriff auf die gängigsten Internet-Dienste gewährt, ist es grundsätzlich auch für den Einsatz als virtuelles Tatmittel geeignet. Die Mög-

---

[264] Jofer, Straftaten im Internet, Seite 72

lichkeiten des jeweiligen Browsers richten sich dabei nach den Fähigkeiten seiner entsprechenden Helper-Applications. Allerdings vermag kaum ein Browser, die umfassenden Funktionsmerkmale eines speziellen Client-Programmes nachzubilden. Daher ist die Verwendung des WWW als virtuelles Tatmittel recht unwahrscheinlich.

Eine Variante, das WWW direkt als virtuelles Tatmittel zu mißbrauchen, stellt die widerrechtliche Verwendung der sogenannten META-Tags dar. Diese META-Tags enthalten u.a. Stichworte, unter denen die Seite in ein Verzeichnis oder in einem Suchdienst aufgenommen wird. Es wurden wiederholt Fälle bekannt, in denen Firmen in die META-Tags ihrer Webseiten bekannte Markennamen geschrieben haben. Das hat zur Folge, daß ein Benutzer, der einen solchen Namen in eine Suchmaschine eingibt, die entsprechende Firma mitangezeigt erhält. Durch diese Vorgehensweise kann eine Firma einen rechtswidrigen Wettbewerbsvorteil gegenüber dem eigentlichen Berechtigten erlangen. Auch wurden Namen von zumeist attraktiven weiblichen Hollywoodstars dazu benutzt, interessierte Benutzer auf Seiten mit sexuellem Hintergrund zu locken.

Eine neuere Form des WWW-Mißbrauchs stellt das Hacken von Websites bekannter Firmen oder Organisationen dar. Hierbei dringen Hacker in einen WWW-Server (oder FTP-Server – siehe auch dort) ein und verändern die abgespeicherten Websites eines Opfers. Der Öffentlichkeit bietet sich dann beim Aufruf der gehackten Internetadresse oft eine vollkommen entstellte Ansicht, die geeignet ist, den Ruf des jeweiligen Opfers enorm zu schädigen. Es existieren auch Adressen im Internet, unter denen man gehackte Websites betrachten kann. Ein bekanntes Opfer ist beispielsweise der Flugzeughersteller Boeing.

9 Strafverfolgung im Internet

9.1 Grundlagen des materiellen Strafrechts

9.1.1 Allgemeines

Dieser Abschnitt beschäftigt sich mit den Grundlagen des Strafrechts im Bereich des Internets[265]. Er behandelt vor allem die durch das Internet neu hervorgebrachten Probleme im allgemeinen Teil des Strafgesetzbuches (StGB). Ferner werden die für den Bereich des Internets relevanten Gesetze und Verordnungen vorgestellt und ihr Praxisbezug erläutert. Die nachfolgenden Ausführungen sollen vor allem die Fragen hinsichtlich der Anwendbarkeit des deutschen Strafrechts, der Verantwortlichkeit der Provider im internationalen Datenverkehr, der Verantwortlichkeit jedes einzelnen Internet-Nutzers und der Anwendbarkeit des herkömmlichen Schriftenbegriffs beantworten.

9.1.2 Territorialitäts -, Ubiquitäts -, Weltrechts – und Personalitätsprinzip

Grundsätzlich regeln die §§ 3 [Geltung für Inlandstaten], 4 [Geltung für Taten auf deutschen Schiffen und Luftfahrzeugen], 5 [Auslandstaten gegen inländische Rechtsgüter], 6 [Auslandstaten gegen international geschützte Rechtsgüter], 7 [Geltung für Auslandstaten in anderen Fällen] und 9 [Ort der Tat] StGB den räumlichen Geltungsbereich des deutschen Strafrechts[266]. Die Bestimmung des räumlichen Geltungsbereiches unseres Strafrechts für eine bestimmte Tat ist unbedingt erforderlich. Gelten die Vorschriften des deutschen Strafrechts für eine Tat nicht, handelt es sich um ein Prozeßhindernis, in dessen Folge die Tat nicht verfolgt werden darf.

Für den Bereich des Internets ist § 4 StGB weitestgehend ohne Bedeutung. Mit der Auslegung der anderen Paragraphen mußte und muß sich immer noch sowohl die Rechtsprechung, als auch die juristische Fachliteratur ausein-

---

[265] Eine kürzere Darstellung (auch strafprozeßrechtlicher Fragen) u.a. bei: Heinzmann/Ochsenbein, Strafrechtliche Aspekte des Internet, Kriminalistik 7/1998, Seite 513 bis 520, Kriminalistik 8-9/1998, Seite 599 bis 606; Ochsenbein, Strafrechtliche Aspekte des Internet, Kriminalistik 10/1998, Seite 685 bis 688.

[266] Das deutsche Strafrecht setzt sich aus dem StGB und einer Reihe verschiedener Nebengesetze, die ebenfalls Strafvorschriften enthalten (z.B.: Versammlungsgesetz oder Waffengesetz), zusammen; der allgemeine Teil des StGB bezieht sich hierbei ebenfalls auf diese Nebengesetze.

andersetzen. Mithin muß festgestellt werden, daß der Prozeß der rechtlichen Bewertung des Phänomens Internet noch nicht abgeschlossen ist. In regelmäßigen Abständen kommt es zu neuen Urteilen, die es bei der polizeilichen Arbeit zu beachten gilt. Die nachfolgenden Ausführungen sollen sich vor allem auf den Bereich der netzspezifischen Verbreitungsdelikte beziehen.

Es ist allgemein bekannt, daß das Internet nicht vor Ländergrenzen halt macht. Nicht umsonst spricht man davon, daß durch das Internet die Länder näher zusammengerückt sind und die Welt kleiner geworden ist. Das Strafrecht bezieht sich weitestgehend auf ein bestimmtes Territorium, nämlich auf ein bestimmtes Hoheitsgebiet eines Staates. Die Besonderheit von Straftaten im Internet ist, daß sie – ähnlich der organisierten Kriminalität – nicht vor Ländergrenzen halt machen. Nahezu alle Delikte haben somit in irgendeiner Weise Auslandsbezug.

§ 3 StGB legt den räumlichen Geltungsbereich des StGB für Inlandstaten fest. In diesem Zusammenhang spricht man vom Territorialprinzip. Das Territorialprinzip knüpft an der Tatsache an, daß das Strafrecht primär den Schutz inländischer Rechtsgüter bezweckt. Gibt also ein Täter die Daten im Inland ein, werden sie auf einem inländischen Server gespeichert und können die Daten auch im Inland abgerufen werden, ist eindeutig § 3 StGB anzuwenden. Fällt eine dieser Bedingungen weg, ist § 3 StGB unanwendbar. Grundsätzlich muß im Bezug zum Internet eine Bedingung wegfallen, da der Täter nicht bestimmen kann, wer seine Daten abruft. Es existieren keine technischen Möglichkeiten, bestimmte Staaten von einem Informationsangebot auszuschließen.

Durch § 9 StGB wird das Territorialprinzip des § 3 StGB durch das sogenannte Ubiquitätsprinzip ergänzt. Dieses besagt, daß der Tatort sowohl der Ort sein kann, an dem gehandelt wurde, als auch der Ort, an dem der Erfolg eingetreten ist oder nach den Vorstellungen des Täters eintreten sollte.

Durch § 5 StGB wird das Territorialprinzip ebenfalls durchbrochen, da der Schutzbereich des StGB auch auf enumerativ aufgezählte Straftaten erweitert wird, wenn sie im Ausland begangen werden. Geschützt sind hier vor allem hochwertige Rechtsgüter des Staates.

Desweiteren schützt § 6 StGB internationale Rechtsgüter durch die abschließende Auflistung weiterer Straftaten, für die ebenfalls das deutsche Straf-

recht gilt. In diesem Zusammenhang spricht man vom Weltrechts- oder Universalprinzip. Von besonderer Bedeutung für die vorliegende Problematik ist hierbei § 6 Nr. 6 StGB, der die Verbreitung pornographischer Schriften in den Fällen des § 184 III StGB unter das Weltrechtsprinzip stellt. Gemeint ist hierbei die Verbreitung sogenannter harter Pornographie - also Darstellungen im Zusammenhang mit Gewalttätigkeiten, sexuellem Mißbrauch von Kindern oder sodomistische Handlungen. Durch § 6 Nr. 6 StGB wird mithin nur dieser spezielle Bereich der netzspezifischen Kriminalität abgedeckt.

§ 7 StGB enthält das sogenannte aktive und passive Personalitätsprinzip, durch welches Auslandstaten in den Fällen durch deutsche Gerichte verfolgt werden können, in denen sie sich gegen einen Deutschen richten und der Täter am Tatort strafbar ist, oder keine Strafgewalt vorhanden ist. Die zweite Konstellation bezieht sich ebenfalls auf solche Auslandstaten. Hierbei kann der Täter aber erst Deutscher werden, Deutscher gewesen sein oder Ausländer sein, der nicht ausgeliefert wurde. Die zweite Alternative ist für den Bereich der Internetstraftaten weitestgehend ohne Bedeutung.

9.1.3 Der Tatortbegriff nach § 9 I StGB

Gemäß § 9 I StGB werden grundsätzlich zwei Varianten des Tatortes unterschieden: der Handlungsort (Ort, an dem der Täter gehandelt hat) und der Erfolgsort (Ort an dem der Erfolg eingetreten ist). Im Sinne der ersten Alternative muß man noch einmal zwischen Handeln und Unterlassen unterscheiden, d.h. daß nicht nur aktives Tun bestraft wird, sondern auch nicht ausgeführte, gebotene Handlungen. Die zweite Alternative (Erfolgsort) wird ebenfalls noch einmal unterschieden. Der Tatort kann somit auch der Ort sein, an dem der Erfolg eingetreten ist oder nach den Vorstellungen des Täters hätte eintreten sollen.

Werden die Daten auf einem inländischen Server geladen, handelt der Täter im Inland, da der Serverstandort entsprechend den Tatort begründet. Unerheblich ist, ob der Täter dabei im Ausland agiert (Beispiel: Ein amerikanischer Staatsbürger lädt kinderpornographische Bilder auf einen FTP-Server, der in Berlin steht). Anders verhält es sich, wenn der Server im Ausland steht.

Hierbei ist es unerheblich, ob der Täter von Berlin oder New York aus tätig wird. Da die Straftäter diese „Gesetzeslücke“ kennen, werden strafrechtlich re-

levante Daten oftmals auf ausländischen Servern gespeichert. Das hat zur Folge, daß die Anwendung des § 9 I Alt. 1 StGB entfällt.

Da aber die strafbaren Inhalte in Deutschland abgerufen werden können, könnte der Erfolgsort im Inland liegen und somit eine Anwendung des § 9 I Alt 2 StGB begründen. Handlungs – und Erfolgsort würden somit auseinanderfallen, da der Täter praktisch das Internet nutzt, um strafbare Inhalte aus der Entfernung zu verbreiten. Diese Argumentation scheint schlüssig, dennoch hat sie gerade in der Literatur eine heftige Diskussion entfacht. Die verschiedenen Argumente für und gegen die Anwendung des § 9 I Alt. 2 StGB werden nun kurz vorgestellt[267]:

Da der Internet-Technologie die Möglichkeit fehlt, bestimmte Informationen nur in einem begrenzten räumlichen Bereich zugänglich zu machen, würde die weite Auslegung des § 9 I StGB dazu führen, daß das gesamte Internetangebot den deutschen Strafvorschriften unterliegen müßte. Dabei würde man nicht beachten, daß die schützenswerten Güter in den verschiedenen Staaten durchaus unterschiedlich sein können. Demnach würde man dem Internet die vielleicht sehr strengen deutschen strafrechtlichen und somit auch gesellschaftlichen Regularien aufdrücken, da deutsche Wertvorstellungen u.a. zum Maßstab für alle Meinungsäußerungen im Internet werden würden. Durch die konsequente Ablehnung des § 9 I Alt. 2 StGB würde eine nicht hinnehmbare Strafbarkeitslücke entstehen, die es den Tätern ermöglichen würde, einfache deutsche Gesetze zu umgehen. Sie könnten beispielsweise ihre strafbaren Inhalte, wenn sie im Inland sonst durch ein Druckerzeugnis verbreitet werden würden, einfach in das dann (straf-) rechtsfreie Internet stellen. Ein solcher rechtsfreier Raum kann in unserer Kommunikationsgesellschaft nicht hingenommen werden.

Da es sich bei der Mehrheit der netzspezifischen Verbreitungsdelikte um sogenannte abstrakte Gefährdungsdelikte handelt, ist es umstritten, ob der unbestimmte Rechtsbegriff „Erfolg“ (§ 9 StGB) solche abstrakten Gefahren überhaupt mit einschließt.

Auf der einen Seite werden die abstrakten Gefährdungsdelikte ausgeklammert, da sie keinen zum Tatbestand gehörenden Erfolg haben und die Ge-

[267] Für nähere Informationen vgl.: Jofer, Strafverfolgung im Internet, Seite 104 bis 111.

fahr üblicherweise die Vorstufe zum Schaden (Erfolg) ist. Auf der anderen Seite wird gerade die abstrakte Gefährdungslage zur Begründung eines Erfolges herangezogen, da nämlich eine mißbilligte Beeinflussung der Außenwelt „erfolgt“ ist[268]. M.E. kann man davon ausgehen, daß der Erfolg eines abstrakten Gefährdungsdeliktes regelmäßig zeitgleich mit der Tatbegehung einsetzt. „Der strafrechtliche Wortsinn des Begriffs des `Erfolgs´ ist nicht identisch mit dem Erfolgsbegriff im allgemeinen Sprachgebrauch. Als wertneutraler Terminus umfaßt er ebenso negative Umstände und läßt sich im Sinne eines `erfolgten Geschehens´ auslegen.“[269]

Mithin kann festgestellt werden, daß Internetstraftaten im Bereich der netzspezifischen Verbreitungsdelikte stets einen „Erfolg“ in Deutschland haben und daher keine reinen Auslandstaten darstellen. Die Anwendung des § 9 I Alt. 2 StGB ist dann zulässig, wenn inländische Rechtsgüter abstrakt gefährdet werden[270]. Durch zwei Haftbefehle des AG Mannheim wurde diese Auffassung erst vor kurzer Zeit bestätigt[271].

Eine Möglichkeit, diese vage Konstruktion etwas sicherer zu machen, sah man in der teleologischen Reduktion des § 9 StGB[272]. „Ein Nutzer, der nach deutschem Recht strafbares Material vom Ausland aus in das Netz einspeist, solle – wegen der sofortigen globalen Erfolgsverursachung – nur dann bestraft werden, wenn der Erfolg nach seiner Vorstellung im Inland eintreten sollte, wenn also seine Publikation final an den deutschen Nutzer gerichtet war.“[273]

Das Problem der teleologischen Reduktion besteht darin, daß für eine solche Beurteilung schon Ermittlungen zu den Motiven des Täters erforderlich sind. Da aber diese Ermittlungshandlungen bereits strafprozessual sein würden, scheidet diese Variante aus, da für diese Ermittlungen der Verdacht einer

---

[268] So z.B.: BGHSt 42, 235 (242) in NJW 1997, 138; BGH, NStZ 1990, 36 (37) (Nachweis bei: Sieber, Internationales Strafrecht im Internet, NJW 29/1999, Seite 2067).

[269] Jofer, Strafverfolgung im Internet, Seite 108

[270] Zu einer anderen Ansicht gelangt u.a. Sieber, Internationales Strafrecht im Internet, NJW 29/1999, Seite 2065 bis 2073, der davon ausgeht, daß abstrakte Gefährdungsdelikte nur dann einen Erfolg begründen können, wenn die rechtswidrigen Inhalte mittels Push-Technologien nach Deutschland gelangen.

[271] AG Mannheim vom 09.04 und 03.05.1999 (42 Gs 1002/99) (Nachweis bei: Sieber, Internationales Strafrecht im Internet, NJW 29/1999, Seite 2065 bis 2073)

[272] Eine kurze Zusammenfassung der verschiedenen Ansätze zur Reduktion bietet: Sieber, Internationales Strafrecht im Internet, NJW 29/1999, Seite 2065 bis 2073, mit Hinweis auf: Kienle, Int. StrafR und Straftaten im Internet, 1998, S. 159 ff.

Straftat nach deutschem Strafrecht vorliegen müßte. Die Motivermittlung würde aber eben erst Aufschluß über die Anwendbarkeit deutscher Strafvorschriften geben!

9.1.4 Art. 296 EGStGB

Gemäß Art. 296 EGStGB ist § 86 I [Verbreiten von Propagandamitteln verfassungswidriger Organisationen] StGB nicht anwendbar, wenn Zeitungen und Zeitschriften, die im Ausland in ständiger, regelmäßiger Folge erscheinen und öffentlich vertrieben werden, nach Deutschland eingeführt werden. Analog kann dieser Artikel auch auf die Verbreitung von Propagandamitteln verfassungswidriger Organisationen über das Internet angewendet werden. Allerdings bleibt Art. 296 EGStGB auf den § 86 I StGB beschränkt. Eine Erweiterung auf andere netzspezifische Verbreitungsdelikte ist nicht zulässig.

9.1.5 Rechtfertigungsgründe

In der Theorie setzt sich eine Straftat grundsätzlich aus drei Komponenten zusammen. Ein Angeklagter kann nach deutschem Strafrecht nur verurteilt werden, wenn in einem rechtsstaatlichen Gerichtsverfahren das zuständige Gericht eine tatbestandsmäßige, rechtswidrige und schuldhafte Handlung des Angeklagten erkennt. Insofern entfällt die Strafbarkeit beim Vorliegen von Rechtfertigungs- oder Entschuldigungsgründen. Die Frage, die sich stellt, ist, ob für einen im Ausland handelnden Täter eine ausländische Erlaubnisnorm vor einem deutschen Gericht einen Rechtfertigungsgrund darstellen kann.

Nach dem Grundsatz der „Einheit der Rechtsordnung“ kann ein bestimmtes Gesetz nichts verbieten, was ein anderes Gesetz erlaubt. D.h. daß man beispielsweise das Strafrecht nicht losgelöst vom bürgerlichen Recht sehen darf. Das bedeutet u.a., daß Rechtfertigungs- oder Entschuldigungsgründe nicht nur aus dem allgemeinen Teil des StGB entnommen werden können, sondern auch aus dem BGB oder anderen Gesetzen.

So stellen z.B. die meisten Eingriffsnormen der StPO oder der Polizeigesetze der Bundesländer Rechtfertigungsgründe für Eingriffsmaßnahmen der

---

[273] Jofer, Strafverfolgung im Internet, Seite 112

Polizei dar[274]. M.E. umfaßt die „Einheit der Rechtsordnung“ nur die gültigen Gesetze eines souveränen Staates. D.h. daß beispielsweise die Gesetze der USA nicht zur bundesdeutschen Rechtsordnung gehören, da sie kein innerdeutsches Recht sind. Daher ist kein Erlaubnistatbestand einer ausländischen Rechtsordnung ein Rechtfertigungsgrund für eine - der deutschen Gerichtsbarkeit - unterliegende Handlung.

9.1.6 Verbotsirrtum nach § 17 StGB

§ 17 [Verbotsirrtum] StGB regelt den Verbotsirrtum für das deutsche Strafrecht. Demnach handelt ein Täter ohne Schuld, wenn ihm bei der Begehung der Tat die Einsicht fehlt, Unrecht zu tun und er diesen Irrtum nicht vermeiden konnte. D.h. daß ein ausländischer Straftäter, der nicht weiß, daß seine Handlungen gegen deutsches Recht verstoßen, nicht schuldhaft handelt. Demnach muß ein ausländischer Täter nur glaubhaft machen, daß er das deutsche Recht nicht kannte. An dieser Stelle muß man bedenken, daß ein Mensch grundsätzlich von der Normen- und Wertevorstellung seines Umfeldes geprägt wird. Diese Normen- und Wertevorstellungen beeinflussen die Gesetzgebung und demzufolge auch das Rechtsbewußtsein der ihnen unterliegenden Menschen.

Daraus resultierend wird klar, daß man prinzipiell von einem Menschen nicht verlangen kann, daß er alle Rechtsordnungen der Welt kennt. Er wird sich also bei der Dateneinspeisung immer an den Vorstellungen seines Gesellschaftskreises orientieren. Es ist dem Nutzer nicht zuzumuten, daß er vor der Dateneinspeisung erst ein umfangreiches Rechtsgutachten einholt. Daher greift grundsätzlich der Verbotsirrtum aus § 17 StGB, wenn die Daten auf ausländischen Servern gespeichert wurden. Eine Ausnahme bilden aber wiederum Deutsche (die solche Daten einspeisen) und Ausländer, denen das deutsche Recht bekannt ist.

---

[274] Durch eine Gewahrsamnahme eines gewalttätigen Demonstranten handeln die eingreifenden Polizeibeamten stets tatbestandsmäßig i.S.d. StGB (Freiheitsberaubung), ihre Handlungen sind aber durch die Eingriffsnormen des Versammlungsgesetzes i.V.m. dem entsprechenden Polizeigesetz gerechtfertigt.

9.1.7 Eingeschränkter Verfolgungszwang der Staatsanwaltschaft nach § 153 c StPO

§ 153 c [Nichtverfolgung von Auslandstaten] StPO bietet neben Art. 256 EGStGB und § 17 StGB eine weitere Möglichkeit, von der Verfolgung von Auslands-taten abzusehen. Insofern wandelt § 153 c StPO das für Straftaten allgemein geltende Legalitätsprinzip speziell für Auslandstaten in das Opportunitätsprinzip um.

Das Opportunitätsprinzip besagt, daß die Staatsanwaltschaft nach pflichtgemäßem Ermessen entscheidet, ob sie die Strafverfolgung aufnimmt oder ablehnt. Das pflichtgemäße Ermessen muß ermessensfehlerfrei ausgeübt werden, was nichts anderes bedeutet, als daß sich die Entscheidung an sachlichen und nachprüfbaren Kriterien ausrichten muß. Willkürentscheidungen sind daher nicht zulässig. Zwei Kriterien nennt § 153 c II StPO kategorisch. Von der Strafverfolgung kann abgesehen werden, wenn sie einen schweren Nachteil für Deutschland herbeiführen würde oder sonstigen überwiegend öffentlichen Interessen entgegensteht.

Das erste Kriterium ist vernachlässigbar. Das zweite Kriterium ist nach h.M. dann gegeben, wenn beispielsweise die Öffentlichkeit kein überwiegendes Interesse an der Aufklärung der Tat hat. Dies wird regelmäßig dann angenommen, wenn durch die Tat keine Gemeinschaftsgüter verletzt wurden. Verletzte Individualrechtsgüter können mithin von Grund auf kein öffentliches Interesse begründen.

9.1.8 Strafbarkeit der Provider

Die vorausgegangenen Ausführungen beschäftigten sich mit der Anwendbarkeit des deutschen Strafrechts auf die eigentlichen Taten und die eigentlichen Täter. Allerdings wurde durch die Problematik auch die Frage aufgeworfen, welche Verantwortung die Provider in diesem Bereich haben, ob sie also allein für das Zugänglichmachen der inkriminierten Informationen strafbar sind. Die Zusammenhänge werden klar, wenn man beachtet, daß die Verbreitung – als wesentlicher Bestandteil der netzspezifischen Verbreitungsdelikte – ohne die Provider nicht möglich ist.

Zu klären bleibt, ob der Provider i.S.d. § 13 [Begehen durch Unterlassen] StGB seinen Tatbeitrag durch Tun oder Unterlassen leistet, ob in letzterer Variante eine Garantenstellung besteht, welche Überwachungs- und Handlungspflichten den Verantwortlichen treffen und wann eine Sperrung verbotener Inhalte möglich und zumutbar ist.

Als erstes soll die Frage geklärt werden, ob das Zurverfügungstellen ein strafbares Tun oder die entsprechende Nichtverhinderung des Zugangs ein strafbares Unterlassen darstellt. Fest steht, daß der Provider durch die Zurverfügungstellung der Informations- und Kommunikationsinfrastruktur einen sogenannten Verursachungsbeitrag zu den strafbaren Verbreitungshandlungen leistet. Ohne dieses Zurverfügungstellen wäre den Kunden ein Mißbrauch des Internets durch Einspeisung strafbarer Inhalte oder Durchführung anderer krimineller Handlungen nicht möglich. Das Zurverfügungstellen selbst ist kein rechtlich unzulässiges Verhalten[275]. Erst durch die strafbaren Handlungen der Kunden wird der Provider quasi in die Handlungen involviert. Daher kann man ggf. dem Provider nur den Vorwurf machen, daß der Datentransfer nicht hinreichend überwacht wurde oder das der Austausch bestimmter Daten nicht unterbunden wurde. Demzufolge kann sich der Vorwurf des Unterlassens nur auf folgende zwei Varianten manifestieren: Nichtüberprüfung von Netzinhalten und Nichtsperrung bei Kenntnis von strafbaren Inhalten.

Grundsätzlich kann man davon ausgehen, daß § 13 StGB anwendbar ist. § 13 StGB spricht, wie § 9 StGB, von einem Erfolg, so daß die gleiche Diskussion über die Anwendbarkeit bei abstrakten Gefährdungsdelikten geführt werden könnte. Da die weite Auslegung des Begriffs „Erfolg“ aber bereits ausführlich begründet wurde, kann an dieser Stelle auf die gemachten Ausführungen verwiesen werden.

9.1.9 Garantenstellung der Provider

Da der Provider durch Unterlassen handeln kann, ist zu klären, ob er eine Garantenstellung hat. Garant ist jeder, der rechtlich dafür einzustehen hat, daß ein „Erfolg“ nicht eintritt. Hat der Provider also im Umkehrschluß keine Garan-

[275] Vergleiche können hier zu den herkömmlichen Kommunikationsmitteln, wie z.B. Telefon, gezogen werden; der Telefon-Anbieter ist auch nicht dafür verantwortlich, wenn das überlassene Telefon mißbraucht wird.

tenstellung, kann er nicht durch Unterlassen handeln. Die Garantenstellung ist Grundlage für eine Strafbarkeit nach § 13 StGB. Durch seine besondere Verantwortung wird der Garant dem aktiv handelnden Täter gleichgestellt. Demzufolge stellt sich die Frage, ob und unter welchen Bedingungen den Provider eine Handlungspflicht trifft.

Die Garantenstellung ist ein unbestimmter Rechtsbegriff, dessen Ausfüllung Aufgabe der Rechtsprechung und der Literatur ist. Diese haben verschiedene Fallgruppen für die Annahme einer Garantenstellung entwickelt. „So kann eine Garantenstellung aus Gesetz, aus der tatsächlichen Übernahme der Verantwortung oder aus einem besonderen Vertrauensverhältnis ebenso entstehen, wie durch die Herbeiführung einer Gefahrenlage (Ingerenz) oder durch Sachherrschaft. Eine neuere Lehre differenziert zwischen Obhutspflichten und Schutzpflichten. Erstere sollen vorliegen, wenn der Garant alle Gefahren abzuwenden hat, die einem Rechtsgut drohen, welches unter seiner `Obhut´ steht; letztere können gegenüber allen Rechtsgütern bestehen, die von einer Gefahrenquelle tatsächlich betroffen sein können und daher geschützt werden müssen.“[276] Alle klassischen Fallgruppen können diesen beiden neueren Kategorien untergeordnet werden. Somit könnte sich eine Garantenstellung für die Provider aus der Möglichkeit ergeben, daß sie gewisse Obhutspflichten gegenüber ihren Kunden haben oder daß sie bestimmte Schutzpflichten treffen, die sich aus der Gefahrenquelle Internet ergeben.

Gemeinhin besteht keine gesetzliche Pflicht für die Provider, Kunden vor den strafbaren Inhalten des Internets zu bewahren. Vertraglich sichert der Provider nur das Zurverfügungstellen des Netzzuganges zu. Er stellt daher eine reine Dienstleistung dar, der Kunde entscheidet selbst, welche Inhalte des Internets er nutzen möchte.

Daß durch die Provider vereinzelt Inhalte gesperrt und sogar bestimmte Filterungssoftware für inkriminierte Inhalte an besorgte Eltern ausgegeben wurden, ändert nichts an der Entscheidungsfreiheit des Kunden, da beispielsweise die Sperrung häufig auf Anregung der Ermittlungsorgane erfolgte.

Eine Garantenstellung durch Ingerenz ist abzulehnen, da sie ein objektiv pflichtwidriges Vorverhalten fordert. Die Dienstleistung „Zurverfügungstellung

---

[276] Jofer, Strafverfolgung im Internet, Seite 126

eines Internetzugangs“ ist zwar kausal, kann aber mithin nicht als pflichtwidriges Vorverhalten klassifiziert werden. Die Risiken entstehen durch das Verhalten Dritter. Diese Risiken können nicht ausgeschlossen werden. In diesem Zusammenhang spricht man auch von der „Allgegenwärtigkeit des Verbrechens“. So ist der Staat auch nicht für Verkehrsstraftaten verantwortlich, die auf seinen Straßen geschehen!

Eine Garantenstellung des Providers durch Kontrolle über den Zugang zu einer Gefahrenquelle (Internet) ist ebenfalls prüfenswert. Der Provider besitzt die tatsächliche Sachherrschaft über die Gefahrenquelle, da es ihm technisch möglich ist, bestimmte Inhalte zu sperren. Hierbei kann es sich um eigene oder vermittelte Inhalte handeln. Somit besteht vielfach für ihn die Möglichkeit, die Gefahren zu beschränken, da er festlegen kann, worauf seine Kunden Zugriff erhalten. Da sich der Kreis der Handlungspflichtigen in der Folge enorm erweitern würde, versuchte man weitere Eingrenzungskriterien zu finden. Man kam zu dem Ergebnis, daß sich die Art und Weise der Verkehrssicherungspflichten nach der spezifischen Gefährlichkeit der beherrschten Sache richten müßten. Infolgedessen wird eine gesteigerte Gefahr gefordert.

Bei den netzspezifischen Verbreitungsdelikten handelt es sich überwiegend um abstrakte Gefährdungsdelikte, die Gemeinschaftsinteressen schützen. Diese abstrakten Gefährdungsdelikte enthalten keine solche gesteigerte Gefährlichkeit. Provider sind nicht die Sachwalter von Gemeinschaftsinteressen. Daher ist eine Garantenstellung grundsätzlich abzulehnen. Gefordert ist an dieser Stelle der Staat, dessen Aufgabe der Schutz von Gemeinschaftsinteressen ist. Erst wenn der Staat durch gesetzliche Regelungen für die Provider Handlungspflichten (Überprüfungs- und Sperrpflichten) schafft, kann sich für diese eine Garantenpflicht ergeben.

9.1.10 Das IuKDG und der MDStV

Eine Garantenstellung des Providers per Gesetz könnte sich allgemein aus dem IuKDG oder dem MDStV ergeben[277]. Grundsätzlich besteht die Möglichkeit, ein Angebot als Teledienst i.S.d. TDG oder als Mediendienst i.S.d.

[277] Eine ältere Abhandlung über die Strafbarkeit von Internet-Providern (ohne TDG) bei: Conradi/Schlömer, Die Strafbarkeit von Internet-Provider, NStZ 8/1996, Seite 366 bis 369 und NStZ 10/1999, Seite 472 bis 477.

MDStV einzuordnen. Der MDStV bleibt bei den folgenden Betrachtungen außen vor, da die Regelungen des § 5 MDStV, der die Verantwortlichkeit für Mediendienste bestimmt, weitestgehend mit denen des § 5 TDG identisch sind[278].

Durch das IuKDG (Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste[279]) vom 22.07.1997 wurde vom bundesdeutschen Gesetzgeber der Versuch unternommen, gesetzlich auf die fortschreitende Entwicklung im Bereich der Informations- und Kommunikationstechnik einzuwirken. Das Gesetz bietet wichtige Anhaltspunkte für die Beurteilung der Verantwortlichkeit von Diensteanbietern der verschiedensten Art. Ferner werden Rechte und Pflichten der Diensteanbieter geregelt. „Mit den ersten 3 Artikeln dieses Gesetzes wurden 3 vollständig neue Gesetze verabschiedet: Das Teledienstegesetz (TDK), das Teledienstedatenschutzgesetz (TDDSG) und das Gesetz zur digitalen Signatur (SigG).“[280] „Das IuKDG hat viele bestehende Gesetze geändert, so u.a. das Strafgesetzbuch, das Gesetz über die Verbreitung jugendgefährdender Schriften, das Urheberrechtsgesetz und das Gesetz über Ordnungswidrigkeiten.“[281]

9.1.11 §§ 2, 3 und 4 TDG

Eines der wichtigsten Gesetze für den Bereich des Internet stellt das TDG dar, da es die wichtigsten Regelungen zum Umgang mit Telediensten enthält.

§ 2 [Geltungsbereich] TDG regelt den Geltungsbereich des Gesetzes. Hierbei bietet Absatz I eine allgemeine Definition des Begriffs „Teledienst“, Absatz II zählt beispielhaft die wichtigsten Anwendungsgebiete auf.

Die Definition des Teledienstes umfaßt zur Zeit alle denkbaren technischen Formen der elektronischen Kommunikationsdienste. Sie gewährleistet auch die Anwendbarkeit auf zukünftige Dienste. Nach § 2 II Nr. 3 TDG gehören Angebote zur Nutzung des Internets oder weiterer Netze zum Anwendungsbereich des TDG. Dabei kann der Anbieter eigene Dienste unterhalten oder Zugang zu fremden Diensten bereitstellen. Von Bedeutung an dieser Stelle sind die Regularien des § 3 [Begriffsbestimmungen] TDG. Hiernach unterscheidet

---

[278] Eine Unterscheidung macht mithin nur bei der Betrachtung der Gefahrenabwehr Sinn.

[279] Für das IuKDG existiert auch der Begriff „Multimediagesetz“.

[280] Jofer, Strafverfolgung im Internet, Seite 133

das Gesetz zwischen Nutzern und Dienstanbietern. Anbieter sind natürliche oder juristische Personen oder Personenvereinigungen, die eigene oder fremde Teledienste zur Nutzung bereithalten. So fällt also auch der private Betreiber einer Homepage oder einer Mailbox unter die Regularien des TDG. Die Provider sind Diensteanbieter i.S.d. § 3 TDG.

Nach § 2 III TDG ist es unerheblich, ob für die Nutzung des Teledienstes ein Entgelt erhoben wird. Gemäß § 2 IV TDG bleiben die Vorschriften des TKG unberührt, so daß beispielsweise auch die entsprechenden Anmelderegelungen weiter beachtet werden müssen. Dennoch richtet sich das TKG vor allem an die Betreiber von Telefon- oder Mobilfunknetzen. Teledienste setzen also – vereinfacht gesagt – auf Telekommunikationsdienste auf.

Nach § 4 [Zugangsfreiheit] TDG sind Teledienste im Rahmen der Gesetze zulassungs- und anmeldefrei. Gewerberechtliche und wirtschaftsrechtliche Anmeldeverfahren sind dennoch zu beachten.

9.1.12 § 5 TDG

Wenn geklärt ist, daß ein bestimmtes Angebot ein Teledienst ist, kann man über die sogenannte Stufenregelung des § 5 [Verantwortlichkeit] TDG die Verantwortlichkeit eines Teleddiensteanbieters im Rahmen der allgemeinen Gesetze – zu denen auch das Strafgesetzbuch und seine Nebengesetze zählen – bestimmen.

Die Stufenregelung enthält drei Verantwortungsstufen für Diensteanbieter. Die Stufen werden durch die Absätze I, II und III des § 5 TDG geregelt. Nach § 5 I TDG ist ein Diensteanbieter für eigene Inhalte, die er zur Nutzung bereithält, voll verantwortlich. Für diese Art Diensteanbieter wird auch der Begriff Content-Provider verwendet.

Der klassischste Anwendungsfall für einen Content-Provider ist der Betreiber einer Homepage. Er ist für den Inhalt seiner Homepage voll verantwortlich.

Nach § 5 II TDG ist ein Diensteanbieter für fremde Inhalte, die er zur Nutzung bereithält, nur dann verantwortlich, wenn er von diesen Inhalten Kenntnis

---

[281] Jaeger, Computerkriminalität, Seite 134

hat und wenn es ihm technisch möglich und zumutbar ist, deren Nutzung zu verhindern. Für diese Art Diensteanbieter wird auch der Begriff Serviceprovider verwendet. In der Regel wird beispielsweise ein Homepage-Betreiber keinen eigenen Server für seine Website unterhalten. Webspace-Anbieter ermöglichen solchen Betreibern das Abspeichern ihrer Seite auf einem ihrer Server. So gibt es kostenfreie Webspace-Anbieter aber auch kostenpflichtige Angebote. Ferner wird durch die meisten Online-Dienste für jeden registrierten Kunden Speicherplatz für Homepages bereitgestellt. Ein weiterer typischer Anwendungsfall für die zweite Variante ist die Bereitstellung von Newsgroups durch einen Provider. In diesen Funktionen ist der Provider dann Serviceprovider, weil er fremde Dienste bereitstellt, nämlich fremde Homepages oder Newsgroups auf seinen Servern.

Nach § 5 III TDG ist ein Diensteanbieter für fremde Inhalte, zu denen er lediglich den Zugang zur Nutzung vermittelt, nicht verantwortlich. Für diese Art Diensteanbieter wird auch der Begriff Accessprovider verwendet. Das automatisierte kurzzeitige Vorhalten fremder Inhalte auf Grund von Nutzeranfragen gilt als Zugangsvermittlung. Gemeint ist hier das Betreiben eines Proxy-Servers. Dabei werden hauptsächlich bestimmte stark frequentierte Webseiten, die eigentlich auf anderen WWW-Servern gespeichert sind, auf einem speziellen Server abgelegt, der an den Accessprovider gekoppelt ist. Das hat zur Folge, daß ein deutscher Benutzer eine Website, die z.B. auf einem amerikanischen Server liegt und stark frequentiert wird, über einen Proxy abruft, da alle Anfragen erst über diesen Server laufen. Liegt eine Website auf dem Proxy[282], wird sie von dort an den Benutzer gesendet. Ist sie nicht „gecacht“, wird die Anfrage an die eigentliche Adresse weitergeleitet. Der Proxy aktualisiert in regelmäßigen Abständen seinen Datenbestand. Der Provider ist verpflichtet, in gewissen Abständen die Proxy-Datenbestände zu löschen.

Der Accessprovider ist – praktisch gesehen – nur der Zugangsanbieter. Er hat überhaupt keinen Bezug zu den Daten, die der Nutzer abruft oder sendet. Die Daten sind überwiegend auf fremden Servern gespeichert.

Es muß beachtet werden, daß man mit den Begriffen vorsichtig umgehen muß. Ein Provider kann durchaus in verschiedene Positionen geraten. So kann

---

[282] In diesem Zusammenhang spricht man von einer „gecachten“ Seite.

er in der einen Situation Content-, in der anderen Service- und wieder in einer anderen nur reiner Accessprovider sein, z.B. T-Online. T-Online ist technisch gesehen ein Online-Dienst. Die technische Qualifizierung ist strikt von der rechtlichen zu trennen. T-Online unterhält eine eigene Homepage, auf der sich Kunden und Interessierte mit den neusten Informationen über den Dienst versorgen können. Diese Homepage ist ein eigenes Angebot – T-Online ist in diesem Zusammenhang Content-Provider. T-Online ermöglicht registrierten Nutzern das Abspeichern einer eigenen Homepage auf den T-Online-Servern. In diesem Zusammenhang ist T-Online dann Serviceprovider. Da T-Online auch die Benutzung des gesamten anderen Teils des Internets ermöglicht, vermittelt es sozusagen den Zugang zu anderen/fremden Inhalten und ist in dieser Funktion Accessprovider. Es kommt also darauf an, wie ein Benutzer seinen Internet-Provider benutzt. Der Provider kann dann dementsprechend nur eine Rolle oder auch alle Rollen zugleich ausfüllen.

Will man nun eine strafrechtliche Verantwortung eines Providers begründen, muß man zuerst überprüfen, ob das TDG anwendbar ist. Es muß also subsumiert werden, daß der Provider ein Teledienst i.S.d. § 3 TDG ist. Danach kann man die Stufenregelung des § 5 TDG anwenden. Ist der Provider Content-Provider, ist er als Urheber voll strafbar, da voll verantwortlich.

Der Serviceprovider ist verpflichtet – wenn technisch möglich und zumutbar – bekannte rechtswidrige Inhalte zu sperren. Voraussetzung ist, daß dem Serviceprovider der Inhalt bekannt ist. Informationen können durch die Polizei oder durch umsichtige Benutzer an den Provider herangetragen werden oder durch den Provider selbst festgestellt werden. Der Serviceprovider wird also zum Garanten, wenn er rechtswidrige Inhalte kennt. Demzufolge entsteht für ihn eine Handlungspflicht, die nur durch die technische Möglichkeit und Zumutbarkeit beschränkt wird. Wird der Serviceprovider seiner gesetzlichen Garantenstellung nicht gerecht, macht er sich wegen Unterlassens strafbar.

Der Accessprovider kann in seiner Rolle nie strafbar sein. Wenn er strafbar wird, ist er entweder Content- oder Serviceprovider. Nach h.M. bezieht sich § 5 IV TDG ausschließlich auf Absatz III, also auf Accessprovider. Daher kann

aus § 5 IV TDG keine strafrechtliche Verantwortung abgeleitet werden[283]. Was passiert nun, wenn ein Accessprovider von rechtswidrigen Inhalten erfährt? Absatz IV regelt eine grundsätzliche Pflicht der Accessprovider, rechtswidrige Inhalte, zu denen sie ja den Zugang vermitteln, zu sperren. Allerdings wird der Accessprovider bei Nichtsperrung kein Garant i.S.d. Strafgesetzbuches und kann daher auch nicht strafrechtlich belangt werden. Eine Bejahung der strafrechtlichen Garantenstellung würde die Grenzen zwischen § 5 II und III TDG in unzulässiger Weise verwischen. Der Accessprovider bleibt weiterhin privilegiert. Der Gesetzgeber bringt damit zum Ausdruck, daß er bei den reinen Zugangsvermittlern lieber auf Selbstkontrolle, als auf strafrechtliche Sanktionen setzt. Diese Vorgehensweise entspricht auch dem Grundsatz des ultima ratio des Strafrechts. Obwohl der Accessprovider nicht strafrechtlich belangt werden kann, ist es möglich, die Sperrverpflichtung auf dem Verwaltungsrechtsweg durchzusetzen. Insbesondere kommen dann Festsetzung von Zwangsgeld, Beugehaft, Ersatzvornahme oder ein Sofortvollzug in Betracht. Ferner kann einem Provider nach § 15 [Widerruf der Lizenz] TKG die erforderliche Lizenz entzogen werden.

An dieser Stelle wird ersichtlich, daß es unbedingt notwendig ist, die jeweilige Stellung des Providers genau festzustellen, da diese Zuordnung erhebliche Konsequenzen für die rechtliche Betrachtungen nach sich zieht.

9.1.13 Sperrung von rechtswidrigen Inhalten

§ 5 TDG enthält weitestgehend abschließende Regelungen für die Verantwortlichkeit von Providern. Sperrpflichten ergeben sich nur, wenn es dem Provider technisch möglich und zumutbar ist. Voraussetzung für eine Sperrung ist die positive Kenntnis über rechtswidrige Inhalte. Daraus muß man schlußfolgern, daß keine Überprüfungspflicht für Provider im Vorfeld besteht, d.h. daß der Provider auf seinen Servern nicht nach strafbaren Inhalten suchen muß. Auch besteht keine Pflicht zu stichprobenartigen Kontrollen. Der Provider muß erst reagieren, wenn er Kenntnis erhält.

---

[283] Vgl. auch: Eichler, Bekämpfung der Kriminalität im Internet : Tagung beim BKA am 14./15.12.1998 mit Anmerkungen, CR 3/1999, Seite 202.

Grundsätzlich existieren verschiedene Möglichkeiten, Daten für Kunden zu sperren. Allerdings gibt es auch genügend Möglichkeiten, dennoch an die inkriminierten Daten zu kommen. Was daher im Einzelfall möglich ist, bestimmt sich nach den Gegebenheiten des Einzelfalls. Die Zumutbarkeit muß sich ebenfalls am konkreten Einzelfall orientieren. Hier sind die individuellen Umstände und Befindlichkeiten des jeweils betroffenen Diensteanbieters zu beachten. Im Zuge einer Zumutbarkeitsprüfung, ist die Lage und die Fähigkeit des Garanten mit der Nähe und Schwere der Gefahr in Beziehung zu setzen. Dabei kann auch eine Kosten-Nutzen-Überlegung herangezogen werden. „Es ist zu untersuchen, welche Beeinträchtigungen im Falle einer Sperre in Kauf genommen werden müssen und welcher Erfolg dadurch erzielt wird.“[284] Es kann somit auch zwischen sogenannten nichtkommerziellen (Behörden, Bildungseinrichtungen) und kommerziellen Unternehmen (Online-Dienste, Zugangsprovider) unterschieden werden. Die Zumutbarkeit einer Sperre muß abgelehnt werden, wenn die Maßnahme unverhältnismäßig (nicht erforderlich oder ungeeignet) ist[285].

Jofer gibt an dieser Stelle zu bedenken, daß das Internet ja so konzipiert ist, daß Informationen schnell und vielfach verteilt werden können[286]. Wenn also ein Provider eine bestimmte Information sperrt, kann der Benutzer durch die Einwahl über einen anderen Provider dennoch an die gewünschten Informationen gelangen.

Hierdurch wird grundsätzlich die Geeignetheit einer Sperrung in Frage gestellt. Als Ergebnis einer aufschlußreichen Diskussion lehnt Jofer die Ungeeignetheit ab, da auch die Verringerung der Zugriffsmöglichkeiten ein rechtspolitisch lohnendes Ziel darstellt und eine privilegierte Stellung des Internets – gegenüber anderen Medien - nicht hinzunehmen ist. Außerdem wird durch die Sperrungen die Gefahr, zufällig auf strafbares Material zu stoßen, gemindert. Da strafbare Inhalte im Internet ohnehin gering sind, wird dieser Anteil durch die Sperrungen weiter vermindert.

Ein weiteres Problem, welches bei der Prüfung der Verhältnismäßigkeit zu beachten ist, ist die teilweise unvermeidliche Sperrung legaler Inhalte, wenn

---

[284] Jofer, Strafverfolgung im Internet, Seite 143

[285] Vgl. auch die detaillierteren Ausführungen zur Gefahrenabwehr.

strafbare Daten gesperrt oder gelöscht werden. Wenn man beispielsweise eine Newsgroup betrachtet, kommt man sehr schnell zu dem Ergebnis, daß es durchaus sein kann, daß eine eigentlich legale Newsgroup auch vereinzelt strafbare Inhalte enthalten kann. Eine Sperrung der gesamten Newsgroup wäre mit unserem Grundgesetz nicht vereinbar, da der Rest der „legalen“ Teilnehmer ohne Zweifel in ihrem verfassungsmäßig geschützten Recht auf Informationsfreiheit – Art 5 II GG – beeinträchtigt werden würd. Daher sind Kompromisse einzugehen und nur Inhalte zu sperren, die überwiegend oder ausschließlich der Verbreitung strafbarer Inhalte dienen. Da Art 5 II GG nicht schrankenlos gewährleistet wird, muß sich das Individuum ggf. überwiegenden Gemeinschaftsinteressen unterwerfen.

9.1.14 Täterschaft und Teilnahme

Der Urheber strafbarer Inhalte ist ohne Zweifel als Täter strafbar. Die Rolle des Providers in einer Garantenstellung kann man nicht so einfach definieren. Sein strafbares Unterlassen i.S.d. § 13 StGB kann er sowohl als Täter (Täterschaft) als auch als Gehilfe (Beihilfe) begangen haben. Insofern ist die Betrachtung der §§ 25 [Täterschaft] und 27 [Beihilfe] StGB von Bedeutung.

Grundsätzlich muß sich die Abgrenzung von Täterschaft und Teilnahme an den Gegebenheiten des Einzelfalls anlehnen. Täter ist, wer eine tatbestandsmäßige und rechtswidrige Tat selbst begeht. Gehilfe ist, wer mit Gehilfenwillen handelt, also die Tat als eigene oder nicht eigene wollte und ein eigenes Interesse am Taterfolg hat, sich an der Tat beteiligt und wenigstens einen Willen zur Tatherrschaft hat.

Im Bereich der netzspezifischen Verbreitungsdelikte liegt Beihilfe vor, wenn der Provider dem Urheber (Haupttäter), bei dessen Verbreitungshandlung Hilfe leistet. Da es sich bei diesen Verbreitungsdelikten um abstrakte Gefährdungsdelikte handelt, kann der Provider nur in der beschriebenen Art handeln, indem er eine bestimmte Gefahr erhöht. „Die Verbreitung der strafbaren Inhalte wird durch das Unterlassen gefördert, das rechtlich mißbilligte Risiko erhöht.“[287] Der Provider müßte mit doppeltem Gehilfenvorsatz handeln. Er muß

---

[286] Für weiterführende Informationen vgl. auch: Jofer, Strafverfolgung im Internet, Seite 145 bis 147.
[287] Jofer, Strafverfolgung im Internet, Seite 153

also die vorsätzliche Haupttat und auch seinen eigenen Tatbeitrag wollen. Wenn der Provider bei positiver Kenntnis bestimmte Daten nicht sperrt, erfüllt er regelmäßig diesen geforderten doppelten Gehilfenvorsatz, da er seinen Kunden bewußt und gewollt den Zugang weiterhin vermittelt.

9.1.15 Strafbarkeit von Links zu Seiten mit strafbaren Inhalten

Der Betreiber einer Homepage kann durch das Setzen von Links auf fremde Homepages verweisen[288]. Diese können strafbare Informationen enthalten. Er kann auch auf eine Website verweisen, die wiederum Links zu Websites mit strafbaren Informationen enthält. Ferner kann ein Homepagebetreiber auf eine legale Website verweisen, auf der dann erst später strafbare Inhalte veröffentlicht werden. Im ersten und zweiten Fall ist zu prüfen, ob sich der Betreiber der Website strafbar gemacht hat. Im dritten Fall ist zu prüfen, ob für den Betreiber eine Pflicht besteht, seine Links ständig daraufhin zu überprüfen, ob die verlinkten Seiten strafbar sind.

In der Literatur treffen grundverschiedene Meinungen aufeinander. „Nach der einen Auffassung sind Links lediglich neutrale Hinweise auf die Meinung eines Dritten und ein Beitrag zur freien Meinungsäußerung. Nach der anderen stellt der Link auf einen rechtswidrigen Inhalt schlicht einen nicht unerheblichen Beitrag zu einer fremden Rechtsverletzung durch die Mitwirkung an der Verbreitung rechtswidrigen Inhalts dar.“[289] [290]

Grundsätzlich kann man davon ausgehen, daß private Homepagebetreiber Diensteanbieter i.S.d. TDG sind[291]. Es wird aber auch die Auffassung vertreten, daß der Homepagebetreiber nur Nutzer eines Teledienstes (in dem Fall Webspace-Anbieter) ist, wenn er nicht mit einem eigenen Server am Netzwerk angeschlossen ist. Diese Ansicht ist nicht haltbar, da § 5 TDG maßgeblich

---

[288] Vgl. auch: Jaeger, Computerkriminalität, Seite 176 bis 180 mit Hinweise auf das Urteil des AG Tiergarten – 260 DS 857/96, vom 30.06.97, abgedruckt in CR 1998, 111 (rechtskräftig).

[289] Bettinger/Freytag, Privatrechtliche Verantwortlichkeit für Links, CR 9/1998, Seite 545 bis 556, die in diesem Zusammenhang einen neueren Überblick über den Meinungsstand in der Literatur bieten; eine weitere Übersicht bei: Vassilaki, Strafrechtliche Verantwortlichkeit durch Einrichten und Aufrechterhalten von elektronischen Verweisen (Hyperlinks), CR 2/1999, Seite 85 bis 93.

[290] Vgl. auch: Eichler, Bekämpfung der Kriminalität im Internet : Tagung beim BKA am 14./15.12.1998 mit Anmerkungen, CR 3/1999, Seite 202, nach dessen Ausführungen bei den Strafverfolgungsbehörden die Ansicht überwiegt, Anbieter von Hyperlinks nach § 5 II und III TDG zu beurteilen.

[291] Im Ergebnis so auch: Flechsig/Gabel, Strafrechtliche Verantwortlichkeit im Netz durch Einrichten und Vorhalten von Hyperlinks“, CR 6/1998, Seite 351 bis 358.

nach der Art der Inhaltsverfügung unterscheidet und nicht nach technischen Gesichtspunkten. Alle erdenklichen Fälle werden durch diese Vorschrift abgedeckt. Es würde keinen Sinn machen, einen Homepagebetreiber, der seine Website auf dem Rechner eines Serviceproviders hostet, als Nutzer zu qualifizieren. Der Begriff Content-Provider sollte in der Hinsicht verstanden werden, daß ein solcher entweder mit einem eigenen Host im Internet vertreten ist, oder die Dienste eines Providers nutzt, der dann zum Serviceprovider wird. Der Serviceprovider hat keinen Einfluß auf die Inhalte, die der Content-Provider auf seinen Rechnern abspeichert. Allein der Content-Provider entscheidet, was er zur Verfügung stellen will. Diese Auslegung der Begrifflichkeiten wird der Praxis gerecht.

M.E. ist der Hompagebetreiber für seine eigenen Inhalte Content-Provider und für fremde Inhalte Accessprovider[292] [293], da durch einen Link nur der Zugang zu fremden Inhalten ermöglicht wird[294]. Daher ist es auch unerheblich, ob ein Anbieter direkt auf eine strafbare Site verlinkt oder ein Benutzer über eine Linkkette auf eine strafbare Homepage gelangt. Der Anbieter des strafbaren Inhalts ist dann wieder Content-Provider.

Für den Content-Provider sind alle Inhalte fremd, auf die er keine Einwirkungsmöglichkeiten hat. Probleme ergeben sich aus dieser Betrachtung erst, wenn man zu dem Ergebnis kommt, dem privaten Homepagebetreiber – in seiner Eigenschaft als Accessprovider – verwaltungsrechtlich zu begegnen. Da der private Homepage-betreiber nicht verpflichtet ist, seine Identität anzugeben (vgl. auch § 6 [Anbieterkennzeichnung] TDG) können die Verwaltungsbehörden keinen Verwaltungszwang anwenden. Ein Rückgriff auf den Serviceprovider ist nur unter speziellen Bedingungen möglich, da die Homepage selbst nicht strafbar ist, sondern lediglich die verlinkten Seiten.

Durch das Setzen von Links kann eine Täterschaft oder Teilnahme begründet werden. Wer in seiner Homepage lediglich mit einem Link auf fremde

---

[292] So auch Wenning, JurPC Web-Dok. 46/1998, Abs. 19 (Nachweisführung bei Jaeger, Computerkriminalität, Seite 178).

[293] Vgl. auch: Eichler, Bekämpfung der Kriminalität im Internet : Tagung beim BKA am 14./15.12.1998 mit Anmerkungen, CR 3/1999, Seite 202.

[294] Im Ergebnis anders: Flechsig/Gabel, Strafrechtliche Verantwortlichkeit im Netz durch Einrichten und Vorhalten von Hyperlinks“, CR 6/1998, Seite 351 bis 358, die zu dem Ergebnis kommen, daß der Anbieter eines Hyperlinks nach § 5 I TDG (Contentprovider) zu behandeln ist.

Inhalte verweist, ist kein Täter i.S.d. StGB. Kopiert der Linkende die Inhalte, erlangt er Verfügungsgewalt. Damit hält er die Inhalte selbst bereit und wird in diesem Bezug Content-Provider und Täter. „Hält ein Dritter die Informationen in Absprache mit dem Linkenden bereit, leistet letzterer einen Tatbeitrag an einer gemeinschaftlich begangenen Tat und ist als Mittäter nach § 25 II StGB strafbar. Für eine strafbare Beihilfe durch das Setzen eines Links auf fremde, nicht übernommene Inhalte, bleibt folglich kaum noch Raum: Hält der Linkende die Inhalte selbst oder in Absprache mit einem Dritten bereit, ist er Täter; vermittelt er nur den Zugang, wird er über § 5 Abs. 3 privilegiert.“[295] Das gleiche gilt für die Angaben von Adressen, die keinen Link darstellen, sondern erst im Adreßfeld des Browsers eingetragen werden müssen[296].

Da keine Haftung für Links besteht, kann daher auch keine Pflicht zur regelmäßigen Prüfung von Links bestehen. Die Homepage mit den Links kann demnach nicht als Gefahrenquelle qualifiziert werden. Die Lösung ist sicherlich nicht ideal, stellt aber mithin einen vertretbaren Kompromiß zwischen absoluter staatlichen Kontrolle und einer gewissen selbstregulierenden Netzkultur dar. Es wäre nicht auszudenken, was passieren würde, wenn jeder Homepagebetreiber ständig seine Links kontrollieren müßte. Der Staat ist gehalten, direkt an die Urheber der strafbaren Inhalte heranzutreten und nicht an die, die lediglich darauf verweisen. Denn letztlich stellen die Urheber die wirkliche Gefahr dar, da ein Link auf einen gesperrten Inhalt ungefährlich ist!

9.1.16 Der Begriff der „Schrift“

Viele Tatbestände des StGB enthalten die Begriffe „Schrift“ oder „Schriften“. Was man im deutschen Strafrecht unter Schrift zu verstehen hat, regelt § 11 [Personen- und Sachbegriffe] StGB. Gemäß § 11 III StGB werden den Schriften Ton- und Bildträger, Datenspeicher, Abbildungen und andere Darstellungen gleichgestellt, wenn die jeweilige Vorschrift auf § 11 StGB verweist.

Für die nachfolgenden Ausführungen ist es von Bedeutung, wie der Begriff Schrift für die Mehrheit der Verbreitungsdelikte ausgelegt wird. Es soll geklärt

---

[295] Jofer, Strafverfolgung im Internet, Seite 159

[296] Jaeger, Computerkriminalität, Seite 180 weist darauf hin, daß viele Browser trotzdem einen Link anzeigen, obwohl die Adresse im HTML-Code nicht als Link, sondern als normaler Text ausgezeichnet ist.

werden, ob beispielsweise das Darstellen eines verbotenen Inhalts auf dem Bildschirm schon rechtswidrig ist, da sich die Daten ja im Arbeitsspeicher des Rechners befinden. Ferner legen einige Browser sogenannte temporäre Verzeichnisse an. Hier werden besuchte Websites automatisch gespeichert. Beim erneuten Aufruf wird erst einmal diese „gecachte“ Seite angezeigt. Erst wenn man explizit die Seite neu einlädt, fordert der Browser vom Server die aktuellste Version an. Da diese temporären Daten auch noch nach dem Ausschalten auf dem Computer vorhanden sind – der Benutzer kann einstellen, nach wieviel Tagen die temporären Daten gelöscht werden – können hier beispielsweise auch strafbare Inhalte automatisch auf der Festplatte gespeichert werden. Was passiert also, wenn der Benutzer durch Zufall auf eine Website mit beispielsweise pornographischen Abbildungen gelangt.

Früher rechnete man nur dauerhaft und auf körperlichen Datenträgern (Diskette, CD-ROM, Festplatte etc.) gespeicherte Daten zu den Darstellungen. Ob Daten in Arbeitsspeichern und darauf beruhende Bildschirmanzeigen auch Darstellungen sein sollten, war umstritten. Art. 4 Nr. 1 IuKDG hat den Schriftenbegriff erst um den Begriff des Datenspeichers erweitert. Durch die Rechtsprechung wurde bestätigt, daß beispielsweise eine Homepage dem Schriftenbegriff unterliegt[297].

Grundsätzlich kann man sich beim „Surfen“ im Internet frei bewegen. Alle zur Verfügung gestellten Angebote kann man ansehen. Damit ist notwendiger Weise eine Darstellung auf dem Bildschirm und eine Speicherung im Arbeitsspeicher verbunden.

Das rein passive Verhalten ist kein Verbreiten, Einführen etc. Problematisch wird es bei der gewollten Speicherung von Inhalten, deren Besitz bereits strafbar ist (z.B.: Kinderpornographie). So gab es wiederholt Strafverfahren gegen „aufmerksame“ Internet-Benutzer, die auf Kinderpornographie gestoßen waren, die Bilder abgespeichert und dann die Polizei in Kenntnis gesetzt hatten. Das bloße Anschauen eines Bildes kann nicht als Besitzverschaffen gewertet werden, da es an der Ausübung der tatsächlichen Sachherrschaft mangelt. Das bloße Anschauen von Bildern kann ebenfalls keinen Vorsatz begrün-

[297] Vgl. auch: OLG Nürnberg, Beschluß vom 23.06.1998 – Ws 1603/97 (GenStA Nürnberg, StA b.d.LG Regensburg), abgedruckt in CR 11/1998, Seite 686.

den. Wenn der Täter die Daten des Arbeitsspeichers hingegen verschicken will – beispielsweise mittels E-Mail – muß er sie notwendiger Weise zwischenspeichern. In dem Moment werden die Daten körperlich, und ein Besitzverschaffen liegt vor.

Ein Problem ergibt sich bei den temporären Verzeichnissen, da ja hier die Bilder automatisch gespeichert werden können. Durchgängig kann der Benutzer einstellen, ob temporäre Daten regelmäßig gelöscht werden oder nicht. Er kann Löschungsintervalle beliebig festlegen. Die Standardausgaben der gebräuchlichsten Browser (Internet Explorer und Netscape Navigator) haben eine automatische Löschfunktion für temporäre Verzeichnisse. Da vom Benutzer nicht verlangt werden kann, sich mit allen Feinheiten eines Programmes auseinanderzusetzen, darf die temporäre Zwischenspeicherung nicht strafbar – als Besitzverschaffen – sein. Erst wenn der Benutzer gezielt die automatische Löschung abschaltet, um eine Strafbarkeit zu umgehen, wird er strafbar[298]. Daher sind immer die Einstellungen des Browsers zu prüfen. Diesen Benutzern – die eine automatische Löschfunktion deaktivieren – kann dann auch zugemutet werden, daß sie eine manuelle Löschung vornehmen, wenn sie durch Zufall auf inkriminierte Inhalte gestoßen sind.

Was passiert, wenn einem Benutzer unaufgefordert E-Mails mit strafbaren Inhalten zugesendet werden. Erhält er unaufgefordert Kinderpornographie, würde er sich grundsätzlich in dem Moment strafbar machen, in dem er die E-Mails vom Server auf seinen Rechner lädt. Vom Benutzer kann verlangt werden, daß er strafbare E-Mails sofort löscht.

Damit zeigt er, daß er keinen Vorsatz bezüglich des Besitzverschaffens hat. Dabei muß die Löschung dauerhaft sein, so daß ein einfaches Verschieben in den Papierkorb von beispielsweise MS Windows nicht ausreichen dürfte, es sei denn, daß der Papierkorb vor Beenden der Sitzung automatisch geleert wird.

---

[298] Hierbei muß vor allem beachtet werden, daß in den Default-Einstellungen der meisten Browser eine automatische Löschung aktiviert ist.

9.1.17 Stop-Seiten und Exclude-Filter

„Auch der Einbau von Stop-Seiten, etwa des Inhalts: `Die folgenden Seiten enthalten pornographisches Material. Bitte bleiben Sie draußen, wenn Sie unter 18 Jahre sind´“[299], sind nicht dazu geeignet, eine strafrechtliche Sanktion auszuschließen, da Jugendliche und Kinder bekanntlich angesichts solcher Verbote erst recht neugierig werden. Das Gericht wird regelmäßig Vorsatz unterstellen müssen, da anerkannt ist, daß der Täter auch einen unerwünschten Erfolg billigen kann, wenn er sich mit dem Endergebnis abfindet[300]. „Selbst wenn man den Vorsatz verneinen würde, kommt immer noch eine Strafbarkeit für fahrlässiges Handeln gem. § 21 [Jugendschutzbereich] III GjSM in Betracht. Pornographische Schriften brauchen gem. § 6 GjSM noch nicht einmal auf dem `Index´ zu stehen, so daß praktisch wie auch rechtlich das Zwischenschalten einer Stop-Seite auf jeden Fall ohne Wirkung ist.“[301]

In der jüngsten Vergangenheit sind verschiedene Filterprogramme aufgetaucht, die den Zugriff auf diverse Seiten verhindern sollen. Hierbei handelt es sich vor allem um Erziehungshilfsmittel für Eltern, die das Surf-Verhalten ihres Kindes effektiver kontrollieren wollen. Durch die Filterprogramme (u.a. Adult-Check, Cyber-Patrol, Surf-Watch) können beispielsweise Seiten mit politischem, religiösen oder sexuellen Inhalt ausgeschlossen werden. Diese Filter können keinen ausreichenden Schutz gewähren, da die Listen der unerwünschten Seiten von den Betreibern gepflegt und ständig aktualisiert werden müssen und die verschiedenen Schutzmechanismen durch die Kinder umgangen werden können. „Ob ein Gericht bei einer Absicherung der Seite mit einem dieser Systeme eine Straflosigkeit des Anbieters dieser Seite annehmen wird, läßt sich nicht mit Sicherheit sagen.

Sieber hat in einem vielbeachteten Aufsatz aus dem Jahre 1996 Straflosigkeit angenommen, da es seiner Meinung nach bereits am Tatbestands-

---

[299] Jaeger, Computerkriminalität, Seite 172
[300] BGH St 7, 369 und 36, 9
[301] Jaeger, Computerkriminalität, Seite 172

merkmal des Zugänglichmachens fehle.“[302] Jaeger lehnt Siebers Argumentation ab[303], was m.E. auch gut begründet wurde.

Demnach bleibt eine Strafbarkeit bestehen, auch wenn der Anbieter einer Website mit pornographischen Inhalten eine Stop-Seite vorschaltet oder seine Seite durch eine Filtersoftware indizieren läßt.

9.1.18 Zusammenfassung

Grundsätzlich ist § 9 I Alt. 3 StGB auf abstrakte Gefährdungsdelikte – also die meisten netzspezifischen Verbreitungsdelikte – anwendbar. Damit ergibt sich die Anwendbarkeit des deutschen Strafrechts für Täter, die inkriminierte Inhalte im Ausland in das Internet einspeisen.

Für die Verbreitung von Propagandamitteln verfassungswidriger Organisationen gemäß § 86 I StGB ist Art. 296 EGStGB analog anwendbar.

Ausländische Erlaubnisnormen sind keine Rechtfertigungsgründe für das deutsche Strafrecht. Grundsätzlich ergibt sich für ausländische Täter, die nicht Deutsche sind und die deutsche Rechtsordnung nicht kennen, ein Verbotsirrtum nach § 17 StGB. Dieser Verbotsirrtum führt regelmäßig zur Straffreiheit.

Um das diplomatische Gleichgewicht zu halten und internationale Beziehungen nicht zu gefährden, kann die Staatsanwaltschaft § 153 c StPO anwenden, der für Auslandstaten das Opportunitätsprinzip begründet. Dabei hat sie nach pflichtgemäßem Ermessen, nach festgelegten allgemeinen Kriterien zu entscheiden.

Das TDG und insbesondere § 5 TDG ist als haftungslimitierende Norm der Anwendung strafrechtlicher Rechtsvorschriften (insbesondere der Garantenfrage) vorgeschaltet. „Im Hinblick auf die Haftung ist wie folgt zu differenzieren: Für eigene Inhalte ist der Provider als Urheber voll verantwortlich.

Für fremde Inhalte, die auf dem Server eines Providers gespeichert sind, […] kann der Anbieter unter bestimmten Vo-raussetzungen verantwortlich sein. § 5 Abs. 2 TDG eröffnet in diesen Fällen den Weg in das StGB. Die in § 5 Abs. 2 normierte individuelle Pflicht zur Nutzungsverhinderung begründet eine Ver-

---

[302] Jaeger, Computerkriminalität, Seite 173 mit weiterem Hinweis auf Sieber, JZ 1996, 429 und 494, hier 496 und OLG Karlsruhe – 1 Ss 24/84, vom 10.05.1984, NJW 1984, 1975

kehrssicherungspflicht. Eine Garantenstellung im Sinne des § 13 StGB ist für diese Fälle zu bejahen [...]. Für Inhalte, zu denen der Provider lediglich den Zugang zur Nutzung vermittelt, ist die strafrechtliche Haftung ausgeschlossen, dies gilt auch, wenn strafbare Inhalte kurzzeitig auf Cache-Servern [Proxy-Server] zwischengespeichert werden. Die Sperrverpflichtung aus § 5 Abs. 4 TDG begründet keine Handlungspflicht, die zu einer Garantenstellung führt und vermag die Haftungsprivilegierung des § 5 Abs. 3 TDG nicht zu überwinden."[304]

„Eine [...] Sperre ist im Regelfall technisch möglich und nur in besonderen Fällen unzumutbar; die Umgehungsgefahr stellt kein Argument für die Mißachtung einer Sperranordnung dar.

Ein Diensteanbieter kann sich durch sein Unterlassen als Täter oder Gehilfe strafbar machen. Die Einordnung hat unter Berücksichtigung der Umstände des Einzelfalls zu erfolgen."[305]

„Wer auf seiner privaten Homepage Links zu fremden Inhalten setzt, ist als Diensteanbieter wie ein Provider privilegiert. [Private Anbieter sind für eigene Inhalte als Content-Provider voll verantwortlich. Für fremde Inhalte, auf die sie verweisen, sind sie als Accessprovider nicht verantwortlich, es sei denn, daß die Inhalte kopiert oder Absprachen mit den Urhebern getroffen wurden.]

Der Schriftenbegriff wurde mit dem IuKDG auf `Datenspeicher´ erweitert. Von der `Körperlichkeit´ des Schriftenbegriffs wurde damit Abschied genommen. Das Verbreiten einer Schrift erfordert nach dem Willen des Gesetzgebers nach wie vor eine körperliche Übergabe. Entstehende Strafbarkeitslücken bei Verbreitungsdelikten können jedoch häufig über das Tatbestandsmerkmal des `Zugänglichmachens´ geschlossen werden.

Durch die Ergänzung des § 184 Abs. 4 und 5 StGB um das Tatbestandsmerkmal der `wirklichkeitsnahen´ Darstellung wird auch die Verbreitung künstlich hergestellter Kinderpornographie verschärft bestraft."[306]

Der Einsatz von Stop-Seiten und Exclude-Filter bewirkt keine Straffreiheit für Anbieter rechtswidriger Inhalte. Die Filter indizieren nicht vollständig, ihre

---

[303] Unter Hinweis auf OLG Stuttgart, NStZ 1992, 38 und CompuServe-Urteil des AG München, NJW 1998, 3836 ff. (nicht rechtskräftig).

[304] Jofer, Strafverfolgung im Internet, Seite 140

[305] ebd., Seite 154

[306] Jofer, Strafverfolgung im Internet, Seite 171

Anwendung ist freiwillig und Stop-Seiten machen potentielle Benutzer erst recht neugierig. Durch Eltern eingesetzte Filterprogramme können durch die Kinder - mehr oder weniger leicht - umgangen werden.

9.2 Ausgewählte Rechtsprobleme aus dem Bereich des StGB

9.2.1 Allgemeines

Wie bereits aus den phänomenologischen Betrachtungen ersichtlich wurde, bietet das Internet und andere Datennetze Straftätern eine Vielzahl von Mißbrauchsmöglichkeiten. Der Schwerpunkt der Kriminalität wird sicherlich im Bereich der netzspezifischen Verbreitungsdelikte liegen. Dabei kommt der Verbreitung von Kinderpornographie und den Propagandadelikten der rechts- und linksextremistischen Szene besondere Bedeutung zu. Folgende Straftatbestände können für das Internet von Bedeutung sein (die Aufzählung ist nicht abschließend):

- § 184 [Verbreitung pornographischer Schriften] StGB
- § 21 [Strafvorschriften] GjSM[307] [308]
- § 86 [Verbreitung von Propagandamitteln verfassungswidriger Organisationen] StGB
- § 86 a [Verwenden von Kennzeichen verfassungswidriger Organisationen] StGB[309]
- § 111 [Öffentliche Aufforderung zu Straftaten] StGB
- § 126 [Störung des öffentlichen Friedens durch Androhung von Straftaten] StGB
- § 130 [Volksverhetzung] StGB
- § 130 a [Anleitung zu Straftaten] StGB[310]

---

[307] Gesetz über die Verbreitung jugendgefährdender Schriften und Medieninhalte

[308] Zur Anwendbarkeit der Vorschriften des strafrechtlichen Jugendmedienschutzes auf im Btx verbreiteten Mitteilungen vgl. auch: Walther, NStZ 1990, 523.

[309] Zur Strafbarkeit von Hakenkreuzen in einer Mailbox vgl. auch: OLG Frankfurt a.M., Beschluß vom 18.03.1998 – 1 Ss 407/97, abgedruckt in NStZ 7/1999, Seite 356 bis 358.

[310] Zur Strafbarkeit beim Setzen von Links vgl. auch: AG Berlin-Tiergarten, Beschluß vom 30.06.1997 – 260 DS 857/96, abgedruckt in CR 2/1998, Seite 111 bis 112.

- § 131 [Gewaltdarstellung] StGB
- § 140 [Belohnung und Billigung von Straftaten] StGB
- § 23 [Öffentliche Aufforderung zur Teilnahme an verbotener Versammlung] VersG[311]
- § 166 [Beschimpfung von Bekenntnissen, Religionsgesellschaften und Weltanschauungsvereinigungen] StGB[312]
- § 185 [Beleidigung] StGB
- § 186 [Üble Nachrede] StGB
- § 187 [Verleumdung] StGB
- § 188 [Üble Nachrede und Verleumdung gegen Personen des politischen Lebens] StGB
- § 189 [Verunglimpfung des Andenkens Verstorbener] StGB
- § 353 b [Verletzung des Dienstgeheimnisses und einer besonderen Geheimhaltungspflicht] StGB
- § 353 d [Verbotene Mitteilungen über Gerichtsverhandlungen] StGB
- § 30 II [Versuch der Beteiligung] StGB (Verabredung zu einem Verbrechen)
- § 303 a [Datenveränderung] StGB
- § 303 b [Computersabotage] StGB
- § 269 [Fälschung beweiserheblicher Daten] StGB
- § 270 [Täuschung im Rechtsverkehr bei Datenverarbeitung] StGB
- § 271 [Mittelbare Falschbeurkundung] StGB
- § 274 [Urkundenunterdrückung; Veränderung einer Grenzbezeichnung] StGB
- § 348 [Falschbeurkundung im Amt] StGB
- § 201 [Verletzung der Vertraulichkeit des Wortes] StGB
- § 202 a [Ausspähen von Daten] StGB

---

[311] Gesetz über Versammlungen und Aufzüge

[312] Zur Strafbarkeit von Beschimpfungen im Internet vgl. auch: OLG Nürnberg, Beschluß vom 23.06.1998 – Ws 1603/97 (GenStA Nürnberg, StA b.d.LG Regensburg), abgedruckt in CR 11/1998, Seite 686.

- § 203 [Verletzung von Privatgeheimnissen] StGB
- § 4 [Strafvorschriften für irreführende Werbung] UWG[313]
- § 6 c [Progressive Kundenwerbung] UWG
- § 17 [Verrat von Geschäfts- oder Betriebsgeheimnissen] UWG
- § 43 [Strafvorschriften] BDSG[314]
- § 10 [Strafvorschriften] HalbleiterschutzG[315]
- § 284 [Unerlaubte Veranstaltung eines Glücksspiels] StGB
- § 29 [Anzeigepflicht, Neuzulassung] ArzneimittelG[316]
- § 14 [Bußgeldvorschriften] AdVermiG[317]
- § 37 [Verbotene Gegenstände] WaffG[318] [319]

Es wird sicherlich verständlich sein, daß nicht alle Probleme aus dem besonderen Teil des StGB und den verschiedenen Nebengesetzen behandelt werden können. Dies wird vor allem dann deutlich, wenn man der Auffassung folgt, daß fast alle Straftatbestände im Zusammenhang mit dem Internet eine Rolle spielen können. Der nachfolgende Abschnitt wird sich nun mit einigen speziellen strafrechtlichen Problemkreisen beschäftigen, die überwiegend für die Praxis Bedeutung haben.

9.2.2 § 86 [Verwenden von Kennzeichen verfassungswidriger Organisationen] StGB

§ 86 StGB stellt das Verbreiten von Propagandamitteln verfassungswidriger Organisationen unter Strafe. Die Vorschrift hat für den Bereich der netzspezifischen Verbreitungsdelikte eine besondere Bedeutung. § 86 StGB schützt den demokratischen Rechtsstaat vor verfassungswidrigen Parteien und ähnli-

---

[313] Gesetz gegen den unlauteren Wettbewerb

[314] Bundesdatenschutzgesetz

[315] Gesetz über den Schutz der Topographien von mikroelektronischen Halbleitererzeugnissen

[316] Arzneimittelgesetz

[317] Gesetz über die Vermittlung der Annahme als Kind und über das Verbot der Vermittlung von Ersatzmüttern

[318] Waffengesetz

[319] Zur Strafbarkeit eines „Terrorist´s Handbook“ über Mailbox vgl. auch: BayObLG, Beschluß vom 11.11.1997 – 4 St RR 232/97, abgedruckt in NJW 1998, 1087 f.

chen Organisationen und ihren Propagandamitteln. Obwohl in Deutschland gem. Art. 9 I [Vereinigungsfreiheit, Verbot von Maßnahmen gegen Arbeitskämpfe] GG weitgehend Vereinigungsfreiheit besteht, kann das BVerfG solche Parteien verbieten, deren Bestrebungen sich gegen die freiheitlich demokratische Grundordnung oder den Bestand der Bundesrepublik Deutschland richten (Art. 21 II [Parteien] GG).

§ 86 StGB bezieht sich nicht auf die verbotenen Organisationen selbst, sondern nur auf ihr Propagandamaterial. Gem. § 86 II StGB werden als Propagandamittel nur die Schriften erfaßt, die sich auch wirklich gegen die freiheitlich demokratische Grundordnung richten.

Die Tathandlung des § 86 I StGB besteht alternativ aus dem Verbreiten und dem Herstellen, Vorrätighalten, Einführen, Ausführen und in Datenspeichern öffentlich Zugänglichmachen. Dabei ist zu beachten, daß alle Alternativen nur dann in Betracht kommen, wenn auch eine Verbreitungsabsicht besteht. Ferner ist § 86 I StGB gem. Art. 296 EGStGB nicht auf Zeitungen und Zeitschriften anzuwenden, die im Ausland in ständiger, regelmäßiger Folge erscheinen und dort allgemein und öffentlich vertrieben werden. Wie bereits erläutert wurde, kann diese Vorschrift auch analog auf Datenspeicher übertragen werden.

Das Zurverfügungstellen von Propagandamaterial in öffentlichen Datenspeichern – darunter kann man jegliche Art von Computernetzwerken verstehen – ist strafbewehrt. Ein Zurverfügungstellen ist öffentlich, wenn eine unbestimmte Anzahl von Personen an die Daten gelangen können[320]. Das wird bei Homepages, Newsgroups und den privaten Bereichen von Mailboxen regelmäßig der Fall sein.

Wenn ein Anbieter nicht genau festlegt, welcher Personenkreis auf das Propagandamaterial zugreifen kann, und es mehr oder weniger vom Zufall abhängt, wer an das Material gelangen kann, ist der Anbieter durchgängig strafbar. Der Endverbraucher, der die Materialien nur für den Eigenbedarf besitzt, ist nach § 86 StGB nicht strafbar, da er in der Regel keine Verbreitungsabsicht hat.

---

[320] Vgl. auch: Tröndle/Fischer, Strafgesetzbuch und Nebengesetze, § 86 Rn. 9a.

9.2.3 § 184 [Verbreitung pornographischer Schriften] StGB

Wie bereits erläutert wurde, unterscheidet man in Deutschland zwischen einfacher Pornographie (§ 184 I StGB) und harter Pornographie (§ 184 III,V StGB). Zur harten Pornographie zählt die Darstellung von Gewalt (Sadismus/Masochismus), sexuellem Mißbrauch von Kindern (Kinderpornographie) und sexueller Handlungen von Menschen mit Tieren (Sodomie). Pornographie läßt sich definieren als „eine grobe Darstellung des Sexuellen in drastischer Direktheit, die in einer den Sexualtrieb aufstachelnden oder die Geschlechtlichkeit in den Schmutz ziehenden oder lächerlich machenden Weise den Menschen zum bloßen (auswechselbaren) Objekt geschlechtlicher Begierde oder Betätigung jedweder Art degradiert [...].“[321]

Einfache Pornographie darf Personen unter 18 Jahren nicht zugänglich gemacht werden. Ein Zugänglichmachen kann auch dadurch erfolgen, daß ein Benutzer Kenntnis vom Inhalt der Schrift erhält[322], demnach reicht das Anbieten eines Bildes auf einer Homepage bereits aus. Von Bedeutung sind an dieser Stelle die Ausführungen zu den Stop-Seiten, Adult-Checks und Exclude-Filtern. Das unverlangte Zusenden solcher Pornographie ist damit auch strafbar. Der Endverbraucher von einfacher Pornographie bleibt, ähnlich wie im § 86 StGB straffrei, da der einfache Besitz grundsätzlich nicht strafbar ist.

Im Bereich der harten Pornographie hat der Gesetzgeber eine umfassende Regelung vorgenommen. Gem. § 184 III StGB werden auch Schriften erfaßt, die einen wirklichkeitsnahen Mißbrauch von Kindern darstellen[323].

Von herausragender Bedeutung ist die Regelung des § 184 V StGB, nach der auch der bloße Besitz von Kinderpornographie strafbar ist. In der Vergangenheit kam es immer wieder zu folgenden Situationen: Aufmerksame Internet-Surfer hatten Kinderpornographie im Internet entdeckt und bei der Polizei gemeldet. Als Beweis hatten sie die Bilder auf ihrer Festplatte abgespeichert. Da dieses Abspeichern aber bereits einen Besitz darstellt, hatten sich die Nutzer bereits strafbar gemacht. Aus dieser Problematik geht klar hervor, daß der Ge-

---

[321] Tröndle/Fischer, Strafgesetzbuch und Nebengesetze, § 184 Rn. 7

[322] Tröndle, Strafgesetzbuch und Nebengesetze, § 184 Rn. 13, § 74 d Rn. 6 und 7

[323] Zum Begriff des Kindes und daraus resultierender Probleme vgl. auch: Bergel/Bley/Dublies/Kleinschmidt/Redlich/Rogge, Seminar Kinderpornographie - RAL 1998/2000, Seite14 bis 24.

setzgeber ein absolutes Verbot für die Kinderpornographie geschaffen hat und keine Strafbarkeitslücken duldet.

Zur Strafbarkeit nach § 184 StGB ist gem. § 15 StGB vorsätzliches Handeln erforderlich. Es sind durchaus Fälle denkbar, in denen man den erforderlichen Verbreitungsvorsatz nicht nachweisen kann. Das GjSM bietet durch § 21 I GjSM einen Auffangtatbestand für diese Fälle, da diese Vorschrift die Verbreitung pornographischer Schriften ebenfalls unter Strafe stellt. An dieser Stelle muß beachtet werden, daß es im GjSM nur um das „Verbreiten“ von Schriften geht, nicht um den Besitz[324]. Gem. § 21 III GjSM reicht für eine Strafbarkeit bereits fahrlässiges Verbreiten aus. Durch § 3 I Nr. 4 GjSM werden auch die elektronischen Informations- und Kommunikationsdienste in den Geltungsbereich des GjSM miteinbezogen. Daher sind kaum Strafbarkeitslücken denkbar.

Grundsätzlich ist das GjSM nur anwendbar, wenn sich die betreffenden Schrift im Index befindet. Gem. § 11 GjSM entscheidet die Bundesprüfstelle über die Aufnahme einer Schrift in den Index[325]. I.S.d. § 6 GjSM werden aber auch sonstige schwergefährdende Schriften erfaßt, die nicht zwingend im Index stehen müssen[326]. Hierzu zählen Schriften nach den §§ 130 II, 131, 184 StGB und Schriften, die offensichtlich dazu geeignet sind, Kinder oder Jugendliche schwer zu gefährden. Diese Schriften unterliegen dann automatisch einem Verbreitungsverbot an Kinder und Jugendliche (§ 3 GjSM), einem Verbreitungsverbot außerhalb von Geschäftsräumen (§ 4 GjSM) und einer Werbebeschränkung (§ 5 GjSM).

9.2.4 Surfen im Internet und Herunterladen von rechtswidrigem Material

Das Surfen im Internet ist grundsätzlich nicht reglementiert. D.h. daß sich jeder Benutzer im Internet frei bewegen kann. Er kann alle Seiten besuchen und sich auch alle Inhalte anschauen und durchlesen. Dies gilt für Propagandamittel i.S.d. § 86 StGB genauso, wie für harte Pornographie i.S.d. § 184 StGB. Rein passives Verhalten kann nie ein Verbreiten, Besitz oder eine ähnli-

---

[324] Vgl. dazu auch die nachfolgenden Abhandlungen über den strafbaren Besitz „harter Pornograpie“ nach § 184 V StGB.

[325] Das Verfahren richtet sich nach der DVO GjSM.

[326] hierzu zählen Schriften nach §§ 130 II, 131, 184 StGB und Schriften, die offensichtlich dazu geeignet sind, Kinder oder Jugendliche schwer zu gefährden

che Handlung sein. Über das reine Anschauen hinaus geht das Abspeichern von Inhalten auf der lokalen Festplatte. Hier kann nach h.M. bereits Besitz, Beziehen oder Vorrätighalten vorliegen. Da die meisten Vorschriften, die den netzspezifischen Verbreitungsdelikten zugeordnet werden, zusätzlich ein Verbreiten oder eine Verbreitungsabsicht fordern, ergibt sich für den Endverbraucher regelmäßig ein strafloser Besitz. Zu beachten ist die Regelung § 184 V StGB. „So hat jetzt auch das AG Hamburg [...] zu recht entschieden, daß derjenige, der Dateien mit Kinderpornographischen Bildern auf seinem Computer vorhält, sich nach § 184 V StGB strafbar macht.“[327]

Gelangt der Surfer auf eine Paßwortgeschützte Seite, darf er nur auf legalem Wege ein Paßwort erwerben. Das Hacken der Paßwortsperre ist nicht zulässig und kann ggf. gem. § 202 a [Ausspähen von Daten] StGB strafbar sein.

9.2.5 Angeben einer falschen Identität

Im Internet ist es üblich, anonym zu bleiben. Viele Benutzer machen in Chat-Foren oder in Webformularen falsche Angaben über ihre Identität. Den wesentlichsten Anteil an der Anonymisierung tragen dabei die FreeMailer. Grundsätzlich ist nichts gegen die Anonymität eines Internetbenutzers einzuwenden. Wie im wirklichen Leben kann er seine wahre Identität weitestgehend geheimhalten. Diese Freiheit garantiert ihm das Recht auf informationelle Selbstbestimmung, welches durch die Rechtsprechung aus Art. 2 I GG abgeleitet wurde.

Wenn ein Benutzer seine wahre Identität aber verschweigt, um jemanden zu täuschen oder zu schädigen, kann sich durchaus eine Strafbarkeit nach den einschlägigen Betrugsvorschriften ergeben.

„Eine Strafbarkeit wegen Urkundenfälschung entfällt nach der herrschenden Ansicht. Zunächst einmal scheitert eine Strafbarkeit nach § 267 StGB am Fehlen einer stofflichen Gedankenerklärung, zumindest fehlt es aber an der Möglichkeit, den Inhalt optisch-visuell zu verstehen. [...] Auch die Fälschung

[327] Jaeger, Computerkriminalität, Seite 168 mit Hinweis auf: AG Hamburg – 141a II-101/97, vom 08.07.1997, abgedruckt in CR 1998, 33 ff.

einer technischen Aufzeichnung ist nicht gegeben: Der Benutzer stellt nämlich hier nur eine inhaltlich unrichtige Aufzeichnung her.“[328]

9.2.6 Anzeigepflichten

Eine Pflicht zur Strafanzeige – bei Kenntnis von einer Straftat – besteht in Deutschland grundsätzlich nicht. Eine Ausnahme bildet der Straftatbestand des § 138 [Nichtanzeige geplanter Straftaten] StGB. Demnach kann auch jemand strafrechtlich belangt werden, der es unterläßt, geplante Straftaten aus dem abschließenden Katalog des § 138 I StGB anzuzeigen. Der Katalog enthält ausnahmslos geplante Straftaten der schweren Kriminalität (z.B. §§ 80 [Vorbereitung eines Angriffskrieges] oder 211 [Mord] StGB), also keine Bagatelldelikte. Die Betonung muß an dieser Stelle auf „geplant“ liegen. D.h. daß für bereits verübte Straftaten keine Anzeigepflicht mehr besteht.

Für den Internetnutzer ergibt sich also nur eine Anzeigepflicht, wenn er beispielsweise auf einer Homepage, in einer Newsgroup oder in einem Chat von dem Tatplan einer Katalogstraftat nach § 138 I StGB erfährt. Wird der Tatplan nicht umgesetzt, kann gemäß § 139 I [Straflosigkeit der Nichtanzeige geplanter Straftaten] StGB von einer Strafe abgesehen werden.

9.2.7 Recht am eigenen Bild

Wenn man auf einer Homepage fremde Bilder einbindet, muß man die Urheberrechte für diese Bilder besitzen oder es muß eine Einwilligung des Urhebers vorliegen. Wenn man ein Bild von sich selbst auf einer Homepage veröffentlicht, behält man gem. § 22 KunstUrhG[329] die Urheberrechte an diesem Bild. Eine Weiterverbreitung oder Weiterverwendung durch Dritte ist nicht gestattet[330].

9.2.8 Newsgroups

Bei Newsgroups unterscheidet man zwischen moderierten und unmoderierten Gruppen. Das besondere an den moderierten Gruppen ist, daß die Bei-

---

[328] Jaeger, Computerkriminalität, Seite 169

[329] Kunsturhebergesetz

[330] Vgl. auch: Jaeger, Computerkriminalität, Seite 176.

träge, die einzelne Teilnehmer senden, durch Menschen geprüft werden, bevor sie der Allgemeinheit zugänglich gemacht werden. Diese Moderatoren prüfen also jede News, bevor sie ins Netz gestellt wird. Wenn sich die Newsgroup moderiert nennt, müssen die Moderatoren m.E. auch wirklich jeden Beitrag prüfen, da sie durch diese Verfahrensweise automatisch eine Verantwortung übernommen haben. Da sie die Möglichkeit der Kenntnisnahme haben, werden sie nach § 5 II TDG eingestuft. Sie sind in diesem Sinne Serviceprovider und für fremde Inhalte verantwortlich, wenn sie davon Kenntnis erhalten. Da alle Beiträge durch ihre Hände laufen, kann man davon ausgehen, daß ein strafbarer Beitrag durch den Moderator gebilligt wurde.

Für unmoderierte Newsgroups ergibt sich die Verantwortlichkeit ebenfalls aus § 5 II TDG. Allerdings ergibt sich für den News-Server-Betreiber erst eine Strafbarkeit, wenn er Kenntnis von einer strafbaren News erhält. Grundsätzlich ist er dann verpflichtet, die betreffende News auf seinem Server zu löschen. In einen anderen News-Server darf er hingegen nicht eingreifen[331].

Fraglich ist, ob auch das Sperren ganzer Newsgroups zulässig ist. Unstrittig ist, daß der Betreiber bestimmte Beiträge ablehnen kann, was ja den moderierten Newsgroups entspricht. Jaeger stellt in diesem Zusammenhang ein 3-Stufen-Modell vor[332]: Danach sollen Newsgroups, die eindeutig auf rechtswidrigen Inhalt schließen lassen (z.B. alt.sex.sodomie oder alt.sex.children), denen der Mißbrauch praktisch immanent ist, von allen Betreibern geschlossen werden. Für alle anderen Gruppen ergeben sich keine Prüf- oder Zensurpflichten. Wenn der Provider allerdings positiv von einem rechtswidrigen Inhalt Kenntnis erlangt, muß er nur den einzelnen Beitrag in der Newsgroup auf seinem Server canceln und nicht die ganze Newsgroup.

Wer rechtswidrige Inhalte an News anhängt, macht in öffentlichen Datenspeichern zugänglich, fordert öffentlich auf etc. und macht sich somit nach den meisten Straftatbeständen, die den netzspezifischen Verbreitungsdelikten zuzuordnen sind, strafbar.

---

[331] Jaeger, Computerkriminalität, Seite 182, geht davon aus, daß ein sogenanntes „Fremdcanceln“ (löschen von News auf fremden Servern) den Tatbestand des § 303 a StGB erfüllen und daß das lediglich durch Notwehr gerechtfertigt sein könnte.

[332] Jaeger, Computerkriminalität, Seite 183 und 184 mit Hinweis auf: Altenhain, CR 1997, 485, 493, der von einer Sperrungspflicht bei einer teilweise inkriminierten Newsgroup ausgeht; Sieber, CR 1997, 657 f., der eine solche Sperrungspflicht bezweifelt.

9.2.9 Chat

Zur Verantwortlichkeit eines Chat-Anbieters sind – soweit ersichtlich – keine umfassenden Ausführungen bekannt. Der Chat-Anbieter hat keine Garantenstellung, da das Anbieten eines Chats an sich keine Gefahrenquelle darstellt. Eine Überwachungspflicht ist demnach nicht herleitbar. Werden in einem Chat strafbare Inhalte verbreitet, kann der Anbieter auch nicht wegen Beihilfe strafbar sein, da er in der Regel keinen Beihilfevorsatz gem. § 27 I StGB haben wird. Werden die Foren allerdings durch den Anbieter allein aus dem Grund eingerichtet, die Verbreitung strafbarer Inhalte zu ermöglichen, ist Beihilfe zu prüfen.

Der Chat-Anbieter unterliegt m.E. den Regelungen des § 5 II TDG. Demnach ist er auch verpflichtet, bei positiver Kenntnis strafbare Inhalte zu sperren. Eine Pflicht zu Stichproben kann mithin nicht abgeleitet werden[333].

Eine Sperrung von Inhalten stellt bei den Chats aber ein größeres Problem dar, als bei den Newsgroups, da die Inhalte nicht dauerhaft gespeichert werden. Der Chat ist ja mehr oder weniger ein unendlich langes Gespräch, in das der Benutzer an beliebiger Stelle einsteigt und es auch jeder Zeit wieder verlassen kann. In den meisten Chats kann beim Clienten eine Funktion eingestellt werden, wieviele Zeilen der Client anzeigen soll. Alle Inhalte, die aus diesem Bereich herausfallen, sind unwiederbringlich verloren. Eine Protokollierung der Gespräche auf den Chat-Servern findet nicht statt. Da also eine Löschung von Inhalten objektiv nicht möglich ist, kann eine Sperrung nur durch den Ausschluß des Betreffenden erfolgen. Dieser kann sich aber unter einem neuen Nickname jederzeit wieder einloggen. Aus dieser Verfahrensweise würde sich also unweigerlich ein „Katz-und-Maus-Spiel“ ergeben.

M.E. ist in diesen Fällen wie folgt zu verfahren. Wenn in einem Channel rechtswidrige Inhalte verbreitet werden, müssen die Beteiligten durch den Operator ausgeschlossen werden[334]. Channels, die überwiegend für die Begehung von Straftaten genutzt werden, müssen komplett gesperrt werden. Eine Prü-

---

[333] Jaeger, Computerkriminalität, Seite 187, mit Hinweis auf: Altenhain, CR 1997, 485, 492 und Einstellungsbescheid der StA beim LG München I – 467 Js 319998/96, vom 16.01.1997.

[334] In Chats, in denen grundsätzlich kein Operator anwesent ist, kann man oft durch die Eingabe eines bestimmten Befehls einen Operator hinzurufen; dieser kann dann die entsprechenden Maßnahmen einleiten.

fung muß die Gegebenheiten des Einzelfalls berücksichtigen. In diesem Sinne können dann auch die Belange eines Einzelnen hinter den Interessen der Allgemeinheit zurückstehen. Das 3-Stufen-Modell von Jaeger ist also auch auf den Chat übertragbar.

Wie bereits dargestellt wurde, gibt es beispielsweise beim IRC die Funktion des Operators. Dieser Operator hat die Aufsicht über einen Channel, da er diesen geöffnet hat. Er entscheidet, welche Benutzer an diesem Channel teilnehmen können. Ggf. kann er auch Benutzer ausschließen. Es lassen sich nun im Wesentlichen zwei Fallgruppen unterscheiden. Zum einen kann der Chat-Anbieter gleichzeitig der Operator sein (z.B. ein Angestellter) oder ein Benutzer eröffnet einen eigenen Channel und wird dadurch zum Operator. Grundsätzlich sind die Ausführungen zu den moderierten Newsgroups auch auf die Channels mit Operator übertragbar. D.h. daß dem Operator eine Überwachungspflicht zuerkannt werden muß. Duldet der Operator die Verbreitung rechtswidriger Inhalte, haftet er ebenfalls.

9.2.10 E-Mail

Auch bei der Benutzung von E-Mail ist es durchaus nicht unüblich, seine Identität geheimzuhalten[335]. Wie bereits dargestellt, ist gegen diese Anonymität nichts einzuwenden. Wird sie aber beispielsweise zum Zwecke eines Betruges oder einer Beleidigung vorgenommen, überschreitet der Betreffende die Grenze der Legalität. Eine Strafbarkeit wegen Fälschung einer Urkunde (§ 267 StGB) oder Fälschung einer technischen Aufzeichnung (§ 268 StGB) entfällt aus den bereits dargelegten Gründen.

Die Fälschung einer bereits existierenden E-Mail stellt eine strafbare Datenveränderung gem. § 303 a [Datenveränderung] StGB dar.

Fraglich ist, wie das unberechtigte Lesen einer E-Mail strafrechtlich zu qualifizieren ist. Es liegt nahe, den Tatbestand des § 202 [Verletzung des Briefgeheimnisses] StGB anzuwenden. „§ 202 StGB regelt eindeutig, daß Tatgegenstand ein `verschlossener Brief´ oder ein `anderes verschlossenes Schriftstück´ sein kann. Ein Schriftstück [...] jedoch ist ein `Stück´ und damit

eine Sache, also ein körperlicher Gegenstand. Eine E-Mail kann ein solcher körperlicher Gegenstand nicht sein.“[336] Demnach ist § 202 StGB auf E-Mails nicht anwendbar. Anders verhält es sich, wenn die E-Mail ausgedruckt und dann auf dem herkömmlichen Postweg weiterverschickt wird.

Ein unberechtigtes Lesen von E-Mails könnte aber unter § 202 a [Ausspähen von Daten] StGB subsumiert werden. Ohne Zweifel gehört die E-Mail zu den Daten, die ausschließlich für den Empfänger bestimmt sind. Fraglich ist, ob eine E-Mail gegen einen Zugriff besonders gesichert ist. M.E. ist das Tatbestandsmerkmal der besonderen Sicherung weit auszulegen. Demnach wird eine einfache Paßwortsicherung für den E-Mail-Account ausreichen[337].

Oft haben Benutzer ihren E-Mail-Clienten so eingestellt, daß sie lediglich eine Schaltfläche betätigen müssen, um ihre E-Mails abzuholen. Der Benutzername und das Paßwort werden dabei automatisch gespeichert, so daß ein immer wiederkehrendes Eingeben durch den Benutzer entfallen kann. Hat der Täter einen ungesicherten Zugriff auf das System selbst und nutzt er dann einen solchen automatisierten Clienten, um fremde E-Mails anzuschauen, macht er sich nicht strafbar. Muß er hingegen erst ein SystemPaßwort umgehen (z.B. das Paßwort des Bildschirmschoners), kann er strafrechtlich belangt werden, obwohl der eigentliche Account selbst nicht geschützt ist. Dies gilt auch für Systembetreiber, die ja durch sogenannte Superuser-Rechte Zugriff auf das gesamte System haben. Der Systembetreiber darf also auch keine fremden E-Mails abrufen oder lesen.

Interessant ist dies auch für die Betreiber von E-Mail-Servern. Sie dürfen in diesen Fällen also auf gar keinen Fall Stichproben in den Benutzeraccounts machen, da sie sich sonst nach § 202 a StGB strafbar machen würden.

Eine Form des Mißbrauchs von E-Mail ist Spamming. Spamming kann zum Zusammenbruch eines E-Mail-Servers führen. Da die Datenverarbeitungsanlage unbrauchbar gemacht wird, könnte beim Zusammenbruch eines Servers

---

[335] Die gängigste Praxis stellt dabei die Benutzung von Remailern des Typs I oder II dar; vgl. auch: Federrath/Berthold/Köhntopp/Köpsell, Tarnkappen fürs Internet, c´t 16/2000, Seite 148 bis 155 und Bleich, Selbstverdunkelung, c´t 16/2000, Seite 156 bis 159.

[336] Jaeger, Computerkriminalität, Seite 187

[337] So auch Jaeger, Computerkriminalität, Seite 188 mit Hinweis auf: Wenning, JurPC Web-Dok. 46/1998, Abs. 21, der davon ausgeht, daß eine E-Mail nur dann geschützt ist, wenn sie selbst ver-

durch Spamming eine Computersabotage gem. § 303 b I Nr.2 [Computersabotage] StGB vorliegen. Eine Unbrauchbarkeit einer technischen Anlage liegt vor, wenn sie ihren Zweck nicht mehr erfüllen kann[338]. Da fahrlässiges Handeln in diesen Fällen ausgeschlossen ist, liegt das eigentliche Problem beim Spamming in der Begründung des Vorsatzes.

Wie bereits erläutert, betrifft das Spamming direkt den Systembetreiber (Betreiber des E-Mail-Servers). Der einzelne Benutzer erhält Junk-Mails. Ungefragt eintreffende E-Mails mit Werbung verstoßen gegen § 1 UWG und sind daher nicht hinzunehmen[339]. Eine Strafbarkeit gem. § 303 a I Nr.2 StGB muß an dieser Stelle regelmäßig entfallen, da der Computer eines einzelnen Benutzers in der Regel keine Datenverarbeitungsanlage von wesentlicher Bedeutung sein wird, wie es § 303 a StGB ausdrücklich fordert. Handelt es sich bei dem betroffenen Rechner um eine Datenverarbeitungsanlage (von wesentlicher Bedeutung) eines fremden Betriebes, Unternehmens oder Behörde, ist eine Strafbarkeit zu prüfen. Das gezielte Überfluten eines Rechners mit E-Mails (Mail-Bombing) ist ebenfalls gem. § 303 a I Nr.2 StGB strafbar.

9.2.11 Suchmaschinen und Verzeichnisse

Das Internet birgt eine unüberschaubare Vielzahl von Informationen. Die Betreiber von Suchmaschinen und Verzeichnissen versuchen durch Suchdienste und Kataloge Ordnung in das Durcheinander zu bringen.

Bei einer Suchmaschine gibt der Nutzer ein bestimmtes Stichwort ein und der Dienst liefert eine Trefferliste mit den gefundenen Inhalten. Der Benutzer kann dann einen Eintrag anklicken und gelangt so auf die betreffende Seite. Den Suchmaschinen liegen Programme zugrunde, die das Internet automatisch nach Inhalten durchsuchen. Dabei „hangeln“ sich die Programme entlang der Links von Seite zu Seite und indizieren diese dann nach Stichworten. Diese Stichworte erhalten sie entweder direkt vom Ersteller der Website über ein

---

schlüsselt ist; Haft, NStZ 1987, 6, 9 f., der davon ausgeht, daß nur Daten geschützt werden, die einen wirtschaftlichen Wert besitzen.

[338] Tröndle, Strafgesetzbuch und Nebengesetze, § 133 Rn. 10

[339] Jaeger, Computerkriminalität, Seite 190, mit Hinweis auf: Ernst, JuS 1997, 776, 780 und Anm. Ernst, NJW-CoR 1997, 494 f.; LG Traunstein – 2 HK O 3755/97 vom 14.10.1997 (EV) und vom 18.12. 1997 (PKH), abgedruckt in NJW-CoR 1997, 494 und CR 1998, 171 f.; LG Berlin – 16 O 201/98, Beschluß vom 02.04.1998, und 16 O 301/98, Beschluß vom 14.05.1998 – angeschlossen; ablehnend Reichelsdorfer, Anm. zu LG Traunstein, CR 1998, 172 f. und Funk, CR 1998, 411 ff.

META-Tags oder leiten diese u.a. aus Überschriften ab. An dieser Stelle wird deutlich, daß bei Suchmaschinen kein Mensch über die Indizierung und die ausgegebene Trefferliste entscheidet. Daher kann sich der Betreiber einer Suchmaschine auch nicht strafbar machen, wenn ein Treffer aus einer Hitliste beispielsweise auf eine Homepage mit rechtswidrigem Inhalt verweist. Ein Gehilfenvorsatz ist ebenfalls abzulehnen, ebenso eine Garantenstellung. Suchmaschinen sind mithin als Accessprovider gem. § 5 III TDG einzustufen. Erhalten die Betreiber positiv Kenntnis von Links auf rechtswidrige Inhalte, sind sie verpflichtet, die Links zu löschen. Zur Durchsetzung der Maßnahme ist nur der Verwaltungszwang möglich.

Verzeichnisse funktionieren grundlegend anders. Hier wird durch eine Redaktion geprüft, welche Websites in den Katalog aufgenommen werden und welche nicht. Verzeichnisse müssen demnach wie Homepage-Betreiber behandelt werden. Ein Link innerhalb eines Verzeichnisses kann daher nur dann strafbar sein, wenn der Betreiber in Kenntnis des rechtswidrigen Inhalts der verlinkten Seite den Link vorsätzlich setzt.

9.2.12 Cookies

Cookies[340] sind kleine Dateien, die ein Server auf der lokalen Festplatte eines Benutzers abspeichert, wenn dieser das erste Mal eine Website besucht. In diesen Dateien werden bestimmte Informationen gespeichert. Diese Informationen sollen vor allem dazu dienen, Einstellungen, die ein Benutzer auf einer Website vorgenommen hat, zu speichern. Der sich daraus ergebende Vorteil ist, daß der Benutzer bei jedem Besuch eine angepaßte Seite bekommt. Zu diesem Zweck liest der Server das Cookie wieder aus. „Selbstverständlich können diese Daten durchaus mißbraucht werden um ein Benutzerprofil eines Anwenders zusammenzustellen, so daß die Cookies [...] aus datenschutzrechtlicher Sicht sehr interessant sind [...]. Die meisten Browser bieten auch eine Funktion an, die das Senden von Cookies unterbindet.“[341]

Gem. § 4 IV [Datenschutzrechtliche Pflichten des Diensteanbieters] TDDSG dürfen Nutzungsprofile nur unter Verwendung von Pseudonymen er-

[340] Cookie (engl.), dt.: Keks

[341] Jaeger, Computerkriminalität, Seite 155, mit Hinweis auf: Bizer, DuD 1998, 277 ff.

stellt werden. D.h. daß personenbezogene Cookies gegen die datenschutzrechtlichen Bestimmungen des TDDSG verstoßen.

9.2.13 Hacker-Tools

Als Hacker bezeichnete man ursprünglich begabte Experten aus dem Computerbereich. Heute wird das Wort „Hacker“ aber fast ausschließlich als Synonym für Kriminelle gebraucht, die mittels Computer und Computernetzwerken Straftaten begehen. Für ihre Zwecke benutzen die Hacker oft selbstgeschriebene Programme, die auch untereinander getauscht werden. Dem Grunde nach kann ein solches Programm immer aus zwei Blickwinkeln betrachtet werden. Zum einen kann es helfen, diverse Sicherheitslücken in einem System aufzudecken und zum anderen kann es aber auch dazu verwendet werden, ein System zum Absturz zu bringen oder in einen Rechner „einzubrechen“. Die Benutzung solcher Programme ist strafbar. Wenn kein Erfolg eintritt, ist auf jeden Fall ein strafbarer Versuch zu prüfen. Fraglich ist, ob das Anbieten eines solchen Programms (Tool) strafbar ist.

Jaeger geht davon aus, daß eine Strafbarkeit grundsätzlich besteht, sich eine Beurteilung aber stets an den Gegebenheiten des Einzelfalls ausrichten muß[342]. Nach seiner Ansicht ist die Grenze zur strafbaren Beihilfe in dem Moment überschritten, in dem der Anbieter solcher Produkte nicht mehr auf einen legalen Einsatz vertrauen darf. Dies kann sich beispielsweise aus der Art der Anpreisung oder der Höhe des Preises ergeben. Wenn die legalen Dienste (z.B. als Administration-Tools) in den Vordergrund gestellt werden, muß wohl von einer Straflosigkeit ausgegangen werden.

9.3 Grundlagen des Strafprozeßrechts

9.3.1 Örtliche und sachliche Zuständigkeit

Ähnlich der Tatortfrage im allgemeinen Teil des deutschen Strafrechts stellt sich aus strafprozessualer Sicht die Frage nach der örtlichen Zuständigkeit der Gerichte und der Staatsanwaltschaft (StA).

---

[342] Jaeger, Computerkriminalität, Seite 38 und 39, mit Hinweis auf: Jaeger, RDV 1998, Heft 6; Jaeger, Brenzlige Bytes – Sind Hacker-Tools strafbar?, c´t 5/98, S.18; LG Frankfurt a.M. – 3-12 O 207/97, vom 04.02.1998, abgedruckt in DuD 1998, 415 ff.

Maßgeblich für die Bestimmung der örtlichen Zuständigkeit der Gerichte sind die §§ 7 ff. StPO. Die Zuständigkeit der StA lehnt sich gemäß § 143 I [Örtliche Zuständigkeit] GVG an die örtliche Zuständigkeit des Gerichtes an. Ermittelnde Polizeibeamte sind der StA untergeordnet. Um in den meisten Bereichen der StPO tätig werden zu können, müssen Polizeibeamte Hilfsbeamte der StA i.S.d. § 152 I,II [Hilfsbeamte der Staatsanwaltschaft] GVG sein. Wer eine solche Hilfsbeamteneigenschaft besitzt, wird auf Landesebene jeweils durch eine Verordnung bestimmt. Auch für Brandenburg existiert eine solche Verordnung[343].

Gemäß § 7 [Gerichtsstand des Tatortes] StPO ist der Gerichtsstand bei dem Gericht begründet, in dessen Bezirk die Straftat begangen worden ist. An welchem Ort die Straftat begangen wurde, regelt sich weitestgehend nach den Vorschriften des allgemeinen Teils des StGB, § 9 StGB. Wenn man der vorangegangenen Argumentation folgt, daß der Tatort an jedem beliebigen Ort der Welt sein kann, an dem beispielsweise strafbare Informationen abgerufen werden können, kann demzufolge auch jede deutsche StA für die Strafverfolgung zuständig sein, also auch jede Polizeibehörde. Eine weitere Eingrenzungsmöglichkeit bieten die §§ 8 [Gerichtsstand des Wohnsitzes oder Aufenthaltsortes] und 9 [Gerichtsstand des Ergreifungsortes] StPO. Ist ein Gerichtsstand nach mehreren Varianten begründbar, ist nach § 12 [Zusammentreffen mehrerer Gerichtsstände] StPO zu verfahren. Danach ist diejenige Stelle zuständig, die zuerst eine Untersuchung eröffnet hat. Befindet sich der Täter also im Inland, ergeben sich keine Verfolgbarkeitslücken. Bei Tätern, die aus dem Ausland agieren ist § 7 StPO anzuwenden.

Hinsichtlich der sachlichen Zuständigkeit ergeben sich für den Bereich der Internetstraftaten keine Besonderheiten. I.S.d. § 160 [Ermittlungsverfahren] StPO hat die StA bei Verdacht einer Straftat den entsprechenden Sachverhalt zu erforschen. Für die Polizei gilt Entsprechendes gemäß § 163 [Aufgaben der Polizei] StPO.

---

[343] Verordnung über die Hilfsbeamten der Staatsanwaltschaft vom 28.12.1995, GVBl. II 1996 S. 62

9.3.2 Ermittlungen mit Auslandsbezug

Für Ermittlungen im Inland gilt grundsätzlich: „Für die Rechtmäßigkeit und Wirksamkeit gerichtlicher Entscheidungen ist die örtliche Zuständigkeit ebensowenig Voraussetzung wie für die Vornahme von Untersuchungshandlungen, § 20 [Handlungen eines unzuständigen Gerichts] StPO.“[344] Wie aber sind Ermittlungen einzustufen, die beispielsweise auch Rechner im Ausland einbeziehen können? Was passiert, wenn deutsche Behörden Daten auf ausländischen Servern sichten?

Grundsätzlich gilt, daß Hoheitsakte – also Akte der Legislative, Exekutive und Judikative – auf fremden Hoheitsgebieten nur im Wege der internationalen Rechtshilfe zulässig sind. Muß sich nun ein Polizeibeamter, der sich dienstlich im Internet bewegt, von allen eventuell betroffenen Staaten eine Erlaubnis holen? Jofer stellt die entscheidende Frage, ob es sich bei der gezielten repressiven Benutzung des Internets durch inländische Strafverfolgungsbehörden überhaupt um einen Hoheitsakt handelt. Normalerweise geht man von einer Völkerrechtsverletzung dann aus, wenn ein ermittelnder Beamter innerhalb eines fremden Hoheitsgebietes handelt. Dabei muß sich der Beamte aber physisch auf dem Hoheitsgebiet befinden[345]. Regelmäßig ist der Beamte bei Online-Ermittlungen aber nicht auf einem fremden Hoheitsgebiet physisch anwesend. Vielmehr agiert er von seinem eigenen Hoheitsgebiet aus. Demnach kann das Territorialitätsprinzip nicht beeinträchtigt sein.

Allerdings existieren auch gegenteilige Auffassungen, die sehr wohl von einem völkerrechtlichen Verstoß ausgehen[346], da der ermittelnde Beamte einen ausländischen Computer aktiviert, also ein wirkliches Geschehen (Ermittlung) im Ausland abläuft. Demzufolge führt die Diskussion nicht zu einem befriedigenden Ergebnis.

Das Internet stellt sich als internationales Medium dar. Der länderübergreifende Charakter des Netzwerkes ist ausdrücklich, auch von staatlicher Seite, erwünscht. Dies wird umsomehr deutlich, wenn man das staatliche Engagement in den Anfangszeiten des Internets berücksichtigt. Es kann nicht der

---

[344] Jofer, Strafverfolgung im Internet, Seite 190 mit Hinweis auf BGHSt NJW 1978, S. 835

[345] Vgl. auch: Jofer, Strafverfolgung im Internet, Seite 190.

[346] Nachweisführung bei Jofer, Strafverfolgung im Internet, Seite 190 bis 196

Wille eines Staates sein, in technischer Hinsicht international zu denken und in rechtlicher Hinsicht national. Der Staat hat m.E. bereits durch die Befürwortung der Internationalität des Netzwerkes einen Teil seiner Souveränität aufgegeben. Die Souveränität wird im Bereich des Internets eingeschränkt aber nicht aufgehoben.

Wenn also ein Staat augenscheinlich auf dem Gebiet eines anderen Hoheitsträgers tätig wird, könnte geprüft werden, wie stark die Rechtskreise beider betroffener Staaten berührt sind. Als Anknüpfungspunkt für diese Prüfung könnte eine Betrachtung des Rechtskreises der jeweils betroffenen Individuen sein. Schlochau geht davon aus, daß eine Handlung auf fremdem Staatsgebiet unbedenklich ist, wenn sie ohne Zwang vorgenommen wird[347]. Dabei soll eine Handlung immer dann Zwang enthalten, wenn Grundrechte berührt werden. Im Gegensatz zur staatlichen Zwangshandlung werden bei schlicht hoheitlichem Handeln (z.B. Streifenfahrt, Zeitung lesen, Plakate anschauen etc.) keine Grundrechte berührt. Es stellt sich also die Frage, ob die staatliche Teilnahme am Internet einen Grundrechtseingriff darstellt oder nicht.

Im Volkszählungsurteil[348] hat das Bundesverfassungsgericht (BVerfG) festgestellt, daß aus Art. 1 I [Schutz der Menschenwürde] i.V.m. Art 2 I [Allgemeines Persönlichkeitsrecht] GG ein Recht auf informationelle Selbstbestimmung (RIS) abgeleitet werden kann. Grundtenor des Urteils ist, daß es keine unwichtigen Daten gibt und jeder selbst bestimmen kann, welche Daten er von sich preisgibt und welche nicht.

Wenn also der Staat von einem Bürger Informationen erlangen will, braucht er dazu eine Ermächtigungsgrundlage. Allerdings ist nicht jede Maßnahme, die den Schutzbereich eines Grundrechts tangiert, als Grundrechtseingriff zu qualifizieren. „Die Rechtsprechung nimmt einen solchen Eingriff an, wenn die Schwelle zur bloßen Belästigung oder alltäglichen Bagatelle überschritten wird. Der Zugriff auf fremde Dateien, die auf Internetservern oder Mailboxen abgelegt sind, stellt deshalb jedenfalls dann einen Eingriff [...] dar, wenn die begehrten Daten nicht für jedermann frei verfügbar sind. Durch Zugangsbeschränkungen oder das Erfordernis einer vorherigen Anmeldung bringt

---

[347] ebd., Strafverfolgung im Internet, Seite 191
[348] BVerfGE 65, 1, 58

der Betreiber Dritten gegenüber zum Ausdruck, daß er seine Informationen nicht jedem preisgeben will. [...] Kein Grundrechtseingriff ist anzunehmen, wenn Daten für jedermann frei auf der Welt und ohne Zugangskontrolle abgerufen werden können [...] Diese Daten sind nicht der Privatsphäre zuzurechnen.“[349]

Es bleibt also festzustellen, daß der Rechtskreis des ausländischen Staates nur unwesentlich beeinträchtigt wird. Ein abgegrenztes Hoheitsgebiet kann es im Internet nicht geben, dennoch gibt ein Staat seine Souveränität nicht auf. Wenn die individuellen Rechte eines ausländischen Staatsbürgers nicht beeinträchtigt werden, wird auch nicht das Schutzbedürfnis des jeweiligen Staates beeinträchtigt. Somit kann sich jede staatliche Behörde so im Internet bewegen, wie es ein – sich legal verhaltender – Bürger auch tun kann. „Reine“ Ermittlungshandlungen müssen sich auf Rechner, die im Inland stehen, beschränken. Notfalls muß vor Eingriffsmaßnahmen der Standort des Rechners bestimmt werden. Das gleiche gilt für präventive Maßnahmen der Polizei. Hierbei wird der Kreis allerdings enger gezogen, da Gefahrenabwehr Sache der Bundesländer ist[350].

9.3.3 Aktive Mitwirkungspflichten von Zeugen und Betroffenen

Die wichtigsten Betroffenen in einem Ermittlungsverfahren sind laut StPO Zeugen und Tatverdächtige/Beschuldigte. Je nachdem, welche Stellung ein Betroffener in einem Strafverfahren hat, ergeben sich daraus für ihn verschiedene Rechte und Pflichten. Welche dieser Rechte und Pflichten für den Bereich der Ermittlungen bei Internetstraftaten von besonderer Bedeutung sind, soll an dieser Stelle aufgezeigt werden.

„Der Zeuge [...] ist ein nicht am Verfahren beteiligter Dritter, der den Ermittlern zur Wahrheitserforschung zur Verfügung steht. Ein Zeuge ist verpflichtet zu erscheinen, auszusagen und ggf. zu beschwören.“[351] Eine Ausnahme ist nur dann möglich, wenn sich der Zeuge auf eines seiner Zeugnisverweige-

---

[349] Jofer, Strafverfolgung im Internet, Seite 192 und 193 mit Hinweis auf BVerwGE 87, 37, 43 f; 90, 112, 121 f. und Bär, CR 1995, S. 234

[350] Die rechtliche Betrachtung der anlaßunabhängigen Recherchen im Internet durch das BKA bleiben erst einmal außen vor.

[351] Jaeger, Computerkriminalität, Seite 202

rungsrechte berufen kann. Diese ergeben sich aus den §§ 52 [Zeugnisverweigerungsrechte aus persönlichen Gründen] und 53 [Zeugnisverweigerungsrechte aus beruflichen Gründen] StPO. Ferner hat der Zeuge gemäß § 55 [Auskunftsverweigerungsrecht] StPO ein Recht, auf alle Fragen die Auskunft zu verweigern, deren Beantwortung ihn selbst oder einen Angehörigen der Gefahr einer Strafverfolgung aussetzen würde. Nach der h.M. haben Zeugen eine Mitwirkungspflicht am Strafverfahren. Man geht davon aus, daß diese Pflichten sehr weit gefaßt sind. Sie werden aus dem Interesse der Allgemeinheit an der Strafverfolgung abgeleitet, dem sich der Einzelne grundsätzlich unterwerfen muß. Bei der Einzelfallbetrachtung ist das Verhältnismäßigkeitsprinzip anzuwenden. Weigert sich ein Zeuge zur Mitwirkung im Verfahren, kann ihm Ordnungsgeld oder Ordnungshaft auferlegt werden.

Fraglich ist, ob ein Zeuge verpflichtet werden kann, seinen Computer zu erklären. Eine solche Pflicht könnte aus der staatsbürgerlichen Mitwirkungspflicht im Beweissicherungsverfahren abgeleitet werden. Entsprechend sind dann die §§ 94 [Gegenstand der Beschlagnahme] und 95 [Herausgabepflicht] StPO anzuwenden. § 95 StPO begründet die allgemeine Pflicht für einen Staatsbürger, beweiserhebliche Gegenstände herauszugeben. Die Herausgabe von Gegenständen beeinträchtigt dabei den Rechtskreis des Betroffenen weitreichender als eine verbale Erklärung einer technischen Anlage.

Gerichtliche Entscheidungen sind – soweit ersichtlich – noch nicht vorhanden. Es ist aber zu vermuten, daß ein Gericht eine solche Pflicht aus der StPO ableiten wird. Im Bereich des Handelsgesetzbuches wurde eine weitgehende Mitwirkungspflicht für Kaufleute durch das OLG Bremen und das OLG Bamberg angenommen[352].

Desweiteren ist fraglich, ob ein Zeuge verpflichtet werden kann, Ausdrukke von Daten zu erstellen oder Kopien anzufertigen. Eine gesetzliche Pflicht ist für diese Fälle – soweit ersichtlich – noch nicht normiert. Das LG Oldenburg hat in einem Urteil bei einem solchen Fall eine Pflicht zur Kostenerstattung verneint[353]. Da sich das Urteil nicht direkt zur Herleitung einer allgemeinen Pflicht heranziehen läßt, kann nur prognostiziert werden, wie zukünftige Gerichte ent-

[352] OLG Bremen, NJW 1976, 685 und OLG Bamberg, JurBüro 1979, 1686

scheiden werden. Da es aber in der Regel für einen Betroffenen verhältnismäßiger sein wird, Daten zu kopieren oder auszudrucken (es besteht ja eine Kostenerstattungspflicht), wird eine Gerichtsentscheidung sicherlich dementsprechend einer allgemeinen Pflicht zustimmen.

Eine Frage von herausragender Bedeutung ist, ob ein Zeuge dazu verpflichtet werden kann, den Ermittlungsbehörden Passwörter seines Computers preiszugeben. Analog ist sicherlich in diesem Zusammenhang auch die Frage zu stellen, ob eine Pflicht zur Entschlüsselung kryptierter Daten oder Sichtbarmachung steganografierter Daten besteht. Soweit ersichtlich existiert auch für diese, in der Praxis durchaus relevanten Fälle, noch keine Rechtsprechung. „Nach der wohl überwiegenden Meinung der rechtswissenschaftlichen Literatur wird eine solche Pflicht aber für Nichtbeschuldigte angenommen.“[354] [355]

Die Pflichten, die für Nichtbeschuldigte abgeleitet wurden, können grundsätzlich nicht für Beschuldigte gelten. Die Rechtsprechung und die Literatur haben aus dem § 136 I [Erste Vernehmung] StPO den Grundsatz der Selbstbelastungsfreiheit (nemo tenetur se ipsum accusare) entwickelt[356].

D.h. daß niemand dazu verpflichtet werden kann, an seiner eigenen Strafverfolgung mitzuwirken. Eine Person, welche die Stellung eines Tatverdächtigen erreicht hat, kann sich also vollkommen passiv verhalten. Diese erlaubte Passivität schließt aber aktive Handlungen gegen Ermittlungen aus. Aktive Gegenwehr ist also verboten. Anderenfalls greifen bestimmte Tatbestände des StGB (z.B. Widerstand gegen Vollstreckungsbeamte gem. § 113 StGB).

Die einzige Pflicht, die der Beschuldigte letztendlich hat – und für deren Nichtbeachtung er dementsprechend auch zur Rechenschaft gezogen werden kann – ist die Pflicht zur Angabe der Personalien[357]. Gemäß § 111 [Falsche Namensangabe] OWiG handelt derjenige ordnungswidrig, der keine oder unrichtige Angaben zu seinen persönlichen Daten macht. Da die Selbstbela-

---

[353] LG Oldenburg, I Qs 52/87, vom 5.6.1987, abgedruckt in CR 1988, 679 (rechtskräftig); eine Kostenerstattung lehnt auch ab: OLG Düsseldorf, vom 24.9.1982, abgedruckt in Der Betrieb 1983, 106.

[354] Jaeger, Computerkriminalität, Seite 212, mit Hinweis auf: Leicht, jur 1986, 390 f. und Bär, CR 1995, 228

[355] vgl. auch: Bär, EDV-Beweissicherung im Strafverfahrensrecht, CR 7/1998, Seite 437, der davon ausgeht, daß Telekommunikationsdienste, die ihren Kunden Verschlüsselungstechik anbieten nach § 9 Abs. 2 FÜV verpflichtet sind, Daten für Ermittlungsbehörden zu entschlüsseln

[356] Vgl. auch: BVerfG, NJW 1981, 1431; BGH St 14, 358, 36 und BGH St 34, 39, 46.

[357] Vgl. auch: BGH St 21, 334, 364 und BGH St 25, 13, 17.

stungsfreiheit ein grundlegendes Prinzip des deutschen Rechtssystems ist, kann ein Beschuldigter daher auch keine Pflicht zur Erklärung eines Computers, zum Ausdruck oder Kopieren von Daten, zur Preisgabe von Passwörtern oder Entschlüsseln[358]/Desteganografieren von Daten treffen. Hier kommt es also im Ermittlungsverfahren auf die technische Raffinesse der auswertenden Computerspezialisten[359] oder das Können des Vernehmers an.

9.3.4 Zusammenfassung

„Rufen staatliche Stellen Daten ab, die für jedermann frei im Netz verfügbar sind, stellt dies keinen Eingriff in grundrechtlich geschützte Rechte dar. Eine Befugnis ist hierfür nicht erforderlich. Das Abrufen öffentlich zugänglicher Daten, die auf einem Rechner im Ausland gespeichert sind, verstößt in diesen Fällen auch nicht gegen völkerrechtliche Grundsätze. Soweit unter Überwindung von Zugangsbeschränkungen auf Daten zugegriffen wird, ist eine ausdrückliche gesetzliche Eingriffsermächtigung erforderlich. Müssen Zugangssperren von im Ausland gespeicherten Rechnern überwunden werden, ist vor diesem Eingriff ein förmliches Rechtshilfeersuchen zu stellen.“[360]

9.4 Ausgewählte Rechtsprobleme aus dem Bereich der StPO

9.4.1 Durchsuchung von Räumlichkeiten und Computern

Die wohl am häufigsten durchgeführte Ermittlungshandlung bei Beschuldigten ist die Durchsuchung von Räumen nach den §§ 102 [Durchsuchung beim Verdächtigen] ff. StPO (Hausdurchsuchung). Bei Dritten ist eine Durchsuchung an die Vorschriften des § 103 [Durchsuchung bei anderen Personen] StPO gebunden. Bei der Durchsuchung ist besonders auf die Vielzahl der Formvorschriften zu achten.

---

[358] Welche Behinderungen sich daraus für die Strafverfolgungsbehörden ergeben und zu den Grundlagen der Verschlüsselung vgl. auch: Leiberich, Verschlüsselung und Kriminalität, Kriminalistik 11/1995, Seite 731 bis 734.

[359] Über die Tätigkeit des EDV-Sachverständigen vgl. auch: Paul, Ein rundrum erfreuliches Berufsbild, Kriminalistik 8-9/1989, Seite 521 bis 526; vgl. auch: Nemes/ Greiner, Die Suche nach elektronisch gespeicherten Beweismitteln, Kriminalistik 2/1999, Seite 115 bis 119, die auch auf die verschiedenen Ermächtigungsgrundlagen eingehen.

[360] Jofer, Strafverfolgung im Internet, Seite 196

Die Durchsuchung steht gem. § 105 I StPO grundsätzlich unter einem Richtervorbehalt. Sie darf durch die StA oder durch Hilfsbeamte der StA nur bei Gefahr im Verzuge angeordnet werden. Wird eine Durchsuchung durch einen Richter angeordnet, stellt dieser einen Durchsuchungsbefehl aus. Dieses Schriftstück führt dann genau die Räume auf, die durchsucht werden dürfen. Eine Durchsuchung nicht aufgeführter Räumlichkeiten ist unzulässig. Daher sollten die Ermittlungsbeamten immer einen sehr umfangreichen richterlichen Beschluß erwirken.

Fraglich ist, ob auch Computeranlagen, die sich in den Räumlichkeiten befinden, durchsucht werden dürfen. Die h.M. geht davon aus, daß dies zulässig ist[361]. Da die Durchsuchung eine sogenannte zweckorientierte Vorschrift ist, muß auch das Einschalten der Anlage zulässig sein. So dürfen die Polizeibeamten ja auch Schubladen öffnen, wenn sie diese durchsuchen wollen! Durch das LG Köln wurde entschieden, daß ein Computer in Betrieb genommen und durchsucht werden kann[362].

Was passiert aber, wenn sich beispielsweise in einem größeren Gebäude ein installiertes LAN befindet, das aus einem Server und mehreren Workstations besteht? Grundsätzlich kann man ja von den Workstations aus auf den Server zugreifen, auch wenn dieser in einem Raum steht, der nicht auf dem Durchsuchungsbeschluß verzeichnet ist. „Da sich der Durchsuchungsbefehl immer auf bestimmte Lokalitäten erstreckt, muß der zu durchsuchende Rechner auch in diesen Räumen stehen. [...] Aus der örtlichen Begrenzung des Durchsuchungsbefehls folgt aber auch, daß eine Durchsuchung des gesamten Netzwerkes von einer Workstation aus nicht gestattet ist.“[363] [364] Ist den Ermittlungsbehörden in solchen Fällen unbekannt, daß sich ein wichtiger Bestandteil eines LAN in einem Raum befindet, der durch die richterliche Anordnung nicht abgedeckt wird, können sie ggf. Gefahr im Verzuge begründen oder eine telefonische Anordnung erwirken. Da Computerdaten sehr leicht und vor allem schnell zu manipulieren sind, dürfte eine Begründung der Gefahr im Verzuge

---

[361] Vgl. auch: Kleinknecht/Meyer-Goßner, Strafprozeßordnung, § 102 Rn. 10 a.

[362] LG Köln, 112 Qs 2/94, vom 11.08.1994, abgedruckt in CR 1995, 419 (rechtskräftig)

[363] Jaeger, Computerkriminalität, Seite 215

[364] So auch: Kleinknecht/Meyer-Goßner, Strafprozeßordnung, § 105 Rn. 5.

nicht schwerfallen. Allerdings darf diese Möglichkeit auch nicht mißbraucht werden, da sonst der Richtervorbehalt systematisch unterlaufen werden würde.

Den Beamten ist es grundsätzlich erlaubt, eine Computeranlage in Betrieb zu nehmen. Fraglich ist, ob ein Rechner auch zur Auswertung von Daten durch die Ermittler genutzt werden darf. Da eine Auswertung originär kein Suchen mehr darstellt, können die repressiven Vorschriften für die Durchsuchung dafür keine Rechtsgrundlage bilden. Hierdurch würde der zweckorientierte Bereich der Vorschriften in unzulässiger Weise überschritten werden.

Wenn sich eine Durchsuchung auch auf einen Computer ausdehnt, ist besonders auf den § 110 [Durchsicht von Papieren] StPO zu achten. Danach steht die Durchsicht von Papieren allein der StA zu. Anders verhält es sich, wenn der Betroffene einer Sichtung durch die Polizei zustimmt. Wendet man die Begriffsbestimmung für „Schriften“ aus dem StGB auf den Begriff der „Papiere“ aus der StPO an, kommt man zu dem Ergebnis, daß Computerdaten auch Papiere sind und deshalb einem besonderen Schutz unterliegen[365]. M.E. kann eine Sichtung der Verzeichnisstrukturen durch Polizeibeamte erfolgen, da diese analog mit der Beschriftung herkömmlicher Büroordner vergleichbar ist. Lediglich das Öffnen und die Kenntnisnahme des Inhalts von Dateien müssen den Polizeibeamten verboten sein.

9.4.2 Sicherstellung/Beschlagnahme von Hardware

Im Bereich der Strafverfolgung gibt es für ermittelnden Beamten grundsätzlich zwei Möglichkeiten, die Hardware (z.B. Rechner, Monitor, Tastatur, Maus, Drucker etc.) eines Beschuldigten sicherzustellen. Man unterscheidet die Sicherstellung/Beschlagnahme von Einziehungs- oder Verfallsgegenständen und die Sicherstellung/Beschlagnahme von Beweismitteln.

Für die Einziehung sind im besonderen Maße die §§ 73 ff. StGB und die §§ 111 b, 111 c StPO von Bedeutung. Die Vorschriften des StGB regeln, welche Gegenstände dem Verfall oder der Einziehung unterliegen.

Für den Bereich der Computerkriminalität haben überwiegend die Einziehungsvorschriften des StGB praktische Relevanz. Gem. § 74 [Voraussetzungen

---

[365] Vgl. auch: Kleinknecht/Meyer-Goßner, Strafprozeßordnung, § 110 Rn. 1.

der Einziehung] StGB müssen Gegenstände, die durch eine vorsätzliche Straftat hervorgebracht wurden (producta sceleris - Tatprodukte) oder die zu ihrer Begehung oder Vorbereitung gebraucht wurden oder bestimmt waren (instrumenta sceleris - Tatwerkzeuge) eingezogen werden. Wenn gem. § 111 b I [Sicherstellung] StPO Gründe die Annahme rechtfertigen, daß die Voraussetzungen der Einziehung vorliegen, können solche Gegenstände sichergestellt werden. Gem. § 111 c I [Beschlagnahme zur Sicherstellung] StPO sind solche Gegenstände grundsätzlich in Gewahrsam zu nehmen.

Bei den meisten Delikten im Bereich der Computerkriminalität spielt der Computer eine zentrale Rolle. D.h. daß er in den wenigsten Fällen kein Tatwerkzeug sein wird. Der Ermittlungsbeamte hat also immer zu prüfen, ob eine Rechneranlage als Tatwerkzeug sichergestellt werden kann. Diese Entscheidung muß sich an den Gegebenheiten des Einzelfalls orientieren und im besonderen Maße verhältnismäßig sein. Es kann nicht bestritten werden, daß der Computer eine wichtige Rolle im privaten und im geschäftlichen Bereich spielt. Wird bei einem kleinen Unternehmen die gesamte Computeranlage sichergestellt, kann das in der heutigen Zeit sehr schnell zum Ruin der Firma führen. Grundsätzlich ist die gesamte Peripherie sicherzustellen. Ausnahmen bilden Geräte, die offensichtlich nichts mit der eigentlichen Tat zu tun haben (z.B. Drucker eines Hackers).

Für die Sicherstellung von Gegenständen als Beweismittel sind die §§ 94 [Gegenstand der Beschlagnahme] und 95 [Herausgabepflicht] StPO einschlägig. Gemäß § 94 I StPO muß der Gegenstand – also die Hardware – als Beweismittel für die Untersuchung von Bedeutung sein. In der Praxis überwiegen aber die Fälle, in denen gerade nicht die Hardware Beweiswert hat, sondern die abgespeicherten Daten. Die Hardware ist nur Träger der beweiswürdigen Daten. Erst bei Spezialgeräten oder besonders alten Modellen kann somit eine Sicherstellung gerechtfertigt sein, da ohne die Anlage kaum eine Sichtung der Daten möglich ist. Eine Sicherstellung von Standardgeräten (auch Peripherie) ist also in der Regel nicht möglich. Allerdings gibt es durchaus auch Beispiele, bei denen die Hardware beweiswürdig ist. So kann die Sicherstellung eines Druckers, mit dem ein Beleidigungs- oder Erpressungsschreiben gedruckt wurde, genauso gut gerechtfertigt sein, wie die Sicherstellung eines CD-Brenners, der zum Raubkopieren verwendet wurde.

Sind die Vorschriften zur Sicherstellung von Beweismitteln auf Hardware nicht anwendbar, bleiben immer noch die Vorschriften über die Einziehung. Probleme kann es dann geben, wenn der Computer nicht das Eigentum des Täters ist.

9.4.3 Überwachen von Mailboxen

Dieser Abschnitt befaßt sich mit den Eingriffsbefugnissen im Bereich der Überwachung von Mailboxen. Dabei sollen die Mailboxen im engeren Sinne betrachtet werden, also Einport- oder Mehrport-Mailboxen. Der Internetdienst E-Mail bleibt erst einmal außen vor.

Prinzipiell unterscheidet man innerhalb einer Mailbox zwischen einem öffentlichen und einem privaten Bereich. Der öffentliche Bereich steht grundsätzlich jedem Benutzer offen, der die Telefonnummer der Mailbox kennt. Über einen Gastzugang kann er sich in den fremden Computer einloggen. Der private Bereich ist vom öffentlichen durch eine besondere Softwaresperre – meist in Form einer Zugangskennung mittels Benutzernamen und Paßwort – abgetrennt. Nur wer eine solche Zugangskennung besitzt, kann in den privaten Bereich gelangen. Ob eine Mailbox beide Bereiche enthält, hängt ganz vom jeweiligen Mailboxprogramm und dem Betreiber ab. Es kann also auch Mailboxen geben, die nur einen der beiden Bereiche besitzen.

Durch das Einloggen in den öffentlichen Bereich einer Mailbox werden keine Grundrechte verletzt, da der Staat so handelt, wie es auch jede beliebige Privatperson könnte. „Derartige Ermittlungshandlungen ohne Zwangscharakter stellen anerkannte kriminalistische Vorgehensweisen dar. Schlichte Datenerhebungen ohne Umgehung von Zugriffsbeschränkungen bedürfen daher keiner speziellen Ermächtigungsgrundlage. Der ermittelnde Beamte kann sein Handeln bereits aus der Aufgabenzuweisung nach §§ 161, 163 StPO legitimieren.“[366] In diesem Sinne könnten diese Informationsquellen auch mit Zeitungen, Litfaßsäulen oder Plakaten gleichgesetzt werden. Für das Lesen solcher allgemein zugänglichen Daten brauchen die Ermittlungsbehörden ja auch keine Ermächtigungsnorm. „Zu den frei zugänglichen, offenen Diensten zählen

[366] Jofer, Strafverfolgung im Internet, Seite 197 mit Verweis auf Bär, CR 1995, S. 491 f. u.a.

selbstverständlich auch diejenigen, auf die man mit einem Pseudo-Paßwort zugreifen kann (`Gast´ oder `guest´).“[367]

Anders sieht es beim privaten Bereich einer Mailbox aus. An dieser Stelle gibt der Betreiber unmißverständlich zu verstehen, daß er nur einem von ihm bestimmten Personenkreis den Zugriff auf seine Daten erlaubt. Würden die Ermittlungsbehörden ohne Eingriffsermächtigung auf die Daten zugreifen[368], würden sie das Grundrecht auf informationelle Selbstbestimmung gemäß Art. 2 I GG des Betreibers und der legitimierten Benutzer verletzen. Desweiteren könnte auch das Grundrecht auf das Brief -, Post- und Fernmeldegeheimnis gemäß Art. 10 I GG tangiert sein, da ja in der Mailbox Nachrichten hinterlassen werden können.

Eine besondere Befugnis der StPO, die sich explizit mit dem Zugriff auf Mailboxen beschäftigt, existiert – soweit ersichtlich – nicht. Daher ist zu prüfen, ob nicht andere Vorschriften anwendbar sind. Zum einen könnte hier der Einsatz eines verdeckten Ermittlers gemäß § 110 a [Verdeckte Ermittler] StPO, eine Durchsuchung gemäß §§ 102 [Durchsuchung beim Verdächtigen], 103 [Durchsuchung bei anderen Personen] StPO oder eine Überwachung des Fernmeldeverkehrs gemäß § 100 a [Voraussetzungen der Überwachung des Fernmeldeverkehrs] StPO vorliegen.

Gemäß § 110 a II StPO ist ein verdeckter Ermittler ein Beamter des Polizeidienstes, der unter einer ihm verliehenen Legende und einer veränderten Identität ermittelt. Die Legende soll auf Dauer verliehen sein[369]. Wird eine Legende nicht auf Dauer verliehen, spricht man von einem nicht offen ermittelnden Polizeibeamten (NOEP)[370]. Dieser findet, soweit anerkannt, seine Ermächtigungsnorm in § 163 StPO[371]. Ein Polizeibeamter kann unter Vortäuschung einer falschen Identität Zugriff zu einem privaten Bereich einer Mailbox erhal-

---

[367] Jaeger, Computerkriminalität, Seite 218

[368] Der Zugriff auf den privaten Bereich einer Mailbox kann u.a. durch die Benutzung einer erschlichenen (unter einer falschen Identität) oder einer fremden Kennung oder durch die Benutzung „diverser“ Software erfolgen.

[369] So auch: Kleinknecht/Meyer-Goßner, Strafprozeßordnung, § 110 a Rn. 2.

[370] Der NOEP wird beispielsweise für Scheinaufkäufe eingesetzt.

[371] Jofer lehnt den Einsatz eines NOEP grundsätzlich ab: Jofer, Strafverfolgung im Internet, Seite 200 und 201 mit Verweis auf Ansicht des LKA/Nordrhein-Westfalen, nach der der Einsatz eines NOEP keine gesetzliche Grundlage hat; anderer Meinung ist: Kleinknecht/Meyer-Goßner, Strafprozeßordnung, § 110 a Rn. 4.

ten[372]. Benutzt der Beamte eine fremde Kennung, handelt er nicht als VE oder NOEP.

Jofer stellt den Einsatz eines VE bei der Erschleichung einer Kennung in Frage, da nach seiner Auffassung die verliehene Legende nicht dauerhaft ist. Letztendlich stimmt er aber dem Einsatz zu[373].

M.E. ist der Auffassung Jofers nicht zu folgen. Die h.M. geht davon aus, daß der Einsatz eines NOEP gem. §§ 161, 163 StPO zulässig ist. Mithin ist die Polizei nicht verpflichtet, Ermittlungstätigkeiten offen durchzuführen. Ein Polizeibeamter, der unter Angabe einer falschen Identität Zugriff auf eine Mailbox erhält, ist ein NOEP. Er ist kein VE, da seine Legende nicht auf Dauer angelegt ist.

Den Online-Zugriff auf eine Mailbox auf die Durchsuchungsvorschriften §§ 102 und 103 StPO zu stützen, ist nicht zulässig, da bei einer Durchsuchung die körperliche Anwesenheit der durchsuchenden Beamten erforderlich ist[374]. Ferner müssen verschiedene Formvorschriften beachtet werden (Inkenntnissetzung des Inhabers, Hinzuziehung von Zeugen etc.). Da diese Vorschriften aber regelmäßig den Erfolg einer Durchsuchung beeinträchtigen müssen, ist sie praktisch nur unter Umgehung der Formvorschriften für die Polizei praxisrelevant. Diese ständige Umgehung wäre nicht zulässig, daher sind die §§ 102 und 102 StPO als Ermächtigung für einen Online-Zugriff unbedingt abzulehnen. Anders verhält es sich, wenn die Ermittlungsbehörden einen Raum durchsuchen und dabei auf einen Rechner stoßen, auf dem ein Mailbox-Programm läuft. Hier ist der Rechner natürlich durch die Durchsuchungsanordnung (bei richterlicher Anordnung) einbegriffen.

Weiterhin könnte auch § 100 a StPO als Ermächtigungsnorm dienen[375]. § 100 a StPO regelt die Überwachung des Fernmeldeverkehrs. Eine Mailbox vereint in sich Eigenschaften des Brief- und Fernmeldeverkehrs. „Der Bundesgerichtshof hat [...] in einem Beschluß aus dem Jahre 1995 den heimlichen Zugriff auf eine Mailbox auf die Regelungen des § 100 a StPO (Telefonüberwachung)

---

[372] Für den Einsatz von NoEP vgl. auch: Hartung, Internet, dp-special April 1998, Seite 13.
[373] Jofer, Strafverfolgung im Internet, Seite 200
[374] ebd., Seite 202
[375] Vgl. auch: Kleinknecht/Meyer-Goßner, Strafprozeßordnung, § 100 a Rn. 2.

gestützt und ihn für zulässig befunden.“[376] Ergänzend dazu stellte der BGH aber auch fest, daß auch bestimmte Grundsätze der Durchsuchung angewendet werden sollen.

Zum einen soll nur der einmalige Zugriff auf eine Mailbox statthaft sein und zum anderen soll eine gewisse Erfolgsvermutung – daß bestimmte Daten gefunden werden – vorliegen. Der BGH hält ausdrücklich den heimlichen Zugriff für rechtlich zulässig, d.h. daß sich der Polizeibeamte nicht zu erkennen geben muß. Obwohl der BGH den heimlichen Zugriff auf eine Mailbox erlaubt, ist die Frage in der juristischen Literatur immer noch umstritten. Daher sollen nun kurz die verschiedenen Standpunkte vorgestellt werden[377].

Im Sinne des BVerfG besteht weitgehend Einigkeit darüber, daß der Begriff Fernmeldeverkehr aus dem § 100 a StPO auch neuere Formen der Telekommunikation umfaßt[378]. Das wird vor allem auch dadurch ersichtlich, daß durch das BegleitG[379] zum TKG der Begriff des Fernmeldeverkehrs im § 100 a StPO durch den Begriff „Telekommunikation“ ersetzt wurde[380]. Zugrundegelegt werden die Begriffsbestimmungen „Telekommunikation“ und „Telekommunikationsanlage“ nach § 3 Nr. 16 und 17 TKG. Danach ist Telekommunikation der technische Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels Telekommunikationsanlagen. Telekommunikationsanlagen sind technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können. Das Versenden, Empfangen und Übermitteln jeglicher elektronischer Daten ist als Telekommunikation zu subsumieren. Ein Computer, auf dem ein Mailboxprogramm läuft ist daher auch eine Telekommunikationsanlage.

---

[376] Jaeger, Computerkriminalität, Seite 217 unter Hinweis auf BGH – 2 BJs 94/94-6 u.a., vom 31.07.1995, abgedruckt in NJW 1997, 1934 ff.

[377] Eine ausführlichere Abhandlung der verschiedenen Ansichten bei: Jofer, Strafverfolgung im Internet, Seite 204 bis 207.

[378] Vgl. auch: BVerfGE 46, 120, 142 f.

[379] Eine Übersicht über die Änderungen durch das BegleitG bei: Felixberger, Staatliche Überwachung der Telekommunikation, CR 3/1998, Seite 143 bis 147.

[380] Vgl. auch: Bär, EDV-Beweissicherung im Strafverfahrensrecht, CR 7/1998, Seite 435, der davon ausgeht, daß alle modernen Kommunikationsmedien von § 100 a StPO erfaßt werden.

Durch die Rechtsprechung wird die Ansicht vertreten, daß der Abruf von Daten ein Überwachen des Fernmeldeverkehrs ist, da sie die Fernmeldeanlage noch nicht verlassen haben. Dagegen spricht der Fakt, daß durch die Ermittlungsbehörden gespeicherte Daten abgerufen werden.

Die Speicherung von Daten ist aber in der Definition des Begriffs Telekommunikation nach dem TKG nicht enthalten.

Vertreter dieser Ansicht werfen ein, daß sich das aktive Abrufen von Daten aus einer Mailbox signifikant vom passiven Überwachen eines Kommunikationsvorgangs unterscheidet. „Bei der `Überwachung´ einer Mailbox wird kein laufender Datenverkehr protokolliert, sondern das Vorhandensein einer Information. Der Zugriff der Ermittler setzt – anders als bei der Überwachung eines Telefonanschlusses – nicht an dem eigentlichen `Echtzeit-Übermittlungsvorgang´ an.“[381]

Der BGH hält die Anwendbarkeit des § 100 a StPO auch deshalb für zulässig, weil durch die Formvorschriften und den abschließenden Straftatenkatalog der Vorschrift eine hohe Eingriffsschwelle vorgegeben wird. Kritiker hingegen stellen sich die Frage, warum bei einer solchen - angebliche hohen - Eingriffsschwelle ergänzend die Vorschriften über die Durchsuchung herangezogen werden müssen, so daß nur ein einmaliger Zugriff möglich ist. Grundsätzlich hat der Richter nämlich gemäß § 100 b II StPO die Dauer der Maßnahme festzulegen. Der BGH weiß also, daß nur eine zeitlich unbegrenzte Maßnahme den Richtervorbehalt aushebeln würde. Denn allein die Beamten würden dann entscheiden, wann sie tätig werden. Sie sind somit von den überwachten Personen unabhängig. Bei der Überwachung eines Telefons hingegen können die Ermittler nur dann Informationen erlangen, wenn auch wirklich ein Telekommunikationsvorgang abläuft.

Die vorangestellten Argumente beschäftigten sich vor allem mit der Auslegung des Begriffes „Überwachen“. Allerdings darf auch nicht vergessen werden, daß der Rechtsprechung des BGH auch das verfassungsrechtliche Analogieverbot entgegenstehen könnte. Gesetzesanalogie liegt vor, wenn ein Gesetz in unzulässiger Weise über die zumutbaren Grenzen hinaus ausgelegt wird. Da

---

[381] Jofer, Strafverfolgung im Internet, Seite 205 mit Hinweis auf: Bär, CR 1996, S. 491, der die Anwendbarkeit des § 100 a StPO für den heimlichen Abruf von Daten aus einer Mailbox ablehnt.

es sich bei den geschützten Rechten um sehr hochwertige Rechtsgüter (Recht auf informationelle Selbstbestimmung, Brief-, Post – und Fernmeldegeheimnis) handelt, müssen die eingreifenden Vorschriften auch genaustens bestimmt, also eindeutig sein. Für ausschweifende Auslegungen darf es keinen Platz geben. „In einem grundrechtssensiblen Bereich wie dem Fernmeldeverkehr hat der Gesetzgeber eine entsprechende Regelungsdichte herzustellen und exakt festzulegen, unter welchen Voraussetzungen ein Fernzugriff auf geschützte Datenbestände zulässig sein soll. [...] Der Versuch des BGH, durch eine kombinierte Anwendung verschiedener Eingriffsnormen neue Befugnisnormen zu kreieren, birgt Gefahren: Macht man die Zusammenschau verschiedener Rechtsgrundlagen zum Zwecke der Legitimation gesetzlich nicht geregelter Eingriffe zur Regel, wären die geschriebenen Befugnisnormen nichts weiter als Versatzstücke einer richterlichen Generalklausel. Eine freihändig vorgenommene richterliche Verhältnismäßigkeitsprüfung ersetzt nicht die fehlende Rechtsgrundlage.“[382] Gegner des BGH-Urteils führen aus, daß es mithin ausschließliche Aufgabe des Gesetzgebers ist, auf technische Neuerungen zu reagieren. Es ist nicht Aufgabe der Gerichte, die Gesetze so auszulegen, daß sie auf Neuerungen anwendbar werden.

M.E. sind beide Auffassungen durchaus vertretbar. Allerdings folge ich der Auffassung des BGH. Entscheidend ist, daß das BVerfG die neuen Formen der Telekommunikation, zu denen auch das Internet und die Mailboxen gehören, unter den Begriff des Fernmeldeverkehrs einordnet. Der einmalige Zugriff auf Daten in einer Mailbox ist als geringeres Mittel einzustufen als die permanente Überwachung eines Anschlusses und eine damit verbundene lückenlose Echtzeit-Protokollierung aller ein- und ausgehenden Daten. Es muß bedacht werden, daß auch eine Datenübermittlung – die ja explizit als Telekommunikation bezeichnet wird – eine Zwischenspeicherung der Daten beinhaltet. Somit kann die letzte Speicherung von Daten auf einer Mailbox durchaus noch zum Übermittlungsvorgang gezählt werden. Erst wenn die Daten die Fernmeldeanlage (Mailbox) verlassen, ist der eigentliche Übertragungsvorgang abgeschlossen. Somit ist der Abruf von Daten aus einer Mailbox auf der Grundlage von § 100 a StPO zulässig. Das Heranziehen der Durchsuchungsvorschriften ist unglücklich

[382] Jofer, Strafverfolgung im Internet, Seite 207

und auch nicht unbedingt notwendig. M.E. hat der Richter auch die Möglichkeit die Einmaligkeit auf Grund des § 100 b II StPO zu begründen. So kann es sich bei diesem einmaligen Vorgehen um eine Konkretisierung der „Art der Maßnahme“ handeln, nämlich nur einmal auf die Mailbox zuzugreifen. Ferner enthält § 100 a StPO eine Konkretisierung des Verhältnismäßigkeitsgrundsatzes, aus dem dann eine gewisse Erfolgswahrscheinlichkeit abgeleitet werden kann.

9.4.4 Sicherstellung/Beschlagnahme von Computerdaten

Wie bereits festgestellt wurde, haben regelmäßig nur die Daten, die auf einem Datenträger gespeichert sind, beweiswürdigen Charakter. Die Rechtsprechung und die Literatur beschäftigten sich daher mit der Frage, ob die Ermittlungsbehörden einen Datenträger sicherstellen können oder ob sie verpflichtet sind, die Daten zu kopieren. Die Möglichkeiten, Daten zu speichern, sind sehr vielfältig. Die gebräuchlichsten Datenträger sind Festplatte, Diskette und CD. Die h.M. und die Rechtsprechung gehen davon aus, daß Datenträger beschlagnahmt werden können[383].

Fraglich ist, ob staatliche Behörden Kopien auf eigene Datenträger machen dürfen. „Die Zulässigkeit von Kopien bejahen: Bär [...] und Schäfer [...]. Ablehnend: Lemcke [...].“[384] Durch das LG Köln wurde ein Fall entschieden, bei dem Datenbestände eines Rechners auf behördliche Datenträger kopiert wurden[385]. Mithin kann man also davon ausgehen, daß das Kopieren von Daten zulässig ist, da sie gemäß § 94 I StPO „auf andere Weise“ sichergestellt werden[386]. In diesem Sinne muß ein Kopieren von Daten auch durchweg als verhältnismäßiger angesehen werden, als die Sicherstellung eines Datenträgers. Durch die Polizei muß in solchen Fällen darauf geachtet werden, daß beispielsweise strafbare Daten nicht in den Händen des Tatverdächtigen verbleiben, da sich sonst für die Ermittler ggf. eine Strafbarkeit durch Unterlassen ergeben könnte.

---

[383] Jaeger, Computerkriminalität, Seite 222, mit Hinweis auf: BGH – StB 33/95, vom 03.08.1995, abgedruckt in CR 1996, 35 ff (Beschlagnahme von Disketten) sowie BGH – I BGS 517/87, vom 23.11.1987, abgedruckt in CR 1988, 142 f. (Mitnahme von Datenträgern zur weiteren Durchsicht).

[384] Jaeger, Computerkriminalität, Seite 222, mit Hinweis auf: Bär, CR 1996, 675, 745; Schäfer, wistra 1989, 13 und Lemcke, Die Sicherstellung gemäß § 94 ..., 1995, S. 100 ff.

[385] LG Köln – 112 Qs 2/94, vom 11.08.1994, abgedruckt in CR 1995, 419 (rechtskräftig)

[386] Vgl. auch: Kleinknecht/Meyer-Goßner, Strafprozeßordnung, § 94 Rn. 16 a.

Da Daten als Papiere angesehen werden, müssen die Ermittler im besonderen Maße auch auf § 97 [Beschlagnahmefreie Gegenstände] StPO achten. So unterliegen beispielsweise schriftliche Mitteilungen zwischen dem Beschuldigten und zeugnisverweigerungsberechtigten Personen grundsätzlich einem Beschlagnahmeverbot.

Der Schriftverkehr kann auch auf elektronischem Wege erfolgen. Da in der polizeilichen Praxis oft ganze Datenbestände kopiert und dann erst ausgewertet werden, sind dem Betroffenen entsprechende Daten nach erfolgter Selektierung zurückzugeben. Eine Selektierung vor Ort kann – angesichts der heutigen Datenmengen – nicht verlangt werden.

9.4.5 Abruf von E-Mails

Es wurde bereits erläutert, wie die allgemeine Beschlagnahme von Computerdaten rechtlich bewertet wird. Wie verhält es sich aber bei elektronischen Nachrichten (E-Mails)?

Für den herkömmlichen Brief sah die StPO zwei Möglichkeiten vor. Zum einen konnte Post direkt bei einer Hausdurchsuchung nach den §§ 102 ff. StPO beschlagnahmt werden oder, wenn sie sich noch auf dem Weg befand, über § 99 [Postbeschlagnahme] StPO.

Fraglich ist, ob die Vorschriften in dieser Form auch auf E-Mail übertragbar sind. Hierbei ergeben sich zwei Hauptfälle. Zum einen kann sich die E-Mail bereits auf dem Rechner des Empfängers, zum anderen aber auch noch auf dem Server eines Providers (hauptsächlich E-Mail-Server) befinden. Im zweiten Fall ist zu prüfen, ob die Ermittler vom Rechner des Beschuldigten aus oder von einem anderen Rechner die E-Mails abrufen dürfen.

Jaeger lehnt sowohl die Anwendung des § 100 a, als auch des § 99 StPO systematisch ab. Er geht davon aus, daß der Gesetzgeber noch keine Regelungen in Bezug auf E-Mails getroffen hat[387] [388]. Dementsprechend kommt er zu dem Ergebnis, daß allein die allgemeinen Vorschriften über die Durchsuchung (§§ 102 ff. StPO) anwendbar sind. D.h. daß nach seiner Auffassung eine Si-

---

[387] Jaeger, Computerkriminalität, Seite 223, mit Hinweis auf: Bär, CR 1996, 750, der die Anwendbarkeit des § 99 StPO ebenfalls ablehnt.

[388] Im Ergebnis so auch: Bär, EDV-Beweissicherung im Strafverfahrensrecht, CR 7/1998, Seite 437, der davon ausgeht, daß nur verkörperte Gegenstände („Post“) von § 99 StPO erfaßt werden.

cherstellung von E-Mails nur im Wege einer Hausdurchsuchung erfolgen kann. In der Konsequenz muß also auch für die Fälle, in denen die E-Mails noch beim Provider lagern, für eben diesen Provider ebenfalls ein Durchsuchungsbefehl erwirkt werden.

Nach der neusten Auffassung des LG Hanau hingegen unterliegen E-Mails in einer Mailbox dem Schutz des Art. 10 GG. Sie können daher nicht nach den §§ 94, 99 StPO beschlagnahmt werden. Ermächtigungsgrundlage für den Zugriff auf sämtliche Inhalte (und so auch E-Mails), die den Betreibern von Telekommunikationsnetzen anvertraut wurden, soll nunmehr § 100 a StPO sein[389].

M.E. können diese Ansichten durchaus bezweifelt werden. Gem. § 99 StPO ist die Postbeschlagnahme eines Beschuldigten bei Personen oder Unternehmen zulässig, die geschäftsmäßig Post- oder Telekommunikationsdienste erbringen. Gem. § 3 Nr. 5 TKG ist „geschäftsmäßiges Erbringen von Telekommunikationsdiensten“ das nachhaltige Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen mit oder ohne Gewinnerzielungsabsicht. Der Begriff Telekommunikation, der in § 3 Nr. 16 TKG legal definiert wird, wurde bereits erläutert. Ohne Zweifel bezieht sich das Erbringen von Telekommunikationsdiensten eindeutig auch auf die E-Mail-Provider[390]. Sie halten die E-Mail ihrer Kunden auf ihren Servern zur Übermittlung bereit. Telekommunikation ist ausschließlich nur über Telekommunikationsanlagen (§ 3 Nr. 17 TKG) möglich. Nachrichten, die über eine Telekommunikationsanlage übertragen werden, sind ausnahmslos identifizierbare elektromagnetische oder optische Signale.

Es würde nicht einleuchten, wenn der Gesetzgeber Telekommunikationsdienste bei der Postbeschlagnahme einbezieht, die Anwendung dann aber abgelehnt wird, weil der Begriff E-Mail nicht im Gesetz auftaucht und der Gesetzgeber statt dessen an den Begrifflichkeiten „Postsendungen“ und „Telegramme“ festhält. Jaeger hat sicherlich Recht, wenn er sagt, daß ein Abrufen der E-Mails von den Vorschriften nicht gedeckt ist. Ich halte es allerdings für verfehlt,

---

[389] Vgl. auch: LG Hanau, Beschluß vom 23.09.1999 – 3 Qs 149/99, abgedruckt in NJW 49/1999, Seite 3647; Kriminalistik 2/2000, Seite 98.

beim E-Mail-Provider eine Hausdurchsuchung anzuordnen, um über diese Möglichkeit auch die Server durchsuchen zu können.

Eine Kopplung der Vorschriften beim E-Mail-Provider wäre sicherlich die günstigste Lösung. Die Durchsuchungsvorschriften dienen dem Betreten der Räume und dem Durchsuchen von Computern. Eine Beschlagnahme von allgemeinen Daten erfolgt dann nach § 94 I StPO, eine Beschlagnahme von E-Mails nach § 99 StPO. Lagern die E-Mails bereits beim Betroffenen, kann eine Sicherstellung auf Grundlage des § 94 I StPO erfolgen.

Für die E-Mails sind ebenfalls die Regelungen über beschlagnahmefreie Gegenstände analog anzuwenden (siehe auch § 97 StPO). Ist bei einer polizeilichen[391] oder staatsanwaltschaftlichen Auswertung von Daten ersichtlich, daß E-Mails solche beschlagnahmefreien Mitteilungen oder Aufzeichnungen darstellen, sind sie dem Beschuldigten zurückzugeben oder bei Vorlage einer Kopie zu löschen.

9.4.6 Zusammenfassung

„Zugriff auf geschlossene, gegen fremden Zugriff durch Paßwort o.ä. gesicherte Dienste ist nach Ansicht des BGH im Rahmen des § 100 a StPO möglich.“[392] Die h.M. der Literatur geht davon aus, daß mithin für einen solchen Zugriff keine Rechtsgrundlage existiert. Nach der Ansicht des BGH darf ein Zugriff nur einmal erfolgen und dann nur, wenn zu vermuten ist, daß sich die gesuchten Daten auch in der Mailbox befinden.

M.E. sind diese Grundsätze direkt aus den Formvorschriften des § 100 b StPO und dem erweiterten Verhältnismäßigkeitsgrundsatz des § 100 a StPO ableitbar. Der BGH führt seine Ansicht auf die Formvorschriften der Durchsuchung zurück und läuft dadurch Gefahr, strafprozessuale Vorschriften unzulässigerweise analog anzuwenden.

---

[390] Da Telekommunikationsdienste nicht unbedingt mit Gewinnerzielungsabsicht arbeiten müssen, fallen auch private Mailboxen, in denen E-Mails ausgetauscht werden, unter die Vorschriften des § 99 StPO.

[391] Gemäß § 110 StPO steht die Durchsicht von Papieren (also auch Computerdaten) allein der StA zu, diese kann allerdings die Auswertung der Polizei übertragen, da sie für die Polizei eine vorgesetzte Behörde im Ermittlungsverfahren ist („StA als Herrin des Verfahrens“).

[392] Jaeger, Computerkriminalität, Seite 219

Erlangt ein Ermittlungsbeamter nur unter Angabe einer falschen Identität eine Zugriffskennung, handelt er als NOEP. Die Rechtsgrundlage ergibt sich aus den §§ 161, 163 StPO.

Das Benutzen fremder Kennungen oder der Einsatz von Software – um in eine Mailbox zu gelangen – wird mithin durch § 100 a StPO gedeckt. Die neuere Rechtsprechung geht davon aus, daß der gesamte Datenverkehr, der einem Telekommunikationsdienst übergeben wird, unter § 100 a StPO fällt.

E-Mails, die noch in einer Mailbox oder auf einem E-Mail-Server lagern, unterliegen den Vorschriften über die Postbeschlagnahme nach § 99 StPO. Ein Abrufen der E-Mail vom Anschluß des Benutzers aus, ist durch § 99 StPO nicht gedeckt. Daher kann eine Anwendung des § 99 StPO nur i.V.m. mit den allgemeinen Durchsuchungsvorschriften erfolgen.

Die Durchsicht sämtlicher Daten unterliegt gem. § 110 StPO der StA, da Daten i.S.d. StPO Papiere sind. Dabei ist es unerheblich, auf welchem Medium die Daten gespeichert wurden. Lediglich die Sichtung von Verzeichnisbäumen durch Polizeibeamte kann noch als zulässig angesehen werden.

10 Gefahrenabwehr im Internet

10.1 Allgemeines

Die nachfolgenden Ausführungen sollen die Notwendigkeit und die rechtlichen Grundlagen für präventivpolizeiliche Maßnahmen im Bereich des Internets darstellen. Die Ausführungen werden sich auf die Probleme bei behördlichen Sperranordnungen für Tele- und Mediendienste beschränken. Dabei orientiere ich mich maßgeblich an den Ausführungen von Zimmermann[393] [394]. Die juristische Literatur hat sich bisher fast ausschließlich mit den straf -, strafprozess -, und zivilrechtlichen Problemen, die durch das neue Medium Internet und den daraus resultierenden verschiedenen Regulierungsansätzen entstanden, beschäftigt. Da aber die Verbreitung von rechtswidrigen Inhalten über das Internet durchaus auch eine Gefährdung der öffentlichen Sicherheit und Ordnung darstellen kann, besteht für die Polizei grundsätzlich auch die Möglichkeit, Maßnahmen zur Gefahrenabwehr durchzuführen.

In diesem Bereich sollen daher vor allem Ausführungen zu den sachlichen und örtlichen Zuständigkeitsabgrenzungen, der Adressatenfrage und dem Grundsatz der Verhältnismäßigkeit, unter Einbeziehung der spezialgesetzlichen Regelungen des Medienrechts, gemacht werden. Insbesondere kommen als polizeiliche Maßnahmen Aufforderungen an Internetanbieter in Betracht, einzelne Internetangebote zu löschen oder den Zugang zu solchen Angeboten für alle Nutzer oder einzelne Nutzergruppen zu sperren. Grundlage für eine verständliche Abhandlung ist eine klare Wahl der Begriffe.

Da es maßgeblich um die Verantwortlichkeiten geht, sollen somit für die Beteiligten auch die Begriffe i.S.d. § 5 TDG und § 5 MDStV verwendet werden. Derjenige, der eigene Inhalte zur Nutzung bereithält ist Content-Provider (Inhaltsanbieter), derjenige, der fremde Inhalte zur Nutzung bereithält ist Serviceprovider (Serviceanbieter) und derjenige, der lediglich den Zugang zur Nutzung fremder Inhalte vermittelt, ist Accessprovider (Zugangsanbieter).

---

[393] Zimmermann, Polizeiliche Gefahrenabwehr und das Internet, NJW 43/1999, Seite 3145 bis 3152

[394] Eine sehr kurze Ausführung bei: Flechsig/Gabel, Strafrechtliche Verantwortlichkeit im Netz durch Einrichten und Vorhalten von Hyperlinks, CR 6/1998, Seite 357 und 358.

10.2 Abgrenzung von TDG und MDStV

Wie bereits im Abschnitt zur Strafverfolgung ausgeführt wurde, besteht vielfach die Möglichkeit, ein Angebot des Internets als Mediendienst i.S.d. MDStV oder als Teledienst i.S.d. TDG zu qualifizieren[395]. Für die Verantwortlichkeitsbestimmung im Strafrecht ist die Wahl des Gesetzes grundsätzlich unerheblich, da § 5 MDStV und § 5 TDG, die ja die Verantwortlichkeit regeln, weitestgehend identisch sind. Für die Gefahrenabwehr hingegen ist es, wie sich noch zeigen wird, von besonderer Bedeutung, nach welcher Rechtsgrundlage ein Angebot behandelt wird. Denn beide Gesetze enthalten unterschiedliche Zuständigkeitsregelungen[396].

Den Kernpunkt der beiden Gesetze bilden die grundverschiedenen Begrifflichkeiten „Teledienst“ (TDG) und „Mediendienst“ (MDStV). Gem. § 2 I [Geltungsbereich] MDStV gilt der MDStV nur für Angebote und die Nutzung von an die Allgemeinheit gerichteten Informations- und Kommunikationsdiensten (Mediendienste) in Text, Ton oder Bild. § 2 II MDStV zählt beispielhaft die Hauptanwendungsbereiche auf. Gem. § 2 I [Geltungsbereich] TDG gilt das TDG nur für die elektronischen Kommunikations- und Informationsdienste, die der individuellen Nutzung dienen.

Bei den Mediendiensten steht nach h.M. eine redaktionelle Gestaltung zur Meinungsbildung im Vordergrund[397]. Das Angebot richtet sich an die Allgemeinheit (z.B. eine Online-Zeitung). Angebote hingegen, die gewerblichen Zwecken dienen, dem persönlichen Bereich entstammen oder lediglich amtliche Informationen verbreiten, werden grundsätzlich nicht der Meinungsbildung dienen und damit dem TDG unterliegen[398]. Eine Einordnung darf nicht pauschal erfolgen, sondern muß sich an den jeweiligen Besonderheiten des Einzelfalls orientieren.

---

[395] Einen Überblick über die Abgrenzung von Network- und Access-Provider und die Rechtsgrundlagen für Sperranordnungen bietet auch: König/Lötz, Sperrungsanordnungen gegenüber Network- und Access-Providern, CR 7/1999, Seite 438 bis 445.

[396] Eine Erläuterung zu den Abgrenzungsmöglichkeiten zwischen TDG und MDStV auch bei: Flechsig/Gabel, Strafrechtliche Verantwortlichkeit im Netz durch Einrichten und Vorhalten von Hyperlinks, CR 6/1998, Seite 351 bis 358.

[397] Vgl. auch: Engel-Flechsig/Maennel/Tettenborn, Neue gesetzliche Rahmenbedingungen für Multimedia, S.13 (Nachweis bei: Zimmermann, Polizeiliche Gefahrenabwehr und das Internet, NJW 43/1999, Seite 3146).

[398] Vgl. auch: Waldenberg, MMR 1998, 124 (125) (Nachweis bei: Zimmermann, Polizeiliche Gefahrenabwehr und das Internet, NJW 43/1999, Seite 3146).

Es kann durchaus sein, daß beispielsweise ein Angebot im WWW als Mediendienst aber auch als Teledienst qualifiziert werden kann. Auf jeden Fall ist eine Abgrenzung aber als erster Schritt durchzuführen.

Wenn man die Anwendbarkeit des TDG oder des MDStV festgestellt hat, stellt sich als nächstes die Frage, ob die Gesetze spezielle Zuständigkeitsregelungen enthalten. Ansonsten müßte geprüft werden, aus welcher Rechtsgrundlage sich Zuständigkeiten ergeben könnten.

10.3 Zuständigkeiten

10.3.1 Sachliche Zuständigkeit

„Für den Bereich der Mediendienste enthält § 18 [Aufsicht] MDStV in Verbindung mit den Umsetzungsgesetzen der einzelnen Bundesländer sowohl für den Bereich des Jugendschutzes wie auch für den Datenschutz eine Sonderzuweisung.“[399]

Gem. § 18 I MDStV ist für den Jugendschutz nach den §§ 8 [Unzulässige Mediendienste, Jugendschutz] und 9 I [Werbung, Sponsoring] MDStV die jeweilig Landesbehörde für den Jugendschutz zuständig. Die Bestimmungen zum Datenschutz nach den §§ 12 bis 16 MDStV überwachen die allgemein zuständigen Datenschutzbehörden des Bundes und der Länder. Die Einhaltung der übrigen Bestimmungen des MDStV unterliegt gem. § 18 I MDStV einer durch Landesrecht zu bestimmenden Aufsichtsbehörde.

In Brandenburg wurde diese Zuständigkeit durch § 2 I Nr. 3 MDStVDurchfG BB[400] der Medienanstalt Berlin-Brandenburg zugewiesen. In anderen Bundesländern ging man einen anderen Weg[401].

In der Praxis wurde folgende Regelung getroffen. Im Auftrag der Jugendminister der Bundesländer durchsucht jugendschutz.net anlaß-unabhängig das

---

[399] Zimmermann, Polizeiliche Gefahrenabwehr und das Internet, NJW 43/1999, Seite 3146

[400] Gesetz zu dem Mediendienste-Staatsvertrag vom 12. Februar 1997 und zur Durchführung medienrechtlicher Staatsverträge (MDStVDurchfG BB) vom 07.07.1997, GVBl 1997 I, S.75

[401] In Baden-Württemberg beispielsweise ist das Sozialministerium für die Einhaltung der jugendschutzrechtlichen Bestimmungen und der Landesdatenschutzbeauftragte für die Einhaltung der datenschutzrechtlichen Bestimmungen des MDStV zuständig.

Internet. Jugendschutz.net nutzt dabei die Crawlertechnik und darf ausschließlich im Bereich der Mediendienste tätig werden[402].

Besondere Beachtung muß § 2 II MDStVDurchfG BB finden. Danach sind alle anderen öffentlichen Stellen befugt und gehalten, Feststellungen über die Verletzung von Bestimmungen des MDStV den nach Abs. I zuständigen Stellen zukommen zu lassen. Erlangt also die Polizei bestimmte Erkenntnisse, die auf einen Verstoß nach dem MDStV hindeuten, muß sie die zuständige Stelle nach § 2 I MDStVDurchfG BB informieren. Diese Stelle kann dann gefahrenabwehrend einschreiten. Die strafprozessrechtlichen Ermittlungsbefugnisse der Polizeibehörden bleiben weiterhin bestehen.

Im Bereich der Teledienste (TDG) werden – im Gegensatz zum MDStV – keine Zuständigkeiten geregelt. Damit bleiben die allgemeinen Ordnungs- und Polizeibehörden für die Gefahrenabwehr zuständig. Es ist allerdings zu beachten, daß weiterhin der Grundsatz: „Polizei ist Ländersache“ gilt. Demnach muß eine Abgrenzung der Zuständigkeiten der einzelnen Bundesländer zur Gefahrenabwehr vorgenommen werden. Diese Abgrenzung kann durch die Bestimmung der örtlichen Zuständigkeit erfolgen.

10.3.2 Örtliche Zuständigkeit

Für die Mediendienste enthält § 18 V MDStV die Regelungen zur örtlichen Zuständigkeit. Demnach ist stets die Behörde zuständig, in deren Bereich ein betroffener Anbieter seinen Sitz, Wohnsitz oder in Ermangelung dessen seinen ständigen Aufenthalt hat. Ergibt sich danach keine Zuständigkeit, so ist diejenige Aufsichtsbehörde zuständig, in deren Bezirk der Anlaß für die Amtshandlung liegt. Diese Regelung lehnt sich an § 3 I Nr.4 und IV 1 a.E. VwVfG an. Die Zuständigkeitsregelung ist nicht alternativ, sondern stellt in ihrer angegebenen Reihenfolge eine Vorgabe für die Beurteilung der Zuständigkeit dar.

Der Bezirk, in dem der Anlaß der Maßnahme liegt (beim Ausschluß der anderen Zuständigkeitsregelungen), ist danach zu bestimmen, wo die geschützten Interessen gefährdet oder verletzt werden, wo also die behördliche Maßnahme wirksam werden soll.

---

[402] Vgl. auch: Eichler, Bekämpfung der Kriminalität im Internet : Tagung beim BKA am 14./15.12.1998 mit Anmerkungen, CR 3/1999, Seite 203.

Im Gegensatz zum MDStV enthält das TDG keine speziellen Regelungen zur örtlichen Zuständigkeit. Geht von einem Teledienst eine Gefahr aus, müssen die Bestimmungen zur örtlichen Zuständigkeit den Polizeigesetzen der Länder entnommen werden. Für Länder, die keine speziellen polizeilichen Zuständigkeitsregelungen haben, ist das jeweilige VwVerfG heranzuziehen. In Brandenburg existiert eine spezialgesetzliche Regelung. Gem. § 5 [Örtliche Zuständigkeit] POG BB ist originär die Polizeibehörde zuständig, in deren Bezirk die polizeilich zu schützenden Interessen verletzt oder gefährdet werden. Gem. § 5 III POG kann das MI BB einer Polizeibehörde Aufgaben im Bezirk anderer Polizeibehörden übertragen. Gem. § 7 [Amtshandlungen von Polizeivollzugsbeamten anderer Länder und des Bundes in Brandenburg] I und III POG ist es möglich, mit Zustimmung des MI BB Teilbereiche der Gefahrenabwehr auch auf Bundesbehörden zu übertragen[403]. In der Praxis erfolgt die Kommunikation mit den Providern über das LKA.

Da – wie bereits dargestellt – ein Internetangebot sowohl in Teilbereichen Mediendienst und in Teilbereichen Teledienst sein kann, würde es dahingehend zu Problemen kommen, daß mehrere Stellen zuständig sein können. In der Literatur wird oft die Meinung vertreten, daß der Gesetzgeber durch das IuKDG und den MDStV eigentlich Normenklarheit schaffen wollte. In der Praxis hingegen hat sich aber oft eine Art „Zwitterstellung“ herausgebildet, da die Abgrenzung von MDStV und TDG nicht so einfach erscheint, wie sie angedacht war. Ob die Regulierung der neuen Medien durch zwei Gesetze in der Praxis und angesichts der sich deutlich abzeichnenden technischen und gesellschaftlichen Entwicklung auf Dauer bestehen kann, wird sich zeigen.

10.4 Materielle Voraussetzungen

Gem. § 7 I [Inhalte, Sorgfaltspflichten, Meinungsumfragen] MDStV müssen die Mediendienste der verfassungsmäßigen Ordnung, den Vorschriften der allgemeinen Gesetze und den gesetzlichen Bestimmungen zum Schutz der persönlichen Ehre entsprechen. Für eine weitere Betrachtung ist primär der Begriff der verfassungsmäßigen Ordnung bedeutsam. Nach der Rechtspre-

[403] Betrachtungen zu den rechtlichen Grundlagen der anlaßunabhängigen Recherchen des BKA im Internet werden an anderer Stelle gemacht.

chung des BVerfG[404] enthält die verfassungsmäßige Ordnung die Gesamtheit der formell und materiell mit der Verfassung in Einklang stehenden Rechtsnormen. Somit werden jegliche Verstöße gegen geltendes Recht erfaßt.

Das TDG kennt eine Regelung wie § 7 MDStV nicht. Allerdings kann eine Argumentation nach allgemein anerkannten juristischen Grundsätzen zu dem gleichen Ergebnis gelangen. Durch ein Gesetz darf nicht erlaubt werden, was durch ein anderes Gesetz verboten wird. Um umgekehrten Sinne kann ein Gesetz nicht verbieten, was ein anderes erlaubt[405]. Die Rechtsordnung muß in sich schlüssig sein.

Dem § 5 TDG und dem § 5 MDStV wird nach h.M. eine Filterfunktion zuerkannt. Diese Filterfunktion macht nichts anderes, als Haftungen zu beschränken. Wenn man den Adressaten einer polizeilichen Maßnahme mit Bezug auf die neuen Medien ermitteln will, könnten die Haftungsprivilegierungen des TDG und des MDStV angewendet werden.

Ob die Haftungsprivilegierungen des TDG für Polizei- und Ordnungsrecht gilt, ist in der Literatur umstritten[406]. Nach h.M. bezieht sich die Haftungsprivilegierung ausschließlich auf die Beurteilung straf- oder zivilrechtlicher Haftung. M.E. ist der Ansicht Zimmermanns zu folgen, der davon ausgeht, daß die im § 5 TDG enthaltene Haftungsprivilegierung nicht für ordnungsbehördliche Maßnahmen gilt. Diese Ansicht kann durch verschiedene Argumente untermauert werden.

In den Gesetzgebungsmaterialien zum TDG heißt es, daß die Absätze I bis III des § 5 TDG strafrechtliche bzw. deliktische Verantwortlichkeit regeln sollen. Es sollte eine Überregulierung der neuen Medien verhindert werden. Ferner spricht § 5 IV TDG explizit die Sperrungsmöglichkeiten nach den allgemeinen Gesetzen an.

---

[404] Vgl. auch: BVerfGE 6, 32, abgedruckt in NJW 1957, S. 297.

[405] Dieser Grundsatz wird beispielsweise bei der Heranziehung von Rechtfertigungsgründen im Strafrecht genutzt; strafrechtliche Rechtfertigungsgründe können sich demnach aus jedem beliebigen Gesetz (BGB, StPO etc.) ergeben.

[406] Vgl. auch: Zimmermann, Polizeiliche Gefahrenabwehr und das Internet, NJW 43/1999, Seite 3147 und 3148 mit Hinweis auf: Regierungsbegründung zu § 5 TDG, BT-Dr. 13/7358, S.19 f.; Müller-Using/Lücke, Archiv für Post – und Telekommunikation (ArchivPT) 1997, 101 (106); Waldenberg, AfP 1998, 373 (373); Engel-Flechsig/Maennel/Tottenborn, NJW 1997, 2981 (2984), die davon auszugehen scheinen, daß der „Filter“ des § 5 TDG auch für Polizei- und Ordnungsrecht gilt.

Somit enthält § 5 IV TDG keine eigenständige Verpflichtung zur Unterlassung von Störungen und somit auch keine Eingriffsermächtigung für die Polizei. Vielmehr wird eine Verpflichtung zur Unterlassung von Störungen und die daraus korrespondierende Eingriffsermächtigung aus den allgemeinen Gesetzen abgeleitet werden müssen. Da im Bereich des TDG die Polizei örtlich und sachlich zuständig ist, könnte eine Sperranordnung auf der Grundlage der Generalklausel des § 10 [Allgemeine Befugnisse, Begriffsbestimmung] PolG BB erfolgen.

„Demgegenüber ist die Funktion von § 5 i.V.m. § 18 II und III MDStV eine andere. § 18 II MDStV enthält – anders als § 5 TDG – eine spezialgesetzliche Eingriffsermächtigung zu Lasten betroffener Anbieter. § 18 III MDStV konkretisiert sodann diese Eingriffsermächtigung, indem er deutlich macht, daß Sperrungsverfügungen grundsätzlich nicht nur gegenüber Anbietern wegen deren eigenen Angeboten oder wegen fremden Inhalten erfolgen können, die sie zur Nutzung bereithalten, sondern in Ausnahmefällen auch gegenüber Anbietern erfolgen können, die lediglich den Zugang zur Nutzung fremder Inhalte vermitteln.“[407]

10.5 Störerbegriffe

Da sich die Ermächtigungsgrundlage im Bereich des TDG aus dem Polizeigesetz ergibt und im Bereich des MDStV aus § 18 II MDStV, müssen die Störerbegriffe dementsprechend auch aus diesen gesetzlichen Grundlagen entnommen werden[408]. „Die Adressatenregelung macht nur eine Aussage über die Inanspruchnahme der richtigen Person.

Sie ersetzt nicht die Aufgabenregelung, insbesondere nicht die Befugnisnorm. Sie ist eine weitere Voraussetzung für die Rechtmäßigkeit polizeilichen Handelns.“[409]

Im Geltungsbereich des MDStV können Maßnahmen gegen den Content-Provider aus § 5 I MDStV abgeleitet werden, da er für eigene Inhalte voll verantwortlich ist. Die Subsidiaritätsklausel des § 18 III MDStV verpflichtet die zu-

---

[407] Zimmermann, Polizeiliche Gefahrenabwehr und das Internet, NJW 43/1999, Seite 3148

[408] Zur Störerfrage vgl. auch: „Strafrechtliche Aspekte des Internet : Lösungen und Möglichkeiten“, Kriminalistik 10/1998, Seite 685 bis 688.

[409] Tegtmeyer, Polizeigesetz Nordrhein-Westfalen, Seite 77

ständigen Behörden, zuerst gegen den Urheber eines Inhalts vorzugehen. Gem. § 5 [Verantwortlichkeit für das Verhalten von Personen] PolG BB könnte der Content-Provider von Telediensten als Verhaltensstörer qualifiziert werden. Als Verhaltensstörer kann nur herangezogen werden, „wer durch eigenes Verhalten die Gefahr oder Störung verursacht hat, oder wer [...] für die Verursachung durch einen anderen neben diesem verantwortlich ist“[410]. Der Content-Provider verursacht durch seine Handlung unmittelbar die Gefahr und ist damit Verhaltensstörer i.S.d. PolG BB.

Maßnahmen gegen den Serviceprovider sind im Rahmen des MDStV nur möglich, wenn er gem. § 5 II MDStV von den rechtswidrigen Inhalten eines Angebotes positive Kenntnis hat. Die positive Kenntnis kann der Anbieter u.a. durch die Aufsichtsbehörde erlangen, die gleichzeitig mit der Inkenntnissetzung des Providers ihre Sperranordnung erläßt[411]. Gem. § 6 [Verantwortlichkeit für den Zustand von Sachen und Tieren] PolG BB könnte der Serviceprovider von Telediensten i.S.d. TDG als Zustandsstörer qualifiziert werden. „Die Verantwortlichkeit für den Zustand einer Sache [...] trifft den Eigentümer und den Inhaber der tatsächlichen Gewalt. Sie sind Störer, wenn von der Sache eine Gefahr für die öffentliche Sicherheit ausgeht. [...] Inhaber der tatsächlichen Gewalt ist derjenige, der die tatsächliche Sachherrschaft hat.“[412] Nach der h.M. ist es unerheblich, wodurch der gefährliche Zustand verursacht worden ist und ob ein Verschulden des Zustandsstörers vorliegt.

Der Serviceanbieter eines Teledienstes ist Zustandsstörer, wenn er strafbare Inhalte eines Contentproviders auf seinen Rechneranlagen bereithält. Er allein hat die technischen Möglichkeiten (Inhaber der tatsächlichen Gewalt), die fremden Inhalte zu löschen[413].

---

[410] ebd., Seite 82

[411] Vgl. auch: Spindler, NJW 1997, 3193 (3196); Koch, Zivilrechtliche Anbieterhaftung für Inhalte in Kommunikationsnetzen, CR 1997, 193 (199); (Nachweis bei: Zimmermann, Polizeiliche Gefahrenabwehr und das Internet, Seite 3148).

[412] Tegtmeyer, Polizeigesetz Nordrhein-Westfalen, Seite 85 und 87

[413] Diese Ausführungen sind differenziert zu sehen; rein technisch gesehen besteht zwischen dem Contentprovider und dem Serviceprovider regelmäßig eine geteilte tatsächliche Herrschaftsgewalt, da beide in der Lage sind, die Inhalte zu löschen; wird die Löschung durch den Serviceprovider vorgenommen, kann der Contentprovider die Inhalte erneut uploaden, auf einen anderen Account ausweichen oder den Serviceprovider wechseln; dies ändert nichts an der Tatsache, daß der Serviceprovider (wenn auch nur einen Teil) der tatsächlichen Herrschaftsgewalt hat.

Maßnahmen gegen den Accessprovider sind unter den strengen Voraussetzungen des § 18 III MDStV möglich. Grundsätzlich sind Maßnahmen als erstes gegen den Content-Provider zu richten. Als nächstes kann der Serviceprovider in die Verantwortung genommen werden. Erst wenn diese Maßnahmen erfolglos durchgeführt wurden oder von vornherein aussichtslos erscheinen, kann eine Maßnahme gegen den Accessprovider gerichtet werden. Der Accessprovider ist im Bereich des TDG weder Verhaltens- noch Zustandsstörer im Sinne des Polizeirechts. Weder hat er durch eigenes Verhalten eine Gefahr verursacht (der Content-Provider als Urheber hat die Gefahr verursacht), noch hat er die tatsächliche Sachherrschaft (oder einen Teil davon), da er Inhalte objektiv nicht löschen kann. Der Accessprovider leitet ausschließlich Daten durch sein Netzwerk und bietet dem Benutzer lediglich das Grundprotokoll TCP/IP[414]. Demnach kann er nicht verantwortlich sein. Eine Inanspruchnahme kann daher nur auf der Grundlage des § 7 [Inanspruchnahme nicht verantwortlicher Personen] PolG BB erfolgen. Die Eingriffsvoraussetzungen sind dementsprechend sehr hoch angesiedelt. So ist das Vorliegen einer gegenwärtigen erheblichen Gefahr zwingend erforderlich. Danach muß das schädigende Ereignis unmittelbar bevorstehen oder bereits eingetreten sein und noch andauern. Ferner muß die Gefahr einem bedeutenden Rechtsgut wie Leben oder Gesundheit oder einem wichtigen Gemeinschaftsgut drohen[415]. An der Gegenwärtigkeit wird es im Internet selten mangeln, da es sich wohl bei der Mehrheit der Fälle um Dauerdelikte handeln wird. Schwierigkeiten wird höchstens das Merkmal „erheblich“ bereiten, denn was sind hochwertige Gemeinschaftsgüter?

Der Schutz der Jugend vor Kinderpornographie (Schutz der ungestörten sexuellen Entwicklung) oder der Schutz vor extremistischer Propaganda (Schutz der freiheitlich demokratischen Grundordnung) sind sicherlich wichtige Gemeinschaftsgüter. Eine Beurteilung muß die Gegebenheiten des Einzelfalls berücksichtigen. „Die grundsätzliche Qualifikation des Zugangsanbieters [als unbeteiligter Dritter] bringt es zugleich mit sich, daß neben den sonstigen Einschränkungen der polizeilichen Handlungsmöglichkeiten dem betroffenen Teleddiensteanbieter grundsätzlich eine angemessene Entschädigung für den ihm

---

[414] In diesem Sinne unterscheidet er sich auch vom reinen Network-Provider/Carrier, der nur die physikalischen Übertragungswege ohne spezifische Internet-Software bereitstellt.

[415] Vahle, Schaubilder zum Polizeirecht, Kriminalistik 2/2000, Seite 138

entstandenen Schaden zu gewähren ist."[416] Insofern, ist für Brandenburg § 70 [Entschädigungsansprüche] PolG BB i.V.m. §§ 38 bis 42 OBG BB zu beachten.

10.6 Sonderproblem – Hyperlinks

Was passiert, wenn der Diensteanbieter durch einen Hyperlink auf ein polizeiwidriges Angebot verweist? Kann eine Sperranordnung auch den Linkenden treffen?

Im Bereich des MDStV stellt sich als erstes die Frage, ob es sich bei dem Verweis und den direkt dahinter liegenden Informationen um eigene Inhalte des Contentproviders i.S.d. § 5 I MDStV handelt[417]. „Bereits die Begründung zu § 5 I MDStV macht [...] deutlich, daß es nicht darauf ankommt, ob es sich um Inhalte handelt, die vom Anbieter ursprünglich selbst verantwortet wurden oder ob sie ein Dritter hergestellt hat."[418] Voraussetzung dabei muß sein, daß sich der Anbieter den Inhalt zu eigen macht. Wenn sich der Anbieter aber vom Inhalt distanziert oder der Link im Kontext der Seite nur eine technische Hilfe zur Auswahl bildet, muß eine Verantwortlichkeit abgelehnt werden. Durch die Rechtsprechung wurde diese Ansicht bestätigt[419].

Im Bereich des TDG kommt man durch die Anwendung allgemeinpolizeilicher Grundsätze zu einem ähnlichen Ergebnis. Demnach ist eine Inanspruchnahme dann möglich, wenn der Anbieter des Links als Zweckveranlasser qualifiziert werden kann[420]. Von einer Zurechnung muß man dann ausgehen, wenn der Linkende durch die Gestaltung seiner Homepage deutlich macht, daß er entweder die Zugriffe auf die polizeiwidrigen Inhalte billigt oder die verweisen-

---

[416] Zimmermann, Polizeiliche Gefahrenabwehr und das Internet, Seite 3149, Fn. 46

[417] Zur ausführlichen Einordnung von Links unter § 5 TDG und § 5 MDStV vgl. auch: Bettinger/Freytag, Privatrechtliche Verantwortlichkeit für Links, CR 9/1998, Seite 546 bis 552.

[418] Zimmermann, Polizeiliche Gefahrenabwehr und das Internet, Seite 3149, Fn. 45

[419] Bestätigt wird diese Auffassung durch das Urteil des LG Hamburg (LG Hamburg, Urteil vom 12.05.1998 – 312 O 85/98, abgedruckt in CR 9/1998, Seite 565); das Gericht hatte den Beklagten zu Schadenersatz gegenüber dem Kläger verurteilt, weil er durch einen Link auf ein Satiremagazin, das die Persönlichkeitsrechte des Klägers verletzte, verwiesen hatte; das Gericht begründete seinen Urteilsspruch damit, daß der Beklagte sich nicht ausreichend von der rechtswidrigen Seite distanziert und keinen sogenannten „Markt der Meinungen" eröffnet hatte; vgl. dazu auch: Vassilaki, Strafrechtliche Verantwortlichkeit durch Einrichten und Aufrechterhalten von elektronischen Verweisen (Hyperlinks), CR 2/1999, Seite 85 bis 93.

[420] Vgl. auch: VGH Mannheim, NVwZ-RR 1995, 663; OVG Lüneburg, NVwZ 1997, 622 (Nachweis bei: Zimmermann, Polizeiliche Gefahrenabwehr und das Internet, Seite 3149).

de Seite so gestaltet ist, daß sie es dem jeweiligen Benutzer geradezu nahelegt, auf die rechtswidrige Seite zuzugreifen.

10.7 Störerauswahl

Prinzipiell kommt die Inanspruchnahme eines Nichtstörers im Bereich der Teledienste nur subsidiär in Frage (§ 7 I Nr.2 PolG BB). Hat die Polizei die Wahl zwischen Handlungs- und Zustandsstörer, besteht nach Auffassung Zimmermanns – abgeleitet aus dem allgemeinen Polizeirecht – für die Polizei nicht die Pflicht, vorrangig den Handlungsstörer (Content-Provider) in Anspruch zu nehmen[421]. Die Polizei hat den Störer auszuwählen, bei dessen Inanspruchnahme die Gefahr am schnellsten und am wirkungsvollsten beseitigt werden kann[422].

Im Bereich der Mediendienste ergibt sich eine identische Reihenfolge aus § 18 III MDStV. Eine Inanspruchnahme des Accessproviders ist nur dann zulässig, wenn eine Sperrverfügung gegenüber dem Content- oder Serviceprovider nicht durchführbar oder nicht erfolgversprechend ist. Insofern ist auch für Mediendienste eine Subsidiaritätsklausel vorhanden. § 18 III MDStV gibt dem Content-Provider keinen Vorzug vor dem Serviceprovider. Demnach muß sich die Behörde – ähnlich wie bei den Telediensten – bei einer möglichen Inanspruchnahme beider Adressaten den Adressaten aussuchen, bei dessen Inanspruchnahme die Gefahr am schnellsten und wirkungsvollsten beseitigt wird.

Die Abwägung, ob ein Serviceprovider oder ein Content-Provider in Anspruch genommen wird, darf nicht willkürlich erfolgen. Grundsätzlich haben die Behörden Auswahlermessen.

Dennoch darf die Auswahl nicht ermessensfehlerhaft sein. Die Behörden sollten bedenken, daß es schon aus Gründen der Verhältnismäßigkeit angebracht sein kann, den Content-Provider dem Serviceprovider vorzuziehen. Allein durch die Löschung der Inhalte beim Urheber kann eine weitere Verbreitung weitestgehend verhindert werden, da bei der Sperrung durch den Serviceprovider die Gefahr besteht, daß sich der Content-Provider einen anderen Ser-

---

[421] Zimmermann, Polizeiliche Gefahrenabwehr und das Internet, Seite 3149, mit Hinweis u.a. auf: VGH Mannheim, Baden-Württembergische Gemeindezeitung (BWGZ) 1996, 606 (610); VGH Mannheim, VBlBW 1990, 257 (260).

[422] Tegtmeyer, Polizeigesetz Nordrhein-Westfalen, Seite 80 und 81

viceprovider sucht. Die inkriminierten Inhalte würden dann einfach an anderer Stelle zu finden sein.

10.8 Grundsatz der Verhältnismäßigkeit

10.8.1 Allgemeines

„Der Verhältnismäßigkeitsgrundsatz hat Verfassungsrang. Er ist Ausfluß des Rechtsstaatsprinzips und ergibt sich im Grunde bereits aus dem Wesen der Grundrechte selbst, die von der öffentlichen Gewalt jeweils nur so weit beschränkt werden dürfen als es zum Schutze öffentlicher Interessen unerläßlich ist […].“[423]

Der MDStV enthält Sonderbestimmungen für die Beurteilung der Verhältnismäßigkeit bei Sperranordnungen an Mediendienste (§ 18 MDStV). Die Kriterien entsprechen aber sehr stark den spezifischen polizeirechtlichen Vorschriften. Für Teledienste ist insofern § 3 [Grundsatz der Verhältnismäßigkeit] PolG BB einschlägig.

Der Grundsatz der Verhältnismäßigkeit besteht nach h.M. aus drei Einzelprinzipien – Geeignetheit, Erforderlichkeit und Verhältnismäßigkeit im engeren Sinne. Nur die Beachtung aller Einzelprinzipien ergibt in der Konsequenz eine rechtmäßige Maßnahme. D.h. daß eine Maßnahme durchaus den Eingriffsvoraussetzungen einer Ermächtigungsnorm entsprechen kann. Wenn sie aber unverhältnismäßig ist, wird sie automatisch rechtswidrig. Die Verhältnismäßigkeit ist demnach ein ungeschriebenes Merkmal jeder Ermächtigungsnorm.

10.8.2 Geeignetheit

Im Bereich des Internets ist eine Sperranordnung geeignet, wenn sie technisch möglich ist und zur Erreichung des Ziels, die Verbreitung bestimmter Inhalte zu verhindern oder einzuschränken, einen Beitrag leisten kann. Es wird wohl jedem klar sein, daß die 100%ige Sperrung niemals erreicht werden kann. Der Benutzer hat die Möglichkeiten, sich über einen anderen Provider einzuwählen, ausländische News-Server zu benutzen oder seine rechtswidrige Homepage bei einem anderen Serviceprovider zu hosten. Rechtswidrige Inhalte

[423] ebd., Seite 69 mit Hinweis auf: BVerfGE 19, S.384

können auf mehrere Server gespiegelt werden, so daß die Sperrung eines Servers keine tiefgreifenden Folgen hat. Dies sind jedoch keine Argumente für die Ungeeignetheit behördlicher Sperranordnungen, da die Einschränkung der Zugriffsmöglichkeiten und die ständige Verunsicherung der Urheber auch schon ein lohnenswertes Ziel darstellen. Wenn nämlich die Urheber ständig gezwungen sind, ihre Angebote zu verlagern oder neue Serviceprovider zu suchen, nimmt die Wahrscheinlichkeit, daß Kinder oder Jugendliche per Zufall an rechtswidrige Angebote gelangen, ab. Eine vollständige Gefahrenabwehr kann nicht erreicht werden. Daher ist dieser Umstand auch nicht als Meßlatte für die Beurteilung der Geeignetheit heranzuziehen[424].

10.9 Erforderlichkeit

Im Gegensatz zur Geeignetheit wird die Erforderlichkeit in § 18 II Satz 1 MDStV explizit angesprochen. Eine Maßnahme ist erforderlich, wenn die Behörde von mehreren geeigneten die Maßnahme anordnet, die den Einzelnen und die Allgemeinheit voraussichtlich am wenigsten beeinträchtigt[425]. Demnach muß das mildeste Mittel angewendet werden.

Für die Praxis bedeutet das ein Pflicht zu differenzierendem Vorgehen, unter weitestgehender Beachtung der Bedürfnisse der Provider und auch der Internetnutzer. Untersagungsverfügungen müssen sich speziell gegen die rechtswidrigen Inhalte richten.

So kann die Löschung einzelner News i.S.d. § 18 II Satz 5 MDStV der Sperrung einer ganzen Newsgroup vorgehen[426]. Bestimmte Angebote können zeitlich beschränkt werden, so daß eine Sperrung nur zu bestimmten Tageszeiten erfolgt (§ 18 II Satz 5 MDStV). Es ist zu beurteilen, gegenüber wie vielen Nutzern eine Sperrung wirksam wird. Richtet sich ein Angebot, in dem vereinzelt rechtswidrige Inhalte auftauchen, an eine größere Anzahl Benutzer, liegt die Eingriffsschwelle sicherlich höher als bei einem kleinen Benutzerkreis. Die Ausführungen bezogen sich auf Mediendienste, sind aber analog auch auf Teledienste anwendbar.

---

[424] Belz/Mußmann, BadWürttPolG, 5. Aufl. (1996), § 5 Rdnr. 3 (Nachweis bei: Zimmermann, Polizeiliche Gefahrenabwehr und das Internet, Seite 3150)

[425] Tegtmeyer, Polizeigesetz Nordrhein-Westfalen, Seite 70

10.10 Verhältnismäßigkeit im engeren Sinne

Die Verhältnismäßigkeit im engeren Sinne ergibt sich aus § 18 II Satz 3 MDStV. Demnach darf eine Untersagung des Angebots nicht erfolgen, wenn die Maßnahme außer Verhältnis zur Bedeutung des Angebots für den Anbieter oder die Allgemeinheit steht. Welche Bedeutung ein Angebot für die Allgemeinheit hat, kann nur am konkreten Einzelfall festgemacht werden.

„Ferner ergibt sich aus § 18 III MDStV einerseits und § 5 IV TDG andererseits, daß Sperrungsverfügungen zu Lasten von Zugangsanbietern stets nur dann zulässig sind, wenn deren Durchführung ihnen auch zumutbar ist.“[427] Dies wird in der Regel bedeuten, daß nur eine zielgerichtete Löschungs- oder Sperrverfügung verhältnismäßig ist.

Kann man bei einer Sperranordnung an einen Content- oder Serviceprovider noch von einer individualisierbaren Sperrungsmöglichkeit ausgehen, sind den Möglichkeiten bei den Accessprovidern enge Grenzen gesetzt. Der Generalbundesanwalt kam zu der Ansicht, daß es dem Accessprovider grundsätzlich zugemutet werden kann, einen Proxy einzusetzen, um dadurch gezielt polizeiwidrige Inhalte zu sperren[428]. Dabei wird aber regelmäßig vergessen, daß diese Einrichtung und die damit verbundene kontinuierliche Anpassung des Systems einen erheblichen technischen Einsatz erfordert.

Ferner wechseln Benutzer oftmals den Anbieter, wenn ein Proxy eingesetzt wird, da es zu Performance-Einbußen kommen kann. Daher kann eine solche Verpflichtung nur dann einen wirklichen Erfolg herbeiführen, wenn alle Provider einen solchen Filter einsetzen müssen. Für die Benutzer bleibt dann immer noch die Ausweichmöglichkeit auf einen ausländischen Provider!

10.11 Die anlaßunabhängige Recherche im Internet durch das BKA

Dieser Abschnitt soll sich mit den Grundlagen der anlaßunabhängigen Recherche des BKA befassen. Es soll aufgezeigt werden, wie es zur Einrichtung der zuständigen Stelle im BKA kam, wie diese arbeitet und welche Ergeb-

---

[426] In diesem Zusammenhang muß die Bedeutung der Newsgroups auch vor dem Hintergrund des Art. 5 [Meinungs – und Pressefreiheit; Freiheit der Kunst und der Wissenschaft] GG gesehen werden.

[427] Zimmermann, Polizeiliche Gefahrenabwehr und das Internet, Seite 3151

[428] Einen Überblick über die allgemein anerkannte Auslegung des Begriffes „Zumutbarkeit“ bei: Eichler, Bekämpfung der Kriminalität im Internet : Tagung beim BKA am 14./15.12.1998 mit Anmerkungen, CR 3/1999, Seite 202.

nisse verzeichnet werden konnten. Die Ausarbeitung erfolgte anhand von verschiedenen behördlichen Unterlagen, die fast ausschließlich VS-NfD[429] sind. Allerdings sind die Ausführungen sehr allgemein gehalten. Daher enthält dieser Abschnitt keine geheimhaltungsbedürftigen Informationen[430].

Im Jahre 1989 hatte sich die AG Kripo erstmals der Frage gewidmet, wie gegen Anbieter von pornographischen oder sonstigen jugendgefährdenden Schriften im Btx vorgegangen werden könnte. Eine Aufgabenübernahme durch das LKA Baden-Württemberg scheiterte an der Kostenfrage.

Erst 1993 wurde das Thema erneut aufgegriffen. Zu dieser Zeit wurde bereits durch das LKA Bayern die Verbreitung kinderpornographischer Bilder und Schriften in den einschlägigen Printmedien erforscht. Dabei wurde festgestellt, daß zunehmend auch die neuen Medien an Bedeutung gewinnen. Anlaß dafür war die Häufung entsprechender Ermittlungsverfahren, die grundlegende Veränderung der Medienlandschaft und die weite Verbreitung elektronischer Medien sowie parlamentarische Aktivitäten in Zusammenhang mit der Verabschiedung des 27. Strafrechtsänderungsgesetzes vom 23.07.1993. In diesem Zusammenhang wurde festgestellt, daß eine zentrale Auswertung erfolgen müsse. Bei der 128. Tagung der AG Kripo wurde der Beschluß gefaßt, daß das LKA Baden-Württemberg in einem Pilotprojekt zunächst die Aufgaben einer zentralen Auswertungsstelle für kinderpornographische Medien übernehmen sollte.

Das LKA Baden-Württemberg legte im November 1995 einen Abschlußbericht vor, der vor allem die Empfehlung enthielt, in jedem LKA eine Ansprechstelle für Kinderpornographie einzurichten[431].

Im Auftrag des bayerischen StMI führten im Rahmen eines Pilotprojektes ab dem 01.01.1995 sowohl das bayerische LKA, als auch das PP München anlaßunabhängige Recherchen in den neuen Medien durch. Den Schwerpunkt bildete die Suche nach Kinderpornographie. Vereinzelt gab es auch anlaßunabhängige Recherchen in Berlin und Baden-Württemberg. Auf der 141. Ta-

---

[429] Verschlußsache – Nur für den Dienstgebrauch

[430] Das Thema „Anlaßunabhängige Recherche im Internet“ stößt auf reges Interesse in den Medien; die Ausführungen lassen sich auch anhand verschiedener journalistischer Beiträge rekonstruieren.

[431] In Brandenburg wurde das Dezernat 34/Prävention mit dieser Aufgabe betraut.

gung der AG Kripo (März 1998) stellte das LKA Bayern einen Erfahrungsbericht zu ihrem Pilotprojekt vor.

Aufgrund eines Beschlusses der Innenministerkonferenz vom Mai 1998 wurde eine gemeinsame Projektgruppe aus Vertretern der AG Kripo, des UARV und des UAFEK eingesetzt, unter dem Arbeitstitel: „Erfordernis, Organisation und Koordination von anlaßunabhängigen Recherchen im Internet“. Die Leitung hatte dabei das LKA Bayern. Der Abschlußbericht der Projektgruppe, der auf der 142. Tagung der AG Kripo (September 1998) vorgestellt wurde, enthielt einige wichtige Schlußfolgerungen.

Die Mitarbeiter der Projektgruppe kamen u.a. zu dem Ergebnis, daß sich aus dem BKAG[432] keine rechtliche Grundlage für eine originäre Erhebung personenbezogener Daten oder für eine verdeckte Datenermittlung ergeben. Diese Möglichkeiten bieten nur die Gefahrenabwehrgesetze der Länder[433]. Durch das BKA, das LKA Mecklenburg-Vorpommern und das LKA Brandenburg wurde die Auffassung vertreten, daß für öffentliche und frei zugängliche Bereiche im Internet keine Ermächtigungsgrundlage notwendig ist. Für nichtöffentliche Bereiche (Paßwortsperren etc.) liegt im BKAG keine Ermächtigungsgrundlage vor. Solche Ermittlungen sind nur dann möglich, wenn ein Anfangsverdacht gem. § 163 StPO vorliegt. Dann könnte auch das BKA – kraft seiner Eilkompetenz – zuständig sein. Allerdings bestand weitgehend Einigkeit darüber, daß eine Zentralstelle beim BKA eingerichtet werden sollte.

Eine Zentralstelle beim BKA ist deswegen sinnvoll, da dadurch Aufgabenüberschneidungen und Doppelarbeit verhindert werden. Weiterhin kann erforderliche Technik konzentriert werden (Kostenfaktor), was einen effektiven Personal- und Mitteleinsatz sicherstellt. Das BKA hat originär eine Zentralstellenfunktion, ist Zentralbüro für die IKPO (Abwicklung des Auslandsverkehrs über das BKA) und führt die Verbunddatei „Kinderpornographie“.

Mit Beschluß der Innenministerkonferenz auf ihrer 153. Sitzung am 19./20. November 1998 (zu TOP 24) wurde das BKA beauftragt, die Aufgabe der anlaßunabhängigen Recherche im INTERNET und den Online-Diensten für das gesamte Bundesgebiet wahrzunehmen und zur Herbsttagung 1999 einen Bericht

---

[432] Gesetz über das Bundeskriminalamt

über die gewonnenen Erfahrungen vorzulegen[434]. Der Erfahrungsbericht verdeutlicht die Vorgehensweise des BKA. Einige wesentliche Grundlagen sollen nun kurz dargestellt werden.

Das BKA nimmt die Aufgabe der anlaßunabhängigen Recherche im Internet im Rahmen des § 2 II und VI BKAG wahr. Zuständige Stelle ist das Fachreferat OA 34. Ab Januar 1999 wurde ein Feinkonzept zur Einrichtung der „Zentralstelle für anlaß-unabhängige Recherchen in Datennetzen“ (ZaRD) erarbeitet. Anfang März 1999 wurde die erforderliche Personalstärke erreicht. Die ZaRD arbeitet nach folgendem Grundkonzept:

- ständige, systematische, anlaßunabhängige, deliktübergreifende Recherche in den Datennetzen, insbesondere im Internet, auf strafrechtlich relevante Inhalte
- Entgegennahme von Hinweisen auch über E-Mail von privater Seite oder anderen Stellen – unbeschadet anderer Zuständigkeiten
- (Vor-)Prüfung auf strafrechtliche Relevanz
- Beweiserhebung, -sicherung und -dokumentation (in Eilfällen)
- weiterführende Verfolgung von Straftaten bis zur Klärung der örtlichen Zuständigkeit und entsprechende Abgabe des ermittelten Sachverhalts
- Informationsaustausch und aufgabenbezogene Zusammenarbeit mit anderen öffentlichen und privaten Stellen und Einrichtungen
- Lagedarstellung
- taktische Öffentlichkeitsarbeit nach innen und außen
- Beteiligung an Aus- und Fortbildungsmaßnahmen

Die spezifischen Ermittlungen in den Fachbereichen des BKA und anderer Fachdienststellen bleiben durch die anlaßunabhängige Recherche unberührt. Demnach können auch auf Landesebene Ermittlungen durchgeführt werden,

---

[433] Hartung, Internet, dp-special April 1998, Seite 13, geht davon aus, daß die Grundlage für die anlaß-unabhängige Recherche im Internet die Polizeigesetze der Länder sind.

[434] Vgl. auch: Eichler, Bekämpfung der Kriminalität im Internet : Tagung beim BKA am 14./15.12.1998 mit Anmerkungen, CR 3/1999, Seite 200 bis 204.

wenn konkreter Anlaß dazu besteht. Da die ZaRD bereits über grundlegende Erfahrungen im Umgang mit den verschiedenen Internet-Diensten verfügt, wird es sich immer anbieten, bei entsprechenden Ermittlungen auf diese Erfahrungen zurückzugreifen[435].

Die Arbeit der ZaRD muß als Vorfeldmaßnahme verstanden werden. Die Zentralstelle sucht nach Ermittlungsansätzen, die kriminalpolizeiliche Sachbearbeitung erfolgt bei den zuständigen Fachdienststellen.

Vom 01.01.1999 bis 13.07.1999 wurden durch die anlaßunabhängige Recherche im Internet durch die ZaRD 519 Verdachtsmeldungen erstellt. Die Fälle verteilen sich auf verschiedene Deliktbereiche. Kinderpornographie bildet den Hauptanteil der recherchierten Fälle[436]. Ca. 90 % der Sachverhalte hatten Auslandsbezug[437].

Nach Ansicht des BKA hat sich die Einrichtung der ZaRD bewährt. Die Entscheidung, eine zentrale Stelle beim BKA einzurichten, war eine richtige Maßnahme, da es im Bereich des Internets vor allem auch auf internationale Zusammenarbeit ankommt. Dies wird vor allem durch den hohen Anteil an Auslandsstraftaten deutlich.

10.12 Zusammenfassung

Grundsätzlich kann die Polizei zur Strafverfolgung und auch zur Gefahrenabwehr im Internet tätig werden. Die juristische Literatur hat sich aber bisher ausschließlich mit straf- , strafprozess- und zivilrechtlichen Problemen auseinandergesetzt. Die Verbreitung rechtswidriger Inhalte im Internet stellt mithin eine Gefahr für die öffentliche Sicherheit und Ordnung dar.

Im Bereich des Internets muß die Polizei entscheiden, ob ein Angebot als Teledienst i.S.d. § 2 TDG oder als Mediendienst i.S.d. § 2 MDStV einzuordnen ist. Die Grenzen sind fließend, eine Einordnung ist nicht immer eindeutig mög-

---

[435] Dafür stehen im BKA die Arbeitsbereiche „Internetermittlungen“ und „EDV-Beweissicherung“ zur Verfügung.

[436] Mithin muß davon ausgegangen werden, daß das Dunkelfeld bei allen Deliktbereichen enorm hoch ist, so daß ein absoluter Rückschluß auf die tatsächliche Verteilung sicherlich nicht unproblematisch ist; das BKA geht davon aus, daß der phänomenologische Schwerpunkt im Bereich der Kinderpornographie liegt.

[437] Diese Prozentzahl ist nicht geeignet, etwas über die tatsächliche geographische Verteilung der Tatverdächtigen auszusagen.

lich. Mediendienste richten sich an die Gemeinschaft und dienen der Meinungsbildung. Teledienste richten sich an den einzelnen Nutzer.

Für den Bereich der Mediendienste enthält § 18 MDStV eine eindeutige sachliche Zuständigkeitsregelung. In Brandenburg erhält die Polizei gem. § 2 MDStVDurchfG BB keine originäre Zuständigkeit für Mediendienste. Allerdings können auch die Polizeibehörden Informationen an die originär zuständigen Stellen weiterleiten. Die strafprozessualen Ermittlungsbefugnisse der Polizei bleiben durch die Regelung unberührt. Da das TDG keine sachliche Zuständigkeit enthält, sind alle Polizei- und Ordnungsbehörden für die Gefahrenabwehr zuständig.

Für Mediendienste ergibt sich die örtliche Zuständigkeit aus § 18 V MDStV. Danach begründet der Geschäftssitz des Anbieters, dessen Wohnsitz oder sein ständiger Aufenthaltsort die örtliche Zuständigkeit. Ist ein solcher Sitz nicht vorhanden, ist die Behörde zuständig, in deren Bezirk der Anlaß für die Amtshandlung liegt. Im Bereich des TDG wird die örtliche Zuständigkeit aus den Polizeigesetzen der Länder oder den allgemeinen Verwaltungsgesetzen entnommen. Für Brandenburg sind die §§ 5 ff. POG BB einschlägig.

Gem. § 7 MDStV müssen Mediendienste der verfassungsmäßigen Ordnung entsprechen. Demnach dürfen sie nicht gegen geltendes Recht verstoßen. Das TDG kennt eine vergleichbare Regelung nicht, sie ist allerdings analog aus hergebrachten juristischen Grundsätzen ableitbar.

Nach der h.M. hat § 5 TDG eine sogenannte Filterfunktion. D.h. daß vor einer strafrechtlichen Prüfung diese Vorschrift anzuwenden ist. M.E. kann diese Filterfunktion nicht auf Adressaten präventivpolizeilicher Maßnahmen angewendet werden.

Demnach ist § 5 TDG auch keine Ermächtigungsgrundlage für gefahrenabwehrende Tätigkeiten. Eine Ermächtigungsgrundlage ist aus den allgemeinen Gesetzen abzuleiten. Demgegenüber enthält § 5 i.V.m. § 18 II und III für den Bereich der Mediendienste eine Eingriffsermächtigung für ordnungsbehördliche Sperranordnungen.

Das TDG muß sich bei der Adressatenregelung auf die Vorschriften der §§ 5 bis 7 PolG BB stützen. Folglich wird zwischen Verhaltensstörern (Content-Provider), Zustandsstörern (Serviceprovider) und nichtverantwortlichen Dritten

(Accessprovider) unterschieden. Im Bereich des MDStV ergibt sich die Adressatenregelung direkt aus § 5 i.V.m. § 18 MDStV. Hier unterscheidet man – wie gehabt – zwischen Content-, Service- und Accessprovider. In beiden Regelungsbereichen (TDG i.V.m. PolG BB und MDStV) ist der Accessprovider durch eine Subsidiaritätsklausel privilegiert. Dem gesetzlichen Willen folgend, sind Anordnungen - wenn möglich - gegen den Content-Provider, als Urheber der Gefahr, zu richten. Besteht aber alternativ die Möglichkeit, auch den Serviceprovider in die Verantwortung zu nehmen, können die zuständigen Behörden kraft eines zugebilligten Auswahlermessens zwischen den Adressaten wählen. Angesichts der Verhältnismäßigkeit sollte eine Maßnahme aber stets zuerst den Content-Provider treffen.

Für das Linken ergeben sich gesonderte Regelungen. Macht sich der Anbieter eines Mediendienstes einen verlinkten Inhalt zu eigen, indem er sich beispielsweise nicht ausreichend vom Inhalt distanziert, ist er als Content-Provider voll verantwortlich. Billigt der Anbieter eines Teledienstes den Zugriff auf rechtswidrige Inhalte oder gestaltet er seine Seite so, daß dem Benutzer nahegelegt wird, auf den rechtswidrigen Inhalt zuzugreifen, wird er Zweckveranlasser und damit verantwortlich.

Der Grundsatz der Verhältnismäßigkeit hat bei Sperranordnungen besondere Bedeutung. Eine Beurteilung muß sich immer an den Gegebenheiten des Einzelfalls ausrichten. § 3 PolG BB enthält den Verhältnismäßigkeitsgrundsatz für Maßnahmen bei Telediensten, § 18 MDStV ist für Mediendienste einschlägig. Eine ordnungsbehördliche Sperranordnung muß insbesondere geeignet, erforderlich und verhältnismäßig im engeren Sinne sein.

11 Schluß

Die Ausführungen haben hoffentlich gezeigt, daß das Medium Internet für die Polizei in vielschichtiger Weise Bedeutung besitzt. Es wurde sicherlich auch deutlich, daß die Rechtslage in den unterschiedlichen Bereichen in ständiger Bewegung ist. Sie muß sich den technischen Entwicklungen anpassen, wenn es nicht zu einem „rechtsfreien Raum - Internet“ kommen soll. Daher sind die Bundesländer gehalten, eng mit dem BKA zusammenzuarbeiten. Auf Dauer wird eine nationale Lösung nicht zu einem vertretbaren Ergebnis führen. Das Internet kennt keine Grenzen. Eine wirksame Bekämpfung der Internetkriminalität kann daher nur durch internationale Zusammenarbeit erreicht werden. Es bleibt zu hoffen, daß EUROPOL in diesem Bereich für die Zukunft eine zentrale Rolle spielen wird.

Doch nicht nur die Rechtslage muß sich den technischen Veränderungen anpassen. Auch die Polizei muß sich weiterhin mit dem Medium Internet beschäftigen. Deshalb ist es von großer Bedeutung, auch schon in der polizeilichen Ausbildung Grundlagen zu diesem Bereich zu vermitteln. Allerdings muß es bei einer Grundlagenvermittlung bleiben, denn die Materie ist so komplex, daß die Polizei nicht auf den Einsatz von Spezialisten verzichten kann. Diese Spezialisten können dann aber nur professionell arbeiten, wenn ihnen auch die entsprechende technische Ausstattung zur Verfügung steht.

Die polizeiliche Forschung im Bereich des Internets muß intensiviert werden. Dabei muß sie eng mit der Praxis zusammenarbeiten. Vor allem im Bereich der Kriminalistik und der Kriminologie bestehen zur Zeit – soweit ersichtlich – noch erhebliche Informationsdefizite. Wissenschaftlich fundierte Lösungsansätze, die sich mit der Internetproblematik beschäftigen, wurden bisher nicht im ausreichenden Maße ausgearbeitet. Will die Polizei „den Zug nicht verpassen“, muß sie ihre Bemühungen in diesem Bereich verstärken.

Es wurde nicht angesprochen, daß für die Polizei auch eigene Nutzungsmöglichkeiten des Internets bestehen. So kann sich die Polizei im Internet präsentieren und in den direkten Kontakt mit dem Internetbenutzer treten. Es ergeben sich dadurch vielseitige Möglichkeiten, Öffentlichkeitsarbeit durchzuführen und polizeiliche Tätigkeiten transparent zu machen.

Da zunehmend die breite Öffentlichkeit das Medium Internet nutzt, ist es möglich, kostengünstig und vor allem sehr schnell (aktuell) und einfach einen großen Teil der Bevölkerung zu erreichen.

Ein weiterer Bereich, der sich für die Strafverfolgungsbehörden ergibt, ist die Nutzung des Internets für Fahndungsmaßnahmen. Die polizeiliche Praxis in den USA zeigt bereits in eindrucksvoller Weise, wie man im Internet Sach- und Personenfahndung durchführen kann. Dabei muß man sich jedoch nicht nur auf die Suche nach Verbrechern beschränken, sondern kann beispielsweise auch Bilder von vermissten Personen veröffentlichen.

Zunehmend hat die Polizei auch die Möglichkeit erkannt, die TCP/IP-Technik für die eigene Kommunikationsinfrastruktur zu nutzen. So können behördliche LANs oder überregionale Extranets auf der Internettechnik aufbauen. Die Technik bietet den Behörden alle Funktionen, die sie benötigen (z.B. E-Mail für die Behördenpost, WWW für Veröffentlichungen).

Ich hoffe, daß meine Ausführungen einen Beitrag dazu geleistet haben, das Thema „Polizei und Internet“ näher in den Blickpunkt der Polizeiwissenschaften zu rücken. Ferner hoffe ich, auch der polizeilichen Praxis ein Stück theoretisches Grundlagenwissen vermittelt zu haben. Ich würde mich über konstruktive Kritik, Anmerkungen und Verbesserungswünsche im Rahmen einer wissenschaftlichen Diskussion freuen.

12 Anlagen

12.1 Anlage 1 – Liste wichtiger Institutionen für das Internet

Organisation	Funktion	URL
DE-NIC (Deutsches Network Information Center)	Vergabestelle für Domain-Namen unterhalb der Top-Level-Domain .de	http://www.denic.de/ [06.08.2000]
ICANN (Internet Corporation for Assigned Numbers and Names)	Nachfolger der InterNIC	http://www.icann.net/ [06.08.2000]
InterNIC (International Network Information Center)	Kollaboratives Projekt zwischen AT&T, General Atomics und Network Solutions, Inc. AT&T. Internationale Vergabestelle für Domain-Namen	http://www.internic.net/ [06.08.2000]
gTLD-MoU (Generic Top Level Domain Memorandum of Understanding)	Organisation für die Schaffung von neuen Top-Level-Domains	http://www.gtld-mou.org/ [06.08.2000]
IAB (Internet Architecture Board)	Organisation zur Dokumentation der Netzstruktur und der grundsätzlichen Abläufe im Internet	http://www.isi.edu/iab/ [06.08.2000]
IANA (Internet Assigned Numbers Authority)	Zentrale Koordinationsstelle für Internet-Protokolle	http://www.isi.edu/iana/ [06.08.2000]

IETF (Internet Engineering Task Force)	Internationale Gemeinschaft von kommerziellen und nichtkommerziellen Aktiven im Internet mit dem Ziel, technische Standards im Internet vorzuschlagen	http://www.ietf.org/ [06.08.2000]
ISOC (Internet Society)	Internationale Organisation für die Kooperation und Koordination von Technologien und Anwendungen im Internet	http://www.isoc.org/ [06.08.2000]
W3-Konsortium	Organisation, die speziell die Weiterentwicklung technischer Standards des World Wide Web koordiniert, etwa HTML oder das HTTP-Protokoll	http://www.w3.org/ [06.08.2000]

Tabelle 17: Liste wichtiger Institutionen für das Internet[438]

[438] Für nähere Informationen vgl.: Alpar, Kommerzielle Nutzung des Internet, Seite 36 – 37.

12.2 Anlage 2 – Die Zukunft des mobilen Datenfunks (Stand 1999)

Verfahren	Zeitrahmen	Merkmale	Bemerkungen
9,6 KBit/s	vorhanden	leitungsorientiert	
14,4 KBit/s	Ende 1999	leitungsorientiert, höhere Geschwindigkeiten auf Kosten der Fehlerkorrektur FEC	V.42bis-Kompression möglich
Direct IP Access	teilweise verfügbar	leitungsorientierte Verbindung direkt ins Internet	Verbindungsaufbau schneller, Grundlage für den paketorientierten Zugang
HSCSD	ab Ende 1999	Kanalbündelung von je 9,6 oder 14,4 KBit/s	nur ein Software-Upgrade
GPRS	ab Ende 1999	paketorientiert, Spitzenraten bis zu 115,2 KBit/s	besonders gut für die mobile Datenkommunikation geeignet
EDGE	ab 2000	paketorientiert, bis zu dreimal so schnell wie GPRS	geplanter Endausbau für vorhandene GSM-Netze
UMTS	ab 2001	bis zu 2 MBit/s	komplett neue Funktechnik

Tabelle 18: Zeitplan für die Entwicklung von mobilen Datenfunknetzen (Stand 1999) [439]

[439] Zivadinovic, Drahtlos anknüpfen, Seite 186

12.3 Anlage 3 – LIST Kommando des Listservers

Kommando	Erläuterung
LIST	liefert eine Liste mit Titel und Kurzbeschreibung der lokal durch den angeschriebenen Listserver verwalteten Diskussionsgruppen
LIST GLOBAL	liefert die Liste aller weltweit existierenden Diskussionsgruppen
LIST /STICHWORT oder LISTGLOBAL /STICHWORT	liefert eine (weltweite) Liste aller Diskussionsgruppen, die zu einem eingegebenen Stichwort existieren
SUBSCRIBE „Newsgroup“ „Name“ „Vorname“	Beitreten der Newsgroup „Newsgroup“
SIGNOFF „Newsgroup“	Austreten aus der Newsgroup „Newsgroup“
INFO	allgemeine Beschreibung der Listserver-Kommandos
HELP	Anforderung eines allgemeinen Hilfedokuments
INDEX	Auflistung aller Archivdateien
GET „Newsgroup“ „Datei“	Abrufen der Archivdatei „Archivdatei“
REVIEW	liefert Informationen zu einer Newsgroup
STATS	Beitragsstatistik

Tabelle 19: LIST Kommando des Listservers[440]

[440] Alpar, Kommerzielle Nutzung des Internet, Seite 60 und 63

12.4 Anlage 4 – Einige Smiles und Abkürzungen im IRC

Smile / Abkürzung	Bedeutung
:-o	Quatschkopf
:-(	traurig
:-<	sehr traurig
:-x	Kuß-Smile
:-)	Humor
(-:	Linkshänder
:-#	Ich sage nichts
:-s	Verstehe ich nicht
:-D	Ich spreche zuviel
=:-)	Punker
:-/	unentschlossen
(:-&	ängstlich
(-)	muß zum Friseur
:-@	Schrei
:-7	gequältes Lächeln
:-)8	User trägt Fliege
.-)	User ist einäugig
:-*	Oops!
lach	User lacht
grins	User grinst
MfG	Mit freundlichen Grüßen

Tabelle 20: Smiles und Abkürzungen im IRC

12.5 Anlage 5 - Ausgewählte indizierungsfähige Medien der BPS

- alle Printmedien, z.B. Bücher, Zeitschriften, Magazine, Broschüren, Flugblätter, Comics u.a.
- Schallplatten und -hüllen, CDs und Tonkassetten
- Computerspiele
- Spiele (vor allem bestimmte Brettspiele, die durch ihren Verlauf beispielsweise den Krieg oder nationalsozialistische Gewalttaten verherrlichen oder verharmlosen)
- Videofilme, soweit sie von der freiwilligen Selbstkontrolle der Filmwirtschaft (FSK) kein Freigabezeichen erhalten haben und wenn sie mit „nicht freigegeben unter 18 Jahren“ gekennzeichnet wurden

Tabelle 21: Ausgewählte indizierungsfähige Medien der BPS[441]

[441] Vgl. auch: Sohne, Pornographie, Seite 18.

13 Verzeichnisse

13.1 Abbildungsverzeichnis

Abbildung 1: Das ARPANet im Dezember 1969.....32
Abbildung 2: Das ARPANet im September 1971.....36
Abbildung 3: Das ARPANet im Juli 1977 42
Abbildung 4: Systematischer Aufbau einer Domain-Adresse 53
Abbildung 5: Vielfalt einer Client-Server-Architektur.....56
Abbildung 6: Der Uniform Resource Locator (URL) 102
Abbildung 7: Zusammenhang „Browser – WWW – Internet“.....107

13.2 Tabellenverzeichnis

Tabelle 1: Klassifizierungsschema für Netztypen 51
Tabelle 2: Beispiele für TLDs 54
Tabelle 3: Internetdienste und ihre TCP-Portnummern 72
Tabelle 4: Ausgewählte Bestandteile eines E-Mail Headers 75
Tabelle 5: MIME-Headerfelder 76
Tabelle 6: Mögliche Einträge für das Headerfeld „content-type“ 77
Tabelle 7: Hauptthemen der Usenet Newsgroups 84
Tabelle 8: Zusätzliche E-Mail-Headerfelder eines Usenet Newsgroup Artikels 85
Tabelle 9: Suchmodi in Archie 89
Tabelle 10: Ablauf einer HTTP-Operation 100
Tabelle 11: URL-Aufbau der wichtigsten Dienste des Internets 103
Tabelle 12: Hyper-G und WWW im Vergleich 113
Tabelle 13: Mögliche Auswirkungen von Pornographie-Konsum 117
Tabelle 14: Die Täter/Täterinnen im Bereich des Kindesmißbrauchs und der Kinderpornographie und ihre Vorgehensweisen 123
Tabelle 15: Erkenntnisse über Opfer von Kinderpornographie und Kindesmißbrauch 124
Tabelle 16: Jargon der Kinderporno-Szene 129
Tabelle 17: Liste wichtiger Institutionen für das Internet 240
Tabelle 18: Zeitplan für die Entwicklung von mobilen Datenfunknetzen (Stand 1999) 241
Tabelle 19: LIST Kommando des Listservers 242
Tabelle 20: Smiles und Abkürzungen im IRC 243
Tabelle 21: Ausgewählte indizierungsfähige Medien der BPS 244

13.3 Literaturverzeichnis

Alpar, Paul	„Kommerzielle Nutzung des Internet: Unterstützung von Marketing, Produktion, Logistik und Querschnittsfunktionen durch das Internet und kommerzielle Online-Dienste“, Berlin, Springer-Verlag, 1996
Bär, Wolfgang	„EDV-Beweissicherung im Strafverfahrensrecht : Änderungen durch das BegleitG zum TKG“, CR 7/1998, Seite 434 bis 439
Bergel, Mario / Bley, Torsten / Dublies, Thomas / Kleinschmidt, Helmut / Redlich, Stefan / Rogge, Ingo	„Seminar Kinderpornographie – Ratsanwärterlehrgang 1998/2000 - Seminarband“, Landespolizeischule Berlin und Fachhochschule der Polizei des Landes Brandenburg (Hrsg.)
Berger-Zehnpfund, Petra	„Kinderpornographie im Internet : Rechtliche Aspekte der Bekämpfung des Kindesmißbrauchs in internationalen Datennetzen“, Kriminalistik 10/1996, Seite 635 bis 639
Bettinger, Torsten	„Abschlußbericht der WIPO zum Internet Domain Name Process“, CR 7/1999, Seite 445 bis 448
Bettinger, Torsten Freytag, Stefan	„Privatrechtliche Verantwortlichkeit für Links“ : Zugleich Anmerkung zum Urteil des LG Hamburg vom 12.05.1998, CR 9/1998, Seite 545 bis 556

Bleich, Holger — „Selbstverdunkelung: Anonymes Mailen in der Praxis“, c´t 16/2000, Seite 156 bis 159

Conradi, Ulrich/ Schlömer, Uwe — „Die Strafbarkeit der Internet-Provider“, NStZ 8/1996, Seite 366 bis 369 und NStZ 10/1999, Seite 472 bis 477

Dierstein, Rüdiger — „Gefahren für die Datenverarbeitung : Programm-Manipulationen – Computerviren und deren Bekämpfung“; Kriminalistik 8-9/1989, Seite 489 bis 516

Drewes, Detlef — „Die Kindersexmafia und ihre unsichtbaren Kanäle“, abgedruckt in: Gallwitz / Manske-Herlyn, Kinderpornographie

Eichler, Alexander — „Bekämpfung der Kriminalität im Internet : Tagung beim BKA am 14./15.12.1998 mit Anmerkungen“, CR 3/1999, Seite 200 bis 204

Ermert, Monika — „Namenspatron : Die neue Internet-Domain-Verwaltung ist endgültig geklärt“, c´t 24/99, Seite 48 ff.

Enders, Ursula — „Die Strategie der Täter – Pornographie mit Mädchen und Jungen – Mißbrauch in Institutionen“, abgedruckt in: Gallwitz / Manske-Herlyn, Kinderpornographie

Endres, Johannes — „DSL – Die Schnelle Leitung : Die Technik hinter T-DSL“, c´t 16/99, Seite 126 ff.

Federrath, Hannes/ Berthold, Oliver/ Köhntopp, Marit/ Köpsell, Stefan — „Tarnkappen fürs Internet: Verfahren zur anonymen und unbeobachtbaren Kommunikation“, c´t 16/2000, Seite 148 bis 155

Felixberger, Stefan — „Staatliche Überwachung der Telekommunikation : Anwendungsbereich und Befugnispalette des Begleitgesetzes zum TKG“, CR 3/1998, Seite 143 bis 147

Fink, Reinhard — „Mailboxen optimal nutzen – das komplette Wissen für die routinierte Anwendung von Mailbox-Netzen“, Franzis-Verlag GmbH, 1995

Fink, Reinhard — „Die Welt von T-Online – Führer durch den größten deutschen Online-Dienst“, 1. Auflage, Bonn, Internat. Thomson Publ., 1996

Flechsig, Norbert/ Gabel, Detlev — „Strafrechtliche Verantwortlichkeit im Netz durch Einrichten und Vorhalten von Hyperlinks“, CR 6/1998, Seite 351 bis 358

Freundt, Mirco — „Das Internet : multimedialer Freiraum oder modernes Handwerkszeug der Polizei“, Standort: Bibliothek der Fachhochschule der Polizei des Landes Brandenburg

Gallwitz, Adolf — „Kinderpornographie ist sexueller Übergriff und Mißbrauch in der Praxis“, abgedruckt in: Gallwitz / Manske-Herlyn, Kinderpornographie

Gallwitz, Adolf/ Manske-Herlyn, Bernhild — „Kinderpornographie : Entwicklung von Gegenstrategien zur Verbesserung der Situation betroffener Kinder“, Bernhild Manske-Herlyn (Hrsg.), Schriftenreihe der Fachhochschule Villingen-Schwenningen Texte Nr. 24, 1999

Goldmann, Günter — „Computerkriminalität und ihre Bekämpfung“, Kriminalistik 8-9/1989, Seite 442 bis 451

Goldmann, Günter/ Stenger, Hans-Jürgen — „Die ganze Welt als Tatort“, Kriminalistik 8-9/1989, Seite 464 bis 478

Harbort, Stephan — „Verbrechen im Cyberspace : Neue Erscheinungsformen zeitspezifischer Computerkriminalität“, Kriminalistik 3/1996, Seite 194 bis 196

Hartung, Thomas — „Internet“, dp-special April 1998, Seite 2 –15

Hafner, Kati/ Lyon, Matthew — „Arpa Kadabra oder die Geschichte des Internet“, [Übersetzung von Gabriele Herbst], 2. Auflage, Heidelberg, dpunkt-Verlag, 2000, orig. Titel: Where wizards stay up late

Heinzmann, Peter/ Ochsenbein, Andreas — „Strafrechtliche Aspekte des Internet : Technische und rechtliche Grundlagen“, Kriminalistik 7/1998, Seite 513 bis 520, Kriminalistik 8-9/1998, Seite 599 bis 606

Jaeger, Stefan — „Computerkriminalität“, 2. Auflage, Augsburg, Interest-Verlag, 1998

Janovsky, Thomas — „Internet und Verbrechen : Die virtuelle Komponente der Kriminalität“; Kriminalistik 7/1998, Seite 500 bis 504

Jofer, Robert — „Strafverfolgung im Internet : Phänomenologie und Bekämpfung kriminellen Verhaltens in internationalen Computernetzen“, Frankfurt am Main, Europäische Hochschulschriften : Reihe 2, Rechtswissenschaften ; Bd. 2555

Kleinknecht, Theodor/ Meyer-Goßner, Lutz — „Strafprozeßordnung, Gerichtsverfassungsgesetz, Nebengesetze und ergänzende Bestimmungen“, 44. Auflage, München, Beck, 1999

König, Christian/ Lötz, Sascha — „Sperrungsanordnungen gegenüber Network- und Accessprovidern“, CR 7/1999, Seite 438 bis 445

Kossel, Axel — „Netzgespräche : Internet-Telefonie in der Praxis“, c´t 10/99, Seite 230 ff.

Kreitzberg, Rolf — „Kunstgriffe und Machenschaften“, Kriminalistik 8-9/1989, S. 453 bis 458

Krempel, Stefan — „Generalüberholung für das Internet : Virtuelles Roundtable-Gespräch zum Status von IPv6“, c´t 20/99, Seite 212 ff.

Kube, Edwin — „Technische Entwicklung und neue Kriminalitätsformen : Was geschieht, was droht“, Kriminalistik 10/1996, Seite 618 ff.

Kuri, Jürgen — „Canned Heat : Die neue Internet-Verwaltung nimmt Gestalt an“, c´t 5/99, Seite 32 ff.

Kuri, Jürgen — „Das globale Netz : Bandbreite satt und neue Zugangsmöglichkeiten für öffentliche Netze, c´t 7/99, Seite 51 ff.

Kuri, Jürgen — „Das vernetzte Haus : Von der automatischen Lichtregelung zum intelligenten Haus“, c´t 22/99, Seite 178 ff.

Kuri , Jürgen — „Sprache im Päckchen : Telefonieren über TCP/IP: Spielerei oder Zukunftstechnik?“, c´t 10/99, Seite 220 ff.

Kuri, Jürgen/ Wiedenhoff, Chris/ Gieselmann, Hartmut — „Virtuelle Zockerrrunden : Multiplayer-Spiele: Das Ende der Einsamkeit“, c´t 2/00, Seite 100 ff.

Laschet, Reiner — „Kinderpornographie – Entstehung, Vertrieb und Bekämpfungsstrategien. Eine aktuelle Bestandsaufnahme aus kriminalpolizeilicher Sicht.“, abgedruckt in: Gallwitz / Manske-Herlyn, Kinderpornographie

Leiberich, Otto — „Verschlüsselung und Kriminalität : Die Behinderung der Kriminalitätsbekämpfung durch Codierungen“, Kriminalistik 11/1995, Seite 731 bis 734

Luckhardt, Norbert — „Das Netz ist immer und überall : IBMs Visionen für die nächste Generation des Internet“, c´t 25/99, Seite 98 ff.

Manske-Herlyn, Bernhild — „Gegenstrategien gegen Pornographie mit Jungen und Mädchen“, abgedruckt in: Gallwitz / Manske-Herlyn, Kinderpornographie

Nemes, Andreas/ Greiner, Wolfgang — „Die Suche nach elektronisch gespeicherten Beweismitteln : Besondere Probleme bei der Durchsuchung und Beschlagnahme“, Kriminalistik 2/1999, Seite 115 bis 119

Neuberger, Christoph/ Tonnemacher, Jan — „Online – Die Zukunft der Zeitung? : Das Engagement deutscher Tageszeitungen im Internet“, Opladen/Wiesbaden, Westdeutscher Verlag, 1999

Ochsenbein, Andreas — „Strafrechtliche Aspekte des Internet : Lösungen und Möglichkeiten“, Kriminalistik 10/1998, Seite 685 bis 688

Paul, Werner — „Ein rundrum erfreuliches Berufsbild : Der polizeiliche EDV-Sachverständige / Eine Problemanalyse“, Kriminalistik 8-9/1989, Seite 521 bis 526

Paulus, Manfred — „Sexuelle Gewalt gegen Kinder und Kinderpornographie“, abgedruckt in: Gallwitz / Manske-Herlyn, Kinderpornographie

Ramm, Frederik — „Recherchieren und Publizieren im World Wide Web“, 2. Auflage, Braunschweig/Wiesbaden, Verlag Vieweg, 1996

Sieber, Ulrich — „Internationales Strafrecht im Internet : Das Territorialitätsprinzip der §§ 3, 9 StGB im globalen Cyberspace“, NJW 29/1999, Seite 2065 bis 2073

Sohne, Frederike — „Pornographie : Anleitung zur sexuellen Gewalt?“, Hamburg, Verlag Dr. Kovač, 1995

Steinke, Wolfgang — „Entwicklung der Computerkriminalität : Ein Bericht, der keinen Anlaß zur Besorgnis gibt“, Kriminalistik 2/1991, Seite 131 f.

Steyer, Ralph — „HTML 4 : Homepage-Design und Web-Publishing“, 1. Auflage, Düsseldorf, Verlag Data Becker, 1998

Tegtmeyer, Henning — „Polizeigesetz Nordrhein-Westfalen“, 8. Auflage, Stuttgart, Boorgerg, 1995

Tröndle, Herbert/ Fischer, Thomas — „Strafgesetzbuch und Nebengesetze“, 49. Auflage, München, Beck, 1999

Vahle, J. — „Schaubilder zum Polizeirecht“, Kriminalistik 2/2000, Seite 137 bis 139

Vassilaki, Irini „Strafrechtliche Verantwortlichkeit durch Einrichten und Aufrechterhalten von elektronischen Verweisen (Hyperlinks) : Anwendbarkeit der allgemeinen Strafrechtsdogmatik auf neue Verhaltensformen“, CR 2/1999, Seite 85 bis 93

Weitemeier, Ingmar „Internet – Medium der Zukunft : Über die Kommunikationsfreiheit ohne Grenzen und die Möglichkeit kriminellen Mißbrauchs“, Kriminalistik 6/1996, Seite 401 bis 405

Zimmermann, Andreas „Polizeiliche Gefahrenabwehr und das Internet“, NJW 43/1999, Seite 3145 bis 3152

Zivadinovic, Dusan „Drahtlos anknüpfen : GPRS: schneller mobil surfen“, c´t 7/99, Seite 186 ff.

Zivadinovic, Dusan „Drahtloses Internet“, c´t 4/99, Seite 30 ff.

Zivadinovic, Dusan „Schneller Surfen : Fast Internet mit und ohne Draht“, c´t 7/99, Seite 44 ff.

14 Index

§§

§ 10 [Allgemeine Befugnisse, Begriffsbestimmung] PolG BB 223

§ 10 [Strafvorschriften] HalbleiterschutzG..... 183

§ 100 a [Voraussetzungen der Überwachung des Fernmeldeverkehrs] StPO 207

§ 102 [Durchsuchung beim Verdächtigen] StPO202, 207

§ 103 [Durchsuchung bei anderen Personen] StPO 202, 207

§ 11 [Personen und Sachbegriffe] III StGB 116

§ 11 [Personen- und Sachbegriffe] StGB..... 175

§ 11 III StGB 116

§ 110 [Durchsicht von Papieren] StPO..... 204

§ 110 a [Verdeckte Ermittler] StPO 207

§ 111 [Falsche Namensangabe] OWiG 201

§ 111 [Öffentliche Aufforderung zu Straftaten] StGB 181

§ 111 b [Sicherstellung] StPO 205

§ 111 c [Beschlagnahme zur Sicherstellung] StPO 205

§ 12 [Zusammentreffen mehrerer Gerichtsstände] StPO..... 196

§ 126 [Störung des öffentlichen Friedens durch Androhung von Straftaten] StGB..... 181

§ 13 [Begehen durch Unterlassen] StGB 163

§ 130 [Volksverhetzung] StGB..... 181

§ 130 a [Anleitung zu Straftaten] StGB..... 181

§ 131 [Gewaltdarstellung] StGB.....116, 182

§ 136 I [Erste Vernehmung] StPO 201

§ 138 [Nichtanzeige geplanter Straftaten] StGB 188

§ 139 I [Straflosigkeit der Nichtanzeige geplanter Straftaten] StGB..... 188

§ 14 [Bußgeldvorschriften] AdVermiG 183

§ 140 [Belohnung und Billigung von Straftaten] StGB 182

§ 143 I [Örtliche Zuständigkeit] GVG..... 196

§ 15 [Widerruf der Lizenz] TKG 170

§ 152 I,II [Hilfsbeamte der Staatsanwaltschaft] GVG 196

§ 153 c [Nichtverfolgung von Auslandstaten] StPO 162

§ 160 [Ermittlungsverfahren] StPO 196

§ 163 [Aufgaben der Polizei] StPO 196

§ 166 [Beschimpfung von Bekenntnissen, Religionsgesellschaften und Weltanschauungsvereinigungen] StGB.....182

§ 17 [Verbotsirrtum] StGB 161

§ 17 [Verrat von Geschäfts- oder Betriebsgeheimnissen] UWG 183

§ 18 [Aufsicht] MDStV 219

§ 184 [Verbreitung pornographischer Schriften] StGB..... 116, 181, 185

§ 184 III StGB.....143

§ 185 [Beleidigung] StGB 182

§ 186 [Üble Nachrede] StGB 182

§ 187 [Verleumdung] StGB 182

§ 188 [Üble Nachrede und Verleumdung gegen Personen des politischen Lebens] StGB.....182

§ 189 [Verunglimpfung des Andenkens Verstorbener] StGB 182

§ 2 [Geltungsbereich] TDG 166

§ 2 I [Geltungsbereich] MDStV 218

§ 2 I [Geltungsbereich] TDG 218

§ 20 [Handlungen eines unzuständigen Gerichts] StPO 197

§ 201 [Verletzung der Vertraulichkeit des Wortes] StGB.....182

§ 202 [Verletzung des Briefgeheimnisses] StGB 191

§ 202 a [Ausspähen von Daten] StGB 182, 187, 192

§ 203 [Verletzung von Privatgeheimnissen] StGB 183

§ 21 [Jugendschutzbereich] III GjSM.....178

§ 21 [Strafvorschriften] GjSM 181

§ 22 KunstUrhG.....188

§ 23 [Öffentliche Aufforderung zur Teilnahme an verbotener Versammlung] VersG 182
§ 25 [Täterschaft] StGB 172
§ 25 II StGB 175
§ 269 [Fälschung beweiserheblicher Daten] StGB 182
§ 27 [Beihilfe] StGB 172
§ 270 [Täuschung im Rechtsverkehr bei Datenverarbeitung] StGB 182
§ 271 [Mittelbare Falschbeurkundung] StGB 182
§ 274 [Urkundenunterdrückung; Veränderung einer Grenzbezeichnung] StGB 182
§ 284 [Unerlaubte Veranstaltung eines Glücksspiels] StGB 183
§ 29 [Anzeigepflicht, Neuzulassung] ArzneimittelG 183
§ 3 [Begriffsbestimmungen] TDG 166
§ 3 [Geltung für Inlandstaten] StGB 155
§ 3 [Grundsatz der Verhältnismäßigkeit] PolG BB 228
§ 30 II [Versuch der Beteiligung] StGB 182
§ 303 a [Datenveränderung] StGB 182, 191
§ 303 b [Computersabotage] StGB 182
§ 303 b I Nr.2 [Computersabotage] StGB 193
§ 348 [Falschbeurkundung im Amt] StGB 182
§ 353 b [Verletzung des Dienstgeheimnisses und einer besonderen Geheimhaltungspflicht] StGB 182
§ 353 d [Verbotene Mitteilungen über Gerichtsverhandlungen] StGB 182
§ 37 [Verbotene Gegenstände] WaffG 183
§ 4 [Geltung für Taten auf deutschen Schiffen und Luftfahrzeugen] StGB 155
§ 4 [Strafvorschriften für irreführende Werbung] UWG 183
§ 4 [Zugangsfreiheit] TDG 167
§ 4 IV [Datenschutzrechtliche Pflichten des Diensteanbieters] TDDSG 194
§ 43 [Strafvorschriften] BDSG 183
§ 5 [Auslandstaten gegen inländische Rechtsgüter] StGB 155
§ 5 [Örtliche Zuständigkeit] POG BB 221
§ 5 [Verantwortlichkeit] TDG 167
§ 52 [Zeugnisverweigerungsrechte aus persönlichen Gründen] StPO 200
§ 53 [Zeugnisverweigerungsrechte aus beruflichen Gründen] StPO 200
§ 55 [Auskunftsverweigerungsrecht] StPO 200
§ 6 [Anbieterkennzeichnung] TDG 174
§ 6 [Auslandstaten gegen international geschützte Rechtsgüter] StGB 155
§ 6 [Verantwortlichkeit für den Zustand von Sachen und Tieren] PolG BB 224
§ 6 c [Progressive Kundenwerbung] UWG 183
§ 6 GjSM 178
§ 7 [Geltung für Auslandstaten in anderen Fällen] StGB 155
§ 7 [Gerichtsstand des Tatortes] StPO 196
§ 7 [Inanspruchnahme nicht verantwortlicher Personen] PolG BB 225
§ 7 I [Inhalte, Sorgfaltspflichten, Meinungsumfragen] MDStV 221
§ 70 [Entschädigungsansprüche] PolG BB 226
§ 74 [Voraussetzungen der Einziehung] StGB ... 205
§ 8 [Gerichtsstand des Wohnsitzes oder Aufenthaltsortes] StPO 196
§ 86 [Verbreitung von Propagandamitteln verfassungswidriger Organisationen] StGB ... 181
§ 86 [Verwenden von Kennzeichen verfassungswidriger Organisationen] StGB ... 183
§ 86 a [Verwenden von Kennzeichen verfassungswidriger Organisationen] StGB ... 181
§ 86 I [Verbreiten von Propagandamitteln verfassungswidriger Organisationen] StGB ... 160
§ 9 [Gerichtsstand des Ergreifungsortes] StPO .. 196
§ 9 [Ort der Tat] StGB 155
§ 94 [Gegenstand der Beschlagnahme] StPO 200, 205
§ 95 [Herausgabepflicht] StPO 200, 205
§ 97 [Beschlagnahmefreie Gegenstände] StPO .. 213
§ 99 [Postbeschlagnahme] StPO 213

3D-Shooter ... 96

A

AberMUD ... 95
abstrakte Gefährdungsdelikte ... 158, 165
Accessprovider ... 168
Adressbereich ... 63
ADSL ... 64, 111
Advanced Research Projects Agency ... *Siehe* ARPA
AG Kripo ... 231
Alias ... 52
ALOHANet ... 39
alt 84
American Standard Code of Information Interchange ... 73
Archie ... 88
arpa ... *Siehe* TLD
ARPA ... 18, 20
ARPA-Internet ... 43
ARPANet ... 45, 46
Art 5 II GG ... 172
Art. 21 II [Parteien] GG ... 184
Art. 296 EGStGB ... 160
Art. 4 Nr. 1 IuKDG ... 176
Art. 9 I [Vereinigungsfreiheit, Verbot von Maßnahmen gegen Arbeitskämpfe] GG ... 184
ASCII ... 73, 98
Asymetric Digital Subscriber Line ... 111
AT&T ... 23, 43
Attachments ... 75
Avatar ... 94

B

Backbone ... 45
Basisprotokoll ... 49
Baumstruktur ... 84
BBN ... 29
bcc ... 75
Because It´s Time Network ... *Siehe* BITNet
Beschlagnahme ... 204, 212
Beugehaft ... 170
Bildschirmtext ... 66
bionet ... 84
bit 84
BITNet ... 44
biz ... 84
BKA ... 131, 230
body ... 73
Body ... 84
Bolt Beranek and Newman ... *Siehe* BBN
BPS ... 116
Browser ... 99, 105
BtM-Handel ... 140
Btx ... 65, 66, 118
Bundesprüfstelle für jugendgefährdende Schriften ... 116

C

California Educational Research Network ... *Siehe* CERFNet
CATENet ... 40, 43
cc 75
ccTLDs ... 53 *Siehe* DNS
CDNet ... 45
CEPT-Standard ... 68
CERFNet ... 45
CERN ... 96
CGI ... 98, 105
Channel ... 92
Charles F. Goldfarb ... 98
chatten ... 92
Chiffreanzeigen ... 127
Clearinghouse for Networked Information Discovery and Retrieval ... 90
Client ... 62
Client-Server-Architektur ... 55
CNIDR ... 90
com ... *Siehe* TLD
comp ... 84
Computer Science Research Network ... *Siehe* CSNet

Computerkriminalität 131
Computerviren 140
Computerwürmer 140
Concatenated Network ..... *Siehe* CATENet
content-description 76
content-id 76
Content-Provider 167, 223
content-transfer-encoding 76
content-type 76
Cookies 194
Cooperation for an Open Systems Interconnection Networking in Europe ..... *Siehe* COSINE
COSINE 47
country code Top Level Domains ..... *Siehe* ccTLDs
Cracker 138
Crowther 95
CSNet 43, 44, 46
Cyberspace 38
Cyclades 40, 47

D

DARPA 39
date 75
Dateitransfer 31
Datex-J/Btx 67
Datex-P-Netz 64, 67
Dazing 139
DCA 26, 43
DCC 147
de 84
Defense Advanced Research Projects Agency. *Siehe* DARPA
Denial-of-Service-Attacks 139
DE-NIC 54, 60
Deutsche Forschungsnetz ..... *Siehe* DFN
Deutsche Network Information Center 60
Deutsches Network Information Center ... *Siehe* DE-NIC
DFN 47
Digitale IDs 78
DikuMUD 95
direct client to client 147
Directory-of-Servers 91
Diskussionsgruppen 80
distribution 85
DNS 45, 52, 59
Domain Name System ..... *Siehe* DNS
Domain-Grabbing 55
DoS 139
download 87
Dungeons und Dragons 38
Dunkelfeld 121, 137
Durchsuchung 202

E

EARN 46
Ebone 47
edu ..... *Siehe* TLD
EDV 131
Eingeschränkter Verfolgungszwang 162
Einport-Mailboxen 69
Elektronische Post 72
E-Mail 37, 72, 103, 139, 191, 213
E-Mail-Account 77
E-Mail-Verteilerlisten 80, 81
Erfolgsort 157
Ersatzvornahme 170
Ethernet 45, 66
EUNet 46
Europäischer Internet-Backbone ..... *Siehe* Ebone
EuropaNET 47
Exclude-Filter 178, 180
Extremismus 142

F

Fedida 66
fido 84
Fido 70
File Transfer Protocol 87
Filterprogramm 178

Finger-Befehl 39
FKK-Hefte 120
Flash 98
FreeMail 77
FreeMailer 187
from 75
FTP 35, 72, 86, 102, 145
FTP-Client 87
FTPMailer 87

G

Garantenstellung 163
Gateway 40, 57
Gefahrenabwehr 217
General Packet Radio Services 110
Generalklausel 223
generic Top Level Domains ..... *Siehe* gTLD
generic Top Level Domains – Memorandum of Understanding 60
Gesetz über die Verbreitung jugendgefährdender Schriften 116
Gesetz zur digitalen Signatur 166
Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste ... 166
GjSM 116
Gopher 72, 89, 102
gov ..... *Siehe* TLD
GPRS 110
Grundsatz der Verhältnismäßigkeit 228
GSM-Netz 69
gTLD-MoU 60
gTLDs ..... 53 *Siehe* DNS

H

Hacker 138, 144, 195
Hacking 138
Haftungsprivilegierung 222
Handlungsort 157
Handshake 31
header 73
Header 37, 84
Headerfelder 74, 85
Hehlerei 140
Hellfeld 137
Helper Application 101
High Speed Circuit Switched Data 110
Hoheitsgebiet 156
home videos 121
Homepage 176
Honeywell 316 34
Honeywell 516 34
Honeywell-516 29
Host 33, 62
Hostnummer ..... *Siehe* IP
HSCSD 110
HTML 97, 98
HTTP 98, 99
Hyper-G 112
Hyperlinks 226
Hypertext 99
Hypertext Markup Language 98
Hypertext Transfer Protocol 99

I

Ibertex 67
IBM 44
ICANN 60
ICCC 35
IKPO 232
IMAP 73
IMP 28, 29, 31
Index jugendgefährdender Schriften 116
Ingerenz 164
Innenministerkonferenz 232
Interactive Mail Access Protocol 73
Interface Message Processors ..... *Siehe* IMP
International Network Working Group . *Siehe* INWG
International Telecommunications Union 60
Internet 47
INTERNET 43

Internet Corporation for Assigned Numbers and Names 60
Internet Network Information Center 60
Internet Phone 93
Internet Protocol ..... *Siehe* IP
Internet Relay Chat 65, 92
InterNIC 60
INWG 35, 40
IP 39, 43, 49, 50, 52
IP-Adresse ..... 59, 63 *Siehe* IP
Iphone 93, 149
Iphone-Client 93
Iphone-Server 93
IPTO 20, 22
IPv4 109
IPv6 109
IRC 65, 92, 128, 147, 190
IRC-Client 92
IRC-Server 92
ISDN 63, 111
ISO 46
ITU 60, 112
IuKDG 165

J

Java 98
JavaScript 98
Junk-E-Mails 142
Junk-Mail 193

K

Kalte Krieg 18
keywords 85
Kinderpornographie 119, 185
KIT-Standard 68
Klasse-A-Netz ..... *Siehe* IP
Klasse-B-Netz ..... *Siehe* IP
Klasse-C-Netz ..... *Siehe* IP
Kommunikationsgesellschaft 158
Kontrolldelikte 137

L

LAN 45, 66
Legalitätsprinzip 162
lines 85
Links 99, 173
Listserver 80, 81
local area network 66
Local Area Network ..... *Siehe* LAN
Local-Level-Domain ..... *Siehe* DNS
login 31
Lolita 129
LPMUD 95
Luxtel 67

M

MAC-Adresse 110
Mail-Bombing 141, 193
Mailbox 118
Mailboxen 206
Mailboxnetze 66, 69
Mail-Client 72
Mailingliste 37
Marc Andreessen 105
Masochismus 185
maus 84
Maus 70
MDStV 165, 218
MDStVDurchfG BB 219
Mediendienst 165, 218
Mehrport-Mailboxen 69
Message Service Group ..... *Siehe* MsgGroup
message-id 75
META-Tags 154
Metcalf 66
mil ..... *Siehe* TLD
MILNet 45, 46
MIME 76, 99
mime-version 76
misc 84

Modem 63
MOG 95
Monitoring 138
Mosaic-Browser 105
MSG 37
MsgGroup 37
MUD 95
Multiplayer-Online-Games 95
Multiple User Dialog 95
Multiple User Dimension 95
Multiple User Dungeon 95
Multipurpose Internet Mail Extension 76

N

NASA 20, 44
National Science Foundation ..... 60 *Siehe* NSF
NCC 33
NCP 33, 45
nemo tenetur se ipsum accusare 201
net ..... *Siehe* TLD
Network Control Center ..... *Siehe* NCC
Network Information Center ..... *Siehe* NIC
Network Measurement Center 27, 28, 30
Network News Transport Protocol 83
Network Solutions Inc 60
Network Virtual Terminal 85
Network Working Group ..... *Siehe* NWG
Netzmodell 24
Netzspezifische Verbreitungsdelikte 133
Netzwerk 24
Netzwerkknoten 24
Netzwerknummer ..... *Siehe* IP
New York State Educational Research Network ..... *Siehe* NYSERNet
news 84
News 72, 80, 142
newsgroup 85
Newsgroup 80
Newsgroups 188
Newsreader 82
News-Server 82
NIC 29
Nickname 92
NNTP 83
NOEP 207
NPL 47
NSF 43, 60
NSFNet 43, 45, 46
NVT 85
NWG 30
NYSERNet 45

O

Obhutspflicht 164
Online-Accounts 62
Online-Dienst 64
Opportunitätsprinzip 162
Ordnungsgeld 200
Ordnungshaft 200
org ..... *Siehe* TLD

P

Packet Radio Network ..... *Siehe* PRNet
Paket 25, 49
Paket-Sniffing 138
Paket-Switching ..... *Siehe* Paketvermittlung
Paketvermittlung 26
Paketvermittlungsnetzwerk 27
PAN 67
Personalitätsprinzip 155
PGP 79
Phänomenologie 131
PKS 136
Polizeibeamte 196
POP 73
Pornographie 115
Portscann 72
Post Office Protocol 73
posten 80

PPP 63
Prestel 67
Pretty Good Privacy 79
PRNet 39
Provider 61, 162
Proxy-Server 168
Pseudonym 92

Q

Quadrupel 50

R

RAND 33
RARE 46
Raubkopierer 148
rec 84
Recht auf informationelle Selbstbestimmung 198
Rechtfertigungsgründe 160
recieved 75
remote-login 86
reply-to 75
Request 100
Request for Comments ..... *Siehe* RFC
Réseaux Associés pour la Recherche Européenne ..... *Siehe* RARE
Réseaux IP Européans 60
Réseaux IP Européens ..... *Siehe* RIPE
Response 100
RFC 31, 35, 37
RFC 1521 76
RFC 821 73
RFC 822 76
RIPE 47, 60
Router 40
Routing 25, 38, 57
Routing-Tabelle 58

S

S/MIME-Spezifikation 79
Sadismus 185
SATNet 39, 40, 46
Schlepper 122
Schrift 175
Schutzpflicht 164
sci 84
Scientology 152
SDS-940 31
Second-Level-Domain ..... *Siehe* DNS
Server 62, 71
Serviceprovider 168
Sextouristen 119
SGML 98
Sicherstellung 204, 212
SigG 166
Sigma-7 31
Simple Mail Transfer Protocol 73
SLIP 63
SM 129
Smiles 93
SMTP 73
Snuff 129
snuff-pornos 125
soc 84
Sodomie 185
Sofortvollzug 170
Softwarepiraten 144
Space Physics Analysis Network ..... *Siehe* SPAN
Spamming 141, 192
SPAN 44
Speichervermittlungsnetzwerk 26
Sperranordnung 224
Sputnik I 19
Sputnik II 19
SRI 28
Staatsanwaltschaft 195
Standleitung 61
Stop-Seiten 178
store-and-forward-Prinzip 62
Störerauswahl 227

Störerbegriff 223
strafbares Unterlassen 163
Strafprozeßrecht 195
Strafverfolgung 155
Structured Generalized Markup Language 98
subject 75
Sub-Level-Domain ..... *Siehe* DNS
Subsidiaritätsklausel 223
Suchmaschinen 193
summary 85
Surfen 186
Szenejargon 128

T

talk 84
Täterkommunikation 134
Täterschaft 172
Tatkommunikation 134
Tatortbegriff 157
Tatwerkzeug 135
TCP 39, 41, 49
TCP/IP ..... *Siehe* TCP oder IP
TCP-Ports 71
TDDSG 166
TDG 165, 166, 218
TeenyMUD 95
Teilnahme 172
Telebox-400 68
Telebrief 68
Teledialoge 68
Teledienst 165, 218
Teledienstedatenschutzgesetz 166
Teledienstegesetz 166
Telefon 23
Telegrafie 23
Telekommunikation 209
Telekommunikationsanlage 209
TELENET 43, 44
Teletel 67
Telex 68
Telnet 31, 72, 85, 103, 145
Telnet-Login 86
Terminal 34
Terminalcontroller 34
Terminalemulation 85
Terminal-IMP ..... *Siehe* TIP
Terminalprogramm 62
Terminalverbindung 62
Territorialitätsprinzip 155
Thread 84
Thule-Netz 152
Tim Berners-Lee 96
Time-Sharing-Systeme 21
TinyMUD 95
TIP 31, 34
TLD ..... 53, 54 *Siehe* DNS
to 75
T-Online 65
Top-Level-Domain ..... *Siehe* DNS *Siehe* TLD
Transmission Control Protocol ..... *Siehe* TCP
Trash 129
Trojaner 140

U

U.S. Air Force 20
U.S. Army 20
U.S. Navy 20
UAFEK 232
UARV 232
Ubiquitätsprinzip 155
UCAR 44
UCLA 27, 28, 30
Uniform Resource Locator 101
Universal Mobile Telecommunications System .. 110
Universität von Kalifornien 28
Universität von Utah 28
University Corporation for Atmospheric Research
..... *Siehe* UCAR

Unix-to-Unix-Copy-Protocol 62
UNO 60
UNO-Kinderhilfswerk 119
upload 87
URI 98, 101
URL 98, 101
URN 101
URN-Verzeichnis 104
Usenet 80, 82, 103, 128, 142
USENet 44
Usenet-Newsgroups 80
UTMS 110
UUCP 44, 82
UUCP-Verbindung 62
UUDECODE 76
UUENCODE 76

V

VE 208
Verbotsirrtum 161
Verein zur Förderung eines Deutschen Forschungsnetzes ..... *Siehe* DFN
Verhaltensstörer 224
Verhältnismäßigkeit 230
Verschlüsselung 78
Verursachungsbeitrag 163
Verzeichnisse 193
Videotel 67
Videotex 66, 67, 118
Videotexnet 67
Virtual Reality Modeling Language 94
Voice over IP 93
VoIP 93, 111
Vollduplexleitung 23
Voll-Duplex-Modus 111
VRML 94, 98
VRML+ 94

W

WAIS 90, 103
WAIS-Client 91
WAP 111
WARBOTS 149
Watergate-Krise 38
Wchat 94
Web-Cam 151
Website-Hacking 147
Weltrechtsprinzip 155
Wide Area Information Server 90
WIN 47
Wireless Application Protokoll 111
Wireless Markup Language 110
Wirtschaftskriminalität 133
Wissenschaftsnetz ..... *Siehe* WIN
Wonderland 119
Woods 95
World Wide Web 96
Worlds Chat 94
WWW 72, 96, 103, 150
WWW-Browser 105
WWW-Client 105
WWW-Formular 104
WWW-Gateway 104
WWW-Server 105

X

X.25 69
XEROX-PARC 45
XML 98
XSL 98

Y Z

ZaRD 233
Zertifikat 79
Zertifizierung 78
Zertifizierungsstellen 79
Zeugnisverweigerungsrecht 200
Z-Net 70
Zustandsstörer 224
Zwangsgeld 170