



www.InfrastrukturInternet- Cyberterror.Netzwerk

**Analyse und Simulation strategischer Angriffe
auf die kritische Infrastruktur Internet**

Wolfgang Fischer



Forschungszentrum Jülich GmbH
Institut für Energieforschung (IEF)
Systemforschung und Technologische Entwicklung (IEF-STE)

www.InfrastrukturInternet- Cyberterror.Netzwerk

**Analyse und Simulation strategischer Angriffe
auf die kritische Infrastruktur Internet**

Wolfgang Fischer

Bibliografische Information Der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen
Nationalbibliografie; detaillierte Bibliografische Daten sind im Internet
über <http://dnb.d-nb.de> abrufbar.

Herausgeber und Vertrieb: Forschungszentrum Jülich GmbH
Zentralbibliothek, Verlag
D-52425 Jülich
Telefon: 02461 61-5368 · Telefax: 02461 61-6103
e-mail: zb-publikation@fz-juelich.de
Internet: <http://www.fz-juelich.de/zb>

Umschlaggestaltung: Grafische Medien, Forschungszentrum Jülich GmbH

Druck: Grafische Medien, Forschungszentrum Jülich GmbH

Copyright: Forschungszentrum Jülich 2007

Schriften des Forschungszentrums Jülich
Reihe Informationstechnik/Information Technology Band/Volume 14

ISSN 1433-5514
ISBN 978-3-89336-474-9

Vollständig frei verfügbar im Internet auf dem Jülicher Open Access Server (JUWEL) unter
<http://www.fz-juelich.de/zb/juwel>

Alle Rechte vorbehalten. Kein Teil des Werkes darf in irgendeiner Form (Druck, Fotokopie oder
in einem anderen Verfahren) ohne schriftliche Genehmigung des Verlages reproduziert oder
unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

DAS INTERNET ZWISCHEN MYTHOS UND INFRASTRUKTUR	1
DIE INTERNETSICHERHEIT ALS DRÄNGENDE AUFGABE	23
Nachhaltige Entwicklung und Sicherheit sind verwoben	27
Kritische Infrastrukturen benötigen Schutz.....	31
Das Internet wird zu einer kritischen Infrastruktur	41
Neue Bedingungen für den Schutz kritischer Infrastrukturen	50
Gefahren für ein sicheres Internet.....	57
<i>Leistungen eines sicheren Internets</i>	<i>57</i>
<i>Beeinträchtigungen eines sicheren Internets.....</i>	<i>62</i>
<i>Offene Fragen zur Sicherheitslage</i>	<i>64</i>
<i>Die Verschärfung der Sicherheitslage</i>	<i>73</i>
<i>Strategien und Mittel von Angreifern</i>	<i>79</i>
Gefahrenbereiche für Internetsicherheit.....	88
<i>Cyberkriminalität, terroristische Aktivitäten im Cyberspace und Cyberkrieg.....</i>	<i>89</i>
<i>Verwobene Gefährdungen von Internetsicherheit</i>	<i>96</i>
Internetsicherheit zwischen technischem und sicherheitspolitischem Konzept....	100
EINE NEUE GEFAHR FÜR EIN SICHERES INTERNET?	117
Was ist Cyberterrorismus?	121
<i>Nutzung des Internets durch Terroristen</i>	<i>124</i>
<i>Terrorismus gegen das Internet</i>	<i>137</i>
SIMULATION STRATEGISCHER ANGRIFFE AUF DIE INFRASTRUKTUR DES INTERNETS.....	145
Simulationsexperiment Regierungskommunikation	146
<i>Ergebnisse der Simulationen.....</i>	<i>148</i>
<i>Internetresilienz - ein differenziertes Bild.....</i>	<i>163</i>
Simulationsexperiment konkurrierende Infrastrukturlösungen	165
Das Internet ist ein relativ resilientes Datentransportsystem.....	169
INTERNETSICHERHEIT ALS BLEIBENDE HERAUSFORDERUNG	173
VERZEICHNIS DER LITERATUR	185

Verzeichnis der Abbildungen und Tabelle

Abbildung 1: Verwobene Gefährdungen im Cyberspace.....	99
Abbildung 2: Dreieck der Verwundbarkeit des Internets.....	145
Abbildung 3: Gemittelte Auslastung der Backbones weltweit.....	149
Abbildung 4: Gemittelte Auslastung der Backbones in Europa.....	151
Abbildung 5: Gemittelte Auslastung der Backbones in Deutschland.....	151
Abbildung 6: Backbones in Deutschland mit Regierungspaketen.....	152
Abbildung 7: Backbones in Europa mit Regierungspaketen.....	153
Abbildung 8: Backbones weltweit mit Regierungspaketen.....	154
Abbildung 9: Verlauf des mittleren Paketverlustes und der mittleren Routinganpassung im Simulationsexperiment Störung IX Frankfurt.....	155
Abbildung 10: Verlauf des mittleren Transportpaketverlustes und der mittleren Anzahl an unzustellbaren Paketen bei Störung des IX Frankfurt.....	155
Abbildung 11: Verlauf der Zusammensetzung der mittleren Anzahl an unzustellbaren Paketen bei Störung des IX Frankfurt.....	156
Abbildung 12: Summierter Gesamtschaden bei IX-Störungen.....	157
Abbildung 13: Wege der Regierungskommunikation innerhalb von Europa beim Ausfall des IX Frankfurt.....	160
Abbildung 14: Wege der Regierungskommunikation in Deutschland beim Ausfall des IX Frankfurt.....	161
Abbildung 15: Positionierung der Kraftwerke im Netzwerk.....	168
Abbildung 16: Verbindungsqualität in Abhängigkeit zur Entfernung bei einem Wurmangriff.....	168
 Tabelle 1: Vergleich der signifikant beeinträchtigten Beziehungen in der Regierungskommunikation bei Störungen der IX Frankfurt, London, Paris.....	 159

Das Internet zwischen Mythos und Infrastruktur

Vor etwa zwanzig Jahren verdrängten Tischcomputer die elektrischen Schreibmaschinen und lösten den Bleistift als alltägliches Werkzeug ab. Damals musste einiges in Bewegung gesetzt werden, um das, was am eigenen Rechner verfasst wurde, in einen anderen Rechner zu übertragen. Eine Diskette wurde eingelegt, die Daten wurden gespeichert, die Diskette wurde entnommen und transportiert - zu Fuß, per Haus- oder Bundespost. Heute sind Disketten nur noch eine Erinnerung an Zeiten, in denen Computer Inseln waren, zwischen denen diese grünen oder schwarzen Datenträger mühsam die Verbindung aufrecht hielten. Im 21. Jahrhundert bewegt ein Finger riesige Datenmengen in Bruchteilen von Sekunden über das Internet zwischen entfernten Rechnern, und künftig soll das mit noch größeren Datenmengen noch rascher geschehen. Dabei hatte sich über viele Jahre kaum jemand für die Wissenschaftler interessiert, die mit Mitteln der US-Regierung [vgl. NRC, 1999] in ihren Labors an einem Datennetz arbeiteten, das breite, bequeme Brücken zwischen den Inseln errichten sollte. Aber die Welt schien auf die Brückenbauer gewartet zu haben. Denn keine Technologie hat sich so rasch verbreitet wie das als Internet bezeichnete Netzwerk, seit die Regierung der USA im Jahre 1995 entschied, die von Forschern und Regierungsangestellten genutzten Hauptstränge des Datentransports für die kommerzielle Nutzung freizugeben. Helfer bei dieser Expansion waren die Browser, Computerprogramme die es ermöglichen, verschiedene Arten von Dokumenten zu betrachten, sowie das Windows-Betriebssystem. Sie ermöglichen Laien eine einfache Nutzung des Netzwerkes. Seit den 90er Jahren hat sich das Internet, wenn auch unterschiedlich dicht gewoben und noch immer auf entwickelte Länder und Regionen zugeschnitten, über große Teile der Welt ausgebreitet [ITU, 2005], [Lepperhoff, Fischer, 2004], [Einemann, 2006].¹

Schon bald machte sich der Mythos Internet breit. Er knüpfte an die konstitutiven Merkmale dieses Informations- und Kommunikationsnetzwerkes, Offenheit, Gleichberechtigung, Innovation, Dynamik, an und fand im Begriff Cyberspace seinen Ausdruck, der einem Science-Fiction-Roman [Gibson, 2001] entnommen wurde.² Internetnutzer konnten in dem Gefühl schwelgen, Zugang zu einem besonderen,

¹ Vgl. den prägnanten Abriss der Internetentwicklung aus topologischer Sicht [Grubestic, Murray, 2005].

² Dort ist der Cyberspace ein vielfältiges Netzwerk mit Sensoren. Abgeleitet ist der Begriff Cyber von Kybernetik (Steuerung, Regelung). Zu den Wirkungen des Romans [Pralle, 2005].

virtuellen Raum zu haben, der eigenen Normen und Regeln folgt, nicht greif- und kontrollierbar ist. So war es nur ein kurzer Weg zu der Unabhängigkeitserklärung des Rinderzüchters, Liedermachers und Internetaktivisten John Perry Barlow im Jahre 1996:³ Er sah mit dem Internet eine Zeit anbrechen, in der sich eine grenzenlose, vernetzte Zivilisation des Geistes unterhalb der Staaten ausbreitet und sich ihrer Macht entzieht, ja Staatsmacht selbst entwertet. Das entsprach dem Geist der Zeit, der nach dem Ende des Ost-West-Konfliktes, mit einer neuen Phase der Globalisierung und dem verstärkten weltweiten Agieren gesellschaftlicher Kräfte den Abschied des handlungsbestimmenden Territorialstaates heraufdämmern sah. Dessen Vision leuchtet gelegentlich noch auf, wenn über ein künftiges neues Internet nachgedacht wird. Aber sie entfaltet keine Kraft mehr, denn die Träume und Projektionen eines Barlow so zerstoßen wie die Illusion, der Staat verabschiede sich als wesentlicher Akteur von der Bühne der Welt.⁴ Heute ist das Internet in vielen Regionen der Welt zu einem alltäglichen Werkzeug geworden, und die Mythen werden nur noch von wenigen weitererzählt.⁵

Was ist nun dieses Internet, dem so viel zugetraut wird, das so viel Aufmerksamkeit findet, dem so viel Zeit und Ressourcen gewidmet werden und das wahrscheinlich mit Isidor von Sevilla (560-636 nach Christus) einen Schutzheiligen bekommen wird, der als einer der gelehrtesten Männer seiner Zeit versuchte, in der Etymologiae (Ursprünge) das gesamte Wissen zusammenzutragen?⁶

Es ist ein sich immer wieder verändernder Zusammenschluss diverser Netze auf der Basis einheitlicher Software (inter-Netz),⁷ aber kein geplantes, zentral gesteuertes und überwacht Gebilde. Das Internet kennt keine zentrale Netzwerksteuerung und -kontrolle und keine einheitliche physikalische Basisstruktur, sondern es lebt aus der Software. Seine zentrale Aufgabe ist es, die in digitale Datenpakete zerlegten Informationen zwischen Rechnern zu transportieren. Essentiell dafür sind das Internet-Protokoll (IP) und das Transmission Control Protokoll (TCP): Das IP ist für die Adressierung der Datenpakete zuständig; das TCP sorgt dafür, dass die Pakete, die von den Rechnern versandt werden, an ihrem Ziel vollständig und richtig zusammenge-

³ Vgl. den Text der Erklärung in Telepolis: <http://www.heise.de/tp/r4/artikel/1/1028/1.html>.

⁴ Vgl. dazu die Arbeiten des Sonderforschungsprogramms: <http://www.staatlichkeit.uni-bremen.de/>.

⁵ Kritisch zu den zugrundeliegenden Weltbildern [Keen, 2006].

⁶ Vgl. <http://www.heiligenlexikon.de/>.

⁷ Zur Information über das Internet und seine Funktionsweise vgl. <http://www.netplanet.org/>; ferner [Grimm, 2005] zu seiner Einordnung in die Informatik, Kommunikations- und Sprachwissenschaften.

setzt werden. Diese Pakete werden vorwiegend durch Kabel, aber auch über Satelliten⁸ und immer öfter drahtlos,⁹ zwischen den Rechnern versandt, die dauerhaft oder zeitweise (dynamisch) über eine eigene IP-Nummer verfügen. Durch diese Nummer, eine Zahlenreihe, ist ein Rechner eindeutig identifizierbar.

Populäre und allgemein zugängliche Anwendungen des öffentlichen Internets¹⁰ sind zwei - durchaus unterschiedliche - Dienste, die von einem Browser auf der Oberfläche des Computerbildschirms optisch verkoppelt werden: Die elektronische Post (E-Mail) mit ihrem Softwareprotokoll SMTP (Simple Mail Transport Protocol) sowie das World Wide Web (WWW), das ein interaktives Hypertext-Informationssystem ist, und als dessen Geburtsstunde die Einführung des ersten Browsers durch Berners-Lee im Jahre 1990 gilt.

In einem doppelten Sinn ist das Internet neutral, und diese Neutralität ist in der Software verankert: Erstens, es bevorzugt keine Datenpakete; das Paket, das zuerst kommt, wird an den Netzknoten bzw. Routern, den Weichen des Netzes, auch zuerst weitergeleitet. Zweitens, das Netz beschäftigt sich nicht mit dem Inhalt digitaler Datenpakete, es transportiert sie nur, seien es freundliche Grüße, wertvolle Wirtschaftsdaten, gefährliche Viren, nützliche Zeitungsausschnitte oder bedrohliche Terrorinformationen. Diese Neutralität wird aber nicht mehr überall als konstitutives Merkmal akzeptiert. Es gibt, vor allem aus ökonomischen Interessen, von Seiten großer Netzbetreiber und, noch weniger ausgeprägt, aus Sicherheitserwägungen¹¹ heraus erste Überlegungen, sie einzuschränken oder aufzugeben. Prinzipiell könnte das mit einem neuen Internetprotokoll, wie dem IPv6,¹² erreicht werden. Soweit das alles einen tiefgehenden Wandel der Internetsoftware erforderlich macht, bleibt das vorerst eine (umstrittene) Vision.

⁸ Ihnen kommt vor allem eine Bedeutung in Regionen zu, die nicht oder zu dünn verkabelt sind; vgl. http://www.en.wikipedia.org/wiki/Satellite_Internet.

⁹ <http://www.de.wikipedia.org/wiki/WLAN>; <http://www.voip-information.de/wimax.html>.

¹⁰ Es steht hier im Mittelpunkt. Daneben gibt es Intranetze, die die IP und TCP nutzen. Sie sind meist nur durch Software vom öffentlichen Netz abgeschlossen, nutzen aber die gleichen Kabelstränge. Sie werden implizit in den hier präsentierten Simulationen berücksichtigt, da die Zerstörung der Kabel oder Internet-Exchange-Points auch sie treffen. Sind sie physikalisch vom öffentlichen Internet getrennt, verfügen sie also über eigene Kabel und Exchange-Points, fallen sie aus der Betrachtung.

¹¹ Sicherheit ist ein vager Begriff, der für Anwendungsbereiche zu spezifizieren ist. In Anlehnung an eine Formulierung des Bundesverfassungsrichtes aus dem Jahre 1985 ist sie gewährleistet, wenn zentrale Rechtsgüter geschützt sind (Leben, Gesundheit, Freiheit, Eigentum des Einzelnen, Unversehrtheit der Rechtsordnung, staatlichen Einrichtungen). Was das konkret bedeutet, wie viel Sicherheit sicher genug ist, bleibt hier offen. Dass es keine absolute Sicherheit, auch keine vollständige Cybersecurity gibt, ist eine triviale, aber notwendige Einsicht.

¹² <http://www.de.wikipedia.org/wiki/IPv6>.

In einigen Bereichen ist eine weltweite Koordination oder Regulierung (governance) des Internets erforderlich: Erstens, für die IP-Nummern (IP-Adressen); jede dieser Nummern darf nur einmal vergeben werden. Zweitens, für die Bereichsnamen (Domain Name), die - wie fz-juelich - unter der deutschen Adresse (.de) so nur einmal zugeordnet werden kann. Drittens, hinsichtlich der Gestaltung des Systems der Rootserver, die Bereichsnamen in IP-Adressen umwandeln (Namensauflösung).¹³ Viertens, hinsichtlich der grundlegenden Software (Protokolle), die überwiegend von gesellschaftlichen Gruppen entwickelt wird, in denen Wissenschaftler den Ton angeben. Die Protokolle enthalten den Geist einer offenen, weitgehend urheberrechtlich nicht geschützten Infrastruktur [vgl. Internet Governance, 2004].

Im Internet spielen diverse Dienstleister (Provider) eine zentrale Rolle. Sie bieten Nutzern den Zugang zum Netzwerk an, wie das Telekommunikationsunternehmen tun; sie stellen die großen Kabelstränge (Netzwerkbetreiber, Carrier), die Router zur Verfügung, über die Datenpakete verteilt werden; und sie bieten Möglichkeiten, Webseiten abzulegen (to host). Eine andere Gruppe der Dienstleister bietet Inhalte an, die prinzipiell von allen anderen Netzteilnehmern abgefragt werden können, von wo aus und mit welchem Zugangs-Dienstleister sie auch immer in das Netzwerk gelangen. Im Netz kann Jedermann prinzipiell ein Anbieter von Inhalten sein, eine Webseite aufbauen, ob Unternehmen, Behörde, nationale, internationale Organisation oder, wie die Juristen sagen, „natürliche Person“, ein Privatmensch - ein Merkmal eines offenen, neutralen Netzes.

Viele Internetnutzer haben keine präzisere Vorstellung davon, wie das Internet funktioniert. Ihnen ist das so gleichgültig wie es für Fernsehzuschauer ohne Interesse ist, wie eine Bildröhre oder ein Flüssigkristallbildschirm aufgebaut ist - nur problemlos und flimmerfrei arbeiten muss das System. Freilich gibt es dabei einen feinen, aber wichtigen Unterschied: Unkenntnis über die Funktionsweise eines Fernsehgerätes beeinträchtigt nicht den Empfang. Fehlt aber jegliches Wissen über den Aufbau und die Funktionsweise des Internets und kommt dazu ein (falsches) Gefühl der Sicherheit, da es keine wahrnehmbaren physischen Kontakte zum Kommunikationspartner gibt, kann sich das rächen. Denn das Netzwerk macht ungeschützte Rechner zu einem Ort, an dem sich jeder Fährige ohne Wissen des Besitzers einnisten kann, um zu tun, was ihm beliebt: Datenpakete können abgefangen, verfälscht oder gelöscht wer-

¹³ Zentral ist hier der Root File der Top Level Domains des US-Unternehmens NSI-Verisign unter der Kontrolle der USA-Regierung; vgl. http://www.de.wikipedia.org/wiki/Top_Level_Domain.

den - dann ist schlechter Empfang garantiert; Daten im Rechner können ausspioniert und Rechner fremder Kontrolle unterworfen werden - dann können das Netz bzw. seine Nutzer über diese Rechner bedroht werden. Solche Gefahren¹⁴ haben etwas mit dem Charakter des Internets als ein Netz der Netze zu tun, in dem alle Rechner untereinander verbunden sind. Und an den Enden der Netze sitzen immer mehr Nutzer an ihren Computern, von denen eine unbekannte Zahl fähig und bereit ist, von der Unwissenheit derer zu profitieren, die ihre Rechner nicht schützen und sich unbedarft im Netz umhertreiben (surfen).

Trotz solcher Gefahren hat sich das Internet in zwei Jahrzehnten aus einem dünnen ARPA bzw. NSFNet für wenige tausend USA-Experten zu einem alltäglich und weltweit genutzten Medium für viele Menschen entwickelt, das, was die Inhalte betrifft, seinen Charakter stark verändert hat.

Niemand weiß genau, wie viele Menschen das Netz heute mehr oder weniger regelmäßig nutzen. Schätzungen,¹⁵ die methodische Unterschiede aufweisen, gehen von mehr als 700 Millionen bis zu gut einer Milliarde aus, und die Zahlen steigen insbesondere in Asien weiter, speziell in China und Indien. Aber, und das wird oft übersehen, fünf Milliarden Menschen haben keinen Zugang zu diesem Netz, und viele von ihnen nutzen noch nicht einmal ein Telefon. Und selbst in den westlichen Staaten bleibt ein digitaler Graben: Meist verfügen nicht mehr als fünfzig bis sechzig Prozent der Haushalte über einen eigenen Netzzugang. Viele der Nutzern freilich bauen ihren Netzzugang fleißig aus: Mitte 2005 waren, vorwiegend in Industriestaaten, knapp 180 Millionen Netznutzer über leistungsfähige Breitbandanschlüsse (Übertragungsgeschwindigkeit von mindestens 256 Kilobit/Sekunde) mit dem Internet verbunden. Sie ermöglichen die Datentransportpotentiale des Netzes besser auszuschöpfen.¹⁶ Heute wird das Internet auch nicht mehr, wie in den Anfangsjahren, vorwiegend in den USA genutzt. Mit 152 Millionen stellen die USA zwar immer noch die größte Gruppe der Nutzer. Aber dann folgen schon China (75), Japan (52), Deutschland (32), Großbritannien (30) und Südkorea (25 Millionen Nutzer). Und wird die Liste der Internetmeister danach geordnet, wie lange Nutzer durchschnittlich im Netz blieben, führt Israel die Liste an, gefolgt von den USA, Finnland, Südkorea, Niederlande und Taiwan

¹⁴ Manchmal werden Gefahr (übergeordneter Begriff) und Gefährdung (zeitlich, räumlich, größenmäßig spezifizierte Gefahr) unterschieden. Das ist hier nicht so. Verzichtet wird auch auf den Risikobegriff. Die Kalkulation der Wahrscheinlichkeit und Folgen von Cyberterrorismus ist bislang nicht möglich.

¹⁵ Vgl. <http://www.internetworldstats.com>; <http://www.clickz.com>; comscore.com.

¹⁶ <http://www.dslforum.org/index.shtml>.

[Shannon, 2006]. Deshalb tauchen neben Englisch mehr und mehr Sprachen im Netz auf:¹⁷ Wer diese Weltsprache nicht lesen kann, findet immer öfter Seiten in seiner Muttersprache.

So überrascht es nicht, dass einer wachsenden Zahl von Menschen der Nutzen des Internets gewaltig erscheint, und es eröffnet scheinbar das Tor zu neuen Welten, auch wenn und wohl gerade weil es, entgegen den Träumen eines Barlow, inzwischen dabei ist, eine symbiotische Beziehung einzugehen mit machtvollen Akteuren aus Wirtschaft, Gesellschaft und Politik. Das, was das Netz nun durch diese Symbiose vor allem an Unterhaltung und Kommunikationsmöglichkeiten bietet, entspricht dem, was sich immer mehr Menschen wünschen, und es formt zugleich ihre Wünsche, Begierden, aber wirkt auch auf die Struktur des Netzes und der ihm angeschlossenen Endgeräte zurück - der Datentransport wird breitbandig, schneller, und Endgeräte werden leistungsfähiger, vernetzt. Die Nutzung des Netzes für (z. T. militärische) Forschung und Entwicklung, seine ursprüngliche Bestimmung, macht deshalb nur noch den kleineren Teil des Verkehrs der Datenpakete aus. Unterhaltung, Spiel und Spaß, alltägliche Kommunikation, Handel und Informationssuche dominieren, und Endgeräte bieten immer mehr Möglichkeiten, das akustisch und visuell zu genießen.

Diese Lebensgemeinschaft, diese vielfältigen Nutzungen, lassen das Internet weiter expandieren. Sie machen es zu einer Schlüsseltechnologie,¹⁸ ermöglichen ihm eine zentrale Rolle unter den Informations- und Kommunikationstechnologien (IuK-Technologien) und künftig vielleicht eine unersetzbare Position als Infrastruktur der Infrastrukturen, auf deren Funktionieren moderne Gesellschaften angewiesen sind. Denn alle digitalen Daten, die in den Alltag integrierte Computer und Sensoren demnächst in ungeheuren Strömen erzeugen sollen (pervasive computing), können auf der Basis des Internetprotokolls zusammengeführt werden [Langheinrich, Mattern, 2003]: Alles kann über das Netzwerk laufen (all over IP). Ein Bestandteil eines solchen Netzes, das breit ausgeworfen werden und tief in die Gesellschaft eindringen soll, könnten Funketiketten werden, die via Rechner an das Netz angebunden werden. Über das Pro und Contra dieser RFID, die schon beginnen, die Logistik zu revolutionieren und vielfältig einsetzbar sind, wird diskutiert [Oertel, Wölk, 2006].

¹⁷ Vgl. <http://www.glreach.com/globstats/index.php3>; <http://www.internetworldstats.com/stats7.htm>.

¹⁸ Da es durch Software (Protokolle) entsteht, ist das Internet keine Technologie im engeren Sinne: Es wird aber von Politik und Gesellschaft so wahrgenommen und wirkt wie eine Schlüsseltechnologie.

In den 90er Jahren wurde in den USA der Schutz dieser sich noch herausbildenden Dateninfrastruktur und anderer kritischer Infrastrukturen zu einer vorrangigen politischen und gesellschaftlichen Aufgabe erklärt [PCCIP, 1997]. Nach einer Definition des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sind solche kritischen Infrastrukturen „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden“¹⁹. Auch wenn nicht immer ganz klar ist, welche Infrastrukturen zu diesen kritischen zählen, gibt es, auch international, einen weitgehenden Konsens, dass Informations- und Kommunikationstechnologien solche Infrastrukturen sind, und das Internet wird immer öfter als eine besonders wichtige IuK-Infrastruktur betrachtet.

Im Laufe der letzten Jahre haben sich auch andere Staaten und internationale Organisationen der Critical Infrastructure Protection (CIP) bzw. der Critical Information Infrastructure Protection (CIIP) als ihr Teilgebiet verschrieben. CIP umfasst alle Strategien, Programme, Maßnahmen und institutionelle Arrangements, die kritische Infrastrukturen weniger verwundbar machen und, sollten sie dennoch beeinträchtigt werden, ihre Funktionsfähigkeit rasch wiederherstellen (recovery). Dabei hat CIP einen Schwerpunkt beim physischen Schutz [CISP, 2004]. CIIP bezieht sich speziell auf die IuK-Infrastrukturen, seit einigen Jahren auch und verstärkt auf das Internet (vgl. umfassend [Abele-Wigert, Dunn, 2006], für Deutschland [NPSI, 2005]). CIIP rückt stark den Schutz vor schädlicher Software, vor Hackerangriffen etc. in den Mittelpunkt. Obwohl sie einen unterschiedlichen Focus haben, lassen sich in der Praxis des Infrastrukturschutzes, bei den konkreten Schutzkonzepten und -maßnahmen, beide Gebiete nicht immer klar trennen. Moteff, Copeland, Fischer, [2003, S. 4] machen darauf aufmerksam, dass „the distinction between physical-security and cyber-security is almost inextricable and not clearly articulated.“ Auch CIIP kommt nicht ohne physischen Schutz aus, und CIP ohne Gewährleistung einer zumindest rudimentären Funktionsfähigkeit der Kommunikationssysteme bleibt illusorisch.

Das Internet als „Schlüssel-“, „Querschnittstechnologie“ oder „Nervensystem“ moderner Gesellschaften ist, teilweise mit erheblicher Verspätung, da seine Potentiale nicht erkannt wurden, zum Gegenstand der nationalen Politik in zahlreichen Staaten

¹⁹ <http://www.bsi.bund.de/fachthem/kritis/index.htm>.

geworden.²⁰ Sie versuchen, durch die breite und intensive Nutzung des Netzes Innovation, Wettbewerbsfähigkeit, ihren Status, Einfluss und ihre Macht zu stärken. Mit dem zweistufigen World Summit on the Information Society (WSIS) im Jahre 2003 und 2005 wurde das Netzwerk auch Thema der internationalen Politik [Kleinwächter, 2004], [Schade, 2004].²¹ Der WSIS wurde von der International Telecommunication Union (ITU) ausgerichtet, die zur Familie der Vereinten Nationen gehört. Damit hat, erstmals seit den Auseinandersetzungen über eine Weltinformationsordnung in den 70er Jahren, als Diktaturen die Ausstrahlung des Satellitenfernsehens in ihr Territorium verhindern wollten [Roth, 1984], eine neue technologische Entwicklung im Kommunikationsbereich weltweite Verhandlungen nach sich gezogen. Die WSIS-Dokumente formulieren das grundlegende Ziel, die Potentiale des Internets für eine globale nachhaltige Entwicklung zu nutzen.²² Dies zu präzisieren, die Mittel dafür bereitzustellen und sinnvoll einzusetzen erweist sich jedoch, wie bei anderen globalen Veranstaltungen auch, als schwierig und konfliktreich. Meist kontroverse Diskussthemata zwischen und innerhalb diverser Interessengruppen und Staaten sind: die digitale Spaltung zwischen „Nord“ und „Süd“ (weniger die digitale Spaltung zwischen den gesellschaftlichen Schichten in den Staaten); die Finanzierung eines digitalen Solidaritätsfonds für den Süden durch den Norden; die Rolle des Marktes bzw. des Staates beim Aufbau des Netzwerkes; die Probleme des geistigen Eigentums und des Schutzes vor der im Internet weit verbreiteten Verletzungen von Urheberrechten;²³ die (gefährdeten) Bürgerrechte auf Informationsfreiheit, Privatsphäre und Datenschutz; die Gefahren für die Internetsicherheit (Cybersecurity),²⁴ denen ein spezielles Thematic Meeting gewidmet wurde.²⁵ Schließlich ist die Regulierung des Internets ein viel beachtetes, kontroverses Thema. Bei ihm steht die Gestaltung und Verwaltung des Namenraums im Vordergrund. Sie wird von der privaten Internet Corporation for Assigned Numbers and Names (ICANN) ausgeübt wird, die nach US-

²⁰ Vgl. das Aktionsprogramm der Bundesregierung Deutschland aus dem Jahre 2006: http://www.bmbf.de/pub/aktionsprogramm_informationsgesellschaft_2006.pdf.

²¹ <http://www.itu.int/wsis/>; die Heinrich-Böll-Stiftung verfolgte den WSIS: <http://www.worldsummit2005.de/>.

²² Vgl. zum Aktionsplan: http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1160|0.

²³ So kann die Digitalisierung von Bibliotheksbeständen die Rechte von Autoren und Verlagen verletzen; vgl. <http://www.dradio.de/dkultur/sendungen/kulturinterview/562485/>.

²⁴ Vgl. [Dunn, 2005]; Cyber- oder Internetsecurity bezeichnet Politiken, Maßnahmen zum Schutz des Internets und seiner Nutzung, aber auch Abschätzung und Bewertung des erreichten Schutzgrades.

²⁵ <http://www.itu.int/osg/spu/cybersecurity/index.phtml>.

amerikanischem Recht der Gemeinnützigkeit organisiert ist und der Aufsicht durch das USA-Handelsministerium unterliegt [Signposts, 2005], [Leib, 2003].

Solche Themen werden in künftigen Diskussionen und Verhandlungen, wie immer sie inhaltlich und organisatorisch ausgestaltet sind, nicht vergessen werden.

Das Internet hat als Teil des schon seit längerer Zeit in Bewegung geratenen Informations- und Kommunikationssektors in Gesellschaft und Kultur, Wirtschaft und Politik Veränderungen auf allen Ebenen angestoßen [v. Oertzen, Cuhls, Kimpeler, 2006], [Siedschlag, 2005], [Castells, 2004], [diMaggio, 2001]. Aber noch lassen sie sich nicht exakt erfassen und bewerten. Denn die Wechselwirkungen von Internet, Gesellschaft und Politik sind im vollen Gang, und sie verändern beide Seiten. Möglicherweise trifft es zu, dass das Internet auf absehbare Zeit das individuelle und soziale Leben zwar stark beeinflussen, aber nicht grundlegend verändern wird [v. Oertzen, Cuhls, Kimpeler, 2006]. Aber die Zukunft ist für Überraschungen gut. Sie ist, in Anlehnung an Max Weber, vorhersehbar unvorhersehbar.

Wie schwierig schon das zu erfassen ist, was durch das Netzwerk und die anderen Kommunikationstechnologien angestoßen wird, zeigt die Vielfalt der Begriffe, mit denen die Veränderungen auf den Begriff gebracht werden sollen: Die neue Gesellschaft wird als Informationsgesellschaft bezeichnet, deren Reifegrad an der Verbreitung und Nutzung von IuK-Technologien bzw. an den transportierten Datenmengen gemessen wird. Andere ziehen Wissensgesellschaft vor, einen Begriff, der einmal Gesellschaft analytisch zu charakterisieren versucht, aber auch normativ-politisch verwendet wird, indem er zu politischer Gestaltung aufruft und eine Gesellschaft als Ziel verkündet, die ihre Wertschöpfung durch Erkenntnis und ihre praktische Anwendung sicherstellt (vgl. [Schade, 2004], [Bechmann et al., 2003], [Poltermann, 2002], [Stehr, 2001]). Ein dritter Begriff, Netzwerkgesellschaft [Castells, 2004], stellt Veränderungen sozialer Strukturen, Systeme und Prozesse in den Vordergrund und sieht z. B. vernetzte, nichthierarchische Organisationen als eine Ausdrucksform der neuen, durch das Internet vernetzten Welt.

Auch wer die Diskussionen darüber, ob solche Großtheorien die Entwicklungen von Gesellschaft richtig beschreiben, nur beiläufig und skeptisch verfolgt, wird die vielfältigen und widersprüchlichen Verflechtungen des Internets mit allen Bereichen des sozialen Lebens und die so angestoßenen Veränderungen nicht ignorieren. Und die

Suche nach neuen Anwendungen, nach neuen Geschäftsmodellen, Lebensentwürfen, die digitalen Lebensstil ausdrücken und zugleich formen, geht weiter.

Das Internet ist verwoben mit Strukturen und Prozessen von nachhaltiger Entwicklung bzw. Globalisierung, und es fördert sie in z. T. widersprüchlicher Weise [Behrens, 2005], [Kopfmüller, 2003], [Sassen, 2002]; es könnte eine neue Stufe der Globalisierung einleiten [Friedman, 2005], indem es Individuen unmittelbar in einen globalen Wettbewerb um Arbeitsplätze stellt, es ermöglicht aber auch die Organisation von Gegenmacht zu Globalisierung; das Netzwerk eröffnet individuelle, kollektive Entwicklungsmöglichkeiten, lässt aber auch Narzissmus, Unwissenheit und Unselbstständigkeit erblühen [Weizenbaum, 2006]; es wird zu einem permanenten Problem des Datenschutzes, da Nutzer normalerweise überall ihre digitalen Spuren hinterlassen [v. Oertzen, Cuhls, Kimpeler, 2006], weshalb Bürgerrechts- und Verbraucherschutzorganisationen fordern, dem Schutz der Privatsphäre ebenso große Aufmerksamkeit zu widmen wie dem Schutz vor Cyberkriminalität; das Internet schafft, unbeeindruckt von Platzen der dotcom-Blase im Jahre 2000, als die Aktienkurse tief fielen, wieder neue Märkte, wird zu einem wichtigen Arbeitsmarkt, Wirtschaftsfaktor [Statistisches Bundesamt, 2006], [OECD, 2005, 2002] und zu einem Bestandteil des Handelssystems;²⁶ es verändert Verwaltungsabläufe, den Arbeitsmarkt, und es belohnt neue Qualifikationen und entwertet Arbeitskräfte mit mangelnden Kenntnissen der neuen IuK-Technologien [v. Oertzen, Cuhls, Kimpeler, 2006]; das Internet trägt möglicherweise zur Steigerung der Produktivität bei;²⁷ es führt bislang getrennte Kommunikations- und Medienmärkte zusammen, schafft dabei neuen Wettbewerb und verändert die Mediennutzung bzw. die bislang dominierenden Medien selbst [Ganswindt et al., 2005]; es gibt Raum für neue Formen der Unterhaltung, die traditionelle Zerstreuung über das Fernsehen verdrängen könnten; es ermöglicht allen Nutzern, sich mit Social Software zu verknüpfen [Sixtus, 2005] und ihre eigenen Inhalte anzubieten (web-2),²⁸ sowohl auf kommerziellen Seiten²⁹ als auch den sehr beliebten Seiten wie myspace oder youtube - hier stellen sich immer mehr Menschen filmisch mit wahnsinnigen Gebärden oder bedächtigen Ausführun-

²⁶ 2004 sollen etwa 12 % des Welthandels direkt über das Internet vermittelt worden sein [Leggate, 2005]; in Deutschland tragen Internetverkäufe Anfang 2005 mit 2,7 % zum Gesamtumsatz der Unternehmen bei [Statistisches Bundesamt, 2006].

²⁷ Der Zusammenhang von Produktivitätsentwicklung und Internet ist strittig; vgl. [Pilat, 2004].

²⁸ Vgl. die Seiten der Erfinder dieses stark expandierenden und kommerziell interessanten "Netzes" Tim O'Reilly und Dale Dougherty: <http://www.oreillynet.com/>.

²⁹ Vgl. etwa <http://www.scale-multimedia.de/>.

gen dem Netzpublikum vor, geben Menschen sorglos intime Details ihrer Privatsphäre preis, knüpfen Isolierte neue Kontakte, und Menschen mit den abwegigsten Ideen, die bislang kaum auf Gleichgesinnte stießen, finden sie doch irgendwo im Cyberspace; dort können in „Strategiespielen“ virtuelle Massaker verübt werden, die vermutlich bei einigen Gestörten die Neigung stärken, das auch in der Wirklichkeit zu tun;³⁰ das Internet ist eine immer wichtigere Informationsquelle für den, der schon viel Wissen hat, das Netz zu nutzen vermag und so noch mehr Nutzbares erfährt [(N)online Atlas, 2005]; aber es ist auch ein Ort, an dem die Dummheit um Anhänger buhlt, und es nährt die Entwicklung moderner Neurosen und Süchte;³¹ das Netzwerk erleichtert die Organisation sozialer Bewegungen (Cyberprotest), trägt dazu bei, die Kontrolle undemokratischer Regierungen über die öffentliche Meinung aufzuweichen [Shane, 2005]; es beeinflusst auch in den Demokratien politische Prozesse und Strukturen, ohne sie aber bislang grundlegend zu verändern [Siedschlag, 2005], [Internet 2005]; es gibt Raum für eine wachsende Zahl von Internet-Tagebüchern (Weblogs), die über interessante, manchmal wenig beachtete Probleme und über Belanglosigkeiten berichten, wirre Reden oder durchaus einflussnehmende politische Kommentierungen anbieten und Politiker unter Dauerbeobachtung stellen; das Internet ist ein Hohlraum, den Falschmeldungen,³² verzerrte Darstellungen der Wirklichkeit, obskure Ideologien, widerliche Darbietungen und verdummende Propaganda füllen, die nun rasch und weltweit Hirne vernebeln kann, weil sie nicht in den Filtern traditioneller Medien hängen bleibt; es ist eine große Gerüchteküche, in der sich die Neigung vieler Menschen auslebt, durch Verschwörungstheorien die komplexe Wirklichkeit auf einfache Modelle zu reduzieren, wie der Münsteraner Soziologe Krysmanski zeigt;³³ es könnte humanitäre und Friedensmissionen erleichtern (Information- and Communication Technology for Peace Initiative),³⁴ und es kann eine Rolle spielen bei der elektronischen Kriegsführung moderner Streitkräfte.

Das Internet und seine Nutzungen bringt Mensch und Gesellschaft viele Vorteile. Aber es kann auch alte Probleme und Herausforderungen verschärfen und neue

³⁰ <http://www.zeit.de/online/2006/49/computerspiele-gewalt-psychologie>.

³¹ Vgl. etwa: <http://www.gin.uibk.ac.at/thema/internetsucht/>; <http://www.online-sucht.de/website.php>.

³² In der Cyberstorm-Übung der USA, Kanadas, Großbritanniens, Australiens, Neuseelands Anfang 2006 spielten Weblogs eine Rolle, die mit Falschmeldungen Cyberangriffe wirksamer machten.

³³ Vgl. <http://www.hjkrysmanski.de/>.

³⁴ Vgl. <http://www.ict4peace.org>.

schaffen [Harriss-White, 2002], [Hundley, 2001], und sie können die nationale und internationale Sicherheit beeinträchtigen:

- Das Internet beschleunigt, in Wechselwirkung mit anderen Technologien und vor dem Hintergrund tektonischer Verschiebungen in der Weltpolitik,³⁵ wirtschaftlichen, sozialen, politischen und kulturellen Wandel, der, zumindest in Übergangsphasen, zu Konflikten und Instabilitäten führen kann.
- Die meisten Nutzungen des Internets und ihre Folgen mögen hinsichtlich ihrer sicherheitspolitischen Auswirkungen Petitessen sein. Das gilt nicht für die zunehmende Einbindung des Internets in die militärischen Kommunikations- und Befehlsstränge [Gerber, 2005]. Sie kommt zwar nicht überraschend, könnte aber das Netz künftig zu einem Ort der Cyberkriegsführung machen.
- Nicht nur potentiell sondern schon heute stellen Entwicklungen eine Gefahr da, die seit einigen Jahren zu beobachten sind und weiter voranschreiten. Im und über das Netzwerk werden Straftaten begangen, unerwünschte Aktivitäten, die in der realen Welt anzutreffen sind, finden auch in Internet ihren Platz, und neue, internetspezifische kommen hinzu; strafbare und, etwa für Kinder und Jugendliche, gefährdende Inhalte werden offeriert [BSI, 2005],³⁶ und diverse Kriminelle nutzen das Netzwerk, beispielsweise um Spam zu versenden, die unerwünscht zugesandten E-Mails, die oft ohne rückverfolgbare Adresse sind.³⁷ Dabei ermöglicht das Internet, dass diese Akteure außerhalb der Jurisdiktion der Staaten bleiben können, in denen sie ihre Taten begehen oder von denen aus Inhalte abgerufen werden, die im Lande selbst verboten sind. Solche und weitere diskriminierte Nutzungen des Internets als ein Tatort und Tatmittel gefährden die Sicherheit *im Cyberspace*. Politiken und Maßnahmen, die diese Gefahren reduzieren sollen, werden oft in einem Spannungsverhältnis zu Bürgerrechten gesehen, wie dem Recht auf freie Information und Datenschutz [Roßnagel, 2006]. Und nicht selten sind sie von nur geringer oder mäßiger Wirksamkeit.
- Das Internet ist dabei, zu einer kritischen Infrastruktur zu werden. Deshalb muss seine Verwundbarkeit gering und seine Funktionsfähigkeit auch bei Naturkatastro-

³⁵ Vgl. als Einführung: Informationen zur politischen Bildung, Heft 291, Sicherheitspolitik im 21. Jahrhundert; http://www.bpb.de/publikationen/MXQU1P,0,0,Informationen_zur_politischen_Bildung.html.

³⁶ Dem Problem widmete sich die EU-Politik früh; vgl. [Commission, 1996; Commission, 1996a]; 1999 Action Plan on Promoting Safe Internet-Use, <http://europa.eu.int/scadplus/leg/en/lvb/l24190.htm>; [Commission, 2002]; vgl. auch http://europa.eu.int/information_society/activities/sip/index_en.htm.

³⁷ <http://www.de.wikipedia.org/wiki/Spam>.

phen, technischen Störungen und bei Angriffen³⁸ gewährleistet sein. Diese Sicherheit des Cyberspace erscheint vielen Experten, zumindest künftig, durch kriminelle, speziell terroristische Akteure bedroht [Talbot, 2004, 2006].

Nun ist das Internet kein Raum, in dem man unter die Diebe und Räuber fällt, sobald man ihn betritt, und fast alle Besuche im Netz gehen ohne Probleme vonstatten. Jedoch ist das Internet, wie die Kriminalstatistik³⁹ zeigt, immer häufiger Tatort bzw. -mittel, wobei es meist um Betrug geht. Aber auch hier zeigt der scharfe Blick, dass die spezifische Netzkriminalität nur einen kleineren Teil der kriminellen Taten ausmacht, die ganz überwiegend in der realen Welt begangen werden. Aber das kann sich ändern. Denn wie alle Orte, die leicht zugänglich, wenig überschaubar, schlecht zu überwachen sind und an denen viel zu holen ist, zieht das Internet dunkle Existenzen, gewöhnliche und politisch motivierte Kriminelle (terroristische Gruppen, Organisationen und Netzwerke) an. Sie haben schnell - und nicht selten schneller als Sicherheitsbehörden - gelernt, dass die konstitutiven Merkmale des Netzwerkes ihre Operationen erleichtern, die Prävention, Präemption,⁴⁰ Abwehr und Strafverfolgung aber erschweren.

Das Internet verändert auch die Lage derer, die sich als einfache Nutzer in das Netz begeben, und sie können rasch zum Opfer werden. Kein Nutzer kann immer sicher sein, dass das, was er auf seinem Bildschirm zu sehen bekommt, wirklich von dem stammt oder das ist, was es vorgibt: Die Internetseite einer Bank kann gefälscht, die Webseite eines Unternehmens oder einer Behörde kann durch heimlich eingespielte Daten Falsches präsentieren, und eine E-Mail muss nicht von dem angegebenen Absender stammen. Jeder Nutzer kann, ohne es zu wollen, mit Inhalten konfrontiert werden, die in seinem Land verboten sind und an denen er kein Interesse hat. Einige Stichworte sind Pornographie, Gewaltdarstellungen, Rechts- und Linksradikalismus. Das kann auch jedem Spaziergänger in der realen Welt passieren. Aber er kann sich, mit einer Hoffnung auf erfolgreiche Strafverfolgung, an die Polizei wenden, oder er begibt sich zur Informationssuche, Unterhaltung nur an Orte oder nutzt nur Medien, von denen er annehmen darf, dass sie nichts Verbotenes anbieten oder zu

³⁸ Definiert als unautorisierte Zugriff(s)versuch auf Informationssysteme. Eckert [2004] unterscheidet passive Angriffe (etwa Abhören) und aktive (z. B. Datenzerstörung, Blockade von Verbindungen). Oft übersehen wird, dass Angreifer sich auch physischer Mittel bedienen können.

³⁹ Vgl. <http://www.bmi.bund.de>, Kriminalstatistik; Internettaten werden seit 2004 gesondert erfasst.

⁴⁰ Prävention soll eine latente Bedrohung beseitigen; Präemption einem unmittelbar bevorstehenden Angriff zuvorkommen.

strafbaren Handlungen aufrufen. Wäre das anders, würde niemand Kinder und Jugendliche ohne Begleitung Erwachsener in Buchhandlungen gehen oder in Zeitschriften lesen lassen. Das Internet kann diese (relative) Sicherheit nicht gewährleisten.⁴¹ Deshalb darf jeder Bürger vom Staat erwarten, ihn im Rahmen von Recht und Gesetz nach Möglichkeit zu schützen und die Fälscher, Versender bzw. Anbieter zur Rechenschaft zu ziehen. Nun lässt sich dieser Anspruch im Internet als transnationalem Netzwerk mit wenigen Kontroll- und Sanktionsmöglichkeiten, verglichen mit der realen Welt, wesentlich schlechter erfüllen (vgl. [Zittrain, 2006]). Deshalb ist Politik aber nicht davon befreit, immer wieder nach neuen, besseren Möglichkeiten zu suchen, diesen Schutz zu gewährleisten. Zwar sind manche Internetspezialisten der Ansicht, dass derjenige, der im Netz nicht selbst für seine Sicherheit Sorge, eben leiden müsse. Individuelles Versagen ist aber kein Grund dafür, dass staatliche Stellen aus der Verantwortung entlassen werden, Bürger nach Recht, Gesetz und Möglichkeit zu schützen. Niemand würde Verständnis dafür haben, dass, sind Schüler nicht aufmerksam genug im Straßenverkehr, die Polizei das zum Anlass nimmt, Geschwindigkeitskontrollen vor Schulen einzustellen.

Auf Gefahren im Netzwerk reagieren viele Nutzer zwiespältig. Einerseits verdrängen sie solche Gefahren um des Genusses willen, so dass nicht jedes Mal die Frage nach der Funktionsfähigkeit und vor allem der persönlichen Sicherheit aufkommt, wenn sie ihre Rechner einschalten. Dazu hat sicher auch beigetragen, dass ein wachsender Teil der Nutzer die Rechner mit Schutzsoftware ausstattet. (Zumindest behaupten das in Deutschland zwischen 80 und 90 Prozent der Nutzer, vgl. [(N)onliner Atlas, 2006].) Sie gibt ihm ein gewisses Vertrauen, sie kann ihn aber auch sorglos machen. Andererseits bleibt bei vielen Nutzern ein Gefühl der Unsicherheit über die Sicherheit im Internet: Vieles bleibt unwägbar, undurchsichtig, und dieses Gefühl trägt mit dazu bei, dass sie ihre Aktivitäten im Netz nicht so entfalten, wie sie das in einem Netz tun würden, das sie als völlig sicher wahrnehmen [Montalbano, 2006].⁴² Diese gefühlte Unsicherheit wird gestärkt durch Erfahrungen mit rätselhaften Computerabstürzen, durch Berichte von Freunden, in Medien und nicht zuletzt durch

⁴¹ Auch Filterprogramme sind kein Allheilmittel, können zu einem Instrument der Einschränkung der Informationsfreiheit werden, bleiben aber ein wichtiges Instrument, wenn sie in geordneter und überprüfbarer Weise entwickelt und eingesetzt werden [Zittrain, 2006].

⁴² Vgl. auch <http://www-03.ibm.com/press/us/en/pressrelease/19154.wss..> Eine Untersuchung in den USA [CSIA, 2005] zeigt, dass die Funktionsfähigkeit des Internets als sehr hoch wahrgenommen (how well is it working?), aber die Sicherheit im Netz (how safe is it?) eher skeptisch gesehen wird.

diverse Studien von Sicherheitsunternehmen über kriminelle Aktivitäten und neuartige Bedrohungen aus dem Netz. Sicherlich trifft es zu, wie Kritiker anmerken, dass es „IT-Sicherheitsanalysen“ gerade der Unternehmen „regnet“, die Sicherheitssoftware verkaufen und die ein Interesse haben, die Gefahren mit grellen Farben zu malen [Garretson, Messmer, 2006]. Aber besorgte, verunsicherte Internetnutzer sind nicht Produkt eines Verkaufstricks oder einem Trugbild aufgesessen. Obwohl es Dissens über Details gibt, stellen auch Sicherheitsbehörden und Computer Emergency Response Teams (CERTs) einen tatsächlichen Anstieg krimineller und sicherheitsgefährdender Aktivitäten fest. Und sie betonen, wie die Politik, dass die Internetsicherheit heute und in Zukunft kein Thema ist, das nur am Rande behandelt werden kann. Soll sich eine Wissensgesellschaft entfalten, nachhaltige Entwicklung durch das Internet gefördert und seine Funktion als zentrale Infrastruktur ausgebaut werden, ist mehr Sicherheit eine notwendige Voraussetzung. Das betrifft sowohl die Sicherheit *im* Cyberspace als auch die *des* Cyberspace. Strittig ist dabei, im welchem Maße und mit welchen Instrumenten dabei die Politik eingreifen muss, die federführend (inter)nationale Sicherheit organisiert, und unter welchem Leitbild die Zusammenarbeit von Staat und Gesellschaft organisiert werden sollte: Ist Internetsicherheit ein Gegenstand der traditionellen Sicherheitspolitik, oder ist angesichts der besonderen Merkmale des Netzwerkes ein anderes Verständnis von Sicherheit notwendig, das wenig staatliche Intervention zulässt und dafür den gesellschaftlichen Akteuren, den Betreibern und Nutzern des Internets, aber auch der Vielzahl der individuellen Nutzer, die größere Verantwortung zuweist?

Die Schwierigkeiten, Internetsicherheit zu gewährleisten, sind vielfältig und haben auch mit der Entstehung des Netzwerkes zu tun. Bei seiner Konstruktion fanden Sicherheitsvorkehrungen wenig Aufmerksamkeit, denn die Erfinder arbeiteten in einer Kultur des Vertrauens in dem kleinen, übersichtlichen Forschungsnetzwerk. Niemand erwartete, dass es zugänglich sein würde für hunderte Millionen Menschen, und dass viele von ihnen seine Funktionsweise erlernen würden, um dann Unerwünschtes, Gefährliches zu tun und das Netz selbst zu bedrohen: „The Internet (...) was designed in a spirit of trust. Neither the protocols for network communication nor the software governing computing systems (nodes) connected to the network were architected to operate in an environment in which they are under attack.“ [PITAC, 2005, S. 7]. Daher hat das Internet heute, wie David C. Clark, ein führender Com-

puterwissenschaftler des renommierten Massachusetts Institute of Technology (MIT) und einer der Erfinder des Netzes feststellt, keinen Sicherheitsrahmen [Markoff, 2005], [Talbot, 2006]. Das regt die Suche nach einem Internet an, das mehr - wenn auch niemals völlige - Sicherheit bieten und deshalb unbesorgter und intensiver genutzt werden kann, von den Bürgern bis hin zu den anderen kritischen Infrastrukturen.

Ein grundlegendes Problem besteht darin, dass es schwer einzuschätzen ist, welchen Gefahren sich künftig das Internet und die IT-Systeme generell gegenübersehen. Nicht nur bestehen Unsicherheiten über den Grad der Gefährdung durch Angreifer. Auch die Entwicklung des Netzwerkes, die ja Einfluss auf seine Verwundbarkeit hat, ist kaum abzusehen. Denn es entwickelt sich technisch schnell, die Software wird komplexer, seine Nutzung wird vielfältiger, und sie kann sich rasch in eine unerwartete Richtung bewegen. Diesen Problemen müssen sich alle stellen, die über ein verändertes Netzwerk nachdenken. Forschungs- und Entwicklungsprogramme wie die Initiative Global Environment for Networking Investigations (GENI) der US-National Science Foundation, der ähnliche Aktivitäten in anderen Ländern folgen, sollen belastbare Perspektiven eröffnen. Ihr Ziel ist es u. a., mit einer relativ kleinen, neuen Netzinfrastruktur, die schrittweise erweitert werden könnte, „(to) enable the vision of pervasive computing and bridge the gap between the physical and virtual worlds by including mobile, wireless and sensor networks (...), to enable control of management of other critical infrastructures“.⁴³

Kritiker befürchten, dass ein verändertes, stärker auf Sicherheit ausgerichtetes Netz auf seine traditionelle Neutralität verzichten würde, sollte es selbst „intelligent“ werden, um etwa Datenpakete auf gefährliche Inhalte für Nutzer und für das Netzwerk zu untersuchen, damit sie rechtzeitig aussortiert werden können. Das sei politisch fragwürdig, da sich Kontrolle und Zensur in das Netz einschleichen könnten. Sie plädieren stattdessen dafür, nicht das Netz, sondern die angeschlossenen Rechner intelligenter und damit sicherer zu machen [Talbot, 2006]. Heftig umstritten sind auch Überlegungen vor allem von Seiten großer Netzbesitzer, aus ökonomischen Gründen die Netzneutralität aufzukündigen. Sie möchten das Internet so umgestalten, dass z. B. die Erreichbarkeit von inhaltlichen Angeboten (etwa durch variierende Ladegeschwindigkeiten) davon bestimmt wird, wie viel Geld ein Inhaltenanbieter an Carrier

⁴³ <http://www.nsf.gov/cise/geni/>; zum wissenschaftsinternen US-Internet2 <http://www.internet2.edu>.

zahlt. Datenpakete könnten also gegen Bezahlung im Netz bevorzugt werden.⁴⁴ Dagegen formiert sich Widerstand in Politik und Gesellschaft, und er schließt nicht nur Anbieter von Inhalten, Dienstleistungen etc. wie Google, Amazon, Microsoft und eBay ein, sondern auch gesellschaftliche Gruppen. Sie haben sich in dem Aktionsbündnis Save the Internet bzw. It's Our Net⁴⁵ zusammengeschlossen. Gerade die zahlreichen kleinen, innovativen, oft individuellen Anbieter von Inhalten fürchten, sich machtlos und benachteiligt dem Oligopol weniger Netzbetreiber gegenüberzusehen. Ein nicht mehr neutrales Internet würde sehr viel Ähnlichkeit mit dem von immer weniger Anbietern beherrschten Fernsehnetz bekommen. Intensiv wird diese Debatte in den USA geführt,⁴⁶ während in anderen Regionen der Welt die Problematik bislang nur zögernd über den Kreis von Expertenzirkeln hinaus angesprochen wird. Inzwischen hat das Thema auch die Europäische Union erreicht.⁴⁷

Ob die Forschungsprogramme und die Überlegungen für neue Netzstrukturen ein neues, auch sichereres Internet hervorbringen, wie stark es sich vom heutigen Netz unterscheiden würde und wie genau es funktionieren könnte, lässt sich angesichts vielfältiger Konzepte, widersprüchlicher Interessen und zahlreicher Beteiligter noch nicht klar erkennen [Eckert, 2004, S. 871ff]. Wahrscheinlich wird dabei auch die künftige Sicherheitslage eine Rolle spielen: Käme es zu einem Angriff, der das Netz großräumig lahm legt, oder würden kriminelle Aktivitäten so überhand nehmen, dass die kommerzielle Netznutzung stark leidet, wäre eine neue politische Ausgangsbedingung geschaffen. Dann erscheint es vorstellbar, dass das offene Internet ersetzt wird durch eine Konfiguration von abgeschlossenen Netzen mit divergierenden Sicherheitsgraden und unterschiedlichen Zugangs- bzw. Nutzungskosten. Viele Netze wären, wenn überhaupt, nur über bewachte Weichen verbunden, an denen alle Datenpakete auf Herkunft, Inhalt und Ziel überprüft würden. Die Vor- und Nachteile einer solchen Konfiguration der Netze sollten schon heute, unter der Randbedingung diverser sicherheitspolitischer Szenarien, exploriert werden.

Es gibt einen breiten Konsens in Politik, Gesellschaft und Wissenschaft, mehr für Internetsicherheit tun zu müssen, ohne dass immer Einigkeit besteht, was genau zu

⁴⁴ In den Simulationen wird ein Netz vorgestellt, das prioritäre Dienste kennt, die der Stabilisierung des Netzwerkes und dem Transport von Datenpaketen kritischer Infrastrukturen dienen.

⁴⁵ <http://www.savetheinternet.com/>, <http://www.itsournet.org/>; vgl. das Stichwort Netneutrality unter http://www.en.wikipedia.org/wiki/Main_Page.

⁴⁶ Vgl. das Hearing vom 7.2. 2006 zum Thema: <http://commerce.senate.gov/hearings/index.cfm>.

⁴⁷ <http://www.heise.de/newsticker/meldung/75524>.

tun ist und welche Auswirkungen das hat. Vor allem in einem Teil der Netzwerkgemeinde, die über Nichtregierungsorganisationen aktiv und kritisch die Entwicklung des Internets begleitet, formieren sich Widerstände, dabei Staat und Politik eine substantielle Rolle zuzugestehen. Das wird besonders spürbar, wenn sicherheitspolitische Aspekte thematisiert werden wie die Nutzung des Internets durch Terroristen, (mögliche) Angriffe von Cyberterroristen und die Suche nach Schutz- und Gegenmaßnahmen. Getrieben von Befürchtungen, das Netz könne einer umfassenden Überwachung, einer Polizei- und Geheimdienstkontrolle unterworfen und in seinen Entwicklungsmöglichkeiten gehemmt werden, bricht sich dann gelegentlich die Neigung Bahn, veränderte sicherheitspolitische Rahmenbedingungen zu ignorieren oder Gefahren kleinzureden, um der Politik keine Legitimation für Eingriffe zu geben - nicht selten ein Nachklang der staatskritischen Visionen von Barlow.

Lange hat die Politik sich nicht um das heranwachsende Internet gekümmert, und erst seit einigen Jahren beginnt sie sich der Aufgabe zu stellen, im Verbund mit Unternehmen und gesellschaftlichen Akteuren mehr Internetsicherheit zu organisieren. Einfach und unstrittig ist das nicht, das Leitbild ist noch nicht ausgemalt, und die bisherigen Resultate des Handelns sind nicht befriedigend. Weder private Nutzer, Unternehmen, Organisationen noch die staatlichen Einrichtungen, die selbst vorbildlich sein wollen, setzen Konzepte und Maßnahmen zum Schutz der Rechner bzw. Netzwerke so um, wie es erforderlich wäre. Die Zwischenbilanz der National Strategy to Secure Cyberspace der USA aus dem Jahre 2003, die weltweit eine vorbildhafte Funktion haben könnte, zeigt, dass auch die Regierungsbehörden ihre Netzwerke nur unzulänglich schützen.⁴⁸ Und eine der verbreiteten Bemühungen, Internetsicherheit zu verbessern, hat ihre Grenzen: Versuche, mittels nachgereicher Programmkorrekturen (patches) die Softwarelücken zu schließen und kriminelle Bedrohungen und Nutzungen des Netzwerkes zu erschweren, hinken oft der Entwicklung der Gefahren nach, schaffen neue Probleme und könnten den stabilen Betrieb des Netzwerkes beeinträchtigen.

Ein zentrales Problem der Internetsicherheit ist der weltumspannende Charakter des Internets. Da Gefahren von jedem Rechner ausgehen können, hängt die Sicherheit des gesamten Netzes und seiner Nutzer davon ab, dass sich die wichtigsten Internetländer gemeinsam darum bemühen, ernsthafte Schwachstellen zu beseitigen. In-

⁴⁸ Vgl. <http://www.whitehouse.gov/pcipb>; kritisch zum Zustand des Schutzes [Pulliam, 2005].

ternationale Zusammenarbeit bei der Cybersecurity ist die politische Kehrseite der weltweiten technischen Netzstruktur. Länder, die nur ein geringes Sicherheitsniveau aufweisen, gefährden das globale Netzwerk und damit alle anderen Staaten und zwingen sie dazu, sich mit hohem Aufwand mehr schlecht als recht gegen Zugriffe und andere Taten zu schützen, die Menschen aus diesen oder über diese Länder versuchen. Dieses Gebot der internationalen Kooperation praktisch umzusetzen, erweist sich, wie in vielen anderen Bereichen der internationalen Politik, als schwierig. Daher bleibt das, was an (durchaus nützlichen) Politiken bzw. Maßnahmen für Internetsicherheit vereinbart und durchgesetzt wird, hinter den Notwendigkeiten zurück. Nicht selten fehlt schon darüber zwischen Staaten ein Konsens, was eine erlaubte oder unerlaubte Nutzung des Netzes ist oder wodurch die Sicherheit des Netzwerkes wirklich gefährdet wird. Und die Durchsetzung des Vereinbarten in einem transnationalen, weitgehend privat betriebenen Netz, das nicht zu überschauen ist, bleibt eine eigene Herausforderung. Trotzdem ist das Bild nicht nur trübe: Politik und Gesellschaft beginnen, die Herausforderungen zu erkennen, und national und international formieren sich Politiken für mehr Internetsicherheit.

In dem vorliegenden Band steht die Sicherheit *des* Internets im Vordergrund, verstanden als die Gewährleistung der Funktions- und Überlebensfähigkeit (survivability) des Netzwerkes selbst. Dabei wird ein spezifischer Aspekt der Aufgabe beleuchtet, die Sicherheit des Internets zu gewährleisten, nämlich die Funktionsfähigkeit des Paketdienstes: Wie gut würde diese grundlegende Dienstleistung des Internets, der Transport von Datenpaketen, noch funktionieren, wenn es zu gezielten Zerstörungen zentraler Austauschknöten (Internet Exchange Points) oder der großen Datenleitungen (Backbones) käme? Dabei werden vor allem Ergebnisse präsentiert, die mit Hilfe des Simulationsmodells Internet Security Simulation (INESS) erarbeitet wurden. Dieses Kapitel dürfte eher Wissenschaftler interessieren, die sich mit Simulationsmodellen und der Internetsicherheit auf tieferen Schichten des OSI-Modells (Open Systems Interconnection Reference Model) befassen. Die Ergebnisse der Simulation zeigen, dass das Netzwerk zwar, wie erwartet, recht redundant ist. Aber es hat in seiner konkreten Topologie einige Schwächen, und würde das Internet sehr intensiv von anderen kritischen Infrastrukturen genutzt, könnte es bei strategischen Angriffen dazu kommen, dass Datenpakete dieser Infrastrukturen teilweise verloren gehen. Beispiele wären die Ausschaltung zentraler Internet Exchange Points oder ein Angriff mit ei-

nem neuartigen Wurm im Kontext eines Internets, das hierarchische Modi des Paketverkehrs kennt.

Da mit INESS vor allem Folgen gezielter Störungen des Paketverkehrs mit strategischer Absicht analysiert wurden, muss der sicherheitspolitische Kontext mit in den Blick genommen werden, mit dem das Internet in Wechselwirkung steht. Dabei findet der schillernde Begriff Cyberterrorismus großes Interesse in Gesellschaft und Politik. Er wird vor dem Hintergrund der Debatte über die Erfordernisse von Internetsicherheit im zweiten Kapitel kritisch analysiert. Dabei wird deutlich werden, dass Terroristen das Internet zwar schon ausgiebig nutzen, aber noch nicht zu ihrem Angriffsziel erkoren haben. Jedoch sollte Cyberterrorismus nicht leichtfertig als reines Phantasieprodukt betrachtet werden, ebenso wenig wie ein Alarmismus angemessen wäre, der zu Überreaktionen führt. Sachgerecht ist eine Politik, die eine neue Gefährdung der Sicherheit wahrnimmt, die erst im Entstehen und deren Wirksamkeit noch nicht klar abzuschätzen ist. Wachsende Gefahren können davon herrühren, dass sich in den nächsten Jahren Kulturen und Organisationsformen sich herausbilden, die ihr Wissen um die Funktionsweise, die infrastrukturelle Bedeutung und ihre Vertrautheit mit dem Internet nutzen, um diese Infrastruktur selbst und mit ihr verbundene kritische Infrastrukturen zum Ziel von Cyberangriffen zu machen.

Internetsicherheit ist aber nur ein Ausschnitt des Politikfeldes Sicherheit von Informations- und Kommunikationssystemen, das zu den übergeordneten Politiken und Maßnahmen zum Schutz kritischer Infrastrukturen gehört. Da dieser Infrastrukturschutz immer öfter als Teil der nationalen Sicherheit bzw. des Heimatschutzes diskutiert wird, wird auch die Politik zum Schutz kritischer (Informations-) Infrastrukturen generell, ihre Entwicklung und ihre Einbindung in die Sicherheitspolitik im ersten Kapitel beleuchtet. Danach wird das Internet als eine (potentiell herausragende) kritische Infrastruktur unter den IuK-Infrastrukturen sowie die Entwicklung der Cybersecurity-Politik in das Zentrum gestellt. Dabei offenbart sich ein Phänomen: Obwohl sich die Internetsicherheit verschlechtert und Cyberterrorismus zumindest als mögliche Gefahr gesehen wird, zeigen Staat und Politik sehr viel Zurückhaltung und Gelassenheit beim Schutz dieser immer wichtigeren Infrastruktur. Während andere Bereiche, die für nationale Sicherheit und Heimatschutz wichtig sind, zunehmend politisch reguliert werden, bleibt Internetsicherheit bislang zu einem guten Teil eine Aufgabe der Privaten, die kooperativ mit staatlichen Stellen und möglichst ohne deren Regulierung gewährleistet werden soll. Auch wenn es dafür gute Gründe gibt,

werden Stimmen lauter, die bezweifeln, dass das auf Dauer so bleiben kann angesichts einer sich verschärfenden Gefährdung der Internetsicherheit.

Viele kritische Infrastrukturen sind schon heute, mehr oder weniger, mit dem Internet und immer mit anderen Informations- und Kommunikationssystemen unterfüttert, die selbst aber (noch) nicht immer mit dem digitalen Netzwerk verbunden sind. Soll die Sicherheit dieser IuK-Infrastrukturen analysiert werden, genügt es daher nicht, sich nur mit Internetsicherheit zu beschäftigen. Erforderlich ist die spezifische Betrachtung der jeweiligen Infrastruktur und der spezifischen Konfiguration der Informations- und Kommunikationssysteme (vgl. [Sonntag, 2005]). Das ist hier nicht zu leisten. Trotzdem ist die Untersuchung der Verfügbarkeit des Pakettransports im Internet bei Störungen ein zwar kleiner, aber methodisch belastbarer Beitrag zur Analyse der Sicherheit einer solchen kritischen Infrastruktur.

Die Internetsicherheit als drängende Aufgabe

Zu Beginn des 21. Jahrhunderts wird immer deutlicher, dass das Internet dabei ist, zu einer wichtigen, vielleicht sogar zu - neben dem Stromnetz - der zentralen kritischen Infrastruktur zu werden. Die Diskussion über die Gefährdung und Sicherung solcher Infrastrukturen ist keinesfalls neu, sie war schon implizit ein Thema in der Zeit des Kalten Krieges, und sie fand nach seinem Ende einen neuen Fokus unter veränderten Rahmenbedingungen: Zu diesen Rahmenbedingungen zählen sicherheitspolitische (neuer transnationaler Terrorismus),⁴⁹ gesellschaftliche (Deregulierung, Privatisierung von Infrastrukturen) und technische (Digitalisierung der IuK-Systeme).

Vor allem in den USA wurden seit den 80er Jahren neue Bedrohungen, ihre Quellen, Formen und ihre Implikationen für die kritischen Infrastrukturen debattiert [Bendrath, 2003]. Diese Debatte fand anfangs bescheidene politische und gesellschaftliche Aufmerksamkeit und wurde mit starker technischer Ausrichtung geführt. In den frühen 90er Jahren gewann eine sicherheitspolitische Diskussion an Gewicht, die sich mit der Bedrohung durch Angriffe von Terroristen, aber auch von unberechenbaren Staaten (rogue states bzw. states of concern; vgl. [Schmittchen, 2006]) auf die neuen Informations- und Kommunikationsinfrastrukturen beschäftigte (Cyberwar). Terroristische Anschläge auf das World Trade Center im Jahre 1993 und ein Gebäude der US-Bundesbehörden in Oklahoma-City im Jahre 1995⁵⁰ fachten zwar die Debatte über den Schutz kritischer Infrastrukturen an, und eine Kommission machte dem Präsidenten dazu Vorschläge [PCCIP, 1997]. Aber sie blieben ohne grundlegende Auswirkungen auf den Infrastrukturschutz und seine Institutionen. So gingen die USA mit einem nicht ausreichend verzahnten, lückenhaften Gefüge von Institutionen und Programmen, die nur dürftige Resultate für den Infrastrukturschutz brachten, in das neue Jahrhundert. Die Terroranschläge des 11. September 2001 brachten eine Wende der Politik: In scharfen Diskussionen und durch die Arbeit von Experten-

⁴⁹ Grenzüberschreitende Zusammenarbeit terroristischer Gruppen gab es schon in den 70er Jahren, meist unter Anleitung palästinensischer Organisationen und mit Unterstützung arabischer Staaten. Als relativ neu gilt der fundamentalistische transnationale Terrorismus [Cronin, 2003]. Transnationaler Terrorismus ist gekennzeichnet durch ideologisch durchtränkte Netzwerkstrukturen mit hoher Flexibilität, aber geringer Formalisierung und Hierarchisierung [Schneckener, 2006]. Spencer [2006] bezweifelt, dass es überhaupt neuen Terrorismus gibt und betont seine Kontinuität. Überwiegend ist Terrorismus heute ein innerstaatliches Problem, das sehr oft mit Separatismus verbunden ist.

⁵⁰ Vgl. zu Taten und Tätern die MIPT Terrorism Knowledge Base: <http://www.tkb.org/Home.jsp>.

gremien wurden Mängel des Heimat- und Infrastrukturschutzes offenbart und Gegenmaßnahmen eingeleitet. Die Etablierung des Department of Homeland Security (DHS)⁵¹ im Jahre 2003 war die größte Reorganisation der US-Bundesbehörden seit 1947, als durch den National Security Act⁵² das alle Teilstreitkräfte umfassende Department of Defense (DoD) und die Central Intelligence Agency (CIA) etabliert wurden. In dem zentralen bundesstaatlichen Ministerium für Heimatschutz mit 180 000 Beschäftigten werden 22 Behörden und Organisationen in einem Stufenplan zusammengeführt [Maxwell, 2004] - ein, wie sich zeigt, äußerst schwieriger Prozess mit bislang noch nicht überzeugenden Ergebnissen. Das DHS soll auf der Grundlage zentraler strategischer Dokumente,⁵³ in Kooperation mit den meist privaten Betreibern, die Sicherheit der kritischen Infrastrukturen gewährleisten und ihre Funktionsfähigkeit rasch wiederherstellen, sollten Angriffe auf sie doch erfolgreich sein – nicht nur für die USA eine Herausforderung [Powner, Rhodes, 2006]. Dabei ist das DHS Teil eines geschichteten Sicherheitskonzepts der USA: Die nach Außen gerichtete (auch präventive) Verteidigung gegen Terrorismus und staatliche Bedrohungen auf internationaler Ebene wird ergänzt durch die Sicherung der Grenzen, die Abwehr des Terrorismus innerhalb des Landes, durch Überwachungsmaßnahmen (domestic terrorist surveillance) sowie durch den Schutz der Infrastrukturen. Dominierend beim Schutz kritischer Infrastrukturen, selbst nach 9/11, ist dabei das zivile Leitbild einer Kooperation von Staat und privaten Betreibern der Infrastrukturen.

Auch wenn vergleichbarere Konzeptionen eines umfassenden Sicherheitskonzeptes erst in der Phase der Ausarbeitung sind,⁵⁴ bewegen sich viele Staaten in diese Richtung. Deutschland widmet sich seit den 80er Jahren explizit dem Schutz kritischer (Informations-) Infrastrukturen, wenn auch nicht mit der gleichen politischen Virulenz und wissenschaftlichen Aufmerksamkeit die USA.⁵⁵ Vorrangig zuständig für den Schutz ist das Innenministerium (BMI) und seine nachgeordneten Einrichtungen. Involviert sind auch das Wirtschaftsministerium über seine Regulierungsbehörde (Bun-

⁵¹ <http://www.dhs.gov/>.

⁵² Text: <http://www.iwar.org.uk/sigint/resources/national-security-act/1947-act.htm>.

⁵³ National Strategy for Homeland Security, National Strategy to Secure Cyberspace; National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, unter <http://www.whitehouse.gov>.

⁵⁴ Für die EU vgl. die Europäische Sicherheitsstrategie von 2003 A secure Europe in a better world; <http://ue.eu.int/uedocs/cmsUpload/78367.pdf>.

⁵⁵ Dort finden sich die meisten „Experten“, was sich auch in der Publikationsdichte widerspiegelt.

desnetzagentur)⁵⁶ sowie das Justizministerium. Schon 1989 wurde das Informations-technologie-Sicherheitsrahmenkonzept verabschiedet, 1991 das BSI als nachgeordnete Behörde des BMI gegründet, in dem Kompetenzen zum Schutz der Informationssysteme gebündelt wurden, die seit den 80er Jahren unter der Ägide des Innenministeriums zusammengeführt worden waren. 1998 wurde die interministerielle Arbeitsgruppe zum Schutz kritischer Infrastrukturen KRITIS eingerichtet, die eng mit den Infrastrukturbetreibern zusammenarbeitet.⁵⁷ In den letzten Jahren legte die Bundesregierung Konzepte zum Schutz kritischer (Informations-) Infrastrukturen vor (vgl. [BSI, 2005]): das Basisschutzkonzept für kritische Infrastrukturen, erarbeitet vom Innenministerium und seinem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)⁵⁸, dem Bundeskriminalamt (BKA) und der Privatwirtschaft [BMI, 2005]); den Nationalen Plan zum Schutz von Informationsinfrastrukturen, an dem ebenfalls unter Führung des BSI diverse staatliche und gesellschaftliche Akteure beteiligt waren [NPSI, 2005]. In einem Umsetzungsplans KRITIS werden, in enger Abstimmung mit den betroffenen Unternehmen, konkrete Maßnahmen erarbeitet, diese Infrastrukturen zu schützen, ein gleichmäßiges Niveau der IT-Sicherheit zu gewährleisten und die Kooperation während und nach Angriffen sicherzustellen, um die Netze in Betrieb zu halten oder rasch wieder flicken zu können.⁵⁹ Außerdem gibt es neue rechtliche Regelungen, die den bislang unzulänglichen, meist durch Generalklauseln abgedeckten Schutz kritischer Infrastrukturen verbessern⁶⁰ bzw. die Computerkriminalität präziser definieren.⁶¹ Dazu kam der Aufbau von Information Technology Information Sharing and Analysis Center,⁶² von CERTs: dem Forschungs-CERT,⁶³ dem CERT der Bundesbehörden,⁶⁴ des Mittelstandes⁶⁵ und weitere, die den deutschen CERT-Verbund bilden.⁶⁶ Diverse gesellschaftlich-politische Aktivitäten zur Internetsicherheit, zur Meldung krimineller Aktivitäten im Netz und zur Information der Nutzer über Ge-

⁵⁶ <http://www.bundesnetzagentur.de>.

⁵⁷ <http://www.bsi.de/fachthem/kritis/>.

⁵⁸ Das BBK ist für den physischen Schutz zuständig; vgl. <http://www.bbk.bund.de/>.

⁵⁹ Zur Planung für die Umsetzungsplan: <http://www.bsi.de/literat/faltb/F17KritischeInfrastruktur.htm>; vgl. den Vortrag von Michael Hange, erreichbar durch die Suchfunktion von <http://www.dgap.org>.

⁶⁰ <http://www.gesetze-im-internet.de/stgb/index.html>;

⁶¹ Sie umfasst im deutschen Recht die Computermanipulation, -spionage bzw. den Softwaredienstahl, die Computersabotage und unbefugte Computernutzung [Tinnefeld, Ehmann, 1998, S. 458f].

⁶² <https://it-isac.org/>

⁶³ <http://www.dfn-cert.de>.

⁶⁴ <http://www.bsi.bund.de/certbund/index.htm>.

⁶⁵ <http://www.mcert.de>.

⁶⁶ <http://www.cert-verbund.de/index.html>.

fahren und den Umgang mit ihnen ergänzen die Bemühungen (vgl. [Abele-Wigert, Dunn, 2006, I, S. 107ff]).⁶⁷

Nach den Erfahrungen des 11. Septembers und den folgenden terroristischen Aktionen haben weitere hochindustrialisierte Staaten, Schwellenländer, aber auch internationale Organisationen bzw. Gremien ebenfalls begonnen, den Infrastrukturschutz insgesamt und den Schutz kritischer Informationsinfrastrukturen speziell als ernstzunehmendes Aufgabenfeld unter neuen Bedingungen zu etablieren. Zu erwähnen sind auf internationaler Ebene besonders die Organisation für Wirtschaftliche Zusammenarbeit und Entwicklung (OECD), die Gruppe der acht führenden Industriestaaten (G8) sowie die Europäische Union. Andere regionale Organisationen wie die der Amerikanischen Staaten oder die Gemeinschaft Asiatischer Staaten widmen dem Problem hingegen deutlich weniger Aufmerksamkeit.⁶⁸ (Jedoch hat der Malaysische Premier auf dem World Congress on Information Technology im Jahre 2006 eine - noch vage beschriebene - International Multilateral Partnership against Cyberterrorism angeregt, die Staaten und Unternehmen zusammenbringen und sich mit „training, security certification, and research and development“ befassen soll.)⁶⁹ Zwar agieren die Staaten bzw. Organisationen beim CI(I)P mit unterschiedlicher Intensität, variierenden Politiken, Maßnahmen, Instrumenten und divergierenden Verantwortlichkeiten der Administrationen, aber es ist Bewegung in die Politik gekommen und einige Tendenzen zur Abstimmung der Politiken sind erkennbar (vgl. ausführlich mit Länderstudien [Abele-Wigert, Dunn, 2006], ferner [CISP, 2004], [Commission, 2005, 2004], [Brömmelhorster, Fabry, Wirtz, 2003], [Ritter, Weber, 2002]).

Die Staaten der EU bewegen sich zwar langsamer als nötig, aber im Vergleich mit außereuropäischen Staaten recht rasch auf eine mehr abgestimmte Politik zu: Der Ansatz der EU ist in dem Politikfeld, das sich mit dem Schutz der Infrastrukturen und dem Schutz vor Terrorismus befasst, konsultativ und koordinierend. Denn sie muss im Rahmen vorhandener Strukturen auf der Basis zwischenstaatlicher polizeilicher und justizieller Zusammenarbeit formuliert und umgesetzt werden. Die Kompetenzen

⁶⁷ Vgl. etwa die von Unternehmen, Gruppen und der Politik getragene Initiative Deutschland sicher im Netz: <https://www.sicher-im-netz.de/>, die von Internetunternehmen getragene no abuse in Internet - Initiative (<http://www.naiin.org/de>) und die Initiative D21 (<http://www.initiaved21.de>).

⁶⁸ Zur OECD: http://www.oecd.org/departement/0,2688,en_2649_34223_1_1_1_1_1,00.html; zur EU: <http://register.consilium.eu.int/pdf/en/05/st13/st13882.en05.pdf>; zur G8-Lyon/Roma-Gruppe: <http://www.auswaertiges-amt.de/diplo/de/Aussenpolitik/GlobaleHerausforderungen/Institutionen/G8-Lyon-Gruppe.html>; zur ASEAN: <http://www.aseansec.org/6269.htm>; zur Empfehlung einer cybercrime-Expertengruppe der OAS von 1999 vgl. <http://www.oas.org>.

⁶⁹ http://www.symantec.com/en/aa/about/news/release/article.jsp?prid=20060627_01.

liegen bei den Staaten, die EU-Kommission hat kein Initiativrecht, und das EU-Parlament ist in den wesentlichen Punkten nicht beteiligt [Gusy, Schewe, 2003], [Monar, 2004]. Innereuropäische Politiken und Maßnahmen stützen sich primär auf die Grundlagen und Mittel zur Bekämpfung grenzüberschreitender Kriminalität, und ein den USA vergleichbares gemeinsames und geschichtetes Schutzkonzept, das auch eine gemeinsame Verteidigungspolitik enthält, ist erst in einem schwierigen Prozess der Herausbildung [Dalgaard-Nielsen, 2004]. Das ist auch unterschiedlichen Wahrnehmungen der neuen Sicherheitslage zu verdanken: In den USA sieht nach 9/11 eine dominierende politische und gesellschaftliche Majorität das Land in einem neuartigen, von den Völkerrechtsregeln nicht erfassten Krieg, auch wenn im täglichen Leben der USA, trotz einiger Eingriffe in Bürgerrechte, davon nur punktuell etwas zu spüren ist, in der Tagespolitik wieder andere Themen in den Vordergrund drängen und das politische System seine alten Mechanismen und Konflikte reaktiviert hat. Europäer neigen noch mehrheitlich dazu, die Terroranschläge als, wenn auch außergewöhnlich schwere, kriminelle Tat einzuordnen. Diese Fokussierung auf Kriminalität auch eine gute Seite. Sie lässt raschere Fortschritte zu, verglichen mit der noch schwergängigeren gemeinsamen Verteidigungspolitik, und hat dazu beigetragen, dass die europäischen Staaten im internationalen Vergleich führend sind beim Cyberkriminalitätsrecht [Gross, 2005].

Aber das Thema kritische Infrastrukturen bleibt nicht auf die traditionelle sicherheitspolitische Agenda beschränkt. Es beeinflusst scheinbar davon unberührte Themen, Folge des Querschnittscharakters, den diese Infrastrukturen für Politik und Gesellschaft haben. So beginnt allmählich die Einsicht Fuß zu fassen, dass Bemühungen um nachhaltige Entwicklung nur erfolgreich sind, wenn Gefährdungen der Sicherheit kritischer Infrastrukturen erkannt und bewältigt werden [Gheorghe, 2003].

Nachhaltige Entwicklung und Sicherheit sind verwoben

Sicherheit ist ein mehrdeutiger, positiv besetzter Wert, ein Ziel, das Individuen und Kollektive anstreben, und eine analytische Kategorie. Daher muss der Begriff präzisiert und inhaltlich ausgefüllt werden, um ihn nutzbar zu machen (vgl. etwa [Haftendorn, 1991]). Gleiches gilt auch für den Begriff nachhaltige Entwicklung, der seit etwa fünfzehn Jahren geradezu inflationäre Verwendung findet und schrittweise in diversen Kontexten zu operationalisieren versucht wird [Banse, Kiepas, 2005], [Coenen,

Grunwald, 2003] [Hake, Schlör, 2003].⁷⁰ Oft wird übersehen, dass Sicherheit, verstanden als staatliche Handlungs-, Abwehr- und Gestaltungsfähigkeit nach Innen und Außen, und nachhaltige Entwicklung in Wechselwirkung stehen: Nachhaltige Entwicklung benötigt (relative) Sicherheit, und Sicherheit bedarf nachhaltiger Entwicklung, damit sie erfolgreich produziert werden kann. Sind politisch-gesellschaftliche, auf unabsehbare Zeit staatlich organisierte Systeme gefährdet, instabil oder ist ihr internationales Umfeld hochgradig unsicher, entfaltet sich Nachhaltigkeit nicht. Zugleich können nationale Systeme bzw. die internationalen Beziehungen nur sicher, also relativ friedlich und stabil sein, wenn Politik und Gesellschaft, national und international gestaltend, Pfade der Nachhaltigkeit beschreiten, die zu weniger Gefährdungen und unkontrollierbaren Konflikten führen.

Nun werden Zusammenhänge von Nachhaltigkeit und Sicherheit vor allem im Kontext regionaler Entwicklungen seit dem Brundtlandbericht [World Commission, 1987] intensiv diskutiert. Insbesondere die Auswirkungen von Umweltveränderungen und Ressourcenübernutzung für das konflikthafte Zusammenleben kleinerer sozialer Einheiten in südlichen Regionen des Globus finden starkes Interesse,⁷¹ und die Forschung bemüht sich um konzeptionelle und methodische Fortschritte, um auch sicherheitspolitische Folgen des Globalen Wandels zu verstehen. Dabei finden auch die (noch vagen) Zusammenhänge von Klimawandel und Konflikt viel Aufmerksamkeit.⁷² Aber systematische Analysen, die Staaten und das internationale System in den Blick nehmen und berücksichtigen, welche Wechselwirkungen zwischen technologischer Innovation, Nachhaltigkeit, (inter)nationaler Politik und Sicherheit sowie ihrer Ressource Macht⁷³ bestehen, gibt es erst in den letzten Jahren [Barnett, Duvall, 2005].

Einen Anstoß für viele dieser Analysen gibt der erweiterte Sicherheitsbegriff, der sich seit den 70er Jahren schrittweise herausgebildet und den traditionellen Begriff der Sicherheit verändert hat, der die Abwesenheit von Krieg meint. (Inzwischen ist auch von vernetzter Sicherheit die Rede.) Stationen dieser Erweiterung sind in den 70er Jahren die Sicherheit der Rohstoffversorgung (wirtschaftliche Sicherheit, vgl. [Hager,

⁷⁰ Richter [2005] sieht hingegen in Nachhaltigkeit ein diskursives Konzept.

⁷¹ Vgl. das Literaturverzeichnis des Institute of Development Studies, <http://www.iisd.org/ic/info/ss9608.htm>.

⁷² Vgl. <http://www.bmu.de>, Suchbegriff Climate Change and Conflict.

⁷³ Was Macht kennzeichnet, ist nicht wirklich klar. Neben harten (ökonomischen, militärischen), weichen Machtmitteln (Diplomatie, Kultur) werden Faktoren benannt wie die Beeinflussung der Agenda, Rechtsetzung, organisatorische Fähigkeiten eines Landes, Institutionen.

1976]), seit den 80er Jahre die Sicherheit der Umwelt (ökologische Sicherheit, vgl. [Homer-Dixon, 1991]), in den 90er Jahre die Sicherheit der menschlichen Entwicklung (human security, vgl. [Owen, 2004])⁷⁴ und insbesondere nach 2001 die Sicherheit und der Schutz kritischer Infrastrukturen. Dieser sich immer mehr erweiternde Sicherheitsbegriff ist umstritten: Zwar verdeutliche er zu Recht, dass die tradierte Trennung zwischen innerer und äußerer Sicherheit obsolet sein und vielfältige Faktoren und Prozesse, auch ökologische Veränderungen, eine Ursache zwischenstaatlicher Gewalt sein können. Aber er trage die Gefahr in sich, dass deshalb weitere Bereiche des Zusammenlebens der (inter)nationalen Sicherheitspolitik untergeordnet und damit militarisiert werden [Brock, 2005]. Zudem erhöhe das neue Verständnis die Anforderungen an Politik, gesellschaftliche Prozesse so zu steuern oder zumindest so zu beeinflussen, dass die Lösung der neuen Sicherheitsprobleme gelingt. Das könnte rasch in eine Überforderung der Politik umschlagen. Sie tut sich zudem oft schwer, innovative Instrumente einzusetzen, die berücksichtigen, dass viele der Ressourcen, die zur Beeinflussung sozialer Prozesse nötig sind, in den Händen (transnationalen) gesellschaftlicher Akteure liegen (Wissen, Kapital, Technik). Diese Akteure verfügen damit über mehr Gestaltungs-, aber auch Blockadepotential. Deshalb ist es offen, ob Konzepte der politisch-gesellschaftlichen Aushandlung und Gestaltung, die oft mit dem Begriff global governance umschrieben werden (vgl. [Zürn, Zangl, 2004], [Kopfmüller, 2003]),⁷⁵ wirklich dazu führen, dass die Probleme, die nachhaltiger Entwicklung im Wege stehen, besser bewältigt werden können.

Trotzdem findet der Begriff erweiterte Sicherheit inzwischen im Politik und Gesellschaft breite Verwendung. Mit seinen Erweiterungen deckt der Sicherheitsbegriff nun die Politikfelder (Säulen) ab, die für nachhaltige Entwicklung eine zentrale Rolle spielen, nämlich Wirtschaft, Umwelt, und, so kann man wesentliche Elemente von human security definieren, Soziales. Die Sicherheit der Infrastrukturen ist eine Herausforderung, die quer zu den drei Säulen liegt. Sie ist notwendige Voraussetzung für die Sicherung der menschlichen Existenz als soziales Wesen, für die Sicherung des gesellschaftlichen Produktivkapitals sowie für die Gewährleistung der inneren und

⁷⁴ Das Konzept wurzelt im UN-Millennium Summit (2000). Human Security formuliert Bürger-, Teilnahme- und Schutzrechte als Anspruch an Politik und Gesellschaft (<http://www.humansecurity-chs.org/index.html>). Sicherheit wird bei human security als economic-, health-security etc. definiert; der klassische Sicherheitsbegriff (innere und äußere Sicherheit) findet dabei keine Aufmerksamkeit.

⁷⁵ Für eine Einführung in den gleichfalls unbestimmten Begriff vgl. Enquete-Kommission des Bundestages Globalisierung der Weltwirtschaft, http://bundestag.de/gremien/welt/glob_end/10.html.

äußeren Entwicklungs- und Handlungsmöglichkeiten eines Landes. Sie werden zu einem guten Teil, aber nicht vollständig und abhängig vom jeweiligen politischen Kontext, von seinen harten Machtpotentialen bestimmt. Nun wird in den Diskussionen über nachhaltige Entwicklung zu oft stillschweigend angenommen, dass jegliche Ausformulierung von Nachhaltigkeit, auch von starker Nachhaltigkeit,⁷⁶ tragfähige Infrastrukturen und genug, auch harte, Machtressourcen erzeugen werde, die mit dazu beitragen, dass sich ein Staat international behaupten kann. Das könnte sich freilich bei einigen Konzepten von Nachhaltigkeit, die z. B. hoffen, die Elektrizitätsversorgung weitgehend auf Erneuerbare aus Wüstenregionen stützen zu können,⁷⁷ als Illusion erweisen. Konzepte starker Nachhaltigkeit betrachten oft die heutigen Infrastrukturen, insbesondere das Energiesystem, nicht auch als eine Quelle von Macht, sondern nur als Hindernisse für den Aufbau eines neuen Systems der Energiegewinnung, das sich den natürlichen Stoffströmen anschmiegen müsse.

So ist die Gewährleistung nationaler und internationaler Sicherheit generell und die Sicherheit kritischer Infrastrukturen speziell eine vernachlässigte Dimension der Debatte über nachhaltige Entwicklung. Weder in der Vergangenheit noch heute weisen die Diskurse über Nachhaltigkeit und Infrastrukturschutz breite und substantielle Berührungen auf. Der Schutz kritischer Infrastrukturen wird eher von denen diskutiert, die sich in der traditionellen sicherheitspolitischen Agenda zurechtfinden, zu der diejenigen kaum Zugang haben, die in der ökologisch, ethisch und sozialpolitisch geprägten Nachhaltigkeitsdebatte eingebunden sind, die wiederum Sicherheitsexperten oft fremd bleibt. Ähnliches ist im politischen Raum zu beobachten, in dem es nicht wirklich gelingt, eine institutionelle Voraussetzung nachhaltiger Entwicklung umzusetzen, nämlich Ressortgrenzen zu überwinden. Eine Verknüpfung von Nachhaltigkeits- und Sicherheitsfragen stößt hier, trotz einiger Ansätze zu ressortübergreifender Politikformulierung, weiter auf Hindernisse. Daher ist die infrastrukturell-sicherheitspolitische Dimension nachhaltiger Entwicklung ein in Politik und Fachwelt zu wenig erkundetes und gestaltetes Terrain.

⁷⁶ Sie betonen ökologische Grenzen und lehnen die Substitution von Umwelt durch Kapital ab. Der ökologische Fußabdruck ist oft Maßstab dieses Konzepts; vgl. <http://www.footprintnetwork.org/>.

⁷⁷ Vgl. etwa den Vorschlag über eine solare Vollversorgung für Europa; http://www.eurosolar.de/de/index.php?option=com_content&task=blogcategory&id=15&Itemid=25.

Kritische Infrastrukturen benötigen Schutz

Die sicherheitspolitische Diskussion hat in vielen Ländern zu einer breiten politischen und gesellschaftlichen Übereinstimmung darüber geführt, dass der Schutz kritischer Infrastrukturen eine drängende Aufgabe ist, die besser gelöst werden muss, langfristig auf der Tagesordnung bleibt. Das führt nicht nur zu einer neuen Sicherheitsforschung, sondern auch zu Diskussionen darüber, was kritische Infrastrukturen sind und welche Merkmale sie kennzeichnen.

Die neue Sicherheitsforschung entfaltet sich langsam in den europäischen Staaten und im Rahmen der Forschungsaktivitäten der EU, und das Internet ist als eine dieser kritischen Infrastrukturen ein Gegenstand der Forschungen: Im Fünften Forschungs-Rahmenprogramms der EU von 1998 bis 2002 wurden entsprechende Arbeiten im Rahmen des Information Society Technologies-Programms angestoßen, und das Sechste und das anstehende Siebente Rahmenprogramm widmen sich ebenfalls dem Schutz der kritischen Infrastrukturen.⁷⁸ Bedeutsam sind auch das European Security Research-Program bzw. die europäische Taskforce CI²RCO, die Forschungen und Entwicklungen speziell zum Schutz kritischer Informationsstrukturen fördern und koordinieren sollen.⁷⁹ Auch in Deutschland gibt es Bewegung. 2006 wurde die erste nationale Sicherheitsforschungskonferenz durchgeführt, die von dem Fraunhofer Verbund Verteidigungs- und Sicherheitsforschung organisiert wurde.⁸⁰ Sie fand wohlwollende Zustimmung der Forschungsministerin Schavan.⁸¹ Lange hat sich ein Teil des deutschen Wissenschaftsbetriebs mit sicherheitspolitischen Themen schwer getan, die allzu leicht in den Verdacht gerieten, einer Militarisierung Vorschub zu leisten. Erst allmählich bewegt sich der Betrieb in Richtung auf Forschungen, die dem Heimatschutz dienen,⁸² und er könnte sich anschicken, wenigstens einen Teil der Lücke zu schließen, die die deutsche Forschung in diesem Themenfeld insbesondere im Vergleich zu den USA offenbart. Dazu müssen die Wirtschafts- und Sozialwissenschaften integriert und Reformen der bisherigen Struktur der Verteidigungsforschung umgesetzt werden. Ab 2007 wird das Forschungsministerium Mittel für die-

⁷⁸ http://ec.europa.eu/enterprise/security/articles/article_2006-09-25-kf_en.htm; <http://www.rp6.de/>.

⁷⁹ <http://www.ci2rco.org/>.

⁸⁰ <http://www.vvs.fraunhofer.de/de/downloads/future-security.htm>.

⁸¹ Vgl. http://www.vvs.fraunhofer.de/de/downloads/future-security/Rede-Schavan_mr_20060704.pdf.

⁸² Auch die Unternehmen beginnen hier aktiv zu werden; vgl. das BITKOM-Forschungsprojekt: http://bitkom.org/de/themen_gremien/37269.aspx.

ses neue Forschungsfeld bereitstellen, das sich u. a. mit der Gewährleistung der Internetverfügbarkeit beschäftigt.

Für Forschungsprogramme, auch über die enge Sicherheitsforschung hinaus, gibt es genug Themen. Schon der Begriff Infrastruktur, der aus der Fachsprache des französischen Eisenbahnbaus des 19. Jahrhunderts stammt, ist facettenreich [Simonis, 1977], [Jochimsen, 1966], und das, was eine Infrastruktur kritisch macht, ist von technischen und politischen Abschätzungen bzw. Bewertungen abhängig [Sonntag, 2005]. Zwar gibt es relativ breit geteilte Vorstellungen darüber, welche materiellen Strukturen und Institutionen⁸³ zu den kritischen Infrastrukturen zählen. Aber keine Übereinstimmung herrscht immer darüber, welche Komponenten innerhalb der als kritisch definierten Infrastrukturen eine besondere Verwundbarkeit aufweisen, wie stark die (inter)nationalen Auswirkungen einer Störung wären, worin die größten Risiken für diese Infrastrukturen liegen (Unfällen, Naturkatastrophen, Terrorismus), wie viel Schutz genug ist, wer ihn vorrangig gewährleisten soll, und aus welcher Perspektive diese Entscheidungen getroffen werden sollen - aus der von Unternehmen und Privaten oder der staatlicher Politik? (vgl. [Metzger, 2004], [Metzger, 2004a], [Reinermann, Weber, 2001]).

Trotz solcher Anfragen gibt es eine Reihe von Infrastrukturen, die Staaten in ihren politischen Verlautbarungen, rechtlichen Regelungen, Programmen und Maßnahmen gleichermaßen als kritisch bezeichnen [Abele-Wigert, Dunn, 2006], [Dunn, 2005], [Dunn, Wigert, 2004], [Commission, 2004]. Dem liegt ein pragmatisches Verständnis von kritischen Infrastruktur zugrunde: Sie müssen zuverlässig und effizient Dienstleistungen erbringen für Individuen, Gesellschaft und für den Staat mit seinen Gewährleistungsfunktionen wie Verteidigung, innere und wirtschaftliche Sicherheit, öffentliche Gesundheit [Moteff, Copeland, Fischer, 2003]. Jedoch konnte sich der Vorschlag [Metzger, 2004a] bislang nicht durchsetzen, angesichts eines solchen funktionalen Verständnisses nicht von kritischen Infrastrukturen, sondern von "critical services robustness" oder „critical services sustainability“ zu sprechen.

Infrastrukturen stehen in einem Spannungsfeld: Sie ermöglichen es Menschen, ihre Dienstleistung zu nutzen und am gesellschaftlich-politischen Leben teilzuhaben, oder sie schließen Menschen aus, weisen sie Mängel auf oder erfordern sie hohe Zu-

⁸³ Der Begriff umfasst Behörden etc., kann aber auch Normen, Regeln etc. einschließen, die soziales Leben erst ermöglichen. Trotz ihrer Bedeutung gelten sie nicht als kritische Infrastrukturen, und sie werden hier nur im Zusammenhang mit dem Begriff hybride Infrastruktur kurz thematisiert.

gangskosten. Entsprechend sensibel werden ihre Entwicklung und Ausgestaltung wahrgenommen. Da sie zugleich gesellschaftlich-politische Handlungsfähigkeit bzw. staatliche Machtentfaltung dienen, können sich hier Konflikte aufbauen. Ein einfacher, egalitärer Zugang für Individuen zu Infrastrukturen und ihre Nutzung als Quelle von Macht für den Staat müssen nicht immer vereinbar sein. Und Schutzmaßnahmen können individuelle Zugangskosten erhöhen und Nutzungsformen und -dauer für Gruppen verändern. Wie viele Ressourcen für den Aufbau, Erhalt und Schutz in welche Infrastrukturen fließen, kann deshalb ein Gegenstand innerstaatlicher Kontroversen sein. Sie könnten sich besonders verschärfen, wenn die Infrastrukturen und ihre Leistungen dem erwarteten Bevölkerungsrückgang in vielen Regionen Europas angepasst werden müssen.

Die Definition des Anti-Terrorismugesetzes der USA, *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* [Patriotic Act, 2001], das der Kongress nach 9/11 erließ und Anfang 2006 in wesentlichen Punkten zeitlich unbegrenzt fortschrieb, greift die Dienstleistungsfunktion von kritischen Infrastrukturen auf: „... the term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters...“. Schon 1996 zählte die Administration Clinton diese kritischen Infrastrukturen offiziell auf [E.O. 13010].

Die Kommission der EU hat ein vergleichbares Verständnis: “Critical infrastructures consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the member states. Critical infrastructures extend across many sectors of the economy, including banking and finance, transport and distribution, energy, utilities, health, food supply and communications, as well as key government services.” [Commission, 2004, S. 3]. Sie nennt auch Kriterien, die Infrastrukturen kritisch machen: “The loss of a critical infrastructure element is rated by the extent of the geographic area which could be affected by its loss or unavailability - international, national, provincial/territorial or local. Magnitude - the degree of the impact or loss can be assessed as none, minimal, moderate or major. Among the criteria which could be used to assess potential magnitude are: (a) Public impact (amount of popu-

lation affected, loss of life, medical illness, serious injury, evacuation); (b) Economic (GDP effect, significance of economic loss and/or degradation of products or services); (c) Environmental (impact on the public and surrounding location); and (d) Interdependency (between other critical infrastructure elements). (e) Political (confidence in the ability of government); Effects of time - This criteria ascertains at what point the loss of an element could have a serious impact (i.e. immediate, 24-48 hours, one week, other). However, in many cases, psychological effects may escalate otherwise minor events." [Commission, 2004, S. 5]. Zwar liegt die Kompetenz im Politikfeld Infrastrukturschutz in der EU bei den Staaten, aber die Kommission kann eine koordinierende, anregende Funktion einnehmen, wie sie das mit ihrem (rechtlich unverbindlichen) Grünen Papier zum European Programme for Critical Infrastructure Protection (EPCIP) tut [Commission, 2005],⁸⁴ um gemeinschaftliches Handeln für CIP zu fördern. Ihre Definitionsversuche sollen zudem den Staaten helfen, nationale Listen kritischer Infrastrukturen zu erstellen, deren Zusammenschau die transnationalen Verflechtungen und wechselseitigen Abhängigkeiten in Europa zeigen, um dann Vorsorge und Krisenplanung zu betreiben. Hier soll dem Critical Infrastructure Warning Information Network (CIWIN)⁸⁵ die Aufgaben zufallen, innerhalb der EU Informationen über Bedrohungen dieser verflochtenen Infrastrukturen, über Maßnahmen, Strategien für ihren Schutz auszutauschen. CIWIN könnte sich über seine Funktion als Forum des Austausches auch in Richtung auf ein schnelles Alarmierungs- und Kommunikationssystem bei Krisen und Angriffen entwickeln und damit dem US-Critical Infrastructure Warning Information Network ähneln.⁸⁶ Die präzise Aufgabenstellung des CIWIN ist noch zu definieren. Jedoch soll es vorhandene Netze weder ersetzen noch duplizieren. CIWIN ist mit der European Network and Information Security Agency⁸⁷ verbunden. ENISA wurde 2004 vorerst nur bis zum 31.12.2008 eingerichtet, dürfte aber dieses Datum überleben. Als ein Zentrum der Expertise widmet sie sich dem Schutz der Informationsinfrastrukturen und des Internets. Obwohl verbindliche Definitionen fehlen und Unterschiede bei Politiken und Maßnahmen zu ihrer Absicherung zu erkennen sind, zeigen die Dokumente, dass es ei-

⁸⁴ Dem soll Ende 2006 ein Kommissionsvorschlag für den Rat folgen.

⁸⁵ <http://www.euractiv.com/Article?tcmmuri=tcm:29-140597-16&type=LinksDossier>.

⁸⁶ CWIN ist ein unabhängiges, überlebensfähiges Netzwerk für Sprache und Daten ist, das „no logical dependency on the Internet or the Public Switched Network“ hat (<http://www.continuitycentral.com/news01838.htm>). Als virtuelles Peer-to-Peer Netz könnte es aber physikalische Verbindungen zum öffentlichen Netz haben.

⁸⁷ <http://www.enisa.europa.eu/>; <http://europa.eu/scadplus/leg/en/lvb/l24153.htm>.

nen Kern von Infrastrukturen gibt, die überall als kritisch bezeichnet werden. Sie wurden schon in E.O. 13010 aufgezählt: Banken und Finanzen, Regierung, Telekommunikation, Notfalldienste (Polizei, Feuerwehr, Rettungsdienst), Energie- bzw. Elektrizitätsversorgung, Gesundheitssystem, Verkehr und Transport, Wasserversorgung [Abele-Wigert, Dunn, 2006, I, S. 388f]; [Dunn, 2005, S. 14]. Dieser Liste wurden in den USA und einigen anderen Staaten besonders gefährdete Einzelanlagen hinzugefügt, z. B. aus dem Chemie-, Nuklearbereich, aber auch kritische Symbole (national monuments). Ihre Zerstörung würde das Selbstvertrauen der Bürger und das Vertrauen in ihr Land und seine Institutionen besonders erschüttern. Solche Symbole sind gemäß des National Infrastructure Protection Plans⁸⁸ der USA beispielsweise die Golden Gate Bridge und das Kapitol. Viele andere Länder haben vergleichbare Symbole, die im- oder explizit als potentielle Anschlagziele besonderen Schutz finden.

Nun ist diese Auflistung kritischer Infrastrukturen von begrenztem Nutzen, da sie nahezu alles enthält, was moderne Gesellschaften an materiellen Infrastrukturen bzw. an Organisationen mit infrastrukturellen Funktionen aufzuweisen haben. Enthält sie noch Sportstadien, findet sie breiteste öffentliche Zustimmung. Eine solche Liste hilft jedoch nicht viel weiter, wenn nicht drei Probleme gelöst werden:

- Eine Hierarchie der kritischen Infrastrukturen zu erstellen, die ihre funktionale Bedeutung für die Lebensfähigkeit eines Landes abbildet.
- Eine Beschreibung der besonders kritischen Komponenten innerhalb jeder Infrastruktur zu verfassen, denn nicht alle sind für die Funktionsfähigkeit gleich wichtig. Nicht jeder Ausfall eines Unternehmensnetzes, nicht jede Störung der Stromversorgung in einer Region ist ein Problem, dem sich nationale (Sicherheits-) Politik widmen muss. Eine Konzentration auf die für (inter)nationale Sicherheit essentiell wichtigen, besonders verwundbaren Schlüsselkomponenten würde wirksames politisches und gesellschaftliche Handeln erleichtern, die Kosten des Infrastrukturschutzes reduzieren und die Rolle der Politik klären helfen. „A more realistic picture that identified the small number of key infrastructure facilities that might be at risk from cyber attacks could have clarified the scope and role of government action and made the problem more manageable.“ [Lewis, 2005, S. 827].

⁸⁸ Vgl. <http://ni2ciel.org/NIPC/Revised-Draft-NIPP-v2.0.pdf>. Erstellt wurde der Planentwurf federführend durch das National Infrastructure Protection Center, NIPC, der Bundespolizei FBI.

- Ein dynamisches Verständnis der Interdependenzen dieser kritischen Infrastrukturen zu entwickeln. Unterschieden werden Verflechtungen innerhalb einer Infrastruktur und zwischen Infrastrukturen. Intra-Interdependenzen kennzeichnen insbesondere den Elektrizitätssektor, den Flug- und Schienenverkehr, und sie könnten auch im Internet wirksam sein.⁸⁹ Störungen an einer Stelle können sich innerhalb der Infrastruktur rasch fortpflanzen, wie das bei Zusammenbrüchen von Stromnetzen in Nordamerika und Europa [Krey, Markewitz, Vögele, 2005], [Farrell, Zerriffi, Dowlatabadi, 2004]⁹⁰ der Fall war. (Zu den Netzzusammenbrüchen trugen weitere Faktoren wie Kommunikationsprobleme sowie unzulänglicher Echtzeit-Datenaustausch bei, deren Beseitigung die jetzt schon meist hohe Widerstandsfähigkeit (Resilienz)⁹¹ der Netze weiter erhöhen kann.) Bei Inter-Interdependenzen können Verknüpfungen zwischen Infrastrukturen dazu führen, dass sich Störungen in einer Infrastruktur auf weitere Infrastrukturen ausbreiten. Solche Kaskadeneffekte werden immer wieder als große Risiken für kritische Infrastrukturen bezeichnet.

Nur wenn diese Aufgaben gelöst sind, können die Ressourcen und Maßnahmen für den Schutz kritischer Infrastrukturen sachgerecht auf die verwundbarsten Punkte und Einrichtungen der Infrastrukturen konzentriert werden, deren Ausfall weit reichende Folgen für ein Land und über es hinaus hätte. Leicht wird ihre Lösung freilich nicht sein. Denn die Infrastrukturen stützen im unterschiedlichen Ausmaß die Funktionen ab, die ein Staat gewährleisten soll [Moteff, Copeland, Fischer, 2003]. So sind, zumindest kurzfristig, funktionierende Finanzinfrastrukturen für die wirtschaftliche Sicherheit, aber nicht für die Verteidigung und die öffentliche Gesundheit von vorrangiger Bedeutung, die aber von einer funktionierenden öffentlichen Wasserversorgung abhängt, die wiederum für Verteidigung nicht von höchster Priorität ist. Verteidigung und wirtschaftliche Sicherheit hängen von Verkehrsinfrastrukturen ab, die für die öffentliche Gesundheit nicht die gleiche Bedeutung haben. Das gilt auch für die IuK-Infrastruktur, obwohl in einigen Ländern eine elektronische Vernetzung des Gesundheitsbereichs abgestrebt wird, die Chancen zur Kostenreduzierung, aber auch neue Gefährdungen bringt. Offensichtlich ist, dass eine funktionierende Elektrizitätsinfrastruktur für alle anderen Infrastrukturen essentiell ist. Ihr Ausfall löst Kaskadeneffekte

⁸⁹ Vgl. dazu das Simulationskapitel.

⁹⁰ Vgl. auch den kurzen Überblick <http://www.thgweb.de/lexikon/Stromausfall>.

⁹¹ Der aus Psychologie und Pädagogik stammende Begriff wird bezeichnet hier die (verschieden ausgeprägte) Fähigkeit eines Systems, seine gestörten Funktionen rasch wieder herzustellen.

aus und kann erhebliche Sicherheitsprobleme verursachen. (Dass dabei der gesellschaftliche Kontext wichtig ist, zeigen zwei Ereignisse: Zwar waren die materiellen Schäden durch den Stromausfall im Münsterland im November 2005 mit möglicherweise über 100 Mio. Euro hoch, aber es gab es zu keinem Zeitpunkt ernsthafte Probleme etwa durch ausufernde Kriminalität. Das war anders bei einem Stromausfall in New York-City im Sommer 1977, als es zu Plünderungen kam.) Stark betroffen von einem Stromausfall wäre auch der Verkehrssektor. Der größte Teil des Schienenverkehrs bliebe liegen, Ampelanlagen und Zapfsäulen würden ausfallen, was die Versorgung mit Lebensmitteln etc. beeinträchtigen würde. Aber der Ausfall der Elektrizität kann für Infrastrukturen mehr oder weniger gravierend sein, je nachdem, ob z. B. Notstromversorgung verfügbar ist und wie lange sie funktioniert. Der Katastrophenschutz kann punktuell Notstromgeräte betreiben, und Krankenhäuser, aber auch wichtige Komponenten der Internetinfrastruktur verfügen über Notstromaggregate bzw. -batterien. Sie können jedoch nur eine recht kurze Zeit überbrücken [Jantsch, 2000]. Das zeigte sich bei dem Angriff auf New York 2001, der zum Zusammenbruch der Stromversorgung im Süden Manhattans für einige Tage⁹² führte. Die Notstromaggregate des Internetdienstleisters Telehouse in New York arbeiteten zwei Tage, fielen dann aber aus, Internetverbindung zwischen Europa bzw. Afrika und den USA wurden beeinträchtigt. Zudem hängen die Endgeräte der Internetnutzer, die das Ziel der meisten Datenpakete sind, nahezu vollständig vom Stromnetz ab. Aber auch die Elektrizitätsversorgung steht nicht für sich allein und ist auf funktionierende Informations- und Kommunikationssysteme, auf funktionierende Gasnetze und partiell auch auf Steinkohle-Transportwege angewiesen.

Solche Kaskadeneffekte sowie deren spezifische regionale Folgen lassen sich bis zu einem gewissen Grad vorhersehen. Ihre detaillierten Auswirkungen aber sind nur schwer zu kalkulieren. Sicherlich haben Arbeitsgruppen wie KRITIS in Deutschland, in denen Infrastrukturbetreiber, weitere Unternehmen und Behörden zusammenarbeiten, einiges an Wissen angesammelt, so wie das in den meisten OECD-Staaten der Fall ist. Trotzdem dürfte auch hier nicht alles bekannt sein über die tatsächlichen, relevanten physikalischen und informationstechnischen Verknüpfungen der Infrastrukturen, ihre verwundbaren Punkte und über ihre Widerstandsfähigkeit auch gegen Störungsimpulse, die von anderen Infrastrukturen ausgehen. Das wäre nicht ü-

⁹² Diese kurze Dauer zeigt, dass der Elektrizitätssektor in allen hoch entwickelten Staaten gut auf großflächigere Störungen vorbereitet ist und Erfahrungen hat, wie sie zu bewältigen sind.

berraschend angesichts komplexer, sich verändernder, vielfach verflochtener Infrastrukturen und der Schwierigkeiten, die immer wieder modifizierte Einbindung und Stellung wichtiger Techniken, Unternehmen bzw. Behörden in diesem Geflecht zu erfassen. Gerade der Informations- und Kommunikationsbereich weist hier eine hohe Dynamik auf. Die Öffentlichkeit kann ohnehin den Grad der Resilienz des infrastrukturellen Gefüges nicht einschätzen, da KRITIS (wie alle anderen Gremien des Infrastrukturschutzes weltweit) keine detaillierten Informationen in die Öffentlichkeit dringen lässt, um Geschäftsgeheimnisse zu hüten und um potentiellen Angreifern kein sensitives Wissen zuzuspielen.

Selbst wenn ausreichende Daten über solche infrastrukturellen Verknüpfungen vorliegen, reichen Planspiele [Hutter, 2004] nicht aus, die Kaskadeneffekte, ihre Folgen und Reaktionen auf diese Störungen darstellen. Zusätzlich ist die Analyse der Interdependenzen durch Modellbildung und Simulation notwendig, um die Prozesse wirklichkeitsnahe und nachvollziehbar zu machen. Bislang verfügen nur die USA über die dafür notwendigen Simulationsmodelle [Cha, 2005], [Brown, Beyeler, Barton, 2004], [Wimbish, Sterling, 2003]. Sie sind im EU-Raum erst in der Entwicklung.⁹³

Nicht nur unzulängliches Wissen erschwert es, eine Hierarchie kritischer Infrastrukturen zu definieren, Schutzmaßnahmen festzulegen und Ressourcen zuzuweisen. Dazu tragen auch divergierende Interessen und ein politischer Prozess bei, der dazu neigt, sich auf das zu konzentrieren, was unter dem Eindruck aktueller Ereignisse und durch einflussreiche Interessen als vorrangige Gefahr festgelegt wird.

Die USA mit ihrem Anspruch, Vorreiter zu sein beim Schutz kritischer Infrastrukturen, zeigen das beispielhaft. Dort wird CIP im Rahmen des Heimatschutzes nach 9/11 einseitig unter dem Paradigma terroristischer Bedrohung betrieben. Natürliche Katastrophen sind zwar nicht konzeptionell vernachlässigt, denn der 2005er National Response Plan⁹⁴ „to manage domestic incidents“ deckt als „all hazard“-Plan neben Terrorismus auch Großunfälle sowie Naturkatastrophen ab. (Das deutsche Basischutzkonzept [BMI, 2005] ist ein vergleichbarer Ansatz.) Praktisch und organisatorisch wurden Naturkatastrophen aber vernachlässigt, wie die Überschwemmungen im Süden der USA während des Hurrikans Katrina im Sommer 2005 offenbarten: Deiche waren schlecht gepflegt, zu niedrig, und die bundesstaatliche Katastrophen-

⁹³ Vgl. die Beiträge auf dem International Workshop On Complex Network and Information Infrastructure Protection 2006: <http://ciip.casaccia.enea.it/cnip06/index.jsp?sel=program> .

⁹⁴ Text: http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0566.xml.

schutzorganisation FEMA⁹⁵ war dem auf Terrorismusabwehr fokussierten DHS unterstellt. Es hatte den all hazards-Ansatz nicht umgesetzt und konnte nur verzögert und anfangs nicht wirksam genug eingreifen [Holdeman, 2005]. Auch in der EU ist noch nicht festgelegt, auf welche Gefährdung(en) der Schutz kritischer Infrastrukturen ausgerichtet werden soll. Im ihrem grünen Papier nennt die Kommission [Commission, 2005, S. 3] drei Ansätze für den Infrastrukturschutz: Einen „all-hazards approach for everything“, einen „all-hazards approach with a terrorism priority“ und einen „terrorism hazards approach“.⁹⁶ In welchem Ausmaß sich die Schutzmaßnahmen dieser drei Ansätze unterscheiden würden, lässt sich nur teilweise absehen. Zumindest für den physischen Schutz bei Informations- und Kommunikationssystemen dürfte die Entscheidung für einen Ansatz Konsequenzen haben: Werden natürliche Risiken stärker berücksichtigt, müssen mehr Ressourcen in den physischen Schutz fließen, denn die physischen Komponenten der Infrastrukturen sind eine Achillesferse bei Naturkatastrophen. Dagegen würde ein Ansatz, der auf Terrorismus fokussiert ist, es nahe legen, Mittel zu konzentrieren auf die Verhütung und Abwehr von Software-, Hackerangriffen etc. auf Netzwerke.

Aber auch im Rahmen einer Schutzpolitik, die sich wie die USA (faktisch) für einen Ansatz entscheidet, besteht keine Garantie, dass er optimal umgesetzt wird. Die im Senat der USA repräsentierten regionalen Interessen erschweren es, die Finanzmittel, die von der Bundesregierung für den Schutz bereitgestellt werden, auf die durch Terrorismus gefährdeten Regionen und ihre Infrastrukturen zu konzentrieren [Marks, 2005].⁹⁷ Jede Region möchte in den Genuss bundesstaatlicher Mittel kommen, so abgelegt sie sein mag. In den USA ist daher die Diskussion kontrovers über vorrangige infrastrukturelle Schutzbereiche, über Maßnahmen und ihre adäquate Finanzierung. Außerdem wird sie von aktuellen Ereignissen beeinflusst, etwa den terroristischen Anschlägen in Madrid 2004 und London 2005 auf Verkehrssysteme [Bellavita, 2005], [Chaddock, 2005].

Auch in anderen Staaten, darunter Deutschland, sind Klagen zu hören über unzulängliche Strukturen und etablierte Interessen. Kritiker beklagen, dort stabilisiere die föderale Struktur eine überholte Trennung von Zivilschutz (Bund) und Katastrophenschutz (Länder und Landkreise bzw. Kommunen), die eine Bewältigung großer

⁹⁵ <http://www.fema.gov/>.

⁹⁶ Das Premium Homeland Security Konzept der BITKOM [2005] verfolgt einen all hazards-Ansatz.

⁹⁷ Vgl. auch den Leitartikel <http://www.nytimes.com/2006/06/02/opinion/02fri1.html?th&emc=th>.

Schadensereignisse erschwere, etwa großräumiger, länger anhaltender Störungen der Infrastruktur (vgl. [Werthebach, 2004], [Vielhaber, Kubovcsik, 2005]). Hinter dieser Trennung stecke ein herkömmliches Bild von Krieg und Verteidigung als zwischenstaatlicher Konflikt: Der Bund wird vorrangig tätig, wenn Deutschland durch fremde Streitkräfte angegriffen wird und der Verteidigungsfall eintritt. In dieses Bild ließen sich Bedrohungen durch terroristische Angriffe unter den gegebenen verfassungsrechtlichen Bedingungen nur einfügen, wenn sie als kriegerisches Ereignis, als militärischer Angriff definiert würden, die den Verteidigungsfall auslösen. Diese Einordnung wurde vom deutschen Verteidigungsminister Franz Josef Jung angeregt⁹⁸ in der in Politik und vor Gericht geführten Debatte um ein Gesetz, das u. a. den Abschuss eines als Waffe eingesetzten Flugzeuges durch die Bundeswehr regeln sollte, sich aber in diesem Punkt als verfassungswidrig erwies.⁹⁹ Befürworter einer Aufhebung der Trennung verweisen zudem darauf, dass die Nordatlantische Verteidigungsorganisation nach 9/11 erstmals den Bündnisfall nach Artikel 5 Nato-Vertrag feststellte.¹⁰⁰ Damit sei, zumindest deklaratorisch, die Beschränkung des Bündnisfalls auf einen zwischenstaatlichen Konflikt überwunden worden. Der Widerstand gegen solche Überlegungen ist jedoch ausgeprägt und wird u. a. damit begründet, dass Polizeikräfte von Ländern und Bund in der Regel in der Lage seien, terroristische Bedrohungen zu bewältigen. Wären sie überfordert, stünde gemäß Notstandsgesetzgebung die Bundeswehr zur Unterstützung zur Verfügung. Dagegen wird eingewandt, dass § 87a Abs. 4 Grundgesetz¹⁰¹ ihren Einsatz nur zum „Schutze von zivilen Objekten und bei der Bekämpfung organisierter und militärisch bewaffneter Aufständischer“ zulässt, was die unterstellte terroristische Gefahrenlage nicht wirklich erfasse. So würde ein (sehr hypothetischer) erfolgreicher Cyberangriff auf die IuK-Infrastrukturen und über sie auf weitere kritische Infrastrukturen, durch den das Land gelähmt würde, einen rechtlich einwandfreien Einsatz der Bundeswehr nicht zulassen.

Diese Debatte über die Rolle der Streitkräfte beim Schutz der kritischen Infrastrukturen und im Rahmen einer Bewältigung der Folgen terroristischer Angriffe, die zum Teil der spezifischen verfassungsrechtlichen Situation Deutschlands zu verdanken

⁹⁸ Vgl. das Interview: http://www.bundesregierung.de/nn_774/Content/DE/Interview/2006/05/2006-05-02-verteidigung-neu-definieren.html.

⁹⁹ Vgl. das Urteil des Bundesverfassungsgerichts zum Luftsicherheitsgesetz von 15. Februar 2006: http://www.bundesverfassungsgericht.de/entscheidungen/rs20060215_1bvr035705.html.

¹⁰⁰ <http://www.nato.int/docu/comm/2001/0109-hq/0109-hq.htm#sp>.

¹⁰¹ Text: <http://www.bpb.de/wissen/VGB5GU,0,0,Gesetze.html>.

ist, wird aber auch in anderen Ländern, etwa den USA [Weston, 2006], [Elsea, 2003], geführt. Sie wird auf der Agenda bleiben und stark beeinflusst werden von der Entwicklung des transnationalen Terrorismus. Welche Bedeutung diese Diskussion künftig für die Cybersecurity haben wird, zumindest soweit es um die Verhütung und Abwehr von Cyberangriffen geht, lässt sich noch nicht absehen. Könnten und sollten die Streitkräfte künftig explizit beauftragt werden, auch die zivilen Netzwerke, speziell das Internet, zu verteidigen - gegen Cyberangriffe durch Staaten, aber auch gegen Angriffe, die eine neue Generation von Terroristen mit dem Ziel durchführen könnte, das Netzwerk und andere kritische Infrastrukturen funktionsunfähig zu machen? Wären solche Operationen mit dem Kriegsvölkerrecht vereinbar, das eine Unterscheidung von Kombattanten und Nichtkombattanten bzw. von zivilen und militärischen Objekten fordert? [Hoch, 2001] Deckt dieses Recht überhaupt diese Form der Auseinandersetzung ab [Brown, 2006]? Kämen die Gegenangriffe rechtzeitig, oder müssten sie präventiv erfolgen, da sonst kritische Infrastrukturen schon Schaden erlitten hätten [Jensen, 2002]? Und könnten sie im Cyberspace überhaupt so gezielt gegen die Angreifer gerichtet werden, dass das zivile Internet weiter funktioniert [Blanke, 2005], [Gaudin, 2004]? Denn die Wege der Cyberangriffe können getarnt, über viele Rechner geführt werden, ohne dass deren Besitzer das bemerken. Wären die Ziele für einen Gegenangriff nicht präzise zu benennen, wäre er schwer einzugrenzen und seine Wirkung für das gesamte Netzwerk kaum zu kalkulieren. Es gibt also eine Reihe offener Fragen.

Das Internet wird zu einer kritischen Infrastruktur

Informations- und Kommunikationssysteme, zu denen vor allem feste und mobile Telefonnetze gehören, sind schon lange kritische Infrastrukturen. Das gilt für hoch entwickelte Industrieländer wie Deutschland (vgl. [NPSI, 2005], [BITKOM, 2005]), für Schwellenländer, aber auch für die große Zahl der Entwicklungsländer. Dort sind Mobilfunknetze in Ballungsgebieten oft eine der wenigen funktionierenden Infrastrukturen sind. Außerdem werden zu diesen IuK-Systemen privat genutzte, abgeschlossene IP-Netzwerke, das öffentliche Internet und seine Endgeräte, etwa Computer, und die Satelliten- und Richtfunksysteme gezählt. Oft gelten auch Supervisory Control and Data Acquisition Systems (SCADA) zu den IuK-Systemen. Diese integrierten Fernsteuerungs- und Fernüberwachungssysteme stellen die Verbindungen her zwischen Leitstellen und diversen physikalischen Einrichtungen mit ihren techni-

schen Prozessen, von Industrieanlagen bis hin zu Kläranlagen und Dämmen. Dabei nutzen SCADA, die zunehmend IP basiert sind, teilweise auch das öffentliche Internet. Verglichen mit dem Aufbau eigener Netze ist das kostengünstiger [Fisher, 2005]. SCADA sind oft - und wie manche behaupten zu Unrecht - dem Verdacht ausgesetzt, durch Cyberangriffe sehr gefährdet zu sein.

In den letzten Jahren haben sich die Informations- und Kommunikationssysteme insgesamt stark verändert und damit die Möglichkeit eröffnet, sie alle in ein einziges IP-Netz zu integrieren. Von Bedeutung sind dabei technische Entwicklungen wie:

- die Digitalisierung, also die Zerlegung von Daten in ihre elementaren Bausteine (Binary Digits oder Bits);¹⁰² dadurch können unterschiedliche Übertragungswege zugunsten eines Netzes entfallen;
- die steigende Verarbeitungs- und Speicherkapazität der Mikroelektronik;¹⁰³
- neue breitbandige Übertragungstechnologien, die Kosten senken. Diese Kostenentwicklung, die verbreitet im IuK-Bereich zu beobachten ist, wird von weltweiten Prozessen der (regulierten) Deregulierung und Marktöffnung gefördert [ITU, 2005a].¹⁰⁴

In Internet bündeln sich diese Veränderungen, so dass es seine Vorzüge ausspielen kann, wie sich an der Voice over IP (VoIP)¹⁰⁵ zeigt, den Telefongesprächen, die über das Internet geführt werden und die einen wachsenden Marktanteil haben. Da Datenpakete ausgetauscht werden, muss nicht mehr, wie bei einem herkömmlichen Telefongespräch, eine exklusive Verbindung zwischen den Teilnehmern geschaltet werden. Datenleitungen stehen vielen Gesprächspaketen offen. Das reduziert die Kosten. VoIP kann prinzipiell das alte Telefonsystem überflüssig machen und den Sprachverkehr in das Internet überführen. Das würde seine Bedeutung unter den kritischen Infrastrukturen deutlich steigern [GAO, 2004], [Robinson, 2003]. Dem Internet wird sogar nachgesagt, dass es sich zu einer Infrastruktur der Infrastrukturen entwickeln kann, vergleichbar mit dem Elektrizitätsnetz [Fox, Anderson, Rainie, 2005], [Global Trends, 2000], [Beck, 2000]. Dann könnten andere Infrastrukturen das Internet nutzen, um auch solche Daten schnell und kostengünstig zu transportieren, die essentiell für ihr eigenes Funktionieren sind.

¹⁰² <http://www.de.wikipedia.org/wiki/Bit>.

¹⁰³ Das Moore-Gesetz über integrierte Schaltungen vgl. <http://www.heise.de/newsticker/meldung/58525>.

¹⁰⁴ Für Europa vgl. die Independent Regulators Group (IRG): <http://irgis.anacom.pt/site/en/>.

¹⁰⁵ Vgl. http://www.en.wikipedia.org/wiki/Voice_over_IP.

In welchem Ausmaß das Internet heute schon diese zentrale Funktion einnimmt, lässt sich auch für die Staaten nicht exakt bestimmen, in denen die Internetnutzung in nahezu allen Lebensbereichen verbreitet ist. Da der Anschluss an das Internet einfach ist, ohne zentrale Registrierung auskommt, und vielfältige Aktivitäten in eigener Regie über das Netz abgewickelt werden, gibt es nur Schätzungen bzw. statistische Erhebungen über die Internetnutzung. Solche Zahlen geben nur erste Hinweise darauf, welche Bedeutung das Netzwerk hat und wie abhängig Staat und Gesellschaft von ihm sind. Geeignete Maßstäbe dafür zu finden ist nicht einfach: Sind qualitative Experteneinschätzungen auf der Grundlage von Erfahrungswerten aus einzelnen Unternehmen, von Verbänden ausreichend? Oder bedarf es breiter empirischer Daten, wie werden sie erhoben und welche könnten es sein? Ist die Abhängigkeit eine Funktion der Datenmenge, die über das Netz transportiert wird, der Häufigkeit der Nutzung pro Einwohner und Tag, des Nutzungsprofils, des Platzes, den das Internet bei der Erledigung der alltäglichen Routineaktivitäten einnimmt? Oder erwächst Abhängigkeit aus der Bedeutung, die das Netz für spezifische kritische Anwendungen von Unternehmen, Behörden etc. hat, und welche sind das? Wird Abhängigkeit an ökonomischen Kriterien gemessen, etwa dem Umsatz von Unternehmen oder Wirtschaftssektoren über das Netzwerk? Oder spielen subjektive Kriterien eine Rolle, also das Gefühl der Nutzer, irgendwie abhängig zu sein vom Internet? - dann wäre schon der Ausfall der E-Mails für ein, zwei Tage für viele Nutzer eine kaum zu schulternde Last.

Heute verläuft die Diskussion über die Bedeutung des Internets als kritische Infrastruktur und die Folgen, die sein Ausfall hätte, zwischen zwei Positionen, und irgendwo dazwischen kann eine realistische Einschätzung ihren Platz finden. Die eine sieht in einem breiteren Ausfall des Internets für einige Tage ein unangenehmes, möglicherweise kostspieliges, aber zu bewältigendes Erschwernis des Lebens. Die andere Position, die weitergreifende und anhaltendere Störungen erwartet, befürchtet gravierende bzw. potentiell katastrophale Auswirkungen.

Ein Grund für diese Divergenz besteht darin, dass sich nicht nur die Einschätzung der Bedeutung des Netzwerkes für das tägliche Tun unterscheidet, sondern auch die Beurteilung der Abhängigkeit kritischer Infrastrukturen von Internet. Während z. B. Freeman, Dynes, Golodner [2005] für den Verkehrssektor nur eine geringe, für die Telekommunikation eine stärkere, für den Bereich Banken eine hohe und für andere

Infrastrukturen wie Elektrizität und den Öffentlichen Sektor¹⁰⁶ einen variierenden Grad der Abhängigkeit sehen, zeichnet Leggate [2005] ein anderes Bild: Nimmt man den Anteil an den Einnahmen als Maßstab, den Firmen in den jeweiligen Infrastrukturen über das Internet erzielen, ist die Abhängigkeit des Finanzsektor vom Internet an geringsten, während sie beim Telekommunikations- und Transportsektor höher ist und steigt. Schließlich bezweifelt Lewis [2005], dass es überhaupt Sektoren gibt, die heute essentiell auf das Internet angewiesen sind. Hier bleibt also genügend Raum für Empirie, Analyse und sachliche Bewertung. Solche Sachlichkeit ist auch geboten, weil Medien, die Aufmerksamkeit auf sich lenken wollen, nicht selten die Diskussionen um die potentiellen Gefahren eines „digitalen Pearl Harbor“ oder eines „Cyber 9/11“, ausgelöst insbesondere durch Cyberterroristen, gierig aufgreifen, sie zuspitzen und suggerieren, schon heute sein das Internet einer solchen Gefahr ausgesetzt [Keith, 2005]. Das ist aber keinesfalls der Konsens von Experten oder der Politik.

Solche Überspitzungen können schädlich sein, falls sie die Aufmerksamkeit und die Ressourcen auf ein Ereignis fokussieren, dessen Eintrittswahrscheinlichkeit schon umstritten ist. Aber ihre breite Ablehnung ist kein Grund für zufriedenes Zurücklehnen. Auch wenn es nicht sicher ist, dass viele kritische Infrastrukturen zur Zeit ganz wesentlich auf ein jederzeit ungestört funktionierendes Internet essentiell angewiesen sind, so wickeln sie doch eine wachsende Zahl von internen und nach Außen gerichteten Interaktionen über das Netzwerk ab. Und es gibt keine objektive, vorgegebene technische oder institutionelle Grenze, die eine Nutzung des Internets beschränkt. Dazu kommt die Kostenersparnis, die mit einer Internetnutzung verbunden sein kann. Unternehmen im Wettbewerb reizt dieses Sparpotential, ebenso wie die chronisch finanziell knappen öffentlichen Einrichtungen.¹⁰⁷ Freilich nutzen Regierung, Behörden nicht immer diese Einsparungsmöglichkeiten bei den Betriebskosten, da sie die hohen Investitionskosten scheuen.

Die Verflechtung des Netzwerkes mit allen Bereichen des Lebens ist in vollem Gang, und ein Ende ist nicht in Sicht. Deshalb kann das Internet als kritische Infrastruktur im Ausbau bezeichnet werden, als eine sich entfaltende Grundlage einer anvisierten

¹⁰⁶ Für essentielle Kommunikationsbedürfnisse haben viele Regierung eigene Netze (in Deutschland das Berlin-Bonn Information Network, vgl. http://www.kbst.bund.de/Anlage304110/pdf_datei.pdf). Solche Netze können physikalisch oder nur logisch, durch Software, vom Internet getrennt sein. In diesem Fall sind erfolgreiche Cyberangriffe aus dem öffentlichen Internet nicht auszuschließen.

¹⁰⁷ Vgl. zum eGovernment-Angebot <http://www.deutschland-online.de/>; zu den partizipativen und demokratisierenden Aspekten von e-government vgl. [Winkel, 2004].

prosperierenden Wissensgesellschaft. Sie soll wirtschaftliche Sicherheit, soziale Entwicklung, Umweltschutz, politische, kulturelle Attraktivität und - quasi im Ergebnis - auch Macht gewährleisten, eine „Währung der Politik“.

Kommt dem Internet (künftig) eine solche zentrale Funktion und eine Rolle als Treibstoff für Machtentfaltung zu, kann es nicht überraschen, dass es in den Blick militärischer Institutionen gerät, zumal sie das Internet verstärkt für ihre Kommunikation nutzen. So heißt es in einem Dokument des Verteidigungsministerium der USA, dass das Internet ein weltweites Gemeinschaftsgut (global common) ist, von dem Bedrohungen abzuhalten und dessen Nutzung auch während und nach Angriffen sicherzustellen ist. Damit wird es der Hohen See, dem Internationale Luft- und dem Weltraum gleichgestellt [DoD, 2005].

Um ein Gemeinschaftsgut zu sein, müsste das Internet dadurch charakterisiert sein, dass es nicht in (nationales) Eigentum gebracht werden kann, es keine rivalisierende Nutzung kennt, und es keinen systematischen Nutzungsausschluss gibt. Gegen seine Charakterisierung als Gemeinschaftsgut spricht, dass seine physikalische Infrastruktur in privatem Eigentum und die Nutzung nicht frei ist, da der Netzzugang Geld kostet. Für die Charakterisierung spricht, dass technisch gesehen das Internet alle Datenpakete gleich behandelt, offen ist und niemand per se von seiner Nutzung ausschließt, der über einen Rechner und einen Netzzugang verfügt. Und die meisten seiner Inhalte stehen den Nutzern kostenlos zur Verfügung, trotz vielfältiger Bemühungen, ihre Zahlungsbereitschaft zu erhöhen. Zwar hat der größte Teil der Menschen nicht die Mittel, sich dem Internet anzuschließen. Aber das alleine spricht nicht gegen das Merkmal global common, denn auch der Zugang etwa zur Hohen See, nach UNO-Seerechtskonvention ein kollektiv verwaltetes Erbe der Menschheit,¹⁰⁸ kann Menschen aus vielen Gründen, auch finanziellen, verschlossen bleiben.

Vermutlich will das DoD mit der Verwendung des Begriffs global common aber keine akademische Diskussion anstoßen, sondern ein politisches Ziel formulieren: Das Internet muss als Gemeinschaftsgut, falls nötig, durch ein aktives Eingreifen abgesichert werden. Aber, und das ist ein weiteres Ziel, eine politische Kontrolle des Internets durch ein multilaterales Gremium, wie auf dem World Summit on the Information Society von einigen Akteuren gefordert, muss verhindert werden. Das erscheint auf den ersten Blick eigenartig, da ein Gemeinschaftsgut seine

¹⁰⁸ Vgl. <http://www.un.org/Depts/los/index.htm>.

gemeinsame, globale Verwaltung durch die Staaten nahelegt. Einer solchen Multilateralisierung stehen jedoch alle bisherigen USA-Administrationen ablehnend gegenüber, da sie die Offenheit des von den USA angestoßenen Netzes durch Regulierungen und Eingriffe beeinträchtigen würde: Nicht die Staatengemeinschaft, eine internationale Organisation, können Rückversicherer des freien, offenen Internets sein, sondern sich selbst sehen die USA in dieser Rolle. Und als Rückversicherer würden sie nur eingreifen, wenn die freie Entwicklung und Nutzung des Netzes substantiell gefährdet wäre. Dieser Eingriff würde alleine dazu dienen, diese Gefahr abzuwenden und das Netz zu sichern. Im alltäglichen Geschehen hingegen soll keine Politik auf die Netzverwaltung einwirken. Daher vertreten die USA in den kontroversen Diskussionen über die Kontrolle des Namensraumes die Position, dass eine private Organisation ein solches Gemeinschaftsgut im täglichen Betrieb sachgerecht und unparteiisch zum Nutzen aller Netznutzer verwalten muss. (Ein angenehmer Effekt ist dabei, dass sich in einem offenen Netz die starken Netzbetreiber bzw. Inhabitanten der USA ungestört entfalten können.) Keine Zustimmung findet deshalb eine zwischenstaatliche Kontrollkörperschaft, die im Dunstkreis der Vereinten Nationen stünde. Denn über sie könnten undemokratische Staaten die Meinungsfreiheit, den freien Zugang der Nutzer zu Informationen blockieren und die Entwicklung des Netzes durch eine politische Zwangsjacke behindern. Zudem, so Vertreter der USA, gebe es bei den Kritikern des Status Quo keinen Konsens über Struktur und Aufgabe einer solchen internationalen Körperschaft.

Diese Argumentation sieht sich dem Einwand gegenüber, warum dann die USA auf ihrem letzten, exklusiven Aufsichtsrecht beharren, wenn eine staatsfreie Verwaltung des Gemeinschaftsgutes vorzuziehen ist. Tatsächlich kann diese Position nur begründet werden, wenn sich die USA, die das Netz mit öffentlicher Finanzierung entwickelt und in den Anfängen aufgebaut haben, als Garanten der Funktionsfähigkeit und Offenheit des Internets verstehen, der dafür über die rechtlichen und die operativen Mittel verfügen muss. Diese Sicht findet in den USA breite Zustimmung, wie ein Editorial der US-liberalen Washington Post („The Internet at Risk“) vom 21. November 2005 nach dem Abschluss des WSIS zeigt.¹⁰⁹ Auch europäische Staaten dürften dem Gedankengang grundsätzlich positiv gegenüber stehen: Multilaterale Kontrolle

¹⁰⁹ <http://www.washingtonpost.com/wp-dyn/content/article/2005/11/20/AR2005112000858.html>.

würde ein Einfallstor für Zensur und Eingriffe, die es im heutigen Verwaltungssystem nicht gibt. Es hat sich bewährt und dient allen Staaten, die an einem freien, offenen Netzwerk interessiert sind. Auch die Weigerung der US-Regierung, der Einführung einer Sex-Top Level Domain zuzustimmen, reflektiert aus ihrer Sicht Vorstellungen über Anstand im öffentlichen Raum und ist keine Zensur, weil sie technisch nicht die Erreichbarkeit solcher Seiten erschwert. (Zudem war die Nachfrage aus dem Milieu gering, so dass ICANN diese TLD-Einrichtung nicht mehr verfolgt.)¹¹⁰

Diese Garantiefunktion muss nicht schon deshalb obsolet sein, weil Staaten, darunter China, aber auch Verbündete der USA wie Ägypten und weitere arabische Staaten, ihren Bürgern die freie Nutzung des Internets versagen, den Zugang zum Netz kontrollieren, den Besuch politisch und kulturell unerwünschter Seiten, darunter viele Weblogs, technisch zu verhindern suchen. China bediente sich dabei der Hilfe von US-Unternehmen. Die USA reagieren darauf, und Cisco, Yahoo, Microsoft und vor allem Google sind in den kritischen Blick auch des US-Kongresses geraten.¹¹¹ Sie haben sich den Zugang zum expandierenden chinesischen Internetmarkt dadurch erkaufte, dass sie sich (wie Medienunternehmen generell) den Zensurbestimmungen des Landes unterwerfen bzw. China beim Betrieb seines Internet-Kontrollsystems (Great Firewall)¹¹² unterstützen. In Einzelfällen sollen sogar Daten an chinesische Behörden übermittelt worden sein, die zur Einkerkierung von Internet-Dissidenten beitrugen. Dieses chinesische Kontrollsystem konzentriert sich auf politische und kulturell-religiöse Informationen, lässt aber, im Gegensatz zu etwa einigen arabischen Staaten, andere Angebote, von Pornographie bis zu fragwürdigen und sogar kriminellen Geschäften, weitgehend ohne Kontrolle im Netz [Barboza, 2006]. Das System widerspricht von China völkerrechtlich zugesagten Bürger- und politischen Rechten, und es ist, so die Opennetinitiative,¹¹³ „pervasive, sophisticated, and effective“. Wie wirksam es wirklich ist, bleibt freilich umstritten. In der täglichen Auseinandersetzung zwischen 30 000 Internetzensoren und einer wachsenden Schar von Kritikern der chinesischen Politik gibt es durchaus einige Erfolge für Chinesen, die über das Internet ihre Meinung frei äußern wollen. Das chinesische Meinungsbild ist mit dem Internet sicherlich bunter geworden, und versierte Nutzer finden Wege, um gesperrte Sei-

¹¹⁰ Ein Argument für die Einführung der TLD ist, dass dann alle unter der TDL gemeldeten Seiten einfach herausgefiltert werden könnten.

¹¹¹ Vgl. <http://www.internationalrelations.house.gov/archives/aphear.htm>.

¹¹² http://www.en.wikipedia.org/wiki/Great_Firewall.

¹¹³ <http://www.opennetinitiative.net/>; sie ist von nordamerikanischen Universitäten getragen. Vgl. ferner Reporters without Borders, http://www.rsf.org/article.php3?id_article=15613.

ten etc. aufzurufen. Einer (in China noch marginalen) aktiven, regimekritischen und versierten Nutzerschaft, wie sie etwa im Iran existiert, wäre auch das chinesische Internet-Kontrollsystem nicht gewachsen. Trotzdem bleibt die Behinderung und Zensur des Internets Teil einer massiven Beschränkung der Informations- und Meinungsfreiheit, die alle Medien umfasst. Darin kommt das Bemühen des chinesischen Regimes zum Ausdruck, die ökonomischen Potentiale des Netzes zu nutzen, ohne dass sich seine regimekritischen Möglichkeiten entfalten. Die Involvierung von US-Unternehmen in diese Beschneidung der freien Internetnutzung hat das US-Außenministerium bewogen, eine Task Force on Global Internet Freedom¹¹⁴ einzurichten, die sich generell dem Problem der völkerrechtswidrigen Zensur und Kontrolle widmen soll. Sie soll Empfehlungen erarbeiten "on policy and diplomatic initiatives to maximize access to the internet and help minimize government efforts to block information" - Ausdruck einer Selbstwahrnehmung der USA als Bewahrer der Internetfreiheit, auch wenn die Handlungsmöglichkeiten gegenüber China sehr begrenzt bleiben und gegenüber einigen Verbündeten aus übergeordneten geostrategischen Gründen nicht genügend genutzt werden.

Alle Argumente der USA-Regierung ändern nichts daran, dass von der Mehrheit der Staaten ihre Sicht nicht geteilt wird, sie sei letzte Instanz im Internet. Diese Position wird in dem Kompromissdokument, das auf der WSIS 2005 in Tunis verabschiedet wurde, zwar nicht explizit in Frage gestellt.¹¹⁵ Aber in den Verhandlungen und danach wurde der Widerstand deutlich. Den Staaten, internationalen und Nichtregierungs-Organisationen sowie Unternehmen werden Anhörungsrechte gewährt in einem nur beratenden Internet Governance Forum (IGF) unter der Schirmherrschaft der Vereinten Nationen.¹¹⁶ Jedoch ziehen auch Kritiker der USA-Position nicht an einem Strang. Die EU und einige weitere Staaten wollen, wie die USA, die Fragen der Netzverwaltung und der US-Sonderrolle nicht in dem für diverse politische und gesellschaftliche Kräfte breit geöffneten IGF, sondern einem parallelen, nichtöffentlichen Prozess behandeln. Denn auch sie sehen durchaus die Vorteile der heutigen Verwaltungsstruktur ohne eine unwägbare multilaterale Kontrolle im Kontext der UNO. Sie möchten aber Wege finden, im existierenden System die Möglichkeiten der USA einzuhegen und selbst stärkeren politischen Einfluss auszuüben, um ihre wirt-

¹¹⁴ <http://www.state.gov/r/pa/prs/ps/2006/61156.htm>.

¹¹⁵ Vgl. <http://www.itu.int/ws/s/docs2/pc3/working/dt15rev5.pdf>.

¹¹⁶ Vgl. <http://www.intgovforum.org/>.

schaftlichen, kulturellen Interessen zur Geltung zu bringen. Länder wie Brasilien und viele Nichtregierungsorganisationen, die wenig oder kaum Gewicht auf die Waagschale bringen, widersprechen dem heftig. Sie betonen die Rolle des IGF, in dem sie ihre Kräfte zu bündeln hoffen.

Sicherlich werden die Kontroversen über die letzte Instanz und die Internetgovernance, in welchem organisatorischen Kontext auch immer, weitergeführt werden [Kleinwächter, 2005]. Der anhaltende Widerspruch gegen die Positionen der USA spricht dafür, dass es eine Rivalität gibt über die Zuständigkeit für einen Kernbereich dieses weltumspannenden Netzwerkes. Eine substantielle Änderung des Status Quo zeichnet sich deshalb noch nicht ab.

Eine Rolle als Garant könnte über die Bemühungen hinausgehen, Beschränkungen der Meinungs- und Nutzungsfreiheit dadurch zu verhindern, dass grundlegende institutionelle Reformen aufgehalten werden. Die USA bereiten sich vor dem Hintergrund potentieller staatlicher, aber auch denkbarer substaatlicher krimineller bzw. terroristischer Bedrohungen auf eine Verteidigung des Netzwerkes gegen strategische Cyberangriffe vor. Damit ist die Frage, ob Streitkräfte künftig explizit den Auftrag haben könnten, das Internet zu verteidigen, aber nicht mit „ja“ beantwortet. Denn der Schutz konzentriert sich noch auf die militärischen Netze, und die Politik der USA (und anderer westlicher Staaten) beim Schutz kritischer Infrastrukturen ist überwiegend von einem zivilen Ansatz gekennzeichnet, der die Kooperation der Politik mit Unternehmen, die Public Private Partnership (PPP) in den Vordergrund stellt. Da aber auch das Militär das öffentliche Internet nutzt, gerät auch dessen Verteidigung in den Blick. Das ist angesichts der Gefährdungslage im Cyberspace als Vorsorgemaßnahmen nachvollziehbar, könnte aber zur Entwicklung von operativen Fähigkeiten zur Cyberkriegsführung führen.¹¹⁷ Damit entstünden fließende Übergänge zwischen dem Bemühen, durch Vorsorge und Schutz die Internetsicherheit zu gewährleisten, und den Fähigkeiten, einen offensiven Cyberkrieg zu führen, um das Netzwerk zu kontrollieren und Anderen seine Nutzung zu versagen.

Verschärfend kommt hier hinzu, dass sich der Cyberspace von der Hohen See, dem Internationalen Luft- und Weltraum in einem wesentlichen Punkt unterscheidet: Letztere lassen sich in völkerrechtlichen Verträgen meist recht gut und zwischen den Staaten einvernehmlich von den nationalen Territorien abgrenzen, wodurch das

¹¹⁷ Vgl. dazu die Dokumente unter <http://iwar.org.uk/iwar/>

zwischenstaatliche Konfliktpotential sinkt. Der Sinn des Internets besteht aber gerade darin, solche Grenzziehungen in einer globalen Verflechtung aufzulösen, in der jeder einzelne Nutzer darauf angewiesen ist, dass das gesamte Netzwerk gut, sicher funktioniert. Denn Störungen an einer Stelle können überraschende Fernwirkungen haben.¹¹⁸ Damit wird nicht nur die Infrastruktur des Internets, die auf dem Grund der Hohen See liegt (wichtige Kabelstränge) zu einem schützenswerten Objekt. Es besteht die Möglichkeit, dass auch Teile des Netzwerkes, die für das Internet insgesamt essentiell sind und auf den Territorien von Staaten liegen bei gravierenden Gefahren für das Internet „vergemeinschaftet“ und - im Zweifel durch den oder die mächtigsten Akteure – quasi von Außen kontrolliert und verteidigt werden. Der Schutz der kritischen Infrastruktur Internet könnte latent zu einer grenzenlosen Aufgabe werden, der sich die Sicherheitspolitik nicht immer mit kooperativen Mitteln widmet. Hier baut sich ein Problematik auf, die Gesellschaft und Politik frühzeitig beachten müssen, wollen sie den Schutz kritischer Infrastrukturen möglichst kooperativ organisieren.

Neue Bedingungen für den Schutz kritischer Infrastrukturen

Das Internet fügt sich in ein Bild ein, das eine fortschreitende wechselseitige, wenn auch nicht immer präzise erfasste Interdependenz kritischer Infrastrukturen zeigt, deren Funktionieren (mehr oder weniger) wichtig für die Staaten ist. Diese kritischen Infrastrukturen sollen auch dann funktionieren, wenn sie besonderen Belastungen oder Angriffen ausgesetzt sind. Dem sollen CIP bzw. CIIP mit seiner speziellen Ausrichtung auf die IuK-Infrastrukturen, vor allem das Internet, dienen. Da Internetsicherheit, so Dunn und Mauer [2006], wenn auch nicht in aller Reinheit, Merkmale eines Gemeinschaftsgutes aufweist, dessen Sicherung nicht allein dem Markt überlassen werden kann, ist politische Intervention notwendig - wie viel, in welchen Bereichen, mit welchen Instrumenten und unter welchen Paradigma (von nationaler Sicherheit bis hin zu rein technisch-organisatorischer Vorsorge), darüber herrscht kein Konsens.

Ob und welche politischen Interventionen es gibt, wird von einem spezifischen Kontext beeinflusst. Im Falle des Internets ist dieses Umfeld dadurch gekennzeichnet, dass das Netzwerk fast vollständig in privatem Besitz ist, und seine Innovationsrate

¹¹⁸ Vgl. dazu das Simulationskapitel und [Fischer, Lepperhoff, Volst, 2003].

sehr hoch ist. Dies legt eine Kooperation von Staat und Privaten nahe, und in den meisten Staaten kommt der Public Private Partnership eine wichtige, oft sogar die zentrale Rolle beim Infrastrukturschutz und insbesondere beim CIIP zu [Lewis, 2005]. PPP bindet die Unternehmen, Dienstleister und großen Rechenzentren ein und muss dabei Rücksicht nehmen auf ihre Interessen.

Eingebunden werden müssen auch möglichst viele individuelle Internetnutzer, die Regeln des Grundschutzes beachten sollten, um unerwünschte Einwirkungen von Außen über das Netzwerk oder einen direkten Zugriff auf ihre Rechner zu erschweren.¹¹⁹ Denn oft sind ungeschützte Rechner ungewollt und unbemerkt Teil eines Cyberangriffs oder anderer krimineller Aktivitäten, die von irgendwo aus dem Netz gesteuert werden. Mit dem Internet werden erstmals auch normale Bürger unmittelbare Akteure des Infrastrukturschutzes, und ihr Verhalten entscheidet mit über den Erfolg oder das Versagen von CIIP-Maßnahmen. Freilich sind hier die Möglichkeiten der Politik weitgehend auf Informations- und Bildungsmaßnahmen begrenzt.

Infrastrukturschutz endet aber nicht bei solchen technischen Maßnahmen. Infrastrukturen sind hybride Systeme, in denen Technik und soziale Strukturen in Wechselwirkung stehen [Volst, 2002]. Praktisch wird diesem theoretischen soziologischen Konzept insoweit Rechnung getragen, als die Sicherheitskultur und die mit ihr verwobenen organisatorischen Maßnahmen eine Rolle spielen beim Infrastrukturschutz [OECD, 2002a], [Winkel, 2000], [Hafner, 1999].

Auch wenn die Begrifflichkeiten neu, Programme und Maßnahmen spezifischer und intensiver geworden sind, hat die Politik schon immer versucht, die materiellen Lebensgrundlagen eines Landes zu sichern, und dabei kam den Bürgern eine, wenn auch sehr begrenzte, Rolle zu. Angriffe auf die Infrastrukturen sind so alt wie der Krieg [Crevelde, 1989], und die Versuche, diese Grundlagen so zu schützen, dass sie trotzdem noch einigermaßen tragen, waren immer Teil der Strategie. Während des Kalten Krieges gab es in Staaten der Nato [Kremer, 1966], besonders aber in der Sowjetunion [Sokolovsky, 1975], den Zivil- bzw. Bevölkerungsschutz, der auch Elemente des Schutzes kritischer Infrastrukturen enthielt. Jedoch stützte sich der Zivilschutz in den westlichen Staaten auf freiwillige Maßnahmen der Bürger und Unter-

¹¹⁹ Ein IT-Grundschutzhandbuch findet sich auf der Seite des BSI: <http://www.bsi.de/gshb/index.htm>. Regeln für einen guten Grundschutz sind u. a.: Kontrolle des Zugangs zum Rechner; aktuelle Schutzsoftware; back-up-Speicherung; Benutzung nicht offensichtlicher und offener Passwörter; drahtlose Verbindungen nur solange halten, wie es wirklich nötig ist; Verschlüsselung wichtiger Informationen.

nehmen. Allmählich setzte sich die Einsicht durch, dass kritische Infrastrukturen schon bei großen nichtnuklearen militärischen Auseinandersetzungen nicht geschützt werden könnten und ihre Funktionsfähigkeit rasch und für längere Zeit verlieren würden. Diese (symmetrische) Verwundbarkeit war seit Mitte der 60er Jahre ein Grund dafür, stabile Abschreckung und kooperative Rüstungssteuerung als sich ergänzende Ziele der Sicherheitspolitik zu verfolgen ([Baudissin, 1982]; mit anderen politischen Intentionen [Roßnagel et al., 1989]).

Seit den 80er Jahren haben technische Innovationen und politische Veränderungen dazu beigetragen, dass sich die Bedrohungskonstellationen und die Wahrnehmung der Gefahren, denen kritische Infrastrukturen ausgesetzt sind, verändert haben [Knop, Frank, 2004], [Geiger 2000]. Das macht eine Ergänzung bzw. Anpassung der Schutzstrategien, -maßnahmen und möglicherweise eine Ergänzung des privatisierten Schutzansatzes durch direkte staatliche Vorgaben und sicherheitspolitisch ausgerichtete Interventionen erforderlich. Auf drei Veränderungen sollen besonders hervorgehoben werden:

- Mit der Expansion des Internets bildet sich eine neue Form der virtuellen Verwundbarkeit heraus, die zu der physischen Verwundbarkeit hinzukommt, die auch diese wie alle anderen Infrastrukturen aufweist: Das Internet selbst kann mit seinen eigenen konstitutiven Mitteln, nämlich Software, angegriffen werden. Zudem können Angreifer über das Netzwerk verdeckt aus der Ferne in die Rechner anderer kritischer Infrastrukturen eindringen. Um solche Angriffe frühzeitig zu erkennen und abzuwehren, ist sehr viel Aufwand nötig, der Erfolg ist alles andere als sicher, und die Wirksamkeit der Abwehrmaßnahmen bleibt schwer vorherzusagen.
- Die Rolle des Staates beim Infrastrukturschutz hat sich verändert, und das stellt alle Beteiligten vor neue Herausforderungen. Durch Liberalisierung (Elektrizitäts-, Gasversorgung) und Privatisierung (Telekommunikation, Schienenverkehr, Wasserversorgung) gehen Infrastrukturen aus dem staatlichen bzw. kommunalen in den Besitz von Privaten über, die im Wettbewerb untereinander stehen (sollen). Der Staat muss sich angesichts dieses neuen Dualismus von Staat und Privaten einlassen auf Diskussionen darüber, an welchen Bedrohungsbilder sich CI(I)P orientieren soll, wo Partnerschaften zwischen Staat und Privaten sinnvoll sind und was den Privaten allein an Maßnahmen und Kosten überlassen bleibt [Andersson, Malm, 2006], [Dunn, Mauer 2006], [Sonntag, 2005]. Dabei kann die Rolle des

Staates sich in den Infrastrukturbereichen durchaus unterscheiden. Da das Internet zu etwa 90 Prozent im Besitz von Privatfirmen ist, musste der Staat hier von Beginn an mit privaten Interessen einen Ausgleich finden. PPP war deshalb ein nahe liegendes Leitbild, das jedoch, so einige Kritiker, „unzulängliche Resultate“ bringt und den Bedrohungen „nicht angemessen“ ist [Andersson, Malm, 2006]. In der Vergangenheit konnten Unternehmen, die wenig oder gar nicht dem Wettbewerb, aber z. T. auch über die Eigentümerstruktur politischen Einflüssen ausgesetzt waren, es sich eher leisten, im- oder explizit gesamtstaatliche Sicherheitsüberlegungen beim Aufbau und Betrieb von Infrastrukturen zu berücksichtigen, da die anfallenden Kosten den Kunden in Rechnung gestellt wurden (oder vom Staat mittelbar übernommen wurden).¹²⁰ Das kann von den privaten Unternehmen in gleicher Weise nicht erwartet werden. Zwar sind auch sie an technisch sicheren Infrastrukturen interessiert und müssen dabei z. T. auch rechtlichen Vorgaben folgen. Aber Unternehmen im Wettbewerb neigen dazu, nur das Nötigste in ihrem Tätigkeitsbereich zu tun, was nicht immer mit den Sicherheitswünschen deckungsgleich sein muss, die aus gesamtgesellschaftlicher Perspektive formuliert werden. Deshalb sehen einige Analytiker Anzeichen für ein Marktversagen beim Infrastrukturschutz [Andersson, Malm, 2006]. So gibt es in den USA Klagen, der Zwang zur Kostenreduktion im Internet führe über Fusionen von Unternehmen zur Stilllegung von Kabelsystemen, zum Aufbau zentralistischer, hierarchischer Speicherstrukturen (hubs und spokes) in der Internettopologie. Das könne zu höherer Verwundbarkeit führen (vgl. [Grubestic, Murray, 2005]; topologische Strukturen mit hierarchischen Elementen finden sich auch in Deutschland, das jedoch vergleichsweise gut vermascht ist, und - etwas ausgeprägter - in andern europäischen Ländern [Lepperhoff, Fischer, 2004]).¹²¹ Auch wird die vom Wettbewerb getriebene Vergabe ehemals eigener IuK-Dienstleistungen durch Unternehmen an andere inländische (outsourcing) oder ausländische (offshoring) Unternehmen gelegentlich als Sicherheitsproblem dargestellt. Hier ist Widerspruch angebracht, zumal viele dieser Sicherheitsbesorgnisse eher in der Sorge um die Abwanderung von Arbeitsplätzen wurzeln. Denn so verbreitet, wie das durch Medienberichte suggeriert wird, sind solche Auslagerungsprozesse nicht, und ein nur geringer Teil

¹²⁰ Ob Infrastrukturen, als sie noch (un)mittelbar Staatsbesitz waren, sicherer, redundanter, weniger störanfälliger waren, wäre einer kritischen Prüfung wert.

¹²¹ Vgl. das Simulationskapitel.

betrifft sicherheitsrelevante Dienstleistungen [CSI/FBI, 2004]. Aber solche Prozesse könnten mit einem Kompetenz- und Bewertungsverlust in den beauftragenden Unternehmen einhergehen, die es erschweren, die Qualität der gelieferten Dienstleistung einzuschätzen.

- Besondere Aufmerksamkeit findet die Veränderung des Bedrohungsspektrums. Innerhalb und gegen die ehemaligen Kernzonen des Ost-West-Konfliktes agieren verstärkt transnational organisierte kriminelle und terroristische Akteure. Dabei nutzen auch terroristische Netzwerke das Internet immer öfter als einen flexiblen, schwer zu kontrollierender Raum für Propaganda, Rekrutierung, Netzwerkbildung, Geldbeschaffung und Information. Zudem, so die Perzeption, steigt mit dem Agieren dieser Akteure, verglichen mit dem Ost-West-Konflikt, die Wahrscheinlichkeit, dass es zu Angriffen auf kritische Infrastrukturen, auch auf und über das Internet, kommt. Denn diese Infrastrukturen könnten attraktive Ziele sein: „Attacking infrastructure (...) has a „force-multiplier“ effect that allows even a relatively small attack to achieve great impact“ [Abele-Wigert, Dunn, 2006, I, S. 26]. Andererseits erhöht sich die Chance, dass Infrastrukturschutz wirksam ist und die Folgen von Angriffen gemildert werden können, da diese Akteure zumindest physische Angriffe nicht mit der Intensität führen können, die von Staaten zu erwarten wäre. Ob das auch für die Wirksamkeit und Folgen eines denkbaren Cyberterrorismus gelten würde, der sich schädlicher Software etc. bedient, wird kontrovers diskutiert.

Es ist eine auch in Deutschland kaum umstrittene Lagebeschreibung [Dietl, Hirschmann, Tophoven, 2006], [Knop, 2005], [Laqueur, 2004], [Weidenfeld, 2004], [Hoffmann, 2001], dass der transnationale, meist islamistisch inspirierte Terrorismus, der immer wieder seine Gestalt wandelt [RAND, 2005], die Randbedingungen der Sicherheitspolitik verändert. Dissens gibt es jedoch darüber, welche Organisationen und Gruppen zu diesem Terrorismus zählen;¹²² wie gut das Wissen über sie ist, was man über sie sicher nicht weiß („known unknowns“) und über welches Unwissen man sich überhaupt nicht klar ist („unknown unknowns“, vgl. [Schneckener, 2005a]); worin genau die sicherheitspolitischen Veränderungen bestehen, die das Auftreten des neuen Terrorismus mit sich bringt, und wie ausgeprägt sie sind; welche politisch-strategischen Konsequenzen zu ziehen sind, also wie mit den neuen Gefahren umgegangen werden soll: Ist die Bekämpfung dieses Terrorismus eher eine Form des

¹²² Vgl. die EU-Terrorliste <http://consilium.europa.eu/showPage.asp?id=631&lang=de&mode=g>; die der USA: <http://state.gov/s/ct/rls/fs/37191.htm>.

Krieges, eine Polizeiaufgabe oder ein wirtschafts- und sozialpolitisches Handlungsfeld, das die Wurzeln des Terrorismus zu beseitigen sucht? Schließlich ist unklar, welche Gefahren von ihm für den Cyberspace ausgehen, ob und unter welchen Bedingungen er zum Ziel von (Cyber-) Terroristen wird.

Das alles erschwert die Einschätzung der sicherheitspolitischen Lage, die während des Ost-West-Konfliktes konzeptionell einfacher zu beschreiben war. Denn in der nördlichen Hemisphäre waren die Bedrohenden (Staaten), ihre Mittel (recht gut einschätzbare Waffensysteme) und die Form einer potentiellen gewaltsamen Austragung eines Konfliktes (zwischenstaatlicher Krieg) bekannt. Zwar sind solche Paradigmen des Krieges nicht hinfällig geworden, wie die Irakkriege der Jahre 1991, 2003 und Szenarien zur Verhütung bzw. Eindämmung der nuklearen Bewaffnung des Irans oder Nordkoreas zeigen. Aber sie treten spätestens seit 2001 in der Perzeption von Politik und Öffentlichkeit zurück vor Bedrohungen durch einen (neuen) Terrorismus [Schneckener, 2006, 2005, 2004, 2002], [DoD, 2005], [Allision, 2005], [Carter, Deutch, Zelikow, 1998]. Er agiert unabhängig von Staaten oder vom Territorium schwacher oder zerfallener Staaten aus, während staatlich gestützter Terrorismus seit einigen Jahren zurückgeht [DoS, 2005] - möglicherweise ein vorübergehendes Phänomen. Da Terrorismus eine direkte Auseinandersetzung mit Streitkräften hoch entwickelter Staaten nicht durchstünde, sucht er asymmetrische Auseinandersetzungen, deren Form und Intensität für eine Lageeinschätzung aus objektiven und subjektiven Gründen schwerer zu antizipieren ist.

Das Modell der west-östlichen Abschreckung lässt sich auf diesen neuen Terrorismus nicht anwenden. Die nukleare Eskalationsdrohung mit ihrer Möglichkeit gegenseitiger Zerstörung verhinderte in den Kernzonen des Ost-West-Konflikt, wie weitgehend auch immer die politischen Ziele der Beteiligten sein mochten, den Einsatz jeglicher militärischer Instrumente, die sich damit selbst als Mittel zur Fortsetzung von Politik wertlos machten [Baudissin, 1982]. Terroristische Akteure agieren subnational, verdeckt, kommen ohne größere oder ganz ohne territoriale Kontrolle aus und setzen Selbstmordattentäter ein. Damit entziehen sie sich einer symmetrischen Abschreckung.¹²³ Ihr Verhältnis von Zielen und Mitteln kann ungebrochen sein, und verfolgen sie absolute, ideologisch oder religiös verbrämte Ziele, die eine Vernichtung

¹²³ Stellungnahmen wie die des französischen Präsidenten 2006 (http://www.botschaft-frankreich.de/article.php3?id_article=1305) oder in US-Dokumenten über die Atomwaffenstrategie (http://www.globalsecurity.org/wmd/library/policy/dod/jp3_12fc2_15mar2005.htm) zielen primär auf Staaten, die terroristischen Gruppen Massenvernichtungswaffen zugänglich machen könnten.

eines Gegners zum Ziel haben, würden sie, so suggerieren Stellungnahmen einiger dieser Akteure selbst, auch Massenvernichtungswaffen einsetzen. Jedoch verfügen solche Gruppen, trotz vieler Gerüchte in Medien, heute sehr wahrscheinlich nicht über diese Waffen [RAND, 2005], [Kelle, Schaper, 2003], und es gibt die (keinesfalls beruhigende) These, sie seien nur für einige wenige islamistische Gruppen interessant, während andere Terrorgruppen fürchteten, dass ihr Besitz sie politische Unterstützung kosten würde [Shahar, 2005]. Da Terrorismus bei der Wahl seiner Mittel opportunistisch ist, könnten auch Angriffe auf das Internet und andere Infrastrukturen zu seinen Optionen gehören [PCCIP, 1997], falls Bedingungen erfüllt sind: eigene Fähigkeiten und Instrumente für solche Angriffe, die Verwundbarkeit kritischer Infrastrukturen und die Chance, die gewünschten Wirkungen zu erzielen. Eine zentrale Rolle spielen die psychologischen und politischen Wirkungen, die in der Angst wurzeln vor den jederzeit denkbaren, in Form, Ort und Konsequenzen nicht vorhersehbaren terroristischen Aktionen, die über Medienberichte weiter verstärkt wird [Palm, Rötzer, 2002].

In diesem neuen Bedrohungsspektrum ändert sich die objektive und vor allem die politisch-psychologische Wirkung der Infrastrukturen. War ihre Verwundbarkeit während des Ost-West-Konfliktes ein Antrieb zur Friedenssicherung, könnten die kritischen Infrastrukturen der hoch entwickelten Staaten nun zu einer offenen Flanke werden. Jedoch müssen bei einer solchen Einschätzung auch die Chancen berücksichtigt werden, die miteinander verknüpfte Infrastrukturen und speziell das Internet für die wirtschaftliche, soziale und kulturelle Entwicklung von Gesellschaften und Staaten haben. Dadurch steigen auch Resilienz und Abwehrmöglichkeiten gegenüber den neuen Bedrohungen: Gerade wegen ihrer komplexen Strukturen und Prozesse sind reiche Gesellschaften weniger verwundbar als arme, da sie über ausreichende Ressourcen und handlungsfähige Institutionen verfügen, die wirksamere Krisenverhütung und -bewältigung ermöglichen. Dabei haben diese Infrastrukturen eine tragende Rolle. Bemühungen, die Verwundbarkeiten kritischer Infrastrukturen abzubauen, müssen daher immer daraufhin überprüft werden, dass sie keine wesentliche Beeinträchtigung der Leistungsfähigkeit dieser Infrastrukturen mit sich bringen und ihre weitere Entwicklung ermöglichen.

Gefahren für ein sicheres Internet

Soll ein sicheres, leistungsfähiges Internet eine infrastrukturelle Grundlage moderner Gesellschaften sein, dürfen akute und zukünftige Gefahren für das Netzwerk nicht ignoriert oder nur beiläufig abgehandelt werden.

Gefahren sind Möglichkeiten, dass Ereignisse einen definierten erwünschten, normalen Zustand eines Systems in einer unerwünschten Weise verändern. Bevor also Gefahren thematisiert werden, ist der Normalzustand eines leistungsfähigen und sicheren Netzwerkes zu definieren. Bislang ist es aber nicht gelungen, die systemische Normalität des kaum zu überschauenden, dynamischen Netzes so präzise zu beschreiben, dass frühzeitig gefährliche Entwicklungen als Normabweichungen zu erkennen sind [Pohlmann, 2005], [Lepperhoff, Fischer, 2004a], trotz der Bemühungen von Unternehmen wie VeriSign,¹²⁴ ein Beobachtungs- und Frühwarnsystem aufzubauen. Jedoch können die wesentlichen Leistungen identifiziert werden, die ein gut funktionierendes, sicheres Internet bereitstellen muss, damit die Nutzer seine Vorzüge genießen.¹²⁵

Leistungen eines sicheren Internets

Diese Leistungen, die generell für den Informations- und Kommunikationsbereich gefordert werden und wesentliche Kriterien für die Einschätzung von Internetsicherheit sind [Sonntag, 2005], [Eckert, 2004], [Schneier, 2000], umfassen:

- die Verfügbarkeit der im Netz transportierten Daten zu dem Zeitpunkt, zu dem Nutzer auf sie zurückgreifen wollen;
- die Integrität der Daten, die unverfälscht und vollständig zwischen Sender und Empfänger übertragen werden müssen;
- die Vertraulichkeit der übermittelten, gespeicherten Kommunikation sowie der Verbindungen, die eine unbefugte Beobachtung bzw. Auswertung nicht zulässt;
- die Authentizität, die Zuordnung der Daten zu einem legitimen Netznutzer, der während des gesamten Kommunikationsvorgangs der gleiche sein muss.

Solche Leistungen zu fordern ist nicht neu. Denn seit Informationen in einem institutionellen Kontext ausgetauscht werden wird versucht, ihre Sicherheit zu gewährleis-

¹²⁴ <http://www.verisign.com/>.

¹²⁵ Natürlich legen Unternehmen in den Verträgen mit Providern die Qualität der Dienstleistung fest und sind auch in der Lage, ihre Teilnetze zu überwachen. Hier aber steht das Netzwerk als Ganzes im Blick, für das es keinen Verantwortlichen gibt.

ten: Durch einen verschlossenen, versiegelten Umschlag, durch Unterschrift(zeichen), einen vertrauenswürdigen Übermittler, der sich legitimieren kann. (Wie wenig erfolgreich das oft war, zeigt die Geschichtswissenschaft, die sich mit zahlreichen gefälschten Dokumenten insbesondere aus dem Mittelalter umherschlagen muss.) Neu ist die Dichte der Kommunikation, ihre höhere Bedeutung durch die starke Verrechtlichung der Beziehungen zwischen den Akteuren, ihre zunehmende Lösung vom Transport durch Individuen durch die Nutzung technischer Übermittlungssysteme, bis hin zur Auflösung der Information zwischen Sender und Empfänger in Datenpakete. Das hat, verglichen mit den frühen Zeiten, als Informationen zu meist persönlich zugestellt wurden,¹²⁶ durchaus dazu geführt, dass die Leistungen heute eher erfüllt werden. Denn Systeme, in denen Menschen die Informationen transportieren, sind nicht nur langsamer, sondern auch verletzlicher.

Aber auch das Internet erfüllt nicht alle dieser Leistungen gleich gut.

Im hohen Maße gewährleistet ist bislang die Verfügbarkeit der Daten. Zwar sehen Labovitz et al. [1999] das Internet im Normalbetrieb, verglichen mit den (nahezu perfekten) Telefonnetzen in hochtechnisierten Gesellschaften, als etwas störanfälliger an. Aber das deckt sich nicht mit den Einschätzungen von CSIA [2005], in deren Umfragen (freilich mit dem Fokus auf die USA) dem Netzwerk eine etwas bessere Leistung als dem Telefon bescheinigt wird. Wer auch immer Recht haben mag, heute ist die Verfügbarkeit des Internets sehr hoch, auch wenn es gelegentlich - meist kleinräumige - technische Störungen und kurze Zeitverzögerungen beim Datentransport gibt, die Nutzern aber meist kaum auffallen. Gezielte Störungen des Internets, durch die der Strom von Datenpaketen unterbrochen wird, sind dagegen bislang selten, von recht kurzer Dauer und bleiben auf kleinere Regionen beschränkt. Sie bleiben aber eine Option für Akteure, die auf diese Weise die eigentliche Funktion des Netzwerkes, den Datentransport, stören wollen. Welche Aussichten bestehen, das durch strategische Angriffe auf Netzknoten, Backbones oder durch ein Wurmprogramm zu erreichen, wird im dritten anhand der Ergebnisse des Simulationsmodells INESS diskutiert.

Dass Informationen nur dem zugänglich sind, für den sie bestimmt sind, war schon immer wichtig. Deshalb setzte sich die Mitte des 19. Jahrhunderts erfundene Post-

¹²⁶ Kommunikation über akustische und optische Signale hat ebenfalls Tradition.

karte¹²⁷ anfänglich nur schwer durch, weil jeder die Information lesen konnte. (Die sinnvolle Reaktion darauf war und ist, nur Unverbindliches oder Banales zu schreiben.) Auch im Internet ist die Vertraulichkeit nicht zu garantieren und technisch sicherzustellen (vgl. [Rotert, 2004]). Das ist kein spezifisches Merkmal dieses Netzwerkes, denn auch Gespräche über das Telefon können belauscht und der Briefverkehr mitgelesen werden. Private, sowohl natürliche als auch juristische Personen, haben sich schon immer - in der Regel illegal - mit Hilfe von Menschen und mit technischen Mitteln bemüht, an vertrauliche Informationen zu gelangen, deren Besitz ihnen Vorteile bringt. Das Internet hat einen Raum eröffnet, in dem, sind die Informationsbesitzer unachtsam und nachlässig, Unbefugte relativ einfach das lesen können, was auf den Rechnern verfasst und gespeichert wird. Mehr Aufwand und ein Zugang zu Dienstleistern bzw. der Zugriff auf Netzknoten oder Kabel ist erforderlich, um Datenpakete zu verfolgen oder aus dem Netz zu fischen.¹²⁸ In der Regel haben hier nur staatliche Stellen einen legalen Zugang, und sie stehen im Zentrum der Aufmerksamkeit, wenn es um die Vertraulichkeit von Daten geht. (Erstaunlicherweise stören sich die meisten Menschen nicht daran, dass sie freiwillig als gläserne Kunden sensible Informationen an weitgehend unkontrollierte Unternehmen geben, um im Gegenzug einige Cent beim Einkauf zu sparen, darunter solche Informationen, die sie mehrheitlich staatlichen Behörden vehement verweigern würden.) Auch wenn der Datenschutz in Deutschland, verglichen mit anderen westlichen Ländern, sehr ausgeprägt ist, ist die Einstellung, die staatliche Neugierde müsse rechtlich und politisch stark eingegrenzt werden, zu Recht fest verwurzelt in rechtsstaatlichen Demokratien. Denn Bürger haben einen Anspruch darauf, dass das, was sie für sich behalten wollen, nicht ohne weiteres von Behörden ermittelt oder erfasst wird. Und Institutionen neigen dazu, legen sie ihre Aufgabenstellung breit aus, das manchmal zu vergessen. Die Beschuldigungen, die in den USA und in Deutschland gegen Geheimdienste erhoben werden, weisen in diese Richtung.¹²⁹ Aber auch in den rechtsstaatlichen Demokratien gibt es Eingriffe in die Vertraulichkeit, die nicht rechtswidrig sind und von den Netzbetreibern unterstützt werden müssen: Unter sehr restriktiven Bedingungen dürfen im Rahmen der repressiven Strafverfolgung durch dazu autorisierte Behörden

¹²⁷ Vgl. <http://www.uni-weimar.de/medien/kulturtechniken/publikationen/relais.html>, dort wird auf eine Publikation von Bernhard Siegert zum Thema verwiesen.

¹²⁸ Einfacher ist das in drahtlosen Netzwerken, wenn keine Sicherheitsvorkehrungen getroffen sind.

¹²⁹ Vgl. zu den Überwachungsaktionen innerhalb der USA [Gellmann, Mohammed, 2006] und zu Aktionen des Auslandsgeheimdienstes BND in Deutschland [Carstens, 2006].

auch Post und Telefon von Personen oder Einrichtungen überwacht werden, wenn sie im Zusammenhang mit bestimmten strafbaren Handlungen oder ihrer Vorbereitung genutzt werden.¹³⁰ Und mit dem Aufkommen des Internets ist es nur konsequent und sinnvoll, diese Regelungen so zu übernehmen, dass unter gleichen Ausgangsbedingungen auch die Kommunikation im Internet überwacht und Vertraulichkeit durchbrochen werden kann. Anders bewertet wird aus guten Gründen eine präventive Überwachung: Einer vorbeugenden Kontrolle des gesamten Netzes bzw. der anderen Kommunikationssysteme und ihrer Inhalte, um auf verdächtige, kriminelle und terroristische Aktivitäten zu stoßen, stehen in Rechtsstaaten in der Regel grundlegende Bürgerrechte und Gesetze entgegen.¹³¹ Weniger intrusiv, durch Gesetz abgesichert, aber durchaus umstritten und für Provider kostspielig, ist die Vorratsspeicherung der Verbindungs- und Standortdaten der Nutzer, die bei der Nutzung von Telefon, E-Mail, WWW anfallen. Sie wird von großen Teilen der Politik und Sicherheitsbehörden vor allem deshalb gefordert, um nach terroristischen Anschlägen über solche Daten die Täter zu ermitteln und weitere Angriffe zu verhüten. Die entsprechende Richtlinie über die Vorratsspeicherung der EU fand im Dezember 2005 bei einigen Veränderungen die Zustimmung des Europäischen Parlaments,¹³² und sie muss, nachdem auch die EU-Justizminister Anfang 2006 zustimmten, in den Staaten umgesetzt werden. (Gegen die Richtlinie klagen vor dem für die Auslegung und Überprüfung des Gemeinschaftsrechts zuständigen Europäischen Gerichtshof (EuGH)¹³³ Irland und die Slowakei.) Sie sieht vor, dass in einem gesetzlichen Rahmen von den Providern die Verbindungsdaten (nicht aber die Kommunikationsinhalte) für sechs bis vierundzwanzig Monate gespeichert und für staatliche Nachfragen bei bestimmten Straftaten bereitgehalten werden müssen. Dies ist als „pauschale Überwachung“ bzw. als „Belastung mit hohen Kosten“ bei einigen Interessengruppen, u. a. aus der deutschen Kommunikationswirtschaft, auf Kritik gestoßen. Jedoch scheint sich der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) abzufinden mit einer Umsetzung der Richtlinie in Deutschland, die sich an ihren Minimalanforderungen orientiert.¹³⁴ Ablehnender a-

¹³⁰ Für Deutschland vgl. http://www.bundesrecht.juris.de/tk_v_2005/index.html.

¹³¹ In welchem Ausmaß und mit welchem Gewinn Geheimdienste die Kommunikation im In- und Ausland überwachen, ist für Außenstehende nicht klar zu erkennen; vgl. [Keefe, 2006].

¹³² http://www.europarl.europa.eu/news/expert/infopress_page/004-3786-348-12-50-901-20051215_IPR03785-14-12-2005-2005-false/default_de.htm/.

¹³³ <http://curia.eu.int/de/transitpage.htm>.

¹³⁴ http://www.bitkom.org/Default_35889.aspx.

giert dagegen der Verband der Deutschen Internetwirtschaft (eco).¹³⁵ Weitere Informationen sollen mit dem (vorläufig auf 5 Jahre befristeten) Gesetz zur Ergänzung des Terrorismusbekämpfungsgesetzes (TBEG) den Sicherheitsbehörden zugänglich gemacht werden, darunter auch dem Bundesnachrichtendienst und dem Militärischen Abschirmdienst.¹³⁶ Kritiker befürchten ein unkompliziertes Abfragen der Bestands- und Nutzerdaten von Online-Anbietern, die praktisch das Surfverhalten der Internetnutzer offen legen. Dem setzt die Regierung entgegen, dass solche Informationen das Wissen über die Verkehrsdaten ergänze und der Zugriff auf die neuen Datensätze nötig sei, um einen Einblick in neue Gefahrenräume zu erlangen.¹³⁷

So zeigt sich auch im Internet, dass zwischen den Bürgerrechten Schutz der Vertraulichkeit, aber auch der Meinungs- und Informationsfreiheit, und dem Recht auf Schutz vor Kriminalität, Terrorismus, deren Gewährleistung allesamt Kernaufgaben des Staates sind [Kröger, Gimmy, 2000], [Tinnefeld, Ehmann, 1998], [Isensee, 1983], ein Spannungsverhältnis besteht.¹³⁸ Dabei hat in den letzten Jahren die Seite der sicherheitspolitischen Vorsorge und der polizeilichen Gefahrenabwehr vor dem Hintergrund terroristischer Bedrohungen an Zugkraft gewonnen, und das wird auch so bleiben. Überwachungsmaßnahmen, auch im Internet, haben, so versichern die Sicherheitsbehörden, zur frühzeitigen Aufdeckung von Anschlägen beigetragen, wie das in Kanada und Großbritannien im Sommer 2006 der Fall war. Befürchtungen, westliche Staaten würden den Datenschutz beiseite schieben, um dann zu Orwell'schen Überwachungsstaaten zu mutieren, erscheinen eher als Ausdruck ideologischer Fixierungen oder ungebändigter Ängste, nicht aber nüchterner Abwägung (vgl. [Schulze, 2006]).

Die Sicherung der Integrität und Authentizität von Daten wird vom Netzwerk selbst nicht wirklich unterstützt, und sie sind heute nicht ohne weiteres gewährleistet, wenn die Nutzer selbst nicht aktiv werden. Sie können kryptographische Verfahren bzw. Public Key Infrastructures¹³⁹ einsetzen, um die Authentizität (sowie Vertraulichkeit und Integrität) übertragener Daten recht gut sicherzustellen. Was fehlt ist eine alltägliche, einfache und verlässliche Authentifizierung. Sie könnte prinzipiell in die Infra-

¹³⁵ Vgl. http://www.eco.de/servlet/PB/menu/1520559_11/index.htm mit einem Überblick über die Entwicklung der EU-Richtlinie im Europäischen Gesetzgebungsverfahren.

¹³⁶ Vgl. den Text unter <http://www.bmi.bund.de>, Stichwort TBEG.

¹³⁷ Vgl. zur Debatte <http://www.heise.de/newsticker/meldung/75621>.

¹³⁸ Vgl. auch die Seite von S. Krempel unter <http://viadrina.euv-frankfurt-o.de/~sk/Pub/politik2.html>.

¹³⁹ Vgl. <http://en.wikipedia.org/wiki/Cryptography>.

struktur des Netzwerkes eingebaut werden [Dyson, 2005]. Möglicherweise würde dadurch aber das Netz komplizierter und störanfälliger.

Auch wenn Authentifizierung gewährleistet wäre, könnten Kommunikationsteilnehmer im Internet nicht feststellen, mit welcher Person, Organisation sie es tatsächlich zu tun haben. Zwar ist das Netz nicht darauf ausgelegt, Anonymität zu sichern, da IP-Nummern über die Provider den Besitzern zugeordnet werden können, so dass „true anonymity is probably not possible on today's Internet“ [Schneier, 2000, S. 65]. Praktisch aber erfordert ein Enttarnen den Zugang zu Providerdaten, über den in der Regel nur berechnete Organisationen verfügen, oder Kenntnis und Aufwand, um die Spuren des Gegenübers im Netz zu verfolgen, was strafbar sein kann, wenn dazu fremde Rechner ausgeforscht werden. Außerdem besteht für kenntnisreiche Akteure z. B. die Möglichkeit, Informationen im Kopf (Header) eines Datenpaketes so zu verändern, dass die Identität des Absenders verschleiert wird - was in einigen Ländern, aber nicht überall verboten ist. Selbst wenn eine alltägliche Authentifizierung garantiert wäre, wäre damit aber nicht die persönliche Identifizierung eines Kommunikationspartners gesichert. Denn der Besitzer einer IP-Adresse muss nicht mit der Person identisch sein, die tatsächlich die Adresse nutzt. Für Missbrauch und Betrug bleibt also genügend Raum. Eine Reaktion darauf ist, beim Handel via Internet nur mit dem in Austausch zu treten, der eine reale Adresse angibt, die bei Bedarf auch vor Ort verifiziert werden kann.

Beeinträchtigungen eines sicheren Internets

Diese zentralen Leistungen, die ein sicheres, funktionierendes Internet gewährleisten soll, nämlich Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität, können durch nahezu alle Faktoren beeinträchtigt werden, die in der Welt wirksam werden. Es sind:

- Naturgewalten (Force Majeure, Acts of God);
- technisches (Hard- und Software-) Versagen, Kapazitätsüberlastung und Unfälle, die verwoben sein können mit den beiden folgenden Faktoren;
- menschliches Versagen (wie Fehlbedienung, Missachtung von Vorschriften);
- institutionelles Versagen (mangelnde finanzielle Ausstattung und organisatorische Umsetzung von Schutzpolitiken, -zielen und -maßnahmen); dadurch werden technisches, menschliches Versagen, gezielte Handlungen erleichtert und die Auswirkungen von Unfällen, Naturkatastrophen, Angriffen verschärft.

- beabsichtigte, gezielte Handlungen (Missbrauch des Netzwerkes für diverse kriminelle Aktivitäten; Angriffe mit Software etc. und mit physischen Mitteln auf das Netzwerk und angeschlossene Rechner).

In der frühen Entwicklungsphase des Internets Anfang der 90er Jahre sahen Experten die Ursachen für Gefährdungen hauptsächlich in Naturgewalten, technischen Störungen und Fehlbedienungen. Zwar wurden schon in dieser Zeit die Gefahren eines Cyberwarfare thematisiert. Aber es war eine noch abstrakte Möglichkeit, und die Bedrohungen durch Cyberkriminalität und -terrorismus gerieten erst allmählich in den Blick. Diese Perzeption hat sich grundlegend geändert. Seit einigen Jahren gewinnt die Überzeugung an Boden, dass, neben der schon heute verbreiteten Nutzung des Netzes für kriminelle bzw. terroristische Geschäfte, künftig von gezielten Angriffen eine sehr große Bedrohung ausgehe [Whitman, 2004]. Attraktive Ziele wären wichtige Netznutzer (Unternehmen, Behörden, Sicherheitsorgane), Netzdienstleister, aber auch Schlüsselkomponenten des Netzwerks und, via Internet, andere kritische Infrastrukturen. Solche Angriffe könnten neben Integrität, Vertraulichkeit und Zurechenbarkeit auch die Verfügbarkeit des Internets beeinträchtigen, etwa wenn das Bereichsnamen-System betroffen wäre oder das Netzwerk mit Datenpaketen überflutet würde. Hier zeigen sich Veränderungen der Wahrnehmung von Gefahrenlagen, die in Wechselwirkungen stehen mit den neuen gesellschaftlich-politischen Bedrohungsbildern, die durch das Auftreten transnationaler terroristischer Akteure entstanden sind.

Für diese Perzeption gibt es gute Gründe, die eine vorsorgende, gefährdungsbewusste Politik beachten muss. Führt sie aber zu einer Fixierung auf die Gefahren, die von solchen Akteuren für das Netz und mit ihm verkoppelte Infrastrukturen ausgehen, können andere Risiken aus dem Blick geraten: Natürliche Ereignisse wie der Hurrikan Katrina, der die Elektrizitäts- und Kommunikationsinfrastruktur in den betroffenen Regionen der USA erheblich beeinträchtigte; Unfälle wie der Tunnelbrand in Baltimore am 18. Juli 2001, der wichtige Glasfaserkabel zerstörte,¹⁴⁰ aber auch menschliches Fehlverhalten und das unvermeidliche technische Versagen. Denn Menschen und Techniken versagen immer wieder, schaffen im täglichen Ablauf die häufigsten Probleme, die oft hohe Kosten verursachen. Zum menschlichen Versagen gehört die Missachtung von Vorschriften und Sicherheitskonzepten, etwa beim

¹⁴⁰ Das Internet und andere Datendienste fielen zwischen Washington und New York zeitweilig aus.

Passwortschutz. Institutionelle und individuelle Schwächen ermöglichen Datendiebstahl, Unterschlagungen etc., aber auch Sabotage. Täter sind oft ehemalige Mitarbeiter oder Innentäter, also Personen, die in einem Unternehmen arbeiten, dort Zugang zu Netzwerken haben oder sich verschaffen und die über interne Kenntnisse der Strukturen, Abläufe und Sicherheitsmaßnahmen verfügen [BSI, 2005], [Insider Threat Study, 2005], [Randozzo, 2004], [Messmer, 2003]. Dass Unternehmen über ein durchaus nicht randständiges Innentäterproblem ungern reden, ist gut zu verstehen, weist es doch nicht zuletzt auf unzulängliche interne Schutzmaßnahmen hin. In einem engen Zusammenhang damit stehen organisatorische Mängel, etwa bei der Überprüfung bzw. konsequenten innerbetrieblichen Umsetzung von Schutzmaßnahmen, denen Unternehmens- und Behördenleitungen zu oft nicht die notwendige Aufmerksamkeit zukommen lassen. Mangelnde Sicherheitskultur ist Teil des institutionellen Versagens, das freilich als ein internes und damit prinzipiell handhabbares Problem erscheint. Schulung, Information und organisatorische Veränderungen gelten als Heilmittel. Äußere Bedrohungen erscheinen in der Wahrnehmung gefährlicher: Sie sind auferlegt, kaum zu beeinflussen oder zu kontrollieren und damit nur schwer zu verhüten. Schutzmaßnahmen müssen aus einer Position der Unkenntnis über Motive, Ziele und Fähigkeiten der Angreifer, der Unsicherheit über den Ablauf des Angriffs, der Defensive und Reaktion formuliert und umgesetzt werden. Sie sind zwar bis zu einem (ungewissen) Punkt Erfolg versprechend, aber oft kostspielig und mit vielen Unwägbarkeiten verbunden, die erhebliche Verwundbarkeiten gegenüber Angriffen zurücklassen können.

Offene Fragen zur Sicherheitslage

Trotz der Vielfalt der Gefahren finden heute in Politik und Gesellschaft diejenigen besondere Aufmerksamkeit, die durch beabsichtigte, gezielte Handlungen und Angriffe hervorgerufen werden können. Dabei richtet sich der besorgte Blick verschärft auf externe Akteure, deren Zahl und Gefährlichkeit inzwischen die der Innentäter übersteigen soll: Ihre Angriffe auf Unternehmen, Behörden etc. nehmen zu, werden öfter von anderen Ländern aus geführt, werden ausgefeilter, organisierter und dienen vermehrt kriminellen Zwecken [FBI, 2006], [PITAC, 2005], [CSI/FBI, 2005], [Pulliam, 2005a], [Symantec, 2006], [CERT/CC, 2003].

Im Rahmen dieser heute vorherrschenden Fokussierung auf kriminelle und potentiell terroristische Täter bleiben Fragen offen. Ihre Beantwortung würde besser Auskunft geben über die Entwicklung der Gefahren und über das, was in Zukunft drohen könnte: Wie viele Angriffe gibt es, wie entwickeln sich die Zahlen? Wie groß sind die Schäden, die diese Angriffe verursachen, und steigen sie? Aus welchen Ländern kommen die Angriffe, wer ist für sie verantwortlich und welche Motive, Ziele treiben die Angreifer?

Es gibt keinen Staat, keine internationale Organisation, kein Unternehmen, das exakt und für die Allgemeinheit verbindlich definiert, wann ein Cyberangriff vorliegt, und es gibt nirgendwo *die* Stelle, die von allen Angriffen erfährt, die in einem Land oder gar weltweit erfolgen. Daher sind Zahlen über Cyberangriffe, die in Publikationen genannt werden, bestenfalls Näherungswerte, im schlechtesten Fall gezielt gestreut, und sie sollten immer unter Vorbehalt stehen.

Weit verbreitet ist die allgemeine Definition eines Angriffs, nämlich ein nicht autorisierter Zugriff bzw. Zugriffsversuch auf Rechner und Netzwerke. (Physische Angriffe erfasst diese Definition nicht. Sie sind aber in der Regel leicht erkennbar.) Die Definition lässt zu, schon den Versuch oder nur den Erfolg als einen Angriff zu betrachten. In einigen Ländern, darunter Deutschland, muss ein Angreifer in das Netzwerk eingedrungen sein, damit juristisch gesehen ein Angriff vorliegt. Für eine sicherheitspolitische Bewertung der Gefährdung, denen Netzwerke ausgesetzt sind, ist das unzureichend, denn die Sammlung von Informationen, das Auskundschaften von Schwachstellen, wichtige Schritte bei der Vorbereitung eines Angriffs, bleibt dann meist unbeachtet. Aber auch die Suche nach Indizien für eine Angriffsvorbereitung kann zu unklaren Ergebnissen führen, wie ein Beispiel zeigt: Ein Ping (ICMP-Echo-Request), ein Programm zur Überprüfung der Erreichbarkeit eines bestimmten Rechners im Internet, ist harmlos, wenn es für Wartungs- oder für Forschungszwecke genutzt wird. Auch die Internet Mapping Software zur Erkundung der Internettopologie [Lepperhoff, Fischer, 2004] nutzte Pings. Ein Ping kann aber auch ein Erkundungssignal sein, mit dem ein Angriff vorbereitet wird, der Rechner mit Datenpaketen überflutet¹⁴¹ - sind Pings schon Teil eines (drohenden) Angriffs und sollten gezählt werden, selbst wenn die Datenflut ausbleibt? Ob ein Angriff vorliegt, kann also von spezifischen und subjektiven Einschätzungen beeinflusst sein. Zudem werden Soft-

¹⁴¹ <http://www.computerbase.de/lexikon/Smurf-Attacke>.

ware- bzw. Hackerangriffe oft erst nachträglich, mit einiger Zeitverzögerung entdeckt, und getarnte Angriffe, die gänzlich unbemerkt bleiben, führen zu einer Dunkelziffer. Ein weiterer Unsicherheitsfaktor liegt in der Methodik der Zahlenerhebung. Zahlen über Angriffe beruhen meist auf Schätzungen bzw. Extrapolationen von mehr oder weniger sporadischen Umfragen in einer variierenden Anzahl von Unternehmen, Behörden etc. bzw. auf freiwilligen Meldungen, die Sicherheitsfirmen oder CERTs zu-gehen. Oft mangelhaft ist die Beteiligung an Umfragen: Auf Fragebögen, die Basis des Computer Crime Survey der US-Bundespolizei FBI sind, reagierten nur etwa zehn Prozent der angeschriebenen Unternehmen. (Neuere Umfragen sollen eine et- was höhere Quote der Antworten aufweisen.) Dies trägt, nicht nur in den USA, wahr- scheinlich zu der Dunkelziffer bei. Denn Unternehmen teilen nicht alle Angriffe mit, da sie befürchten, dass die Strafverfolgungsbehörden, werden Angriffe bekannt, aktiv werden und Probleme in Unternehmen offen legen, die zu einem Reputationsverlust führen. Es gibt aber auch Entwicklungen, die Dunkelziffern aufhellen. Wahrscheinlich steigt die Zahl der gemeldeten Angriffe, weil sie durch mehr und bessere Systeme (intrusion detection systems) erkannt werden. Zudem kann eine steigende Zahl von Meldungen die Bereitschaft bislang Zögernder erhöhen, Zahlen zur Verfügung zu stellen.

Nun legen die Untersuchungen der Sicherheitsbehörden, Forschungseinrichtungen und CERTs nahe, dass es nicht nur eine stärkere Erfassung, sondern eine tatsäch- lich steigende Zahl von Angriffen gibt. Das heißt aber nicht notwendigerweise, dass das Internet immer stärker bedroht wird. Das wäre der Fall, wenn die Zahl der Angrif- fe in Relation zur ebenfalls wachsenden Bevölkerung des Netzwerkes steigt, also die Angriffe pro Million Internetnutzer über die Jahre hinweg signifikant zunehmen wür- den. Schon die Unbekannten in der Gleichung, die Zahl der Internetnutzer und die der Angriffe, erschweren eine solche Aussage. Zudem führt ein kriminelleres Internet nicht per se dazu, dass die Gefahren für Nutzer und Netzwerk größer werden und die Schäden zunehmen. Denn nicht jeder Angriff ist wirksam, und es ist wahrscheinlich, aber keinesfalls sicher, dass die Wirksamkeit der Angriffe tendenziell steigt und sie schwerwiegendere Folgen haben. Denn hier kommt der Angegriffene ins Spiel, der lernen und durch eine wirksame Verteidigung, durch planvolles Krisenmanagement die Auswirkungen von Angriffen dämpfen kann. Leider scheint die Lernkurve der Be- drohten, obwohl auch sie steigt, nicht so steil zu verlaufen wie die der Angreifer.

Wie wirksam ein Angriff ist, ist nicht einfach an einer Skala abzulesen, die an allen Orten und zu allen Zeiten gleich ist. Ein belastbares, breit genutztes Bewertungssystem fehlt, das Angriffe in eine breit genutzte Gefahren- und Wirkungsskala einordnet (rating). Aber es gibt einen universellen Maßstab, mit dem die Auswirkungen eines Angriffs, freilich erst im Nachhinein, gemessen werden könnten - seine Kosten, also der Verzehr von Werten, die ein Angegriffener besitzt. Was sich so einfach anhört, ist in der Praxis aber schwer zu ermitteln. Das gilt für die Kosten der einzelnen Angriffe und für die, die gesamtgesellschaftlich anfallen. Daher überrascht es nicht, dass es divergierende Schätzungen darüber gibt, welche Kosten den Unternehmen, dem öffentlichen Sektor und, auch sie dürfen nicht vergessen werden, den einzelnen Bürgern durch Schadsoftware, Hacken etc. und seine Folgen, aber auch durch die Bemühungen entstehen, solche Folgen erst gar nicht eintreten zu lassen, sie also mit technischen, organisatorischen und pädagogischen Maßnahmen zu verhüten.

Folgt man der Literatur [CSI/FBI, 2004], sinken die Kosten, die ein durchschnittlicher Angriff mit sich bringt. Da die Zahl der Angriffe jedoch rascher wächst, steigen die Gesamtkosten. Wie hoch sie sind, können weder Polizei noch Sicherheitsunternehmen präzise beantworten. "Several computer security consultation firms produce estimates of total worldwide losses attributable to virus and worm attacks and to hostile digital acts in general. The 2003 loss estimates by these firms range from \$ 13 billion (worms and viruses only) to \$ 226 billion (for all forms of overt attacks)." Keine dieser Schätzungen ist wirklich belastbar, denn die Methodik, die ihnen zugrunde liegt, ist „basically anecdotal“ (Zitate [Cashell, 2004, Summary]). Systematische Forschungen stecken noch in den Kinderschuhen [Scalet, 2005], aber es gibt Hoffnung, dass sie ihnen entwachsen könnten.

Eine geeignete Methodik muss

- die (in)direkten Aufwendungen für Sicherheitsmaßnahmen erfassen, die getätigt werden, um Angriffe zu verhüten und abzuwehren (Abwehrkosten). Dazu gehören die Aufwendungen für den Erwerb von Schutzsoftware, intrusion-detection Systemen etc., für die Umsatzzahlen einschlägiger Unternehmen einen Anhaltspunkt liefern. Sie müssen ergänzt werden um die Kosten für die Installation, Aktualisierung der Software sowie für die Blockade von Speicher- und Prozessorkapazitäten, die der Betrieb dieser Systeme mit sich bringt. Schließlich fallen vergesellschaftete Kosten an wie die Ausgaben für Behörden, die sich mit Internetsicherheit, Strafverfolgung etc. befassen, aber auch die Kosten, die zur

Absicherung militärischer Netzwerke notwendig sind, soweit sie auf das öffentliche Internet aufsetzen bzw. mit ihm verkoppelt sind.¹⁴² Kaum zu erfassen und monetär zu bewerten sind die zeitlichen Aufwendungen der privaten Netznutzer, die selbst oder mit freundschaftlicher Hilfe ihre Rechner abzusichern suchen.¹⁴³

- die direkten und indirekten individuellen, betriebs- und volkswirtschaftlichen Kosten ermitteln, die trotz Vorsorge durch Cyberangriffe verursacht werden (Folgekosten). In der Regel beziehen sich die zitierten Untersuchungen auf Kosten, die Angriffe verursachen, die tatsächlich stattgefunden haben, wobei oft eine Dunkelziffer eingerechnet wird, von der nicht klar ist, wie sie ermittelt wird. Da Angaben von Unternehmen über Schäden und Kosten spärlich fließen, müssen auch hier Schätzungen weiterhelfen - keine stabile Basis für eine tragfähige Kalkulation. Vereinzelt gibt es auch Versuche, die Auswirkungen strategischer Angriffe monetär zu quantifizieren, die das Netz großräumig, für einige Tage beeinträchtigen und weite Teile der Volkswirtschaft in Mitleidenschaft ziehen würden. Da es sie bislang nicht gab, müssen Annahmen getroffen werden, etwa über den Einbruch des elektronischen Handels, der Internet-Bankgeschäfte etc. und über weitere volkswirtschaftliche Effekte - eine schwer zu lösende Aufgabe, setzt sie doch gute Kenntnisse über die Abhängigkeit der Sektoren vom Netzwerk voraus.

Alle Untersuchungen über Folgekosten, ob sie tatsächliche oder hypothetische Angriffe zum Gegenstand haben, müssen zuerst die Umsatzverluste abschätzen, die Cyberattacken nach sich ziehen. Zu berücksichtigen sind weitere direkte Kosten, die bei Unternehmen, Behörden anfallen, wenn sie Schäden beheben und Systeme wieder anfahren, also Ausgaben für den Einsatz von Experten, für Überstunden. Sie können, wie bei technischen Störungen, recht gut ermittelt werden, falls Unternehmen solche Zahlen erheben und verfügbar machen. (Wiederum sind die Schäden, die bei den individuellen privaten Netznutzern entstehen, bestenfalls grob zu schätzen.) Schwer zu beziffern sind indirekte Kosten: durch den sinkenden Marktwert eines Unternehmens, dem Kunden nach einem Angriff weniger vertrauen; durch Produktivitätsverluste, die ein Angriff nach sich zieht; durch Ausweichmaßnahmen, wenn angesichts potentieller Gefährdungen oder bei Angriffen verstärkt die bisher genutzten Kommunikationswege anstelle der effizienteren Netzwerke beschritten werden; durch Kosten, die Folge der höheren

¹⁴² Aus diesem öffentlichen Netz werden täglich zahlreiche Angriffe auf militärische Rechner geführt.

¹⁴³ Zu einem Versuch der monetären Bewertung vgl. <http://post-gazette.com/pg/06225/712889-96.stm>.

Auslastung von Netzkapazitäten sind, die diverse Angriffe und Schadsoftware verursachen (ein eher marginaler Faktor).

Mutige methodische Schritte haben Schweizer Forscher getan [Dübendorfer, Wagner, Plattner, 2004]. Sie haben ein Modell zur Abschätzung betrieblicher Kosten strategischer Störungen des Internets entwickelt, das in Richtung volkswirtschaftlicher Kosten weiterentwickelt werden kann. Nach einem Szenario, das mit diesem Modell gerechnet wurde, brächte der Ausfall des gesamten Internets in der Schweiz für eine Woche durch einen Cyberangriff - ein für Angreifer zweifellos herausforderndes Szenario – Verluste von fast sechs Milliarden Schweizer Franken, etwa 1,2 Prozent des Schweizer Bruttosozialprodukts. (Diese Angaben, so die Quelle der Daten, das Unternehmen mi2g,¹⁴⁴ würden sich mit eigenen Kalkulationen decken.) Der Löwenanteil dieser Kosten stammt wahrscheinlich von den unterstellten Umsatzverlusten der Unternehmen. Ähnliche Schritte werden in den USA gegangen. Die ersten Ergebnisse von Modellrechnungen zeigen, jedoch nur für spezifische Sektoren [Dynes, Andrijicic, Johnson, 2006], dass die Folgekosten von Ausfällen des Internets über gut eine Woche zwar hoch, wenn auch geringer als oft erwartet sind.

Jedoch müssen die größten Kosten, mag es um Unternehmen oder die Volkswirtschaft gehen, nicht immer Folge eines Ausfalls des Netzwerkes sein. Möglicherweise gefährlicher wäre es, wenn Angreifer unbemerkt Daten verändern, mit denen Unternehmen, Behörden etc. längere Zeit arbeiten, so die U.S. Cyber Consequences Unit, die für das Heimatschutzministerium arbeitet [Jackson, 2006] und sich auch mit der Kosteneffektivität von Cybersecurity-Maßnahmen befasst. Der Aufwand, die Fehler wieder rückgängig zu machen, falls das überhaupt gelänge, wäre enorm. Maßnahmen für Cybersecurity müssen das berücksichtigen und nicht fixiert sein auf den Aufbau einer Line, die Unternehmen, Behörden etc. mit Software nur nach Außen verteidigt (perimeter defense). Sie müssen auch interne Strukturen und Prozesse entwickeln, die flexibel genug sind, rasch solche Durchbrüche zu entdecken und mit ihren Folgen umzugehen.

Individuelle und kollektive Kosten können auch durch Spam anfallen. Spam ist seit Mitte der 90er Jahre mit der Verbreitung der E-Mail-Adressen zu einem ernsthaften, kostspieligen Problem geworden, das sich nun auch auf Mobiltelefone und VoIP ausweiten könnte. Spam ist zwar weder ein Angriff im engeren Sinne noch ein prinzipiell

¹⁴⁴ Vgl. <http://mi2g.com/> via Suchfunktion "More than 1% GDP drop estimated".

neues Marketingkonzept. Aber er gewinnt durch das Internet eine andere Qualität und kann durch das massenhafte Auftreten durchaus Merkmale eines Angriffs haben, wenn er den Eingangsbereich für die elektronische Post (Mailbox) verstopft. Im Gegensatz zur schon lange vertrauten Zusendungen unerwünschter Papierreklame, die vergleichsweise teuer ist und daher gezielter erfolgt, wird Spam an eine große Zahl von Internetnutzer ziemlich blind verstreut. Der Massenversand ist möglich, weil die Versandkosten für den Versender gering und weitgehend unabhängig von der Zahl der verschickten E-Mails sind. Nutzt er dazu sogar, illegal und heimlich, fremde Rechner als Zombies,¹⁴⁵ entlastet ihn das dann von allen Kosten [BSI, 2005]. Die Schätzungen über den Anteil von Spam an den etwa 30 Milliarden E-Mails, die Mitte 2006 täglich verschickt wurden, reichen von 40 bis zu 80 Prozent. Spam muss aussortiert, gelöscht werden, und er belastet schmalbandige Netzteile stark - alles das ist mit Kosten verbunden, die sich nicht immer klar als Abwehr- oder Folgekosten einordnen lassen. Denn das Löschen einer ungeöffneten Spam-Nachricht kann die Freisetzung eines Schadprogramms verhindern. Denn gefährlich und kostenträchtig wird Spam besonders dann, wenn er nicht nur Reklame, sondern solche Schadprogramme enthält und Teil anderer krimineller Aktivitäten ist. Da schon die Basiszahlen (Anteil des Spam an den E-Mails, Grad der Durchseuchung mit Schadprogrammen) unsicher sind, überrascht es nicht, dass auch die Schätzungen der Gesamtkosten durch Spam weit auseinander liegen: Zwischen einigen bis über 20 Milliarden Dollar pro Jahr.

Welche Zahl auch immer richtig ist - Spam verursacht Kosten, kann gefährlich sein und ist allzeit lästig. Deshalb gibt es seit Jahren Versuche, der Ausbreitung von Spam entgegenzutreten. An ihnen beteiligen sich neben Staaten und internationalen Organisationen große Internetfirmen, und die Bemühungen zielen darauf ab, die Versender von Spam zu identifizieren, sie straf- und zivilrechtlich zu verfolgen. In immer mehr Ländern ist Spam verboten, freilich ohne dass jederzeit eine wirksame Strafverfolgung gewährleistet ist, die aufwändig und teuer ist. Von internationaler Seite ist die OECD besonders aktiv, regional die EU-Staaten und national die USA, neuerdings auch Südkorea.¹⁴⁶ Das geschieht nicht ohne Grund, denn 2005 stamm-

¹⁴⁵ Ein Zombie ist ein Rechner, den Schadsoftware zum Teil eines roBOTNETworks (botnets) macht, das von dem Schreiber der Software oder von einem Kunden, der das botnet mietet, gesteuert wird.

¹⁴⁶ [http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_ITU_Bueti_Survey.pdf](http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_ITU_Bueti_Survey.pdf;);
<http://oecd-antispam.org/>; für die EU COM(2004)28 final,
<http://europa.eu/scadplus/leg/en/lvb/l24190a.htm>.

ten aus den USA, mit sinkender Tendenz, noch immer ca. 25 Prozent des weltweiten Spam, gefolgt von Südkorea (20 Prozent) und der VR China mit etwa 15 Prozent.¹⁴⁷ (Solche Zahlen sind nur begrenzt zuverlässig, sie verändern sich von Jahr zu Jahr, und der von .com-Adressen versandte Spam ist keinem Land zuzuordnen.) In Deutschland hat der Verband der Internetwirtschaft eco eine Anti Spam Task Force eingerichtet,¹⁴⁸ der Gesetzgeber strebt ein verändertes und, wegen eines angeblich unzulänglichen Verbraucherschutzes, umstrittenes Teledienstegesetz (Anti-Spam-Gesetz) an: Es sieht Geldstrafen vor, wird der Absender verschleiert oder der kommerzielle Charakter einer E-Mail verborgen.¹⁴⁹ Auch jeder Nutzer kann sich an der Spam-Abwehr durch Schutzprogramme und durch die Meldung von Spam beteiligen.¹⁵⁰

Ob alle diese Aktivitäten wirklich dauerhafte Erfolge bringen, ist nicht sicher. Viele der Aktionen und Maßnahmen erfolgen ad hoc, wenig abgestimmt, und zahlreiche Firmen tummeln sich Netz, die mehr oder weniger wirksame Gegenmittel anpreisen. Sind sie es dann wirklich und drängen Spamversender in die Defensive, drohen Gegenschläge: Im Juni 2006 führten kriminelle Versender, vermutlich aus Russland, erfolgreiche Cyberangriffe auf die kleine Anti-Spam-Firma Blue Security (und ihre Kunden) durch, die wirksam Spam abwehrte, weil sie selbst aggressiv agierte und ähnliche Mitteln wie die Versender einsetzte.¹⁵¹

Die Diskussion über die Kosten, die Cyberangriffe mit sich bringen, beschäftigt nicht nur Unternehmen und Wissenschaft, sondern auch die Politik. Meist geht es um mehr als die Suche nach exakten Zahlen. Gerne werden Kostenschätzungen aufgegriffen, wenn sie als Beleg dafür dienen können, dass es um die Cybersecurity mehr oder weniger schlecht steht, je nach Interessenposition. Verschwiegen werden dabei oft die Probleme von Methodik und Daten, und nur selten ist zu lesen, dass alle Zahlen bestenfalls Tendenzaussagen sind. Skepsis ist also angebracht gegenüber allen Kostenzahlen für Wirtschaft und Gesellschaft. Das heißt aber nicht, dass der Bot-schaft, die sie transportieren sollen, grundsätzlich mit Misstrauen zu begegnen ist: Das Internet ist sehr wichtig geworden, Angriffe können schweren Schaden stiften, und deshalb ist Internetsicherheit eine Herausforderung für Politik und Gesellschaft.

¹⁴⁷ <http://www.sophos.com/pressoffice/news/articles/2006/07/dirtydozjul06.html>.

¹⁴⁸ Vgl. http://www.eco.de/servlet/PB/menu/1214375_11/index.html.

¹⁴⁹ <http://www.heise.de/newsticker/meldung/74271>; [heise.de/newsticker/meldung/59484](http://www.heise.de/newsticker/meldung/59484).

¹⁵⁰ Vgl. z. B. die Seite <http://www.wettbewerbszentrale.de/de/beschwerdestelle/default.asp?bereich=2>.

¹⁵¹ Vgl. die Beiträge von T. Fischermann: zeit.de/online/2006/21/blue-security-spam; zeit.de/2006/21/Spam_xml; zeit.de/online/2006/21/blue-security-spam-faq.

Ein weiteres Problem bereitet die Identifizierung der geographischen Herkunft der Angreifer. Erkennen lässt sich ein Grundmuster, das sich aus dem Verzeichnis der Zombierechner der Sicherheitsfirma Ciphitrust¹⁵² ergibt, von denen es Mitte 2005 etwa 11,5 Millionen geben soll [Matai, 2005]. Angriffe werden überwiegend von Rechnern aus geführt, die in Ländern mit guter, breitbandiger Internetinfrastruktur stehen (vgl. [Symantec, 2006]): den USA, der EU, Südkorea, Taiwan, Japan, aber auch Russland und der VR-China, wo es Ende 2005 schon etwa 50 Millionen Breitbandnutzer gibt. Jedoch muss das nicht heißen, dass die Angreifer auch aus diesen Ländern stammen. Sie können in anderen Weltregionen sitzen und von dort aus die Angriffe steuern, die sie nur deshalb über die genannten Staaten führen, weil deren breitbandige Infrastruktur große Datenmengen transportieren kann, weil dort viele ungeschützte Rechner zu ferngesteuerten Botnets gehören oder weil die Aufklärung und Strafverfolgung, wie in China, wenig wirksam ist [Sturgeon, 2006]. Daher sind Zahlen über die Herkunft der Angriffe insbesondere dann mit Vorsicht zu genießen, wenn mit ihnen politische Interpretationen einhergehen wie Sicherheitsprobleme seien vorwiegend hausgemacht, Cyberangriffe in westlichen Staaten würden überwiegend von ihnen selbst aus geführt, und Attacken aus Staaten mit unberechenbaren, diktatorischen Regimen oder aus schwachen Staaten heraus seien eher selten und wenig wirksam. Der Vorstandsvorsitzende der Sicherheitsfirma mi2g, glaubt sogar zu erkennen, dass politische Instabilität und Angriffslust zusammenhängen: „The higher the number of digital attacks originating per capita the greater the political and social instability in the country.“ [Matai, 2005]. Eine Erklärung dafür könnte sein, dass für Angreifer in solchen Ländern die Gefahr einer Strafverfolgung gering ist. Skeptisch muss aber stimmen, dass diese Staaten meistens über eine nur schwache, oft auf einem wackeligen Telefonnetz basierende Internetinfrastruktur verfügen. Sie ist nicht der ideale Ausgangspunkt für Angriffe. Ohnehin sagen Herkunftszahlen per se nichts aus über die Gefährlichkeit und schon gar nichts über Organisation und Motivation der Angreifer. Soll der Verursacher eines Angriffs identifiziert werden, ist oft aufwändige Internet-Forensik¹⁵³ durch Spezialisten notwendig, die bislang meist per Hand erfolgen muss und beileibe nicht immer zum Ziel führt. Nicht alle Länder und ihre Behörden, schon gar nicht alle Unternehmen und nur wenige Private haben die Möglichkeiten, eine solche Spurensuche zu betreiben. Sie kann zudem rechtlich heikel

¹⁵² <http://ciphitrust.com/resources/statistics/zombie.php>.

¹⁵³ <http://www.de.wikipedia.org/wiki/IT-Forensik>.

sein, da sie oft ohne (strafbares) Eindringen in fremde Rechner schnell zu Ende geht.¹⁵⁴ Ein automatisches Verfolgen und Identifizieren von Angreifern würde Veränderungen bei Protokollen und im Routingsystem erfordern. Dadurch ginge eine Stärke des Netzes verloren: Nutzern, die einige technische Vorkehrungen beachten, haben eine Chance, mit einer (freilich ungewissen) Wahrscheinlichkeit ihre Anonymität zu wahren (s. u.). Dies stützt, ein positiver Effekt, die freie Meinungsäußerung. Aber selbst wenn einzelne Angreifer identifiziert werden, bleiben ihre persönlichen, soziologischen, politischen, kulturellen Charakteristika häufig im Dunkeln: Agieren sie alleine, gehören sie zu einer Gruppe, welche Ziele und Motive treiben sie? Datenbänke und Modellierung, die Informationen über Angriffe, Angriffsmuster und Angreifer zusammentragen bzw. sie durch Vermutungen ergänzen, sollen mehr Licht werfen auf diese Charakteristika [Parker, Devost, 2005], [Parker, 2003].

Die Verschärfung der Sicherheitslage

Alle diese berechtigten Anfragen an die Zahl der Angriffe, ihre Auswirkungen, Herkunft und Merkmale dürfen nicht darüber hinwegtäuschen, dass sich sehr wahrscheinlich in der Realität, sicher aber in der vorherrschenden Wahrnehmung von Fachwelt, Politik und Öffentlichkeit die Sicherheitslage im Internet über die Jahre verschlechtert hat, dass sie sich weiter verschärfen wird [Cybersecurity, 2005, S. 9ff], und dass Angreifer immer besser die Vorteile zu nutzen wissen, die ihnen das Netzwerk bietet:

- Grundsätzlich haben Angreifer im Netzwerk den Vorteil, dass sie Zeitpunkt, Mittel, Dauer und Ziel eines Angriffs bestimmen. Zudem können sie von jedem Punkt aus jedes Ziel erreichen. Das zwingt einen Verteidiger dazu, sich prinzipiell auf alle denkbaren Angriffe von allen Orten des Netzes aus vorzubereiten. Eine solche Lage kann auch den Fähigen und Willigen überfordern: „Defending modern information system could also be likened to defending a large, thinly-populated territory in the nineteenth century Wild West: the men in black hats can strike anywhere, while the men hats have to defend everywhere.“ [Anderson, 2001].
- Personen oder Gruppen haben eine gute Chance unbeobachtet und unerkannt zu bleiben, wenn sie die Funktionsweise des Internets kennen und z. B. Proxy-

¹⁵⁴ Überlegungen, dass staatliche Stellen mit richterlicher Zustimmung in dringenden Fällen online Rechner durchsuchen dürfen, sollten nicht vorschnell beiseite geschoben werden.

Caching-Server¹⁵⁵ oder dynamische IP-Nummern für ihre Netzaktivitäten nutzen (vgl. [Rotert, 2004]). Diese an sich sinnvollen Dienste können missbraucht werden - die negativen Seiten der Chance, im Netz anonym zu bleiben. Zwar fallen auch hier Verbindungs- und andere Daten an, die nur der Provider kennt und die prinzipiell von Strafverfolgungsbehörden eingesehen werden können. Aber stehen die Server im Ausland, reicht der Arm der Behörden nicht immer so weit.

- Der zeitliche, personelle und finanzielle Aufwand für Identifikation, Überwachung, Abwehr und für die Verfolgung von kriminellen Aktivitäten und Angreifern im Netz durch darauf spezialisierte Unternehmen, Nachrichtendienste, Strafverfolgungsbehörden oder engagierte Individuen ist hoch und hängt oft von der Kooperationsbereitschaft anderer Staaten ab, wie das Beispiel der Proxy-Server zeigt: Die originären Nutzerdaten liegen zwar auf diesem Server, aber steht er im Ausland, sind Strafverfolgungsbehörden auf zwischenstaatliche Kooperation angewiesen. Zudem sind die Behörden in einem Netz rechtlicher Regelungen, etwa des Datenschutzes, eingebunden, das inzwischen zwar breitere Maschen aufweist, aber weiterhin ihre Bewegungsfreiheit deutlich beschneidet, was prinzipiell einem Rechtsstaat angemessen ist. Vergleichbare Probleme haben Angreifer nicht, und die Kosten, die bei ihnen anfallen, sind meistens gering. Im Netz findet sich aktuelle Software, die es ermöglicht, Sicherheitslücken in der Nutzer- und Betreibersoftware rasch auszunutzen. Verschlüsseln Kriminelle zudem ihre Kommunikation mit Hilfe von Privacysoftware, kann sie von Polizei und Geheimdiensten nur mit sehr großem Aufwand entschlüsselt werden: Angriffsvorbereitungen und andere kriminelle Aktivitäten können verborgen bleiben [Wilson, 2006].
- Recht und Gesetz lassen sich oft nur schwer durchsetzen. Politische Grenzen, unterschiedliche Straftatbestände, politisch gewollte Kooperationsmängel erschweren die Ermittlung und Strafverfolgung, und die praktische Zusammenarbeit kann sich verheddern im Gestrüpp divergierender Interessen und unterschiedlicher Fähigkeiten und Handlungsbereitschaften der Sicherheitsbehörden. Das Strafmaß schreckt Cyberangreifer und -kriminelle nicht ab, wenn sie mit hoher Wahrscheinlichkeit darauf vertrauen können, nicht ermittelt oder angeklagt zu werden.

¹⁵⁵ Vgl. <http://www.uni-duesseldorf.de/Proxy/Artikel.shtml>.

Das heißt aber nicht, dass das Internet ein gesetzesfreier Raum ist, wie manche befürchten und andere erhoffen. Denn jeder Internetnutzer ist den Rechtsnormen unterworfen, die in dem Land gelten, in dem er lebt. Das löst aber nicht das (ganze) Problem. Denn die grenzüberschreitende Rechtssetzung, Kriminalitätsverhütung und Strafverfolgung sind erst im Aufbau, während das Internet schon lange die Möglichkeit gewährt, von Außen in einem Land zu operieren, ohne dass das territorial gebundene Rechtssystem dem jederzeit effektiv entgegenwirken kann. Zwar gibt es durchaus erfolgreiche internationale juristische Zusammenarbeit bei der Strafverfolgung, die sich auch auf Auslieferungsabkommen stützt: So soll ein Brite, der in US-Netze eingedrungen ist, ausgeliefert werden.¹⁵⁶ Aber die Vertiefung und Verbreiterung der Kooperation trifft immer wieder auf Probleme, wie die Konvention des Europarates über Cyberkriminalität¹⁵⁷ zeigt. Sie soll als erste internationale Vereinbarung über Straftaten im Cyberspace einheitliches materielles und prozessuales Recht schaffen sowie die Rechtshilfe verbessern. Die Konvention benennt Verstöße gegen Integrität, Vertraulichkeit, Verfügbarkeit von Daten und Systemen, computergestützten Betrug und Fälschung, inhaltsbezogene Delikte (Verstöße gegen Kinder-, Jugendschutz) sowie Urheberrechtsverstöße als Straftatbestand. Sie ist zwar in Kraft, war aber Mitte 2006 nur in zwölf Staaten in nationales Recht umgesetzt (darunter Frankreich, Ungarn, Dänemark), während weitere 33 Länder, auch Deutschland, sie lediglich gezeichnet haben. Denn es gibt diverse Vorbehalte gegen ihre Ratifizierung, etwa hinsichtlich ihrer Auswirkungen auf innerstaatliches Recht, sowie Verzögerungen bei der Umsetzung in nationales Recht. Ein Zusatzprotokoll gegen rassistische und fremdenfeindliche Akte im Internet ist mit sechs Ratifikationen (und weiteren 24 Unterzeichnungen) Anfang 2006 in Kraft getreten. Es musste außerhalb der Cyberkriminalitäts-Konvention vereinbart werden, da es in den USA ein nahezu grenzenloses, durch Verfassung¹⁵⁸ und Rechtsprechung des Obersten Gerichtshofes¹⁵⁹ geschütztes Recht auf Meinungsfreiheit gibt. Es deckt sehr oft auch rassistische, fremdenfeindliche etc. Äußerungen, die in anderen Staaten nicht geduldet

¹⁵⁶ <http://www.heise.de/newsticker/meldung/72953>.

¹⁵⁷ Vgl. <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>.

¹⁵⁸ Vgl. First Amendment: <http://usconstitution.net/const.html>.

¹⁵⁹ Etwa *Smith versus California*, 1959: <http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=us&vol=361&invol=147>; aggressiv verteidigt seit 90 Jahren die American Civil Liberties Union mit diversen Klagen eine unbegrenzte Meinungsfreiheit (<http://aclu.org>).

werden.¹⁶⁰ Wären die Bestimmungen des Protokolls in die Konvention eingegangen, könnten die USA nicht Mitglied werden. Trotzdem ist es bislang nicht gelungen, die Konvention über die Hürden des Senats zu heben. Zwar hat das Senate Foreign Relations Committee dem notwendigen Gesetz zugestimmt, aber in Plenum des Senats steht die Abstimmung noch aus. Zwei Drittel der Senatoren müssen „ja“ sagen, damit der Präsident die Konvention für die USA in Kraft setzen kann. Auch das Drängen der dem Vertrag wohlgesonnenen privaten US-Cyber Security Industry Alliance (CSIA), endlich zu ratifizieren,¹⁶¹ hat noch keinen Erfolg gezeigt.

Über die Konvention hinaus gibt es in der EU vielfältige und durchaus fruchtbringende Bemühungen, die Internetsicherheit rechtlich und organisatorisch besser auszugestalten. Daher gilt im internationalen Vergleich die EU in der Rechtssetzung als so weit vorangeschritten, dass führende Köpfe der CSIA feststellen: „Europe's cybercrime laws are ‘light years ahead’ of those in the US“ [Gross, 2005]. Die EU beschäftigt sich seit Ende der 80er Jahren mit der Sicherheit im und, verstärkt nach 2001, mit der Sicherheit des Internets. Wichtige Stationen sind die schon genannten Aktivitäten zum Kinder- und Jugendschutz und die entsprechenden Aktionspläne.¹⁶² Ende 1999 hatten die Mitgliedstaaten der EU bei der Sitzung des Europäischen Rates in Tampere die Notwendigkeit anerkannt, Einigkeit zu erreichen über Definitionen für bestimmte Straftaten, auch für solche, die mit moderner Technologien wie dem Internet begangen werden, sowie über ihre Sanktionierung. Der Kommission fiel die Aufgabe zu, Vorschläge zu entwickeln. Ein Jahr später hob der Europäische Rat auf seiner Tagung in Lissabon die Bedeutung hervor, die einer wettbewerbsfähigen, wissensbasierten Wirtschaft zukommt, in der das Internet eine wichtige Rolle spielt. Mit der (nach ihrem Scheitern 2005 neu gestarteten) Lissabon-Strategie sollte Europa innerhalb von zehn Jahren an die Spitze der Weltwirtschaft katapultiert werden.¹⁶³ Die Kommission musste nun Konzepte, Strategien und Programme entwickeln, die die Möglichkeiten der neuen Technologien ausschöpfen und zugleich die Informationsnetze sicherer machen. Zahlreiche Aktivitäten innerhalb der EU begannen: Seit dem Jahre 2000 laufen Aktionsprogramme zur Sicherheit von Netzwerken und zur Be-

¹⁶⁰ Solche Seiten, die in den USA abgelegt sind, können zwar durch Provider so gesperrt werden, dass sie von Deutschland aus nicht direkt zugänglich sind. Über Umwege gelingt das aber trotzdem.

¹⁶¹ Vgl. https://www.csialliance.org/publications/csia_whitepapers/CSIA_CoE_Convention.PDF.

¹⁶² Action Plan on Promoting Safer Use of the Internet, <http://europa.eu.int/ISPO/iap/decision/de.html>; <http://europa.eu.int/ISPO/iap/>.

¹⁶³ <http://www.de.wikipedia.org/wiki/Lissabon-Strategie>.

kämpfung der Computerkriminalität im Rahmen des eEurope-Programms.¹⁶⁴ Im Januar 2000 veröffentlichte die Kommission als Diskussionspapier ihre Mitteilung zur Schaffung einer sicheren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität (KOM(2000) 890 endg.).¹⁶⁵ Dieses Dokument enthält eine breite Analyse, die zu Empfehlungen über Maßnahmen und Initiativen für die Sicherheit von Informationsinfrastrukturen und zur Bekämpfung von Computerkriminalität führt. Betont wird, dass folgende Bedingungen erfüllt sein müssen, damit Cyberkriminalität wirksam bekämpft werden kann: Angemessene materielle und prozessuale gesetzliche Regelungen in allen relevanten Staaten, um auch internationalem (Cyber-) Terrorismus zu begegnen; genügend und gut ausgebildetes Personal bei den Strafverfolgungsbehörden; die bessere Zusammenarbeit zwischen allen Beteiligten, von den Behörden über Unternehmen bis hin zur Einbeziehung der großen Zahl der Netznutzer; die Durchführung konkreter Informations-, Schutzkampagnen und Maßnahmen. Im Jahre 2001 wurde die Einführung eines Europäischen Haftbefehls angeregt¹⁶⁶ und von den Staaten aufgegriffen, der für Computerkriminalität relevant ist. Er erwies sich aber in seiner rechtlichen Ausformung in Deutschland als verfassungswidrig und damit als nichtig.¹⁶⁷ 2001 veröffentlichte die Kommission ihre Mitteilung Network and Information Security: Proposal for a European Policy Approach (KOM(2001) 298 endg.).¹⁶⁸ Sie beschäftigte sich mit der Sicherheit der kritischen Infrastrukturen, definierte Angriffsformen auf Informationssysteme (Hacking, Denial of Service, Schadsoftware, Spoofing),¹⁶⁹ empfahl präventive Maßnahmen und formulierte einen europäischen Politikansatz für Netzsicherheit. Unter dem Eindruck von 9/11 legte die Kommission 2001 einen Vorschlag für einen Rahmenbeschluss des Rates zur Terrorismusbekämpfung vor (KOM(2001) 521 endg.).¹⁷⁰ Darin wird auf die Gefahr von Terroranschlägen auch auf Infrastrukturen, darunter Informationssysteme, hingewiesen, und die Verbesserung der Zusammenarbeit in der EU gefordert, u. a. durch die Angleichung der Rechtsvorschriften. Am 13. Juni 2002 wurde der Vorschlag in rechtsverbindlicher

¹⁶⁴ http://europa.eu.int/information_society/eeurope/2005/index_en.htm.

¹⁶⁵ <http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeComDE.pdf>.

¹⁶⁶ Vgl. <http://europa.eu/scadplus/leg/en/lvb/l33167.htm>.

¹⁶⁷ Vgl. <http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg05-064.html>

¹⁶⁸ http://europa.eu.int/information_society/eeurope/2002/news_library/pdf_files/netsec_en.pdf.

¹⁶⁹ Die Begriffe werden auf den folgenden Seiten erläutert.

¹⁷⁰ http://eur-lex.europa.eu/LexUriServ/site/de/com/2001/com2001_0521de01.pdf.

Form als Rahmenbeschluss des Rates zur Terrorismusbekämpfung umgesetzt.¹⁷¹ Im April 2002 präsentierte die Kommission den Vorschlag für einen Rahmenbeschluss des Rates über Angriffe auf Informationssysteme vor (KOM(2002) 173 endg.).¹⁷² Das Dokument vervollständigt und präzisiert den Aspekt der Angriffe auf Informationssysteme, der in KOM(2001) 521 angesprochen wurde. Beide gehören damit inhaltlich zusammen und lenken auch den Blick auf den Schutz des Internets gegen Angriffe. In dem Dokument von 2002 schlägt die Kommission eine Angleichung der einzelstaatlichen Strafrechtsvorschriften gegen Angriffe auf Informationssysteme und eine Stärkung der justiziellen Zusammenarbeit vor. Darüber hinaus enthält es insbesondere Begriffsbestimmungen wie Elektronisches Kommunikationsnetz, Computer (-daten), Informationssystem, juristische Person, befugte Person und unrechtmäßig. Enthalten sind dort auch Strafbestimmungen, um sicherzustellen, dass schwerwiegende Angriffe auf Informationssysteme in allen Mitgliedstaaten durch verhältnismäßige, wirksame und abschreckende Strafen geahndet werden. Am 24. Februar 2005 verabschiedete der Ministerrat auf dieser Grundlage den Rahmenbeschluss 2005/222/JI über Angriffe auf Informationssysteme (Framework Decision 2005 222/JHA), der auch die Strafverfolgung bei Hacken erleichtern wird.¹⁷³ Die nun anstehende Umsetzung des Rahmenwerks in den Staaten soll die EU¹⁷⁴ zum Vorreiter bei der Regulierung dieses schwierigen Politikfeldes machen. Weitere Meilensteine europäischer Politik sind die Errichtung der ENISA und die Richtlinie zur Vorratsspeicherung von Daten.

Alles das macht die EU jedoch noch nicht zu einer unbezwingbaren Festung der Internetsicherheit. Das ist schon deshalb nicht der Fall, weil global die Dinge rechtlich und im praktischen Vollzug noch deutlich ungeordneter sind. Wie wichtig die Angleichung des materiellen Rechts ist, zeigt auch der Fall des Loveletter-Virus im Jahre 2000. Der Programmierer, ein philippinischer Student, musste freigelassen werden, da zur Tatzeit in seiner Heimat das Schreiben von Viren nicht verboten war. Seither gibt es zwar Fortschritte beim Aufbau der rechtlichen und organisatorischen Grund-

¹⁷¹ <http://eurocrim.jura.uni-tuebingen.de/cms/de/doc/54.pdf>.

¹⁷² Proposal for a Council Framework Decision on Attacks against Information Systems; europa.eu.int/eur-lex/de/com/pdf/2002/com2002_0173de01.pdf; das Dokument zielt auch darauf ab, das Recht innerhalb der EU kompatibel zu machen mit der Cybercrime-Konvention.

¹⁷³ <http://europa.eu/scadplus/leg/de/lvb/l33193.htm>; einige der genannten EU-Dokumente finden sich auch unter <http://qlinks.net/quicklinks/status.htm#comcrime>.

¹⁷⁴ Zum Entwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität in Deutschland vgl. die Pressemeldung und den Text vom 20.9.06 unter <http://www.bmj.bund.de>.

lagen von Cybersecurity in einer Reihe von Staaten.¹⁷⁵ Jedoch verbreiten sich vergleichbare, kompatible Rechtssysteme in diesem neuen Politikfeld international noch immer sehr zäh, und die Probleme der Internetsicherheit finden in vielen Staaten in Politik und Behörden nicht die notwendige Aufmerksamkeit (vgl. [Schjolberg, Hubbard, 2005]). Deshalb ist international Cybersecurity und der Schutz von luk-Infrastrukturen generell noch immer ein Flickenteppich mit Löchern: „... solutions to CIIP challenges vary from country to country and are obviously influenced by historical, geographical, political, organizational, or cultural peculiarities or tradition, as well as by the resources at hand.“ [Abele-Wigert, 2006, S. 76].

Neben solche multilateralen, formalen Abkommen, die politisch und sachlich anspruchsvolle und oft schwer umzusetzende Formen der Kooperation sind, muss die aktive polizeiliche Bekämpfung von Cyberkriminalität in allen wichtigen Staaten treten. Dabei können pragmatische, informelle bzw. schon länger genutzte regionale Kooperationsformen zur Bekämpfung von Cyberkriminalität zum Einsatz kommen. Auch hier sind europäische Staaten im Rahmen des Europäischen Polizeiamtes Europol aktiv und führend.¹⁷⁶

Lassen Gesetzgebung und ihr praktischer Vollzug international und in vielen Nationen noch sehr zu wünschen übrig und hinken Schutzmaßnahmen oft der Bedrohung nach, könnten sich in einigen Ländern dauerhafte Sanktuarien für Cyberkriminalität oder -terrorismus herausbilden. Schwächelt die Sicherheit dort, leiden auch Staaten, die entschlossener nach Cybersecurity streben. Das hätte gravierende Auswirkungen auf die Sicherheit im und des Cyberspace insgesamt.¹⁷⁷ Darüber, wie dann mit solchen Räumen umgegangen würde, lässt sich nur spekulieren. Denkbar wäre, dass sie sogar, gehen von ihnen reale Bedrohungen aus, die nicht anders abzuwehren sind, zum Ziel offensiver, eventuell sogar präventiver Cyberoperationen werden könnten.

Strategien und Mittel von Angreifern

Angreifer und andere kriminelle Akteure können auf ein breites Spektrum von Mitteln und Strategien zurückgreifen, um im Internet die Integrität, Vertraulichkeit, Verfüg-

¹⁷⁵ Vgl. dazu die Informationen zu den Nationen in dem Gateway to Cybersecurity der ITU: <http://www.itu.int/cybersecurity/index.html>; einen ersten Einblick in die Rechtslage einiger Staaten gibt <http://cybercrimelaw.net/laws/survey.html>.

¹⁷⁶ Vgl. Stichwort Cyber-Kriminalität - rechtliche Rahmenbedingungen unter <http://www.bmi.bund.de/>; mit dem Europol-Vertrag vom 1.10.1998 besitzt das Amt eine rechtliche Grundlage.

¹⁷⁷ Vgl. das Interview mit Peter Swire: <http://www.zeit.de/online/2006/20/interview-swire>

barkeit, Zurechenbarkeit zu beeinträchtigen und um weiteren illegalen Aktivitäten im Netzwerk nachzugehen [Powner, 2005], [Gelbstein, Kamal, 2002], [Commission, 2001], [Convention, 2001]. Dabei passen sich die Akteure immer wieder den technologischen Entwicklungen an, reagieren auf Maßnahmen der Verteidigung und modifizieren ihr Vorgehen.¹⁷⁸ Diese Mittel und Strategien sind in der Regel, aber nicht immer, in einer steigenden Zahl von Staaten strafbewehrt. Ihr Einsatz erfordert in vielen und vermutlich in immer mehr Fällen nur mäßige Kenntnisse, da Schadsoftware im Internet verfügbar ist, und solche Angriffe können durchaus wirksam sein [Morel, 2006]. Fundierte Kenntnisse von Software, der Funktionsweise des Internets bzw. der angeschlossenen Rechner und ihrer Technik sind notwendig, wenn die Absichten der Akteure strategisch und die Angriffsziele spezifischer sind, etwa Netzwerke bzw. Rechner kritischer Infrastrukturen oder SCADA-Systeme, die über das Internet zugänglich sind.

Um ihre Ziele zu erreichen, können Angreifer vielfältige Wege und Strategien verfolgen und sich diverser Mittel bedienen:

- Sie versuchen, unbemerkt und nicht autorisiert einen Zugang zu Rechnern bzw. Netzwerken zu bekommen, um möglichst eine Rolle einzunehmen, die Systemkontrolle gewährleistet. Solche Root- oder Administratorenrechte gestatten es, Rechner vollständig zu kontrollieren und für eigene Zwecke zu nutzen. Hacken ist ein dafür genutztes Mittel. Technisch gesehen ist Hacken das Eindringen in ein System, um zu verstehen, wie es funktioniert, damit es verändert werden kann. Was in dieser Formulierung so harmlos daherkommt, ist aber meist eine kriminelle Tat. Hackerorganisationen,¹⁷⁹ um ihren Ruf besorgt, drängen deshalb darauf, Hacker anhand ihrer Fähigkeiten und vor allem ihrer Ziele zu unterscheiden:
 - Die begabten Sneakers wollen aus ehrlichen Motiven die Softwarehersteller auf Sicherheitslücken aufmerksam machen, die sie schließen sollen. Tatsächlich haben z. B. Microsoft und das FBI Kontakte zu ihnen,¹⁸⁰ und das Konzept der Ethical Hacker greift diesen Gedanken auf: Unternehmen bieten Kurse für

¹⁷⁸ Vgl. den Kaspersky-Bericht für 2006: <http://www.viruslist.com/en/analysis?pubid=204791914>.

¹⁷⁹ Ob der Computer Chaos Club e. V. (<http://www.ccc.de/>) eine Hackerorganisation ist oder nicht - er wird oft so bezeichnet.

¹⁸⁰ <http://www..com/index.php?id=2037517>.

Experten an, in denen diese sich in das Denken der Angreifer versetzen, um Schwachstellen in den eigenen Netzen zu finden, die sie dann schließen.¹⁸¹

- Unbedarfte Script Kiddies wollen Unfug treiben und Schaden stiften mit vorgefertigter Software, ohne aber weitreichende - und schon gar nicht politische - Ziele zu verfolgen.
- Die zerklüftete Gruppe der Hacktivists greife aus - so dürfe man unterstellen - manchmal ehrenwerten politischen Motiven diejenigen an, die sie als Gegner definieren [Jordan, Taylor, 2004]. Das Schadenspotential ist dabei latent hoch.
- Wirklich gefährlich sei die Gruppe der Cracker, die ihre kenntnisreichen Angriffe mit krimineller Energie und Absicht durchführen (Unterschlagung, Betrug etc., vgl. [Schell, Martin, 2004, S. 111ff]). Tatsächlich nimmt die Zahl dieser Kriminellen zu, und sie verbinden sich mit dem organisierten Verbrechen [McAfee, 2005], [Evers, 2005], [Jackson, 2004].

Ob diese Differenzierung den Ruf von Hackerorganisationen verbessert, sei dahingestellt. Aber sie ist für Einschätzungen der Gefahren sinnvoll, wenn sie Cyberterrorismus als potentielle eigenständige Bedrohung berücksichtigt, wie das [Parker et al., 2004] in ihrer ausführlichen Arbeit über die Merkmale von Cyberangreifern tun. Auch Sicherheitsunternehmen differenzieren Angreifer nach individuellen und kollektiven Merkmalen,¹⁸² und Forscher des Terrorist Research Centers¹⁸³ bemühen sich, die Fähigkeiten und Motive solcher Angreifer zu modellieren, um Abwehrmaßnahmen auf die gefährlichsten Bedrohungen und Strategien zu konzentrieren.¹⁸⁴ Ergebnisse wurden auf Tagungen des in Seattle ansässigen, international agierenden IT-Sicherheitsunternehmens BlackHat¹⁸⁵ vorgestellt [Parker, Devost, 2005], [Parker, 2003]. Keinesfalls aber darf diese Differenzierung der Akteure und eine Hierarchisierung der Gefährdungen den Blick dafür verstellen, dass das illegale, vorsätzliche und unbefugte Eindringen in Computer immer und überall strafbar sein muss, soll Internetsicherheit erhöht werden, und dass das in der Konvention des Europarates, in EU-Regelungen und in vielen

¹⁸¹ Vgl. die Seiten des International Council of Electronic Commerce Consultants, <http://eccouncil.org/>.

¹⁸² Die größte Datenbank über Hackergruppen und ihre Merkmale hat <http://mi2g.com/>.

¹⁸³ <http://terrorism.com/> /.

¹⁸⁴ Miller [2002] beschreibt hingegen Angreifer nur über ihre technischen Kenntnisse, die Art und Weise des Angriffs und die eingesetzten Werkzeuge, da bei ihm die unmittelbaren Reaktionsmöglichkeiten des Angegriffenen im Mittelpunkt stehen. Soziologische, motivationale Merkmale des Angreifers sind uninteressant, werden aber bei einer sicherheitspolitisch orientierten Betrachtung wichtig.

¹⁸⁵ <http://blackhat.com/>.

nationalen Gesetzen auch so gesehen wird. Auf dieser Grundlage kann, wie bei anderen Straftatbeständen auch, das öffentliche Interesse an der Strafverfolgung bzw. das Strafmaß von den Zielen der Angreifer beeinflusst werden. Ein Notwehr- oder Nothilferecht zur Identifizierung von Lücken in der Software durch illegales Hacken existiert nicht, auch wenn auf manchem so genannten Hackerkongress dieser Eindruck erweckt wird.¹⁸⁶

- Angreifer versuchen, die Arbeit von Routern, von Servern und damit die Funktionsfähigkeit des Netzwerkes selbst zu beeinträchtigen. Dazu können beispielsweise (distributed) Denial of Service (dDoS)-Angriffe ausgeführt werden, in denen Botnets eine weitere große Rolle spielen. Sie überschwemmen Rechner mit einer Flut von Datenpaketen, die aus allen Richtungen des Internets kommen. Mit dDoS-Angriffen wurde auch die Firma Blue Security zum Aufgeben gezwungen, und ein solcher Angriff hatte im Jahre 2002 einen Kernbereich des Internets, das Bereichsnamen-System, zum Ziel. Die dreizehn überwiegend von unabhängigen Organisationen betriebenen zentralen Root Name Server, von denen zehn in den USA stehen, wurden geflutet. Neun Server konnten ihre Aufgabe nicht oder kaum mehr erfüllen, aber die verbleibenden gewährleisteten, dass das Bereichsnamen-System den Angriff noch halbwegs funktionsfähig überstand. Mit der Anycast-Technik wurde inzwischen die Resilienz dieses Systems erhöht und die Massierung der Rootserver in den USA praktisch beendet: Anfragen werden nun in 100 weltweit verteilten Rootservern ortsnäher bearbeitet, so dass ein solcher dDoS-Angriff heute weniger wirksam wäre.¹⁸⁷ Aber die Bedrohung bleibt,¹⁸⁸ und Anfang 2006 gab es einen ähnlichen Angriff auf die Namensserver einer Top Level Domain. Fehlt eine gute, manchmal kostengünstige, meist aber kostspielige Vorbereitung auf einen dDoS-Angriff, müssen die Server vom Netz genommen werden. Fallen dann Unternehmensserver aus, sind sie für einige Stunden oder Tage für Kunden nicht mehr zu erreichen, und sie müssen Umsatz- und Vertrauensverluste hinnehmen. Dramatischer wäre es, würde ein dDoS-Angriff das Bereichsnamen-System trotz der Innovation längere Zeit lahm legen. Dann könnte ein Auseinanderfallen des globalen Internets drohen, da die Aktualisierung der Namens-Server

¹⁸⁶ Vgl. Chaos Communication Congress 2005, <http://www.ccc.de/congress/2005>; Berichte: heise.de.

¹⁸⁷ <http://www.root-servers.org/>; <http://www.dns.net/>; der von VeriSign (<http://www.verisign.com/>) betriebene A-Server bleibt der DNS-Schlüsselrechner; zu Anycast vgl. <http://www.de.wikipedia.org/wiki/Anycast>.

¹⁸⁸ Vgl. <http://computerwelt.at/detailArticle.asp?a=102718&n=5>.

durch die übergeordneten Root-Server nicht mehr gewährleistet wäre. Das würde wahrscheinlich, im Gegensatz zu dem Ausfall des Unternehmensnetzes, als gesamtgesellschaftliches, als sicherheitspolitisches Problem wahrgenommen.

- Durch den Einsatz schädlicher Software werden Daten unbefugt modifiziert, unterdrückt oder zerstört, um Schaden zu stiften oder eigenen Vorteil zu erlangen. Eingesetzt werden dafür Viren, logische Bomben, Würmer und trojanische Pferde, die diversen Zwecke dienen können. Viren sind Schadprogramme,¹⁸⁹ die sich nicht selbst vermehren, sondern dazu Hilfe brauchen, etwa von E-Mails. Erste Viren wurden in den 60er Jahren eher spielerisch entwickelt, und erst später bekamen sie einen schädlichen Charakter. In Rechnern außerhalb von Labors (in the wild) tauchten Viren Anfang der 80er Jahre auf. Da es keine einheitliche Konvention für die Kategorisierung von Viren gibt und immer neue geschrieben werden, ist ihre Zahl unbekannt: Schätzungen reichen bis zu 300 000,¹⁹⁰ und niemand kann wissen, ob es nicht doch mehr gibt. Von den Viren sind geschätzt nur etwa ein bis zwei Prozent freigesetzt.¹⁹¹ Logische Bomben treten durch ein Ereignis in Aktion (ein festgelegtes Datum, durch eine E-Mail), bleiben aber auf den Bereich beschränkt, in dem sie abgelegt wurden und vermehren sich nicht. Würmer enthalten Programme, die zur Selbstvermehrung führen, möglichst viele Rechner befallen und dazu Lücken in Programmen oder Protokollen nutzen. Würmer sind oft Transportmittel für Viren. Zusatzcodes erzeugen aus Viren und Würmern trojanische Pferde. Solche Trojaner, neuerdings angeblich Stars der kriminellen Internetszene, sind Programme, die sich in einem (nützlichen) Programm verstecken und Daten etc. suchen, identifizieren und weiterleiten, sich auf Rechnern einnisten, um sie zu kontrollieren und in Botnets einzubinden. Seit einiger Zeit treten vermehrt Keylogger-Softwareprogramme in Erscheinung, die über Trojaner in Rechner eingeschleust werden. Sie protokollieren die Eingaben an der Computertastatur, und die so gewonnenen Daten werden an den Versender der Software weitergeleitet. Der hat dann z. B. die Möglichkeit, aus den Daten über die Tastaturnutzung Passwörter, Kontonummern etc. zu identifizieren.¹⁹² Damit kann der Softwareschutz umgangen werden.

¹⁸⁹ Vgl. die Seite des Virendestruktors & Unternehmers Kaspersky: <http://www.kaspersky.com/de/>.

¹⁹⁰ Diese Zahl nennt Kaspersky in: <http://www.sueddeutsche.de/computer/artikel/454/65389/>.

¹⁹¹ <http://www.symantec.com/region/de/avcenter/wissenswertes.html>; freigesetzte Viren werden genannt unter <http://www.wildlist.org/>.

¹⁹² [Gttp://www.de.wikipedia.org/wiki/Keylogger](http://www.de.wikipedia.org/wiki/Keylogger); <http://www.heise.de/security/news/meldung/73213>.

- Um Daten (rechtswidrig) abzufangen, Kommunikationsinhalte mitzulesen und Nutzer zu überwachen, gibt es einige Mittel: Sniffer-Programme spähen aus, was in einem Netz oder in Rechnern geschieht, um Informationen und Daten abzufangen. Ursprünglich war diese Software nur ein Instrument der Systemadministratoren, um Abläufe im Netz zu verfolgen. Spyware ist eine Software, die heimlich nach persönlichen Daten sucht, etwa Passwörtern, Kontonummern der Nutzer. Die etwas harmlosere Adware kundschaftet individuelle Gewohnheiten, Präferenzen aus, um sie für Zwecke des Marketing zu nutzen. Eine klare Unterscheidung beider ist oft schwierig, und auch heimlich installierte Adware kann zur Kontrolle über den Rechner führen.¹⁹³
- Durch arglistige, falsche Darstellung (malicious misrepresentation, phishing und identity theft) wollen kriminelle Akteure in den Besitz von Informationen kommen. Das Grundprinzip besteht darin, Nutzern zur Preisgabe von Geheimzahlen und wertvollen Daten zu bewegen. So kann eine fremde Person unberechtigt die Identität eines Nutzers annehmen, im Netz agieren und diverse Geschäfte, Abbuchungen etc. tätigen. Dazu werden unbedarfte Nutzer zum Beispiel auf Seiten gelockt, die denen ihrer Bank täuschend ähnlich sind, oder sie werden durch gefälschte E-Mails zur Preisgabe der Information bewegt. Neuerdings gibt es solche Versuche auch via VoIP. Über ein Band werden automatisch zahlreiche VoIP-Nutzer angerufen und unter einem Vorwand genötigt, Kreditkartennummern etc. preiszugeben. Solche social engineering genannten Strategien, die auf Vertrauen, Neugierde, aber auch Geldgier und viele andere menschliche Süchte setzen, werden häufig angewandt. Sie werfen für kriminelle Täter vielfältigen Nutzen ab und können den Softwareschutz bzw. die Verschlüsselungen zwischen Sender und Empfänger von Datenpaketen unterlaufen.¹⁹⁴

Es gibt also vielfältige Möglichkeiten, die Sicherheit des Internets und die Sicherheit im Internet zu gefährden, und sie können diversen Zwecken dienen: Der Erpressung von Unternehmen [Bednarski, 2004] oder der Störung des Bereichsnamen-Systems, wobei die Motive reichen können von dem einfachen Interesse an der Machbarkeit bis hin zum Testen der Überlebensfähigkeit des Internets, dem dann größere Angriffe folgen könnten; der Störung oder Manipulation von Rechnern kritischer Infrastruk-

¹⁹³ <http://www.de.wikipedia.org/wiki/Spyware>.

¹⁹⁴ <http://www.de.wikipedia.org/wiki/Phishing>.

turen, die über das Internet erreichbar sind; der (Industrie-) Spionage, dem Diebstahl geistigen Eigentums, von Geld und Gut. Neue Bedrohungsräume entstehen, wenn die Software von mobilen Rechnern und anderen programmierten Geräten, etwa in Kraftfahrzeugen, drahtlos und ungeschützt mit und über Computernetze kommunizieren. Viren könnten Programme verändern und die technischen Systeme beeinträchtigen. Auch alle programmierbaren mobilen Systeme, etwa die Smartphones, die eine Kombination von Mobiltelefon und kleinen Computern sind, sind durch Viren gefährdet. Damit entstehen neue Verwundbarkeiten und bislang nicht verfügbare Angriffsoptionen.

Oft gerät bei der Fixierung auf virtuelle Angriffe aber aus dem Blick, dass auch physische Angriffsmittel eine Gefahr für Netzwerke und Rechner sind [Poulsen, 2006]. Sie sind empfindlich gegen direkte physische Einwirkung und immer schon dann gefährdet, wenn ihnen jemand zu nahe kommt, der üble Absichten verfolgt. Deshalb gibt es Ein- und Zugangskontrollen für und innerhalb von Rechenzentren, Serverräumen etc.. Aber auch jenseits dieser Einrichtungen lauern Gefahren durch einfache, überall verfügbare Mittel, mit denen Glasfaserkabel durchtrennt werden können. Tatsächlich geschieht das immer wieder, freilich meist nicht aus Absicht. Die Ursache liegt meist in schlecht vorbereiteten Tiefbauarbeiten, aber auch dem Einsatz von Schleppnetzen, dem Ablassen von Ankern ohne Blick auf die Seekarte – rasch ist ein Tiefseekabel zertrennt. Schon sehr viel schwerer aufzutreiben sind, zumindest in westlichen Staaten, Sprengstoffe, deren Explosion Gebäude mit wichtigen Teilen der Kommunikationsinfrastruktur zerstören können. Da solche Gefährdungen aber nicht auszuschließen sind, werden sie auch in Deutschland im Basisschutzkonzept für kritische Infrastrukturen aufgegriffen. Physischer Schutz spielt deshalb auch beim IT-Grundschutz eine Rolle. Rechenzentren, zentrale Server und Router sind meist in geschützten Räumen oder gar Bunkern untergebracht, die sie vor physischen Einwirkungen schützen, zu denen auch Erdbeben, Feuer, Wassereinbruch zählen.

Werden die Erfahrungen zugrunde gelegt, die es mit den wenigen gezielten und den zahlreicheren unbeabsichtigten Zerstörungen von Internetkabeln gibt, zeigt sich: Ihre Auswirkungen sind fast immer lokal oder regional begrenzt, von kurzer Dauer und halten nur selten mehrere Tage an. Auch ist ein totaler Netzausfall in einer Region selten. Meist wird nur die Qualität der Dienstleistung beeinträchtigt, wodurch die Ladegeschwindigkeit von Seiten geringer wird. Eine gezielte Zerstörung von großen

Rechenzentren, Netzknoten etc. außerhalb von Kriegshandlungen gibt es bislang nicht, und die Zerstörungen von Internet-Infrastrukturkomponenten in New York durch den Terrorangriff vom September 2001 war ein nicht beabsichtigter Nebeneffekt.

Große Gefahren auch für verbunkerte Anlagen des Netzwerkes gehen von Angriffsmitteln aus, die hohe Energieflüsse erzeugen, die ungeschützte elektronische Komponenten und Datenträger zerstören: Electromagnetic Pulse (EMP)- bzw. High Powered Microwave (HPM)-Waffen [Mojert, 2001]. EMP-Energieflüsse sind seit Anfang der dreißiger Jahre des 20. Jahrhunderts bekannt, und durch die atmosphärischen Kernwaffentests wurde ihre potentielle strategische Bedeutung offensichtlich, denn in einem weiten Umkreis fielen Radios, Funkgeräte aus. Eine US-Untersuchungskommission [Foster, 2004] lässt daher keinen Zweifel daran, dass, würde eine Kernwaffe in einer Höhe zur Explosion gebracht, die für einen EMP optimal wäre, es zu einer breiten Zerstörung der elektronischen Systeme in allen zivilen Infrastrukturen käme. (Der Ausfall des Internets wäre freilich eher nachrangig verglichen etwa mit den katastrophalen Auswirkungen einer Auslöschung der Strom-, Telefoninfrastruktur sowie des Ausfalls fast aller Kraftfahrzeuge.) Obwohl der Schutz der militärischen Informations- und Kommunikationsinfrastruktur als besser gilt, wären auch hier gravierende Folgen zu erwarten. Trotz dieses Zerstörungspotentials konnten aber kontrollierbare militärstrategische Optionen für den Einsatz von EMP-Waffen nicht entwickelt werden, soweit sie ihre Energie aus der Zündung von Nuklearwaffen beziehen (NEMP). Die Gefahr, dass es zu einem großen nuklearen Krieg käme, wäre zu hoch, und der Kernwaffeneinsatz ist moralisch, politisch und möglicherweise auch völkerrechtlich [Kötter, 2002] diskriminiert. Die Weiterverbreitung von Kernwaffen und Trägersystemen (weit reichende ballistische Raketen bzw. Marschflugkörper) könnten solche Angriffsszenarien aber wahrscheinlicher werden lassen. Substaatliche Akteure spielen in einem solchen NEMP-Szenario bislang keine Rolle, da sie weder über Kernwaffen noch über die notwendigen Trägersysteme verfügen. Aber die technische Entwicklung geht weiter [Abrams, 2003], und die benötigte Energie kann auf anderen Wegen als durch Atomexplosionen erzeugt werden. Dadurch wird der Einsatz solcher Waffen wahrscheinlicher. Es gibt Berichte, einige Staaten würden ihren Einsatz in Operationsplänen vorsehen, HPM-Waffen seinen

schon durch Streitkräfte der USA eingesetzt worden,¹⁹⁵ und sie könnten auch für Terroristen interessant sein. Da Ergebnisse der intensiven Forschungs- und Entwicklungsarbeiten der Geheimhaltung unterliegen, bleibt es offen, wie gut die Informationen über ihren Entwicklungsstand außerhalb der damit befassten Militärs bzw. der einschlägigen Unternehmen sind. Das Internet ist daher voller Spekulationen¹⁹⁶ über den Einsatz und Nutzen solcher Systeme für diverse Zwecke, potentiell auch für terroristische Aktionen. Jedoch erscheinen diese Waffen als nur begrenzt geeignet für diese Akteure. Zwar können High Power Microwave-Waffen prinzipiell aus Komponenten gebaut werden, die durch es im Markt zu kaufen gibt. Aber dann wären sie relativ groß, hätten ein hohes Gewicht, und um sie einzusetzen, müssten sich Personen dem Ziel nähern. Das erhöht die Möglichkeit ihrer Entdeckung und die Chance, dass Schutzmaßnahmen greifen. Selbst wenn solche Hürden überwunden wären, bliebe die Wirksamkeit der Angriffe lokal begrenzt. Aktionen, sollen sie mehr als nur räumlich beschränkte Wirkungen zeigen, würden so umfangreicher technischer und organisatorischer Vorbereitungen erfordern, dass sie bislang die Möglichkeiten substaatlicher Gruppen überschreiten.

Auch die Diskussion über Schutzmaßnahmen hält an. Denn die Politik muss von der Verwundbarkeit entwickelter Gesellschaften mit ihren überall präsenten Rechnern und Netzwerken sowie davon ausgehen, dass sich wirkungsvolle EMP- und HPM-Waffensysteme in den Arsenalen von immer mehr Staaten befinden. Auch kann sie nicht ausschließen, dass terroristische Gruppen sie in ihren Besitz bringen. Verschärfend kommt hinzu, dass die Entwicklung der zivilen elektronischen Systeme sich nach dem Ende des Ost-West-Konflikts weitgehend ohne die Berücksichtigung solcher Angriffszenarien vollzogen hat. So wurden in den westlichen Staaten fast alle zivilen EMP-Simulatoren abgeschafft, mit denen die Verwundbarkeit elektronischer Systeme getestet wurde. Dass heißt aber nicht, heute sei alles schlecht: Elektronische Komponenten verfügen teilweise über eine, freilich nur sehr begrenzt wirksame Abschirmung gegen elektromagnetische Einwirkungen, um sie für den täglichen Gebrauch zu rüsten. So sind Flugzeuge relativ gut abgeschirmt, da sie sich in einer Umwelt mit starker elektromagnetischer Einwirkung bewegen. Abgeschwächt gilt das für Kraftfahrzeuge, und Teile der zivilen Computer- und Netzinfrastruktur sind in

¹⁹⁵ <http://www.dw-world.de/dw/article/0,,810610,00.html>.

¹⁹⁶ Die google-Suche, Stichwort microwave-weapon, ergab 26000 Treffer in 0,04 Sekunden, die von google scholar 68 in 0,1 Sekunden, darunter zuverlässige Quellen wie <http://www.globalsecurity.org>.

Strukturen untergebracht, die einen begrenzten Schutz bieten gegen EMP und HPM [Fonash, 2005], [Grubescic, Murray, 2005]. Zudem können betriebliche Maßnahmen, die den Blitzschutz verbessern, auch dem Schutz vor elektromagnetischer Einwirkung durch Waffen dienen [Chisholm, 2005]. Die Meinungen gehen aber darüber auseinander, wie praktikabel, teuer und wirksam ein Grundschutz der zivilen Infrastruktur gegen großräumige Angriffe wäre. Protagonisten eines Schutzes [Ijaz, Abrahamson, 2006] übersehen, dass er sehr breit *und* wirksam sein müsste, da schon der Ausfall eines Teils von wichtigen Komponenten zu Störungen führen, die sich weiter ausbreiten und so auch besser geschützte Bereiche beeinträchtigen. Das am schwächsten geschützte Glied der verwobenen Infrastrukturen wäre das Einfallstor der Verwundbarkeit. Daher ist nicht zu erwarten, dass kostspielige, umfassende und in ihrer Wirksamkeit dann doch schwer einzuschätzende Schutzmaßnahmen gegen große EMP bzw. HPM-Angriffe umgesetzt werden.

Auch wenn der kalkulatorische Schaden, insbesondere ausgelöst durch den NEMP, immens sein mag. Ihm steht eine nur geringe Eintrittswahrscheinlichkeit gegenüber, und die plausibleren Angriffsszenarien durch kriminelle Akteure lassen auf begrenzte Auswirkungen hoffen. Dies ist keine gute Voraussetzung für die Bereitschaft, eine hohe Schutzprämie zu zahlen. Eine verbleibende, prinzipiell hohe Verwundbarkeit durch strategische EMP bzw. HPM-Angriffe wird hingenommen, da sie durch die Instrumente der allgemeinen Verteidigungspolitik abgedeckt werden, nämlich der Drohung mit militärischen Präventions- oder Gegenmaßnahmen. Hingegen erscheint, zumindest in den Kernstaaten des Internets, der physische Schutz der zentralen kritischen Komponenten dieser Infrastruktur gegen Angriffe mit explosiven Stoffen etc. relativ gut zu sein.

Gefahrenbereiche für Internetsicherheit

Kriminelle, substaatliche Akteure können die Mittel und Strategien je nach ihren Fähigkeiten nutzen, um die Verfügbarkeit, Integrität, Vertraulichkeit des Internets zu beeinträchtigen, wenn das ihren Zielen dient. Sie verfolgen aber auch Ziele, die sie nur dann erreichen können, wenn das Internet ungestört funktioniert und es seine Stärken ausspielt. Damit teilen diese Akteure das Interesse, das auch andere Nutzer am Internet haben: E-Mails sollen erfolgreich übermittelt, große Datenmengen rasch übertragen, Informationen jederzeit abrufbar oder von einem Server auf den nächsten transportierbar sein, Daten sollen verschlüsselt werden und Suchmaschinen effizient

arbeiten. Diese quasi normale Nutzung des Internets durch kriminelle Akteure kommt in der Regel ohne den Einsatz von Schadsoftware oder Hacken aus. Hacker, Virenschreiber etc. können sogar stören, falls sie das Netz beeinträchtigen. Natürlich ist ein solches Interesse krimineller Akteure an einer funktionierenden Infrastruktur nicht auf das Internet beschränkt. Sie schätzen auch ein gutes Telefon-, Verkehrs-, Transportsystem etc., um Straftaten vorzubereiten, zu begehen und um illegale Inhalte, Propaganda zu verbreiten. Jedoch hat das Netzwerk, wie noch gezeigt wird, Vorzüge, die es besonders interessant machen für kriminelle bzw. terroristische Gruppen.

Cyberkriminalität, terroristische Aktivitäten im Cyberspace und Cyberkrieg

Die Entwicklung der Sicherheitslage im Internet verweist auf zwei Dimensionen der Gefährdung von Cybersecurity, die sich überschneiden und von denen Gefahren für die nationale und die internationale Sicherheit ausgehen können:

- Gefährdungen durch *Cyberkriminalität*, also durch kriminelle Aktivitäten im Cyberspace. Dazu zählen etwa Onlinebetrug, Netzwerksabotage zum Zwecke der Erpressung, Betriebsspionage, Urheberrechtsverstöße, Kinderpornographie, Geldwäsche und andere Varianten des (organisierten transnationalen) Verbrechens. Neben dieser Cyberkriminalität gibt es Taten, die in der realen Welt begangen werden, bei deren Vorbereitung das Netzwerk, wie andere Infrastrukturen auch, aber genutzt wird, um die Erfolgchancen zu erhöhen. Wann diese (punktuelle) Vermischung von Kriminalität und Cyberspace es rechtfertigt, schon von Cyberkriminalität oder noch von gewöhnlicher, realer Kriminalität zu reden, ist ein Problem der Abgrenzung. In Medien und Öffentlichkeit scheint es eine Neigung zu geben, alles als Cyberkriminalität zu definieren, was mit dem Netzwerk in Berührung kommt. Sinnvoll ist das nicht, und niemand würde von Telefonkriminalität reden, nur weil bei der Absprache einer Tat das Sprachnetz genutzt wurde. Rigide Definitionen sind also gefordert, wie das im Bereich der Kriminalstatistik versucht wird, und als Kriterium bietet sich der Ort an, an dem die Tat begangen wurde: Cyberkriminalität findet im und über das Netzwerk statt. Solange eine solche Definition nicht einhellige Zustimmung findet, müssen Behauptungen, die immer lukrativere Cyberkriminalität bringe mit gut 100 Mrd. US-Dollar pro Jahr mehr Geld ein als der weltweite Drogenhandel [Leyden, 2005], mit Vorsicht genossen werden. Trotz dieser Mahnung zur begrifflichen Achtsamkeit zeigen Praxisberichte

und Studien,¹⁹⁷ dass Cyberkriminalität wächst, sie die *Sicherheit im Cyberspace* erheblich gefährdet, und dass sie - so die Ergebnisse der Enquete-Kommission des Bundestages Globalisierung der Weltwirtschaft - mit Strukturen und Prozessen der Globalisierung verwoben ist.¹⁹⁸

- Gefährdungen durch terroristische Aktivitäten. Sie können in zwei Ausprägungen auftreten:

Erstens, als inzwischen klar erkennbare terroristische Nutzung des Internets [Weimann, 2006]. Dieser *Terrorismus im Cyberspace* nutzt das Netzwerk für Propaganda, Informationsbeschaffung und -übermittlung, Netzwerkbildung, Geldbeschaffung, Rekrutierung. Hier ist das Internet vor allem ein Instrument, um die Netzwerke zu stärken, kriminelle Taten in der physischen Welt vorzubereiten bzw. besser ausführen zu können bzw. ein Tatort, wenn beispielsweise Betrug begangen wird, um Geld zu beschaffen oder Daten ausgespäht werden. Daraus erwächst, wie durch Cyberkriminalität, ein Problem für die Sicherheit im Cyberspace. Terroristen im Cyberspace sollen Kontakte haben zu gewöhnlichen Cyberkriminellen, um deren Potentiale zu nutzen, und ihre Taten unterscheiden sich z. T. nicht in Ausführung und Substanz. Daher ist es im Netz zuweilen nicht leicht festzustellen, ob gewöhnliche Kriminelle oder Terroristen am Werk sind.

Zweitens, als - noch hypothetischer - *Cyberterrorismus* im engeren Sinne. Sein Ziel ist es, durch den Einsatz von Schadsoftware, Hacken etc. die ungestörte, sichere Nutzung des Internets zu beeinträchtigen und, via Internet, weitere kritische Infrastrukturen anzugreifen und in ihrer Funktion zu beeinträchtigen. Solcher Terrorismus gegen das Internet bedroht die *Sicherheit des Cyberspace*. Das Internet ist Ziel bzw. das Mittel der Tat, soweit über das Netz andere kritische Infrastrukturen angegriffen werden. Falls der Einsatz physischer Mittel speziell dazu dient, die Funktionsfähigkeit des Internets teilweise oder vollständig zu stören, kann auch das als Cyberterrorismus definiert werden.

¹⁹⁷ Einblick gibt die Arbeit der schweizerischen Koordinationsstelle zur Bekämpfung der Internet-Kriminalität, <http://www.cybercrime.admin.ch/>; vgl. ferner die Aktivitäten des BKA <http://www.bka.de/profil/zentralstellen/zard.html>; vgl. auch <http://www.crime-research.org/>, die Seiten des Cyber Law Consultant and Advocate Boaz Guttman <http://4law.co.il/> sowie [McAfee, 2005].

¹⁹⁸ Vgl. http://bundestag.de/gremien/welt/glob_end/5_2_2_2.html.

- Zu diesen Gefährdungen könnte sich künftig eine weitere gesellen, die erhebliche negative Auswirkungen auf das Netzwerk und seine Nutzung haben könnte - Cyberwarfare, die Netzwerk-Kriegsführung.

Cyberwarfare wäre Teil des traditionellen Konzepts der Informationskriegsführung [Libicki, 1995], [Wilson, 2004],¹⁹⁹ die das Ziel verfolgt, die eigenen Informations- und Kommunikationssysteme zu schützen, die des Gegners lahm zu legen und die Propagandaschlacht zu gewinnen. Auch wenn gelegentlich der Eindruck erweckt wird, ein solcher Cyberwarfare könne auf Netzwerke beschränkt bleiben, wäre er ein Baustein umfassender - wahrscheinlich eskalierender - militärischer Handlungen, mit allen ihren Gefahren [Blancke, 2005], [Siedschlag, 2002].

Ob Cyberwarfare heute nur eine Idee, schon ein Konzept oder gar eine sich entfaltende Option ist, die künftig fest verankert sein wird in den militärischen Arsenalen, bleibt unklar. In Medien werden oft Angriffe mehr oder weniger organisierter Hacker zwischen verfeindeten Staaten als Cyberwar bezeichnet, ebenso wie Angriffe krimineller Spamversender auf Unternehmen, etwa die Sicherheitsfirma Blue Security. Diese Attacken erfüllen aber nicht die Merkmale von Krieg, denn auch in einem Cyberkrieg müssen gemäß einer gängigen Definition von Krieg beide Seiten organisiert sein und mindestens eine muss reguläre Streitkräfte einsetzen.²⁰⁰ Gerade die Wissenslücken über das, was geschieht und was geplant ist, bieten Spekulationen viel Raum. Eine Suche im Internet unter dem Stichwort Cyberwarfare stieß bei google in 0,26 Sekunden auf 560 000 Einträge. Die wissenschaftlich orientierten Suchmaschine sind bescheidener: google.scholar liefert 322 Treffer in 0,10 Sekunden, scirus knapp 1800 Treffer, davon 18 in Journalen.

Vielleicht ist da, wo Rauch ist, auch Feuer: Es gibt immer wieder Meldungen, etwa zwanzig Staaten seinen dabei, die Möglichkeiten des Cyberwarfare auszuloten bzw. solche Kriegsführungskapazitäten aufzubauen, die Streitkräfte der USA besäßen offensive wirkungsvolle Cyberfähigkeiten²⁰¹ und hätten sie bei den militärischen Auseinandersetzungen zwischen Nato und Serbien im Jahre 1999 eingesetzt; und die VR-China gäbe offensiven Operationen gegen Netzwerke im Rahmen der breiten Mo-

¹⁹⁹ Vgl. auch die Seite der Federation of American Scientists <http://www.fas.org/irp/wwwinfo.html>.

²⁰⁰ Vgl. <http://www.sozialwiss.uni-hamburg.de/publish/lpw/Akuf/index.htm>; die Definition sollte so angepasst werden, dass ein Cyberkrieg auch geführt würde, wenn ein Staat die Netzwerkangriffe nicht durch Streitkräfte, sondern durch andere organisierte und ihm unterstellte Gruppen durchführt.

²⁰¹ Vgl. den Vortrag von H.-M. Winkels vom Oktober 2003 über Information Warfare unter http://www1.logistik.fh-dortmund.de/IT-Sicherheit/08a_M&MVortrag.pdf, S. 26.

dernisierung ihrer Streitkräfte sogar Priorität [DoD 2006], [Brookes, 2005] - ein Rüstungswettlauf im Cyberspace sei also schon im Gange. Ob das so ist, bleibt im Dunkeln, da alle Informationen vage sind. Darüber, wie es um die Aussichten steht, einen Wettlauf durch Rüstungskontrolle zu verhüten oder einzudämmen, besteht hingegen Klarheit: Substantiellen Ansätze sind nicht zu erkennen. So ließ eine Tagung der Heinrich-Böll-Stiftung über Rüstungskontrolle im Cyberspace Ratlosigkeit zurück [Heinrich-Böll-Stiftung, 2001]. Weder ist es, wie bei konventionellen und nuklearen Waffensystemen möglich, den Aufbau der Cyberfähigkeiten mit nationalen technischen Mitteln zu überwachen, noch ließe sich ihre Beschränkung in einem Rüstungskontrollregime verifizieren, von dem zivile Netze profitieren würden. Auch eine neue Publikation [Brown, 2006] weist keinen Weg, wie eine denkbare Konvention zum Schutz von Netzwerken umgesetzt und verifiziert werden könnte.

Sicherlich wäre es keine Überraschung, wenn sich nicht nur die USA, sondern auch weitere hochentwickelte Länder auf die Verteidigung des öffentlichen Internets vorbereiten. Denn sie legen besonderen Wert auf seine ungestörte Nutzung, und einige der komplexen militärischen IuK-Netzwerkstrukturen haben Berührungspunkte mit dem Internet. Sie sollen in den hoch entwickelten Staaten im Rahmen einer (visionären) netzwerkzentrischen Kriegsführung bis hin zur operativen Ebene, selbst für einzelne Soldaten, Verwendung finden.²⁰² Diese zentrale Bedeutung rückt die militärischen Netze und latent das öffentliche Internet in den Focus eines Angreifers, aber auch der Verteidigung, die versuchen könnte, den Schutz des Internets als Teil der Sicherung der militärischen Netzwerke zu organisieren.

Wie intensiv das Militär Netzwerke nutzt, lässt sich am Beispiel der USA verdeutlichen: Das Verteidigungsministerium der USA hat die größte administrative Kommunikations- und Informationsinfrastruktur des Landes (vergleichbares dürfte für andere hoch entwickelte Staaten gelten).²⁰³ Sie wird weiter ausgebaut, um die Bandbreitenlücke [Erhard, 2004] zu schließen, die sich bei großen militärischen Operationen wie dem Irakkrieg 2003 auftrat, als die interne militärische Kommunikation geradezu explodierte. Zu dieser Infrastruktur gehören „3.5 million PCs and 100000 local-area-networks at 1500 sites in 65 countries, and it runs thousands of applications on 35,

²⁰² Vgl. Quadrennial Defense Review Report des US-DoD von 2006, <http://defenselink.mil/qdr/report/Report.pdf>.

²⁰³ Für Deutschland, wo das IT-Projekt Herkules umgesetzt werden soll, vgl. die Beiträge in der Zeitschrift <http://www.soldat-und-technik.de>; vgl. ferner die Beiträge in der ÖMZ, Österreichische Militärische Zeitschrift, <http://www.bmlv.gv.at/omz/>.

major voice, video and data networks.” [Tiboni, 2005]. Auch für den militärischen Bereich bietet die Umstellung dieser Infrastruktur auf das IP-Modell große Flexibilitäts- und Kostenvorteile [Gerber, 2005]. Das Militär nutzt auch das zivile, öffentliche Internet und bedient sich für viele Zwecke der relativ preiswerten gängigen zivilen (commercial-off-the-shelf) Soft- und Hardware [Baddeley, 2005]. Diese militärische Nutzung des zivilen Internets gefährdet es latent, weil es zum potentiellen Ziel wird und legt nahe, über seinen Schutz durch speziell dafür aufgestellte Streitkräfte nachzudenken.

Dass der Schutz der militärischen Netze hohe Bedeutung hat, zeigt die Einrichtung der Joint Task Force - Global Network Operations Center des US-Strategic Command (USSTRATCOM)²⁰⁴ im Jahre 2004. Das Zentrum ist zuständig für Betrieb und Sicherung (Verteidigung) dieser Militärnetze, und es ist möglich, dass dabei auch über den Schutz des Internets nachgedacht wird. Wie notwendig es ist, militärische Netzwerke zu schützen, zeigen die zunehmenden Hacker- und andere Angriffe: Im ersten Halbjahr 2005 soll es allein 500 Versuche pro Tag gegeben haben, in das Netzwerk des Verteidigungsministeriums einzudringen, ein deutlicher Anstieg gegenüber dem Vorjahr mit 150 Angriffen pro Tag. Seit einigen Jahren gibt es systematische Versuche, in militärische Netzwerke der USA einzudringen, um (möglicherweise erfolgreich) geheime Informationen zu stehlen. Für sie wurde der Codename Titan Rain vergeben [Graham, 2005], [Thornburgh, 2005]. Wahrscheinlich sitzen die Angreifer in China, und es gibt gute Gründe zu vermuten, dass sie im Auftrag der chinesischen Regierung arbeiten. Beweise dafür fehlen jedoch [Krüger, 2005].

Was auch immer zutreffen mag - auf jeden Fall sind Aufwand und Kosten zur Abwehr solcher Angriffe auch für den militärischen Bereich hoch [Tiboni, 2005]. Aus alledem darf aber nicht auf eine breite Verwundbarkeit der militärischen Systeme durch Cyberangriffe geschlossen werden. Denn es gibt unterschiedliche Grade an Sicherheit, die militärische Netze bieten, also ein Schichtenkonzept der Sicherheit, das von unverschlüsselter Nutzung des Internets bis hin zu physikalisch abgekoppelten Kommunikations- und Führungssystemen reicht.²⁰⁵ Diese strikte Trennung vom Internet hat ihren Grund. Denn solange militärische Netzwerke physisch mit ihm verbunden sind, besteht, zumindest theoretisch, die Möglichkeit, die Militärnetze über das öffent-

²⁰⁴ http://www.stratcom.mil/fact_sheets/fact_jtf_gno.html.

²⁰⁵ Vgl. Defense Information Systems Agency, <http://www.disa.mil/index.html>; auch zivile und behördliche Netzwerke, etwa das Schengener Informationssystem (<http://europa.eu/scadplus/leg/de/lvb/l33183.htm>), sind nicht mit dem Internet verbunden.

liche Internet erfolgreich anzugreifen, wie gut auch immer die Bewachung der Schnittstellen mit dem Internet ist. Die physische Abkopplung hingegen gewährleistet, dass essentielle militärische Fähigkeiten zu Information, Command, Control and Communication nicht über das Internet geschmälert werden können. So ist z. B. das US-Secret IP Router Network nicht mit ihm verbunden. Eine Schichtenstruktur hat auch das im Aufbau befindliche Global Information Grid (GIG) der USA, das zu dem umfassenden, integrierten militärisch-politischen Breitbandssystem werden soll, das alle militärischen Ebenen und sicherheitspolitischen Akteure verbindet und auch Alliierten einen Zugang gewährt [GAO, 2004a].²⁰⁶ Andere Staaten verfolgen vergleichbare Schichtenstrukturmodelle.

Solche und andere Vorsorgemaßnahmen haben dazu geführt, dass bislang Angriffe nur weniger wichtige Netzwerke der Streitkräfte beeinträchtigt haben. „Classified systems“ wie das SIPRNet,²⁰⁷ „have not been compromised.“ [Graham, 2005]. Aber auch in einer Schichtenstruktur können Probleme im Internet nicht vorhergesehene Folgen für militärische Bereiche haben: So trennte das DoD beim Auftreten des Code Red-Wurmes das nicht klassifizierte Nonsecure Internet Protocol Router Network (NIPRN)²⁰⁸ vom öffentlichen Internet. Die Folge war überraschend: „This protective measure disabled the Army Corps of Engineer’s command control of the locks on the Mississippi River, since the NIPRnet was used to transmit commandos through to the locks through the Internet.“ [PITAC, 2005, S. 8]. Offensichtlich war nicht überall bekannt, dass das Internet genutzt wurde.

Informationsüberlegenheit war immer ein Trumpf der Strategie [Denning, 1999]. Deshalb werden in Planungen und Übungen sicherlich die neuen Netzwerke und die Abhängigkeiten des Militärs von ihnen berücksichtigt. Vermutlich werden Möglichkeiten durchgespielt, offensive Operationen in Netzwerken zu führen. Dafür spricht, dass es kaum möglich erscheint, Netze allein mit defensiven Maßnahmen gegen massive Cyberangriffe zu verteidigen, die durch staatliche Stellen geführt werden. Es ist im militärischen Bereich ohnehin fragwürdig, allein auf der technischen Ebene zwischen offensiven und defensiven Systemen zu unterscheiden. Entscheidend ist das Gesamtbild, das Zusammenspiel von politisch-strategischen Zielen, Fähigkeiten und Einsatzkonzepten (Posture), das in der Bilanz eine mehr offensive oder mehr de-

²⁰⁶ Vgl. auch <http://www.answers.com/topic/global-information-grid>.

²⁰⁷ Vgl. zum Secret Internet Protocol Router Network vgl. <http://www.disa.mil/main/prodsol/data.html>.

²⁰⁸ Zum NIPRN vgl. <http://www.disa.mil/main/prodsol/data.html>.

fensive Ausrichtung erzeugt. Selbst bei einer politischen Defensivorientierung verfügen Streitkräfte über technisch offensive Cyberfähigkeiten, und Personal, das Programme zur Abwehr von Viren schreibt, kann auch Virenprogramme entwickeln. Gerade diese technische Vermischung von Offensive und Defensive stellt eine Herausforderung für innovative Köpfe dar, wirksame, verifizierbare Wege für Rüstungskontrolle im Cyberspace zu finden - noch rauchen sie, und die Ergebnisse lassen auf sich warten. Bis dahin könnte die Nutzung des Cyberspace durch Streitkräfte begleitet sein von einem Ringen zwischen Angriff und Verteidigung, das militärisches Denken und Handeln schon immer geprägt hat.

Gemessen an Cyberkriminalität, Cyberterrorismus und insbesondere einem Cyberwarfare findet sich am anderen Ende der Skala der Gefährdungen das, was als Belästigung, Vandalismus oder Sachbeschädigung im Cyberspace bezeichnet werden kann. Dazu zählt etwa die verbreitete Entstellung von Webseiten (defacement) aus allen möglichen, auch politischen Gründen, oder das ungezielte Freisetzen von Schadsoftware, dem viele Anlässe, in der Regel aber keine politischen Motive zugrunde liegen. Solche Ereignisse sind relativ häufig, ihre Wirkung bleibt aber normalerweise gering. Verantwortlich dafür sind fast immer Einzelne oder kleine Grüppchen, die sich beweisen wollen und dafür Programme schreiben, vorhandene nutzen oder sich mit experimentellem Hacken versuchen. Diese Aktionen und ihre Folgen sind allemal lästig, meist strafbar und können in Einzelfällen auch großen Schaden stiften. Dann ist, wie beim Sasser-Wurm, ihre Einordnung als kriminelle Tat eindeutig, was sich auch im Strafmaß ausdrückt: Der junge Wurmschreiber wurde in Deutschland 2005 wegen Computersabotage zu einem Jahr und neun Monaten Jugendstrafe auf Bewährung verurteilt. Solche Aktionen unterscheiden sich von sicherheitspolitisch relevanten Angriffen darin, dass sie überwiegend ohne oder mit nur geringer krimineller Energie und bar aller politisch-strategischer Motive erfolgen. Das schränkt zumindest ihre politische Wirksamkeit ein: Diese Ereignisse sind lästige, strafbare Handlungen mit variierendem Schadenspotential, aber keine Bedrohung der wirtschaftlichen Leistungsfähigkeit von Unternehmen oder gar der wirtschaftlichen, der nationalen Sicherheit, und der größte Teil der Fachwelt, der Politik und Gesellschaft teilt diese Einschätzung.

Verwobene Gefährdungen von Internetsicherheit

Das Internet ist realen, potentiellen und vielleicht auch nur hypothetischen Gefährdungen ausgesetzt. Politik und Gesellschaft, die den Schutz kritischer Informationsinfrastrukturen gewährleisten wollen, können es sich aber nicht leisten, Gefährdungen nur deshalb zu ignorieren, weil sie vage und noch nicht zu greifen sind.²⁰⁹

Konzeptionell, planerisch müssen sie erfasst werden, und Maßnahmen zum Schutz kritischer Infrastrukturen generell und des Internets speziell sollten so gestaltet sein, dass sie zumindest einem *Minimalschutz* auch bei terroristischen Aktivitäten im und gegen den Cyberspace bieten - was auf Seiten der Nutzer in Deutschland dann der Fall ist, wenn der vom BSI geforderte Grundschutz gewährleistet ist.

Zusammenfassend zeigt *Abbildung 1* die Gefährdungen von Internetsicherheit, die von gezielten Handlungen ausgehen, setzt sie untereinander in Beziehung, ordnet ihnen CI(I)P-Bereiche zu und stellt sie in den Kontext der Politikfelder innere und äußere Sicherheit, denen staatliche Instrumente wie Polizei und geheimdienstliche Aufklärung (Intelligence) zugeordnet sind. Das Gesamtbild bietet die konzeptionell Grundlage, auf der die essentiellen Gefahren diskutiert, identifiziert und bewertet werden können, um ihnen gezielt mit (sicherheits-) politischen und technischen Maßnahmen zu begegnen. Die Abbildung soll nicht suggerieren, alle die Gefährdungen beeinträchtigten heute schon mit hoher Intensität die Cybersecurity. Sie soll den schon fassbaren (Cyberkriminalität, Cybervandalismus, terroristische Nutzung des Cyberspace) und sich möglicherweise entfaltenden Gefährdungen (Cyberterrorismus, Cyberwarfare) ihrem Platz zuweisen im Kontext der Politik und der gesellschaftlich-politischen Schutzmaßnahmen.

Die Gefährdungen der Cybersecurity tragen mit dazu bei, äußere und innere Sicherheit weiter zu verzahnen: Zwar fordern terroristische Aktivitäten im Cyberspace in ihren beiden Varianten und Cyberkriminalität zuerst die innere Sicherheit heraus, während Cyberkriegsführung vor allem die äußere Sicherheit berührt. Aber diese Bedrohungsformen könnten verwoben sein, und Terrorismus und Kriminalität haben eine transnationale Dimension gewonnen. Ohne internationale Kooperation kann ihnen nicht wirksam entgegengetreten werden. Cyberwarfare könnte mit Cyberterrorismus verwoben sein. CIIP muß darauf vorbereitet sein, dass sie sich

²⁰⁹ Cyberwarfare wird in *Abbildung 1* aufgeführt, spielt aber in den weiteren Ausführungen keine Rolle, da diese Form der militärischen Auseinandersetzung das öffentliche Internet in nicht kalkulierbarer Weise beeinträchtigen würde. Daher greift auch das Simulationskapitel diese Gefährdung nicht auf.

gleicher Mittel und Strategien bedienen. CIP mit seinem Focus auf dem physischen Schutz richtet sich hingegen in erster Linie gegen gewöhnlichen Terrorismus, der sich physischer Gewalt bedient, aber koordiniert mit Cyberangriffen operieren könnte [Hennessy, Patterson, Lin, 2003], sowie partiell gegen herkömmliche Kriminalität. Auch Cyberwarfare könnte koordiniert sein mit physischen Angriffen durch terroristische Akteure. Deshalb benötigt die IuK-Infrastruktur, darunter Server und Router des Internets, physischen Schutz, der auch Vorsorge gegen Naturkatastrophen bietet. Schnittstellen kann es auch geben zwischen terroristischen Aktivitäten im Netz und Cyberkriminalität, so wie es sie heute schon gibt zwischen terroristischen und kriminellen Gruppen in verschiedenen Regionen des Globus. Transnational organisierte kriminelle und terroristische Gruppen weisen Ähnlichkeiten auf (Netzwerk- und Zellenstruktur, vergleichbare Taktiken etc.), die dazu führen können, dass sie voneinander lernen und kooperieren [Makarenko, 2004], etwa beim Drogenhandel [Wilson, 2006]. Dass Kriminalität inzwischen ausgiebig das Internet nutzt und so seine transnationalen Strukturen stärkt, zeigen McAfee [2005] und Grabosky [2004]. Solche Cyberkriminellen könnten Verbindungen zu terroristischen Netzwerken knüpfen, über die Wissen und Können transportiert werden, um aus Terroristen Cyberterroristen zu machen. Befähigte Cyberkriminelle könnten zudem Terroristen Dienstleistungen für Cyberangriffe, Informationsbeschaffung etc. anbieten. Nicht zum Kernbereich der inneren Sicherheit gehört der verbreitete Vandalismus im Cyberspace, der zwar polizeilicher Eingriffe und rechtlicher Sanktionierung bedarf, aber eher eine Bewältigung durch wirksame Schutzmaßnahmen auf Seiten der Betroffenen nahelegt.

Bilder mit verflochtenen Bedrohungen legen es nahe, Intelligence eine wachsende Rolle auch bei der Beobachtung von (inzwischen schon traditioneller) Cyberkriminalität zuzuweisen. Eine weitere Konsequenz wäre, so ein Beobachter der kriminellen Szene, dass Regierungen untersuchen, „whether the ‚war on terror‘ should be linked more closely to international efforts to prevent cyber-crime, and perhaps also the ‚war on drugs‘“ [Wilson, 2006, S. 88].

Internetsicherheit kann nur erfolgreich sein, wenn alle relevanten Akteure einbezogen werden bei den grundlegenden Maßnahmen zum Schutz des Internets: Die einschlägigen staatlichen Akteure, in Deutschland etwa das BSI, die großen Rechenzentren, die privaten Netzbetreiber und Inhaltsanbieter. Notwendig ist auch die breite Beteiligung aller Nutzer: Der vielen Millionen Privaten in den Haushalten, der Sicher-

heitsverantwortlichen in den Behörden, den Unternehmen bis hin zu den klein- und mittelständigen Betrieben,²¹⁰ die alle ihr Augenmerk auf ein hohes Sicherheitsbewusstsein der Beschäftigten, auf praxistaugliche institutionelle Vorkehrungen und auf eine sichere Software lenken müssen. Hier gibt es noch Nachholbedarf, und ein Anstoß könnten die neuen Kreditrichtlinien nach Basel II für Unternehmen sein: Bei der Bewertung ihrer Bonität und der Kreditkonditionen werden ab 2007 Maßnahmen berücksichtigt, die operationelle betriebliche Risiken minimieren. Zu diesen Maßnahmen gehört die Informationssicherheit, für die es die international anerkannte ISO Norm 17799 gibt, deren Anwendung zudem der Geschäftsleitung haftungsrechtlichen Schutz bietet.²¹¹ Weist die Informationssicherheit Lücken auf, drohen höhere Zinsen und theoretisch auch Haftungsansprüche gegen das Management.²¹²

Zu einer verbesserten Internetsicherheit gehört, dass die den Markt dominierenden Windows-Programme, die - wie Software generell - Mängel aufweisen [Geer, 2003], durch die Installation der Programmkorrekturen rechtzeitig so verbessert werden, dass die erkannten Lücken geschlossen werden. Dass diese Installation ausbleibt, weist auf institutionelle Mängel in Unternehmen, Behörden und auf das mangelhafte Sicherheitsbewusstsein von Beschäftigten und Bürgern hin. So konnten im Jahre 2005 Zotob-Würmer einige Netze von Unternehmen lahm legen, die es versäumt hatten, die schon Wochen vorher verfügbaren Windows-Patches zu installieren. Aber auch die Patch-Software hat nicht selten Mängel, die wiederum Möglichkeiten für Angriffe eröffnet. Ob es fehlerfreie Software geben kann, bleibt umstritten [Klotz, 2005]. Dass fehlerhafte Software kostspielig ist, ist offensichtlich. Nach einer Studie des USA-National Institute of Standards and Technology sollen die Kosten, die durch Softwarefehler entstehen, in den USA zwischen 22 und 60 Mrd. US-Dollar pro Jahr liegen [RTI, 2002] - deutlich mehr als die unteren Kostenschätzungen für Schäden durch Würmer und Viren weltweit (13 Mrd. US-Dollar). Um solche Kosten künftig zu reduzieren, gibt es das Common Vulnerability Scoring System in den USA. Es ist „designed to provide open and universally standard severity ratings of software vulnerabilities“.²¹³ Seine Nutzbarkeit wird von großen Unternehmen

²¹⁰ Sie benötigen oft besondere Unterstützung, vgl. <https://www.sicher-im-netz.de/?sicherheit/ihre/mittelstand/default> ; <http://www.mittelstand-sicher-im-internet.de/>.

²¹¹ Vgl. <http://27000.macassistent.com/> ; der IT-Grundschutz gemäß BSI ist in wesentlichen Aspekten identisch mit den Vorgaben dieser Norm.

²¹² <http://www.manager-magazin.de/unternehmen/mittelstand/0,2828,326413,00.html>.

²¹³ <http://first.org/cvss/>.

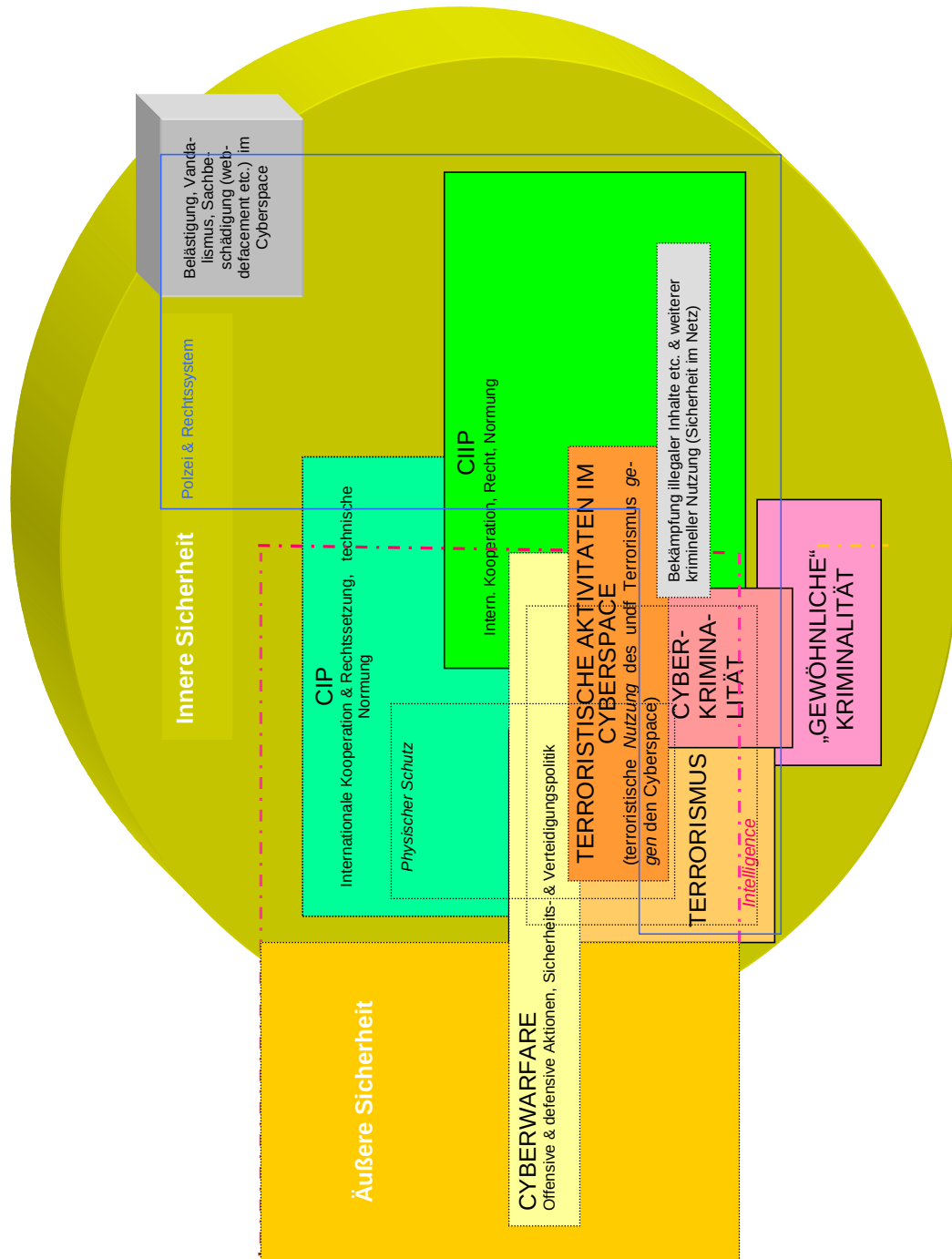


Abbildung 1: Verwobene Gefährdungen im Cyberspace

getestet. Vielleicht könnten auch neue Haftungsregeln dazu beitragen, dass es besser Software gibt. So empfiehlt Schneier [2004] denen, die durch schlechte Software geschädigt wurden, gesetzliche Möglichkeiten zu Klagen gegen die Softwareproduzenten zu geben - was auf massiven Widerspruch mit dem Argument stößt, dies habe negative Auswirkungen auf Softwareinnovationen, da niemand mehr innovative, latent ab er auch anfällige Software entwickeln würde (vgl. [Cashell, 2004]).

Internetsicherheit zwischen technischem und sicherheitspolitischem Konzept

Politik und Gesellschaft stehen vor der Aufgabe zu klären, welche die größten Gefahren für die Internetsicherheit sind und wie mit ihnen umzugehen ist. In Abbildung 1 ist ein buntes Bild der realen und hypothetischen Gefährdungen und ihrer Beziehungen zusammengetragen. Sie können Ausgangspunkt sein für eine solche Analyse, die zu einer sachlich angemessenen und mehrheitsfähigen Einschätzung führt. Diese Forderung ist freilich wohlfeil angesichts der unterschiedlichen Wahrnehmungen der sicherheitspolitischen Lage, die in und zwischen Staaten zu beobachten ist. Insbesondere erschwert das verstärkte Auftreten nichtstaatlicher Akteure die immer komplizierte Einschätzung der Fähigkeiten und Absichten von (potentiellen) Angreifern, die zu einer Gefahrenanalyse gehört [Haimes, Longstaff, 2002].

Nun gibt es nur wenige die bestreiten, dass die Sicherheitslage im Internet schwieriger geworden ist und deshalb die Schutzvorkehrungen besser werden müssen. Jenseits dieser allgemeinen Lagebeschreibung aber beginnt der Raum, in dem Kontroversen über die spezifischen Gefahren ausgetragen werden. So ist strittig, in welchem Maß transnationale kriminelle und vor allem terroristische Akteure dafür Verantwortung tragen: Was könnten sie im Cyberspace anrichten, über welche Fähigkeiten verfügen sie, und beabsichtigen sie überhaupt, terroristische Aktionen gegen den Cyberspace auszuführen, und was werden sie künftig wollen und können? Nicht nur fehlt eine belastbare Faktenbasis, sondern auch die einvernehmliche Einordnung der bruchstückhaften Erkenntnisse in einen sicherheitspolitischen Kontext, in dem die angemessenen Strategien, Mittel und Maßnahmen entwickelt und die Rollen der Beteiligten festgelegt werden: Soll Internetsicherheit im Kontext der Sicherheitspolitik durch staatliche Vorgaben formuliert und umgesetzt werden? Oder sollte Politik, sich zurücknehmend, nur mit den Privaten gemeinsam die Leitlinien entwickeln, um sie dann mit weichen Instrumenten zu Schutzmaßnahmen anregen, deren konkrete Umsetzung diesen privaten Akteuren obliegt? Sind Befürchtungen gerecht-

fertigt, die Offenheit und Freiheit des Netzwerkes werde angesichts einer übertrieben ausgemalten Bedrohung durch Gesetze und die sicherheitspolitische Praxis über Gebühr eingeschränkt? Oder muss die Sorge geteilt werden, dass sich Politik und Gesellschaft konzeptionell und praktisch nur unzulänglich auf terroristische Bedrohungen im und durch das Internet vorbereiten?

Manches daran erinnert an vergangene Diskussionen. Es ist das Merkmal von Demokratien, dass - bei aller grundsätzlichen Übereinstimmung über die Notwendigkeit, Maßnahmen zu treffen - Probleme der inneren und äußeren Sicherheit kontrovers behandelt werden. Unterschiedliche Werte und Ziele treffen aufeinander, und Wissenslücken werden aufgefüllt durch Einschätzungen, die in politisch-gesellschaftlichen Vorstellungen und Konzepten wurzeln, die nicht immer offengelegt werden. So entspannten sich im Westen in den 70er und 80er Jahren Debatten darüber, ob schon die größere Zahl an Waffen (capabilities) der Beleg für eine Bedrohung durch den Warschauer Pakt sei, oder ob dafür auch die Absichten (intentions) bekannt sein müssten, die zum Aufbau dieser Fähigkeiten führen. Sie könnten, so Kritiker des „traditionellen“ militärischen Denkens, defensiv sein. Damals setzten sich in den Nato-Staaten die politischen Kräfte durch, die argumentierten, die Fähigkeiten seien ausschlaggebend für eine Abschätzung der Gefährdung [Steury, 1996]. Denn die Absichten eines Gegners seien kaum zu erkennen und könnten sich rasch ändern.

Mit dem Auftreten transnationaler terroristischer Organisationen verkehrt sich diese Situation. Bei ihnen ist von aggressiven Absichten auszugehen, ohne dass klar ist, wohin, auf welche Infrastrukturen sie ihre Aggressionen richten, über welche Fähigkeiten, über welches Spektrum an Mittel sie verfügen, und wie wirkungsvoll sie von ihnen eingesetzt werden können. Häufig wird von „künftig hohen“, von „wachsenden“ Fähigkeiten terroristischer Gruppen zu Cyberangriffen gesprochen, ohne dass klar wird, was diese Fähigkeiten eigentlich ausmacht und welche Bedeutung sie im Spektrum terroristischer Handlungsoptionen haben könnten, d. h. ob für Terroristen das Internet ein lohnendes Ziel ist.

Um einer Antwort näher zu kommen ist es sinnvoll, sich generell mit den Fähigkeiten zu beschäftigen, über die Angreifer aller Couleur im Cyberspace verfügen können. Cyberterroristen wären eine Subgruppe dieser Akteure, die freilich durch Verbindung mit Staaten und Cyberkriminellen erweiterte Handlungsfähigkeiten erlangen könnten.

Denning [2000] unterscheidet drei Stufen wachsender Fähigkeiten von Angreifern. Diese Differenzierung bietet einen qualitativen Ansatz, um im Rahmen einer Gefahrenanalyse sich einem Konsens darüber zu nähern, was Cyberterrorismus heute und zukünftig können könnte, und welche Voraussetzungen dafür gegeben sein müssen. Die Fähigkeiten von Angreifern können sein

- “simple-unstructured (basic hacks against individual systems using tools created by someone else; if there is an organization it possesses little target analysis, command and control, learning capability);
- advanced-structured (capability to conduct more sophisticated attacks against multiple systems or networks and, possibly, to modify or create basic hacking tools; organization conducts elementary target analysis, command & control and learning capability);
- complex-coordinated (capability for coordinated attacks against integrated, heterogeneous defenses; ability to create sophisticated hacking tools; highly capable target analysis, command and control, organization learning capability).” Dazu gehören auch Fähigkeiten, digitale Spuren zu verwischen (covering tracks).

Zweifellos stellt die erste Stufe für terroristische Akteure per se kein Problem dar. Schon die z. T. ausgeprägte und ausgefeilte Internetnutzung durch terroristische Gruppen ist dafür ein deutlicher Hinweis. Über welche Potentiale sie verfügen und ob sie heute das Netzwerk mit zumindest punktuelltem Erfolg angreifen könnten, ist aber nicht eindeutig einzuschätzen. Es gibt zu wenige belastbare Informationen über das Wissen und Können solcher Gruppen, und Angriffe durch Cyberterroristen, die Einblicke in Fähigkeiten gestatten, sind nicht bekannt. Daher bleibt unklar, ob sie sich schon hin zur zweiten Stufe mit „advanced-structured capabilities“ bewegen. Jedoch würden, trotz verstellter Einblicke, nur ausgemachte sicherheitspolitische Pessimisten terroristischen Gruppen heute die Potentiale zusprechen, die die dritte Stufe kennzeichnen.

Aber das ist die Aufnahme eines Moments, und die Fähigkeiten terroristischer Gruppen werden künftig weiter wachsen. Drei Entwicklungen tragen dazu bei:

- Die Rekrutierung unter technisch Gebildeten, deren Berufs- und Lebensperspektiven sich nicht aufhellen, wird weitergehen. Das gilt insbesondere für Menschen aus einigen Staaten Arabiens, Afrikas und Südamerikas, aber auch für Gruppen von Immigranten und ihre Nachkommen in westlichen Staaten.

- Der Anteil der Menschen an der Gesamtbevölkerung, die technisches Wissen haben, wird durch bessere Bildungssysteme in vielen Staaten zunehmen, und die Verlagerung von Softwareentwicklung in Länder mit geringeren Lohnkosten wird dort das Expertenwissen mehren. In solchen Ländern dürften zugleich die Rekrutierungschancen hoch sein.
- Mit dem absoluten Wachstum der Weltbevölkerung wird die Zahl der Menschen steigen, die fähig sind, komplexe technische Probleme zu meistern. Selbst unter der Annahme, nur ein konstanter Anteil von ihnen ließe sich rekrutieren, stünden Terroristen wesentlich mehr fähige Unterstützer und Helfer zur Seite.

Insgesamt wird in den nächsten Dekaden den terroristischen Organisationen eine wachsende Anzahl gut ausgebildeter, perspektivloser, zorniger und hasserfüllter (vorwiegend) junger Männer zur Verfügung stehen, die eine deutlich erhöhte Cyberkompetenz in diese Organisationen tragen werden. (Möglich erscheint es, dass gut ausgebildete Frauen künftig eher bereit sein könnten, sich an einem Cyberterrorismus zu beteiligen, da diese nichtphysische Form des Angriffs eher mit einem auch traditionellen weiblichen Rollenbild vereinbar wäre.) Ob mit dem Grad der Organisation, wie bei Denning unterstellt, auch die Fähigkeiten von Angreifern wachsen, ist empirisch schwer zu belegen, erscheint aber plausibel. Zwar kann ein Einzelner mit Schadsoftware, wie Sasser und andere Würmer zeigen, ein erhebliches Angriffspotential entfalten, gemessen am verursachten Schaden. Ist das Ziel eines Angriffs aber umfassender, auf materielle bzw. politisch-psychologische strategische Wirkungen ausgerichtet, erfordert er mehr: Aufklärung über Stärken und Schwächen des Ziels, exakte Planung und Tarnung des Angriffs, zielgerichtete Mittel und Kontrolle ihres Einsatzes, um bei Bedarf erneut anzugreifen. Sollen Angriffe überhaupt denkbar sein, die das Funktionieren des Internets großräumig (zumindest in großen Teilen eines Kontinents) und längerfristig (einige Tage und mehr) beeinträchtigen bzw. die via Internet andere kritische Infrastrukturen stören, erscheinen strategische Fähigkeiten notwendige Voraussetzungen. Sie können - wenn überhaupt - nur differenzierte Organisationen bereithalten könnten. Offen bleibt, welche Größe, welchen Organisationsgrad, welche technischen Kompetenzen und Mittel eine Organisation haben müsste, und was davon überhaupt für Cyberterroristen (oder andere kriminelle Akteure) erreichbar ist, ohne auf Unterstützung durch staatliche Ressourcen oder durch kompetente kriminelle Hackerorganisationen zurückgreifen zu müssen, die sich als Dienstleister für diverse Zwecke herausbilden könnten.

Gibt es keine Klarheit, können Vermutungen, Extrapolationen und Analogien zu divergierenden Perzeptionen der Sicherheitsperspektiven führen, in die zudem politische, wirtschaftliche, institutionelle Interessen und Ziele einfließen. Das Resultat sind unterschiedliche Vorstellungen über die Bedrohungslage im Cyberspace, die es schwer machen, zu gemeinsamen Konzepten darüber zu kommen, welche Aufgaben Internetsicherheit zu lösen hat und ob bzw. in welchem Grade sie ein Aufgabenfeld (inter)nationaler Sicherheitspolitik und ihrer Instrumente werden muss (vgl. [Abele-Wigert, 2006], [Dunn, Mauer, 2006], [Dunn, 2005], [Lewis, 2005]).

Mit Hilfe von vier Bildern soll vor dem Hintergrund von Abbildung 1 gezeigt werden, wie solche Vorstellungen über die Bedrohungslage idealtypisch aussehen können, vor welchen Aufgaben die Internetsicherheit im Kontext des jeweiligen Bildes steht, und welche Rolle dabei Staat und Politik spielen. Zwei Randbedingungen werden verändert, und diese Veränderungen bringen Modifikationen des Ergebnisses: Der angenommene Grad der Abhängigkeit von Gesellschaft und Staat vom Internet sowie die Fähigkeiten, die Angreifern zugesprochen werden. Es gibt weitere Randbedingungen, die hier als gegeben unterstellt werden: Aggressive Absichten der Angreifer und eine Verwundbarkeit der Infrastruktur, die aber durch Politiken und Maßnahmen verringert werden kann, was bei einer abschließenden Bewertung zu berücksichtigen ist.²¹⁴ Die Bilder stellen Internetsicherheit dar als Problem der technischen, sektoralen, der wirtschaftlich-gesellschaftlichen und (inter-) nationalen Sicherheit, wobei von Bild zu Bild das Bedrohungsniveau steigt:

Internetsicherheit als ein Problem der technischen Sicherheit für Nutzer.

Sicherheitsprobleme können durch technische Experten und mit technischen Mitteln (firewalls, anti-virus software, intrusion detection etc.) gelöst werden, da Cyberkriminalität wenig ausgeprägt ist, Störungen überwiegend in kurzzeitig, nur lokal spürbaren Unfällen, technischem Versagen ihre Ursache haben oder durch Personen mit geringen Fähigkeiten ausgelöst werden, deren Handlungen weder koordiniert noch politisch motiviert sind. Internetsicherheit ist hauptsächlich eine Aufgabe, die Unternehmen, Behörden, gesellschaftliche Einrichtungen und Private für sich selbst und vor Ort lösen. Beeinträchtigungen des Netzwerkes bringen zwar Kosten mit sich, bleiben aber ohne große Folgen und eher ein Ärgernis, da die Bedrohungslage nicht hoch und die Netzinfrastruktur selbst kein Ziel ist. Insofern

²¹⁴ So sollen, wie etwa im deutschen NPSI vorgesehen, international vernetzte Krisenzentren die Prävention, Krisenreaktion und die strukturellen Sicherheit der IuK-Systeme gewährleisten.

spielt auch der Grad der Abhängigkeit von Internet, den Gesellschaft und Staat aufweisen, eine geringe Rolle: Wie hoch er auch wäre, die Bedrohung ist objektiv gering. Daher ist Internetsicherheit als technisches Konzept auf die Verhütung und Beseitigung von kurzfristigen Gefährdungen bzw. Störungen betrieblicher Abläufe im Rahmen eines lokalen Sicherheitsverständnisses ausgelegt. Zwischenstaatliche Kooperation spielt nur eine begleitende Rolle, und die Aufgaben staatlicher Stellen bleiben, über die eigenen Vorsorge hinaus, darauf beschränkt, Informationen etwa über zuverlässige Technik zur Verfügung zu stellen, die eine effizientere und effektive Umsetzung der örtlichen, privaten Maßnahmen erleichtern.

Ein solches Verständnis von Internetsicherheit ist angesichts der Sicherheitslage im Netz kaum noch anzutreffen.

Internetsicherheit zur Gewährleistung einer funktionierenden sektoralen Infrastruktur.

In diesem Bild sind immer mehr Unternehmen intern, miteinander und mit Kunden vernetzt, der öffentliche Sektor, Behörden und Einrichtungen sowie gesellschaftliche Organisationen setzen zunehmend das Internet für interne und externe Prozesse ein. Damit stehen diese Sektoren bzw. die Betreiber des Internets aus eigenem Interesse in der Verantwortung, durch verstärkte und untereinander abgestimmte Vorkehrungen die Kontinuität und Sicherheit von Kernbereichen ihrer Arbeit zu gewährleisten. Die Bedrohungslage hat sich verschärft: Schadsoftware, aber auch Hacken und andere strafbare Handlungen führen zu ernsthafteren Problemen durch die Vernichtung, den Diebstahl sensibler Daten etc., es gibt Angriffe etwa mit botnets, die auf das Lahmlegen von Unternehmensnetzen, -diensten abzielen. Verglichen mit dem ersten Gefährdungsbild sind Angreifer professioneller, zielgerichteter und können auch von begrenzten politischen bzw. von kriminellen Motiven geleitet sein. Ihre Angriffe können länger andauern und sich wiederholen. Unternehmen, Behörden etc. müssen ihre Sicherheitsvorkehrungen intensivieren und die lokale Perspektive zugunsten eines breiteren Sicherheitsansatzes überwinden. Internetsicherheit ist auf die Verhütung, Abwehr und Beseitigung von Störungen und Beeinträchtigungen ausgerichtet, die wichtige Unternehmen, Wirtschaftssektoren bzw. staatliche Funktionsbereiche belasten. Der Staat hält sich mit direkten Eingriffen und rechtlichen Vorgaben weitgehend zurück, aber staatlichen Einrichtungen, die sich mit Netzsicherheit befassen, und spezialisierten Strafverfolgungsbehörden kommt eine anleitende Funktion bei der Zusammenarbeit mit Privaten zu. Kennzeichen der Politik ist die Partnerschaft von Staat und großen Netznutzern bzw. -betreibern, und die kooperativ entwi-

ckelten Maßnahmen und Programme regen vorrangig die Eigeninitiative der Privaten an. Der Staat bemüht sich international um eine wirksame, rechtlich und administrativ abgesicherte Kooperation zum Schutz des Cyberspace.

Dieser Ansatz, in dem zwischen den privaten Akteuren und der Politik ausgehandelte Schutzstrategien und -konzepte dominieren, wird heute in vielen Staaten praktiziert.

Internetsicherheit für wirtschaftliche Sicherheit und gesellschaftliche Stabilität.

Die Bemühungen der Politik sind auf die Abwehr von Bedrohungen und Gefahren für die kritische Infrastruktur gerichtet. Sie gehen von organisierten kriminellen und terroristischen Akteuren mit weiter wachsenden Fähigkeiten aus, die das Internet immer stärker für ihre Zwecke nutzen, legale Nutzungen durch ihre Aktionen deutlich weniger attraktiv machen, die Funktionsfähigkeit des Netzwerkes großräumig und längerfristig bedrohen und via Internet andere kritische Infrastrukturen in ihrer Funktion zu beeinträchtigen versuchen. Dabei können sich wiederholende Angriffe Tage bis Wochen dauern, damit sie wirksamer werden, und es besteht die Möglichkeit, dass sie mit konventionellen Anschlägen koordiniert werden. Da die Bedeutung des Internets für die wirtschaftliche, politische und gesellschaftliche Leistungs- und Handlungsfähigkeit eines Landes sehr hoch ist, kommt dem Staat und seinen Organen, einschließlich der Geheimdienste, die führende, aktive Rolle bei der Verhütung und Abwehr solcher Aktionen zu. Internetsicherheit ist als gesamtgesellschaftliche, politische Aufgabe im Rahmen der inneren Sicherheit darauf ausgerichtet, Störungen kritischer Infrastrukturen, ganzer Wirtschaftssektoren, öffentlicher Einrichtungen zu verhüten und zu beseitigen, um wirtschaftliche Sicherheit und gesellschaftliche Stabilität zu gewährleisten. Da die Bedrohung virulent und die ökonomischen, politischen und gesellschaftlichen Kosten eines längeren Netzausfalls sehr hoch wären, müssen alle wichtigen Beteiligten für sich und für das Netz insgesamt verbindliche Konzepte entwickeln und umsetzen, die ein rasches Wiederanfahren des Internets ermöglichen (recovery). Angesichts der Gefährdungslage und der Abhängigkeit vom Netz tritt Public Private Partnership, die aber weiterhin eine punktuelle Rolle spielt, zurück vor regulativen Eingriffen des Staates, der über die nationalen Maßnahmen hinaus sehr intensiv nach internationalen Schutzkonzepten und -strategien sucht. Überwachung und Kontrolle des Netzwerkes durch staatliche Stellen werden essentiell.

Dieses Bild malt nicht die heutige Politik für Cybersecurity ab, die von einer solchen Stringenz weit entfernt ist. Es enthält aber Farbtöne, die sich in der heutigen Diskussion wiederfinden, etwa die Forderungen nach einer stärkeren Netzwerküberwa-

chung und die Hinweise auf einen starken Anstieg der Bedrohung. Aus solchen Diskussionen könne in den nächsten Jahren das folgende Verständnis von Internetsicherheit erwachsen, das heute die Debatte beileibe nicht prägt, sie aber zumindest rhetorisch punktuell zu beeinflussen beginnt.

Internetsicherheit als prioritäre Aufgabe der (inter)nationalen Sicherheit.

Politisch organisierte und durch staatliche Stellen umgesetzte bzw. kontrollierte Internetsicherheit hat Vorrang, da Staat und Gesellschaft sowie ihre kritischen Infrastrukturen in allen wesentlichen Funktionen vom Internet abhängen, das strategisch bedroht wird durch politisch motivierten Terrorismus, der „complex-coordinated capabilities“ hat. Damit besteht die reale Gefahr, dass Cyberterrorismus das Netzwerk sehr großräumig und für einen längeren Zeitraum (Wochen) lahm legen könnte und auch andere kritische Infrastrukturen mit in Leidenschaft zieht (Szenario des digitalen Pearl Harbor). Eine Kooperation mit gegnerischen staatlichen Stellen ist dabei nicht auszuschließen. Diese Gefährdung erfordert, über den wirkungsvollen Schutz des Cyberspace durch Überwachung, Schutzsoftware etc. hinaus, den Einsatz aller geeigneten sicherheitspolitischen Institutionen und Mittel, um solche Angriffe zu verhüten oder ihre Ausführung zu stoppen und beeinträchtigte Infrastrukturen rasch wieder anzufahren. Der die ersten beiden Bilder charakterisierende Verzicht des Staates auf Eingriffe bzw. seine Beschränkung zugunsten eines privaten Schutzkonzeptes wird abgelöst durch ein neues staatlich-politisches Sicherheitsregime, dem sich Gesellschaft und Wirtschaft auch bei hohen Kosten unterordnen müssen. Selbst Private an ihren Rechnern müssen sich Vorschriften hinsichtlich der Aktualisierung ihrer Schutzsoftware unterwerfen, die auf jedem verkauften Rechner installiert und nicht umgangen werden kann. Mit seinen eigenen und den von ihm angeordneten Maßnahmen würde der Staat den Schutz der „fünften Dimension“,²¹⁵ des Cyberspace [Matai, 2005], organisieren und durchsetzen. Dafür schließen sich die Staaten zusammen, die gemeinsam eine „wohlwollende Hegemonie“ über das Internet auszuüben versuchen, um seine Nutzbarkeit in Zeiten permanenter, akuter Bedrohung zu gewährleisten. Denkbar wäre, dass diese Cyber-Sicherheitsstaaten zu diesem Zweck auch explizit offensive Fähigkeiten für Operationen im Cyberspace aufbauen, um das Netzwerk frühzeitig und entschieden vor Angriffen zu sichern. Dazu könnten spezifischen Einheiten inner- oder außerhalb der Streitkräfte eingerichtet werden. Nachge-

²¹⁵ Die anderen Dimensionen sind, neben dem Territorium, die auch vom DoD [2005] genannten: See, Luftraum, Weltraum.

dacht wird auch über den Aufbau sicherer, überwachter und (partiell) vom öffentlichen, eher unsicheren Internet abgeschlossener IP-Netze oder über prioritäre Paketdienste. Dadurch soll gewährleistet werden, dass die Datenpakete, mit denen die kritischen Infrastrukturen ihre essentiellen Funktionen aufrecht erhalten, mit hoher Sicherheit das Netzwerk unbeeinträchtigt durchqueren können.

Diese idealtypische konzeptionelle Differenzierung von Internetsicherheit darf nicht zu der Annahme verleiten, Maßnahmen für Cybersecurity im Kontext des jeweils folgenden Bildes könnten auf alles das verzichten, was z. B. das lokal-technische Verständnis von Internetsicherheit erfordert. Angemessen ist ein Verständnis, in dem das nächste Bild über das vorhergehende gelegt wird, so dass die erreichte Stufe der Internetsicherheit auf der Wirksamkeit der vorhergehenden aufbaut, sie integriert bzw. Elemente neu definiert und ihnen einen Platz zuweist in dem veränderten Kontext. So ist die Vorbereitung auf das Wiederanfahren eines gestörten Internets immer essentiell, wobei die Schwierigkeiten leicht unterschätzt werden, gerade beim Internet [Powner, Rhodes, 2006]. Denn "(t)here are no clear accountabilities or guarantees for the continuity of operation of the Internet." [Leggate, 2005, S. 7]. Die Lösung dieses Problems würde dann freilich dringender und zugleich schwieriger, wäre das Netzwerk durch strategische Angriffe betroffen.

Die vier Bilder können dazu beitragen, die Bedeutung von Ereignissen, von Aktionen und Angriffen im Cyberspace besser einzuschätzen. Dadurch können auch ungerechtfertigte Aufregung vermieden werden, die immer wieder in Medien zu finden sind. So ist etwa der Ausfall von Servern durch denial-of-service-Angriffe, die Entstellung von Webseiten, das Hacken von Rechnern in einem Unternehmen oder in einer Behörde, die Beeinträchtigung oder der Ausfall des Internets in einer Region oder bei einem oder mehreren Unternehmen per se kein ernsthaftes volkswirtschaftliches (wirtschaftliche Sicherheit) und schon gar nicht ein gesamtstaatlich-sicherheitspolitisches Problem (nationale Sicherheit). Deshalb ist in Abbildung 1 der häufig anzutreffende Vandalismus im Cyberspace nur einem abgelegenen Randbereich der Gefährdung von Internetsicherheit zugeordnet und spielt für die innere Sicherheit keine Rolle. Er muss vorrangig durch technische, institutionelle Lösungen bei den Nutzern selbst und durch gängige straf- bzw. haftungsrechtliche Instrumente bewältigt werden.

Auch zeigen diese Bilder, dass die Struktur und Intensität der heute praktizierten Politik für Cybersecurity bislang hinter dem zurückbleiben, was zu erwarten wäre ange-

sichts der oft anzutreffenden Ausmalung von Bedrohungen im und für das Netzwerk und der oft zitierten Abhängigkeit der Gesellschaft vom Internet. Zweifellos hat das Konzept der Internetsicherheit in den Staaten mit intensiver Netznutzung schon die erste technische Stufe überwunden, und sie wird eingefügt in die zweite, sektorale Stufe. Und Stimmen werden lauter, die dritte oder, heute selten zu vernehmen, die vierte Stufe zu betreten. Bislang aber sind sie nicht laut genug, und, wie bei der CIP generell, prägt heute das zivile Leitbild der Public-Private-Partnership die Bemühungen um Cybersecurity. Es ist charakterisiert durch den Vorrang des Privatsektors, eine deutliche Zurückhaltung staatlicher Stellen, den weitgehenden Verzicht auf staatliche Regulierung („hands-off-approach“) sowie die Vorbildfunktion des Staates beim Schutz der eigenen Infrastruktur (was jedoch nicht immer gelingt, wie sich in den USA zeigt [Pulliam, 2005]).

Dieser Ansatz einer Privatisierung der Internetsicherheit ist in den USA sehr früh festgelegt worden,²¹⁶ und er wurde im Kern auch von den meisten anderen OECD-Staaten übernommen. Erfolge hängen dabei von der Mitarbeit der Infrastrukturbetreiber, der Internetdienstleister und großer Unternehmen ab, die bereit sein müssen, Vorsorge und Krisenmanagement zu betreiben. Der Staat steht dabei mit Rat und Tat zur Seite, indem er den Aufbau von Institutionen für Cybersecurity fördert. Dabei spielen die zahlreichen nationalen CERTs eine wichtige Rolle, die sich weltweit im Forum of Incident Response and Security Teams (FIRST) zusammengeschlossen haben²¹⁷ und Konferenzen, Seminare und Training veranstalten. Zur Zeit sind dort CERTs aus 35 Ländern vertreten, als einziger Kontinent fehlt Afrika, dessen Internetnutzung außerhalb Südafrikas und jenseits großer Städte noch marginal ist.²¹⁸

Diese Zurückhaltung und Gelassenheit von Staat und Politik, darauf machen Autoren [Dunn, Mauer 2006], [Lewis, 2005], [Grubestic, Murray, 2005] aufmerksam, erstaunt: Das Internet wird als zentraler Baustein einer Wissensgesellschaft, als Machtressource gehandelt, die wachsenden Bedrohungen werden betont, denen das Internet ausgesetzt ist, und andere Bereiche, die für nationale Sicherheit und Heimatschutz wichtig sind, werden zunehmend reguliert - aber die Internetsicherheit bleibt weitgehend eine privat organisierte Aufgabe. Ohne Kritik bleibt das nicht. Es wird die Klage laut, die Privaten ließen eine Sicherheitslücke, denn das Gut Sicherheit entstehe im

²¹⁶ Vgl. die Presidential Decision Directive (PDD) 63 Critical Infrastructure Protection von 1998 der Administration Clinton; Text unter <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>.

²¹⁷ [first.org](http://www.first.org).

²¹⁸ Vgl. die Quellen unter <http://www-sul.stanford.edu/africa/elecnet.html>.

Cyberspace nicht wie von selbst aus privatem Handeln, und der private Ansatz zeitige bei der Cybersecurity (und der CIP generell) nicht immer die erhofften Resultate: „While in theory, individuals and companies in a liberalized economy have strong incentives to provide effective emergency preparedness and crisis management, in reality, private motivation is unlikely to be sufficient to provide an optimal amount of emergency preparedness for society as a whole.“ ([Andersson, Malm, 2006, S. 142], ähnlich [Dunn, Mauer, 2006]). Die Ursachen für dieses Marktversagen können vielfältig sein: Unternehmen berücksichtigen nur die Kosten von Störungen, die bei ihnen selbst anfallen, gesellschaftliche Kosten geraten nicht in den Blick; nationale Sicherheit ist ein Kollektivgut, das bereitzustellen keine Aufgabe der Unternehmen ist, und sie haben weder die Informationen noch den Auftrag abzuschätzen, welches Schutzniveau gesellschaftlich notwendig ist; Unternehmen könnten darauf bauen, dass sie bei großen Krisen und Störungen auf staatliche Hilfe rechnen dürfen - dann unterfinanziert der Markt die Sicherheitsvorkehrungen. So gerät auch das Kernstück der Internetsicherheit in die Kritik: Public Private Partnership „may be an unreliable and unpredictable way of closing the gap in national emergency preparedness and crisis management in deregulated sectors of the economy. ... It is relatively easy for government and private actors in a PPP to agree on the existence of a problem or on the need to resolve it. It is, however, much harder to agree on what should be done about it, who should be responsible for implementing the solution, who should assume legal responsibility for potential damages, and who should bear the costs of implementing countermeasures.“ [Andersson, Malm, 2006, S. 151].

Wenn das so ist, das Internet eine essentielle Bedeutung hat und die Sicherheitslage deutlich schlechter wird, wäre zu erwarten, dass sich Politik entschließt, auf der Grundlage eines neuen Bildes der Gefährdungslage diese Sicherheitslücke zu schließen und zu versuchen, die Gefährdung der Netzsicherheit zu minimieren. Wie in anderen sicherheitsrelevanten Bereichen auch, würde auch direkt regulierend eingegriffen durch Gesetze, Verordnungen oder zumindest mittelbar gesteuert durch starke ökonomische Anreize (Subventionen, Steuern, Haftung). Stattdessen, so Kritiker, beläßt es die Politik weitgehend bei einem Konzept, dessen Wirksamkeit angesichts der diskutierten Gefährdungslage schon heute als fragwürdig erscheint. Und auch der Verweis auf den (wahrscheinlichen) Aufbau militärischer Cyberwarfare-Fähigkeiten in westlichen Staaten helfe da nicht, denn der ziele schon aus politischen Gründen nicht darauf ab, über ein Instrument zur Kontrolle des zivilen

Cyberspace zu verfügen, sondern er diene primär dem Schutz der militärischen Netzwerke.

Konstatiert wird also ein Zwiespalt einerseits zwischen der deklarierten oder zumindest der absehbaren Bedrohungslage, der behaupteten zentralen gesellschaftlichen Funktion des Netzwerkes, und andererseits der Konzeption und Praxis der Internet-sicherheit, die durch ein Zurücktreten des Staates gekennzeichnet ist. Für ihn gibt es mehrere Erklärungen, von denen aber keine für sich alleine überzeugt:

- Die Gefährdung wird übertrieben dargestellt, und die Politik ist sich dessen bewusst. Insoweit entspricht die heutige Konzeption und Praxis der Cybersecurity der tatsächlichen Lage.

Unklar wäre hier, wie die Lücke zwischen deklarerter Gefahr und bescheidenem Handeln politisch legitimiert wird, und welche Erkenntnisse dieser objektiven, beruhigenden Gefahreinschätzung zugrunde liegen.

- Politik und Gesellschaft ignorieren die Gefährdung oder schätzen sie falsch ein. Fehleinschätzungen und Ignoranz gibt es immer wieder. Da aber die Sicherheitslage allgemein als Folge des transnationalen Terrorismus als bedrohlich angesehen wird, wäre zu klären, warum ausgerechnet bei der Cybersecurity das nicht zur Kenntnis genommen würde.

- Die Gefährdung wird als hoch erkannt, aber ein substantieller Rest an Gefährdung wird von der Politik akzeptiert. Denn neue Konzepte und Maßnahmen, sie zu minimieren, wären betriebs- und volkswirtschaftlich zu kostspielig.

Auch das würde einen Konsens über das Ausmaß der Gefahren und damit über die Kosten erfordern, die nötig wären, um diese Gefahren weiter zu reduzieren.

- Unternehmen, die das Netz und im Netz dominieren, wollen staatliche Intervention verhindern, die ihnen hohe Kosten auferlegen würde. Dazu sind sie in der Lage, wie immer die Einschätzung der Gefährdungssituation auch sein mag.

Dieses einflusstheoretische Argument müsste begründen, warum der Staat im Falle der Cybersecurity, nicht aber in anderen Sektoren davor zurückscheut, Vorgaben zu machen, worin also der spezifische Einfluss der Internetwirtschaft bestünde.

- Staat und Politik glauben, über genügend Fähigkeiten und Mittel verfügen, um frühzeitig Cyberangriffe zu erkennen und zu unterbinden. Daher sind wirklich gefährliche Angriffe nicht zu erwarten, und die, mit denen zu rechnen ist, können mit einem privaten Sicherheitskonzept bewältigt werden.

Dies wäre ein zweifellos selbstbewusstes, aber auch ein riskantes Denken, auf das es keine substantiellen Hinweise gibt.

- Das Internet ist und wird auch künftig nicht so wichtig für die Funktionsfähigkeit von Gesellschaft und Staat sein, wie das oft dargestellt wird. Folglich wären die Auswirkungen auch erfolgreicher Cyberangriffe sehr begrenzt.

Das wäre eine problematische Einschätzung. Denn die Schwierigkeiten, den Grad der Abhängigkeit vom Netzwerk präzise zu bestimmen und insbesondere den künftigen vorherzusagen, sind Legion. Neue Technologien und Geschäftsmodelle kommen in die Märkte, und diese un gelenkten gesellschaftlich-technologischen Vernetzungsprozesse verändern das Internet und seine Nutzung.

- Angesichts des fast ausschließlich privat betriebenen Internets und des Eigeninteresses der Privaten an einer Lösung der Probleme ist das heutige Konzept hinlänglich und angemessen. Denn die technologische Dynamik des Internets so hoch, dass staatliche Regulierung immer nachhinken würde.

Dem stehen die Hinweise auf ein Marktversagen entgegen, und per se ist das Nachhinken für Politik kein Grund, auf Regulierung zu verzichten.

- Die Leitbilder und Instrumente traditioneller staatlicher Sicherheitspolitik sind nicht kompatibel mit den Herausforderungen der Cybersecurity, so Dunn und Mauer [2006]. Denn diese Leitbilder sind Abschreckung und Abwehr von Angriffen, die im Kontext von Cybersecurity anderes definiert werden müssen: Abschreckung gegen Cyberangriffe durch die Androhung von Vergeltung ist bestenfalls im Kontext von zwischenstaatlichem Cyberwarfare vorstellbar, nicht aber gegen die alltäglichen Angriffe im Netz und auch nicht gegen Cyberterrorismus. Erfolgversprechend ist hier nur die Kooperation der Staaten auf der Basis eines breiten Grundschutzes. Diese Zusammenarbeit muss die technischen, rechtlichen und institutionellen Möglichkeiten schaffen, um Angreifer rechtzeitig zu erkennen, der Strafverfolgung zuzuführen in der Hoffnung, dass davon eine Generalprävention ausgeht, und sie muss gewährleisten, Angriffe möglichst abzuwehren und Störungen rasch zu beseitigen. Dazu ist die Kooperation der privaten Akteure notwendig, seien es die Angegriffenen selbst, die ein solches Ereignis melden und zur Identifizierung der Täter beitragen müssen, oder der Dienstleister, die Verbindungsdaten etc. zur Aufklärung liefern müssen. Auch die Abwehr von Angriffen, zumindest ihr operativer, praktischer Teil, muss weitgehend vor Ort durch die Angegriffenen selbst geschehen, und sie trägt zuerst immer einen defensiven Cha-

rakter. Klassische Sicherheitspolitik kann hier nicht helfen. Damit wird staatliches Handeln nicht überflüssig, aber es muss sich dem neuen Kontext anpassen: Der Staat hat die Aufgabe, günstige rechtliche und institutionelle Bedingungen für die Handlungsfähigkeit der Privaten zu schaffen, die eigenen Infrastrukturen zu sichern, das Sicherheitsbewusstsein aller Internetnutzer und Provider zu stärken, (transdisziplinäre) Forschung und Entwicklung zu fördern, die Internetsicherheit zum Gegenstand hat, und sie muss im Rahmen der internationalen Zusammenarbeit eine Kultur und Praxis der Sicherheit etablieren. Diese „law enforcement/cyber-crime perspective“ [Dunn, Mauer, 2006, S. 197] wird von den meisten Staaten eingenommen, sie drückt eine „desecuritization“ der Cybersecurity [Dunn, Mauer, 2006, S. 200] und in einem Politikansatz aus, der privatem Handeln einen Vorrang gibt.

Das sind durchaus starke Argumente, die sicherheitspolitische, institutionelle und technische Aspekte geschickt verweben, und sie leisten einen wichtigen Beitrag zu der Erklärung, warum die heute vorherrschende Konzeption und Praxis der Internetsicherheit solchen Abstand hält von den traditionellen Konzepten und Instrumenten der Sicherheitspolitik. Ob diese Politik freilich noch hinlänglich und konsensfähig wäre, käme es zu einem weiteren starken Bedeutungszuwachs des Netzes *und* zu einer Verschärfung der Sicherheitslage, insbesondere durch drohenden Cyberwarfare oder -terrorismus, darf bezweifelt werden. Der auf Marktkräfte, private Vorsorge und Partnerschaft konzentrierte Ansatz der Cybersecurity könnte sich als unzulänglich erweisen.

Welche auch immer die Gründe dafür sein mögen - die Lücke zwischen der breit deklarierten Gefahreinschätzungen und der praktischen Politik mit ihrer geringen staatlichen Eingriffstiefe ist nicht zu übersehen. Aber das kann eine Momentaufnahme sein, und die Staaten haben die Option aktiv einzugreifen, wenn der bisherige Ansatz der Cybersecurity versagen sollte. Das ist explizit in der PPD-63,²¹⁹ aber auch in den nachfolgenden US-Heimatschutzstrategien wie der National Strategy for Homeland Security bzw. der National Strategy to Secure Cyberspace²²⁰ so vorgesehen. Vergleichbares gilt für die anderen Staaten, auch für Deutschland.

Tatsächlich gibt es vermehrt Stimmen, die diese aktive, regulierende und gesetzgeberische Rolle der Politik einfordern: Die privaten Betreiber der Internetinfrastruktur

²¹⁹ Dort steht, „regulation will be used only in the face of a material failure of the market...“.

²²⁰ Texte unter <http://www.whitehouse.gov/pcipb>.

und die Nutzer verließen sich darauf, dass immer die Anderen ihre Sicherheit mit organisierten (vgl. [Flynn 2004, 2004a]). Und selbst wenn die Betreiber ihren unmittelbaren Verantwortungsbereich, also ihren Teil der Infrastruktur, wirksamer gegen Angriffe und ihre Folgen absichern würden, bliebe eine Lücke. Denn in einem kaum zu überschauenden, planlos miteinander verbundenen Netzwerken kann es durch Angriffe zu Störungen und Schäden kommen, die keinem unternehmerischen Verantwortungsbereich zuzuordnen sind, sondern die nur, wenn überhaupt, aus einer übergeordneten Perspektive auf das gesamte Netzwerk zu verhüten bzw. zu bewältigen sind. Sie könne nur die Politik einnehmen, der deshalb eine größere Rolle zukommen müsse beim Schutz dieser kritischen Infrastruktur, und Politik müsse dafür sorgen, dass die erkannten Lücken geschlossen werden. Aber auch solche Forderungen nach einer aktiveren Politik sind noch weit weg von dem, was als traditionelle „securitization“ der Internetsicherheit verstanden werden könnte, die sie etwa das vierte Bild nahe gelegt. Zudem bleiben sie oft vage und beschreiben nicht präzise die neue Verteilung der Aufgaben zwischen Staat und Privaten - was hieße mehr staatliche Intervention konkret, welche Ziele und Instrumente zur Verbesserung der Cybersecurity hätte Politik ihren Arsenalen, die sie in dem Sicherheitskonzept, das von privatem Handeln geprägt ist, nicht nutzen könnte?

Wohin sich die Konzepte, Politiken und Maßnahmen für Internetsicherheit entwickeln, bleibt umstritten und offen. Politisches Handeln ist meist kein planvolles, beständiges Ansteuern von lange debattierten und dann vereinbarten widerspruchsfreien Zielen, denen angepasste Instrumente zugeordnet werden. Es ist das Reagieren auf Ereignisse im Kontext von Wahrnehmungen, die um Hegemonie ringen. Ob ein Ereignis wie ein Cyberangriff einen großen Schaden bringen muss, oder ob schon eine politisch-gesellschaftlich breit getragene Veränderung der Gefährdungswahrnehmung ausreichen würde, damit der Staat aktiver und leitend in die Gestaltung und Umsetzung der Internetsicherheit eingreift, lässt sich daher nicht im Voraus beantworten. Sicherheit ist kein Zustand, sondern ein Prozess, in dem das (kollektive) Sicherheitsgefühl eine wichtige Rolle spielt. Deshalb kann - von der individuellen bis hin zur gesellschaftlichen Ebene - die gefühlte Sicherheitslage von der abweichen, die, durchaus fehlbare, Experten als angemessen definieren. Auch wenn es zutreffen sollte, dass eine großräumige, erhebliche und längerfristige Beeinträchtigung des Internets nur bei entwickelten technischen und strategisch-organisatorischen Fähigkeiten der Angreifer denkbar ist und diese noch nicht zu erkennen sind, darf daraus nicht ge-

geschlossen werden, Cyberterrorismus sei auch künftig keine Gefahr und könne ohnehin nur dann Wirkung zeigen, wenn er zu Toten, Verletzten und hohen materiellen Verlusten führe. Sich wiederholende Störungen des Internets, Angriffe auf Server etc., die für sich wenig bedeutend sind, sich aber häufen und als Teil einer breiteren terroristischen Strategie erscheinen oder gar offen so deklariert werden, könnten eine politisch-psychologische Dynamik auslösen, die dazu führt, diese Ereignisse als nationale Bedrohung wahrzunehmen, selbst wenn die Wirkungen objektiv gering und zudem nicht anders wären, als wenn sie Folge der Aktionen Unpolitischer wären. Sicherlich käme diese Wahrnehmungseskalation schneller in Gang, würde durch einen Cyberangriff ein medienwirksamer Effekt in der physikalischen Infrastruktur erzielt, etwa ein Stromausfall für auch nur kurze Zeit. Wenig beruhigen würde es dann, wenn die Cyberangriffe nur mäßige Kenntnisse, aber aggressive politische Ziele offenbaren. Denn sie könnten auf eine erste Phase eines Lernprozesses hindeuten, der auf den Erwerb von exzellenten, koordinierten Fähigkeiten ausgerichtet ist. Da Cyberterrorismus immer die Absicht zu unterstellen wäre, die wirtschaftliche und nationale Sicherheit zu untergraben, müsste er, um seinem Ziel näher zu kommen, `nur` die geeigneten Fähigkeiten erwerben, also ein Lernprozess durchlaufen - eine sicherlich sehr schwierige Aufgabe, die aber bei günstigen Randbedingungen nicht als unlösbar erscheint. Breite Beunruhigung und ein Druck auf die Politik, rasch, demonstrativ und damit vielleicht auch wenig planvoll zu handeln, könnten sich dann aufbauen. Insofern ist die Bewältigung solcher Ereignisse auch ein Ringen um Normalität, um einen ruhigen, selbstbewussten Umgang mit Angriffen und ihren Folgen. Zugleich kann Sicherheitspolitik nicht den schlechtesten Fall ignorieren, zumindest nicht in zeitlich ausgreifender Perspektive. Deshalb muss sie Voraussetzungen dafür schaffen, auch die alltäglichen Ereignisse im Internet zu beobachten und auszuwerten, um frühzeitig Muster zu erkennen, die auf solche Lernprozesse deuten. Und sie muss Konzepte und Strukturen entwickeln, die rasch auf Cyberterrorismus reagieren können.

Die Politik für Cybersecurity stützt sich heute stark auf eine „law enforcement/cyber-crime perspective“, und sie betont die Eigeninitiative der Privaten. Zweifel werden lauter, ob sie damit für die Zukunft gerüstet ist. So bewegt sich Cybersecurity in ein dunstiges sicherheitspolitisches Feld hinein, dessen Position und Größe in der politisch-gesellschaftlichen Landschaft noch nicht präzise bestimmt ist, und dessen Ränder verschwimmen: Zeichnen sich Cyberwarfare-Potentiale ab, die für alle Netzwerke bedrohlich sind? Lauert im Nebel der Cyberterrorismus, oder geht die Gefahr nur von

den kriminellen Kräften aus, mit denen sich Staat und Gesellschaft auch auf anderen Feldern herumschlagen müssen? Ist die Politik in der Gefahr, über das Ziel hinauszuschießen und die Gesellschaft mit einem traditionellen Sicherheitskonzept zu überziehen, das nicht nur in Konflikt mit Bürgerrechten kommen, sondern auch die weitere Entwicklung und Nutzung des Internets erschwert, mit hohen Kosten belastet, ohne dass sein Nutzen gewährleistet ist? Oder wird es Zeit, sich auch in der Internetsicherheit auf eine Gefahr vorzubereiten, die sich heute nur schemenhaft abzeichnet, aber rasch zu einer Realität werden könnte - den Cyberterrorismus?

Eine neue Gefahr für ein sicheres Internet?

Das Internet ist heute nicht nur ein wichtiger und angenehmer Ort, an dem fast alles das getan werden kann, was auch in der physischen Welt möglich ist. Er ist auch ein unkontrollierter - und vielleicht unkontrollierbarer - Raum, in dem Gefahren lauern. Schon vor dem 11. September 2001 wurde Cyberterrorismus als eine dieser Gefahren gesehen, wenn ihm auch nicht allzeit und in jedem Land die gleiche Aufmerksamkeit gewidmet wurde. Seither sind in der Diskussion vermehrt Stimmen zu vernehmen, die eindringlich vor dieser Gefahr warnen. Sie werden in Europa nach einer Phase der Schwerhörigkeit zumindest seit einigen Jahren deutlicher wahrgenommen, und die Bemühungen um einen rechtlichen und organisatorischen Rahmen zur Bekämpfung der modernen Kriminalität richten sich im- und explizit auch gegen diese Gefahren im und für den Cyberspace. Noch immer aber klingen die Stimmen in den USA lauter und besorgter, und während Cyberterrorismus in Europa meist als eine potentielle, noch entfernte Möglichkeit gesehen wird, erscheint in den Diskussionen der USA diese Gefahr oft als akuter und drängender - ohne dass auch hier die Rhetorik ein Pendant fände in einer entschlossenen staats- und sicherheitspolitisch orientierten Praxis der Internetsicherheit.

Einer der Gründe für diese Fokussierung auf Cyberterrorismus liegt darin, dass sich in den USA zahlreiche Sicherheitsforschungsinstitute mit dem Thema befassen und es auf der Tagesordnung halten. Auch das hat seine Ursachen: In den USA wurde das Internet erfunden, es ist als neue Infrastruktur, deren technische Merkmale die Distanz bedeutungslos machen, tief und breit im Lande verankert, von weltweit agierenden Banken in Manhattan bis hin zu abgelegenen Farmen in Montana, die ihre Produkte mit Hilfe des Netzwerkes verkaufen. Dieser offene, selbstverständliche Umgang mit neuen Technologien lässt wenig Zweifel daran aufkommen, dass Terroristen ebenso rasch die Möglichkeiten des Netzes für ihre Zwecke erkennen. Schließlich hat die Furcht von Cyberterrorismus mit der Geographie zu tun: In der Öffentlichkeit der USA herrscht die Vorstellung, zumindest aber die Hoffnung, zwei Ozeane würden das Land vor äußeren Bedrohungen schützen. Das war und ist sicherlich nicht falsch, soweit es eine Invasion der USA betrifft - eine abwegige Vorstellung. Sehr viel weiter trägt diese Hoffnung allerdings nicht. Schon in den 60er Jahren ließen technologische Entwicklungen die Bedeutung des Raumes schwinden, als die UdSSR atomar bewaffnete Unterseeboote und Interkontinentalraketen in Dienst stell-

te, deren Atomsprengköpfe die USA in Minuten erreichen können. Aber diese strategische Grenznachbarschaft des atomaren Zeitalters wurde verdrängt, oder man jagte der Illusion nach, mit einem umfassenden Raketenabwehrschirm die Unantastbarkeit des Territoriums zu sichern. Auch der islamistische Terrorismus, der mit dem 1993er World Trade Center-Anschlag seine Präsenz den USA zeigte, schien mit Grenzkontrollen jenseits der Ozeane gehalten werden zu können. Umso größer war der Schock des 11. September 2001: Die untereinander nicht vernetzten Behörden hatten schlampig gearbeitet, sich wechselseitig das Leben schwer gemacht und waren knapp an Ressourcen. Die Hoffnung ging nicht auf - der Terrorismus hatte die Ozeane überquert. Trotzdem wurde das Konzept, die geographische Lage zu nutzen, um wirkungsvollen Schutz zu organisieren, nicht aufgegeben. Im Gegenteil. Intensive Grenzüberwachungen, die z. T., wie beim Flug- und Seeverkehr, auf die Abflug- bzw. Verladeorte jenseits der Ozeane vorgelagert werden, neue Informations- und Überwachungssysteme sollen dazu beitragen, das Einschmuggeln von gefährlichen Materialien, das Einsickern von Terroristen zu verhindern. Und das im Aufbau befindliche bescheidene Raketenabwehrsystem möchte die Bedrohungen ausschalten, die etwa von künftigen atomar bestückten Raketen Nordkoreas ausgehen könnten. Die USA sollen eine Insel der Sicherheit bleiben, und die Gefahren jenseits der Meere gehalten werden. Hier nun kommt das Internet ins Spiel, das in den Perzeptionen von Bürgern, Politikern und Experten beide Stränge symbiotisch zusammenbringt, nämlich den Bedeutungsverlust der Distanz und die Gefährdungen durch den Terrorismus: Terroristen können jenseits der Ozeane ihre Pläne schmieden, und das Internet ermöglicht es ihnen, sie in den USA auszuführen. Grenzkontrollen greifen nicht, Terroristen müssen nicht einreisen - per Mausklick greifen sie das Land an, zerstören kritische Infrastrukturen und schaden den Menschen. Zudem können sie (mit einer ungewissen Wahrscheinlichkeit) überraschend angreifen und anonym bleiben - eine militärische Antwort wäre ziellos.

Die Europäer haben nie auf den Schutz durch räumliche Distanz setzen können. Die Territorien sind vergleichsweise klein, die zahlreichen, verwinkelten Landgrenzen schwer zu kontrollieren, und sie bilden günstige Transitrouten für Illegale und möglicherweise auch für Terroristen, die zudem an Rändern der eigenen Metropolen heranwachsen. Und Europäer ertrugen über 40 Jahre eine extreme Zusammenballung konventioneller und taktisch-nuklearer Waffen, die über eine mehr oder weniger große Distanz auf sie zielten. Daher ist auch das Ende der Distanz durch das Internet für

die kollektive Erfahrung Europas keine wirkliche Neuigkeit - selbst wenn das Internet Terroristen neue Optionen bringt.

Nun gibt es in den USA Spötter, die Cyberterroristen heute und auch morgen nur in reißerischen Spalten von Zeitungen, in enthüllenden Fernseh-, Radiosendungen oder in der deftigen Gerüchteküche des Internets am Werke sehen. (Vermutlich gibt es auf der östlichen Seite des Atlantiks mehr dieser Spötter.) Wer aber nicht bei ihnen sitzen, sondern über die Gefahren ernsthaft sinnieren möchte, wird sich eine Antwort von Experten über das tatsächliche Ausmaß der Gefahren erhoffen. Aber sie klingt nicht einhellig, denn auch unter ihnen treffen Positionen und Denkschulen aufeinander. In ihren Lehren ist alles zu finden von „keiner“ bis hin zu „großer“ Gefahr durch Cyberterrorismus. Ihr Disput wurzelt weniger in der Einschätzung der heutigen Situation. Alle Experten würden wohl der Formulierung des Leiters der FBI-Cyber Division, L. Reigel, zustimmen, der im Dezember 2005 feststellte, „that since 9/11 terrorists have become much more sophisticated at using the Internet to their ends,“ dass er aber keine Kenntnis habe von „any major organized attempts to launch cyber attacks against the U.S.“.²²¹ Auch für andere Staaten liegen keine Hinweise auf solche Cyberangriffe vor, wie die Aussage des deutschen Innenministers Otto Schily 2003 zeigt.²²² Ihre Ursache hat die kontroverse Diskussion in unterschiedlichen Einschätzungen darüber, wie wahrscheinlich es ist, dass sich künftig Cyberterrorismus entwickelt und wie wirksam seine Angriffe sein könnten. Hier stehen sich diejenigen gegenüber, die aufrütteln wollen [Arquilla, 2003], [Verton, 2003], [Messmer, 2002], [Homer-Dixon, 2002], [Schwartau, 2000], [Arquilla, Ronfeldt, 2001, 1996] und die, denen es eher um die Beruhigung einer als zu schrill empfundenen Diskussion geht [Pollitt, 2005], [Leventhal, 2004], [Bendrath, 2003], [Clark, 2003], [Ward, 2003], [Green, 2002], [Lewis, 2005, 2002], [Schneier, 2005, 2003, 2001, 2000].

Die Aufrüttler hegen keinen Zweifel daran, dass es Cyberterrorismus bald geben wird, und sie fürchten ein digitales Pearl Harbor: Cyberterroristen machen das Internet funktionsunfähig bzw. attackieren über das Netz kritische Infrastrukturen, mit schwerwiegenden Folgen. Dieses Bedrohungsbild bestimmt zwar nicht die Tagesordnung, findet aber vor allem in den USA in Politik und Gesellschaft Aufmerksamkeit, und Sicherheitsverantwortliche von US-Unternehmen halten es für durchaus be-

²²¹ <http://www.fbi.gov/page2/dec05/reigelbriefing120705.htm>.

²²² http://www.bmi.bund.de/cln_012/nn_122688/Internet/Content/Nachrichten/Archiv/Pressemitteilungen/2003/06/Schily__und__Ridge__vereinbaren__Kooperation__Id__92348__de.html.

trachtenswert.²²³ Es erfährt aber auch massive Kritik. Die Möglichkeit eines solchen Angriffs erscheint den Beruhigern als „alarmistische Übertreibung“, die zu viel Aufmerksamkeit von den drängenden Gefährdungen der Internetsicherheit abzieht, etwa durch gewöhnliche Kriminalität. Cyberterrorismus gilt gar als eine Erfindung, als ein Schwindel, der, politisch instrumentiert, es ermöglicht, die Bürgerrechte zu beschneiden. Die Denkschule der Beruhiger sieht eine sehr geringe Wahrscheinlichkeit für große, erfolgreiche und wirksame Cyberangriffe generell und speziell durch Terroristen. Ward [2003] schreibt: „The threat posed by cyber-terrorism has been overhyped and the net is unlikely to become a launch pad for terror attacks.“ Und einige Beruhiger stellen selbst denjenigen, die, wie Weimann,²²⁴ den Cyberterrorismus nur als potentielle Drohung, als eine schwarze Wolke am Horizont sehen, die spöttische Frage, ob diese Wolke nicht von dem Rauch stamme, in den sich die zahlreichen Cyberterrorismusstudien aufgelöst hätten.

Zwischen den Extremen steht eine Gruppe, die man als Gefährdungsbewusste bezeichnen kann und die, bei allen Unterschieden in der Einschätzung, eine Einsicht teilt: Gegenwärtig ist die Gefahr eines Cyberterrorismus noch hypothetisch, aber sie könnte real und deutlich größer werden. Denn terroristische Organisationen lernen und könnten Schwachstellen erkennen und ausnutzen. Deshalb raten Gefährdungsbewusste zur vorsorglichen Beobachtung und Analyse der Entwicklungen und zur behutsamen Vorbereitung auf diese Gefahr (vgl. [Weimann, 2006], [Wilson, 2005, 2006], [Schmidt, 2003], [Geiger, 2000]). Aus dieser Gruppe heraus werden Zweifel laut, dass wirksame Cyberangriffe wirklich so einfach wären, wie es von Aufrütlern oft unterstellt wird. So vertritt der ehemalige Leiter der Abteilung für Cybersecurity im US-DHS, Amit Yoran, die Ansicht: „If it were so simple to take down the Internet with a few keystrokes, we would have seen this already.“ (zitiert nach [Leventhal, 2004]).

Neben dieser inhaltlichen Kontroverse ist ein weiteres Merkmal der Diskussionen die Unbekümmertheit, mit der das Wort Cyberterrorismus verwendet wird. Das gilt vor allem für Medien [Keith, 2005], gelegentlich aber auch für die Fachliteratur. Cyberterrorismus wird nicht immer definiert, obwohl der Begriff durchaus Unterschiedliches bezeichnen kann. Damit verliert er an Erklärungskraft und kann politisch instrumentiert werden. Schon im ersten Kapitel wurde das Problem thematisiert und die Unter-

²²³ Vgl. cio-today.com/story.xhtml?story_id=37447.

²²⁴ Vgl. <http://www.sicherheit-heute.de/suche,1395,2.htm>.

scheidung eingeführt zwischen einer terroristischen Nutzung des Cyberspace und Terrorismus gegen den Cyberspace. Sie wird nun weiter entfaltet.

Was ist Cyberterrorismus?

Cyberterrorismus verbindet die Begriffe Terrorismus und Cyber, die beide Raum für Interpretation lassen.

Terrorismus wird in Politik und Gesellschaft oft verwendet, aber häufig bleibt unklar, was und wer damit gemeint ist. So überrascht es nicht, dass global die Bemühungen, sich politisch auf eine Definition von Terrorismus zu verständigen, bislang erfolglos und vermutlich eine unendliche Geschichte sind. Auch die Sozialwissenschaften haben keinen expliziten Konsens gefunden, sind aber einer breit getragenen Definition näher [Quenivet, 2005], [Kerr, 2003]²²⁵ da sie sich um politischen Konsens und rechtliche Feinheiten nicht scheren müssen.

Der Dissens auf internationaler Ebene hat eine wesentliche Ursache darin, dass Terrorismus eine militärische Strategie, wenn nicht gar nur eine Taktik ist, die diverse ideologisierte Akteure für verschiedenartige Ziele benutzen [Schneier, 2003], [Münkler, 2004, 2002]. Stimmen sie mit diesen Zielen überein, unterstützen eine Reihe von Staaten, je nach politischer Interessenlage, terroristische Gruppen oder stellen sich ihnen zumindest nicht entgegen. Das dürfte ein wesentlicher Grund dafür sein, dass es in den Vereinten Nationen nicht gelingt, im Konsens festzulegen, was Terrorismus kennzeichnet und wer Terrorist ist. Auch der Vorschlag des High Level Panel on Threats, Challenges and Change aus dem Jahre 2004²²⁶ konnte das nicht ändern. Zwar ist aus wissenschaftlicher Sicht eine Abgrenzung von Guerilla/Partisan und Terrorismus/Terrorist möglich, da erstere in der Regel nur reguläre Truppen angreifen [Folscheid, 2001]. Sie führt aber nicht per se zu einer positiven, einer Legaldefinition von Terrorismus, die international politisch und rechtlich nutzbar ist. Bleibt sie aus, fällt es Staaten leichter, wie in der Erklärung zum 60. Jahrestag der Gründung der Vereinten Nationen geschehen, sich auf die Verurteilung des Terrorismus in „allen seinen Formen und Ausprägungen“ zu einigen - im Zweifelsfall gilt dann Organisation A, B ... in einigen Staaten eben nicht als terroristisch. Dieses Definitionsdefizit min-

²²⁵ Vgl. als Einführung <http://www.weltpolitik.net/Sachgebiete/Globale%20Zukunftsfragen/>.

²²⁶ "any action ... that is intended to cause death or serious bodily harm to civilians or non-combatants, when the purpose of such an act, by its nature and context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act; <http://www.un.org/secureworld/report.pdf>, S. 49; zu weiteren Definitionen, meist aus den USA vgl. <http://terrorismfiles.org/encyclopaedia/terrorism.html>.

dert auch die Wirksamkeit der Empfehlungen, die im Bericht des Generalsekretärs *Uniting Against Terrorism: Recommendations for a global counter-terrorism strategy*²²⁷ niedergelegt sind.

Daraus darf nicht geschlossen werden, es mache sich nur Beliebigkeit breit. Kerr [2003] hat in einer Untersuchung von 109 akademischen und offiziellen Definitionen von Terrorismus drei Elemente identifiziert, die ihnen zumeist gemeinsam sind: „the use of violence; political objectives; the purpose of sowing fear within a target population.“ Das kommt dem nahe, was in den westlichen Staaten als Merkmale des Terrorismus gesehen und in rechtliche Definitionen gegossen wird: Einschlägig sind z. B. die Aufzählung von Tatbeständen im Rahmen der Anti-Terrorismus-Konventionen des Europarates²²⁸ oder in dem Straftatenkatalog des §129 a des deutschen Strafgesetzbuches, der EU-Recht angepasst wurde und terroristische Vereinigungen charakterisiert. Dort heißt es, dass ihre Taten dazu bestimmt sind „die Bevölkerung auf erhebliche Weise einzuschüchtern, eine Behörde oder eine internationale Organisation rechtswidrig mit Gewalt oder durch Drohung mit Gewalt zu nötigen oder die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen, und durch die Art ihrer Begehung oder ihre Auswirkungen einen Staat oder eine internationale Organisation erheblich schädigen kann.“²²⁹

Der Begriff Cyberspace ist nicht selbsterklärend. Abgeleitet ist er von Kybernetik, und er kann als die (facettenreiche) Wissenschaft von der Computertechnik verstanden werden. Inzwischen ist er zu einem Synonym für das Internet und zugleich für das geworden, was man in ihm tun kann. Da das Internet aber im Kern nur ein Datentransportnetz für diverse Nutzungen ist, spezifizieren zusammengesetzte Wort diese Nutzung. So gibt es Cyber-Politik, -Wirtschaft, -Kultur, -Medizin, -Sex, -Forensik, -Polizei, -Krieg ... und auch -Terrorismus. Terrorismus macht also etwas in und mit dem Internet.

Werden zwei nicht konsensfähige bzw. vage Definitionen zusammengebracht, entsteht sicherlich kein klarer Begriff. Daher werden die Vorschläge, Cyberterrorismus zu definieren, auch mangels praktischer Erfahrungen mit ihm, meist nicht als zufrieden stellend betrachtet (vgl. [Gordon, Ford, 2002], [Siedschlag, 2002], [Lewis, 2002]), und es gibt den Vorschlag, den Begriff wegen seiner Unzulänglichkeiten gar nicht

²²⁷ <http://www.un.org/unitingagainstterrorism/contents.htm>.

²²⁸ http://www.coe.int/T/E/Legal_Affairs/Legal_co-operation/Fight_against_terrorism/default.asp.

²²⁹ Text: <http://www.gesetze-im-internet.de/stgb/index.html>.

zu verwenden [Schmidt, 2003]. Wer das nicht möchte, ist auf Definitionsversuche angewiesen. Kerr [2003] stellt einige vor: Das FBI definiert Cyberterrorismus als "any premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents." Für das National Infrastructure Protection Center des FBI ist Cyberterrorismus "a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda." Denning "defines cyberterrorism as unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear." J. A. Lewis sieht Cyberterrorismus gegeben, wenn "computer network tools" genutzt werden "to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population." (alle Zitate [Kerr, 2003]). Nach Pollit [2005] ist Cyberterrorismus ein "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents." Und Wilson definiert ihn als „the use of computers as weapons, or as targets, by politically motivated international, or sub-national groups, or clandestine agents who threaten or cause violence and fear in order to influence an audience, or cause a government to change its policy“ ([Wilson 2005], ähnlich [Cybersecurity, 2002]).

An dieser Stelle soll nicht der Versuch unternommen werden, in dieses Meer von Definitionen einzutauchen, um den gemeinsamen Grund zu erkunden. Sicher müssen Definitionen von (Cyber-)Terrorismus, die nationales und internationales Recht ausfüllen, präzise und einvernehmlich sein. Wie weit diese Vereinheitlichung aber in anderen Bereichen, etwa der Sicherheitspolitik, getrieben werden sollte, sei dahingestellt. Möglicherweise genügt für effektives Handeln eine pragmatische Definition, die Kerr's drei Elemente (use of violence; political objectives; the purpose of sowing fear) und die Art und Weise zusammenbringt, wie Terroristen das Internet heute nutzen und was sie künftig mit ihm anstellen könnten. Das führt zu der - schon eingeführten -

Unterscheidung zwischen einer *terroristischen Nutzung* des Internets und dem *Cyberterrorismus* im engeren Sinne, dessen Ziele es ist, die Nutzbarkeit des Internets zu beeinträchtigen und über das Netzwerk weitere kritischen Infrastrukturen anzugreifen.

Terroristen können also das Internet nutzen oder es zum Mittel bzw. Ziel von Angriffen machen. Ersteres ist heute schon Wirklichkeit, letzteres erst eine Möglichkeit, über deren Wahrscheinlichkeit und Realisierbarkeit gestritten wird.

Nutzung des Internets durch Terroristen

Terroristen nutzen das Internet, wie sie auch andere Kommunikationstechnologien nutzen, wenn sie sich davon Vorteile versprechen. Das erstaunt nicht, denn kriminelle Akteure, sind sie doch Teil der Gesellschaft, haben sich schon immer der Technologien bedient, die sie bereitstellt, sei es die Eisenbahn, das Auto, Flugzeug oder das Telefon, das sich vor fast 100 Jahren zu verbreiten begann. Natürlich war und ist das mit Bemühungen der staatlichen Stellen verbunden, durch Polizeistreifen, Überwachung etc. Informationen zu gewinnen und die Bewegungs- und Kommunikationsmöglichkeiten dieser Akteure einzuschränken. Das ist beim Internet und seiner Nutzung durch Terroristen nicht anders: Nachrichtendienste und Polizei durchstreifen das Netz auf der Suche nach Seiten und Servern, über die terroristische Kommunikation und Information laufen, nach Verdächtigem und Verbotenem, nach Strukturen und Verbindungen zwischen Akteuren, nach Informationen, die Aufklärung von Straftaten erleichtern und Anschläge verhindern.

Welche Behörde zuständig ist, welches Ausmaß an Überwachung notwendig ist, wo ihre Grenzen liegen, ob und wie viel Wissen zwischen Nachrichtendiensten und Polizei ausgetauscht, in welchem Maße die Informationsfreiheit beschränkt werden darf, alles das ist oft national und international strittig. Nur zu gerne würden einige Staaten, die unter dem Deckmantel des Kampfes gegen Kriminalität und Terrorismus die Freiheiten, die das Internet eröffnet, beschneiden, dafür internationale Billigung erhalten. Diesen Balanceakt zwischen Überwachung und Freiheit musste auch der Weltgipfel WSIS 2005 bestehen. Er formulierte im Rahmen seiner Visionen einer Informationsgesellschaft mit Blick auf die Nutzung des Internets durch Kriminelle und Terroristen: „While recognizing the principles of universal and non-discriminatory access to ICTs [Information and Communication Technologies] for all nations, we support the activities of the United Nations to prevent the potential use of ICTs for pur-

poses that are inconsistent with the objectives of maintaining international stability and security, and may adversely affect the integrity of the infrastructure within States, to the detriment of their security. It is necessary to prevent the use of information resources and technologies for criminal and terrorist purposes, while respecting human rights.”²³⁰ Und auch die Strategie des Generalsekretärs Uniting Against Terrorism will, bei allen Maßnahmen gegen die terroristische Nutzung des Internets, die Entwicklungs- und Nutzungsmöglichkeiten des Netzes nicht beschneiden.

Diese Freiheit und Offenheit des Internets gibt Terroristen und ihren Sympathisanten die Möglichkeit, es für ihre Zwecke zu nutzen. Schon in der frühen Zeit des Internets stellten radikale Islamisten Seiten in das Netz, die in englischer Sprache ein Publikum suchten. Aber sie waren eher rudimentär mit Postercharakter. Mit der Verbreitung und Entwicklung des Internets, mit besseren Browsern und neuen Diensten, aber auch wegen des hohen Fahndungsdrucks in der realen Welt, hat sich die terroristische Nutzung des Internets, auch durch islamistische Terrorgruppen, deutlich weiterentwickelt [Wilson, 2006], [Glasser, Coll, 2005]. Neben den Sicherheitsbehörden beobachten und analysieren heute auch Wissenschaftler und gesellschaftliche Gruppen detailliert diese Nutzung [Weimann, 2006, 2005, 2004], [Conway, 2006, 2005, 2002], [Kohlmann, 2005], [Musharbash, 2005], [Kristof, 2005], [Lewis, 2005a], [Krempel, 2004], [Kumler, 2004], [Thomas, 2003], [Tsfati, Weimann, 2002], [Paz, 2002]. Auch die Politik zeigt Besorgnis: Die Innenminister von Frankreich, Deutschland, Italien, Polen, Spanien und Großbritannien sind im März 2006 übereingekommen,²³¹ unter Beteiligung von Europol die Internetnutzung durch terroristische Strukturen zu analysieren (Check the Web).

Das Ergebnis solcher Analysen wird eindeutig sein: Terroristen nutzen verstärkt und intensiv das Netzwerk. Sie richten Diskussionsforen (chatrooms) ein, die breit zugänglich sind, abgeschlossene Austauschzirkel (Mailing Groups) und mehr oder weniger leicht zu findende Webseiten. Weniger klar hingegen sind die Einzelheiten: Etwa die Zahl der terroristischen Internetauftritte, ihre Bedeutung für terroristische Gruppen und die Wirksamkeit ihrer Aktivitäten im Netz. Aussagen wie es gäbe im Jahre 2004 etwa 4500 „terrorist related websites“ [Weimann, 2004], sind eher ein Hinweis auf eine Größenordnung denn eine belastbare Zahl. Der Begriff terrorist related website ist genauso wenig einvernehmlich definiert wie der des Terrorismus; eine

²³⁰ <http://www.itu.int/wsis/docs/geneva/official/dop.html>.

²³¹ http://www.bmi.bund.de/cln_012/nn_122688/Internet/Content/Nachrichten/Pressemitteilungen/2006/03/Innenministertreffen__Heiligendamm.html.

unbekannte Zahl von Seiten ist nur Eingeweihten bekannt, und es ist einiger Aufwand oder spezifische Software nötig,²³² sie zu entdecken (das gilt um so mehr für Mailing Groups und für einen Teil der Foren); die Anzahl der Webseiten variiert unter Verfolgungsdruck und sagt nichts darüber aus, welche (un)mittelbaren Gefahren von den dahinter stehenden Organisationen ausgehen. Auch ist die Funktion der Seiten unterschiedlich: Nur ein Teil der terroristischen Gruppen, Organisationen und Netzwerke operiert international, viele bleiben, zumindest was ihre Aktionen betrifft, auf (südliche) Länder und Regionen beschränkt, in denen ein breiter Zugang zum Netz aus vorwiegend ökonomischen und infrastrukturellen Gründen fehlt. Haben sie eine Internetpräsenz, richtet sie sich zwar auch auf die technisch versierten und relativ kaufkräftigen Minderheiten im eigenen Land, die einen privaten oder - vorwiegend - einen Netzzugang über Cybercafes haben. Vor allem dient die Präsenz der Beeinflussung der öffentlichen Meinung, der Politik in hoch entwickelten Ländern sowie von Bürgern der Länder, in denen sie operieren, die aus politischen oder ökonomischen Gründen im westlichen Ausland leben. Mit der weiteren Verbreitung und intensiveren Nutzung des Internets in den Ländern, die heute noch über eine schwache Infrastruktur verfügen, werden solche Terroristen bei ihrer Netznutzung stärker das örtliche Umfeld berücksichtigen.

Für welche Zwecke nutzen Terroristen heute das Internet? Weimann [2006] identifiziert acht: „Psychological warfare, propaganda, data mining, fund raising, recruitment, networking, information sharing, planning and coordination.“ Conway [2006, 2005] kondensiert aus der Literatur fünf zentrale Zwecke. Danach eignet sich das Internet aus Sicht von Terroristen für:

- Propaganda

Auch Terroristen haben das Problem, Aufmerksamkeit zu finden in einer Welt, die mit Nachrichten überflutet wird. Zwar gewinnen sie mit direkten Drohungen und Aktionen rasch das Interesse traditioneller Medien, die noch immer die größte Reichweite haben. Aber es fällt ihnen schwer, mit alltäglicher Propaganda deren Wahrnehmungsschwelle zu durchbrechen. Daher ist die Einwirkung auf das breite Publikum und die Orientierung von Sympathisanten und Unterstützern nur sehr begrenzt möglich. Zudem haben Terroristen keinen unmittelbaren Einfluss darauf, wie sie, ihre Ziele und Aktionen in den Medien präsentiert werden. Das Internet

²³² Im Herbst 2005 gab die PAN AMP AG (<http://www.panamp.de>), die u. a. fremdsprachige Suchprogramme vertreibt, bekannt, ein von ihr entwickeltes Programm in türkischer Sprache habe Seiten mit Informationen der Al-Qaida entdeckt.

gewährt ihnen diese Möglichkeiten: Sie legen Seiten an, die an allen Orten jederzeit gelesen werden können, sie bestimmen die Inhalte ihrer Botschaften selbst, und setzen mediale Effekte (Ton, Bild) sowie interaktive Möglichkeiten ein, die heute im Netz gerne gesehen werden. Das Internet bietet sogar die Möglichkeit, sich auf die Netznutzer einzustellen: Server können deren Sprache anhand ihrer Browser erkennen und sie zu einer landessprachlichen Seite lenken. Das Netzwerk ist ein direkter, nicht gefilterter Kommunikationskanal zu Zielgruppen, die über das Netz auf das Angebotene reagieren können.

Damit Propaganda wirken kann, muss den Zielgruppen deutlich gemacht werden, dass das, was präsentiert wird, auch wirklich authentisch ist, also von der Gruppe stammt, die sie vorgibt zu sein. Dieses für das Netz charakteristische Problem wird dadurch gemildert, dass typische Sprechweisen, Schlüsselworte oder Webseiten gewählt werden, die schon als vertraute Quellen bekannt sind.

Mit einer so elaborierten Internetnutzung entsteht ein Raum, der genutzt wird für Desinformation, die manipulative Selbstdarstellung bzw. Präsentation des Gegners, der durch Drohungen beeinflusst wird, und für die Selbstvergewisserung der Sympathisanten und Unterstützer, die mit Parolen und Aufrufen versorgt werden. Die Internetpräsenz ermöglicht, breite Unterstützung, große Ressourcen und starken Einfluss zu suggerieren. Das stärkt die Anhängerschaft und kann Bedrohungen potenzieren. Freilich ist diese Präsenz nur *ein* Mittel der Propaganda, und traditionelle Medien genießen wegen ihrer Verbreitung oft den Vorzug. So gehen Videos an Sender, die sie in das weltweit sendende Satellitenfernsehen einspeisen, wie an den arabischen Sender al-Dschasira.²³³ Parallel dazu erfolgt eine Verbreitung über das Internet.

- **Netzwerkbildung**

Das Internet macht es möglich, weit verstreute Beteiligte und Unterstützer in vielschichtige Strukturen einzubinden, die rasche Kommunikation ermöglichen und dabei, je nach Bedarf, einer breiten Beziehungspflege oder einer intimen, abgeschotteten Kommunikation und Koordination dient. Die intensive Nutzung des Internets als *ein* Weg der Bildung von abgeschlossenen Zirkeln belegt die Festnahme des Ingenieurs Mohammed Khan im Juli 2004 in Pakistan: Er verschlüsselte Botschaften des bin Laden und versandte sie per E-Mail. Aus die-

²³³ Vgl. <http://english.aljazeera.net/NR/exeres/55ABE840-AC30-41D2-BDC9-06BBE2A36665.htm>; zur Einschätzung des Senders [Miles, 2005].

sen und weiteren Gründen ist Verschlüsselungssoftware in den kritischen Blick von Sicherheitsbehörden geraten. Da sie aber auch Daten für legitime Zwecke verschlüsselt und so ihren Missbrauch durch kriminelle Gruppen verhindert, wird diese Software, genau wie Proxy-Server bzw. Anonymisierungsdienste, zu einer janusköpfigen (dual use) Technologie - sie hat positive und negative Effekte zugleich. Ob es sinnvoll und möglich ist, ihre Ausbreitung und ihren Einsatz zu kontrollieren, wird schon lange kontrovers und bislang ergebnislos diskutiert [Ackermann, 1998]. Denn trotz aller Probleme präferiert heute in den westlichen Staaten eine politische und gesellschaftliche Majorität die freie Nutzung solcher Software, da ihr Nutzen überwiege.²³⁴ Eine Möglichkeit, trotzdem ihren Missbrauch einzudämmen, bestünde darin, gesetzliche Grundlagen dafür schaffen, dass die Schlüssel unter bestimmten Bedingungen den Ermittlungs- und Strafverfolgungsbehörden ausgeliefert werden müssen. Darüber wird z. B. in Großbritannien kontrovers diskutiert [Espiner, 2006]. Ein solcher Schritt könnte jedoch dazu führen, dass zwar rechtswidrig, aber unkontrolliert freie Verschlüsselungssoftware ohne Schlüsselweitergabe aus dem Netz auf britischen Rechnern installiert würde, was den Effekt der Gesetzgebung hintertreiben würde. Anonymität und Verschlüsselung werden Herausforderungen bleiben für die Arbeit der Sicherheitsbehörden, auch bei der Terrorabwehr.

- Rekrutierung

Propaganda, Mobilisierung von Sympathisanten und die Rekrutierung von Aktivisten sind miteinander verwobene Aktivitäten. Dabei ist das Internet hilfreich. Es ermöglicht, in multimedialer Form ein breites Publikum anzusprechen, aus einem Sympathisantenkreis diejenigen herauszufinden und einzubinden, die stärker an den Zielen und Aktionen interessiert sind. Zum Einsatz kommen interaktive Technologien, die etwa in offenen Diskussionsforen nach Stichworten suchen, die auf Sympathien hindeuten. Aber auch die Einbindung von (potentiellen) Mitgliedern in geschlossene Diskussionsforen, die nur mit Schlüsselwort oder persönlicher Empfehlung zugänglich sind, wird genutzt. Wie erfolgreich diese Rekrutierungsbemühungen sind, können, wenn überhaupt, nur Nachrichtendienste einschätzen. Es gibt Berichte, dass sich in einigen wenigen Fällen Zellen gebildet haben aus Personen, die sich im Netz kennen gelernt haben bzw. die so angesprochen wurden.

²³⁴ Vgl. die Thesen unter <http://www.datenschutzzentrum.de/material/themen/pgp/thesen.htm>; der Bundesbeauftragte für Datenschutz hat die Seite <http://www.bfd.bund.de/>.

Wo und wie das geschehen ist, ob (moderierte und abgeschlossene) Foren dabei eine Rolle gespielt haben, bleibt im Dunkeln. Häufiger sollen nach diesen Berichten hingegen existierende Gruppen mit Hilfe des Internets untergestützt und zusammengehalten worden sein.

Auch bei der Rekrutierung dürfte noch immer gelten, dass der direkte Kontakt, die persönliche Ansprache ausschlaggebend und häufiger ist.

- Informationsbeschaffung und -verbreitung

Wie andere Nutzer können Terroristen das Internet nutzen, um Informationen zu sammeln und zu verbreiten. Denn das Internet ist eine große offene Bibliothek, in der sich alle Verständigen bedienen können. Das Informationsangebot übertrifft das einzelner Bibliotheken, und die Digitalisierung ganzer Bibliotheksbestände wird diesen Vorsprung ausbauen. Dazu kommen zahllose privat eingestellte Informationen und das, was dunkles Netz (dark web) genannt wird²³⁵ - versteckte Seiten, die nur für Eingebundene in einem System ebenbürtiger Rechner (peer-to-peer) zugänglich sind.

Recherchen im Internet versprechen mit Suchmaschinen Erfolg, und auch abgelegene Themen und Quellen können gut bearbeitet werden. Von Vorteil ist dabei, dass Terroristen nicht physisch in Bibliotheken, in öffentlichen Räumen präsent sein zu müssen, mit allen damit verbundenen Risiken. Diese Informationsbeschaffung kann reichen von harten technischen Fakten über die Analyse der öffentlichen Meinung und ihre Beeinflussbarkeit bis hin zur Sammlung von Angaben über Personen und Terrorziele. Ob Terroristen dabei data mining-Techniken (statistische Modelle, Algorithmen etc.) einsetzen, die scheinbar nicht zusammenhängende Informationen zusammenführen sollen, ist unbekannt. (Sie kommen aber durch Sicherheitsbehörden zum Einsatz, um frühzeitig Muster zu erkennen, die auf terroristische Aktionen hinweisen [Seifert, 2004].²³⁶) Informationen werden dann, gelegentlich komprimiert als Handbücher, in das Netz gestellt, um technische, strategische und taktische Handlungsanleitungen für terroristische Nutzer zu geben. Dass Handbücher von Terroristen öffentlich zugänglich sind, ist freilich keine Erfindung des Internets. In den 60er und 70er Jahren wurden Handlungsanweisungen der lateinamerikanischen „Stadtguerilla“ durch Verlage veröffentlicht [Alves, Detrez, Marighela, 1971].

²³⁵ Vgl. http://en.wikipedia.org/wiki/Dark_web.

²³⁶ Zur Kritik an ihrer Nutzbarkeit vgl. S. 135.

Für dieses Informationsangebot im Internet wird oft der Begriff virtuelle oder digitale Bibliotheken gebraucht, die als Teil einer „open university of jihad“ [Paz, 2002] ein kleines Studium im Netz ermöglichen sollen. So schreibt Kohlmann [2005]: „With the strategic and military knowledge now available on the Internet, you could literally take a correspondence course in terrorism - assuming (...) you can read Arabic“. Aber auch in anderen Sprachen, vorwiegend in Englisch, sind Publikationen im Netz zu finden, aus denen Terroristen, aber auch andere Gruppen und gewaltbereite Individuen ihren Nutzen ziehen können bzw. die speziell für eine Nutzung durch Terroristen gut verborgen in das dunkle Netz gestellt werden [Weimann, 2004], [Thomas, 2003]. Jedoch ist die Qualität der im Netz präsentierten Informationen sehr unterschiedlich. Nutzer müssen die Fähigkeiten haben, etwa das auszusortieren, was an falschen oder unvollständigen technischen Informationen präsentiert wird.

Während die Informationen im Netz über den Bau konventioneller Sprengsätze, die aber nur zu einem Teil über Suchmaschinen aufzufinden sind, relativ präzise zu sein scheinen, wird viel darüber spekuliert, ob das Internet hilfreich ist bei der Herstellung von Massenvernichtungswaffen. Was Kernwaffen betrifft, gibt es breite Übereinstimmung, dass das nicht so ist. Die grundlegende Physik und grobe Blaupausen sind schon lange bekannt, aber es fehlt das geeignete Kernmaterial, das bislang in der notwendigen Qualität und Menge nicht auf dem Schwarzmarkt aufgetaucht ist. Zudem ist der Bau eines Sprengkörpers ein äußerst schwieriges, großindustrielles Unterfangen, das nur Staaten schultern können. Radioaktiv verschmutzte Sprengkörper sind einfacher herzustellen, wenn das hoch radioaktive Material verfügbar ist. Für ihren Bau muss kein grundlegendes Wissen aus den tiefen Gründen des Internets gezogen werden. Über Chemikalien, Bakterien und Viren wird, wie die Expertin für Biowaffen, Elisabeth Hauschild, in einem Interview mit dem Onlinemagazin Sicherheit-heute feststellt, im Netz viel geschrieben, und es sei erschreckend, wie einfach es Gruppen der organisierten Kriminalität und Terroristen damit gemacht wird.²³⁷ Aber auch in diesen Bereichen sind, bis auf den Anschlag der Aum-Sekte mit Chemikalien [Clinehens, 2000] und die bislang nicht aufgeklärte Ausbringung von Milzbrandsporen in den USA Ende 2001,²³⁸ keine konkreten Ergebnisse bekannt geworden, die zeigen, dass Terroristen die

²³⁷ http://www.sicherheit-heute.de/politik/terrorismus,172,Drohen_chemische_biologische_und_nukleare_Terroranschlaege,news.htm.

²³⁸ <http://www.washingtonpost.com/wp-dyn/content/article/2006/10/13/AR2006101301417.html>.

Techniken beherrschen. Probleme wie Beschaffung, Zucht, Verarbeitung und Ausbreitung der empfindlichen biologischen Organismen stellen hohe Hürden bei biologischen Waffen dar.

Trotzdem bleibt das Netz eine Fundgrube für Terroristen, und nicht selten enthalten Seiten von Organisationen, Personen für Terroristen nützliche Informationen, die weder Verbindung mit ihnen haben noch ihnen zunutze sein wollen. Als Reaktion auf das wachsende Angebot solcher sensibler Informationen gibt es vor allem nach 9/11 Diskussionen, Bestrebungen und in vielen Fällen auch konkrete Schritte, sie erst gar nicht oder nicht länger in das Internet einzustellen.²³⁹ Dieses durchaus berechnete Anliegen, das in westlichen Staaten in der Regel auf die freiwillige Beteiligung der Informationshalter angewiesen ist, bringt nicht weniger verständliche kritische Anfragen mit sich: Es sei beliebig schwierig, kostspielig und willkürlich, Informationen als sensibel zu definieren. Zudem werde Forschern die Informationsbeschaffung erschwert, und der terroristische „open source threat“ sei nur ein willkommenes Argument, um die Wissensquellen von Bürgerinitiativen etc. auszutrocknen. Auch nütze es nichts, Informationen, die im Internet weltweit gestreut und in traditionellen Bibliotheken präsent sind, von Servern zu nehmen. Rasch würden sie - mit Hilfe von Scannern - wieder im Netz sein.

Tatsächlich dürften Bemühungen, das Informationsangebot im Internet zu begrenzen, immer der tatsächlichen Entwicklung nachhinken und sie kaum beeinflussen. Ein Beispiel ist Google Earth,²⁴⁰ das einen detaillierten Blick auf wichtige Orte des Globus gestattet, und dessen Dienst für viele Nutzer und für den Anbieter selbst (finanziell) attraktiv ist (vgl. [Svoboda, 2005]). Kaum war Google Earth im Internet verfügbar, gab es Befürchtungen, Terroristen und andere Kriminelle könnten nun Anschläge, Fluchtwege auskundschaften, ohne sich der Gefahr einer frühzeitigen Entdeckung auszusetzen.

Wie auch immer die tatsächlichen Gefahren gesehen werden, zu denen ein solcher Dienst und andere Informationen beitragen könnten - es gibt nicht selten keine Möglichkeit, durch politische Intervention oder rechtliche Schritte Seiten mit inkriminiertem Inhalt aus dem Netz zu nehmen. Oft fehlt schon die rechtliche Handhabe, da präsentierte Inhalte in dem Land, in dem der Server steht, gegen kein Gesetz verstoßen. Das Netzwerk mit seiner verflochtenen wirtschaftlichen

²³⁹ Sicherheitsbedenken erschwerten beispielsweise die Veröffentlichung einer Dissertation von Gorman über die Topologie des Internets; vgl. [Gorman, Malecki, 2000; Gorman et al., 2003].

²⁴⁰ <http://earth.google.com/>.

und technologischen Dynamik entzieht sich auch hier vielen Eingriffs- und Regulierungsversuchen.

- Geldbeschaffung und -transferierung

Auch internationaler Terrorismus benötigt Geld, selbst wenn die Kosten, die zur Durchführung großer terroristischer Anschläge aufgebracht werden mussten, bislang recht bescheiden waren. Sie lagen zwischen einigen zehn- und einigen hunderttausend US-Dollar. Es gibt vielfältige nationale²⁴¹ und internationale Bemühungen, an denen Interpol wesentlich beteiligt ist,²⁴² um die Geldquellen zu verstopfen. Zu ihnen zählt die noch nicht in Kraft gesetzte Konvention des Europarates über Geldwäsche, Terrorismusfinanzierung sowie Ermittlung, Beschlagnahme und Einziehung von Erträgen aus Straftaten; ferner die Aktivitäten der von der Gruppe der sieben Industriestaaten 1989 gegründeten Financial Action Task Force (FATF).²⁴³ Insgesamt sind die Ergebnisse der Bemühungen aber eher durchgewachsen [Lichtblau, 2005]; [Kaplan, 2006].

Dabei rückt auch das Internet in den Blick. Denn als interaktives Medium ist es geeignet, Geld einzuwerben und unmittelbar über das Netz diskret zu transferieren, etwa unter Zuhilfenahme von Portalen für anonyme Geldtransfers. Wahrscheinlich nutzen Terroristen auch Mittel wie Abfangen von Geheim- und Kreditkartennummern etc., um an Geld zu kommen. Dabei sind Kooperationen mit gewöhnlichen und auch mit transnationalen organisierten Kriminellen möglich [Swartz, 2005], [Makarenko, 2004], auch um Geld zu waschen.²⁴⁴

Bei Geldbeschaffung und -transferierung scheint das Internet aber bislang nur eine untergeordnete Rolle zu spielen. Heute haben direkte, diskrete Sammlungen mit Hilfe von Vorfelddorganisationen und traditionelle, informelle Geldtransfers über Mittelsmänner und spezielle Banken (hawala - Vertrauen)²⁴⁵ für die Finanzen des Terrorismus eine größere Bedeutung.

- Unklar ist, ob und in welchem Ausmaß die direkte Planung von Anschlägen, operative Entscheidungen und Maßnahmen (command and control) über das

²⁴¹ Die USA werteten Daten der in Belgien ansässigen internationalen Society for Worldwide Interbank Financial Telecommunications (<http://www.swift.com>) aus; als Überblick für die USA: [Weiss, 2005].

²⁴² Vgl. <http://www.interpol.int/Public/FinancialCrime/MoneyLaundering/default.asp>.

²⁴³ Vgl. <http://conventions.coe.int/Treaty/Commun/ListeTraites.asp?CM=8&CL=GER>; <http://www.fatf-gafi.org>; vgl. die Dokumentation des Workshops Public-Private Co-operation in Combatting the Financing of Terrorism, Zürich, Dezember 2005; <http://pforum.isn.ethz.ch/events/index.cfm?action=detail&eventid=255>.

²⁴⁴ Vgl. <http://www.anti-geldwaesche.de/>; zum Stichwort Geldwäsche s. <http://www.bmi.bund.de>.

²⁴⁵ Vgl. dazu <http://www.interpol.int/Public/FinancialCrime/MoneyLaundering/hawala/default.asp>.

Internet kommuniziert werden (so [Thomas, 2003]). Hier gehen die Positionen der Beobachter auseinander. Möglicherweise spielen Opportunitäten eine Rolle, also die technische Verfügbarkeit, die Überwachungssicherheit, aber auch die Umstände vor Ort. Jedoch ist der Austausch einiger E-Mails im Vorfeld von Terroranschlägen allein kein Hinweis auf eine bemerkenswerte operative Rolle des Netzwerkes.

Das Internet bietet Terroristen aber nicht nur einen neuen Operationsraum. Es wird auch beobachtet durch Sicherheitsbehörden, und Terroristen müssen deshalb abwägen zwischen seinen Vorteilen und Risiken.

Soll eine terroristische Seite in die Öffentlichkeit wirken, muss sie relativ leicht zu finden sein. Das ermöglicht es Sicherheitsbehörden, sie in Zusammenarbeit mit Providern rasch zuzuschlagen, soweit das rechtlich möglich ist. Auch Private unterstützen solche Bemühungen, etwa das Search for International Terrorist Entities-Institute (SITE), dessen stellvertretende Leiterin Rita Katz durch ein Buch über das Aufdecken eines islamitischen Netzwerkes [Katz, 2003] bekannt wurde, ferner die auf Islamismus spezialisierte Internet-Haganah sowie das Northeast Intelligence Network.²⁴⁶

Solche Erfolge sind angesichts der Flexibilität des Internets oft von kurzer Dauer. Seiten finden rasch einen neuen Provider, um mit einem leicht veränderten Domain Namen wieder aufzutauchen. Schwierig wird es, wenn die Webseiten in Ländern abgelegt sind, in denen es Sympathien für solche Gruppen gibt, die Terrorismus anders definieren und eine bestimmte Gruppe nicht als terroristisch qualifizieren, in denen die Strafverfolgung schlecht funktioniert, oder wenn es schlicht zu lange dauert, bis ein rechtliches Verfahren zur Sperrung einer Seite abgeschlossen ist - dann ist sie schon zum nächsten Provider überspielt. Und stellt der die Seite in das Netz, ohne einen Blick auf die Inhalte zu werfen, sind ihre Betreiber zumindest für einige Zeit wieder online. Aus solchen Gründen hat es Forderung gegeben, terroristische Seiten durch Hacken und Softwareangriffe aus dem Netz zu drängen (vgl. [Lettice, 2005]).

Nicht immer ist es aus Sicht der Terrorismusabwehr sinnvoll zu versuchen, terroristische Webseiten, Foren etc. zu schließen. Sind sie erst einmal entdeckt, können sie für Geheimdienste, Polizei, aber auch für Forscher von Nutzen sein, die authentische Informationen über und aus den terroristischen Gruppen und seinem Umfeld gewinnen. (Wie authentisch und wie wichtig sie wirklich sind, müssen Experten entschei-

²⁴⁶ <http://www.siteinstitute.org>; <http://www.haganah.org.il/haganah/index.html> (die Haganah war während der britischen Mandatszeit eine zionistische Untergrund-Militärorganisation und bildete den Grundstock der israelischen Armee); ferner <http://www.homelandsecurityus.com>.

den. Denn die Möglichkeit, dass Nachrichtendienste mitlesen, ist solchen Gruppen bewusst. Hier können In- und Desinformation ineinander übergehen.) Foren können aber auch kritische Stimmen auf sich ziehen, die der verbreiteten Ideologie widersprechen und so die Rekrutierungsfunktion der Seiten schwächen. Es gibt sogar Behauptungen, dass zerstrittene Gruppen wechselseitig versuchen, ihre Seiten lahm zu legen bzw. schlecht zu reden. Schließlich legen Nachrichtendienste (vermutlich) eigene Seiten an, die wie die von Terroristen erscheinen, um Aktivisten, Sympathisanten etc. anlocken, sie zu identifizieren und ihren Diskussionen zu folgen.

Selbst die vorsichtige, versteckte Nutzung des Netzwerkes, der intime Austausch unter terroristischen Akteuren hinterlässt Spuren. Polizei und Nachrichtendienste versuchen, ihnen zu folgen, um Netzwerke und ihre Planungen frühzeitig zu erkennen. Die USA haben „terrorist surveillance“ zu einem zentralen Element ihrer Strategie gemacht, und ihre auf Überwachung spezialisierten Dienste wie die National Security Agency/Central Security Service“ (NSA/CSS)²⁴⁷ und das National Reconnaissance Office (NRO)²⁴⁸ haben wahrscheinlich Möglichkeiten, die Kommunikation über das Internet weltweit zu beobachten. Wenn identifizierte Personen bzw. E-Mail-Adressen gezielt überwacht werden, ist das relativ einfach: Die Datenpakete werden, etwa durch Sniffer-Programme, direkt am Rechner oder bei einem Service-Provider, herausgefischt und kopiert. Wesentlich aufwändiger wird es, wenn in der Datenflut des Internets quasi blind nach Strukturen gesucht wird, die auf Muster terroristischer Netzwerke und einen Informationsaustausch hinweisen.²⁴⁹ Um hier Einsichten zu gewinnen, müssen alle Datenpakete - zumindest an bestimmten Netzknoten, über die Daten aus verdächtigen Regionen kommen - kopiert und zu Rechnern von Nachrichtendiensten geleitet werden, um sie mit data mining-Systemen zu durchsuchen. Da schätzungsweise allein bis zu zehn Milliarden E-Mails pro Tag durch das Netz gehen, erfordert eine so breite Überwachung einen erheblichen Aufwand. Arkin [2005] spricht davon, dass täglich allein die NSA „intercepts and records more than 650 million `events` worldwide“, wobei diese Zahl auch den Datenanfall aus Telefonüberwachung einschließt. Dieser Wust an Daten wird elektronisch verarbeitet, um anhand

²⁴⁷ <http://www.nsa.gov/>; gegründet 1952, ist sie als Teil des DoD die geheime Verschlüsselungs- und Abhörorganisation; vgl. auch <http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/>.

²⁴⁸ <http://www.nro.gov/index.html>; die „Augen und Ohren“ des DoD und der CIA im Weltraum.

²⁴⁹ Die US-Administration unterschied bei der Verteidigung des NSA-Abhörprogramms zwischen gezieltem Abfangen (monitoring), das mit richterlicher Zustimmung die Auswertung von Inhalten einschließt, und der „weniger intrusiven“ Suche nach Strukturen, Netzen der Kommunikation (detection), ohne schon Inhalte auszuwerten; <http://www.washingtontimes.com/op-ed/20060123-093307-8640r.htm>. Vergleichbares könnte für andere westliche Staaten mit ähnlichen Programmen gelten.

festgelegter Kriterien (Begriffe, Namen, Adressen, diverse IP-, Telefon-, Kreditkartennummern etc.) Interessantes zu finden, das dann, zunehmend auch unter Beteiligung von Menschen, weiter untersucht, gegebenenfalls übersetzt, durch sachkundige Experten ausgewertet und dann in einem Gesamtbild bewertet wird. (Möglicherweise bekommen Analytiker deutlich weniger als ein Prozent der Daten überhaupt zu sehen.) Kritiker verweisen auf wichtige Aspekte: Der Nutzen von data-mining-Systemen sei fraglich [Schneier, 2006], da terroristische Verschwörungen nur wenige typische Muster aufweisen, die solche Systeme benötigen,²⁵⁰ um erfolgreich mit wenigen Fehlalarmen zu arbeiten.²⁵¹ Viele Fehlalarme würden institutionelle und personelle Ressourcen binden, und der Versuch, ihre Rate zu senken, erhöhe die Wahrscheinlichkeit, dass wichtige Informationen unbemerkt bleiben. Zweitens, die eigentliche Herausforderung liege in der Auswertung der gesammelten Daten, und es gäbe Hinweise auf erhebliche Verzögerungen, speziell bei der Übersetzung. Große ungenutzte Archive seien die Folge. Deshalb dürften Terroristen davon ausgehen, dass ein Teil ihres Austauschs ungelesen das Internet durchqueren oder nicht (angemessen und zeitnah) übersetzt und ausgewertet werden. Drittens gäbe es Gegenstrategien von Terroristen. Sie könnten sich in Webseiten einhacken und dort in einem verborgenen Directory ihre Daten ablegen, die Mitwisser abrufen; sie könnten, was nicht belegt ist, Steganographie nutzen, also Informationen in Bildern, Audiofiles etc.²⁵² verstecken, die trotz mathematischer Fortschritte²⁵³ kaum zu finden wären; schließlich gäbe es Austauschmöglichkeiten, bei denen die Information selbst nicht das Netz durchqueren muss - mehrere Personen „share a single E-Mail account, and the person writing the message doesn't send it but saves it as a draft. Then the recipient logs in and reads the draft without it ever actually being transmitted.“ [Kristof 2005]; vgl. auch [Hirsh, 2006].

Wie die intensive Netznutzung zeigt, scheint aus Sicht terroristischer Organisationen, trotz der Bemühungen der Sicherheitsbehörden, die Bilanz von Chancen und Risiken positiv zu sein: Der Überwachungsaufwand ist hoch, seine Ergebnisse vermutlich durchwachsen, die medialen und kommunikativen Möglichkeiten des Internets sind verlockend. Es wäre, so Cronin [2003, S. 51], naiv anzunehmen “that what is good

²⁵⁰ Ihr erfolgreicher Einsatz von durch Kreditkartenfirmen beruht gerade darauf, dass klar definierte Profile (die Ausgabenmuster der Nutzer) vorliegen, die frühzeitig Kartenbetrug erkennen lassen.

²⁵¹ Er lenkt die Aufmerksamkeit auf ein Netz, das sich nach genauer Analyse als nicht existent erweist.

²⁵² Vgl. <http://www.de.wikipedia.org/wiki/Steganographie>.

²⁵³ http://www.bsi.de/presse/pressinf/251104_cast.htm.

for international commerce and international communication is not also good for international terrorists.” Und deshalb wäre es fahrlässig, wenn sich die Sicherheitsbehörden nicht rüsten würden, um diese wohl intensiver werdende, verfeinerte Nutzung zu begrenzen, um das Internet so zu überwachen, dass es zu einer feindlichen Umgebung für Terroristen (und für andere Kriminelle) wird.

Dazu bedarf es der intensiven Beteiligung der europäischen Staaten. Immerhin sind zwei der fünf größten Bedrohungen, die in der Europäischen Sicherheitsstrategie von 2003 genannt sind,²⁵⁴ direkt mit dem Netzwerk verknüpft: internationaler Terrorismus und (grenzüberschreitende) organisierte Kriminalität. Eine solche Anstrengung fügt sich ein in die Anti-Terrorstrategie der Vereinten Nationen, die ein Kapitel enthält „Denying access to recruits and communication by countering terrorist use of the Internet“. Dass es bei allen diesen Bemühungen zu Konflikten über die rechtliche Zulässigkeit, die politische Wünschbarkeit und die Verteilung der Kosten bestimmter Maßnahmen kommen kann, liegt in der Natur der Sache.

Jedoch wäre es ein Fehler anzunehmen, eine stärkere Netznutzung durch Terroristen führe zwangsläufig zu einem Bedeutungsverlust anderer Kommunikationsformen, insbesondere der persönlichen Begegnung und des direkten Austauschs von Datenträgern, die unauffällig mitgeführt werden können. Deshalb raten Kritiker (vgl. [Hirsh, 2006]) gerade den US-Behörden, sich nicht zu stark zu fixieren auf die Netzwerküberwachung, falls sie finanziell und personell auf Kosten traditioneller Methoden der Nachrichtendienste geht.

Unklar ist, ob die Netznutzung durch Terroristen die Zahl und Gefährlichkeit ihrer Aktionen erhöht [Conway, 2005, S. 28ff], ebenso wie es noch nicht sicher ist, dass das Internet wirklich das Medium wird, „mit dessen Hilfe die totalitären Islamisten den Sprung von der militärischen Kader-Organisation zur global agierenden Bewegung vorbereiten“ [Musharbash, 2005]. Zu weit hergeholt erscheint das jedoch nicht, denn eine verstärkte terroristische Nutzung, verbunden mit immer besseren Soft- und Hardware-Kenntnissen, kann die Struktur terroristischer Organisationen, aber auch ihr Aktivitätsspektrum verändern. Die Übergänge zwischen Sympathisanten, Unterstützern und Aktiven verschwimmen, die organisatorischen Strukturen werden noch flacher, beweglicher und netzwerkartiger [Arquilla, Ronfeldt, 2001]. Aus diesen Netzwerken heraus könnten sich rasch, kaum vorhersehbar und für kurze Zeit, kleine

²⁵⁴ Die anderen Gefahren sind die Proliferation von Massenvernichtungswaffen, regionale Konflikte, zerfallen(d)e Staaten; vgl. A Secure Europe in a better World - The European Security Strategy; <http://www.iss-eu.org/solana/solanae.pdf>.

Gruppen herauskristallisieren, die physische Angriffe durchführen. Ein zweiter Effekt kann die Herausbildung von terroristischen Kulturen und Organisationsformen sein, die ihr Wissen um die Funktionsweise, die infrastrukturelle Bedeutung und ihre Vertrautheit mit dem Internet nutzen, um diese Infrastruktur selbst und mit ihr verbundene kritische Infrastrukturen zum Angriffsziel zu machen. Es ist wichtig, nicht nur die Internetnutzung durch Terroristen zu analysieren und möglichst zu begrenzen, sondern auch ihre sozialen Strukturen, Kompetenzen, den Wandel der ihrer Organisationen, der Funktionsweise und Operationen unter dem Einfluss des Cyberspace zu verstehen. Dabei könnte sich auch zeigen, dass das Internet dazu beiträgt, interne Konflikte und Fragmentierung innerhalb terroristischer Bewegungen zu forcieren. Das Netz erleichtert Zersplitterung, denn auch Abweichler und Abspalter finden irgendwo noch Gleichgesinnte, auf die sie in der realen Welt kaum gestoßen wären. Das verschärft Konflikte zwischen einer wachsenden Zahl diverser Bewegungen, Gruppen, und Grüppchen, erschwert ihre Überwachung und schafft Raum für unvorhersehbare Koalitionsbildungen, über ideologische und politische Grenzen hinweg.

Terrorismus gegen das Internet

Es ist keine Neuigkeit, dass technische Störungen, Unfälle etc. kritische Infrastrukturen generell und auch das Internet beeinträchtigen, und solche Ereignisse treten immer wieder auf [Grubestic, Murray, 2005]. Hauptursache ist die fahrlässige Zerstörung von Kommunikationskabeln, oft durch schlecht vorbereitete Bauarbeiten. Deshalb sollen sich Unternehmen in den USA über die zentrale Nummer 811 vor dem Beginn von Bauarbeiten darüber informieren, ob und wo in ihrem Baugebiet wichtige Infrastrukturen vergraben sind [Poulsen, 2006].

Angriffe durch substaatliche Akteure auf kritische Infrastrukturen mit physischen Mitteln sind hingegen in westlichen Industriestaaten selten. Aber es gab und gibt sie: So wurden in den 60er Jahren in Südtirol von der Unabhängigkeitsbewegung Strommasten gesprengt. Anschläge gegen Infrastrukturen verübte auch die Irisch Republikanische Armee, und die Attentate auf öffentliche Verkehrsmittel in Madrid 2004 und London 2005 brachten diese Infrastruktur örtlich kurzfristig zum Erliegen. Auch die Angriffe auf das Pentagon, die Zerstörung der Zwillingtürme in New York und der durch den Absturz in Pennsylvania vereitelte Angriff auf das Weiße Haus im Jahre 2001 können als Anschläge auf kritische Infrastrukturen der Administration und Finanzwelt verstanden werden. Dabei legten diese Terroranschläge die Verwundbar-

keit moderner Gesellschaften und einiger ihrer Infrastrukturen bloß: Der Luftverkehr in den USA wurde für einige Tage lahm gelegt, die Verkehrsinfrastruktur und Telekommunikation in Großraum New York erheblich beeinträchtigt. Mobiltelefone fielen wegen Netzüberlastung aus, und der Einsturz des Welthandelszentrums und einiger benachbarter Gebäude ließ zeitweise an einigen, z. T. weit entfernten Orten das Internet ausfallen. Denn Anlagen des Telekommunikationsunternehmens Verizon wurden beschädigt und ein wichtiger Glasfaserring im Zentrumskomplex durchtrennt. Dazu kam die Überlastung der Server von Nachrichtenagenturen durch die hohe Zahl von Seitenaufrufen, eine mittelbare Folge der Angriffe. Trotzdem erwies sich das Internet insgesamt als recht robust und arbeitete bald wieder unbeeinträchtigt - ganz so, wie sich das seine Erfinder gedacht hatten [NRC, 2003]. Vereinzelt wurden Telekommunikationssysteme aber auch gezielt zerstört [Gorman, 2003], möglicherweise, wie in Spanien, durch baskische Terroristen im Juni 2002: Zur gleichen Zeit wurden Backbones der spanischen Gesellschaft Telefonica zertrennt, so dass regionale Internet-Dienstleistungen schlechter oder gar nicht verfügbar waren [Heise, 2002].

Zahlreicher sind die Angriffe mit Software und durch Hacken. Es gibt Berichte, Hacker seien über das Internet in Rechner anderer kritischer Infrastrukturen eingedrungen oder Viren hätten sie beeinträchtigt. Auch Schadsoftware hinterlässt Spuren. So versandte der Wurm SQLSlammer zahlreiche User Datagram Protocol - Pakete, die in vielen Regionen der Welt stark erhöhten Paketverkehr auf Backbones und dadurch steigenden Paketverlust brachten, so dass die Nutzbarkeit des Internet zeitweise an einigen Orten eingeschränkt war und weitere kritische Infrastrukturen litten: Bankautomaten funktionierten nicht, Buchungssysteme von Fluggesellschaften verweigerten ihren Dienst. Ein weiteres Beispiel findet sich in einem Zeitungsartikel, in dem behauptet wird, im März 2005 „hackers gained access to the electronic control systems of the nation's electric power grid“; zudem habe der MSBlast-Wurm die Reaktion der Netzbetreiber auf den Stromausfall im Mittleren Westen und Nordwesten der USA im August 2003 zumindest erschwert ([Hoopes, 2005]). Aber solche Meldungen bleiben vage, und es ist durchaus denkbar, dass der angebliche Zugang zum Kontrollsystem auf einen Zugriff auf die Webseite beschränkt war. Schließlich zeigt sich ein populärer Fall, bei dem es einem Angreifer gelungen ist, in ein Kontroll- und Steuerungssystem einzudringen, bei genauer Betrachtung in einem anderen Licht. Green [2002] schreibt: “An Australian man used an Internet connection to re-

lease a million gallons of raw sewage along Queensland's Sunshine Coast after being turned down for a government job. When police arrested him, they discovered that he'd worked for the company that designed the sewage treatment plant's control software." Hier haben sich also spezifische Innentäterkenntnisse und unzureichender Schutz der Rechner ergänzt. Generell ist festzuhalten, dass Erwartungen, große Cyberangriffe stünden bevor, nicht eingetreten sind: So blieben während der Invasion der Streitkräfte einer „Koalition der Willigen“ in den Irak im Jahre 2003 die zuvor beschworenen massiven Cyberangriffe aus, ebenso wie der von der Sicherheitsfirma IDC,²⁵⁵ ein Ableger der Bostoner International Data Group, vorhergesagte wirkungsvolle Angriff von Cyberterroristen auf das Internet.²⁵⁶

Möglicherweise bauen sich aber neue Verwundbarkeiten auf, die Angreifer reizen könnten. Die SCADA-Systeme zur Steuerung von Prozessen in der physikalischen Infrastruktur, insbesondere in dem Elektrizitätssektor, gelten als potentiell wertvolle Ziele für Cyberterroristen, und „the hacking community is becoming increasingly aware of SCADA ... and is beginning to focus their attention on them.“ [Byres, Lowe, 2004, S. 7]. Lange wurden diese Systeme, nutzten sie doch proprietäre Netzwerke und Techniken, als weitgehend immun gegenüber Cyberangriffe von Außen betrachtet. Das beginnt sich nach Meinung einiger Experten zu ändern, seit SCADA-Systeme aus ökonomischen Gründen immer öfter über das Internet gesteuert werden und billigere, überall verfügbare Techniken bzw. Software zum Einsatz kommen. Eine zweite Entwicklung scheint die unbedachte, nicht immer allen Entscheidungsträgern bekannte Verknüpfung von Internet und SCADA zu sein. Damit haben Hacker prinzipiell die Möglichkeit, SCADA zu manipulieren oder außer Funktion zu setzen, um Schäden in der physikalischen Welt anzurichten [Byres, Lowe, 2004]. Jedoch gehen die Meinungen darüber auseinander, wie wahrscheinlich es ist, dass das gelingt. Eine Hürde bleibt, neben den üblichen Abwehrsystemen gegen Hacken und Viren, die Komplexität der meisten SCADA-Systeme, an der „all but the most experienced hacker“ scheitern würden [Kotadia, 2005]. Die meist robusten Systeme sind zudem auf Störungen und das erneute Anfahren ausgerichtet, so dass „cyberterrorists would need to attack multiple targets simultaneously for long periods.“ [Wilson, 2005, S. 10f]. Auf einer Tagung des Unternehmens Blackhat²⁵⁷ Anfang 2006 hat

²⁵⁵ <http://www.idc.com>.

²⁵⁶ Vgl. <http://www.news.com.com/2100-1001-977780.html>.

²⁵⁷ <http://blackhat.com>.

eine Studie des Unternehmens Internet Security Systems Inc²⁵⁸ [ISS, 2006] für die IT-Sicherheit kritischer Infrastrukturen und Industrieanlagen in den USA speziell unter Berücksichtigung der SCADA ein kritisches, wenn auch nicht alarmistisches Bild gezeichnet. „There is neither cause to panic nor cause to ignore the issue. ... Our own experience penetrating systems leads us to believe that it should be taken seriously.“ Denn die Untersuchung zeigte, dass „industry (is) in denial about how much they are connected to the Internet“, und dass es „numerous uncontrolled interconnects“ zum Internet gibt [Zitate: ISS, 2006]. Die „sichere Trennung von Office- und Produktionsnetzen (ist) ein Mythos“, wie Heise in seinem Bericht zur Tagung feststellt.²⁵⁹

Um zu einer belastbaren Risikoabschätzung für SCADA-Systeme zu kommen, wurde in den USA ein 8.5 Millionen US-Dollar teures Forschungsprogramm unter der Ägide des DHS gestartet, das die Verwundbarkeit der SCADA-Systeme und ihre Schutzmöglichkeiten untersucht [Fisher, 2005].

Ein Resümee hat festzuhalten, dass es physische terroristische Angriffe auf Infrastrukturziele immer wieder gibt, aber die Internet-Infrastruktur von ihnen weitgehend verschont blieb. Cyberangriffe, die gezielt auf die Funktionsfähigkeit des Netzwerk abzielen, etwa dDoS-Angriffe, kommen vereinzelt vor, und einige wenige Versuche waren erfolgreich, über das Netz die Rechner anderer kritischer Infrastrukturen so zu beeinträchtigen, dass Anlagen nicht mehr normal funktionierten. Jedoch waren diese Angriffe von spezifischen Voraussetzungen abhängig, in ihren Auswirkungen begrenzt und hatten keinen erkennbaren terroristischen Hintergrund.

Das alles kann aber nicht wirklich beruhigen, und es gibt heute in Wissenschaft und Politik breite Übereinstimmung, dass die Gefahr eines Terrorismus gegen den Cyberspace existiert. Wie groß sie ist, bleibt kontrovers, und über mögliche Folgen gibt es sehr unterschiedliche Einschätzungen. Deshalb wird hier auf den Begriff Risiko verzichtet. Denn er fordert eine Quantifizierung der Eintrittswahrscheinlichkeit und Folgen, die zuverlässig bislang niemand liefern kann.²⁶⁰ Um das Risiko von Cyberterrorismus einzuschätzen, müssten die Fragen beantwortet werden:

- Welche Fähigkeiten haben Cyberterroristen?
- Welche Absichten verfolgen sie?

²⁵⁸ <http://iss.net/>.

²⁵⁹ <http://www.heise.de/newsticker/meldung/69063>.

²⁶⁰ Vgl. als Einführung <http://www.de.wikipedia.org/wiki/Risiko>.

- Welche Objekte (Ziele) sind besonders gefährdet, welche Auswirkungen hätte ein Angriff, wie hoch ist die Verwundbarkeit der Ziele? Welche Effekte hätte ihre Störung, d. h. wie ist der Grad der Abhängigkeit anderer Strukturen und Akteure vom Internet, die Wirksamkeit der Verteidigung, die Redundanz, also die Flexibilität, mit der das beeinträchtigte technische System, aber auch die Gesellschaft, die verbleibende Wirkung eines Angriffes verarbeitet? Schließlich spielt auch der Grad an Selbstsicherheit und -vertrauen von Gesellschaft und Politik eine Rolle, der sie mehr oder weniger in die Lage versetzt, mit Schäden und Verlusten zu leben bzw. sie mehr oder weniger widerstandsfähig macht gegen die im- und expliziten Drohungen mit weiteren Aktionen.

Bislang ist keine Frage unter den Experten einvernehmlich beantwortet.²⁶¹ Ungeklärt ist auch, welche Resilienz, Robustheit, welche Reaktions- und Anpassungspotentiale die Infrastrukturen hätten, die Opfer eines erfolgreichen Cyberterrorismus sind, um diesen Impuls und seine Auswirkungen abzumildern. Das ist ein Mangel, denn die Potentiale verweisen auf ein Verständnis von hybrider Infrastruktur, das über deren technisch-materielle Form hinaus auch ihre Einbindung in das konkrete gesellschaftlich-politische und individuelle Umfeld einschließt. Wird es berücksichtigt, kann sich ein angemessenes Verständnis von Verwundbarkeit entfalten: Nur wenn alle Potentiale ausgeschöpft sind, über die der Angegriffene verfügt, um noch ein Mindestmaß an Handlungsfähigkeit zu erhalten, offenbart sich der tatsächliche Grad an Verwundbarkeit. Die Größe dieser Potentiale ist nicht nur abhängig von der Resilienz der Infrastruktur, die durch Hard- und Software zu erhöhen ist. Um die Verwundbarkeit zu ermitteln, sind alle Strukturen und ihre Verarbeitungsmechanismen zu berücksichtigen, in die der Impuls abgegeben wird, aber auch die Akteure, ihre sozialen Einbindungen und ihre Wahrnehmungen des Ereignisses, die mit darüber entscheiden, ob aus einem Störungsimpuls ein (schwerer) Schaden wird. Hier kommen politisch-psychologische Aspekte in das Spiel, nämlich die Fähigkeit der Menschen und eines Landes, mit der Furcht umzugehen, den Terrorismus verbreiten will.

Sicherlich wäre es klug, will Terrorismus Angst verbreiten, einfach keine zu haben, und aus statistischer Sicht gibt es dafür Argumente [Mueller, 2004]: Das Risiko, zum Opfer von Terrorismus zu werden, ist - bislang - statistisch gesehen marginal, die materiell-physikalischen Schäden durch terroristische Aktionen sind gering verglichen mit dem Kapitalstock (Brutto-Anlagevermögen), und die ökonomischen Verluste re-

²⁶¹ Vgl. <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/>.

sultieren vor allem aus Panikreaktionen der Börsen bzw. der Einschüchterung von Touristen und Investoren [Frey, Lüchinger, Stutzer, 2004], die sich bei vernünftigem Handeln weitgehend vermeiden ließen; schließlich sind globale ökonomische Auswirkungen des Terrorismus kaum zu spüren - das Wachstum der Weltwirtschaft beträgt seit 2001 etwa 20 Prozent.²⁶²

Der Vorschlag, Ruhe zu bewahren, ist sicherlich sinnvoll. Jedoch funktioniert die Wahrnehmung von Gefahren anders: Unfreiwillige, von Externen auferlegte Gefährdungen, auf die man selbst keinen Einfluss hat, werden überschätzt und erzeugen Ängste. Sicherlich sollte eine abwägende Politik sich bemühen, einer kühlen, objektiven Betrachtung der Gefahren Raum zu geben und Ängste einzudämmen, um terroristische Strategien in einem Kernbereich zu treffen. Dazu gehört deutlich zu machen, dass transnationaler Terrorismus, so wie wir ihn heute kennen, das Funktionieren westlicher Staaten bei rationalem Verhalten der Bedrohten nur marginal beeinträchtigen kann. Aber eine solche generelle, beständige Gelassenheit gibt es nur in Lehrbüchern. Denn keine Gesellschaft akzeptiert, dass sie ab und zu zum Ziel von Massenmördern wird, ohne dass sich seine Menschen und die Politik verändern. Dazu kommt, dass die Furcht bleibt vor dem, was kommen kann und was über das hinausgeht, was bislang an Erfahrung mit Terrorismus gemacht wurde, etwa ein Einsatz von Kernwaffen und biologischer Waffen. Für objektive statistische Schadensbewertungen wäre dann kein Raum mehr, die ja, durchaus zynisch, beweisen könnten, dass die Zerstörung zweier Städte in Japan durch Atombomben die spätere dynamische Entwicklung des Landes nicht verhindert hätte. Mit ihrem Einsatz wäre eine Schwelle überschritten, die zu politischen und gesellschaftlichen Zuständen führen würde, die jenseits der Erfahrung lägen. Auch deshalb ist es die zentrale Aufgabe jeglicher Sicherheitspolitik, unter *allen* Umständen zu verhüten und zu verhindern, dass terroristische Gruppen sich in den Besitz solcher Waffen bringen. Gegen ihren Einsatz würden auch die Folgen verblassen, die wirksamer Terrorismus gegen den Cyberspace für Gesellschaften brächte, die auf funktionierende Netzwerke angewiesen ist.

Fehlen objektive Maßstäbe und entwickeln Gesellschaft und Politik kein vorherrschendes Verständnis, wie sie mit den Gefahren umgehen, weitet sich in Zeiten der Bedrohung der Raum, in dem politisch-gesellschaftliche Akteure miteinander um Hegemonie ringen über die Einschätzung der Gefahren, über die notwendige Intensität

²⁶² Zu Schätzungen der Kosten von Terrorismus s. auch [Brück, Schumacher, 2004], [Leibfritz, 2004].

der CIP, CIIP und anderer Maßnahmen sowie ihr Verhältnis zu dem sicherheitspolitischen Instrumentenkasten der Politik. Bei diesem Ringen spielt z. B. die gesellschaftliche Akzeptanz oder Ablehnung von so vielschichtigen, assoziativen Begriffen wie „Digital Pearl Harbor“ oder „cyberwarfare“ als Charakterisierung der Gefahren eine wesentliche Rolle. Ob (potentieller) Terrorismus gegen den Cyberspace gesellschaftlich mit dem Bild von Pearl Harbor oder, eher abwertend, mit Graffiti verbunden wird, da man ihm nicht viel mehr als die Entstellung von Webseiten zutraut, beeinflusst ganz wesentlich die Politik für Cybersecurity.

Trotz aller Vorbehalte und Anfragen gibt es, wie dargelegt, gute Gründe, sich nicht entspannt zurückzulehnen und darauf zu hoffen, Terrorismus gegen den Cyberspace sei auch künftig nur eine weit entfernte Möglichkeit und bleibe eine virtuelle Schmiererei. Er ist eine neue Gefährdung für die Sicherheit des Internets und anderer kritischer Infrastrukturen, die freilich erst im Aufbau ist und deren Ausprägung und Wirksamkeit noch nicht klar abzuschätzen ist. Dabei muss dieser Terrorismus gar nicht in der Lage sein, jederzeit wirksam und andauernd große Teile des Netzes unbenutzbar zu machen. Seine Wirkung könnte Terrorismus gegen den Cyberspace schon entfalten, wenn er erfolgreich immer wieder Störungen produziert, die Zweifel aufkommen lassen an einer freien, ungestörten und sicheren alltäglichen Nutzung des Netzes. In Analogie zur Marinestrategie würde es diesem Terrorismus, ganz im Sinne des asymmetrischen Kampfes, reichen, eine „fleet in being“ zu sein:²⁶³ Nicht die - ohnehin unerreichbare - Kontrolle über die Nutzung des Netzwerkes wird angestrebt, sondern die Fähigkeit, immer wieder die Netznutzung zu stören. Das brächte hohe Kontrollkosten und erschwert, dass sich das Internet und sein Gebrauch so entfalten, wie das aus ökonomischen und anderen Gründen politisch gewollt und gesellschaftlich präferiert wird.

Wie gefährdet ist nun diese kritische Infrastruktur Internet? Im folgenden Kapitel werden Ergebnisse des Simulationsmodells Internet Security Simulation vorgestellt. Das Modell widmet sich einem Aspekt detaillierter, den Pakettransport des Internets und der Auswirkungen strategischer Störungen für diese zentrale Dienstleistung des Netzwerkes.

²⁶³ http://www.en.wikipedia.org/wiki/Fleet_in_Being.

Simulation strategischer Angriffe auf die Infrastruktur des Internets

Die strategische Störung der Funktionsfähigkeit des Internets ist eine Option, die Cyberterrorismus anstreben könnte. Das Modell INESS kann eine der denkbaren Varianten dieses Terrorismus, die Störung zentraler Internet Exchange Points (IX) bzw. Backbones und seine Folgen für den Paketverkehr, simulieren. Die Leitfrage der Simulationsexperimente lautet: Ist das Internet als ein sich selbst regulierendes paketorientiertes Netzwerk bei solchen Störungen so tolerant bzw. überlebensfähig,²⁶⁴ dass der Paketverkehr weitgehend sichergestellt ist?

Da die Verwundbarkeit bzw. Überlebensfähigkeit des Internets abhängt von der Topologie, der Verteilung der Kapazitäten bei Backbones und IX und von der Paketmenge, also dem Verkehr im Internet und damit der Auslastung von Backbones und IX, werden alle drei Variablen in Simulationsmodell Internet Security Simulation berücksichtigt (*Abbildung 2*). Die Funktionsweise des Modells, dass das Internet mit seinen wesentlichen Eigenschaften, einschließlich des Routing,²⁶⁵ nachbildet, wurde an verschiedenen Stellen ausführlich beschrieben [Fischer, Lepperhoff, 2005], [Fischer, Lepperhoff, 2004], [Fischer, Lepperhoff,

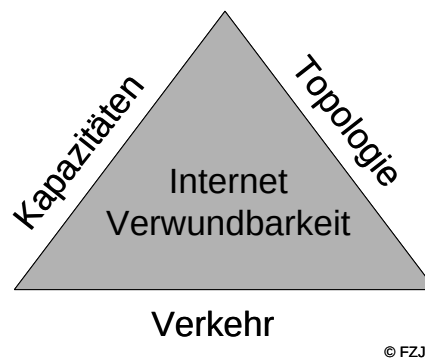


Abbildung 2: Dreieck der Verwundbarkeit des Internets

Volst, 2003], [Lepperhoff, Fischer, Volst, 2002]. Deshalb wird an dieser Stelle darauf verzichtet. Vorgestellt werden die Ergebnisse von Experimenten, die unterschiedliche Nutzungen des Internets durch Akteursgruppen bzw. Institutionen abbildet. Für eine Familie von Experimenten wurde das Modell INESS modifiziert, um die Auswirkungen (hypothetischer) prioritärer Dienste auf den Paketverlust zu untersuchen.²⁶⁶

²⁶⁴ In Grubestic/Murray [2005, p. 802] findet sich die Definition: Überlebensfähigkeit ist „the ability of a network computing system to provide essential services in the presence of attacks and failures, and recover full services in a timely manner.“

²⁶⁵ <http://www.de.wikipedia.org/wiki/Routing>.

²⁶⁶ Private Intranetze, die die gleichen Kabel wie das öffentliche Internet nutzen und nur durch Software abgesondert sind, wären bei Ausfällen von Backbones und IX gleichermaßen beeinträchtigt.

Simulationsexperiment Regierungskommunikation

Um die Auswirkungen strategischer Angriffe zu simulieren, wurde beispielhaft eine hypothetische deutsche politisch-administrative Infrastruktur entworfen, die als Regierung bezeichnet wird.²⁶⁷ Untersucht wurde, welche Auswirkungen eine strategische Störung von IX und Backbones auf die Kommunikation innerhalb dieser kritischen Infrastruktur Regierung hat, wenn sie über das öffentliche Internet erfolgen würde. Die Kommunikation wird durch Datenpakete abgebildet, die zwischen den nationalen Regierungsakteuren, aber auch mit weiteren Regierungen und internationalen Organisationen weltweit über das Internet ausgetauscht werden. Maßstab für die Überlebensfähigkeit des Internets ist der Verlust an Datenpaketen generell und speziell der Regierungspakete sowie die Qualität der Verbindungen zwischen den Akteuren.

Die Simulation enthält zwei Varianten der Regierungskommunikation: Erstens, eine Regierungskommunikation, bei der ein über die Zeit verteiltes Kommunikationsverhalten nachgebildet ist. Akteure der fiktiven Regierung tauschen untereinander Datenpakete aus, die von INESS zufällig in einer vorgegebenen Zeitspanne abgeschickt werden. Zweitens, die Kommunikation als Bandbreite mit einer Kapazität von 240 Megabit/Sekunde (MBit/s). Diese extreme Größe des Datenstroms wurde aus methodischen Gründen gewählt: Während beim Modus der verteilten Zeit die Pakete während eines günstigen Zeitfensters, in dem es keine Störungen gibt, unterwegs sein können, ist dies bei der Bandbreite nicht möglich. Hier speisen alle Akteure der Regierung pro Zeitschritt²⁶⁸ jeweils ein identisches Paket zu jedem anderen Akteur ein, so dass dauerhaft eine Kommunikation aufrechterhalten wird. Damit ist die Paketproduktion in Phasen mit und ohne Störungen identisch. Kommen also Pakete nicht an, liegt das nicht an einem ungünstigen Zeitpunkt der Versendung, sondern hat andere Gründe wie mangelnde Ausweichrouten via Backbones im Netzwerk.

Die vom Modell erzeugten Pakete der Regierung treffen im Backbonenetz auf die von einem Nutzungsmodell produzierten Pakete, die private bzw. gewerbliche Nutzung repräsentieren und als Hintergrundrauschen bezeichnet werden. Sie stehen bei Störungen mit den Paketen der Regierung im Wettbewerb. In den Simulationsexperimenten wurde das Hintergrundrauschen variiert, um die Wirkung unterschiedlicher

²⁶⁷ Eine Grundlage der folgenden Ausführungen ist eine Studie, die Anfang 2003 von Fischer, Leperhoff, Volst für das BSI erstellt wurde; vgl. <http://www.bsi.bund.de/literat/studien/iness/index.htm>.

²⁶⁸ INESS bildet die Zeit durch Zeitschritte ab, die keine feste realzeitliche Zuordnung haben. Weil die Analyse die langfristigen Störungsauswirkungen, aber nicht ihren Zeitverlauf betrachtet, ist es für die Bestimmung des Schadens unerheblich, wie lange eine solche Störung in Wirklichkeit dauert.

Auslastungen des Internets auf den Verlust von Regierungspaketen zu analysieren: Gerechnet wurde der Normalfall der Paketproduktion (100 Prozent), ihre Verdoppelung, um zu sehen, welche Auswirkungen eine maximale Auslastung der Netzkapazitäten hat, sowie eine Erhöhung um 50 Prozent, um abzuschätzen, ob die Auswirkungen stetig mit der Verkehrserhöhung zunehmen oder nur abrupt im Bereich des Maximalen (Verdoppelung) ansteigen.

Da es keine öffentlich zugängliche Quelle gibt, die das gesamte Internet beschreibt, wurden für die Simulation Daten über die Netzstruktur und -kapazitäten von Telegeography genutzt [Telegeography, 2004, 2003 2002a, 2002b, 2001a, 2001b]. Das in der Simulation genutzte Netz besteht aus 527 Backbones und aus 185 IX. Die Kapazitäten der Backbones wurden wegen fehlender Daten zum Teil geschätzt: Die geringste Kapazität beträgt 155 MBit/s, die größte 140.698 MBit/s. 24 Backbones haben weniger als 1000 MBit/s, während fünf mehr als 100.000 MBit/s Kapazität aufweisen. 56 Prozent der Backbones transportieren zwischen 1001 MBit/s und 10.000 MBit/s. In diesem Bereich liegt der Schwerpunkt. Da Angaben über die Kapazitäten von IX in der Regel fehlen, wurde für die Simulation angenommen, dass sie etwas über der Summe der Kapazitäten liegen, die alle Backbones aufweisen, die über den jeweiligen IX verbunden sind. Alle diese Daten können nur in einer ersten Näherung plausibel sein und sollen der Simulation als Futter dienen, damit sie ihre Funktionsfähigkeit beweisen kann. INESS kann andere Datensätze, seien sie abgeleitet oder empirisch erhoben, jederzeit verarbeiten.

Gerechnet wurden drei Basiszenarien ohne Störungen: Erstens, das Basisexperiment. Hier arbeitet INESS nur mit dem Hintergrundrauschen. Modellbedingt ergeben sich hier minimale Paketverluste. Dieses Szenario ist Voraussetzung dafür, den Einfluss der Regierungskommunikation auf die Auslastung des Internets und den Paketverlust abzuschätzen. Zweitens, ein Basisexperiment der Regierungskommunikation in der Bandbreite. Drittens, ein Basisexperiment mit verteilter Regierungskommunikation. Diese beiden Läufe definieren für die jeweilige Kommunikationsform der Regierung (Bandbreite, verteilt) eine Nulllinie, an der ein Paketverlust gemessen wird, der sich als Folge der Störungsszenarien ergibt.

Die im Modell verwendeten Szenarien der strategischen Störungen sind: Erstens, Störungen von IX. Sie werden im Modell extern vorgegeben - als Störung der wichtigsten IX in Europa, nämlich der (im Modell) aggregierten IX Frankfurt, London und Paris. Dabei wurden die Störungen für jeden einzelnen IX simuliert, nicht aber

zugleich für zwei oder für alle drei IX. Mehr als einen solchen IX zur selben Zeit zu stören erscheint im Kontext eines Szenarios, das Terrorismus gegen den Cyberspace unterstellt, als sehr unwahrscheinlich. Denn im Modell ist ein IX ein künstliches Aggregat aus verschiedenen IX in einer Stadt, die in der Realität von diversen Unternehmen an unterschiedlichen Standorten betrieben werden und die alle zugleich ausgeschaltet werden müssten.²⁶⁹ Zweitens, für weitere Simulationsrechnungen werden bis zu fünf europäische bzw. fünf deutsche Backbones²⁷⁰ (wiederum aggregiert) gleichzeitig gestört, die den meisten Paketverkehr transportierten (Hintergrundrauschen und Regierungskommunikation zusammen). INESS wählt diese Backbones selbst aus und greift dabei immer auf den Kabelstrang zurück, der im vorhergehenden Zeitschritt die meisten Pakete transportierte. Analog zu dem Argument bei den IX ist die Störung von fünf Backbones das Maximum dessen, was uns im Kontext terroristischer Szenarien als plausibel erschien.

Ergebnisse der Simulationen

Störungen wirken sich in INESS auf den Transport von Paketen aus, und sie können auf zweierlei Weise zum Ausdruck kommen:

Erstens, als Paketverlust, der sich aus der Anzahl an unzustellbaren Paketen, dem Transportpaketverlust und dem Pufferverlust zusammensetzt. Die Anzahl an unzustellbaren Paketen gibt an, wie viele Pakete verloren gehen, weil z. B. kein Weg bekannt oder kein freier Backbone zum Ziel vorhanden ist. Der Transportpaketverlust beschreibt, wie viele Pakete vernichtet worden sind, weil die Verarbeitungskapazität eines IX aufgebraucht ist. Pufferverlust tritt auf, wenn der TCP-Puffer voll ist, weil mehr Pakete produziert als ausgeliefert werden. Einen Überblick über das Schicksal der Regierungspakete gewährleistet der Gesamtschaden. Er bezeichnet die Summe aller Schadenspunkte,²⁷¹ die den Regierungspaketen zugewiesen und die im Netz vernichtet wurden. Zusätzlich wird die Kommunikationsmatrix der Regierung untersucht, die angibt, wie viele Pakete zwischen den Regierungsakteuren an den IX er-

²⁶⁹ Solche IX in unserem Modell haben können verglichen werden mit Collocation Centers oder Carrier Hotels.

²⁷⁰ Von deutschen Backbones ist die rede, wenn sie unmittelbar zwei IX in Deutschland verbinden.

²⁷¹ Im Modus Bandbreite erhält jedes Regierungspaket einen Schadenspunkt; im Modus verteilt werden E-mail drei, WWW zwei und Videokonferenzen ein Schadenspunkt zugeordnet.

folgreich versandt wurden. Damit können lokale Beeinträchtigungen in den Beziehungen zwischen IX aufgespürt werden.²⁷²

Zweitens, als Laufzeitverlängerung. Eine Verlängerung der Transportdauer der Datenpakete kann für Echtzeitanwendungen wie Videokonferenzen u. U. kritisch sein, während sie für E-Mail, WWW etc. wenig bedeutsam ist, da sie im Bereich von Millisekunden und Sekunden liegen. Längere Wege bedeuten in INESS, dass Pakete über mehr IX geführt werden, d. h. die Anzahl der HOP²⁷³ erhöht sich. INESS bildet die Paketlaufzeiten aber nur grob ab, weil von physikalischen Eigenschaften der Übertragungsmedien abstrahiert wird.

Analyse der Basisexperimente

Zwei Arten von Kommunikation simuliert INESS: die Kommunikation der Regierung und das Hintergrundrauschen. Jeder IX erzeugt Pakete dieses Rauschens und empfängt sie, und einige von ihnen produzieren bzw. erhalten zusätzlich die Pakete der Regierungskommunikation. In den Läufen des Simulationsexperimentes Hintergrundrauschen (Basisszenario) werden zusammen gut 4,5 Millionen Pakete erzeugt. Mit dem Modus verteilte Regierungskommunikation werden kaum mehr Pakete produziert, d. h. die Produktion der Regierungspakete fällt hier nicht ins Gewicht. Der Modus Bandbreite der Regierungskommunikation steigert die Produktion der Pakete dagegen um 40 Prozent gegenüber dem Basisszenario auf dann etwa mehr als 6.4 Millionen Pakete. Die zusätzlich erzeugten Regierungspakete verändern den Produktionsschwerpunkt aller Pakete: Er wandert nach Deutschland, da dort die Regierungspakete an den einschlägigen IX entstehen, die mit Regierungsbehörden bestückt sind. Mit diesen zusätzlichen Paketen steigt die Belastung der Backbones generell und speziell in Deutschland: Die mittlere Auslastung aller Backbones wächst durch die Regierungskommunikation im Modus Bandbreite von 8,5 auf 9,3 Prozent, ein freilich noch immer bescheidener Wert. *Abbildung 3* zeigt die weltweite Auslastung der Backbones. Die roten Linien zeigen Backbones, die (in beide Richtungen zusammen) über ca. 70 Prozent ausgelastet sind und meist an die Ränder des Netzwerkes zu Regionen bzw. Länder führen, die einen recht hohen Paketverkehr des Hintergrundrauschens produzieren, aber im Simulationsmodell sehr wahrschein-

²⁷² Genutzt wird der Mann-Whitney-U-Test, der trotz Zufallsschwankungen in der Paketproduktion statistisch signifikante Unterschiede im Paketverlust etc. diagnostizieren kann. Als Signifikanzniveau werden die in der Literatur üblichen 5 Prozent verwendet.

²⁷³ Die Länge eines Pfades zwischen Sender und Empfänger eines Paketes, gemessen an der Zahl der IX (Router).

lich mit weniger Backbones angebunden sind, als das in Wirklichkeit der Fall ist - Angaben zu ihnen lagen für unsere Simulation nicht vor. Daher gehen wir davon aus, dass diese hohen Auslastungen an diesen Rändern des Internets Modellartefakte sind. Da aber der Schwerpunkt der Analysen auf dem innereuropäischen, speziell deutschen, sowie auf dem transatlantischen Paketverkehr liegt, sind die Auswirkungen dieser randständigen hohen Netzauslastung auf die Simulation gering. Die *Abbildungen 4* und *5* bestätigen das: Sie zeigen die Auslastung der Backbones in Europa bzw. in Deutschland, die sich deutlich entspannter darstellt. Stark ausgelastet sind hier nur wenige Backbones, die, was in den Abbildungen nicht gezeigt wird, relativ geringere Kapazitäten aufweisen.

Im Simulationsexperiment Basis Bandbreite wurden gut 400.00 Transportvorgänge von Regierungspaketen über 221 von 527 Backbones registriert. Die meisten Regierungspakete werden innerhalb Deutschlands transportiert, wo sich die Regierungsakteure konzentrieren. *Abbildung 6* zeigt diese Struktur, wobei die Dicke der Striche die

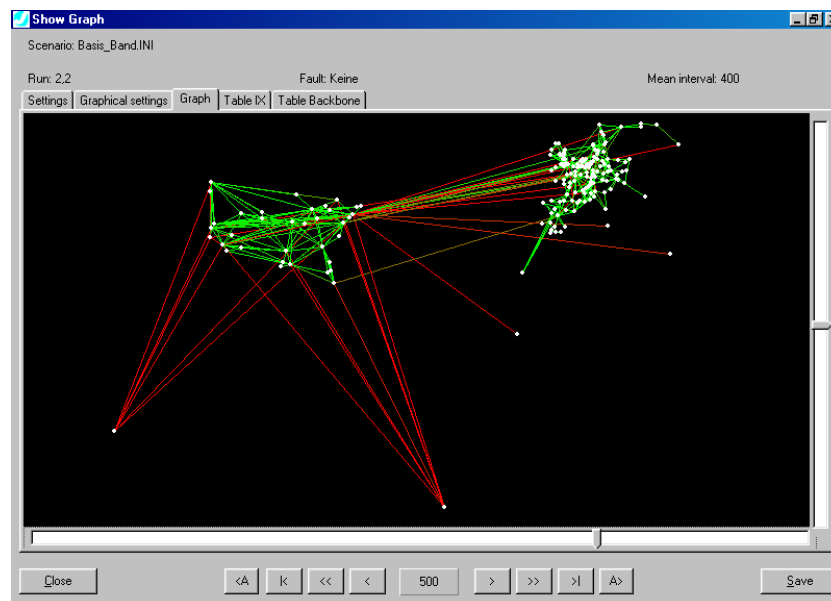


Abbildung 3: In der Beobachtungsphase gemittelte Auslastung der Backbones weltweit (Basis Bandbreite, Paketproduktion 100 %)

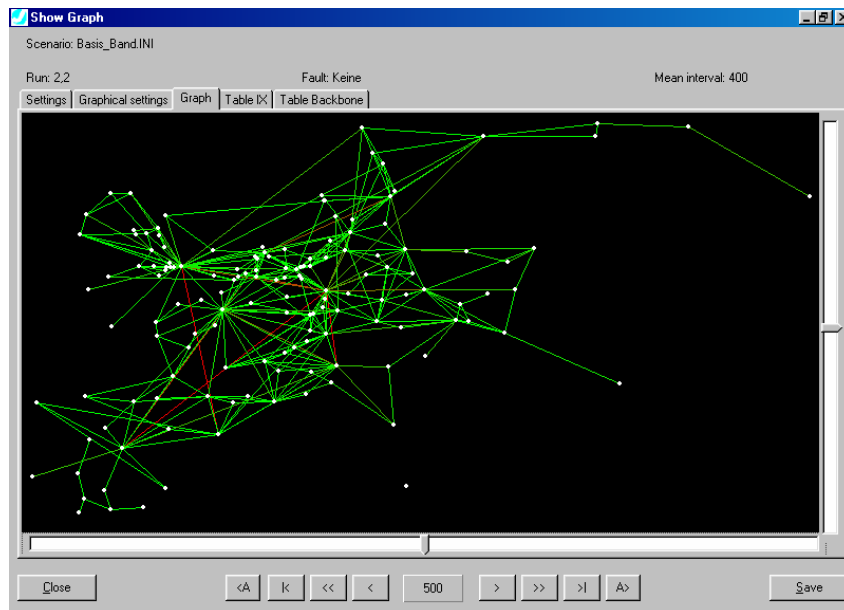


Abbildung 4: In der Beobachtungsphase gemittelte Auslastung der Backbones in Europa (Basis Bandbreite, Paketproduktion 100 %)

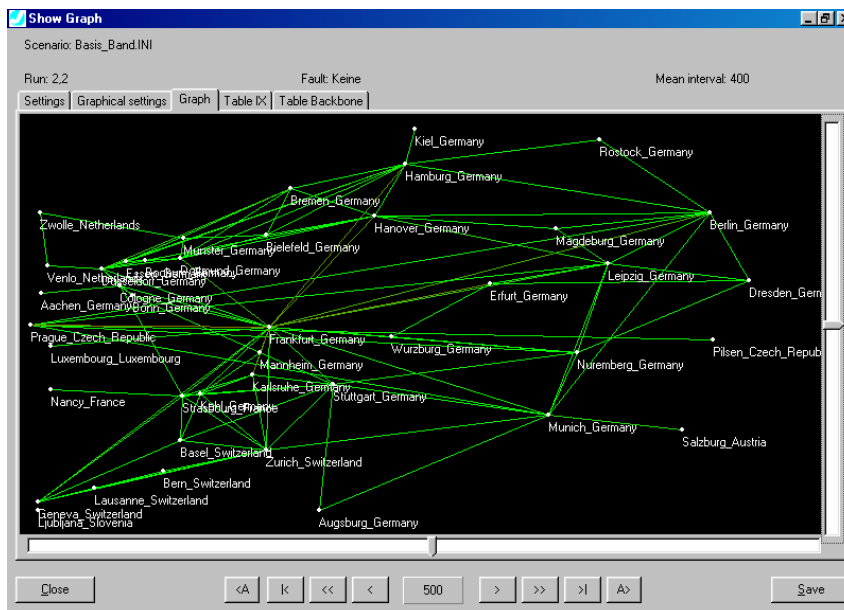


Abbildung 5: In der Beobachtungsphase gemittelte Auslastung der Backbones in Deutschland und Umgebung (Basis Bandbreite, Paketproduktion 100 %)

Menge der transportierten Regierungspakete zeigt. Insgesamt werden knapp 217 000 Transportvorgänge von Regierungspaketen (knapp 54 Prozent aller Regierungspakete) innerhalb von Deutschland registriert, die von 57 der 76 Backbones übertragen werden. Innerhalb von Europa (ohne Deutschland) sind es 128 000 Transportvorgänge (32 Prozent der Regierungspakete), und auf die restliche Welt entfallen 60.125 (15 Prozent). Der internationale Anteil der Regierungskommunikation wird über 128 von 308 Backbones des innereuropäischen Internets (*Abbildung 7*) und über 36 von 143 außereuropäische Backbones (*Abbildung 8*) geführt. Außerhalb von Europa sind die transatlantischen Backbones bedeutend, die New York und Washington mit ihren wichtigen Institutionen anbinden und als alternative Routen bei Störungen in Europa dienen.

Ein Vergleich der Läufe des Hintergrundrauschens mit den Läufen von Basis Bandbreite zeigt, dass es zu einem Paketverlust der Regierungskommunikation schon ohne strategische Störungen kommt, die Verluste jedoch an den Rändern des Netzwer-

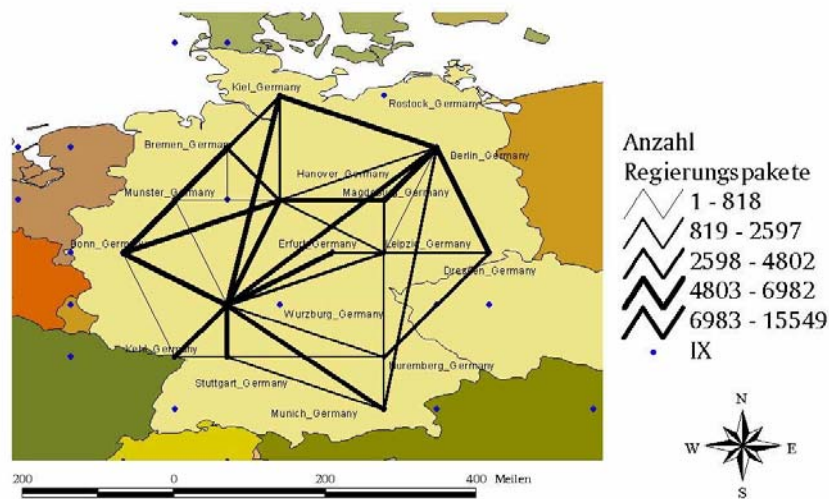


Abbildung 6: Backbones in Deutschland mit Regierungspaketen. IX ohne Kontakt mit Regierungspaketen sind als Punkt zu sehen.

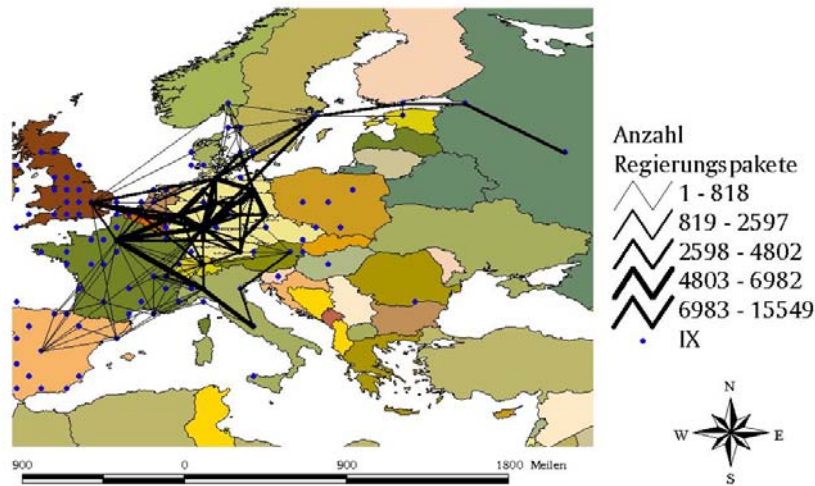


Abbildung 7: Backbones in Europa mit Regierungspakete.

kes anfallen. Diese Engpässe dürften der hohen Auslastung des simulierten Backbone-netzes geschuldet und sicherlich Artefakte sein. Jedoch ist in nur 29 Fällen die Abweichung von der erwarteten Paketmenge signifikant für das Niveau von 5 Prozent nach dem Mann-Whitney-U-Test.

Strategische Störungen von IX

Für das Simulationsexperiment werden entweder der aggregierte IX Frankfurt, London oder Paris gestört. Der dabei entstehende Paketverlust wird über die Anzahl an unzustellbaren Paketen, den Transportpaketverlust sowie den Pufferverlust gemessen, der in den Läufen aber erst dann auftritt, wenn das Hintergrundrauschen erhöht wird.

Diese Messgrößen beschreiben den Gesamtzustand des Netzes. Daraus ergeben sich noch keine Aussagen über die Regierungskommunikation. Sie sind erst möglich, wenn der Gesamtschaden ermittelt ist, der sich explizit auf die Regierungskommunikation bezieht und einen Überblick über die vernichteten Regierungspakete gibt. Im Modus Bandbreite ist der Gesamtschaden gleich der Anzahl an vernichteten Regierungspaketen, da sie nur mit einem Dienst vertreten sind, dem ein Schadenspunkt zugewiesen wurde. Hingegen ist im Modus verteilt der Gesamtschaden gleich der

Summe der Schadenspunkte der vernichteten Pakete, die mehrere Dienste mit unterschiedlichen Schadenspunkten repräsentieren.

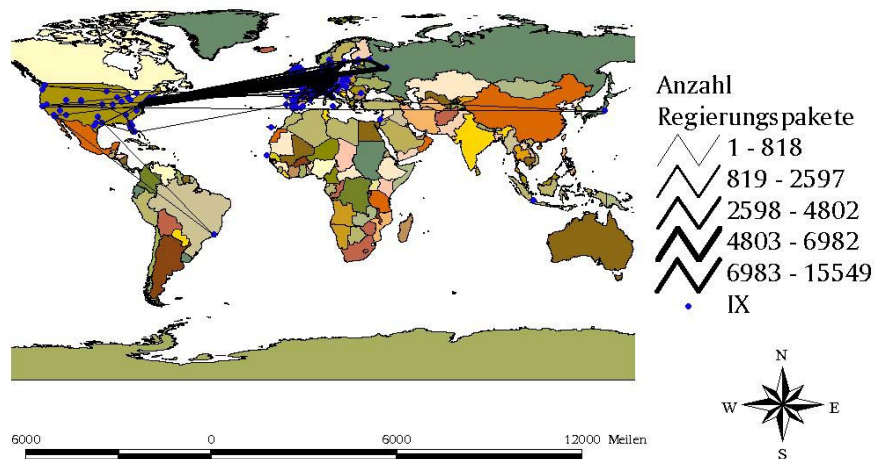


Abbildung 8: Backbones weltweit mit Regierungspaketen.

Am Beispiel der Störung des IX Frankfurt im Modus Bandbreite soll gezeigt werden, welche generellen Effekte bei einer Störung auftreten. *Abbildung 9* zeigt für einen Lauf des Simulationsexperimentes, wie sich der Transportpaketverlust und die Anzahl an unzustellbaren Paketen zusammengenommen sowie das Routing verändern. Es zeigt sich, dass der Paketverlust in die Höhe schnell. Die Ursache liegt im Transportpaketverlust, denn weiterhin schicken die benachbarten IX Datenpakete nach Frankfurt, die von INESS bei ihrer Ankunft sofort vernichtet werden, da IX Frankfurt als nicht mehr existent definiert ist. *Abbildung 10* weist den Transportpaketverlust aus. Dass weiterhin Pakete nach Frankfurt gehen hat seinen Grund darin, dass eine Anpassung des Routing erst mit einer zeitlichen Verzögerung erfolgt. Wegen der zentralen Lage der Stadt im Backbonenetz verbreiten sich aber die Löschungen des Weges nach Frankfurt sehr schnell und es werden aktuelle Routinginformationen (Updates) weitergegeben, in denen neue Routen für die gelöschte Route vorgeschlagen werden. Sobald sich die Störung von Frankfurt in den Routingtabellen niedergeschlagen hat, sinkt der Transportpaketverlust, da weniger Pakete nach dem

nicht mehr existenten IX Frankfurt gesandt werden. Dafür steigt die Anzahl an unzustellbaren Paketen an. Die Ursachen, warum diese Pakete nicht zustellbar sind, ändern sich im Zuge der Aktualisierung des Routing (*Abbildung 11*): Fehlende Pfade nehmen als Ursache ab und die Zahl blockierter Backbones nimmt zu. Denn mit dem Update werden neue Pfade bekannt, aber die Pakete, die nun verstärkt über sie strömenden, blockieren die Backbones öfter.

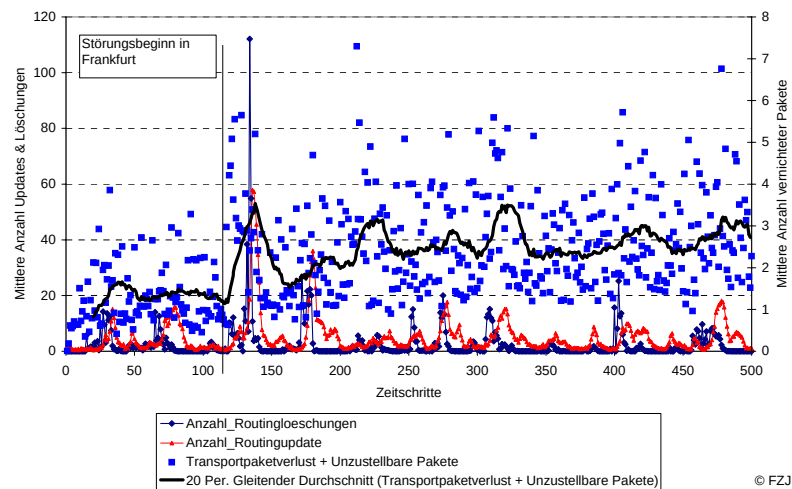


Abbildung 9: Verlauf des mittleren Paketverlustes und der mittleren Routinganpassung im Simulationsexperiment Störung IX Frankfurt Modus Bandbreite. Die Werte sind über alle IX gemittelt. (Paketproduktion Hintergrundrauschen 100 %).

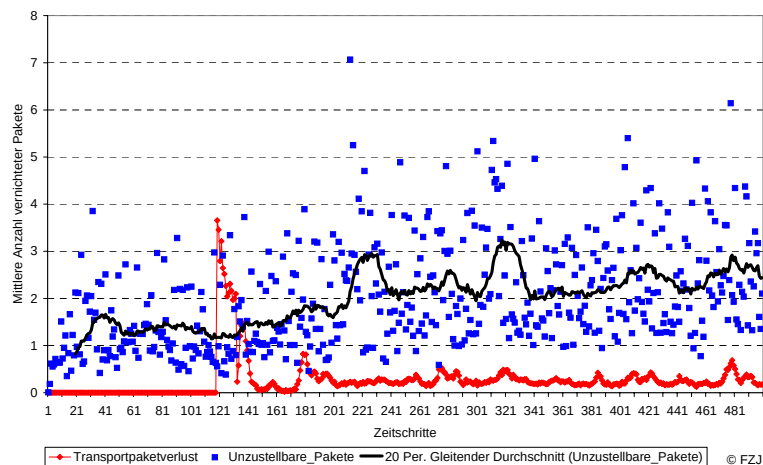


Abbildung 10: Verlauf des mittleren Transportpaketverlustes und der mittleren Anzahl an unzustellbaren Paketen bei Störung des IX Frankfurt im Modus Bandbreite (Paketproduktion Hintergrundrauschen 100 %).

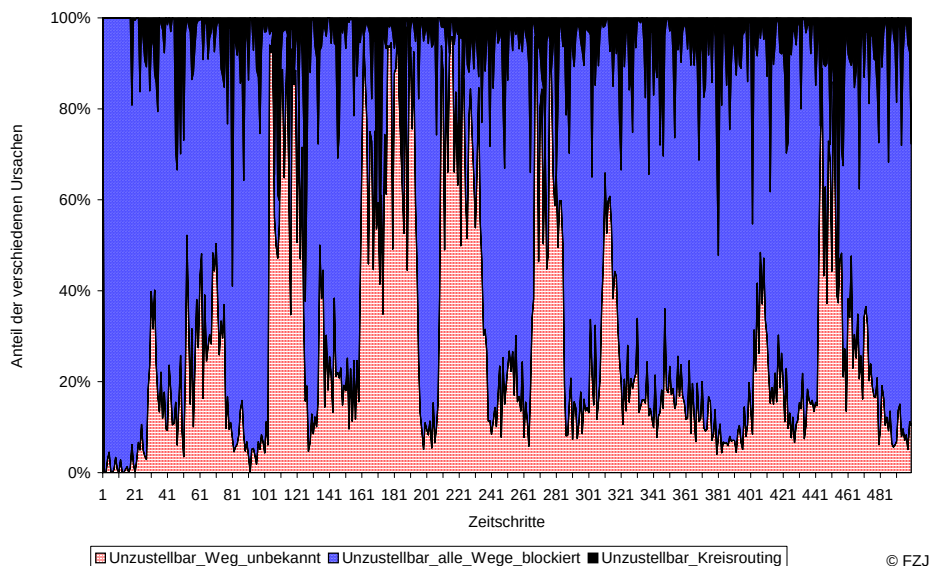


Abbildung 11: Verlauf der Zusammensetzung der mittleren Anzahl an unzustellbaren Paketen bei Störung des IX Frankfurt im Modus Bandbreite (Paketproduktion Hintergrundrauschen 100 %); unzustellbarer Weg = kein Weg zum Ziel bekannt; unzustellbar alle Wege blockiert = Wege bekannt, aber blockiert.

Nun wird der Gesamtpaketverlust analysiert, um einen Eindruck von den Auswirkungen auf das Gesamtnetz zu bekommen. Dazu werden die Folgen der Störungen in den IX Frankfurt, London und Paris verglichen. Außerdem wird der Gesamtschaden für die Regierungspakete ermittelt.

Analysiert wird, ob es, bezogen auf das Basisszenario (Basis Bandbreite), bei Störungen der IX überhaupt zu einem signifikant erhöhten Paketverlust kommt. In der Beobachtungsphase vernichteten alle IX bei einer Störung des IX Frankfurt (im Modus Bandbreite) zusammen gut 1,4 Millionen Pakete²⁷⁴, bei einer Störung des IX London (Bandbreite) fast 1.63 Millionen Pakete und bei einer Störung des IX Paris (Bandbreite) 1.44 Millionen Pakete. Zum Vergleich: Die Anzahl an unzustellbaren Paketen plus der Transportpaketverlust lag im Szenario Basis Bandbreite, d.h. ohne Störungen, bei 1.2 Millionen Paketen. Die Erhöhung des Paketverlustes, die erhöhte Anzahl an unzustellbaren Paketen und der Transportpaketverlust sind signifikant, bezogen auf das Basisszenario.

²⁷⁴ Transportpaketverlust und Anzahl an unzustellbaren Paketen zusammengekommen.

Der Gesamtschaden steigt bei den Störungen deutlich an: *Abbildung 12* zeigt den summierten Gesamtschaden für die IX-Störungen, verglichen mit dem Basisszenario. Die Schadenszunahme ist jeweils signifikant. Ein Vergleich zeigt, dass die Störung

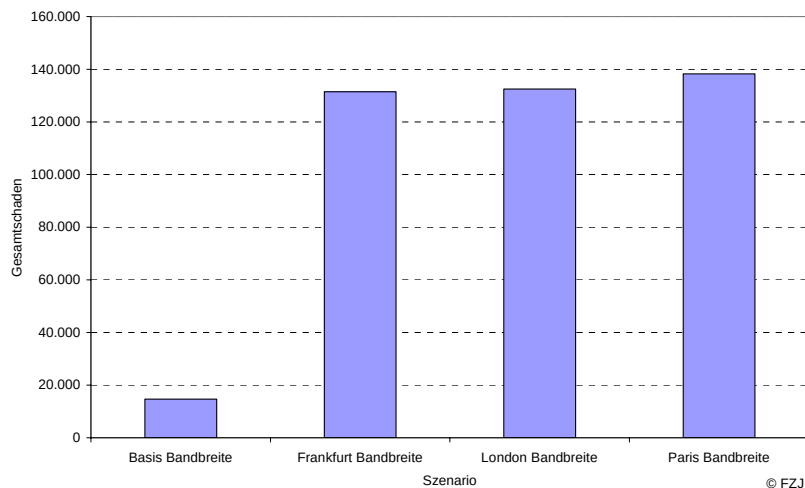


Abbildung 12: Summierter Gesamtschaden bei unterschiedlichen IX-Störungen.

des IX Frankfurt und des IX London einen ähnlichen Gesamtschaden bringen. Paris ragt hervor: Hier zeigt die Auswertung, dass die Erhöhung des Gesamtschadens im Vergleich zu dem Ausfall des IX London mit 0,011 und zu dem IX Frankfurt mit 0,003 signifikant höher ist. Generell ist bei den Störungen der IX jedoch zu bedenken, dass die hohen Schadenspunkte, die *Abbildung 12* ausweist, z. T. dadurch zustande kommen, dass mit der Störung von IX die dort produzierten Regierungspakete nicht abtransportiert werden und so verloren gehen.

Nun soll die Kommunikation im Regierungsnetz, also die Beziehungen der Akteure untereinander, detaillierter untersucht werden.

Bei der Auswertung der Basisszenarien wurde ermittelt, dass 29 Beziehungen der Regierungskommunikation schon im Basisszenario Basis Bandbreite ohne Störungen signifikant beeinträchtigt sind. Diesen Auswirkungen auf die Regierungskommunikation, die datenimmanent sind, stehen diejenigen gegenüber, die durch Störungen der IX hervorgerufen werden. So beeinträchtigt eine Störung des IX London 61 Beziehungen der Regierungskommunikation (ohne die Regierungskommunikation von und nach London, die qua Definition mit der Störung ausfällt), davon 20 signifikant.

Wird der IX Paris gestört, werden 83 Beziehungen (ohne Regierungskommunikation von und nach Paris) beeinträchtigt, davon 52 signifikant. Eine Störung des IX Frankfurt betrifft mehr Beziehungen der Regierungskommunikation, da deren Wege oft über Frankfurt führen: Sie beeinträchtigt 89 Beziehungen (ohne Regierungskommunikation von und nach Frankfurt), davon 26 signifikant. *Tabelle 1* stellt diese signifikanten Beeinträchtigungen zusammen. Dabei ist zu beachten, dass die in der Spalte Basis Bandbreite markierten beeinträchtigten Beziehungen zu den Artefakten zählen. Sie wurden nur aus systematischen Gründen verzeichnet, sind aber nicht der Störung, sondern den Daten geschuldet und deshalb mit einem A für Artefakt versehen. Jedoch zeigt Tabelle 1, dass bei IX-Ausfällen diese artifiziellen Störungen in einigen Fällen nicht mehr auftreten. Dieser Effekt ist eine Folge der Entlastung des Netzes durch Vernichtung von Paketen. Wie die Tabelle zeigt, sind bei einem Ausfall des IX Frankfurt sechs Beziehungen signifikant beeinträchtigt. Davon entfällt nur eine auf eine innerdeutsche Beziehung. Von den drei beeinträchtigten Beziehungen mit Moskau sind zwei schon im Simulationsexperiment Basis Bandbreite gestört und fallen damit aus der Betrachtung heraus. Insgesamt bleiben beim Ausfall des IX Frankfurt, gemessen an der wichtigen topologischen Stellung, die diese Stadt innerhalb von Europa und Deutschland einnimmt, die Beeinträchtigungen erstaunlich gering. Bemerkenswert ist, dass die Störung des IX London keine Beziehung signifikant beeinträchtigt, sofern sie nicht direkt von dort ausgeht oder nach London führt. Durch den Ausfall des IX London wurden jedoch einige Beziehungen entlastet, da Paketverlust und Routing einige Strecken entlasten. Überraschend ist das Ergebnis für die Störung des IX Paris: Im Vergleich zu allen betrachteten Störungen tritt die größte Anzahl signifikant beeinträchtigter Beziehungen auf, nämlich 32. Der Schwerpunkt mit 29 signifikant beeinträchtigten Beziehungen entfällt auf Rom. Damit sind von den 42 möglichen Beziehungen von und nach Rom 29 signifikant beeinträchtigt. Darunter ist auch die wichtige Beziehung Rom-Berlin, die in beiden Richtungen gestört ist. Damit zeigt sich, dass sich die Auswirkungen von Störungen nicht nur auf nahe, sondern auch auf entfernte IX erstrecken. Das ist aus einer rein topologischen Perspektive, also der Anordnung von IX und Backbones, nicht ersichtlich. Rom ist kein genereller Flaschenhals, da die Erreichbarkeit dieses IX in den beiden anderen Störungsszenarien (Frankfurt und London) kaum beeinträchtigt ist.

Kommt es zu einem Ausfall des IX Frankfurt, nehmen die Regierungspakete neue

Beziehung	Basis Bandbreite	Störung IX FF Bandbreite	Störung IX LO Bandbreite	Störung IX PA Bandbreite
Bonn Germany -> Rome Italy				A
Bremen Germany -> Rome Italy				A
Karlsruhe Germany -> New York City US				
Kiel Germany -> Karlsruhe Germany				
Kiel Germany -> Rome Italy				
London UK -> Hanover Germany			*	
Magdeburg Germany -> Rome Italy				A
Moscow Russia -> Hanover Germany		A		
Moscow Russia -> Karlsruhe Germany				
Moscow Russia -> Magdeburg Germany				
Moscow Russia -> Rome Italy		A		A
Munich Germany -> New York City US				
Rome Italy <-> Berlin Germany				
Rome Italy -> Bonn Germany				
Rome Italy -> Bremen Germany				
Rome Italy <-> Cologne Germany				
Rome Italy <-> Dusseldorf Germany				
Rome Italy <-> Erfurt Germany				
Rome Italy <-> Frankfurt Germany				
Rome Italy <-> Hamburg Germany				
Rome Italy <-> Hanover Germany				
Rome Italy -> Kiel Germany				
Rome Italy <-> London UK				
Rome Italy -> Magdeburg Germany				
Rome Italy -> Kiel Germany				
Rome Italy <-> New York City US				
Rome Italy <-> Washington DC US				
Stuttgart Germany -> New York City US				
Stuttgart Germany -> Rome Italy				

Tabelle 1: Vergleich der signifikant beeinträchtigten Beziehungen in der Regierungskommunikation bei Störungen der IX Frankfurt, London und Paris im Modus Basis Bandbreite, Hintergrundrauschen 100 Prozent. Beeinträchtigungen sind dunkelgrau. < - > bezeichnet Beeinträchtigung in beide, -> in eine Richtung. A verweist darauf, dass die Beeinträchtigung schon in Basis Bandbreite auftrat. *Durch die Störung im IX London wird die Verbindung London - Hannover qua Definition unterbrochen.

Wege. *Abbildung 13* zeigt diese Wege für Europa und *Abbildung 14* für Deutschland. Da um Frankfurt ein Backbonering liegt, der Redundanz erhöht, erreichen die inner-deutschen Regierungspakete meistens über Umwege ihr Ziel. Das vermaschte Netzwerk in Deutschland spielt hier seine Möglichkeiten aus.

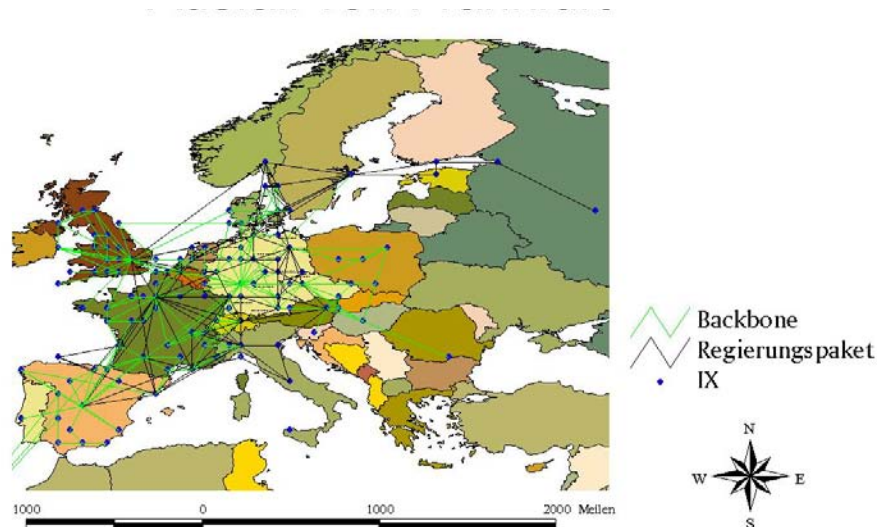


Abbildung 13: Wege der Regierungskommunikation innerhalb von Europa beim Ausfall des IX Frankfurt, Modus Bandbreite, Paketproduktion 100 %.

Die Folgen eines Ausfalls des IX London unterscheiden sich von denen, die in Frankfurt zu beobachten sind: Da London für Großbritannien ein zentraler Punkt der Anbindung an das weltweite Backbonenetz ist, ergeben sich bei seinem Ausfall einige Probleme. Die Folgen eines Ausfalls des IX Paris liegen zwischen denen Frankfurts und Londons: Da Frankreich nicht ganz so vernetzt ist wie Deutschland, aber Paris nicht in gleicher Weise wie der IX London der zentrale Anbindungspunkt ist, liegen die Auswirkungen zwischen den beiden Extremen. Teile Frankreichs werden bei einer Störung beeinträchtigt, und auch der innereuropäische Datenverkehr leidet. Stark beeinträchtigt ist die Erreichbarkeit Roms. Dies hat seine Ursache darin, dass bei einem Ausfall des IX Paris der Verkehr in den Süden und Südosten Frankreichs gelenkt wird, um Paris zu umgehen. Dort ist Rom angebunden, so dass erhöhter Paketverkehr zu steigenden Paketverlusten führt.

Zwar nimmt bei diesen drei Szenarien auch die Anzahl vernichteter Regierungspakete zu, aber der Gesamtschaden steigt deutlich geringer an. Denn Regierungspakete werden von gut angebundenen IX produziert und empfangen. Sie weisen meist verschiedene alternative Pfade zueinander auf, die über genügend Kapazitäten verfügen, um auch bei Störungen von IX und einer steigenden Paketzahl noch relativ gut zu funktionieren. Der Paketverlust tritt also nicht auf den Hauptwegen der Regierungspakete auf, so dass der Paketverlust viel häufiger Pakete des Hintergrundtra-

schens, weniger aber Regierungspakete trifft. Die IX-Störungen reduzieren den verkehrsbedingten Anstieg des Gesamtschadens. Denn durch die Störung gehen Pake-

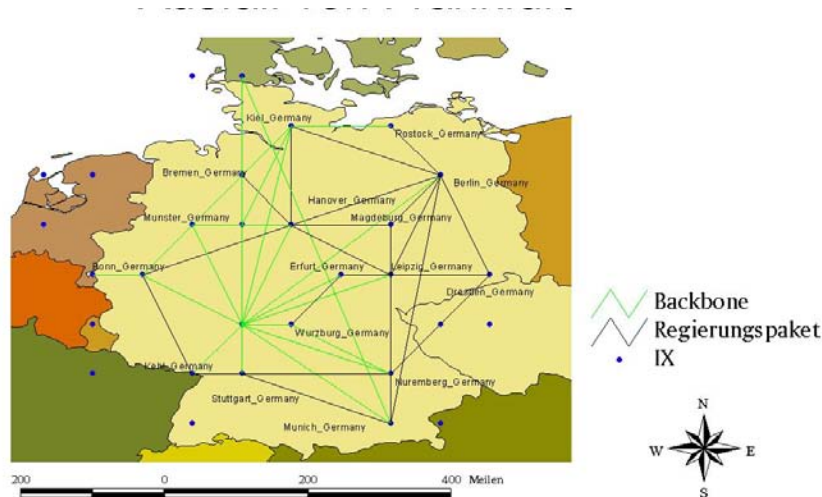


Abbildung 14: Wege der Regierungskommunikation in Deutschland beim Ausfall des IX Frankfurt, Modus Bandbreite, Paketproduktion 100 %.

te des Hintergrundrauschens verloren und die Netzteile, über die die meisten Pakete der Regierungskommunikation laufen, werden entlastet. Insbesondere bei einer Störung im IX London fällt der Anstieg des Gesamtschadens niedriger aus. Hier tritt der Effekt besonders deutlich auf, dass es bei Störungen der IX zu einer Entlastung des Backbonnetzes kommen kann, da viele Pakete des Hintergrundrauschens vernichtet werden.

In den bisherigen Simulationsexperimenten wurde untersucht, wie sich Störungen der Regierungskommunikation auswirken, die über eine Bandbreite erfolgt. Nun wird der zweite Modus der Regierungskommunikation untersucht, der einer verteilten Zeit. In diesem Modus schwankt die Anzahl an gesendeten Paketen über die Zeit, da ein zeitlich variables Kommunikationsverhalten abgebildet wird. Insgesamt werden, verglichen mit Bandbreite, im Modus verteilt wesentlich weniger Regierungspakete erzeugt. Wiederum steht die strategische Störung der IX Frankfurt, London und Paris im Zentrum, auch bei steigender Produktion der Hintergrundpakete.

In diesem Fall nimmt die Anzahl vernichteter Pakete zu, d.h. der Paketverlust steigt. Jedoch sind davon fast nur Pakete des Hintergrundrauschens betroffen. Im Vergleich zum Basisszenario verteilt, das ohne Störungen gerechnet wird, ist der Paketverlust

bei jeder Störung eines IX signifikant erhöht. Die höchste Anzahl vernichteter Pakete entsteht wiederum, wenn der IX London gestört ist.

Die Regierungskommunikation ist in diesem Simulationslauf deutlich weniger betroffen. Zwar werden mehr Pakete des Hintergrundrauschens produziert, aber im Modus verteilt sind weniger Regierungspakete unterwegs, wodurch die Gesamtbelastung des Netzes sinkt. Diese Entlastung betrifft insbesondere das innereuropäische Netz, in dem bevorzugt die Pakete der Regierungskommunikation unterwegs sind. Zudem werden die Regierungspakete zu unterschiedlichen Zeitpunkten produziert, so dass nur ein Teil von ihnen in der verlustreichen Zeit direkt nach der Störung unterwegs ist, in der das Routing erst zu wirken beginnt. Einige sind bereits vor der Störung angekommen und andere werden erst deutlich nach der Störung erzeugt, wenn sich der Transport durch die Aktualisierung des Routing wieder stabilisiert hat. Alle diese Effekte verhindern einen hohen Verlust an Regierungspaketen, wodurch der Gesamtschaden gering bleibt. Auch sind in diesem verteilten Modus signifikante Beeinträchtigungen in Beziehungen zwischen IX im Vergleich zum Modus Bandbreite deutlich seltener. Das Internet wird mit diesen Störungen, sind doch weniger Datenpakete unterwegs, die IX und Backbones überlasten, deutlich leichter fertig.

Strategische Störung von Backbones

INESS untersuchte, ob bereits eine Störungen von wenigen Backbones zu einer signifikanten Beeinträchtigung der Regierungskommunikation führt. Im ersten Szenario Backbone Bandbreite Europäisch wurden innereuropäische und im zweiten Szenario Backbone Bandbreite Deutsch nur innerdeutsche Backbones gestört. Die Regierungskommunikation wurde im intensiven Modus Bandbreite betrieben.

Die Simulationsläufe zeigten, dass in keinem Fall mit fünf Backbones eine gesetzte Schadensschwelle²⁷⁵ erreicht wird. Daher wird die Regierungskommunikation im Modus Bandbreite nur marginal beeinflusst durch dieses - von seinen impliziten Annahmen her - recht weitgehende Angriffsszenario: Fünf Backbones koordiniert über Europa bzw. Deutschland zu (zer)stören, wäre für Terrorismus gegen den Cyberspace sehr anspruchsvoll. Auch ergibt eine Erhöhung der Paketproduktion auf 200 Prozent kein anderes Bild. Da schon in diesem Modus mit starker Regierungskommunikation kein nennenswerter Gesamtschaden auftritt, wurde der Modus verteilt mit seinen wenigen Regierungspaketen nicht simuliert.

²⁷⁵ Die Schadensschwelle gibt einen Wert an für den in allen IX aufgelaufenen Schaden geteilt durch die Anzahl an IX und Backbones.

Als Fazit ist festzuhalten, dass mit dem hier verwendeten Verfahren die fünf Backbones nicht gefunden wurden, deren Störung die Regierungskommunikation signifikant belasten.

Internetresilienz - ein differenziertes Bild

Die Auswertung der Simulationsläufe zeigt, dass das Internet grundsätzlich eine hohe Resilienz auch bei strategischen Angriffen aufweist. Auch eine Verdoppelung der Paketproduktion verändert das Bild nicht qualitativ. INESS konnte zeigen, dass die Zerstörung von bis zu fünf der zentralen europäischen bzw. deutschen Backbones keine Erfolg versprechende Angriffsoption ist, die sehr schwere Netzstörungen nach sich zieht. Mit unserem Verfahren und unter den simulierten Bedingungen wurden nicht jene fünf Backbones gefunden, deren gemeinsame Störung die Regierungskommunikation belasten würde. Zwar ist nicht ausgeschlossen, dass mit einem modifizierten Verfahren eine Relativierung der Ergebnisse zustande kommen könnte, jedoch sprechen die Simulationen dafür, dass das Backbonenetz in Deutschland und in großen Teilen Europas hinlänglich vermascht und damit resilient ist, um auch mit strategischen Störungen der Backbones fertig zu werden. Backbones zu stören mag aber dann einen Sinn machen und durchaus gefährlich sein, wenn damit Akteure abgeschnitten werden sollen, die in Netzteilen mit geringer oder fehlender Vermaschung lokalisiert sind, in denen auch noch steigender Paketverkehr zu verzeichnen ist.

Differenzierter stellt sich die Situation dar, wenn es um die Folgen der Störung von IX geht. Dann wird die Regierungskommunikation signifikant beeinträchtigt, falls diese Kommunikation in dem intensiven Modus Bandbreite erfolgt, ohne dass das Hintergrundrauschen erhöht werden muss. Erfolgt hingegen die Kommunikation im Modus verteilt und werden deshalb deutlich weniger Regierungspakete zeitlich versetzt versandt, ist die Gefahr geringer, dass sie vernichtet werden. Zwar gibt es Paketverluste und einen höheren Gesamtschaden als Folge einer Störung der IX. Diese (bezogen auf die Zahl der Datenpakete) bescheidenere Regierungskommunikation funktioniert aber auch während einer solchen strategischen Störung hinlänglich gut. Deshalb beziehen sich die folgenden Aussagen nur auf den Modus Bandbreite der Regierungskommunikation:

Die Folgen eines Ausfalls des IX Frankfurt sind, im Gegensatz zu verbreiteten Erwartungen, bemerkenswert gering. Zwar werden einige Beziehungen im Kommunikati-

onsnetzwerk der Regierung zwischen einigen IX durch den Ausfall signifikant beeinträchtigt, aber die Regierungspakete erreichen meistens über Umwege ihr Ziel. Das ist dem relativ gut vermaschten Netzwerk in Deutschland zu verdanken.

London ist für Großbritannien ein zentraler Punkt der Anbindung an das europäische und das weltweite, speziell das nordamerikanische Backbonenetz. Somit ergeben sich bei einem Ausfall des IX London einige Probleme für die Anbindung Großbritanniens an die Welt. Der Paketverlust steigt signifikant, jedoch ist die Regierungskommunikation nur geringfügig betroffen. Verantwortlich dafür ist der generell zu beobachtende Effekt, dass es bei Störungen der IX zu einer Entlastung, zu einer Entstörung des Backbonnetzes und damit von Verbindungen kommt, da viele Pakete des Hintergrundrauschens vernichtet werden. Dieser Effekt kann das erste, entspannende Janusgesicht genannt werden. Die Eigentümer der vernichteten Pakete schauen in das grimmige, zweite Janusgesicht. Seine verlorengegangenen Pakete schaffen Raum für das Durchkommen der Regierungspakete.

Da Frankreich weniger vernetzt ist, verglichen mit Deutschland, aber Paris nicht in gleicher Weise wie der IX London der zentrale Anbindungspunkt ist, liegen die Folgen einer Störung des IX Paris zwischen den beiden: Verbindungen in Teilen Frankreichs werden beeinträchtigt und die innereuropäische Regierungskommunikation leidet. Bei der Störung des IX Paris wird ein Phänomen exemplarisch deutlich, das als Fernwirkung bezeichnet werden kann: Durch diese Störung ist die Erreichbarkeit des IX Rom stark beeinträchtigt, d.h. ihre Folgen sind in einer von der Störung weit entfernten Netzregion spürbar. Denn umgeleiteter Paketverkehr führt anderen Orts zu erhöhtem Verkehr und zu steigenden Paketverlusten. Daraus erwächst das Interesse, dass ein entfernt liegender Staat ein Interesse am Schutz des Netzes in Regionen haben muss, die weit weg von ihm liegen.²⁷⁶ Gelingt das nicht, drohen auch in „seinem“ Netzwerk spürbare Paketverluste, so dass die Nutzbarkeit des Internets leidet.

Fernwirkung und Janusgesichter beschreiben unabhängige Dimensionen der Wirkung von Störungen. Die Fernwirkung bezieht sich auf die räumliche und die Janusgesichter auf die materielle Dimension: Verbindungen werden entstört oder beeinträchtigt.

²⁷⁶ Solche Fernwirkungen gibt es auch in Strom-Verbundnetzen. Hier bestehen jedoch bessere Simulationsmöglichkeiten, um Effekte von Netzausfällen vorherzusagen. Zudem ist ein Krisenmanagement durch Steuerungszentralen möglich, das in gleicher Weise im Internet nicht gegeben ist.

Simulationsexperiment konkurrierende Infrastrukturpakete

Für diese Simulation (vgl. [Fischer, Lepperhoff, 2005]) wurde INESS modifiziert. Während die vorangegangenen Experimente auf einer Modellierung des heutigen egalitären Internets beruhten, das alle Datenpakete gleich behandelt, wurde eine Internetwelt simuliert, die prioritäre Datenpakete kennt. Zudem wurden zwei kritische Infrastrukturen in INESS eingeführt. In der Simulation wird angenommen, dass jede für sich ihre Datenpakete über ein Netzwerk austauschen, das insgesamt 145 IX und 383 Backbones umfasst. Eine dieser kritischen Infrastrukturen ist ein virtueller Stromerzeuger (CI Kraftwerk), dessen Datenpakete zwischen einem Kontrollzentrum und 13 im Netz verteilten Kraftwerken ausgetauscht werden, die koordiniert gefahren werden müssen. Die zweite Infrastruktur umfasst 14 Gesundheitszentren, die alle untereinander Datenpakete versenden. Diese 28 Bestandteile der kritischen Infrastrukturen gehören zu 28 IX in verschiedenen Regionen des simulierten Netzes. Zusätzlich sind wieder Datenpakete unterwegs, die Routinginformationen sowie diverse Nutzungen repräsentieren, etwa video on demand. Zusammen erzeugen sie die Hintergrundpakete. Alle 145 IX, die in der Simulation vertreten sind, produzierten bzw. empfangen diese Pakete, auch diejenigen, zu denen die Bestandteile der beiden CI gehören.

Im Basis-Simulationsexperiment werden aus methodischen Gründen alle Datenpakete, wie im heutigen Internet, gleich behandelt (Nullpriorität). Dagegen geht die zentrale Experimentfamilie von einem implementierten Prioritätssystem aus, d.h. Datenpakete werden bevorzugt weitergeleitet, wie das in einer IPv6 Umwelt möglich wäre. Dieses Prioritätssystem hat im Modell zwei Ausprägungen:

Erstens, eine technisch genannte Ausprägung der Hierarchie, die drei Klassen kennt: Pakete mit Routinginformationen, die immer Vorrang haben; die zweite Klasse teilen sich gleichberechtigt die Pakete für Echtzeitanwendungen (Data Stream) und die Datenpakete der beiden Infrastrukturen. Den niedrigsten Rang nehmen Pakete des Hintergrundrauschens ein. Folglich gibt es nicht nur Wettbewerb zwischen den drei Klassen von Datenpaketen, sondern auch innerhalb der zweiten Klasse.

Zweitens, eine als politische bezeichnete Hierarchie, in der fünf Prioritätsstufen festgelegt sind: Wieder stehen Routing-Datenpakete an erster Stelle, aber zweite Priorität haben die Pakete der kritischen Infrastruktur Kraftwerk; danach folgen die Pakete

des Gesundheitssystems, dann die des Data Stream.²⁷⁷ Abgeschlossen wird die Hierarchie von den Paketen des verbleibenden Hintergrundrauschens. (Alle diese Prioritäten können in INESS verändert werden.)

Die Simulationsexperimente untersuchen wieder die Auswirkungen eines Ausfalls von IX und außerdem die Folgen eines strategischen Wurmangriffs (ohne IX-Ausfälle). Dabei werden die Wirkungen jeweils für ein Netzwerk mit und ohne Prioritäten untersucht. Das Augenmerk liegt auf dem Paketverlust für die beiden kritischen Infrastrukturen - können sie ihre Funktionsfähigkeit vom Internet abhängig machen, auch angesichts der Gefahr von Cyberangriffen?

Während beim Ausfall eines zentralen IX, wie schon in vorangegangenen Simulationen, der Paketverlust stark ansteigt, wenn alle Pakete gleichberechtigt sind (Basisexperiment), sinkt der Verlust generell, wenn Prioritätsdienste eingeführt werden. Denn Routingpakete haben Vorrang, und das stabilisiert das Netzwerk erheblich. Politische Prioritäten reduzieren auch den Paketverlust der beiden Infrastrukturen um 21 Prozent, den anderer Pakete um nur zwei Prozent. Die Verbindungen zwischen den IX, die Pakete der Infrastrukturen austauschen, verbessern sich: Während ohne Prioritätsdienste 52 Verbindungen erhebliche Qualitätseinbußen erleiden,²⁷⁸ reduziert die politische Priorität die Zahl auf 45 Verbindungen. Wie zu erwarten, begünstigt das fünfstufige Prioritätensystem die Kraftwerksinfrastruktur, während die der Gesundheit einen Preis zu zahlen hat: Auf einem erheblichen Teil der Verbindungen innerhalb dieser kritischen Infrastruktur steigt der Paketverlust.

Um die Folgen eines Angriffs mit einem Wurm für die Gesundheits- und Kraftwerksinfrastruktur zu untersuchen, wird ein weit gestreuter Befall unterstellt: Jeder der 145 IX produziert zusätzlich zu seiner normalen Paketproduktion Wurmpakete. In einer Netzumwelt mit Prioritätsdiensten hat ein Wurmschreiber zwei extreme theoretische Möglichkeiten: Er befähigt den Wurm, die höchste Prioritätsstufe einzunehmen, die eigentlich den Routingpaketen vorbehalten ist - dieser Wurm wird hier Alptraum-Wurm genannt. Oder er schreibt einen harmlosen Wurm, der sich in die niedrigste Priorität fügt, also die Pakete des Hintergrundrauschens verstärkt.

Dieser relativ harmlose Wurm hat nur bescheidene Folgen für den Pakettransport. Zwar gehen viele Pakete verloren, aber darunter befinden sich - neben Paketen des Hintergrundrauschens - sehr viele Wurmpakete, die zahlreich an den IX produziert

²⁷⁷ Sie wird politisch genannt, weil explizit eine Rangfolge der kritischen Infrastrukturen und damit ihre Bedeutung festgelegt wurde.

²⁷⁸ Definiert als 20 Prozent und mehr Paketverlust.

werden, einige Backbones überlasten und dann verloren gehen. Die Verluste höher-rangiger Pakete sind dagegen sehr bescheiden. Wie in den Simulationsexperimenten zu IX-Störungen bewährt sich, dass die vorrangigen Routingpakete das Netzwerk recht stabil halten. Der Alptraum-Wurm hingegen lässt den Paketverlust deutlich ansteigen. Dabei ist es für den gesamten Paketverlust kein großer Unterschied, ob technische oder politische Prioritäten umgesetzt sind - er bleibt hoch.

Eine genauere Betrachtung der Paketverluste der beiden kritischen Infrastrukturen zeigt, dass der Charakter des Wurmes entscheidend für die Folgen ist. Verglichen mit einem Wurmbefall in einer Umwelt ohne Prioritäten sinkt bei einem harmlosen Wurm in einer Umwelt mit technischen Prioritäten der Infrastruktur-Paketverlust um 42 Prozent, während der Verlust anderer, nachgeordneter Pakete nur um 3 Prozent abnimmt. Der Alptraum-Wurm hingegen erhöht den Paketverlust der beiden Infrastrukturen um 23 Prozent (technische Prioritäten) und immerhin noch um 15 Prozent im Falle der politischen Prioritäten, die die Folgen des Wurmbefalls für sie etwas dämpfen.

Die Analyse der Auswirkungen für die kritische Infrastruktur Kraftwerk zeigt, dass der Alptraum-Wurm die Verbindung zwischen dem Kontrollzentrum und den Kraftwerken 1, 2, 7 und 11 stark beeinträchtigt, unabhängig von dem Prioritätssystem. Jedoch kann mit beiden Prioritätssystemen die Verbindung zu Kraftwerk 14 wieder hergestellt werden, die im Szenario des Wurmangriffs ohne Priorität stark litt (*Abbildung 15*). Im Gegensatz zu dem Szenario des IX-Ausfalls, in dem die Gesundheitsinfrastruktur am stärksten beeinträchtigt war, sind im Szenario des Alptraum-Wurms die Verbindungen dieser Infrastruktur weniger betroffen. Das ist der Topologie des Internets zu verdanken. Wie die Abbildung zeigt, sind die IX, in denen die Gesundheitseinrichtungen (schwarze Dreiecke) liegen, eher im Zentrum des Netzwerkes, während die beeinträchtigten Kraftwerke (schwarze Punkte) an der Peripherie angesiedelt sind. Hier gibt es, im Gegensatz zum inneren Bereich des Internets, weniger Ausweichstrecken für die Datenpakete, die von und zum Kontrollzentrum mitten des Netzwerkes reisen müssen.

Aber die Entfernung vom Kontrollraum allein ist kein Indikator für eine schlechte Verbindung. Denn es gibt Kraftwerke, die an der Netzperipherie angesiedelt sind und

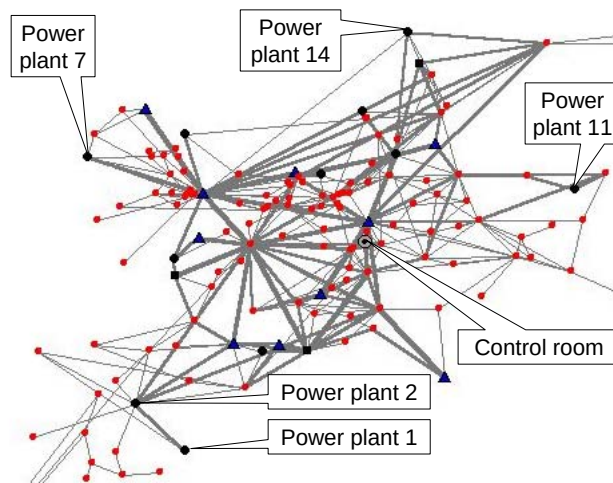


Abbildung 15: Positionierung der Kraftwerke 1, 2, 7, 11 und 14 im Netzwerk.

trotzdem keine Verbindungsprobleme haben. *Abbildung 16* zeigt die Zahl der Verbindungen mit guter Qualität in Abhängigkeit von dem Weg, den die Datenpakete zurücklegen müssen (gemessen in HOP). Anlagen der Infrastrukturen, die vier HOP entfernt sind, haben die besten Verbindungen, während die nahen und fernen Anlagen größere Probleme bekommen. Offensichtlich gibt es keinen Zusammenhang zwischen Entfernung und Verbindungsqualität. Weitere Faktoren wie die Topologie des Netzes, die Auslastung der Verbindungen, spielen eine Rolle.

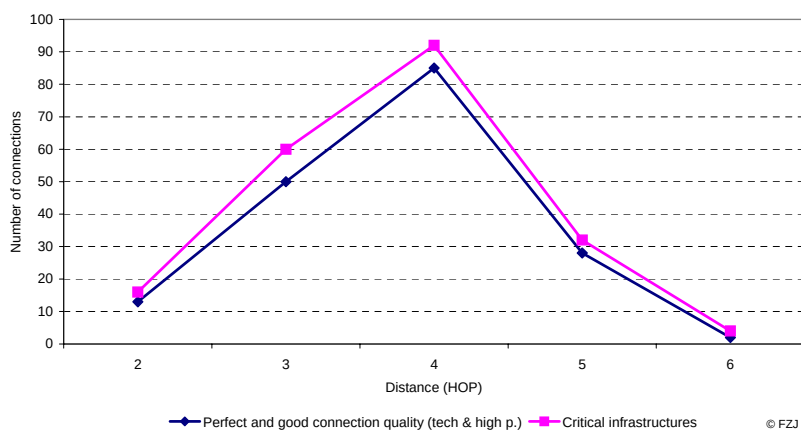


Abbildung 16: Qualität der Verbindung in Abhängigkeit zur Entfernung bei einem Alptraum-Wurmangriff mit technischen Prioritäten.

Die INESS-Ergebnisse zeigen, dass bei Angriffen die Prioritätsdienste, etwa in einer IPv6-Welt, eine Dialektik von Erleichterung und Erschwernis in sich tragen. Sie stellen sicher, dass Routingpakete ihre Ziele erreichen, so das Netzwerk stabilisieren und Paketverluste in Grenzen halten, verglichen mit einem egalitären Pakettransport. Freilich kann das auf Kosten von Paketen gehen, die geringe Priorität haben.

Die Simulation zeigt, dass politische Prioritäten (mit dem hier unterstellten Schema) die kritische Infrastruktur Kraftwerke begünstigt, auf Kosten der Gesundheitsinfrastruktur (und der anderen nachrangigen Pakete). Daher wären politische Diskussionen über die Bedeutung, die CI zugewiesen wird, notwendig. Schwerwiegende Probleme kann hingegen die Hierarchie der Datenpakete bringen, falls ein Wurm in die Lage versetzt würde, die höchste Prioritätsstufe zu erklimmen, auf der sinnvollerweise nur die Routingpakete sein sollten. Die Autoren fassen zusammen [Fischer, Lopperhoff, 2005, S. 491]: "Different threats may call for different priority policy schemes. Therefore a ranking of CIs may be beneficial in some cases only. The situation is different during a worm attack. Now the crucial variable is the worm's `character`. Only a nice version of a worm, classifying itself into the lowest priority class, reduces the packet loss for CIs. But a `nightmare` worm, making use of the priority system and taking up the highest priority class, increases CI packet losses. Therefore, the remedy a defender introduces for a crisis situation, the priority service, could be abused by those attacking the network.

Future security simulation has to take into account the (well known in the military field) dialectics of defence and offence. Furthermore, we have to understand how critical infrastructures cope with packet losses, how they respond and which options they have to keep these infrastructures functioning during packet losses. Simulation is useful for the `coupling` of data packet losses and institutional response. Current developments using the Internet for telephone calls (Voice over IP) stress the need for further research. If the telephone network should become Internet-based, thus reducing redundancy for other important data packets, then this would mean that it is high time for a discussion on politically defined priority schemes to begin."

Das Internet ist ein relativ resilientes Datentransportsystem

Die Experimente zeigen, dass das simulierte Internet, zumindest in Europa, relativ resilient ist gegen die simulierten Störungen. Da INESS die Funktionsweise dieses Netzwerkes nachbildet, wird die These formuliert, dass die Aussage grundsätzlich

auch für das reale Internet gilt. Terrorismus gegen den Cyberspace, der die Funktionsfähigkeit des Internets durch sie wesentlich beeinträchtigen möchte, darf daher keinesfalls auf eine einfach zu erhaschende, große Erfolgchance hoffen.

Aber das Internet ist eben nur relativ resilient. So hätten strategische Störungen von IX erhebliche Auswirkungen auf den Pakettransport und die Verbindungsqualität zwischen IX. Das Internet kann bei solchen Störungen zwar seine immanente Flexibilität nutzen, die im Pakettransport angelegt ist. Aber diese - verglichen etwa mit dem analogen Telefonnetz oder dem steuerungsaufwändigen Stromnetz - hohe immanente Resilienz reicht nicht hin, um allen Schaden bei IX-Ausfällen abzuwenden. Ihre Folgen würden in z. T. weit entfernten Netzteilen spürbar, und die Infrastrukturen, die zeitkritische Datenpakete etwa zur Steuerung von essentiellen Prozessen versenden, könnten in Probleme geraten. Die Zerstörung von Backbones hingegen erweist sich als keine wirkungsvolle Option, soweit negative Auswirkungen auf das breitere Netzwerk das Ziel sind. Sie bleiben weitgehend aus.

Deutlich weniger Paketverluste wären gemäß der Modellsimulationen zu erwarten, wenn es Prioritätsdienste gäbe, die Routingpakete vorrangig weiterleiten. Hohe Priorität könnte auch Paketen kritischer Infrastrukturen das Durchkommen erleichtern, wenn es zu Störungen käme. Solche neuen Dienste gingen aber mit neuen Verwundbarkeiten einher: Auch wenn ein solcher Wurm nur in der Modellierung mit INESS frei ist, würde ein Angriff mit einem Wurm, der für sich die höchste Prioritätsstufe einnimmt, schwerwiegende Auswirkungen haben. Datenpakete kritischer Infrastrukturen, die ihre wichtigen Informationen über das Internet senden, gingen in großer Zahl verloren. Ist, wie im Modell, eine kritische Infrastruktur Kraftwerk darauf angewiesen, innerhalb von Sekunden via Internet neue Kapazitäten im Stromnetz zu mobilisieren bzw. vom Netz zu nehmen, könnte der simulierte Angriff auf IX zu Instabilitäten im Stromnetz führen. Möglicherweise wäre dann der kostengünstigere Datentransport über das öffentliche Internet auch künftig für essentielle Steuerungssignale, selbst bei prioritären Diensten, aus Sicherheitsgründen nicht sinnvoll.

So notwendig die Betrachtung des gesamten Netzes auch ist, sagt das wenig darüber aus, wie sich strategische Störungen auf regionale oder lokale Akteure auswirken, die von funktionsfähigen Verbindungen essentiell abhängig sind. Ihnen hilft die Versicherung nicht, das Netz werde insgesamt sogar mit strategischen Störungen gut fertig, wenn sie an besonders stark betroffenen Verbindungen sitzen, die zudem recht weit vom originären Störungsort entfernt sein können. Um genauer solche kritischen

Akteure und ihre spezifischen Verwundbarkeiten bei Störungen simulieren zu können, bedarf es jedoch einer wesentlich feineren Beschreibung der Topologie. Dies führt zu einem zweiten Punkt. Die Simulationsexperimente weisen auf die Voraussetzungen hin, die gegeben sein müssen, damit die hohe Resilienz des Internet gewahrt bleibt: Einmal ein günstiges Verhältnis zwischen Kapazität und Verkehr und, drittens, eine angemessene Topologie (siehe Abbildung 2). Alle Faktoren, die sich beständig verändern, in ihrem Zusammenspiel zu beobachten, ist eine beständige Aufgabe. Sie sollte einer neutralen Stelle gestellt werden, etwa in Deutschland dem BSI, und einer entsprechenden europäischen Einrichtung, die angesichts des weltweiten Charakters des Netzwerkes weitere (inter)nationale Partner aus Wirtschaft und Regierung braucht. Ein solches kontinuierliches Monitoring hat zur Voraussetzung, dass die Datenlage über Topologie, Kapazitäten von Backbones und Internet Exchange Points sowie über den in den letzten Jahren drastisch wachsenden Datenverkehr vollständig und qualitativ hochwertig ist und bleibt. Hier sind deutlich Lücken zu erkennen.

Internetsicherheit als bleibende Herausforderung

Effiziente, ineinander greifende Infrastrukturen bilden das Rückgrat wirtschaftlich-technologischer Leistungsfähigkeit, ermöglichen individuelle Teilhabe am gesellschaftlichen Leben, und sie sind ein Fundament staatlicher Handlungsfähigkeit und Macht. Ihr Aufbau, ihre Erhaltung und Sicherung erfordern hohe Investitionen und benötigen komplexe Institutionen. Zugleich sind sie, mehr oder weniger, potentiell verwundbare Strukturen, die durch Naturgewalten, technisches, menschliches, institutionelles Versagen und durch beabsichtigte, gezielte Handlungen in ihrer Leistungsfähigkeit beeinträchtigt werden können.²⁷⁹ Im Rahmen des unverzichtbaren Infrastrukturschutzes, der sich solchen Gefährdungen widmet, kommt der Sicherheit der Informationsinfrastrukturen generell und des (öffentlichen) Internets speziell eine besondere Bedeutung zu. Denn das Internet hat das Potential, sich zu einer Infrastruktur der Infrastrukturen zu entwickeln, über die alle digitalen Daten ausgetauscht werden können.²⁸⁰ Cybersecurity, Internetsicherheit, wird ein immer wichtigeres Handlungsfeld für Gesellschaft und Politik auf nationaler und, dem Charakter des globalen Netzes entsprechend, auf internationaler Ebene. Sie widmet sich verstärkt den Sicherheitsgefahren, ihrer Abwehr und Bewältigung, die von diversen gesellschaftlich-politischen Akteuren ausgehen und eine sichere, störungsarme Nutzung des Netzwerkes zu beeinträchtigen drohen.²⁸¹ Der Schutz dieser sich weiter entfaltenden Infrastruktur Internet ist eine Herausforderung, die in Zukunft keinesfalls leichter zu bewältigen sein wird.

Sicherlich ist das Internet kein Raum, in dem man unter die Diebe und Räuber fällt, sobald man ihn betritt. Fast immer verläuft die Nutzung des Netzwerkes ohne Probleme, und noch immer werden kriminelle Taten ganz überwiegend in der realen Welt begangen. Aber sie finden immer öfter ihren Platz im weltweiten Netzwerk, und die Warnungen vor dem, was noch droht, nehmen zu. Obwohl es offene Fragen zur Sicherheitslage im Internet gibt,²⁸² hat sie sich wahrscheinlich in der Realität, sicher aber in der vorherrschenden Wahrnehmung von Fachwelt, Politik und Öffentlichkeit über die Jahre hinweg verschlechtert, und eine Trendwende zeichnet sich nicht

²⁷⁹ Vgl. S. 23ff; 62ff in diesem Band.

²⁸⁰ Vgl. S. 41ff.

²⁸¹ Vgl. S. 50ff.

²⁸² Vgl. S. 64ff.

ab.²⁸³ Insbesondere den Gefährdungen der Cybersecurity, die von beabsichtigten, gezielten Handlungen ausgehen, gilt die besorgte Aufmerksamkeit. Zu ihnen zählen:

- gewöhnliche kriminelle Aktivitäten (*Cyberkriminalität*). Die Täter begehen ihre kriminellen Handlungen im Internet oder sie nutzen das Netzwerk, um in der realen Welt erfolgreicher zu agieren. Ein großer Teil der Straftaten, die dort begangen werden, haben auch in Internet ihren Platz gefunden, und neue internetspezifische Taten kommen hinzu.
- terroristische Aktivitäten, die in zwei Ausprägungen auftreten:
 - Als inzwischen klar erkennbare terroristische *Nutzung* des Internets, um Propaganda zu betreiben, Informationen zu gewinnen und zu übermitteln, um Netzwerk zu bilden, Geld zu beschaffen und um Helfer, Mittäter zu rekrutieren (Terrorismus *im* Cyberspace). Ziel dieser Internetnutzung ist es, Handlungsmöglichkeiten in der physischen Welt zu verbessern und zu erweitern.²⁸⁴
 - Als noch hypothetischer Terrorismus *gegen* den Cyberspace, als *Cyberterrorismus* im eigentlichen Sinne. Terroristischen Gruppen wollen durch den Einsatz von Schadsoftware, Hacken etc. die ungestörte, sichere Nutzung des Internets beeinträchtigen und, via Internet, weitere kritische Infrastrukturen angreifen und in ihren Funktionen stören.²⁸⁵

Die vor allem in den USA, nun aber auch in Europa recht intensiv geführte Diskussion über diesen Cyberterrorismus und die von ihm ausgehenden Gefahren ist vor dem Hintergrund eines (neuen) transnationalen Terrorismus zu sehen, der seit dem Beginn des 21. Jahrhunderts die nationalen und internationalen Politiken stark beeinflusst.

Eine Bilanz der Diskussionen über Cyberterrorismus führt zu einem recht eindeutigen Ergebnis:²⁸⁶ In Fachwelt und Politik herrscht breite Übereinstimmung darüber, dass es bislang keinen Terrorismus gegen den Cyberspace gab und auch heute nicht gibt. Zwar sind verbreitet Hackerangriffe, Angriffe mit Schadsoftware etc. zu beobachten, und vereinzelt richten sie sich auch gegen Kernbereiche des Internets wie das System der Namensauflösung. Aber ein terroristischer Hintergrund lässt sich bislang nicht nachweisen. Anfang 2003 stellte der damalige deutsche Innenminister Otto Schily nach einem Treffen mit dem ehemaligen Minister für Homeland Security der

²⁸³ Vgl. S. 73ff.

²⁸⁴ Vgl. S. 124ff.

²⁸⁵ Vgl. S. 137ff; zu den physikalischen Einwirkungsmöglichkeiten auf das Netzwerk vgl. S. 85ff.

²⁸⁶ Vgl. S. 117ff.

USA, Tom Ridge, fest, dass es keine Anhaltspunkte für eine besondere Gefahr für Computersysteme und -netze durch den internationalen Terrorismus gibt.²⁸⁷ Dieses Lagebild scheint auch heute noch zuzutreffen, auch wenn eine allgemeine, abstrakte Gefährdung des Cyberspace durch terroristische Aktionen besteht, die seit einigen Jahren für alle Bereiche des öffentlichen Lebens vorhanden ist.²⁸⁸

Die konkreten Gefahren, denen sich Betreiber und Nutzer des Internets ausgesetzt sehen, sind deshalb nicht gering zu achten: Sie umfassen die nun schon traditionelle, weiter um sich greifende Internetkriminalität in ihren vielfältigen Formen, den Datendiebstahl, die -veränderung, -sabotage, die Versendung von Spam, die wachsende Gefährdungen der Privatsphäre, Spionage im und durch das Netzwerk; ferner Cyberangriffe, die sich gegen wichtige Server richten und deren Gründe vielfältig sein können - von individueller Neugierde, ob der Angriff eine Wirkung zeigt bis hin zur Erpressung von Unternehmen durch kriminelle Banden. Aber solche Angriffe, selbst wenn sie Server für einige Zeit ausschalten oder bedeutsame Nutzer zeitweise an der Netznutzung hindern, sind per se keine Bedrohung der nationalen Sicherheit, deren Abwehr eine zentrale Aufgabe der Politik ist. Sie bereitet vor allem den privaten Netzbetreibern, -nutzern und Softwareherstellern z. T. erhebliche Probleme und Mühen, und ihnen fällt die Aufgabe zu, sich individuell und abgestimmt gegen solche Angriffe abzusichern. Leider gelingt das nicht selten nur mehr schlecht als recht,²⁸⁹ weil die Sensibilität für Gefahren fehlt oder weil Nutzer hoffen, auch bei Verzicht auf (nicht selten aufwändige) Schutzmaßnahmen ungeschoren davonzukommen.

Wann und unter welchen Bedingungen aus (immer lästigen und oft kostspieligen)²⁹⁰ Angriffen und den anderen kriminellen, terroristischen Aktivitäten im Netzwerk eine reale (inter)nationale Sicherheitsgefährdung erwächst, ist in der Fachwelt umstritten. Dunn [2005, S. 10] stellt dazu fest: "It is (...) highly controversial whether risks linked to the Internet and other information infrastructure constitute a real national security threat, since the menacing scenarios of major disruptive occurrences in the cyber-domain triggered by malicious actors have remained just that - scenarios, even when

²⁸⁷

http://www.bmi.bund.de/cln_012/nn_122688/Internet/Content/Nachrichten/Archiv/Pressemitteilungen/2003/06/Schily__und__Ridge__vereinbaren__Kooperation__Id__92348__de.html.

²⁸⁸ Nur kurz skizziert wurde in diesem Band die Diskussion über einen (zwischenstaatlichen) „Rüstungswettlauf im Cyberspace“ und seine erheblichen Gefahren auch für zivile Netzwerke. In welchem Ausmaß sich Staaten auf Cyberkrieg vorbereiten, ist schwer einzuschätzen; vgl. S. 91ff.

²⁸⁹ Natürlich stehen auch staatliche Einrichtungen in der Pflicht, sich abzusichern. Zudem beraten und unterstützen staatliche Stellen wie das BSI die Privaten.

²⁹⁰ Vgl. S. 67ff.

one takes into account that there have been some few incidents with the potential for grave consequences.”

Trotzdem gibt es gute Gründe, sich nicht unbekümmert zurückzulehnen und darauf zu hoffen, man werde mit den heutigen Problemen auch künftig fertig, und der Terrorismus gegen den Cyberspace sei auch in Zukunft nur eine weit entfernte, abstrakte und sicherheitspolitisch irrelevante Möglichkeit, auf die sich Politik und Gesellschaft nicht ernsthaft vorbereiten müssen. Ebenso wenig angemessen wie eine solche leichtfertige Unbekümmertheit ist ein dröhnender Alarmismus, der ein „digitales Pearl Harbor“ oder einen „Cyber 9/11“ unmittelbar bevorstehen sieht. Überreaktionen und Fixierung auf eine Gefährdung, deren Konturen noch verschwommen sind, wären die Folgen. Angemessen ist eine Politik, die eine neue Gefährdung der Sicherheit des Internets und anderer kritischer Infrastrukturen wahrnimmt, die sich freilich erst herausbildet und deren Ausprägung und Wirksamkeit noch nicht klar abzuschätzen ist. Diese gefährdungsbewußte Politik muss die Prozesse genau beobachten, die einen Terrorismus gegen den Cyberspace wahrscheinlicher werden lassen, sie muss die Verflechtungen der diversen Gefährdungen, vor allem zwischen (Cyber-) Kriminalität und Cyberterrorismus, erkennen,²⁹¹ sich behutsam auf einen Cyberterrorismus vorbereiten und kontinuierlich die der Bedrohung angemessenen Konzepte und Maßnahmen entwickeln.

Die Prozesse, die Cyberterrorismus wahrscheinlicher machen, sind verwoben mit weltweiten politisch-gesellschaftlichen Trends, die Ordnungsstrukturen schwächen, ohne immer wirksame neue zu produzieren, und sie werden forciert durch die spezifischen Merkmalen und Entwicklungen des Internets selbst:

- Es eignet sich für asymmetrische Auseinandersetzungen, denn selbst kleine Gruppen können von jedem Punkt des Netzwerkes aus wichtige Rechner in den Ländern bedrohen, deren Machtpotential auch nur den Gedanken an eine Konfrontation mit gleichen Mitteln auf Augenhöhe verbietet.
- Mit der Zahl der Nutzer nimmt die Anzahl der Menschen zu, die destruktive Absichten und bessere Kenntnisse der Software haben; politische Ziele und technische Fähigkeiten finden häufiger zueinander, und Cyberkulturen könnten sich herausbilden, die terroristische Netzwerke befruchten oder in sie übergehen.

²⁹¹ Vgl. Abbildung 1, S. 99.

- Die Mittel für Angriffe (Hacker-tools) sind im Internet weit verbreitet, leicht zugänglich und werden besser. Kaum ist eine Softwarelücke erkannt, steht ein Schadprogramm bereit, um sie zu nutzen.
- Die Dienste im Internet werden zahlreicher und die Anwendungen vielfältiger, die verwendete Software einheitlicher und sie weist - trotz Verbesserungen - oft Mängel auf. Tendenziell nimmt so die Verwundbarkeit des Netzwerkes zu.
- Künftig könnten kritische Infrastrukturen das Internet für den Transport von essenziellen, zeitkritischen Datenpaketen nutzen, etwa virtuelle Kraftwerke, der Gesundheitssektor und Wasserver- und Wasserentsorgung. Erfolgreiche Angriffe, die Folgen auch in der physischen Welt zeigen, würden Politik, Gesellschaft und die freie Nutzung des Netzwerkes negativ beeinträchtigen.
- Der zeitliche, personelle und finanzielle Aufwand für Identifikation, Überwachung, Abwehr und für die Verfolgung von kriminellen Aktivitäten und Angreifern im Netz ist hoch, und Kriminelle haben eine gute Chance unbeobachtet und unerkannt zu bleiben, wenn sie die Funktionsweise des Internets kennen.
- Jede Verteidigung im Internet muss aus der schwierigen Position der Defensive und Reaktion formuliert und umgesetzt werden, während der Angreifer den Zeitpunkt, die Dauer, Mittel und das Ziel eines Angriffs bestimmt und von jedem Punkt des Netzes aus operieren kann. Das zwingt Verteidiger dazu, sich mühselig und mit hohen Kosten auf diverse Angriffe aus allen Richtungen des Netzes vorzubereiten.
- Die Entwicklung international abgestimmter Konzepte, um kriminelle Aktivitäten und die Herausbildung eines Cyberterrorismus zu verhindern oder zumindest seine Wirksamkeit zu dämpfen, ist schwierig, stockend; sie wird nicht selten durch mangelnde Kooperationsbereitschaft oder wenig ausgebildete Fähigkeiten zur Zusammenarbeit, zur Verhütung und Abwehr von Cyberangriffen beeinträchtigt.

Aber das Internet selbst hat seine Stärken, und es würde Angreifern mit strategischen Absichten das Leben schwer machen. Erfolgreiche Angriffe auf seine Funktionsfähigkeit wären nur denkbar, wenn Cyberterroristen sehr kompetent, gut organisiert wären und - dies würde die Aussicht auf Erfolg erhöhen - eine Unterstützung durch kompetente staatliche Stellen erhielten. Ob und wann das der Fall sein wird, bleibt im Dunkeln. Zudem müssten, sollen Angriffe ihre intendierte Wirkung voll entfalten, weitere Bedingungen erfüllt sein: Die Staaten müssten in aller Breite und Intensität vom Internet abhängig sein, und ihre Vorbereitung auf Cyberabgriffe und die

Bewältigung der Angriffsfolgen müsste nachlässig und unzulänglich sein. Politik und Gesellschaft verfügen aber über technische, organisatorische und politische Spielräume, um Cybersecurity wirksamer zu gestalten.

Aber auch bei günstigen Voraussetzungen für Cyberterroristen wäre es nicht sicher, dass Angriffe strategische Auswirkungen hätten und einem Zusammenbruch des Internets in weiten Regionen führen würden, der länger als nur wenige Tage anhält. Denn das Netzwerk ist, wie von seinen Erfindern gewollt, relativ flexibel und resilient, wenn einige Bedingungen erfüllt sind. Das zeigen die Ergebnisse des Simulationsmodells INESS.²⁹²

Das Modell bildet die grundlegenden Eigenschaften des Internets auf der Ebene des Pakettransports, der zentralen Dienstleistung dieser Infrastruktur, ab. INESS kann Folgen zu simulieren, die beispielsweise Angriffe auf zentrale Internet Exchange Points (IX) und auf große Backbones für den Pakettransport haben.

Die Simulationen, die sich auf das Internet in Europa und den USA konzentrieren,²⁹³ zeigen, dass die Zerstörung von (landgestützten) Backbones keine sinnvolle Option zur strategischen, großräumigen und länger andauernden Unterbrechung des Verkehrs mit Datenpaketen ist.²⁹⁴ Zwar würde die Durchtrennung bedeutender Kabel den Paketverkehr beeinträchtigen, das Internet langsamer machen und eventuell schlecht angebundene Regionen zeitweise vom Netzzugang trennen. Aber es gibt meist alternative Routen, die, obwohl sie während der Störungen oft überlastet sind, noch immer den Pakettransport einigermaßen sicher stellen. Auswirkungen der Kabelzerstörungen bleiben daher, so die Simulation, lokal-regional begrenzt. Zudem ist die Reparatur der Backbones auf dem Festland, verglichen mit Seekabeln, unproblematisch. Störungen wären in der Regel nach Stunden oder wenigen Tagen behoben.

Gravierender, aber auch schwerer zu realisieren, wäre die Ausschaltung von Internet Exchange Points: Sie hätte deutlich stärkere Auswirkungen auf den Pakettransport und die Verbindungsqualität zwischen IX. Auch hier zeigt die Simulation, dass der Schaden, gemessen am Verlust von Datenpaketen, hinter dem zurückbleibt, was oft befürchtet wird, wenn Medien und Fachwelt solche Szenarien qualitativ diskutieren.

²⁹² Vgl. S. 145ff.

²⁹³ Für diese Regionen ist die Netzstruktur feiner abgebildet, während im Rest der Welt nur die größten Backbones und IX in die Simulation eingehen.

²⁹⁴ Die Unterbrechung wichtiger Seekabel, von denen es relativ wenige gibt, hätte wahrscheinlich stärkere Auswirkungen. Da ihre gezielte Zerstörung als unwahrscheinlicher eingeschätzt wurde, wurden die Folgen nicht mit INESS simuliert.

Es gelingt im Modell im Rahmen der vorgegebenen Szenarien nicht, den Paketverkehr so entscheidend zu beeinträchtigen, dass es zu einem großräumigen Ausfall des Internets käme. Die meisten Verbindungen über das Internet zwischen den IX bleiben intakt, auch wenn es bei einigen Verbindungen sehr große Paketverluste gibt.

Noch schwerwiegendere Folgen wären zu erwarten, wenn es gelänge, in einer denkbaren Internetwelt, die (im Gegensatz zu heute) prioritäre Dienste kennt, ein Schadprogramm (Wurm) zu schreiben, das die höchste Prioritätsstufe einnimmt. In einem modifizierten INESS-Modell kommt diese erste Priorität eigentlich nur den Routinginformationen zu. Die Simulationsergebnisse²⁹⁵ zeigen, dass ein solcher Wurm das Netzwerk schwer belastet und den Transport wichtiger Datenpakete kritischer Infrastrukturen beeinträchtigen würde. Sie nehmen im Modell die zweite Prioritätsstufe in einer Internetwelt ein, die eine ganze Prioritätenabfolge kennt. Aber auch dann funktioniert der Transport dieser Infrastrukturalpakete in vermaschten Regionen des Internets weiterhin recht gut, auch wenn dort weit überdurchschnittliche Verluste bei den nachrangigen Paketen (bezeichnet als Hintergrundrauschen) zu verzeichnen sind. INESS zeigt, dass Prioritätsdienste generell eine Dialektik von Erleichterung und Erschweren in sich tragen und deshalb mit Bedacht eingeführt werden sollten: Käme es zu einer Zerstörung von IX (ohne dass der gefürchtete Wurm auftritt), können Prioritäten sicherstellen, dass Routingpakete ohne größere Verluste ihre Ziele erreichen. Das Netzwerk würde dadurch stabilisiert und Paketverluste blieben in Grenzen, verglichen mit einem (heutigen) egalitären Pakettransport. Die Gefahren für das Netz steigen jedoch auch ohne eine IX-Zerstörung erheblich, falls ein Wurm die höchste Prioritätsstufe erklimmen könnte. Das zu verhüten wäre erste Priorität der Cybersecurity-Politik.

Die Simulationsexperimente weisen auch auf die Bedingungen hin, die gegeben sein müssen, damit eine hohe Resilienz des Internet gewährleistet ist: Freie Kapazitäten bei Backbones und IX, gemessen am Datenverkehr, um bei Störungen zusätzliche Pakete aufzunehmen, sowie eine günstige, `vermaschte` Topologie des Netzwerkes.²⁹⁶ Ob das dauerhaft in allen wichtigen Regionen des Internets vor dem Hintergrund eines jetzt und künftig weiter steigenden Datenverkehrs durch marktbezogene Entscheidungen sichergestellt wird, bleibt eine offene Frage.

²⁹⁵ Vgl. S. 165ff.

²⁹⁶ Vgl. Abbildung 2, S. 145.

Die Simulationen erfassen aber nicht alle Gefahren, die von einem künftigen Cyberterrorismus ausgehen könnten. Er verfügt über mehr Optionen, etwa Hacken,²⁹⁷ die INESS nicht nachahmen kann. Zielt ein Angriff, mit welchen Mitteln des Cyberspace auch immer, darauf ab, einzelnen wichtigen Internetnutzern den Zugriff auf das Netz zu versagen bzw. dessen sichere Nutzung zu verhindern, sind eher direkte, gezielte Cyberangriffe gegen diese Rechner zu erwarten. Der Umweg über die Ausschaltung eines IX und den so induzierten Paketverlust, der möglicherweise gar nicht bei dem anvisierten Opfer auftritt, wäre beschwerlich und wenig erfolgversprechend. Auch das Eindringen über das Internet in Supervisory Control and Data Acquisition Systems anderer kritischer Infrastrukturen, so schwer das in der Praxis auch ist, sind gefährliche Angriffsmöglichkeiten, die Terroristen anstreben könnten. Gelängen sie, könnten diese SCADA-Systeme so manipuliert werden, dass die physische Umwelt beeinträchtigt wird, etwa durch Öffnen von Staudämmen. Unklar ist jedoch, in welchem Maße solche Systeme überhaupt via Internet zugänglich sind. Forschungsprojekte widmen sich diesem Problemfeld.

Transnationaler Terrorismus und die latente Drohung des Cyberterrorismus lösen einen Impuls aus, staatliches und gesellschaftliches Handeln wieder stärker an sicherheits- und machtpolitischen Herausforderungen zu orientieren, und in dem Kontext neuer Bedrohungen gewinnt auch der Schutz kritischer (Informations-) Infrastrukturen an Bedeutung. Er wird jedoch, entgegen mancher sicherheitspolitischer Rhetorik, vor allem durch privates Handeln gewährleistet, während sich die Politik mit direkten Eingriffen und strikten Vorgaben zurückhält. Das gilt auch und insbesondere für die Cybersecurity.²⁹⁸ Der Impuls, angesichts neuer Bedrohungen in einem Kontext, in dem kritische Infrastrukturen latent gefährdet sind, zu einem Sicherheitsstaat zu werden, trifft in westlichen Ländern auf Hindernisse und Vorbehalte und schwächt sich ab. Dafür gibt es eine Reihe gesellschaftlich-politischer Gründe, aber auch struktureller Ursachen: Der Staat muss seinen Zuschnitt und seine Rolle im Zeitalter der Globalisierung noch finden, und er kann angesichts der Privatisierung von Infrastrukturen keine Politik zum Schutz der kritischen Infrastrukturen verfolgen, die Interessen privater Infrastrukturbesitzer vernachlässigt, ihre Wettbewerbs- und Innovationsfähigkeit gefährdet. Das zeigt sich besonders beim Internet, das zu 90 Prozent in privatem Besitz ist, und der Cybersecurity. Sie ist national ohnehin nicht

²⁹⁷ Vgl. S. 80ff.

²⁹⁸ Vgl. S. 107ff.

zu gewährleisten, und die Mittel staatlicher Sicherheitswahrung, vor allem die Streitkräfte, helfen hier weniger und sind nicht erste Wahl beim Schutz dieser kritischen Infrastruktur. Stattdessen legen die Rahmenbedingungen nahe, den guten Schutz der privaten Netze und der Rechner durch Software, institutionelle Vorkehrungen, Bewusstseinsbildung und Wissen ins Zentrum zu stellen. Das alles setzt eine aktive Mitwirkung der Netzbetreiber und möglichst vieler Internetnutzer voraus, die den größten Teil der Maßnahmen mit eigenen Mitteln in eigener Verantwortung umsetzen müssen. Dabei kommt dem Staat eine wichtige, aber meist kontextbezogene Rolle zu. Eine unmittelbare Funktion kommt ihm vor allem im Rahmen seiner polizeilichen Aufgaben zu, die zur Einrichtung von Cyberpolizeidienststellen führt. Der Schwerpunkt der staatlichen Aktivitäten liegt jedoch bei:

- der Unterstützung von *Forschung*, um die Gefahren für die kritische Informationsinfrastrukturen frühzeitig und sachgerecht einzuschätzen;
- der *Bewusstseinsbildung* für die Gefahren und die Schutzmöglichkeiten bei allen Internetnutzern, den Netzbetreibern und Inhaltenanbietern;
- einer Unterstützung der *technischen Vorsorge*, um - auch bei staatlichen Stellen - mehr sichere Hard- und Software einzusetzen; denn aus Sicht von Benutzern des Internets unterscheidet sich der softwaretechnische Schutz vor Cyberterrorismus erst einmal nicht von dem Schutz vor Cyberkriminalität und anderen unerwünschten Aktivitäten im Netzwerk;
- beizutragen zur *Früherkennung* von Verwundbarkeiten, von Angriffen und zur *Vorbereitung* des Krisenmanagements, erfolgreiche Schutzpolitik (best practice) anzuregen und Erfahrungen zu vermitteln; den Aufbau von CERTs oder ISACs auf nationaler und internationaler Ebene anzuregen, die bei Vorsorge- und Krisenmaßnahmen eine wichtige Rolle spielen;
- Planung und Aufbau des nationalen bzw. grenzüberschreitenden *Krisenmanagements*, einschließlich der Durchführung von Übungen mit privaten und staatlichen Netznutzern und -betreibern;
- Schaffung besserer *internationaler* rechtlicher und praktischer *Grundlagen* für Cybersecurity.

Hier steht die Politik erst am Anfang eines beschwerlichen Weges, obwohl, vor allem in Europa, speziell in der EU, durchaus Erfolge zu verzeichnen sind.²⁹⁹ Aber noch immer behandeln Staaten den Schutz kritischer Informationsinfrastrukturen zu oft als

²⁹⁹ Vgl. S. 74ff.

nur nationale Aufgabe, „even though the information infrastructure transcends many boundaries. Whereas many governments have supported national initiatives and policies and have set up new organizations or working groups for dealing with CIIP (Critical Information Infrastructure Protection, W. F.), many obstacles remain to be overcome, especially for an international dialog. Best practices and possible solutions to CIIP challenges vary from country to country and are obviously influenced by historical, geographical, political, organizational, or cultural peculiarities and traditions, as well as by resources at hand.“ (vgl. [Abele-Wigert, 2006, S. 67].

Zur Aufgabe der Politik gehört es auch, immer wieder kritisch zu prüfen, ob der bisherige Ansatz, weitgehend auf staatliche Regulierung und Intervention zu verzichten, vorwiegend kontextbezogen zu agieren und die Privaten, die Betreiber und Nutzer des Netzes, in die hauptsächliche Verantwortung für Cybersecurity zu stellen, bei einer sich verändernden Gefährdungslagen noch angemessen ist.³⁰⁰ Dabei sollte Politik vorausschauend, weniger reaktiv agieren und sich konzeptionell und planerisch auf das Mögliche einstellen. Das Internet, so viele negative Effekte es auch begleiten, entwickelt sich zu einer breit genutzten kritischen Infrastruktur mit hoher Attraktivität, kolossaler Bedeutung und einem großen Nutzen. Deshalb würde es überraschen, wenn eine solche Infrastruktur nicht irgendwann auch zum Ziel von Terroristen würde, die durch Angriffe auf das Netzwerk ihren Zielen ein Stück näher zu kommen hoffen. Es wird kaum gelingen, dieser Gefahr ausweichen. Sie kann nur sorgfältig eingeschätzt werden, und die dann als notwendig erachteten Maßnahmen für Cybersecurity, die von realistischen Analysen über die Sicherheitslage und ihre Perspektiven angeleitet werden, müssen sich der Gefährdung anpassen.

Wohin sich diese Politik für Cybersecurity auch immer entwickelt, welche Rolle dabei die Privaten einnehmen, welche Aufgaben dem Staat zufallen wird mit seinem Instrumentenkasten, darunter seinen sicherheitspolitischen Organen, deren Bedeutung bei einer erkennbaren Gefährdung durch Cyberterrorismus wachsen dürfte - den Nutzen des Internets bekommt nur der, der auch die mit ihm verbundenen Risiken in Kauf nimmt. Internetsicherheit lässt sich nicht vollständig gewährleistet, ebenso wenig wie die `reale` Welt auf völlige Sicherheit hoffen darf, zumindest nicht in dem Sinne, dass gezielte Angriffe immer verhütet und zuverlässig abgewehrt werden können. Ziel der Bemühungen muss eine möglichst weltweite Kultur der Internetsicherheit sein, die Prävention eine größere Wirksamkeit gibt, die Identifikation der Täter und ih-

³⁰⁰ Vgl. S. 109ff.

re Strafverfolgung glaubwürdig verbindet und gute Aussichten schafft, bei Angriffen von Cyberterroristen zu bestehen und unabwendbare Folgen kalkulierbar zu begrenzen.

Cybersecurity bleibt eine Herausforderung, die nur durch gemeinsame Anstrengung aller derer bewältigt werden kann, die ein Interesse an einem sicheren Netzwerk haben, das eine hohe Verfügbarkeit aufweist, die Integrität der Daten, die Vertraulichkeit der Kommunikation sowie die ihre Authentizität sichert. Schneier [2001, S. 6] schreibt: „Network security risks will always be with us. The downside of being in a highly connected network is that we are all connected with the best and worst society. (...) The best we can do is to manage the risks (...).“

Verzeichnis der Literatur

Bücher, Zeitschriften, Dokumente

- ABELE-WIGERT, I. (2006) *Challenges Governments Face in the Field of Critical Information Infrastructure Protection (CIIP): Stakeholder Perspectives*. In ABELE-WIGERT, I., DUNN, M. A. *International CIIP Handbook*, Vol. II, 55-68.
- ABELE-WIGERT, I., DUNN, M. A. (2006) *International CIIP Handbook*, 2 Volumes. Eidgenössische Technische Hochschule Zürich, ETH Zürich; www.crn.ethz.ch/. (ABELE-WIGERT, DUNN I = Vol. 1, ABELE-WIGERT, DUNN II = Vol. 2.).
- ABRAMS, B. (2003) The Dawn of the E-Bomb. *IEEE Spectrum Online*, 11/2003; <http://www.spectrum.ieee.org/archive/1543>.
- ACKERMANN, W. M. (1998) Encryption: a 21st Century National Security Dilemma. *International Review of Law, Computers & Technology*, 12, 371-394.
- ALLISON, G. (2005) Nuclear Accountability. *Technology Review*, July 2005; <http://www.technologyreview.com/Energy/14597/>.
- ALVES, M., DETREZ, C., MARIGHELA, C. (1991) Zerschlagt die Wohlstandsinselfn der Dritten Welt. Mit dem Handbuch des Guerilleros von Sao Paulo. Reinbek bei Hamburg (Rowohlt).
- ANDERSON, R. (2001) Why Information Security is Hard. University of Cambridge, Cambridge, UK; <http://www.acsac.org/2001/papers/110.pdf>.
- ANDERSSON, J. J., MALM, A. (2006) Public-Private Partnership and the Challenge of Critical Infrastructure Protection. In ABELE-WIGERT, I., DUNN, M. A. *International CIIP Handbook*, Vol. II, 139-167.
- ARQUILLA, J., RONFELDT, D. F. (1996) *The Advent of Netwar*. Rand Publications. Santa Monica, CA; www.rand.org/
- ARQUILLA, J., RONFELDT, D. F. (Eds.) (2001) *Networks and Netwars: The Future of Terror, Crime and Militancy*. RAND Netwar Series. Santa Monica, CA.
- BADDELEY, A. (2005) Commercial message. *C⁴ISR Journal*, August 08, 2005, <http://www.c4isrjournal.com/>.
- BANSE, G., KIEPAS, A. (Hrsg.) (2005) *Nachhaltige Entwicklung: Von der wissenschaftlichen Forschung zur politischen Umsetzung*. Berlin, edition sigma.

- BARNETT, M., DUVALL, R. (Eds.) (2005) *Power in Global Governance*. Cambridge/UK 2005, Cambridge University Press.
- BAUDISSIN, W. GRAF von (Hrsg. Bührlé, C., von Rosen, C.) (1982) *Nie wieder Sieg*. München, Piper.
- BECHMANN, G., et al. (2003) *Across the divide. Work, organization and social exclusion in the european information society*. Berlin, edition sigma.
- BECK, K. (2000) Die Zukunft des Internet - aus der Sicht internationaler Experten. *TA-Datenbank-Nachrichten*, 9, 82-86.
- BEDNARSKI, G. M. (2004) *Enumerating and Reducing the Threat of Transnational Cyber Extortion against Small and Medium Size Organizations*. Information-Week, The Heinz Scholl Carnegie Mellon University, Pittsburg; http://i.cmpnet.com/infoweb/1005/IWK_CMU_Cyber_Extortion_Study.pdf.
- BEHRENS, M. (Hg.) (2005) *Globalisierung als politische Herausforderung. Global Governance zwischen Utopie und Realität*. Wiesbaden, VS-Verlag.
- BELLAVITA, Ch. (2005) Changing Homeland Security: The Issue-Attention Cycle. *Homeland Security Affairs*, 1/2005, <http://www.hsaj.org/?fullarticle=2.3.5>.
- BENDRATH, R. (2003) *The American Cyber-Angst and the Real World - Any Link?* In LATHAM, R. (Ed.) *Bombs and Bandwidth: The Emerging Relationship between IT and Security*. New York, Powells, 49-73.
- BITKOM (2005) *Homeland Security. Vernetzte Sicherheit aus der Sicht der deutschen ITK-Industrie*. Berlin, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.; www.bitkom.org/.
- BLANCKE, S. (2005) Information Warfare. *Aus Politik und Zeitgeschichte*, ApuZ 30-31/2005, 24-32.³⁰¹
- BMI (2005) Bundesministerium des Inneren, Schutz Kritischer Infrastrukturen – Basisschutzkonzept. Empfehlungen für Unternehmen www.bmi.bund.de/nr_122688/Internet/Content/Broschueren/2005/Basisschutzkonzept__kritische__Infrastrukturen.html.
- BROCK, L. (2005) Vom „erweiterten Sicherheitsbegriff“ zur globalen Konfliktintervention. *Wissenschaft & Frieden*, 4/2005; <http://www.iwif.de/wf405-24.htm>.

³⁰¹ ApuZ-Artikeln sind zugänglich unter bpb.de/.

- BRÖMMELHÖRSTER, J., FABRY, S., WIRTZ, N. (2003) *Internationale Aktivitäten zum Schutz Kritischer Infrastrukturen*. Bonn, Bundesamt die Sicherheit in der Informationstechnik, BSI; www.bsi.de/fachthem/kritis/paper_studie.pdf.
- BROOKES, P. (2005) *The Art of (Cyber) War*. The Heritage Foundation, Washington D.C.; <http://www.heritage.org/Press/Commentary/ed083005a.cfm>.
- BROWN (2006) A proposal for an international convention to regulate the use of information systems in an armed conflict. *Harvard International Law Journal*, 47, 179-222; <http://www.harvardilj.org/print/73?sn=1>.
- BROWN, T., BEYELER, W., BARTON, D. (2004). Assessing infrastructure interdependencies: the challenge of risk analysis for complex adaptive systems. *International Journal of Critical Infrastructures*, 1, 108-117; <http://www.inderscience.com/browse/index.php?journalID=58&year=2004&vol=1&issue=1>.
- BRÜCK, T., SCHUMACHER, D. (2004). Die wirtschaftlichen Folgen des internationalen Terrorismus. *Aus Politik und Zeitgeschichte*, ApuZ 3-4/2004, 41-46.
- BSI (2005) *Die Lage der IT-Sicherheit in Deutschland 2005*. Bonn, Bundesamt für Sicherheit in der Informationstechnik; www.bsi.de/literat/lagebericht/index.htm.
- BYRES, E. P., LOWE, J. (2004) *The Myths and Facts behind Cyber Security Risks for Industrial Control Systems*. British Columbia Institute of Technology, Burnaby, Australia & PA Consulting Group, London, UK; http://www.tswg.gov/tswg/ip/The_Myths_and_Facts_behind_Cyber_Security_Risks.pdf.
- CARTER, A. B., DEUTCH, J., ZELNIKOW, P. (1998) Catastrophic Terrorism: Tackling the New Danger. *Foreign Affairs*, 77, 80-94.
- CASHELL, B. et al. (2004) *The economic impact of cyber-attacks*. CRS Report for Congress, Congressional Research Service, Washington D.C.; http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf.
- CASTELLS, M. (Ed.) (2004) *The network society: a cross-cultural perspective*. Cheltenham u. a., Edward Elga.
- CERT/CC (2003) *Overview. Incident and Vulnerability Trends*. Software Engineering Institute, Carnegie Mellon University, Pittsburgh; www.cert.org/.
- CISP (2004) *EAPC/PfP Workshop on Critical Infrastructure Protection & Civil Emergency Planning: Dependable Structures, Cybersecurity and Common Stan-*

- dards*. Zurich, Switzerland, 9-11 September 2004, Center for International Security Policy; www.eda.admin.ch/international_security.
- CLARK, D. (2003) Computer security officials discount chances of 'digital Pearl Harbor'. *National Journal's Technology Daily*, 6/3/2003; <http://www.govexec.com/dailyfed/0603/060303td2.htm>.
- CLINEHENS, H. A. (2000) Aum Shinrikyo and Weapons of Mass Destruction. A Case Study. Air Command and Staff College, Air University, Maxwell Air Force Base, Alabama; <https://research.maxwell.af.mil/papers/ay2000/acsc/00-040.pdf>.
- COENEN, R., GRUNWALD, A., (Hrsg.) (2003) *Nachhaltigkeitsprobleme in Deutschland. Analyse und Lösungsstrategien*. Berlin 2003, edition sigma.
- COMMISSION (1996) *Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Service*. European Commission COM(96)483 final, Brussels, 16.10.1996; <http://europa.eu.int/>.
- COMMISSION (1996a) *Communication on Illegal and Harmful Content of the Internet*. European Commission COM(96)487, Brussels, 16.10.1996; <http://europa.eu.int/>.
- COMMISSION (2001) *Network and Information Security: Proposal for a European Policy Approach*. Communication from the Commission COM(2001) 298 final; <http://europa.eu.int/>.
- COMMISSION (2002) *Folgemaßnahmen zum mehrjährigen Aktionsplan der Gemeinschaft zur Förderung der sicheren Nutzung des Internet durch die Bekämpfung illegaler und schädlicher Inhalte in globalen Netzen*. Mitteilung der Kommission der Europäischen Union KOM(2002) 152 endg..
- COMMISSION (2003) *Towards a knowledge based Europe. The European Union and the information society*. European Commission, Brussels 2003.
- COMMISSION (2004) *Critical Infrastructure Protection in the fight against terrorism*. Commission of the European Communities, Communication from the Commission to the Council and the European Parliament. Brussels, 20.10.2004, COM(2004) 702 final..
- COMMISSION (2005) *Green Paper on a European Program for Critical Infrastructure Protection*. Commission of the European Communities. Brussels, COM(2005) 576 final..

- CONVENTION (2001) *Convention on Cybercrime*. Council of Europe, Budapest 2001
<http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.
- CONWAY, M. (2006) Terrorism and the Internet. *New Media – New Threat? Parliamentary Affairs*, 59, 283-298
- CONWAY, M. (2005) *Terrorist ,use' of the Internet and fighting back*. Paper presented at Safety & Security in a Networked World: Balancing Cyber-Rights & Responsibilities. Oxford; <http://www.oii.ox.ac.uk/microsites/cybersafety/?view=papers>.
- CREVELD, VAN, M. (1989) *Technology and War: from 2000 B.C. to the Present*. New York 1989, The Free Press.
- CRONIN, A. K. (2003) Behind the Curve. Globalization and International terrorism. *International Security*, 27, 30-58.
- CSI/FBI (2005): Computer Security Institute/Federal Bureau of Investigation, *Computer Crime and Security Survey 2005.*, San Francisco, CA; <http://www.gocsi.com/> oder www.fbi.gov.
- CSI/FBI (2004): Computer Security Institute/Federal Bureau of Investigation, *Computer Crime and Security Survey 2004.*, San Francisco, CA; <http://www.gocsi.com/> oder www.fbi.gov.
- CSIA (2005) Cyber Security Industry Alliance, *National Agenda for Information Security in 2006*. Arlington, VA; www.csialliance.org/.
- CYBERSECURITY (2005) *Cyber Security: A Crisis of Prioritization. Report to the President*. President's Information Technology Advisory Committee. Arlington/VA; http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.
- CYBERSECURITY (2002) *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*. Computer Science and Telecommunications Board, National Research Council, Washington D.C.; <http://csrc.nist.gov/>.
- DALGAARD-NIELSEN, A. (2004) *Homeland Security. American and European responses to September 11th*. In PILEGAARD, J. (Ed.) *The politics of European security*. Danish Institute for International Studies. Copenhagen, 159-178; http://www.diis.dk/graphics/Publications/Books2004/jpi_eurosecurity.pdf.
- DENNING, D. E. (1999) *Information Warfare and Security*. Reading/MA, ACM Press (Addison-Wesley).

- DENNING, D. E (2000) *Cyberterrorism*. Georgetown University, Washington D.C.; <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>.
- DiMAGGIO, P. et al. (2001) Social Implications of the Internet. *Annual Review of Sociology*, 27, 307-336.
- DoD, DEPARTMENT OF DEFENSE (2006) Department of Defense, Annual Report to Congress: Military Power of the People's Republic of China 2006. Washington, D.C.; <http://www.defenselink.mil/pubs/china.html>.
- DoD DEPARTMENT OF DEFENSE (2005) *Strategy for Homeland Defense and Civil Support*. Department of Defense. Washington D.C.; www.defenselink.mil/.
- DIETL, W.; HIRSCHMANN, K., TOPHOVEN, R. (2006) *Das Terrorismus-Lexikon: Täter, Opfer, Hintergründe*. Frankfurt/M, Eichborn.
- DoS (2005) *Country reports on Terrorism 2004*. Department of State. Washington D.C.; www.state.gov/.
- DÜBENDORFER, T., WAGNER, A., PLATTNER, B. (2004) *An Economic Damage Model for Large-Scale Internet Attacks*. 13th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises, Modena, Italy; http://www.tik.ee.ethz.ch/~ddosvax/publications/papers/WETICE-ES-duebendorfer-economic_damage_model.pdf.
- DUNN, M., MAUER, V. (2006) Towards a Global Culture of Cybersecurity. In ABELE-WIGERT, I., DUNN, M. A. *International CIIP Handbook*, Vol. II, 191-206.
- DUNN, M. (2006) *Understanding Critical Information Infrastructures: An Elusive Quest*. In ABELE-WIGERT, I., DUNN, M. A. *International CIIP Handbook*, Vol. II, 27-53.
- DUNN, M. (2005) *A comparative analysis of cybersecurity initiatives worldwide*. International Telecommunication Union (ITU). Geneva; http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf.
- DUNN, M., WIGERT, I. (2004) *Critical Information Infrastructure Protection. International CIIP Handbook 2004*, Edited by A. Wenger/J. Metzger. ETH, Zürich; http://cms.isn.ch/public/docs/doc_454_290_en.pdf.
- DYNES, S., ANDRIJICIC, E., JOHNSON, M. E., 2006, Costs to the U.S. Economy of Information Infrastructure Failures: Estimates from Field Studies and Economic Data. Paper presented at The Fifth Workshop on the Economics of In-

- formation Security (WEIS 2006), University of Cambridge, England;
<http://weis2006.econinfosec.org/prog.html>
- DYSON, E. (2005) Das zuverlässige Netz. *Aus Politik und Zeitgeschichte*, ApuZ 30-31/2005, 3-6.
- E.O. 13010 (1996) *Executive Order 13010, Critical Infrastructure Protection*. Washington D.C.; <http://www.fas.org/irp/offdocs/eo13010.htm>.
- ECKERT, C. (2004) *IT-Sicherheit. Konzepte-Verfahren-Protokolle*. München Wien. Oldenbourg.
- EINEMANN, E. (2006) *Das Internet in Deutschland. Differenzierungen, Spaltungen, Kopplungen*. Marburg, Schüren.
- ELSEA, J. (2003) The Posse Comitatus Act and Related Matters: A Sketch. Congressional Research Service, Report for Congress, Updated May 19, 2003. CRS, Washington, D.C.; <http://www.thememoryhole.org/crs/more-reports/RS20590.pdf>.
- ERHARD, D. G. (2004) Standing in the Strategic Bandwidth Gap: A View of Military Communications in 2012. *Air, Space Power Chronicles*, 9 March 2004; <http://www.airpower.maxwell.af.mil/airchronicles/cc/ehrhards.html>.
- FARRELL, A. E., ZERRIFFI, H., DOWLATABADI, H. (2004) Energy Infrastructure and Security. *Ann. Rev. Environm. Resour.*, 29, 421-469; <http://arjournals.annualreviews.org/doi/pdf/10.1146/annurev.energy.29.062403.102238?cookieSet=1>.
- FBI, FEDERAL BUREAU OF INVESTIGATIONS (2006) Computer Crime Survey, Houston; <http://houston.fbi.gov/pressrel/2006/ho011906.htm>.
- FISCHER, W., LEPPERHOFF, N. (2004) *Wie verwundbar ist das Internet?* In von KNOP, J., FRANK, H. (Hrsg.) *Netz- und Computersicherheit*. Bielefeld, Bertelsmann, 209-230.
- FISCHER, W., LEPPERHOFF, N. (2005) Can critical infrastructures rely on the Internet? *Computers & Security*, 24, 485-491; http://www.elsevier.com/wps/find/journaldescription.cws_home/405877/description#description.
- FISCHER, W., LEPPERHOFF, N., VOLST, A. (2003) *Internet under Threat. Simulation of Survivability with INESS*. In GRIMM, R., KELLER, H. B., RANNENBERG, K. (Eds.) *Informatik 2003: Mit Sicherheit Informatik*. Lecture

- Notes in Informatics (LNI), Series of the German Informatics Society (GI). Bonn, 45-56; www.gi-ev.de/.
- FISHER, D. (2005) Researchers to tackle SCADA Security. *EWeek.com.*, 3/4/2005; <http://www.eweek.com/article2/0,1759,1772610,00.asp?kc=EWRSS03129TX1K0000614>.
- FOLSCHEID, A. (2001) *Terrorismus und Guerilla: Versuch einer Begriffserklärung*. EIKon Diskussionspapier 2/01. Saarbrücken; http://www.uni-saarland.de/fak3/fr31/praxis/fols/per_fol_ver.htm.
- FONASH, P. M. (2005) *Terrorism and the EMP Threat to Homeland Security*. Statement before the United States Senate Committee on the Judiciary. Subcommittee on Terrorism, Technology, and Homeland Security. Washington, D.C.; http://kyl.senate.gov/legis_center/subdocs/030805_fonash.pdf.
- FOSTER, J. S. et al. (2004) *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack*. Alexandria, VA; http://www.globalsecurity.org/wmd/library/congress/2004_r/04-07-22emp.pdf.
- FOX, S., ANDERSON, J. Q., RAINIE, L. (2005) *The Future of the Internet*. Pew Internet & American Life Project. Washington, D.C.; http://www.pewinternet.org/PPF/r/145/report_display.asp.
- FLYNN, St. E. (2004) The Neglected Home Front. *Foreign Affairs*, 83; <http://www.foreignaffairs.org/20040901faessay83504/stephen-e-flynn/the-neglected-home-front.html>.
- FLYNN, St. E. (2004a) *America the Vulnerable*. New York, HarperCollins.
- FREEMAN, M., DYNES, S., GOLODNER, A. (2005) *The Known Unknown of Cyber Security and Cyber terrorism*. Version April 2005. Institute for Security Technology Studies. Hanover NH; <http://www.ists.dartmouth.edu/library/119.pdf>.
- FRIEDMAN, T. L. (2005) *The World is Flat. A Brief History of the Twenty-First Century*. New York, NY, Farrar, Straus and Giroux; www.fsgbooks.com/.
- GANSWINDT, T., HEISKEL, D., SCHLÄFFER, C. (2005) *Wirtschaftliche und politische Chancen der Informationsgesellschaft*. Boston Consulting Group (BCG), Deutsche Telekom und Siemens Communications (Com); http://download-dtag.t-online.de/deutsch/aktuelles/051214_ICT-Studie.pdf.

- GAO (2004) *Cybersecurity for Critical Infrastructure Protection*. United States Government Accountability Office, Technology Assessment. Washington D. C.; <http://www.gao.gov/cgi-bin/getrpt?GAO-04-321>.
- GAO (2004a) *Defense Acquisitions. The Global Information Grid and Challenges Facing Its Implementation*. United States Government Accountability Office, Technology Assessment. Washington D.C.; <http://www.gao.gov/new.items/d04858.pdf>.
- GARRETSON, C., MESSMER, E. (2006) It's raining IT security surveys. *TechWorld*, 3/20/2006; <http://www.techworld.com/security/features/index.cfm?FeatureID=2350>.
- GEER, D. et al. (2003) *CyberInsecurity: The Cost of Monopoly*. Computer & Communications Industry Association. Washington D.C.; <http://www.ccianet.org/filings/cybersecurity/cyberinsecurity.pdf>.
- GEIGER, G. (Hg.) (2000) *Sicherheit der Informationsgesellschaft*. Baden-Baden, Nomos.
- GELBSTEIN, E., KAMAL, A. (2002) *Information Insecurity*. A survival guide to the uncharted territories of cyber-threats and cyber-security. New York, United Nations ICT Task Force & the United Nations Institute for Training and Research.
- GERBER, CH. (2005) Converging on Network Security. *Military Information Technology Online Edition*, 9; <http://www.military-information-technology.com/article.cfm?DocID=384>.
- GHEORGHE, A. V. (2003) Risks, sustainability and governance: a new landscape for critical infrastructures. *International Journal of Critical Infrastructure*, 1, 118-124; <https://www.inderscience.com/browse/index.php?journalID=58>.
- GIBSON, W. (2001) *Neuromancer*. München¹¹, Heyne.
- GLOBAL TRENDS 2015 (2000) *Global Trends 2015 - A Dialogue About the Future With Nongovernment Experts*. National Intelligence Council (NIC). Washington D.C.; www.cia.gov/.
- GORDON, S., FORD, R. (2002) Cyberterrorism. *Computers & Security*, 21, 636-647; http://www.elsevier.com/wps/find/journaldescription.cws_home/405877/description#description.

- GORMAN, S. P. (2003) *Is there a Cybersecurity threat to national security: An interpretative analysis*. George Mason University. Fairfax/Virginia; http://policy.gmu.edu/imp/research/Cyber_threat_paper.pdf.
- GORMAN, S. P. et al. (2003) *The Revenge of Distance: Vulnerability Analysis of Critical Information Infrastructure*. George Mason University. Fairfax/Virginia; <http://arxiv.org/ftp/cond-mat/papers/0310/0310427.pdf>.
- GORMAN, S. P., MALECKI, E. J. (2000) The networks of the Internet: an analysis of provider networks in the USA. *Telecommunication Policy*, 24, 113-134; www.elsevier.com/.
- GRABOWSKY, P. (2004) The global Dimension of Cybercrime. *Global Crime*, 6, 146-157; <http://taylorandfrancis.metapress.com>.
- GREEN, J. (2002) The Myth of Cyberterrorism. *Washington Monthly*, November 2002; www.washingtonmonthly.com/.
- GRIMM, R (2005) *Digitale Kommunikation*. München. Oldenbourg.
- GRUBESIC, T. H., MURRAY, A. T. (2005) Spatial-historical landscapes of telecommunication network survivability. *Telecommunication Policy*, 29, 801-820; www.elsevier.com/.
- GUSY, C., SCHEWE, C. S. (2003) Polizeiliche und justizielle Zusammenarbeit. In WEIDENFELD, W., WESSELS, W. (Hrsg.) *Jahrbuch der Europäischen Integration 2002/2003*. Bonn, 185-192. Europa-Union-Verlag.
- HAFNER, D. (1999) *Analyse der Auswirkungen neuer Organisationsformen auf die Anforderungen an die Sicherheitskultur eines Unternehmens*. Diplomarbeit am Institut für Informatik der Universität Zürich; http://arvo.ifi.unizh.ch/events/SIS/SIS2000/misc/DA_Hafner.pdf.
- HAFTENDORN, H. (1991) The Security Puzzle: Theory-Building and Discipline-Building. *International Studies Quarterly*, 35, 3-17.
- HAGER, W. (1976) Westeuropas wirtschaftliche Sicherheit. Arbeitspapiere zur Internationalen Politik. Europa Union Verlag, Bonn.
- HAIMES, Y., LONGSTAFF, T. (2002) The role of risk analysis in the protection of critical infrastructures against terrorism. *Risk Analysis*, 22, 439-444; www.blackwell-synergy.com.

- HAKE, J.-Fr., SCHLÖR, H. (2003) The Asymmetry of Sustainable Development and their Consequences. *World Resources Review*, 15, 498-517; www.globalwarming.net.
- HARRISS-WHITE, B. (Ed.) (2002) *Globalization and Insecurity: Political, Economic and Physical Challenges*. Hampshire New York, Palgrave.
- HEINRICH BÖLL STIFTUNG (Hg.) (2001) *Rüstungskontrolle im Cyberspace*. Dokumentation einer Internationalen Konferenz der Heinrich-Böll-Stiftung am 29/30. 6. 2001. Berlin; <http://www.boell.de/>.
- HEISE (2002) Tausende Spanier nach Sabotage-Aktion ohne Telefon. *Heise Online* <http://www.heise.de/newsticker/data/gr-15.06.02-003/>.
- HENNESSY, J. L., PATTERSON, D. A., LIN, H. S. (2003) *Information Technology for Counterterrorism*. National Research Council, Computer Science and Telecommunications Board. Washington, D.C., The National Academies Press; www.nap.edu.
- HOCH, M. (2001) Krieg und Politik im 21. Jahrhundert. *Aus Politik und Zeitgeschichte*, APuZ 20/2001, 17-25.
- HOFFMANN, B. (2001) *Terrorismus - der unerklärte Krieg*. Frankfurt/M (Fischer).
- HOMER-DIXON, T. (1991) On the Threshold: Environmental Changes as Causes of Acute Conflict. *International Security*, 16, 76 -116.
- HOMER-DIXON, T. (2002) The Rise of Complex Terrorism. *Foreign Policy*, January/February; http://www.homerdixon.com/download/rise_of_complex_terrorism.pdf.
- HUNDLEY, R. et al. (2001) *The Future of the Information Revolution in Europe*. Conference Proceedings. RAND, Santa Monica CA; www.rand.org/publications/CF/CF172/.
- HUTTER, R. (2004) *Wie lassen sich offene und hoch technologisierte Gesellschaften schützen? Das Beispiel "Cyber-Terror"*. In WEIDENFELD, W. (Hg.) *Herausforderung Terrorismus*, 173-196.
- INSIDER THREAT STUDY (2005): *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*. United States Secret Service & Software Engineering Institute Carnegie Mellon University Pittsburgh; <http://www.cert.org/archive/pdf/insidercross051105.pdf>.
- INTERNET (2005) Internet Macht Politik. *Welttrends*, 13, www.welttrends.de/.

- INTERNET GOVERNANCE (2004) *Internet Governance: The State of the Play*. The Internet Governance Project. Syracuse University, Atlanta & Wissenschaftszentrum Berlin für Sozialforschung; www.InternetGovernance.org.
- ISENSEE, J. (1983) *Das Grundrecht auf Sicherheit. Zu den Schutzpflichten des freiheitlichen Verfassungsstaates*. Berlin u.a., de Gruyter.
- ISS, INTERNET SECURITY SYSTEMS (2006) *SCADA Security and Terrorism: We're not crying wolf*. Atlanta 2006; <http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf>.
- ITU (2005) International Telecommunication Union. *World Telecommunication Indicators 2004/2005 edition*. ITU Geneva; <http://www.itu.int>.
- ITU (2005a) International Telecommunication Union. *Trends in Telecommunication Reform. Regulating in the broadband world*. 6th Edition 2004-2005. ITU Geneva.
- JACKSON, W. (2006) What happens when the Net is attacked?. *Government Computer News*, 7/24/06, http://www.gcn.com/print/25_21/41399-1.html?topic=security.
- JACKSON, W. (2004) Motives, methods of hackers are changing. *Government Computer News*, March 29; http://www.gcn.com/vol1_no1/daily-updates/25404-1.html.
- JANTSCH, S. (2000) *Die Bedrohung der nationalen Informationsinfrastruktur und mögliche Auswirkungen auf den Einsatz*. In GEIGER, G. (Hg.) *Sicherheit der Informationsgesellschaft*. Baden-Baden, Nomos, 27-133.
- JENSEN, E. T. (2002) Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense. *Stanford Journal of International Law*, 38, 207-240; <http://sjil.stanford.edu/>.
- JOCHIMSEN, R. (1966) *Theorie der Infrastruktur*. Tübingen, Mohr.
- JORDAN, T., TAYLOR, P. A. (2004) *Hackivism and Cyberwars: Rebels with a Cause?*. London, Routledge.
- KAPLAN, E. (2006) Tracking Down Terrorist Financing. Council on Foreign Relations; New York/Washington, DC; www.cfr.org/.
- KATZ, R. (2003) *Die Terroristenjägerin. Wie ich das Netzwerk des islamistischen Terrors aufdeckte*. München (C. Bertelsmann).

- KEEFE, P. R. (2006) Der globale Lauschangriff. *Aus Politik und Zeitgeschichte*, ApuZ 42/2003, 24-31.
- KEEN, A. (2006) The second generation of the Internet has arrived. It's worse than you think. *The Weekly Standard*, 2/15/2006; www.weeklystandard.com/.
- KEITH, S. (2005) *Fear-mongering or fact: The construction of 'cyber-terrorism' in the U.S, U.K. and Canadian news media*. Paper presented at Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities. Oxford/England; <http://www.oii.ox.ac.uk/microsites/cybersafety/?view=papers>.
- KELLE, A., SCHAPER A. (2003) *Terrorism using biological and nuclear weapons: a critical analysis of risks after 11 September 2001*. Frankfurt am Main, Peace Research Institute; <http://www.hsfk.de/downloads/prifrep64.pdf>.
- KERR, K. (2003) Putting cyberterrorism into context. *AusCERT Member Newsletter*, 7. The University of Queensland, Brisbane; <http://national.uscert.org.au/render.html?it=3552>.
- KLEINWÄCHTER, W. (2005) Erbsenzählen nach der Cyberschlacht. *Telepolis*, 24.11.2005; www.heise.de/.
- KLEINWÄCHTER, W. (2004) *Macht und Geld im Cyberspace*. Hannover, Heise; <http://www.dpunkt.de/buch/3-936931-22-4.html>.
- KLOTZ, K. (2005) Software ohne Fehl und Tadel. *Technology Review*, 21.6.2005; www.heise.de/.
- KNOP, J. von, FRANK, H. (Hrsg.) (2004) *Netz- und Computersicherheit*. Bielefeld, Bertelsmann.
- KNOP, K. von (Hg.) (2005) *Countering Modern Terrorism. History, Current Issues and Future Threats*. Bielefeld, Bertelsmann.
- KÖTTER, W. (2002) Anwendung oder Nichtanwendung von Kernwaffen? *Welt-Trends*, 35, 86-102; http://opus.kobv.de/ubp/volltexte/2006/947/pdf/35_sp_koetter.pdf.
- KOPFMÜLLER, J. (Hg.) (2003) *Den globalen Wandel gestalten - Forschung und Politik für einen nachhaltigen globalen Wandel*. Berlin, edition sigma; <http://www.itas.fzk.de/>.
- KOTADIA, M. (2005) Critical infrastructure vulnerability for next 20 years. *ZDNet Australia*, July 21, 2005, <http://www.zdnet.com>.

- KREMER, B. (1966) Die Kunst zu überleben. Zivilverteidigung in der Bundesrepublik. München, Osang.
- KREMPL, S. (2004) terror.web. c` t 16/2004; <http://www.heise.de/>.
- KREY, V., MARKEWITZ, P., VÖGELE. S. (2005) Energietransport und -verteilung. *BWK*, 57, 49-57; <http://www.eBWK.de>.
- KRÖGER, D., GIMMY, M. A. (Hrsg.) (2002) *Handbuch zum Internetrecht. Electronic Commerce, Informations-, Kommunikations- und Mediendienste*. Berlin u.a., Springer 2002²; <http://www.jurawelt.com/literatur/medienrecht/7334>.
- KRÜGER, A. (2005) Im Pentagon regiert der Konjunktiv. *Telepolis*, 29.8.2005; <http://www.heise.de/>.
- KUMLER, E. (2004) Terrorists rely on Tech Tools. *PC World*, 7.7.2004; <http://www.pcworld.com/>; <http://www.siteinstitute.org/index.asp>.
- LABOVITZ, C. et al. (1999) *Experimental Study of Internet Stability and Wide-Area Backbone Failures*. Ann Arbor, Michigan; <http://www.eecs.umich.edu/techreports/cse/1998/CSE-TR-382-98.pdf>.
- LANGHEINRICH, M., MATTERN, F. (2003) Digitalisierung des Alltags. *Aus Politik und Zeitgeschichte*, ApuZ 42/2003, 6-12.
- LAQUEUR, W. (2004) *Krieg dem Westen: Terrorismus im 21. Jahrhundert*. Berlin, Ullstein.
- LEGGATE, J. S. (2005) *Business Concerns for the Internet*. Hearing before the Committee on Science. U.S. House of Representatives. Washington, D.C.; <http://gop.science.house.gov/hearings/full05/sept15/Leggate%20written%20testimony%20final.pdf>.
- LEIB, V. (2003) *ICANN und der Konflikt um die Internet-Ressourcen*. Dissertation, Universität Konstanz, 312 Seiten; Konstanzer Online-Publikations-System, www.volker-leib.de/.
- LEIBFRITZ, W. (2004). Auswirkungen des Terrorismus auf die Volkswirtschaften und die Wirtschaftspolitik. *Aus Politik und Zeitgeschichte*, ApuZ 3-4/2004, 47-54.
- LEYDEN, J. (2005) Cybercrime 'more lucrative' than drugs. *The Register*, 29th November 2005; www.theregister.co.uk/.

- LEPPERHOFF, N., FISCHER, W. (2004) *The Internet in Germany. Atlas of Providers and Regions*. Schriften des Forschungszentrums Jülich, Jülich; <http://wwwzb.zb.kfa-juelich.de/publikationen/schriftreihe.asp?Schriftreihe=45>
- LEPPERHOFF, N., FISCHER, W (2004a) Internet Monitoring. Einfaches Erkennen von Störungen. *Informatik Spektrum*, Juni 2004, 238-247; www.springer.com/.
- LEPPERHOFF, N., FISCHER, W, Volst, A. (2002) *Simulation of Internet failures with INESS*. In Proceedings of the IADIS International Conference WWW/Internet 2002. Lissabon, IADIS Press, 276-282; www.iadis.org/.
- LETTICE, J. (2005) U K police chiefs seek powers to attack terror web sites. *The Register*, 23rd July 2005; www.theregister.co.uk/.
- LEVENTHAL, T. (2004) Homeland Security official urges prudent cyber approach. *Govexec.com*, April 13, 2004; www.govexec.com/.
- LEWIS, J. A. (2002) *Assessing the Risk of Cyber Terrorism, Cyber War and Other Cyber Threats*. Center for Strategic & International Studies. Washington, DC; http://www.csis.org/component/option,com_csis_experts/task,view/id,111/.
- LEWIS, J. A. (2005) Aux armes, citoyens: Cyber security and regulation in the United States. *Telecommunications Policy*, 29, 821-830; www.elsevier.com/.
- LEWIS, J. A. (2005a) *The Internet and Terrorism*. Center for Strategic & International Studies. Washington, D.C.; http://www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf.
- LEYDEN, J. (2005) Cost of US cyber attacks plummets. *The Register*, 18th July 2005; <http://www.theregister.co.uk/>
- LIBICKI, M. C. (1995) *What Is Information Warfare?* Springfield, Va, National Defense University; Text unter: <http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA367662&Location=U2&doc=GetTRDoc.pdf>
- MAKARENKO, T. (2004) The Crime-terror Continuum: Tracing the Interplay between Transnational Organised Crime and Terrorism. *Global Crime*, 6, 129-145; http://www.silkroadstudies.org/new/docs/publications/Makarenko_GlobalCrime.pdf.
- MATAI, D. K. (2005) *Cyberland Security: Organized Crime, terrorism and the Internet*. Oxford Internet Institute, University of Oxford. Oxford/UK; http://www.oii.ox.ac.uk/collaboration/lectures/20050210_matai_speech_v1.0_web.pdf.

- MAXWELL, B. (Ed.) (2004) *Homeland Security: a documentary History*. Washington, D.C., CQ Press; <http://www.cqpress.com/product/Homeland-Security-A-Documentary-History.html>.
- MCAFFEE (2005) *Virtual Criminology Report*. McAfee, Santa Clara CA; http://brief.weburb.dk/archive/00000156/01/UK_McAfee_report.pdf.
- MESSMER, E. (2002) President's advisor predicts cybercatastrophes unless security improves. *Network World*, August 7, 2002; www.networkworld.com/.
- MESSMER, E. (2003) Security Experts: Insider threat loom largest. *NetworkWorld Fusion*, December 8, 2003; www.nwfusion.com.
- METZGER, J. (2004) Das Konzept „Schutz kritischer Infrastrukturen“ hinterfragt. *Bulletin 2004 zur schweizerischen Sicherheitspolitik*; Forschungsstelle für Sicherheitspolitik der ETH Zürich. Zürich; http://www.crn.ethz.ch/publications/crn_team/detail.cfm?lng=en&id=6802.
- METZGER, J. (2004a) *An Overview of Critical Infrastructure Protection (CIP): A Critical Appraisal of a Concept*. Workshop on Critical Infrastructure Protection and Civil Emergency Planning: Dependable Structures, Cybersecurity and Common Standards, organised by the Governments of Switzerland and Germany; Zürich; <http://www.crn.ethz.ch/about/milestones/2004.cfm>.
- MILES, H. (2005) *Al-Dschasira. Ein arabischer Nachrichtensender fordert den Westen heraus*. Hamburg, Europäische Verlagsanstalt.
- MILLER, T. (2002) *Rating the Enemy: "How to identify the enemy"*. The SANS Institute, Bethesda, Maryland; http://koot.biz/docs/overig/how_to_identify_the_enemy.html.
- MINKWITZ, O. (2003) *Ohne Hemmungen in den Krieg? Cyberwar und die Folgen*. Hessische Stiftung für Friedens- und Konfliktforschung, HSK-Report 10/2003. Frankfurt/M.; www.hsfk.de/.
- MOJERT, C. (2001) *Electromagnetic weapons*. In Heinrich-Böll-Stiftung (Hg.) *Rüstungskontrolle im Cyberspace*. Dokumentation einer Internationalen Konferenz der Heinrich-Böll-Stiftung am 29/30. 6. 2001. Berlin, Heinrich-Böll-Stiftung; www.boell.de/.
- MONAR, J. (2004) *Die EU und die Herausforderung des internationalen Terrorismus*. In WEIDENFELD, W. (Hg.) *Herausforderung Terrorismus*, 136-172.

- MONTALBANO, E. (2006) *Cybercrime concerns affecting Net use*. *Techworld*, 1/26/06; www.techworld.com/.
- MOREL, B (2006) *A Methodology for Measuring the Capabilities to Counter Cyber-security-related offences*. Paper presented WSIS Action Line Facilitation Meeting: Building confidence and security in the use of ICTs (C5) Partnerships for Global Cybersecurity, 15 – 16 May 2006, ITU, Geneva; <http://www.itu.int/osg/spu/cybersecurity/2006/presentations/morel-methodology-for-measuring-16-may-2006.pdf>.
- MOTEFF, J., COPELAND, C., FISCHER, J. (2003) *Critical Infrastructures: What makes a Critical Infrastructure Critical?* Congressional Research Service, Washington, D. C; <http://www.fas.org/irp/crs/RL31556.pdf>.
- [MUELLER, 2004] False Sense of Insecurity? *Regulation*, Fall 2004; www.cato.org/pubs/regulation/regv27n3/v27n3-5.pdf.
- MÜNKLER, H. (2002) *Die „neuen“ Kriege*. Hamburg, Rowohlt; www.rowohlt.de/.
- MÜNKLER, H. (2004) *Ältere und jüngere Formen des Terrorismus*. In WEIDENFELD, W. (Hg.) *Herausforderung Terrorismus*, 29-43.
- MUSHARBASH, Y. (2005) Neues Betriebssystem für Al-Qaida. *Internationale Politik (IP)*, 60, 22-27; www.internationalepolitik.de/.
- (N)ONLINER ATLAS (2006) *(N)onliner Atlas 2006*. tns Infratest Bielefeld, initi@tive.d21; <http://www.nonliner-atlas.de/>.
- (N)ONLINER ATLAS (2005) *(N)onliner Atlas 2005*. tns Infratest.; www.nonliner-atlas.de/.
- NPSI (2005) *Nationaler Plan zum Schutz der Informationsinfrastrukturen*, Hg.: Bundesministerium des Innern. Berlin; www.bmi.bund.de/.
- NRC (2003) *The Internet under Crisis Conditions. Learning from September 11*. National Research Council. Washington, D.C., The National Academies Press; <http://www.nap.edu/books/0309087023/html/>.
- NRC (1999) *Funding a Revolution: Government Support for Computing Research*. National Research Council, Computer Science and Telecommunications Board. Washington D.C., The National Academies Press; <http://books.nap.edu/books/0309062780/html/>.

- OECD (2002) *Measuring the Information Economy 2002*. Organisation for Economic Co-Operation and Development. Paris; <http://www.oecd.org/dataoecd/16/14/1835738.pdf>.
- OECD (2002a) *OECD Guidelines for the Security of Information Systems and Networks*. Organisation for Economic Co-Operation and Development. Paris; <http://www.oecd.org/dataoecd/16/22/15582260.pdf>.
- OECD, (2005) *OECD Communications Outlook 2005*. Organisation for Economic Co-Operation and Development. Paris; http://www.oecd.org/document/15/0,2340,en_2649_201185_35269391_1_1_1_1,00.html.
- OERTEL, B., WÖLK, M. (2006) Anwendungspotenziale „intelligenter“ Funktetiketten. *Aus Politik und Zeitgeschichte*, ApuZ 5-6/2006, 16-23.
- von OERTZEN, J., CUHLS, K., KIMPELER, S. (2006) *Wie nutzen wir Informations- und Kommunikationstechnologien im Jahre 2020?* Ergebnisse einer Delphi-Befragung. FAZIT-Schriftenreihe, Forschungsbericht / Band 3. MFG Stiftung Baden-Württemberg; http://www.fazit-forschung.de/fileadmin/_fazit-forschung/downloads/FAZIT-Delphi_Band3.pdf.
- OWEN, T. (2004) Human Security - Conflict, Critique and Consensus: Colloquium Remarks and a Proposal for a Threshold-Based Definition. *Security Dialogue*, 35, 373-387
- PALM, G., RÖTZER, F. (Hrsg.) (2002) *MedienTerrorKrieg: Zum neuen Kriegsparadigma des 21. Jahrhunderts*. Hannover, Telepolis; www.dpunkt.de/.
- PARKER, T. et al. (2004) *Cyber Adversary Characterization: Auditing the Hacker Mind*. Sebastopol, CA, Syngress Publishing; <http://syngress.oreilly.com/>.
- PARKER, T., DEVOST, M. (2005) *Characterising the threats to our nations information system*. BlackHat Federal 2006; <http://blackhatbriefings.com/presentations/bh-federal-06/BH-Fed-06-Parker-Devost-up.pdf>.
- PARKER, M. (2003) *Threat Assessment and Cyberterrorism*. BlackHat, Seattle, WA; <http://blackhatbriefings.com/presentations/bh-usa-03/bh-us-03-parker.pdf>.
- PATRIOTIC ACT (2001) *Patriotic Act, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*, Section 1016(e). Washington, D.C; Text: [http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3162.ENR](http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3162.ENR;); www.epic.org/privacy/terrorism/usapatriot/.

- PAZ, R. (2002) *Tangled web: international networking of the Islamist struggle*. Washington Institute for Near East Policy. Washington, D.C.; <http://www.washingtoninstitute.org/templateC05.php?CID=1501>.
- PCCIP (1997) *Critical Foundations: Protecting America's Infrastructures*. President's Commission on Critical Infrastructure Protection. Washington D.C.; <http://www.fas.org/sgp/library/pccip.pdf>.
- PILAT, D. (2004) *The ICT Productivity Paradox: Insights from Micro Data*. Organisation for Economic Co-Operation and Development, OECD Economic Studies No. 38; Paris; <https://www.oecd.org/dataoecd/15/54/35028181.pdf>.
- PITAC (2005) *Cyber Security: A Crisis of Prioritization*. President's Information Technology Advisory Committee, Arlington, VA.; http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.
- POHLMANN, N. (2005) *Internetstatistiken*. CIP Europe 2005. Critical Infrastructure Protection, Eds. B. M. HÄMMERLI, S. D. WOLTHUSEN. Rheinische Friedrich-Wilhelms-Universität Bonn, 19. September 2005.
- POLLIT, M. (2005) *Cyberterrorism-Fact or Fancy?* FBI Laboratory. Washington, D.C.; <http://www.cs.georgetown.edu/~denning/infosec/pollitt.html>.
- POLTERMANN, A. (Hg.) (2002) *Gut zu Wissen: Links zur Wissensgesellschaft*. Münster, Dampfboot-Verlag; <http://www.dampfboot-verlag.de/>.
- POULSEN, K. (2006) The Backhoe: A Real Cyberthreat. *Wired*, January 23, 2006, <http://www.wired.com/>.
- POWNER, D. (2005) *Critical Infrastructure Protection. Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities*. United States Government Accountability Office. Washington, D.C.; <http://www.gao.gov/>.
- POWNER, D., RHODES, K. (2006) Internet Infrastructure. Challenges in Developing a Public/Private Recovery Plan. United States Government Accountability Office. Washington, D.C.; <http://www.gao.gov/>.
- PULLIAM, D. (2005a) Government computers top target for cyberattacks. *govexec.com*, August 5, 2005; <http://www.govexec.com/>.
- PULLIAM, D. (2005) Cybersecurity rating rises - barely. *Govexec.com*; February 16, 2005; <http://govexec.com/>.

- QUENIVET, N. (2005) The World after September 11: Has it really changed?. *The European Journal of International Law*, 16, 561-577;
<http://www.ejil.org/journal/Vol16/No3/art9.pdf>.
- RAND (2005) *Trends in Terrorism. Threats to the United States and the Future of the Terrorism Risk Insurance Act*. The RAND Corporation. Santa Monica CA;
<http://www.rand.org/pubs/monographs/MG393/index.html/>.
- RANDOZZO, M. R. et al. (2004) *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*. Carnegie Mellon Software Engineering Institute, Pittsburgh; <http://www.cert.org/archive/pdf/bankfin040820.pdf>.
- REINERMANN, D., WEBER, J. (2001) *Analysis of Critical Infrastructure: The ACIS methodology*. Paper presented at First GI Workshop on CIP, ETH Zürich;
<http://www.gi-ev.de/fachbereiche/sicherheit/fg/kritis/CIP-Workshop-GI-03.pdf>.
- RICHTER, E. (2005) Nachhaltigkeit – zeitgemäße Definition eines politischen Begriffs. *Leviathan*, 33, 257-272.
- RITTER, S., WEBER, J. (2002) *Critical Infrastructure Protection: Survey of worldwide Activities*. Federal Office for Information Security (BSI). Bonn;
http://www.bsi.bund.de/english/themes/kritis/kritis_papers_e.htm.
- ROBINSON, S. (2003) *U.S. Information Security Law IV*. SecurityFocus Symantec Corporation. Cupertino CA; <http://www.securityfocus.com/infocus/1710>.
- ROßNAGEL, A. (2006) Datenschutz im 21. Jahrhundert. *Aus Politik und Zeitgeschichte*, ApuZ 5-6/2006, 9-15.
- ROßNAGEL, A. et al. (1989), Die Verletzlichkeit der „Informationsgesellschaft“. Opladen, Westdeutscher Verlag².
- ROTERT, M. (2004) Internetüberwachung zwischen Anspruch und Wirklichkeit. *Kriminalpolitik* 6/2004, 468-473;
http://www.gten.de/downloads/KRIMI_Rotert_neu.pdf.
- ROTH, P. (1984) *Cuius regio, eius informatio. Moskaus Modell für die Weltinformationsordnung*. Graz u.a.. Styria-Verlag.
- RTI (2002) *The Economic Impacts of Inadequate Infrastructure for Software Testing*. Prepared by Research Triangle Park (RTI) for National Institute of Standards & Technology (NIST). U.S. Department of Commerce. Washington, D.C.;
<http://www.nist.gov/director/prog-ofc/report02-3.pdf>.

- SASSEN, S. (Ed.) (2002) *Global networks, linked cities*. New York u.a., Taylor & Francis; <http://www.taylorandfrancis.co.uk/>.
- SCALET, S. D. (2005) Pulling Threads on E-crime. *SCO Online*, July 2005; www.csoonline.com/.
- SCHADE, K. (2004) „*Informationsgesellschaft*“ als globales Konzept? Freie wissenschaftliche Arbeit zur Erlangung des akademischen Grades eines Magister Artium. Freie Universität Berlin, FB Politik- und Sozialwissenschaften; <http://www.worldsummit2005.de/>.
- SHELL, B., MARTIN, C. (2004) *Cybercrime. A Reference Handbook*. Santa Barbara, CA Denver, Col Oxford UK, ABC CLIO; <http://www.bsos.umd.edu/gvpt/lpbr/subpages/reviews/schell-martin605.htm>.
- SCHMIDT, H. A. (2003) Is Cyberspace Secure? An Interview with Howard A. Schmidt. *The New Atlantis*, 1, 114-121; <http://www.thenewatlantis.com/archive/1/interview.htm>.
- SCHNECKENER, U. (2006) Transnationaler Terrorismus. Charakter und Hintergründe des „neuen“ Terrorismus. Frankfurt/M, Suhrkamp; <http://www.suhrkamp.de>.
- SCHNECKENER, U. (2005) Fragile Staatlichkeit als globales Sicherheitsrisiko. *Aus Politik und Zeitgeschichte*, ApuZ 28-29/2005, 26-31.
- SCHNECKENER, U. (2005a) *Die soziale Konstruktion des „Terrorexperten“*. Stiftung Wissenschaft und Politik (SWP). Berlin; <http://www.swp-berlin.org/forschungsgruppen.php?id=80&page=5>.
- SCHNECKENER, U. (2004) *Transnationale Terroristen als Profiteure fragiler Staatlichkeit*. Stiftung Wissenschaft und Politik (SWP). Berlin; http://www.swp-berlin.org/de/common/get_document.php?asset_id=1288.
- SCHNECKENER, U. (2002) *Netzwerk des Terrors*. Stiftung Wissenschaft und Politik (SWP). Berlin; http://www.swp-berlin.org/de/common/get_document.php?asset_id=177.
- SCHNEIER, B. (2006) Why Data Mining Won't Stop Terror. *Wired News*, 3/9/2006; www.schneier.com/.
- SCHNEIER, B. (2005) Terrorists don't do movie plots. *Wired News*, 9/8/2005; www.schneier.com/.
- SCHNEIER, B. (2004) Information security: How liable should vendors be?. *Computerworld*, 10/28/2004; www.computerworld.com/.

- SCHNEIER, B. (2003) *Beyond Fear. Thinking Sensible About Security in an Uncertain World*. New York , Copernicus Books; www.schneier.com/book-beyondfear.html.
- SCHNEIER, B. (2001) *Managed Security Monitoring: Network Security for the 21st Century*. Counterpane Internet Security Inc.. Mountain View CA; <http://www.counterpane.com/msm.pdf>.
- SCHNEIER, B. (2000) *Secrets & Lies. Digital Security in a Networked World*. Indianapolis, Indiana, Wiley Publishing; <http://www.counterpane.com/sandl.html>.
- SCHJOLBERG, S., HUBBARD, A. M. (2005) *Harmonizing National Legal Approaches on Cybercrime*. Background Paper at the Thematic Meeting on Cybersecurity for The World Summit on the Information Society. ITU. Geneva; http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf.
- SCHMITTCHEN, D. (2006) „Rogue States“ – „Schurkenstaaten“. SWP Diskussionspapier, Stiftung Wissenschaft und Politik (SWP). Berlin; http://www.swp-berlin.org/common/get_document.php?id=1597.
- SCHWARTAU, W. (2000) *Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Disruption*. New York, Thunder's Mouth; <http://www.networkworld.com/>.
- SEIFERT, J. W. (2004) *Data Mining: An Overview*. Congressional Research Service, Report for Congress, Updated December 16, 2004. CRS, Washington, D.C.; <http://www.fas.org/irp/crs/RL31798.pdf>.
- SHAHAR, Y. (2005) *Non-Conventional Terrorism: Challenges & Response*. In KNOP, K. von (Hg.) (2005) *Countering Modern Terrorism. History, Current Issues and Future Threats*. Bielefeld, Bertelsmann, 361-380; <http://www.wbv.de>.
- SHANE, P. M. (Ed.) (2005) *Democracy Online: the Prospects for Political Renewal through the Internet*. New York; London: Routledge; <http://www.uoc.edu/uocpapers/dt/eng/shane.html>; http://papers.ssrn.com/sol3/papers.cfm?abstract_id=583143.
- SIEDSCHLAG, A. (2002) *Internationale Sicherheitspolitik im Internetzeitalter*. In SIEDSCHLAG, A. (mit A. BILGERI) *Kursbuch Internet und Politik, Band 2/2002*; Opladen, Westdeutscher Verlag; www.kursbuch-internet.de/; <http://homepage.uibk.ac.at/~c40290/cyberwar.pdf>.

- SIEDSCHLAG, A. (Hg.) (2005) *Kursbuch Internet und Politik 2004/2005*. Wiesbaden, VS-Verlag für Sozialwissenschaften; <http://www.vs-verlag.de/>.
- SIGNPOSTS (2005): *Signposts in Cyberspace: The Domain Name System and Internet Navigation*. Committee on Internet Navigation and the Domain Name System: Technical Alternatives and Policy Implications, National Research Council. Washington D.C., The National Academies Press; http://www7.nationalacademies.org/cstb/pub_dns.html.
- SIMONIS, U. E. von (Hg.) (1977) *Infrastruktur: Theorie und Politik*. Köln, Kiepeheuer & Witsch.
- SIXTUS, M. (2005) Das Web sind wir. *Technology Review*, July 2005; http://www.sixtus.net/article/614_0_2_0_C/.
- SOKOLOVSKY, V. D. (1975) *Soviet Military Strategy*. Edited with an analysis and commentary by H. F. SCOTT. New York, Crane, Russak.
- SONNTAG, M. (2005) *IT-Sicherheit kritischer Infrastrukturen*. München, Beck; www.beck-shop.de/.
- SPENCER, A. (2006) Questioning the Concept of 'New Terrorism'. *Peace Conflict & Development*, 8, (online Journal); <http://www.peacestudiesjournal.org.uk/docs/Feb%2006%20SPENCER%20version%202.pdf>.
- STATISTISCHES BUNDESAMT (2006) *Informationstechnologie in Unternehmen und Haushalten 2005*. Wiesbaden; http://www.destatis.de/download/d/veroe/Pressebrochure_IKT2005.pdf.
- STATISTISCHES BUNDESAMT (2006) *Informationstechnologie in Unternehmen und Haushalten 2005*. Wiesbaden, Statistisches Bundesamt; www.destatis.de/informationsgesellschaft/.
- STEHR, N. (2001) Moderne Wissensgesellschaften. *Aus Politik und Zeitgeschichte*, APuZ B 36/2001, 7-13.
- STEURY, D. P. (Ed.) (1996) *Intentions and Capabilities: Estimates on Soviet Strategic Forces, 1950-1983*. History Staff, Center for the Study of Intelligence, Central Intelligence Agency. Washington, D.C.; <https://www.cia.gov/cia/publications/intellit/intell.shtml>.

- STURGEON, W (2006) Analysis: A globetrotter's guide to cyber crime. *Silicon.com*, 9 May 2006; <http://software.silicon.com/malware/0,380000310039158777,00.htm>.
- SYMANTEC (2006) *Internet Security Threat Report*. Symantec. Cupertino, CA/USA; <http://www.symantec.com/>.
- TALBOT, D. (2006) Universal Authentication. *Technology Review*, March/April 2006; www.technologyreview.com/.
- TALBOT, D. (2004) The Internet is broken. *Technology Review*, 108, 62-69; deutsche Version: <http://www.heise.de/tr/artikel/69890>.
- TELEGEOGRAPHY (2004). Global Geographic Internet Database and Report 2004. Washington D.C., www.telegeography.com.
- TELEGEOGRAPHY (2003) Terrestrial Bandwidth 2003; Global Internet Geography. Washington D.C..
- TELEGEOGRAPHY (2002a): US Internet Geography 2003. CD-ROM. Washington D.C..
- TELEGEOGRAPHY (2002b): Terrestrial Bandwidth 2003. CD-ROM. Washington D.C..
- TELEGEOGRAPHY (2001a): International Bandwidth 2001. CD-Rom. Washington D.C..
- TELEGEOGRAPHY (2001b): Packet Geography 2002. Washington D.C..
- THOMAS, T. L. (2003) Al Queda and the Internet: The Danger of "Cyberplanning". *Parameters*, Spring 2003, 112-123; <http://carlisle-www.army.mil/usawc/Parameters/03spring/thomas.pdf>.
- TINNEFELD, M.-Th., EHMANN, E. (1998) *Einführung in das Datenschutzrecht*. München, Wien (3. Aufl.), Oldenbourg; www.oldenbourg.de/.
- TSFATI, Y., WEIMANN, G. (2002) www.terrorism.com: Terror on the Internet. *Studies in Conflict and Terrorism*, 25, 317-332; <http://www.tandf.co.uk/journals/titles/1057610X.asp>.
- VERTON, D. (2003) *Black Ice: The Invisible Threat of Cyber-Terrorism*. New York, Mc-Graw Hill / Osborne; <http://books.mcgraw-hill.com/getbook.php?isbn=0072227877&template=osborne>.

- VIELHABER, J., KUBOVCSIK, N. (2005) *Homeland Security – Deutschlands offene Flanke?*. Arbeitspapiere der Konrad-Adenauer-Stiftung, Bonn; http://www.kas.de/publikationen/2005/6679_dokument.html.
- VOLST, A. et al. (2002) *Hybride Infrastruktur Internet*. 2. Österreichische Konferenz für Technikfolgenabschätzung (TA02). Wien; <http://www.oeaw.ac.at/ita/ta02/abstracts.htm>.
- WEIDENFELD, W. (Hg.) (2004) *Herausforderung Terrorismus. Die Zukunft der Sicherheit*. Wiesbaden, VS-Verlag für Sozialwissenschaften; www.vs-verlag.de/.
- WEIMANN, G. (2004) *www.terror.net. How Modern Terrorism Uses the Internet*. United States Institute of Peace, Washington, D.C.; Special Report 116. March 2004. www.usip.org.
- WEIMANN, G. (2005) *Terror Online: How do Terrorists use the Internet?* In KNOP, K. von (Hg.) *Countering Modern Terrorism. History, Current Issues and Future Threats*. Bielefeld, Bertelsmann, 87-109.
- WEIMANN, G. (2006) *Terror on the Internet . The New Arena, the New Challenge*. Washington, D.C., The United States Institute of Peace; http://www.usip.org/newsmedia/weimann_press/index.html
- WEISS, M. A. (2005) *Terrorist Financing: U.S. Agency Efforts and Inter-Agency Coordination*. Congressional Research Service, Report for Congress. CRS, Washington, D.C.; <http://www.fas.org/sfp/crs/terror/RL33020.pdf>.
- WEIZENBAUM, J. (mit G. WENDT) (2006) *Wo sind sie, die Inseln der Vernunft im Cyberstrom?* Freiburg; Basel; Wien. Herder; http://www.herder.de/index_html.
- WERTHEBACH, E. (2004) *Deutsche Sicherheitsstrukturen im 21. Jahrhundert*. Aus Politik und Zeitgeschichte, APuZ B 44/2004, 5-13.
- WESTON, M. (2006) *Review of the Posse Comitatus Act after Hurricane Katrina*, U.S. Army War College, Carlisle Barracks, Pennsylvania; <http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA448803&Location=U2&doc=%20Get%20TRDoc.pdf>.
- WHITMAN, M. E. (2004) *In defense of the realm: understanding the threats to information security*. *International Journal of Information Management*, 24, 43-57; www.sciencedirect.com/.

- WILSON, C. (2004) *Information Warfare and Cyberwar: Capabilities and Related Policy Issues*. Congressional Research Service, Report for Congress. Washington, D.C; <http://www.fas.org/irp/crs/RL31787.pdf>.
- WILSON, C. (2005) *Computer Attack and Cyberterrorism: Vulnerabilities and policy issues for Congress*. Congressional Research Service, Report for Congress. 2005. Washington, D.C.; <http://www.fas.org/sgp/crs/terror/RL32114.pdf>.
- WILSON, C (2006) *Terrorist Capabilities for Cyber-attack*. In ABELE-WIGERT, I., DUNN, M. A. *International CIIP Handbook*, Vol. II, 71-88.
- WIMBISH, W., STERLING, J. (2003) *The National Infrastructure Simulation and Analysis Center (NISAC)*. U.S. Army War College, Center for Strategic Leadership. Carlisle, PA; <http://www.carlisle.army.mil/usacsl/Publications/CSL%20Issue%20Paper%206-03.pdf>.
- WINKEL, O. (2000) Netzwerksicherheit - (k)ein Thema für Sozialwissenschaftler. *Rubin*, 2/2000, 6-12. Ruhr-Universität Bochum; http://www.ruhr-uni-bochum.de/rubin/rbin2_00/pdf/artikel_g1_netzwerk.pdf.
- WINKEL, O (2004) Zukunftsperspektive Electronic Government. *Aus Politik und Zeitgeschichte*, ApuZ B 18/2004, 7-15.
- WORLD COMMISSION, 1987 World Commission on Environment and Development: Our Common Future. Oxford New York Toronto; Oxford University Press.
- ZITTRAIN, J, (2006) *Internet Points of Control*. Boston College Law Review, Forthcoming, http://www.bc.edu/schools/law/lawreviews/meta-elements/journals/bclawr/44_2/10_FMS.htm.
- ZÜRN, M., ZANGL, B. (Hrsg.) (2004) *Verrechtlichung - Baustein für Global Governance?* Bonn, Dietz, <http://www.dietz-verlag.de/>.

Zeitungsartikel

- ARKIN, W. M. (2005) Inside NSA's World. *Washington Post*, December 20, 2005; http://blog.washingtonpost.com/earlywarning/2005/12/inside_nsas_world.html/
- ARQUILLA, J. (2003) Interview. *Frontline*, April 24, 2003, <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/arquilla.html>.
- BARBOZA, D. (2006) The Wild Web of China: Sex and Drugs, Not Reform. *The New York Times*, March 8, 2006; www.nytimes.com/.

- CARSTENS, P. (2006) Die Observation der Rechercheure. *Frankfurter Allgemeine Zeitung*, 16. Mai 2006; www.faz.net.
- CHA, A. E. (2005) Computers Simulate Terrorism's Extremes. *Washington Post*, July 4, 2005; www.washingtonpost.com/wp-dyn/content/article/2005/07/03/AR2005070300880.html.
- CHADDOCK, G. R. (2005) London bombs prod US security Steps. *The Christian Science Monitor*, July 13, 2005; <http://www.csmonitor.com/2005/0713/p01s03-uspo.html?s=rrel>.
- CHISHOLM, P. (2005) Protect our electronics against EMP attack. *The Christian Science Monitor*, December 19, 2005; <http://www.csmonitor.com/2005/1219/p25s02-stct.html>.
- CONWAY, M. (2002) Reality Bytes: Cyberterrorism and Terrorist 'use' of the Internet. *Firstmonday*, 7; http://firstmonday.org/issues/issue7_11/conway/index.html.
- ESPINER, T. (2006) British legislation to enforce encryption key disclosure. *News.com*, May 19; http://news.com.com/British+legislation+to+enforce+encryption+key+disclosure/2100-7348_3-6073654.html.
- EVERS, J. (2005) Hacking for dollars. *CNET News*, July 6, 2005; http://news.com.com/Hacking+for+dollars/2100-7349_3-5772238.html.
- FREY, B. S., LÜCHINGER, S., STUTZER, A. (2004) Wirtschaftliche Schäden des Terrorismus. *Neue Zürcher Zeitung*, 12. Juni 2004; <http://www.nzz.ch/2004/06/12/fw/page-article9NJ1L.html>.
- GAUDIN, S. (2004) Plan to Counterattack Hackers Draws More Fire. *Internetnews*, April 5; www.internetnews.com/dev-news/article.php/3335811.
- GELLMANN, B., MOHAMMED, A. (2006) Data on Phone Calls Monitored. *Washington Post*, May 12, 2006; <http://pqasb.pqarchiver.com/washingtonpost/>.
- GLASSER, S. B., COLL, S. (2005) The Web as Weapon. *Washington Post*, August 9; <http://pqasb.pqarchiver.com/washingtonpost/search.html>.
- GRAHAM, B. (2005) Hackers Attack Via Chinese Web Sites. *Washington Post*, August 25; <http://pqasb.pqarchiver.com/washingtonpost/search.html>.
- GROSS, G. (2005) US government slammed for failing on cybersecurity. *Techworld*, 12/14/2005; <http://www.techworld.com/security/news/index.cfm?NewsID=4996>.

- HIRSH, M. (2006) The NSA's overt problem. *Washington Post*, January 1, 2006; <http://pqasb.pqarchiver.com/washingtonpost/search.html>.
- HOLDEMAN, E. (2005) Homeland Security in a perfect world. *The Christian Science Monitor*, September 2, 2005; <http://csmonitor.com/2005/0902/p09s01-coop.html>.
- HOOPES, N. (2005) Hoopes, N., New focus on cyber-terrorism. *The Christian Science Monitor*, August, 16. 2005; <http://www.csmonitor.com/2005/0816/p01s02-stct.html>.
- IJAZ, M., ABRAHAMSON, J. (2006) Secure the USA against bloodless terrorist warfare. *The Christian Science Monitor*, January 4, 2006; <http://search.csmonitor.com/2006/0104/p09s01-coop.html>.
- KOHLMANN, E. (2005) Al Qaeda and the Internet. *Washington Post*, August 8, 2005; <http://pqasb.pqarchiver.com/washingtonpost/search.html>.
- KRISTOF, N. D. (2005) Terrorists in Cyberspace. *The New York Times*, December 20, 2005; <http://select.nytimes.com/>.
- LICHTBLAU, E. (2005) Turf wars hinder U.S. attack on terror cash, agency says. *The New York Times*, November 29, 2005; <http://www.solami.com/nyterrorcash.htm>.
- MARKOFF, J. (2005) Scientists to weave a tighter Net. *The New York Times*, August 30, 2005; <http://www.iht.com/articles/2005/08/29/business/net.php>.
- MARKS, A. (2005) Security funding: New York vs. Wyoming. *The Christian Science Monitor*, October 24, 2005; <http://csmonitor.com/2005/1024/p01s03-uspo.html>.
- PRALLE, U. (2005) Der Traum vom Cyberspace. *Neue Zürcher Zeitung Online*, 3. September 2005; <http://www.nzz.ch/2005/09/03/li/articleCLLWT.html>.
- SCHULZE, G. (2006) Mehr Sicherheit wagen. *Die Welt*, 5.9.2006; <http://www.welt.de/data/2006/09/05/1023223.html>.
- SHANNON, V. (2006) The End User: More world on the web. *International Herald Tribune*, May 10, 2006; <http://www.iht.com/articles/2006/05/10/business/ptend11.php>.
- SVOBODA, E. (2005) Google's open skies raise cries. *The Christian Science Monitor*, December 1, 2005; <http://csmonitor.com/2005/1201/p13s01-stct.html>.

- SWARTZ, J. (2005) Terrorists' use of Internet spreads. *USA Today*, February, 26th, 2005; http://www.usatoday.com/money/industries/technology/2005-02-20-cyber-terror-usat_x.htm.
- TALBOT, D. (2004) Zeit für ein neues Netz. *Technology Review* 03/2006; www.heise.de/.
- THORNBURGH, N. (2005) The Invasion of the Chinese Cyberspies. *Time*, August 29, 2005; <http://www.time.com/time/magazine/printout/0,8816,1098961,00.html>.
- TIBONI, F. (2005) The new Trojan war. *fcwcom*, August 22, 2005; <http://www.fcw.com/article90262-08-22-05-Print>.
- WARD, M. (2003) Cyber terrorism 'overhyped', *BBC News Online*; <http://news.bbc.co.uk/go/pr/fr/-/1/hi/technology/2850541.stm>.

Hinweis: Alle Webseiten wurden im Januar 2007 überprüft; das Datum der letzten Abfrage wird deshalb nicht gesondert ausgewiesen.

1. **SAM - Untersuchung von Aushandlungen in Gruppen mittels Agentensimulation**
von N. Lepperhoff (2002), VI, 278 Seiten
ISBN: 978-3-89336-298-1
2. **Praxisbezogene IDL-Programmierung**
von M. Busch, R. Bauer, H. Heer, M. Wagener (2002), XVI, 216 Seiten, 12 farb. Abb.
ISBN: 978-3-89336-308-7
3. **Segmentierung von Volumendatensätzen mittels dreidimensionaler hierarchischer Inselstrukturen**
von J.-F. Vogelbruch (2002), V, 191 Seiten, zahlr. farb. Abb.
ISBN: 978-3-89336-309-4
4. **ComputerMathematik mit Maple**
von J. Grotendorst (2003), VI, 274 Seiten mit beiliegender CD-ROM, zahlr. farb. Abb.
ISBN: 978-3-89336-325-4
5. **ComputerMathematik mit Maple – Zweite überarbeitete und erweiterte Auflage**
von J. Grotendorst (2004), VI, 294 Seiten mit beiliegender CD-ROM, zahlr. farb. Abb.
ISBN: 978-3-89336-354-4
6. **The Internet in Germany: Atlas of Providers and Regions**
by N. Lepperhoff, W. Fischer (2004), VIII, 103 pages, many coloured fig.
ISBN: 978-3-89336-358-2
7. **Störstellen in Galliumnitrid-basierenden Transistoren**
von M.J. Wolter (2004), V, 132 Seiten, 19 farb. Abb.
ISBN: 978-3-89336-361-2
8. **Programming in C++: Audio-Visual Lecture of the course "Object-oriented programming in C++"**
von B. Mohr, M. Boltes, R. Koschmieder (2004), DVD (18 hours, 22 minutes recorded in 15 sessions)
ISBN: 978-3-89336-369-8
9. **Fabrication and characterization of planar Gunn diodes for Monolithic Microwave Integrated Circuits**
by S. Montanari (2005), c. 150 pages, 26 col. fig.
ISBN: 978-3-89336-396-4
10. **IDL Referenz der ICG-Daten-Struktur**
von R. Bauer (2006), XIV, 130 Seiten
ISBN: 978-3-89336-426-8

11. **Piezoresponse Force Microscopy and Surface Effects of Perovskite Ferroelectric Nanostructures**
by F. Peter (2006), 106 pages
ISBN: 978-3-89336-444-2
12. **Molecular Electronic Building Blocks Based on Self-Assembled Monolayers**
by B. Lüssem (2006), 138 pages
ISBN: 978-3-89336-454-1
13. **Josephson Tunnel Junctions with Ferromagnetic Interlayer**
by M. Weides (2007), IX, 144 pages
ISBN: 978-3-89336-472-5
14. **www.InfrastrukturInternet-Cyberterror.Netzwerk**
Analyse und Simulation strategischer Angriffe auf die kritische Infrastruktur
Internet
von W. Fischer (2007), 213 Seiten
ISBN: 978-3-89336-474-9

Das Internet entwickelt sich zu einer kritischen Infrastruktur. Internetsicherheit (Cybersecurity) ist deshalb ein wichtiges gesellschaftliches Ziel und ein neues Politikfeld auf nationaler, europäischer und internationaler Ebene. Cybersecurity widmet sich den Sicherheitsgefährdungen, ihrer Abwehr und Bewältigung, die von diversen gesellschaftlich-politischen Akteuren ausgehen und die eine sichere, störungsarme Nutzung des weltumspannenden Netzwerkes zu beeinträchtigen drohen. Zu diesen Gefährdungen zählen „gewöhnliche“ kriminelle Handlungen (Cyberkriminalität) sowie terroristische Aktivitäten, die in zwei Ausprägungen auftreten: (1) Als inzwischen klar erkennbare terroristische Nutzung des Internets, um Propaganda zu betreiben, Informationen zu übermitteln, um Netzwerk zu bilden, Geld zu beschaffen, um Helfer, Mittäter zu rekrutieren etc. (Terrorismus im Cyberspace). (2) Als ein noch hypothetischer, aber sich abzeichnender Terrorismus gegen den Cyberspace (Cyberterrorismus); er zielt darauf ab, die ungestörte, sichere Nutzung des Internets zu beeinträchtigen, was auch negative Folgen für die Funktionsfähigkeit weiterer kritischer Infrastrukturen hätte.

Das Buch setzt sich mit diesen Gefahren auseinander, beschreibt die Grundzüge der Politik für Internetsicherheit und präsentiert Ergebnisse des Modells INESS, das die Auswirkungen strategischer Störungen des Internets auf den Transport von Datenpaketen simuliert.

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft



Band/Volume 14
ISBN 978-3-89336-474-9

Informationstechnik
Information Technology