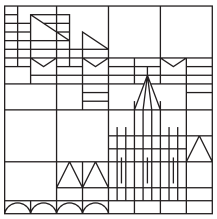
Sicherheit in elektronischen Netzen

Globale Steuerungsmechanismen zur Sicherung kritischer Informationsinfrastrukturen im Hinblick auf elektronischen Handel

Dissertation
zur Erlangung des akademischen Grades
des Doktors der Sozialwissenschaften (Dr. rer. soc.)

an der

Universität Konstanz



Sektion Politik–Recht–Wirtschaft
Fachbereich Politik- und Verwaltungswissenschaft

vorgelegt von

Dipl.-Verw.Wiss. **Dirk Hyner**

Tag der mündlichen Prüfung: 28. Juli 2014
Referent: Prof. Dr. Volker Schneider
Referent: Prof. Dr. Wolfgang Seibel

Vorwort

Der Mensch und die von ihm erschaffene Technik sind zwei der faszinierendsten Phänomene. Diese Arbeit liegt daher nicht ganz zufällig im Schnittpunkt technischer und sozialer Systeme, welche sie aus kybernetischer Perspektive betrachtet und zu erklären sucht. Sie beruht in wesentlichen Teilen auf einem von der Volkswagen-Stiftung finanziell geförderten Forschungsprojekt und wurde im Herbst 2013 vom Fachbereich Politik- und Verwaltungswissenschaft der Sektion Politik–Recht–Wirtschaft der Universität Konstanz als Dissertation angenommen. Für die Veröffentlichung wurde sie noch einmal vereinzelt um neuere Literatur ergänzt.

Was wäre unser Leben ohne die Anderen, die Verwandten und Freunde, Kommilitonen und Kollegen, Vorbilder und Wegbegleiter, die uns immer wieder in Höhen und Tiefen zur Seite stehen und mit Rat und Tat ein ums andere Mal neue Perspektiven eröffnen? So soll sie an dieser Stelle – wie in den meisten Vorworten üblich – auch nicht fehlen, die Danksagung an jene, die mich auf dem oft verschlungenen Weg zur Abfassung dieser Arbeit ein Stück begleitet und vorangebracht haben.

Besonderer Dank gebührt hier vor allem meinem Doktorvater und akademischen Lehrer Prof. Dr. Volker Schneider, der mich bereits als studentische Hilfskraft sowie später als wissenschaftlichen Mitarbeiter an seinem Lehrstuhl für materielle Staatstheorie stets in außergewöhnlichem Maße gefördert und motiviert hat. Ihm verdanke ich viele interessante Ideen und Anregungen, nicht zuletzt jene zur Erstellung der vorliegenden, von ihm betreuten Arbeit. Ebenso danken möchte ich Prof. Dr. Wolfgang Seibel für die Erstellung des Zweitgutachtens sowie die Übernahme des Vorsitzes in der mündlichen Prüfung. Dankbar bin ich auch Dr. Achim Lang und Dr. Marc Tenbücken für die teils kontroversen, immer aber produktiven Diskussionen. Gerne erinnere ich mich ferner an die zeitweise Bürogemeinschaft mit Karina Frainer.

Ganz herzlich danke ich schließlich meinen Eltern für ihre in jeder Hinsicht und zu jeder Zeit vorbehaltlose Unterstützung, die wesentlich zum erfolgreichen Gelingen dieser Arbeit beigetragen hat.

Hamburg, Oktober 2014 *Dirk Hyner*

Zusammenfassung

Für moderne Gesellschaften sind vernetzte Informations- und Kommunikationstechnologien kritische Infrastruktursysteme. Sie spannen elektronische Handlungsräume auf, in die sich mehr und mehr ökonomisch relevante Transaktionen verlagern. Eine funktionale Beeinträchtigung dieser Systeme durch kriminell, terroristisch oder militärisch motivierte Angriffe ist daher prinzipiell problematisch, ihre Sicherung im Umkehrschluß von zunehmender Bedeutung. Durch die komplexe Verflechtung sozialer Akteure und technischer Artefakte ergibt sich hierbei ein sozio-technischer Steuerungsbedarf. Im Hinblick auf diesen Steuerungsbedarf untersucht die vorliegende Arbeit, in welchen institutionellen Mechanismen private und öffentliche Akteure Ressourcen zur Produktion des kollektiven Gutes Sicherheit in elektronischen Netzen mobilisieren.

In der Einleitung wird zunächst die Relevanz des Themas verdeutlicht. Es wird auf die Fragestellung sowie die Forschungsmethodik qualitativer Fallstudien und quantitativer Strukturanalysen eingegangen. Ferner wird die Eingrenzung und Auswahl der untersuchten Fallstudien beschrieben. Zuletzt folgt ein kurzer Abriß des bisherigen Forschungsstandes in der Literatur.

Das zweite Kapitel beschäftigt sich aus theoretischer Perspektive mit der Steuerung sozialer Systeme. Am Anfang stehen metatheoretische Überlegungen zum Phänomen des Seins sowie zu den Möglichkeiten und Grenzen seiner Erkenntnis im Rahmen des Bewußtseins und damit zugleich der Schaffung von Wissen. Es folgen abstrakte Ausführungen zu Mechanismen der Ordnungsbildung und Kybernetik in komplexen Systemen. Schließlich werden diese im Hinblick auf die institutionelle Steuerung sozio-technischer Systeme mit Hilfe politik- und sozialwissenschaftlicher Ansätze konkretisiert.

Die globale Informationsgesellschaft als Kontext steht im Mittelpunkt des dritten Kapitels. Zunächst werden hier die Begriffe der Information sowie der Kommunikation eingegrenzt. In Sonderheit wird der Begriff der Information in seinem Bedeutungsgehalt entlang dreier Dimensionen erschlossen. Es folgt ein vertiefender Abriß der historischen Entwicklung technischer Systeme zur Verarbeitung, Speicherung, Übertragung und Verteilung von Information. Zuletzt wird die gegenwärtig herausgehobene ökono-

mische Bedeutung der Ressource Information im Lichte unterschiedlicher gesellschaftstheoretischer Ansätze aufgezeigt.

Das vierte Kapitel skizziert die Sicherheit elektronischer Netze als soziales Problem. Es beleuchtet vernetzte Informationssysteme als kritische infrastrukturelle Basis ökonomischer Transaktionen in modernen Gesellschaften. Die Vielzahl möglicher Angriffsvektoren sowie das resultierende Bedrohungsszenario des Cybercrime wird näher erläutert. Abschließend wird auf mögliche Maßnahmen zum Schutz elektronischer Netze eingegangen und verdeutlicht, daß elektronischer Sicherheit der Charakter eines globalen Kollektivgutes zukommt.

Im fünften Kapitel wird die Produktion elektronischer Sicherheit empirisch analysiert. Zunächst wird auf den institutionellen Rahmen einer rechtlich-formalen Regulierung sowie diverse Beispiele informeller Ko- und Selbstregulierung eingegangen. Sodann werden zentrale Akteure und deren relevante Ressourcen im Hinblick auf ihren Beitrag zur Produktion von Sicherheit in elektronischen Netzen untersucht. Besondere Berücksichtigung findet die Problemlösungskapazität einzelner Akteure sowie jener Koordinationsbedarf, der sich aus der Dispersion relevanter Ressourcen ergibt. Schließlich wird die Konfiguration der Fallbeispiele nachgezeichnet und deren Koordinations- und Kooperationsnetzwerk analysiert.

Die Konklusion faßt die gewonnenen Erkenntnisse schematisch zusammen. Sie zeichnet den kybernetischen Regelungsprozeß zur Sicherung kritischer Informationsinfrastrukturen exemplarisch nach und unterstreicht die besondere Bedeutung, die in diesem Kontext polyzentrale Akteursnetzwerke als flexible und dynamische Steuerungsstruktur haben.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

(ISC)2	International Information Systems Security Certification Consortium
ACLU	American Civil Liberties Union
AES	Advanced Encryption Standard
AIDS	Acquired Immune Deficiency Syndrome
AIT	AIT Global
AKSIS	Arbeitskreis Schutz von Infrastrukturen
APEC	Asia-Pacific Economic Cooperation
ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
ASIS	ASIS International
B2B	Business-to-Business
B2C	Business-to-Consumer
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BKA	Bundeskriminalamt
BMVg	Bundesministerium der Verteidigung
BNE	Bruttonationaleinkommen
BSA	Business Software Alliance
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfGE	Bundesverfassungsgerichtsentscheid
BWL	Betriebswirtschaftslehre
C2C	Consumer-to-Consumer
CCC	Chaos Computer Club
CCU	Cybercrime Unit
CDT	Center for Democracy and Technology
CERN	Conseil Européen pour la Recherche Nucléaire
CERT/CC	Computer Emergency Response Team/Coordination Center
CFAA	Computer Fraud and Abuse Act
CIA	Central Intelligence Agency
CIAO	Critical Infrastructure Assurance Office
CIDDAC	Cyber Incident Detection and Data Analysis Center
CIIP	Critical Information Infrastructure Protection
CoE	Council of Europe, Europarat
CSC	Computer Sciences Corporation

CSI	Computer Security Institute
CSIA	Computer Security Industry Alliance
CSIS	Center for Strategic and International Studies
CSNET	Computer Science Network
DAC	Discretionary Access Control
DARPA	Defence Advanced Research Projects Agency
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DMCA	Digital Millenium Copyright Act
DNS	Domain Name System
DoS	Denial of Service
DSL	Digital Subscriber Line
DSTI	Directorate for Science, Technology and Industry
eBusiness	Electronic Business
EC	European Comission, Europäische Komission
eCommerce	Electronic Commerce
eGovernment	Electronic Government
eMail	Electronic Mail
eMarket	Electronic Market
eProcurement	Electronic Procurement
EFF	Electronic Frontier Foundation
EGG	Gesetz zum elektronischen Geschäftsverkehr
ENISA	European Network and Information Security Agency
EPIC	Electronic Privacy Information Center
EPSKI	Europäisches Programm für den Schutz kritischer Infrastrukturen
EP3R	European Public-Private Partnership for Resilience
ETH	Eidgenössische Technische Hochschule
EU	European Union, Europäische Union
EuGH	Europäischer Gerichtshof
EUROPARL	European Parliament, Europäisches Parlament
EWG	Europäische Wirtschaftsgemeinschaft
FBI	Federal Bureau of Investigation
FIRST	Forum of Incident Response and Security Teams
FTC	Federal Trade Commission
FTP	File Transfer Protocol
G2C	Government-to-Consumer
G8	Gruppe der acht führenden Industriestaaten
GATT	General Agreement on Tariffs and Trade
GCSOC	Global Chief Security Officer Council
GI	Gesellschaft für Informatik
GII	Global Information Infrastructure
GILC	Global Internet Liberty Campaign

GIP	Global Internet Project
GIPI	Global Internet Policy Initiative
GLBA	Gramm-Leach-Bliley Act
GUI	Graphical User Interface
GVBl.	Gesetz- und Verordnungsblatt
HDSG	Hessisches Datenschutzgesetz
HIPAA	Health Insurance Portability and Accountability Act
HP	Hewlett-Packard
HTCIA	High Technology Crime Investigation Association
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
I3P	Institute for Information Infrastructure Protection
IAB	Internet Architecture Board
IABG	Industrieanlagen-Betriebsgesellschaft
IANA	Internet Assigned Numbers Authority
IBM	International Business Machines
IC3	Internet Crime Complaint Center
ICANN	Internet Corporation for Assigned Names and Numbers
ICC	International Chamber of Commerce
ICCB	Internet Configuration Control Board
ICCP	Information, Computer and Communications Policy
IDC	International Data Corporation
IDEA	International Data Encryption Algorithm
iDEFENSE	Infrastructure Defense
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFIP	International Federation for Information Processing
IGF	Internet Governance Forum
IKT	Informations- und Kommunikationstechnologie
INWG	International Network Working Group
IP	Internet Protocol
IRS	Intrusion Response System
ISA	Internet Security Alliance
ISACA	Information Systems Audit and Control Association
ISDN	Integrated Services Digital Network
ISF	Information Security Forum
ISO	International Organization for Standardization
ISOC	Internet Society
ISPAB	Information Security and Privacy Advisory Board
ISS	Internet Security Systems
ISSA	Information Systems Security Association

IuK	Information und Kommunikation
IuKDG	Informations- und Kommunikationsdienstegesetz
ITAA	Information Technology Association of America
ITU	International Telecommunication Union
ISAC	Information Sharing and Analysis Center
IT	Information Technology, Informationstechnologie
JKomG	Justizkommunikationsgesetz
KB	Kilobyte
MAC	Mandatory Access Control
MDS	Multidimensionale Skalierung
MDStV	Mediendienste-Staatsvertrag
MI	McConnell International
MIT	Massachusetts Institute of Technology
MS	Microsoft
NASA	National Aeronautics and Space Administration Agency
NATO	North Atlantic Treaty Organization
NCSA	National Cyber Security Alliance
NCSP	National Cyber Security Partnership
NHTCU	National High-Tech Crime Unit
NIAC	National Infrastructure Advisory Council
NIC	Network Information Center
NII	National Information Infrastructure
NIPC	National Infrastructure Protection Center
NIST	National Institute of Technology
NMC	Network Management Center
NSA	National Security Agency
NSC	National Security Council
NSF	National Science Foundation
NSFNET	National Science Foundation Network
NW3C	National White Collar Crime Center
OECD	Organization for Economic Co-operation and Development
PC	Personal Computer
PCIPB	President's Critical Infrastructure Protection Board
PGP	Pretty Good Privacy
PI	Privacy International
PKI	Public Key Infrastructure
PPG	Produktpirateriegesetz
PwC	PricewaterhouseCoopers International
RAND	RAND Corporation
Rs.	Rechtssache
RSA	RSA Security
SANS	SysAdmin/Audit/Network/Security Institute

SAP	SAP AG
SCI	Southeast Cybercrime Institute
SigG	Signaturgesetz
SigVO	Signaturverordnung
SMTP	Simple Mail Transfer Protocol
SRI	SRI International
StGB	Strafgesetzbuch
StrÄndG	Strafrechtsänderungsgesetz
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TDG	Teledienstegesetz
TDDSG	Teledienstedatenschutzgesetz
TKG	Telekommunikationsgesetz
TKÜV	Telekommunikations-Überwachungsverordnung
TMG	Telemediengesetz
TRIPS	Trade-Related Aspects of Intellectual Property Rights
U.C.C.	Uniform Commercial Code
UCLA	University of California Los Angeles
UK	United Kingdom
UN	United Nations
UrhG	Urheberrechtsgesetz
US	United States
USA	United States of America
US-DHS	United States Department of Homeland Security
US-DoD	United States Department of Defense
US-DoJ	United States Department of Justice
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VwVfG	Verwaltungsverfahrensgesetz
WAP	Wireless Application Protocol
WiKG	Gesetz zur Bekämpfung der Wirtschaftskriminalität
WINKI	Warn- und Informationsnetz für kritische Infrastrukturen
WIPO	World Intellectual Property Organization
WSIS	World Summit on the Information Society
WTO	World Trade Organization
WWW	World Wide Web
ZKDSG	Zugangskontrolldiensteschutz-Gesetz

1 Einleitung

> Society cannot afford to prepare for every eventuality, but it can create a foundation on which an effective response is quickly constructed.
>
> *Arens u. Rosenbloom (2003: 34)*

1.1 Relevanz des Themas

Spätestens seit den Terroranschlägen des 11. September 2001 stehen sicherheitspolitische Themen wieder vermehrt im Mittelpunkt des öffentlichen Diskurses, nachdem diese mit dem Ende der Blockkonfrontation des Kalten Krieges in der letzten Dekade des 20. Jahrhunderts zunächst scheinbar an Bedeutung verloren hatten. Charakteristisch für die Bedrohungslage des 21. Jahrhunderts sind asymmetrische Konfliktformen, in denen die Grenzen zwischen militärischer Kriegsführung, Kriminalität und Terrorismus – und damit zwischen innerer und äußerer Sicherheit – zunehmend verschwimmen (vgl. Arreguín-Toft 2005; Münkler 2006).

Akteure, die zu schwach sind, Konflikte auf konventionellen, durch Haager Landkriegsordnung und Genfer Konventionen regulierten Schlachtfeldern für sich zu entscheiden, entgrenzen diese Konflikte und verlagern sie teilweise oder ganz auf die zivilgesellschaftliche Achillesferse ihres zumeist westlichen Gegners. Der hohe Grad an Komplexität und Technologisierung westlicher Gesellschaften, der einerseits deren militärische wie ökonomische Überlegenheit begründet, macht diese andererseits zugleich in außergewöhnlichem Maße anfällig für Störungen jeder Art. Aufgrund der Vielfalt und Dynamik möglicher Bedrohungen lassen sich komplexe, sozio-technische Systeme jedoch nicht einfach statisch gegen jede denkbare Form der Störung härten. Vielmehr bedarf es zu ihrer Sicherung flexibler Möglichkeiten der Reaktion, welche intelligente Steuerungsmechanismen voraussetzen.

Wissen und Information dienen der Reduktion der Komplexität moderner Gesell-

schaften und fungieren daher als zentrale Steuerungsressource. Technische Systeme, die der Verarbeitung, Speicherung, Übertragung und Verteilung von Informationen dienen, sind in Folge dessen in zunehmendem Maße kritisch für das reibungslose Funktionieren solcher Gesellschaften. Zugleich verlagern sich in der Informationsgesellschaft immer mehr Interaktionen in den virtuellen Raum elektronischer Netze. Dies gilt auch und vor allem für wirtschaftliche Transaktionen. Kritische Informationsinfrastrukturen werden so nicht nur aus politischen und militärischen, sondern auch aus wirtschaftlichen Motiven zu einem lohnenden Angriffsziel.

Für jedes dieser Motive lassen sich einschlägige Beispiele finden. So berichtete etwa Bloomberg[1] am 27. August 2014 von einem kurz zuvor stattgefundenen umfangreichen Hackerangriff auf die amerikanische Großbank JP Morgan, in dessen Verlauf mehrere Gigabyte sensibler Daten gestohlen worden seien und der Ähnlichkeit zu vorangegangenen Angriffen auf europäische Banken aufweise. Die Urheber dieser Angriffe vermuten FBI und NSA offenbar im Umfeld russischer Regierungsorganisationen und bringen sie daher in Zusammenhang mit den gegen Rußland im Zuge der Ukraine-Krise verhängten Sanktionen, was auf einen politischen Hintergrund schließen ließe. Als prototypisches Beispiel militärisch motivierter Angriffe im Internet kann vermutlich der im Juni 2010 entdeckte Internet-Wurm namens „Stuxnet“, der auf die Sabotage iranischer Anlagen zur Anreicherung waffenfähigen Urans spezialisiert war, gelten.[2] Ganz offensichtlich ökonomische Motive hatten acht Tatverdächtige, die nach einem Bericht der Neuen Osnabrücker Zeitung[3] angeklagt sind, Postbank-Kunden mittels Phishing um mehr als 1,3 Mio. Euro geschädigt zu haben.

Sicherheit zielt letztlich auf den dauerhaften Fortbestand eines Systems. Dessen Sicherung ist daher eng mit Steuerungsstrukturen zur Abwehr potentieller Bedrohungen und somit zur Aufrechterhaltung einer funktionierenden Ordnung verknüpft. In freiheitlichen Gesellschaften besteht Konsens, daß eine solche Ordnung jedoch kein Selbstzweck sondern stets nur notwendige Grundlage einer möglichst umfassenden persönlichen Handlungsfreiheit sein sollte. Wilhelm von Humboldt schrieb 1792: „Ohne Sicherheit vermag der Mensch weder seine Kräfte auszubilden noch die Früchte der-

1 Vgl. <http://www.bloomberg.com/news/2014-08-27/fbi-said-to-be-probing-whether-russia-tied-to-jpmorgan-hacking.html>.

2 Vgl. <http://www.heise.de/security/meldung/Das-Stuxnet-Duo-Boesartige-Geschwister-2053847.html>.

3 Vgl. <http://www.noz.de/deutschland-welt/niedersachsen/artikel/506870>.

selben zu genießen; denn ohne Sicherheit ist keine Freiheit.“ (von Humboldt 1851: 45). Dahinter steht die Erkenntnis, daß ohne ein gewisses Maß an dauerhafter Ordnung kein zielgerichtetes Handeln und folglich keine Handlungsfreiheit möglich ist. Dennoch wird hier ein offensichtliches Dilemma erkennbar, denn jede Form sozialer Ordnungsbildung engt per se Freiheitsgrade des Einzelnen ein. Sicherheit steht mithin immer in einem gewissen Spannungsverhältnis zur Freiheit, deren Voraussetzung – aber eben auch Begrenzung – sie ist.

Das beschriebene Spannungsfeld zieht sich von der Augusteischen Zeit, als die Pax Romana erstmals einen Ausgleich zwischen Libertas und Securitas suchte, über das mittelalterliche Lehnswesen, das auf einem Tausch von Freiheit gegen Sicherheit basierte, bis in die Neuzeit, in der Benjamin Franklin 1775 notierte: “They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety.” (Franklin u. Franklin 1818). Selbstverständlich setzt es sich auch im virtuellen Raum elektronischer Netze fort und muß auch hier fortlaufend neu austariert werden. Je nach persönlicher Interessenlage gibt es Akteure, die eher zu bürgerlichen Freiheitsrechten oder aber zu stabilen Ordnungsstrukturen als Grundlage sicherer Transaktionen tendieren. Wie sich vor diesem Hintergrund in der globalen Informationsinfrastruktur stabile Ordnungsstrukturen herausbilden, gehört zu den spannenden Fragen unserer Zeit.

1.2 Fragestellung und Forschungsmethodik

Da elektronische Informations- und Kommunikationssysteme die infrastrukturelle Basis der Informationsgesellschaft bilden (vgl. Abschnitt 4.1), ist eine zuverlässige Sicherheit dieser Systeme für moderne Gesellschaften von kritischer Bedeutung. Zugleich handelt es sich bei der Sicherheit vernetzter IT-Systeme jedoch um ein Kollektivgut (vgl. Abschnitt 4.3.1), weshalb dessen ausreichende Bereitstellung nicht problemlos vorausgesetzt werden kann. Erkenntnisinteresse der vorliegenden Studie ist es daher, den Prozeß der Sicherung elektronischer Netzwerke aus dem theoretischen Blickwinkel einer politischen Kybernetik nachzuzeichnen. Die zentrale Frage ist dann: *Wie funktioniert der kybernetische Regelungsprozeß der Produktion und Distribution elektronischer Sicherheit innerhalb des komplexen sozio-technischen Systems einer globalen Informationsgesellschaft?*

Hierfür sind u. a. folgende Teilfragen zu klären:

- Welche wesentlichen Akteure sind an der Produktion und Distribution des

Gutes Sicherheit in elektronischen Netzen beteiligt?

- Welche Interessen verfolgen diese Akteure?
- Wie koordinieren sich die Akteure untereinander?
- Was sind die institutionellen Rahmenbedingungen ihres Handelns?
- Was sind die zentralen Ressourcen im Produktionsprozeß?

Zur empirischen Untersuchung der Fragestellung werden sowohl qualitative Fallstudien als auch quantitative Methoden der Strukturanalyse herangezogen.

Fallstudien erlauben – im Gegensatz zur isolierenden Perspektive der quantitativ-vergleichenden Methode – eine kontextspezifische Betrachtung einzelner Untersuchungsobjekte. Eine solche Betrachtung erscheint insbesondere dann vorteilhaft, wenn sich das Erkenntnisobjekt nicht oder nicht eindeutig gegen seinen Kontext abgrenzen läßt (vgl. Yin 2003: 13). Gerade bei themenspezifischen Akteurnetzwerken ist dies häufig der Fall. Hier bietet sich alternativ die Untersuchung eines egozentrierten Netzwerkes im Rahmen einer Fallstudie an.

Welchen Beitrag kann nun ein Fallstudiendesign aus erkenntnistheoretischer Perspektive zur Genese und/oder Überprüfung von Wissen leisten? Geläufig ist hier Windelbands[4] Unterscheidung zwischen idiographischer und nomothetischer Wissenschaft. Erstere strebt danach, die konkrete Gestalt eines einzigartigen Erkenntnisobjektes – insbesondere dessen spezifisch-singuläre Eigenschaften – in zumeist narrativer Form mit dem Ziel eines auf den Einzelfall bezogenen Verstehens intensiv zu beschreiben. Letztere hingegen abstrahiert von jedem spezifisch Singulären und konzentriert sich ausschließlich auf die mehreren Objekten allgemeinen Eigenschaften, um induktiv zu einer theoretischen Klassifikationshierarchie zu gelangen, die extensiv eine Vielzahl von Objekten umfaßt und eine deduktive Erklärung des Einzelfalls zuläßt (vgl. hierzu Abschnitt 2.1.1). Möglich wird dies durch den Vergleich einer Vielzahl experimenteller, quasi-experimenteller oder ex-post-facto Fälle, die im Hinblick auf korrelierende Eigenschaften (abhängige und unabhängige Variablen) statistisch analysiert werden. Während die idiographische Methode also alle Eigenschaften eines einzelnen Falles in dessen situativem Kontext ohne Anspruch auf eine etwaige Generalisierbarkeit der Ergebnisse untersucht, hat die nomothetische Methode genau diese induktive Verallgemeinerung zum Ziel und beschäftigt sich daher ausschließlich mit den mehreren – von ihrem si-

4 Vgl. hierzu Windelbands Straßburger Rektoratsrede von 1894, abgedruckt in Windelband (1919).

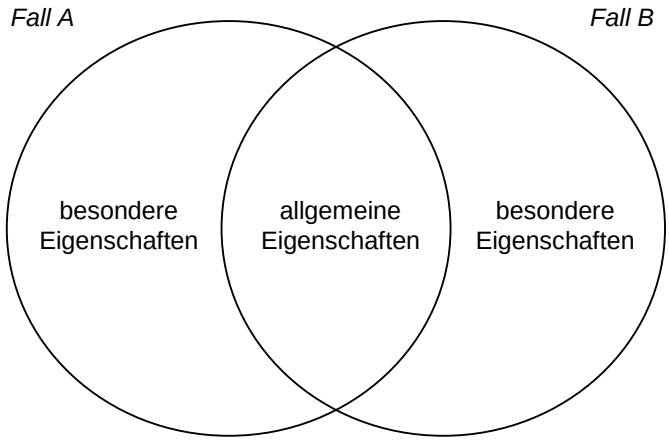


Abbildung 1.1: *Allgemeine und besondere Eigenschaften im Venn-Diagramm*

tuativen Kontext weitgehend isolierten – Objekten gemeinsamen Eigenschaften sowie deren nomologischer Korrelation zueinander (vgl. hierzu Abbildung 1.1).

Obwohl Studien, die sich auf einzelne oder wenige Fälle beziehen, i. d. R. mit der idiographischen Methode assoziiert werden, können sie unter gewissen Bedingungen auch im Rahmen einer nomothetischen Forschung von Nutzen sein (vgl. Eckstein 2000). Dies trifft insbesondere auf solche Studien zu, die Verba (1967) als „disciplined-configurative“[5] charakterisiert. Diese Studien zeichnen sich im Gegensatz zu einem rein deskriptiven bzw. verstehenden Vorgehen durch eine theoriegeleitete und mithin erklärende Fallinterpretation aus, sind also um eine „kausale Rekonstruktion“ (Mayntz 2002b: 14 ff.) bemüht. Sie können daher bis zu einem gewissen Grade sowohl dazu beitragen Hypothesen zu testen, als auch explorativ Lücken im bestehenden Theoriegebäude zu identifizieren und dementsprechend neue Hypothesen zu generieren (George u. Bennett 2005: 19 ff.). Ein solches Vorgehen basiert dann wesentlich auf dem in Abschnitt 2.1.1 erläuterten abduktiven Schluß: Die konkreten Eigenschaften des untersuchten Falles werden als Konsequenz einer theoretisch hergeleiteten Implikation interpretiert und hieraus auf eine mögliche Antezedenz rückgeschlossen.

Die Problematik eines derartigen Rückschlusses wird insbesondere in Abschnitt 2.1.1 erörtert: Ein abduktiver Schluß ist weder kausal noch probabilistisch begründbar, da

5 Der Terminus „disciplined-configurative“ nimmt einerseits auf die ganzheitlich verstandene *Gestalt* (Konfiguration) eines Einzelfalls Bezug, verweist aber andererseits auch darauf, daß diese nicht rein idiographisch zu untersuchen ist, sondern daß eine solche Untersuchung ebenfalls durch eine theoretische Erklärung des Vorgefundenen zu „disziplinieren“ ist.

ein und dieselbe Konsequenz zumeist Folge verschiedener Antezedenzen sein kann. Systemtheoretisch findet dieser Umstand seinen Ausdruck in der Äquifinalität (von Bertalanffy 1972) offener Systeme, i. e. deren Eigenschaft, einen bestimmten Endzustand oftmals von mehr als einem Ausgangszustand aus erreichen zu können. Hinsichtlich einer auf empirischen Fallstudien beruhenden Erkenntnis ergeben sich hierdurch einige Einschränkungen (vgl. George u. Bennett 2005: 161 f.). So bleibt etwa die Validität einer bestimmten theoretischen Erklärung für den konkreten Zustand eines Einzelfalles weitgehend unklar, da nicht ausgeschlossen werden kann, daß sich dieser Zustand möglicherweise auch unter eine andere – nicht weniger erklärungskräftige – Implikation subsumieren läßt. Ebenso gelten für die Fallauswahl besondere Voraussetzungen. Darf diese beim Induktionsschluß aus stochastischen Gründen zur Vermeidung einer statistischen Verzerrung nicht durch die abhängige Variable (Konsequenz) gesteuert sein (vgl. Abschnitt 2.1.1), so trifft dies auf einen abduktiven Schluß nicht zu, da dieser nicht auf probabilistischen Annahmen beruht. Ganz im Gegenteil kann es hier von heuristischem Nutzen sein, das Erkenntnisobjekt hinsichtlich der abhängigen Variable zu selektieren, da häufig gerade der Vergleich besonders ähnlicher oder kontrastierender Fallbeispiele das theoretisch Problematische offenbart.

Aus der in Abschnitt 2.2 eingenommenen theoretischen Perspektive ergibt sich als zentrales Untersuchungsobjekt der vorliegenden Studie das Politikfeld der an der Produktion und Distribution des Gutes Sicherheit in elektronischen Netzen beteiligten Akteure. Dieses kann aus makroskopischer Perspektive zunächst als themenspezifischer Sonderfall eines globalen Politiknetzwerkes interpretiert und hinsichtlich seiner Steuerungsprozesse analysiert werden (vgl. Abschnitt 5.2). Aufgrund der großen Anzahl von Akteuren im Feld bietet sich hierzu das quantitative Verfahren der Clusteranalyse zur Aufdeckung struktureller Muster in besonderer Weise an. Um jedoch eine größere analytische Tiefenschärfe zu erzielen, müssen die fraglichen Steuerungsprozesse darüber hinaus mikrofundiert – also auf die Handlungen konkreter Akteure zurückgeführt – werden. Aus Gründen der Vereinfachung erfolgt eine solche Rückbindung üblicherweise nur bis zur Meso-Ebene korporativer Akteure. Dementsprechend werden hier aus dem gesamten Feld zehn Organisationen als Fallbeispiele herausgegriffen und im Kontext ihres jeweiligen egozentrierten Netzwerkes vergleichend analysiert (vgl. Abschnitt 5.3). Da diese zehn Fälle exemplarische Ausschnitte bzw. Unterfälle des gesamten Netzwerkes darstellen, entspricht ein solches Vorgehen konzeptuell einer Mehrebenenanalyse im Rahmen einer „embedded case study“ (Yin 2003: 42 ff.).

1.3 Empirische Eingrenzung: Auswahl der Fallstudien

Nach Schneider u. Hyner (2006: 161) läßt sich die Menge der an einer spezifischen Problemlösung beteiligten Akteure, Institutionen und Ressourcen aus mindestens drei theoretischen Perspektiven analysieren:

> If we conceive it to be a field of structural forces in which organizations interact and share resources and perceptions to resolve collective problems, we can view it as an 'organizational field' (DiMaggio u. Powell 1983; Janning 1998). If we emphasize co-evolution and adaption with regard to technological innovation and environmental changes, we might call it 'organizational ecology' (Baum 1996). And finally, if we apply the perspective of public policy analysis to this policy topic, we emphasize joint action, cooperation, resource exchange and even conflict. From this perspective, it would be most appropriate to label this configuration a transnational 'policy domain' (Laumann u. Knoke 1987) or 'policy network' (Kenis u. Schneider 1991).

Entsprechend der in Abschnitt 2.2 eingenommenen theoretischen Perspektive wird diese Menge in der vorliegenden Untersuchung als Politikdomäne (*Policy Domain*) aufgefaßt. Benson (1982: 175) verwendet hierfür alternativ auch den Begriff des *Policy-Sektors*: „The policy sector is a collection of interorganizational networks consisting of resource dependencies between organizations." Der Fokus liegt demnach primär auf Prozessen der Kooperation der Akteure sowie des Austausches von Ressourcen in einem Policy-Netzwerk. Zur empirischen Eingrenzung derjenigen (korporativen) Akteure bzw. Organisationen, die auf nationaler oder internationaler Ebene an der Produktion des globalen Kollektivgutes elektronischer Sicherheit in relevanter Weise beteiligt sind, d. h. über wichtige Ressourcen zur Problemlösung verfügen und/oder ein besonderes Interesse an der Sicherheit elektronischer Netze haben, wurde in Anlehnung an das Vorgehen von Laumann u. Knoke (1987: 94 ff.) eine mehrstufige Kombination aus Inhalts- und Reputationsanalyse gewählt (vgl. hierzu Abbildung 1.2).

Zunächst wurden in den Online-Ausgaben der beiden globalen Zeitschriften *Computerworld*[6] und *Financial Times*[7] für den Zeitraum der drei Jahre 2000 bis 2002 sämtliche auf den Begriff „Cybercrime" Bezug nehmenden Artikel ermittelt. Die Wahl fiel auf die genannten Publikationen, da beide zusammen sowohl die technischen als auch die politisch-wirtschaftlichen Aspekte des Themenfeldes abdecken und sich zugleich an

6 Vgl. <`http://www.computerworld.com`>.

7 Vgl. <`http://www.ft.com`>.

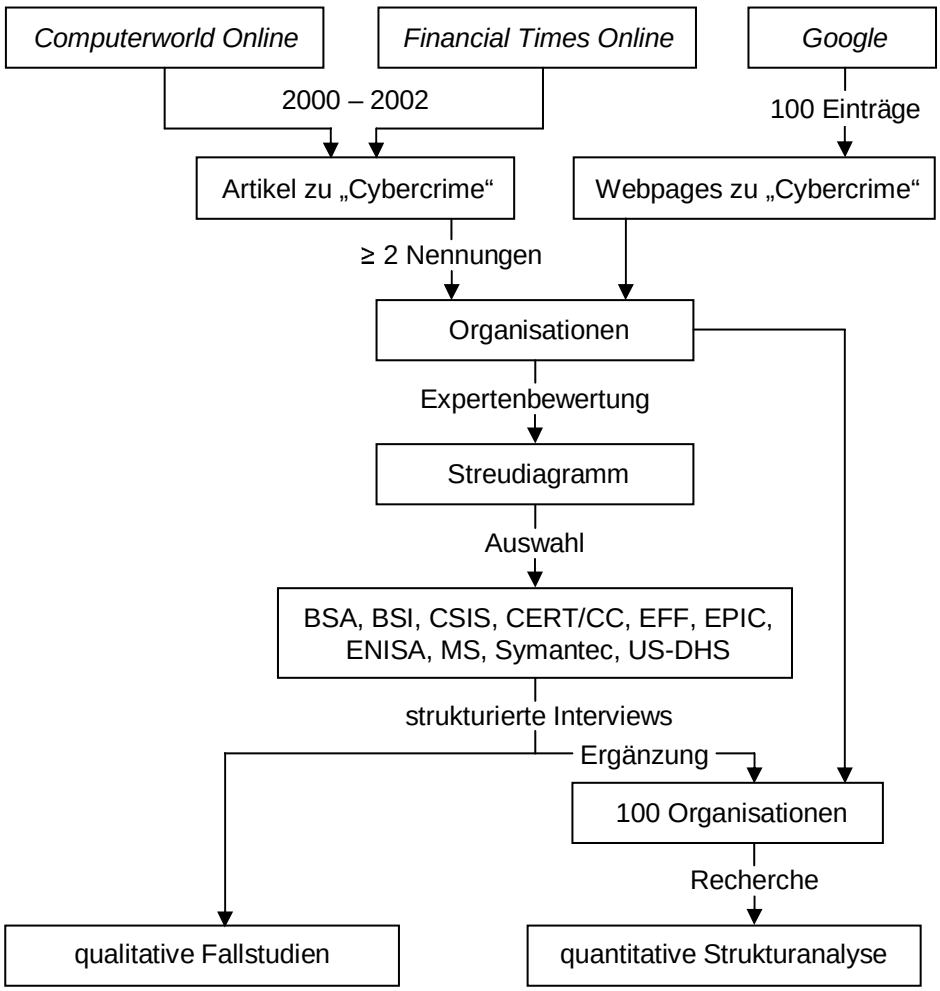
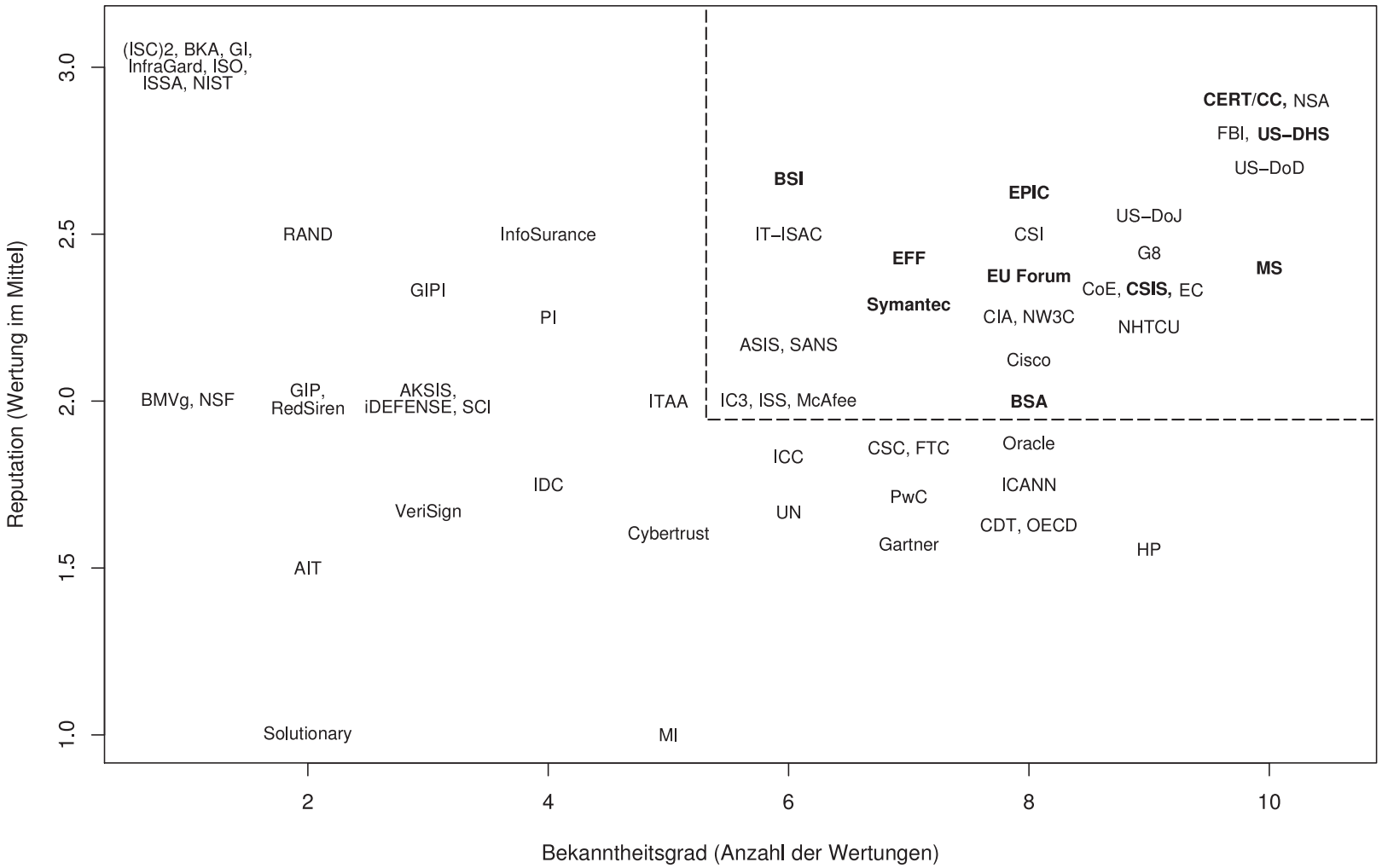


ABBILDUNG 1.2: *Schematischer Aufbau der Untersuchung*

ein globales Publikum wenden. Dennoch mag in der Wahl zweier englischsprachiger Publikationen die Gefahr einer Verzerrung zugunsten des anglo-amerikanischen Kulturraumes liegen. Dies erscheint allerdings angesichts begrenzter Forschungsmittel insofern vertretbar, als zumindest eine anfängliche und inter-subjektiv nachvollziehbare Annäherung an das relevante Akteurs-Set auf globaler Ebene möglich wird.

Sodann wurden aus diesen Artikeln all jene Organisationen herausgefiltert, die im Zusammenhang mit dem Politikfeld elektronischer Sicherheit Erwähnung fanden. Zugleich wurde die Häufigkeit der Nennungen der einzelnen Organisationen gezählt, wobei Organisationen, die innerhalb eines Artikels oder in verschiedenen Artikeln zu dem selben Thema und in der selben Zeitungsausgabe mehrfach erwähnt wurden, nur einfach



Datenquelle: Vorläufige Expertenbefragung. *Codierung*: 1 "less important", 2 "important", 3 "very important".

Abbildung 1.3: *Reputation und Bekanntheitsgrad der Akteure*

in die Wertung eingingen. Aufbauend hierauf wurde eine Liste jener Organisationen erstellt, die nach den oben genannten Kriterien zwei oder mehr Nennungen erhalten hatten. Diese Liste wurde in einem weiteren Schritt zusätzlich um solche Organisationen erweitert, die auf den mittels der Hypertext-Suchmaschine *Google*[8] ermittelten 100 meistverlinkten WWW-Seiten zum Stichwort „Cybercrime“ mit dem Politikfeld elektronischer Sicherheit in Verbindung gebracht wurden.

Die resultierende Organisations-Liste wurde zur vorläufigen Strukturierung des Akteurfeldes zehn ausgewählten internationalen Experten postalisch zur Bewertung und Ergänzung vorgelegt. Zur Ermittlung der Reputation der einzelnen Organisationen wurde folgende geschlossene Frage gestellt:

> Electronic information and communication systems such as the Internet are becoming more and more important for business transactions (eCommerce). The protection of these systems from criminal attacks is thus a crucial matter.
>
> Below you will find a list of world-wide organisations, companies, interest associations, and state agencies. In your view, what role do they play in planning, elaborating on and implementing measures and techniques to protect information and communication systems?

Die vorgegebene Skala möglicher Antworten reichte von „less important“ über „important“ bis „very important“. Ebenso konnte eine Organisation als nicht bekannt gekennzeichnet oder weitere wichtige Organisationen hinzugefügt werden, so daß im Ergebnis nicht notwendiger Weise jede Organisation von jedem Experten eine Wertung erhielt. In Folge dessen ließen sich je Organisation zwei Indizes errechnen: Eine arithmetisch gemittelte Reputation[9] im kontinuierlichen Wertebereich von eins bis drei einerseits, sowie ein – als Anzahl der auf die betreffende Organisation entfallenden Wertungen gemessener – diskreter Bekanntheitsgrad zwischen eins und zehn andererseits. Beide Indizes sind in Abbildung 1.3 in einem Streudiagramm abgetragen.[10]

In diesem Streudiagramm befinden sich jene Organisationen, die gemäß dieser Expertenbefragung sowohl eine hohe Reputation (≥ 2.0) als auch einen hohen Bekannt-

8 Vgl. <`http://www.google.com`>. Zu den Besonderheiten des Page-Ranking-Verfahrens von *Google* vgl. ferner Brin u. Page (2001).

9 Streng genommen ist das Merkmal der Reputation lediglich ordinal skaliert. Um einen arithmetischen Mittelwert errechnen zu können, wurde hier jedoch eine Intervallskalierung unterstellt. Dieser liegt die Annahme zugrunde, daß der Abstand zwischen den Ausprägungen „less important“ (1) und „important“ (2) äquivalent zu jenem zwischen „important“ (2) und „very important“ (3) ist.

10 Zur Bedeutung der Abkürzungen vgl. das Organisations-Glossar in Appendix A.

TABELLE 1.1: *Status und Scope der Organisationen, die nach der vorläufigen Expertenbefragung sowohl einen Bekanntheitsgrad* > 5 *als auch eine Reputation* ≥ 2.0 *aufwiesen*

	public	*mixed*	*private non-profit*	*private for-profit*
global	CIA, G8, NSA	**CERT/CC**	ASIS, **BSA**, **CSIS**, **EFF**, **EPIC**, SANS	Cisco, CSI, ISS, McAfee, **MS**, **Symantec**
regional	CoE, EC, **(ENISA)**	EU Forum		IABG
national	**BSI**, FBI, IC3, NHTCU, NW3C, **US-DHS**, US-DoD, US-DoJ	IT-ISAC		

heitsgrad (> 5) aufweisen, im oberen rechten Quadranten (hier gestrichelt dargestellt). Es liegt daher nahe, die im Rahmen einer vergleichenden Fallstudie näher zu untersuchenden Fallbeispiele aus diesem Quadranten auszuwählen. Die Wahl fiel (in alphabetischer Reihenfolge) auf folgende zehn Organisationen (in Abbildung 1.3 fett gedruckt): Business Software Alliance (BSA), Bundesamt für Sicherheit in der Informationstechnik (BSI), Center for Strategic and International Studies (CSIS), Computer Emergency Response Team/Coordination Center (CERT/CC), Electronic Frontier Foundation (EFF), Electronic Privacy Information Center (EPIC), European Network and Information Security Agency (ENISA), Microsoft (MS), Symantec, US Department of Homeland Security (US-DHS). Da es sich bei der ENISA um eine neu gegründete europäische Behörde handelt, die zum Zeitpunkt der Inhalts- und Reputationsanalyse noch nicht existierte, wurde diese ersatzweise für das EU-Forum herangezogen.

In Tabelle 1.1 sind die Organisationen des oberen rechten Quadranten nach *Status* und *Scope* aufgeschlüsselt. Ersichtlich wird hier, daß die gewählten Fallbeispiele (in Tabelle 1.1 fett gedruckt) zugleich sowohl alle Ebenen zwischen „national“ und „ global“, als auch alle *Status* zwischen „private for-profit“ und „public“ abdecken. Mit jeweils einem Repräsentanten dieser zehn Organisationen wurde im Jahr 2004 ein persönliches, strukturiertes Interview geführt. Im Verlauf dieser Interviews erweiterte sich die Menge der relevanten Organisationen noch einmal auf insgesamt einhundert Akteure, die in Appendix A jeweils mit einer Kurzbeschreibung glossatorisch zusammengefaßt sind.

1.4 Stand der Forschung

In Tabelle 1.2 findet sich eine Synopse zentraler politikwissenschaftlicher Literatur im Bereich der Regulierung vernetzter IuK-Technologien. Auffällig ist, daß sich nur sehr wenige Studien explizit sicherheitsrelevanten Themen zuwenden. Ist dies der Fall, so liegt der Fokus nahezu ausschließlich auf Teilaspekten wie etwa dem Datenschutz oder der Privatsphäre (Bennett 1988; Raab 1993, 2006; Farrell 2002, 2003; Long u. Quek 2002; Newman 2007), illegalen Inhalten (Zürn et al. 2000) oder unerwünschter Werbung (Just et al. 2006). Ausnahmen stellen hier das seit 2002 alle zwei Jahre erscheinende *International CIIP Handbook* (Abele-Wigert u. Dunn 2006), die Sammelbände von Sofaer u. Goodman (2001b) und Lewis (2003a), die Dissertation von Schulze (2006), die Journalartikel von Mendez (2005), Walden (2005) und Bauer (2009) sowie eine OECD-Studie (OECD 2012) dar. Vereinzelt werden Bedrohungen im Cyberspace auch als lediglich aus politischen Gründen konstruiert erachtet (bspw. Dunn Cavelty 2008).

Das *International CIIP Handbook* befaßt sich hauptsächlich deskriptiv mit nationalstaatlichen Politiken und Akteuren. Schulze (2006) analysiert in Sonderheit vergleichend die nationalen Politiken zum Schutz kritischer Informationsinfrastrukturen in Deutschland und den USA. Die Sammelbände von Lewis (2003a) sowie Sofaer u. Goodman (2001b) umfassen eine Reihe von Artikeln, in denen Möglichkeiten und Grenzen einer inter- und transnationalen Kooperation sowie internationaler Regime zum Schutz elektronischer Netzwerke diskutiert werden. Walden (2005) untersucht internationale Harmonisierungsbemühungen im Bereich nationaler Schutzpolitiken und der Artikel von Mendez (2005) analysiert den Einfluß föderaler Strukturen auf die Cybercrime-Politik der Europäischen Union. Bauer (2009) beleuchtet die Koevolution ökonomischer Anreizstrukturen, die zur Bedrohung kritischer Informationsstrukturen einerseits – sowie zu Bemühungen zu deren Schutz andererseits – führen. Die Studie der OECD (2012) vergleicht schließlich analytisch die Sicherheitsstrategien von zehn ausgewählten Staaten. Ebenfalls vergleichend geht Shackelford (2014) vor, konzentriert sich hierbei allerdings auf die rechtlichen Regulierungsbemühungen einzelner Staaten und sei deshalb hier nur der Vollständigkeit halber erwähnt.

Ganz allgemein scheint ein gewisser Konsens hinsichtlich einer zunehmenden Bedeutung von Mechanismen der Selbst- und Ko-Regulierung in globalen elektronischen Netzwerken zu bestehen (vgl. etwa Holitscher 1999; Christiansen 2000; Froomkin 2000; Marsden 2000a; Price u. Verhulst 2000; Latzer et al. 2002; Schneider 2002; Newman

TABELLE 1.2: *Ausgewählte Literatur zur Regulierung vernetzter IuK-Technologien*

Literatur	*Fokus*
Bennett (1988)	Politikfeld Datenschutz
Raab (1993, 2006)	Datenschutz-Governance
Schneider et al. (1994)	Harmonisierung europäischer Telekommunikationspolitiken
Eisner Gillett u. Kapor (1997)	Selbstregulierung des Internet
Johnson u. Post (1997)	rechtliche Regulierung des Internet
Schmidt u. Werle (1998)	internationale Standardisierung im Telekommunikationssektor
Abbate (1999a)	Governance von Informationsnetzwerken
Holitscher (1999)	Internet-Governance
Christiansen (2000)	(Selbst-)Regulierung des Internet
Marsden (2000b)	Regulierung der globalen Informationsgesellschaft (Sammelband)
Zürn et al. (2000)	Regulierung illegaler Inhalte im Internet
Cave u. Mason (2001)	Regulierung der Infrastruktur des Internet
Sofaer u. Goodman (2001b)	transnationale Kooperation zum Schutz elektronischer Netzwerke (Sammelband)
Baird (2002)	Internet-Governance
Farrell (2002, 2003)	Datenschutz zwischen USA und EU
Latzer et al. (2002)	Selbst- und Ko-Regulierung im Mediamatiksektor
Leib (2002)	Internet-Governance am Beispiel ICANN
Long u. Quek (2002)	Datenschutz zwischen USA und EU
Schneider (2002)	(Selbst-)Regulierung im IuK-Sektor
Lewis (2003a)	internationale Kooperation zum Schutz elektronischer Netzwerke (Sammelband)
Newman u. Bach (2004)	Selbstregulierung im IuK-Sektor in der EU und den USA
Mendez (2005)	Mehrebenen-Regulierung von Cybercrime in der EU
Walden (2005)	internationale Harmonisierung von Schutzpolitiken
Abele-Wigert u. Dunn (2006)	Übersicht von 20 nationalen und 6 internationalen Politiken zum Schutz kritischer Informations-Infrastrukturen
Just et al. (2006)	Regulierung unerwünschter Werbung
Schneider u. Hyner (2006)	Security-Governance im Internet
Schulze (2006)	Schutz kritischer Informations-Infrastrukturen in Deutschland und den USA
Newman (2007)	Schutz der Privatsphäre in Europa
Bauer (2009)	Koevolution ökonomischer Anreizstrukturen für Cybercrime and Cybersecurity
OECD (2012)	Vergleich von zehn nationalen Sicherheitsstrategien
Pawlak u. Wendling (2013)	Globale Regulierungsregime zum Schutz des Cyberspace
Shackelford (2014)	Analyse der rechtlichen Regulierung kritischer Informationsinfrastrukturen in China, der EU, Indien, dem UK und den USA

u. Bach 2004). Andererseits betonen Baird (2002) und Lewis (2003b) die nach wie vor bestehende Notwendigkeit staatlicher Initiative wenn nicht gar Intervention gerade in sicherheitsrelevanten Bereichen. Diese aber setze eine verstärkte internationale Kooperation öffentlicher Akteure voraus.

Keine der angeführten Studien untersucht allerdings die Bereitstellung des globalen Kollektivgutes Sicherheit in elektronischen Netzen aus der theoretischen Perspektive politischer Netzwerke, wie dies etwa – allerdings aus einer sehr viel umfassenderen sicherheitspolitischen Perspektive – bei Krahmann (2005) und Eilstrup-Sangiovanni (2005) der Fall ist. Da Politiknetzwerke in der Theorie globaler Steuerungsprozesse jedoch als vielversprechender Ansatz diskutiert werden (vgl. Abschnitt 2.2.3), verheißt gerade eine solche Untersuchung interessante Einsichten.

2 Die Steuerung sozialer Systeme

2.1 Zur Kybernetik komplexer Systeme

2.1.1 Ontologische und epistemologische Vorüberlegungen

Der Begriff des *Wissens* ist für die vorliegende Arbeit von doppeltem Interesse, da es einerseits Anspruch jeder wissenschaftlichen Arbeit ist, Wissen zu vermehren, andererseits aber Information als spezifische Form des Wissens eine zentrale Voraussetzung zielgerichteten Handelns darstellt. Letzteres gilt gerade in modernen Gesellschaften, in denen Information zu einer, wenn nicht gar *der* zentralen Ressource avanciert. Wissen ist somit elementarer Bestandteil jeden Handlungssystems und daher auch des zu untersuchenden Erkenntnisobjektes. Es erscheint deshalb sinnvoll, an den Anfang einige ideengeschichtliche und methodische Gedanken zum Begriff des Wissens sowie den Möglichkeiten seiner Erkenntnis zu stellen.

Ethymologisch hat Wissen (althochdeutsch *wizzan*, mittelhochdeutsch *wizzen*) zunächst dieselbe indogermanische Wurzel wie das lateinische *videre* und meint ursprünglich „gesehen haben“, was den Charakter des Wissens als einer auf Wahrnehmung beruhenden Erkenntnis unterstreicht (Drosdowski et al. 1989: 816). Der Begriff als solcher ist eng verwandt mit den Begriffen „weisen“ im Sinne von *zeigen*, „beweisen“ im Sinne von *belegen* und „witzig“ im Sinne von *geistreich*. Bei Kuhlen (1995: 38) findet sich Wissen nominal definiert als Ansammlung von Modellen „über Objekte bzw. Objektbereiche und Sachverhalte“, die „mit einem zu belegenden Anspruch für wahr“ gehalten werden. Entsprechend wurde schon in der griechischen Antike Wissen ($\epsilon\pi\iota\sigma\tau\eta\mu\eta$ – *episteme*) von anderen Aussagen wie Meinungen, Vermutungen und Annahmen ($\delta o\xi\alpha$ – *doxa*) explizit dahingehend unterschieden, daß ihm ein höherer Wahrheitsgehalt beigemessen werden könne, weil es im Gegensatz zu jenen begründbar sei.

Die antike und mittelalterliche Philosophie verbindet Wissen zunächst eng mit der metaphysischen und damit ontologischen Frage nach dem Urgrund des Seins, über das etwas ausgesagt werden soll. Idealistische Denkrichtungen verweisen hierbei in der Tra-

dition der Platonischen Ideenlehre auf eine transzendente Welt der Ideen[11], die als formende Ursache der Ursprung alles Seienden sei. Materialistische Philosophien hingegen berufen sich zumeist auf Demokrits Lehre von den Atomen und sehen in der Materie als Träger der Form das eigentlich Seiende. Die Aristotelische Kategorienlehre verbindet beide Vorstellungen im Begriff der Substanz, die allem Seienden in essentieller, artspezifischer Form zugrundeliege und zugleich als Träger weiterer veränderlicher Eigenschaften (Akzidenzien) fungiere.

Aufgrund seiner Eigenschaften kann nach Aristoteles alles Seiende begrifflich klassifiziert werden, indem bestimmte Arten (*species*) unter Angabe ihrer essentiellen Eigenschaften (*differentia specifica*) innerhalb einer allgemeineren Gattung (*genus*) abgegrenzt (definiert) werden. Entsprechend schreibt jede Aussage einer Entität die Zugehörigkeit zu einer übergeordneten Klasse als Prädikat zu und setzt damit zwei Begriffe in hierarchischen Bezug zueinander. Hierauf läßt sich eine allgemeine Aussagenlogik gründen, mit deren Hilfe innerhalb der korrespondierenden Begriffshierarchie sowohl vom Konkreten zum Abstrakten induktiv aufgestiegen, als auch in umgekehrter Richtung vom Universellen zum Speziellen deduktiv abgestiegen werden kann. Eine solche Logik ermöglicht die systematische Begründung von Aussagen im Wege eines deduktiven Beweises.

Grundlegend sind hierbei die von Aristoteles systematisch untersuchten Syllogismen. Als zentrale argumentative Schemata verdichten sie zwei gegebene Aussagen (Prämissen) deduktiv zu einer dritten (Konklusion). Möglich ist dies immer dann, wenn eine der beiden Prämissen (*propositio minor*) über einen gemeinsamen Mittelbegriff (*terminus medius*) auf einen Spezialfall der anderen, allgemeineren Aussage (*propositio maior*) rekurriert, sich diese also unter jene subsumieren läßt. Die *propositio maior* kann dabei auch als Implikation (Konditional), die *propositio minor* als Antezedenz und die Konklusion als Konsequenz aufgefaßt werden. Zugleich impliziert der notwendige Rekurs auf das Allgemeinere eine prinzipielle Letztbegründungsproblematik, da das Allgemeinste selbst nicht weiter begründbar ist. An die Stelle der Begründung muß eine Axiomatik treten, die sich bei Aristoteles auf induktive Evidenz beruft.

Mit der cartesianischen Wende rückt zu Beginn der Neuzeit ein weiterer Aspekt in den Mittelpunkt wissenschaftstheoretischer Überlegungen. Descartes unterstreicht mit seinem berühmten Diktum „cogito ergo sum“ explizit, daß am Anfang jeder Erkenntnis

11 Das altgriechische $\iota\delta\varepsilon\alpha$ (*idea*) meint in diesem Sinne *Vorstellung* oder *Urbild*.

ein bewußtes Ich steht, welches sich als wahrnehmende Instanz (Erkenntnissubjekt) von den wahrgenommenen Entitäten (Erkenntnisobjekten) distanziert, wobei es diese begrifflich zu erfassen bzw. gedanklich zu erschließen sucht. Hieraus folgt unmittelbar die epistemologische Frage nach der prinzipiellen Erkennbarkeit eines Seins jenseits des Bewußtseins, womit sich der Fokus von der Ontologie zur Epistemologie verschiebt. Zugleich stellt die Spaltung von Sein und Bewußtsein auch die traditionelle Ontologie vor neue Herausforderungen. Dies ist vor allem das erstmals von René Descartes als solches formulierte Leib-Seele-Problem, hinter dem sich die basale Frage verbirgt, ob sowohl Materie als auch Geist eigenständige Wesenheiten seien (Dualismus), oder ob sich das eine auf das andere oder gar beides auf ein drittes Prinzip zurückführen lasse (materialistischer bzw. idealistischer sowie neutraler Monismus). Ein weiteres Problem ergibt sich aus dem unklaren ontologischen Status gedanklich verallgemeinernder Vorstellungen, insbesondere der Frage, ob diese tatsächlich Formen der realen Welt widerspiegeln (Realismus) oder bloße Ordnungsstrukturen des Verstandes sind (Nominalismus).

Die epistemologische Frage nach der Erkennbarkeit des objektiven Seins bzw. des konkret Seienden knüpft daran unmittelbar an. Für René Descartes – und in der Folge rationalistische Denker wie Baruch de Spinoza, Gottfried Wilhelm Leibniz und später Immanuel Kant – kann sich das denkende Subjekt zunächst nur seiner eigenen Existenz zweifelsfrei bewußt sein, weshalb allein die ihm eigene Vernunft und mit ihr die Methode der Deduktion Grundlage jeder Erkenntnis sei. Die Philosophen des Empirismus – insbesondere Francis Bacon, David Hume und John Locke – hingegen unterstellen, daß ein Zugang zur objektiven Welt ausschließlich aufgrund sinnlicher Wahrnehmung möglich sei, weshalb Erkenntnis unmittelbar aus empirischer Erfahrung und damit Induktion resultiere. Jedoch weist bereits Hume darauf hin, daß allein die Phänomene an sich zweifelsfrei erkennbar seien, während die Kausalbeziehungen zwischen ihnen lediglich dem menschlichen Bedürfnis nach Ordnung entsprängen und sich einem induktiven Beweis entzögen. Auch Kant erkennt prinzipiell die Möglichkeit empirischer Erfahrung an, postuliert aber zugleich a priori existente Begriffsmuster und Kategorien der Vernunft wie Kausalität, Raum und Zeit, die jeder Wahrnehmung transzendental vorausgingen und daher jede Erkenntnis subjektiv vorstrukturierten, und lenkt so den Blick auf die Beschränkungen subjektiven Erkenntnisvermögens.

Neben Deduktion und Induktion findet sich bei Charles S. Peirce eine weitere – als Abduktion bezeichnete – Erkenntnismethode. Der argumentative Aufbau von Deduktion, Induktion und Abduktion läßt sich mit Hilfe von Prädikatenlogik und Mengentheo-

rie zur Veranschaulichung vereinfachend[12] wie folgt formalisieren: Es sei Ω die Menge aller möglichen Erkenntnisobjekte $x \in \Omega$. Die Konstante a bezeichne dann ein konkretes Objekt $a \in \Omega$. Ferner seien P und Q Prädikate zur Beschreibung bestimmter Objekteigenschaften.[13] M_P sei die Menge aller durch P, M_Q die Menge aller durch Q ausgezeichneten Objekte, so daß gilt: $M_P =_{def} \{x \in \Omega \,|\, P(x)\}$ und $M_Q =_{def} \{x \in \Omega \,|\, Q(x)\}$. Alle drei Argumentationsmuster lassen sich dann als Kombination folgender dreier Aussageformen darstellen, wobei jeweils von zwei Aussagen (Prämissen) auf die verbleibende dritte (Konklusion) geschlossen wird:

$$\forall x \, (P(x) \rightarrow Q(x)) \tag{2.1}$$

$$P(a) \tag{2.2}$$

$$Q(a) \tag{2.3}$$

Die generelle Universalaussage der Form 2.1 (Implikation) besagt, daß allen Objekten, auf die P zutrifft, auch Q zu eigen ist. Umgekehrt ist Q zwar notwendige, nicht aber zwingend auch hinreichende Bedingung für P. Die singulären Aussagen der Form 2.2 (Antezedenz) und 2.3 (Konsequenz) besagen, daß dem konkreten Objekt a die Eigenschaften P und Q zu eigen sind, beschreiben also Einzelbeobachtungen.

Die *Deduktion* schließt von zwei Prämissen der Form 2.1 und 2.2 auf eine Konklusion der Form 2.3. Sie argumentiert, weil ein Objekt a gemäß der Prämisse 2.2 die Eigenschaft P besitze, sei ihm auch Q zu eigen. Da nach der Implikation 2.1 Q von P determiniert wird, wird der Wahrheitswert der Antezedenz 2.2 zwingend auf die Konsequenz 2.3 transferiert. Folglich ist ein solcher Schluß wahrheitserhaltend. Aufgrund der Implikation 2.1 gilt: $M_P \subseteq M_Q$; aufgrund der Antezedenz 2.2: $a \in M_P$. Es folgt in der Konsequenz 2.3 transitiv: $a \in M_Q$. Damit ist zugleich unmittelbar einsichtig, daß eine deduktive Konklusion keinerlei heuristischen Nutzen hat, da sie weder bezüglich der Objekte, noch bezüglich der Eigenschaften über das in den Prämissen gesagte hinausgeht, sondern lediglich bestehende Aussagen analytisch transformiert.

Die *Induktion* hingegen schließt von zwei Prämissen der Form 2.3 und 2.2 auf eine

12 Aus Gründen der Vereinfachung werden hier nur einstellige Prädikate – also nur Aussagen über Eigenschaften ein und desselben Objektes – berücksichtigt.

13 Nach Bunge u. Mahner (2004: 25 ff.) muß zwischen den Begriffen „Eigenschaft“ und „Prädikat“ insofern unterschieden werden, als ersterer reale Attribute referenziert, während letzterer sich auf deren begriffliche bzw. kognitive Repräsentanzen bezieht.

Konklusion der Form 2.1. Sie argumentiert, wenn ein Objekt a sowohl eine Eigenschaft P als auch eine Eigenschaft Q aufweise, könne mit einer gewissen Wahrscheinlichkeit ein implikativer Zusammenhang zwischen beiden Eigenschaften hergestellt werden. Um diesen zweifelsfrei zu beweisen müßte gelten: $M_P \subseteq M_Q$. Gemäß der Antezedenz 2.2 gilt: $a \in M_P$. Ferner gilt gemäß der Konsequenz 2.3: $a \in M_Q$. Daraus folgt aber nicht notwendiger Weise $M_P \subseteq M_Q$, sondern nur, daß M_P und M_Q nicht disjunkt sind: $a \in M_P \cap M_Q$. Ein induktiver Schluß ist daher logisch nicht zwingend und somit auch nicht wahrheitserhaltend, es kann ihm kein sicherer Wahrheitswert zugeordnet werden. Da jedoch M_P und M_Q nicht disjunkt sind, impliziert die Tatsache, daß ein beliebiges Objekt x die Eigenschaft P besitzt offenbar auch, daß ihm zumindest tendenziell ebenfalls Q zu eigen ist. Es besteht also eine konditionale Wahrscheinlichkeit für Q in Abhängigkeit von P und damit ein stochastischer Zusammenhang zwischen beiden Eigenschaften.

Legt man nun dem induktiven Schluß nicht nur die Beobachtung eines einzelnen Objektes a, sondern die einer Menge $A =_{def} \{a_1 \dots a_n\}$ von Objekten zugrunde, für die $A \subset M_P$ gilt, und kann von einer zufälligen Disposition der Eigenschaft Q für alle $x \in A$ ausgegangen werden, ist also A nicht das Ergebnis einer (teilweisen) Selektion nach Q, so kann aus der Häufigkeitsverteilung von Q für alle $x \in A$ die konditionale Wahrscheinlichkeit von Q in Abhängigkeit von P geschätzt werden, weil nach dem Gesetz der großen Zahlen mit steigendem n die Häufigkeitsverteilung stochastisch gegen eben diese Wahrscheinlichkeit konvergiert. Die Begründung eines Induktionsschlusses ist somit letztlich probabilistisch und daher prinzipiell fallibel. Da die Induktion jedoch die Aussage der Prämisse 2.3 hinsichtlich der Eigenschaft Q auf alle Elemente der Menge M_P erweitert, führt sie zugleich neues Wissen synthetisch ein, ist also unbestreitbar von einem gewissen heuristischen Nutzen.

Die *Abduktion* schließlich folgert von zwei Prämissen der Form 2.1 und 2.3 auf eine Konklusion der Form 2.2. Sie argumentiert, wenn die Antezedenz 2.2 wahr wäre, wenn also a die Eigenschaft P zukäme, so ließe sich aufgrund der Implikation 2.1 erklären, warum a in der Konsequenz 2.3 auch Q zu eigen ist. Es wird also unterstellt, daß gilt: $a \in M_P$. Bekannt ist jedoch nur, daß in der Konsequenz 2.3 gilt: $a \in M_Q$. Aus der Implikation 2.1 folgt sodann lediglich zwingend, daß Q für P notwendige, nicht aber zugleich auch, daß es für dieses hinreichende Bedingung ist. Es gilt also: $M_Q \supseteq M_P$. Im Grenzfall $M_Q = M_P$ gälte dann auch: $\forall x\,(Q(x) \rightarrow P(x))$. In diesem Fall ginge die Abduktion also in eine Deduktion über. Gilt aber $M_Q \supset M_P$, so folgt daraus, daß prin-

zipiell auch gelten könnte: $a \in M_Q \triangle M_P \Leftrightarrow a \notin M_P$. Ein abduktiver Schluß kann daher nur intuitiv begründet werden. Es können ihm weder Wahrheitswerte noch Wahrscheinlichkeiten zugeordnet werden. Vielmehr hat er rein hypothetischen Charakter. Zugleich aber weist er den höchsten heuristischen Nutzen auf, da die Konklusion $P(a)$ dem Objekt a die bisher an ihm unbekannte spezifische Eigenschaft P zuschreibt und somit dessen vollkommen neue Klassifizierung ermöglicht. Die Abduktion erschließt also das Mögliche bzw. Problematische, die Induktion das Wahrscheinliche bzw. Assertorische und die Deduktion das Notwendige bzw. Apodiktische.

Peirce geht weiter davon aus, daß die Vernunft nur auf der Grundlage von Zeichen operieren könne. Daher interpretiere das Subjekt auch jede sinnliche Erfahrung als Zeichen. Diese Interpretation vollziehe sich abduktiv, indem von einer als Zeichen wahrgenommenen Eigenschaft Q auf einen möglichen Zusammenhang $P \rightarrow Q$ und daraus wiederum auf P als Definitionskriterium einer begrifflichen Klassifizierung der Erkenntnisobjekte geschlossen werde, wodurch neues Wissen entstehe. Dieses ist jedoch aufgrund des intuitiven Charakters der Abduktion zunächst hypothetischer Natur, weshalb ein unmittelbarer Zugang zur Realität der Erkenntnisobjekte nicht möglich sei. Maßstab des Wahrheitswertes einer Aussage könne daher auch nicht die von der Korrespondenztheorie des Realismus geforderte Übereinstimmung von Begriff und Realität sein, da die Realität selbst nur ein unscharfer Begriff sei (Peirce 1878). Vielmehr liege der Nutzen einer Erkenntnis vor allem darin, daß sie intersubjektive Gültigkeit besitze und daher in einem konkreten Interaktionskontext Wirksamkeit entfalten könne. Die Peircesche Philosophie des Pragmatismus erhebt diesen Nutzen daher zum zentralen Kriterium des Wahrheitswertes einer Aussage. Im Ergebnis besteht somit jeder Erkenntnisprozeß letztlich aus einem Dreiklang von Abduktion, Deduktion und Induktion. Aus abduktiv gewonnenen Hypothesen werden deduktiv Handlungsstrategien hergeleitet und diese schließlich in einer konkreten Handlung einer induktiven Bewährung unterzogen.

Parallel zu Peirce beschäftigt sich auch Ferdinand de Saussure mit semiotischen Fragen, allerdings bezieht er den Begriff des Zeichens im Gegensatz zu diesem ausschließlich auf sprachliche Begriffe. Mit Namen wie Ludwig Wittgenstein, Gottlob Frege und Bertrand Russell verbindet sich dann im Rahmen des *Linguistic Turn* eine allgemeine Hinwendung von Philosophie und Wissenschaftstheorie zu einer sprachanalytischen Betrachtung des Erkenntnisprozesses. Es rückt vermehrt die semantische Frage nach den begrifflichen Strukturen, auf und innerhalb derer jede Form der Erkenntnisgewinnung diskursiv operiert, in den Mittelpunkt des Interesses. Im Strukturalismus geht es dabei

zunächst um die strukturellen Relationen der Begriffe zueinander, während der Post-Strukturalismus stärker die sie konstituierenden Differenzen hervorhebt.

Konstruktivistische Theorien hingegen fokussieren auf die intersubjektiven Konstruktionsprozesse kognitiver Strukturen. Der Radikale Konstruktivismus postuliert hier eine selbstreferentielle, operationale Geschlossenheit des neurobiologischen Erkenntnisapparates und steht daher der Erkennbarkeit einer objektiven Realität prinzipiell skeptisch gegenüber (vgl. Maturana 1980). Der Wahrheitswert einer Aussage reduziert sich so auf ihre Widerspruchsfreiheit im Rahmen eines hermetisch abgeschlossenen, autopoietischen Aussagesystems (Kohärenztheorie). Der Methodische Konstruktivismus hingegen bestreitet die Erkennbarkeit einer objektiven Realität nicht grundlegend, konstatiert aber als zentrale These, daß sich das Subjekt diese ausschließlich mittels einer konstruierten Begrifflichkeit kognitiv aneignen könne. Diese Begrifflichkeit ist für den Methodischen Konstruktivismus schon allein deshalb teleologisch, weil jede Form von Sprache per se auf den Zweck der Kommunikation ausgerichtet ist. Diese Orientierung am Handeln spiegelt sich auch in der Konzeption des Subjektes als *homo faber* wider, der weite Teile seiner Lebenswelt faktisch selbst erschafft, weshalb Erkennen sowohl Entdecken als auch Erfinden bedeute (vgl. bspw. Mittelstraß 2001). Ausgangspunkt jeder Wissenschaft ist dann eine explizite Rekonstruktion ihrer Terminologie auf Grundlage einer dialogischen und damit interaktiven Logik.

Auch der Neo-Positivismus des Wiener Kreises um Moritz Schlick und Rudolf Carnap bemüht sich unter dem Einfluß des *Linguistic Turn* um eine klärende Rekonstruktion wissenschaftlicher Termini im Wege einer logischen Analyse, sucht dabei jedoch zugleich über die empirische Verifikation eine Rückbindung an die objektive Realität. Zentrale Forderung ist, daß jede wissenschaftliche Aussage auf elementaren Basissätzen – also konkreten Beobachtungen – beruhen, oder aber sich als synthetisches Wissen aus solchen Beobachtungen logisch ableiten lassen müsse. Genau diese induktive Verifizierbarkeit aber bestreitet Popper (1934, 1972) angesichts der Fallibilität eines jeden Erweiterungsschlusses grundlegend. Albert (1968, 2000) weist ferner darauf hin, daß auch jeder Versuch einer deduktiven Verifikation allgemeiner Aussagen in einem Trilemma münde, da er entweder einen logischen Zirkelschluß, einen infiniten Regreß oder eine willkürliche Dogmatik zum Ausgangspunkt nehmen müsse, und unterstreicht damit noch einmal das bereits angesprochene Letztbegründungsproblem.

In der Folge sieht der Kritische Rationalismus prinzipiell von der Möglichkeit abschließender Erkenntnis ab, geht aber als hypothetischer Realismus dennoch von der

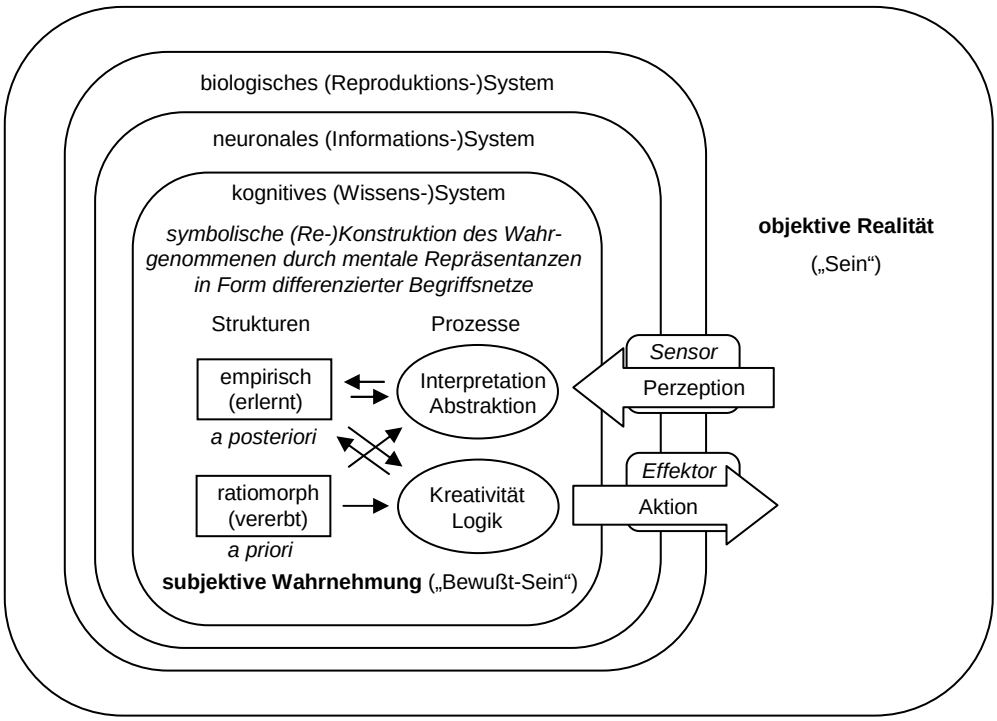


ABBILDUNG 2.1: *Systemtheoretisch modellierter Erkenntnisprozeß*

Existenz einer objektiven Wirklichkeit jenseits unseres Bewußtseins aus, über die mittels intuitiver Vernunft hypothetische Aussagen getroffen werden können. Die empirische Erfahrung übernimmt dabei die Funktion eines kritischen Regulativs der an sich fehlbaren Vernunft. Möglich wird dies aufgrund einer Asymmetrie in der Verifikation und Falsifikation allgemeiner Aussagen. Diese resultiert aus dem Umstand, daß affirmative Universalaussage $\forall x\,(P(x) \rightarrow Q(x))$ und negierende Partikularaussage $\exists x\,(P(x) \wedge \neg Q(x))$ kontradiktorisch sind.[14] Eine negierende Partikularaussage läßt daher einen zweifelsfreien Rückschluß auf die Falschheit der korrespondierenden affirmativen Universalaussage zu. Einzelbeobachtungen können somit als methodische Selektoren zur Überprüfung deduktiv hergeleiteter Theorien herangezogen werden. Diese Theorien behalten jedoch dauerhaft hypothetischen Status, da sie nicht abschließend zu beweisen, sondern nur durch wiederholt mißlungene Falsifikation evolutionär fortschreitend zu „erhärten“ sind. Daraus folgt zugleich, daß ein endgültiges Urteil über den Wahr-

14 Gleiches gilt auch im Verhältnis von negierender Universalaussage $\forall x\,(P(x) \rightarrow \neg Q(x))$ und affirmativer Partikularaussage $\exists x\,(P(x) \wedge Q(x))$.

heitswert einer allgemeinen Aussage letztlich nicht möglich ist, sondern ihr lediglich eine vorläufige, epistemische Wahrscheinlichkeit unterhalb der absoluten Sicherheit zugeschrieben werden kann. Mithin kann im Prozeß der Erkenntnis die objektive Realität bestenfalls asymptotisch approximiert werden.

Das Erkenntnismodell des Kritischen Rationalismus verbindet sich auf natürliche Weise mit einer an Konrad Lorenz (1973) orientierten Evolutionären Erkenntnistheorie (vgl. Kappelhoff 2003b). Diese erklärt Struktur und Funktionsweise des menschlichen Erkenntnisapparates als Ergebnis eines biologischen Adaptionsprozesses. Ist der Erkenntnisapparat für Kant noch subjektiv a priori und somit transzendental vorgegeben, so versteht ihn die Evolutionäre Erkenntnistheorie als genotypische Prädisposition und daher zugleich als evolutionsgeschichtlich a posteriori. Kognitive Wissensstrukturen bilden aus einer solchen Perspektive das Resultat einer evolutionären Mehrebenen-Adaption. Abbildung 2.1 faßt die bisher vorgestellten Aspekte der Erkenntnisgewinnung noch einmal im Vorgriff auf die im nächsten Abschnitt erläuterten systemtheoretischen Konzepte modellhaft zusammen.

2.1.2 Ordnungsbildung in komplexen Systemen

Jede Einzelwissenschaft setzt ein metaphysisches Paradigma (Kuhn 1962) schon deshalb voraus, weil sie zur Definition ihrer eigenen Terminologie einen archimedischen Punkt, eine ontologische Taxonomie jenseits ihres eigenen Horizonts, benötigt. Erst von einem solchen Punkt aus kann sie ihr eigenes Begriffsnetz ausdifferenzieren, ohne zugleich den Anschluß an den allgemeinen Wissenschaftsdiskurs zu verlieren. Es stellt sich somit die Frage, welche Anforderungen an eine dementsprechende Ontologie zu richten sind. Ausgehend von den in Abschnitt 2.1.1 skizzierten Überlegungen läßt sich hierfür eine Reihe von Kriterien herleiten:

1. Aufgrund des Letztbegründungsproblems der Deduktion sowie einer prinzipiellen Fallibilität des Induktionsschlusses kann auch eine ontologische Theorie nur hypothetischen und damit vorläufigen Modellcharakter haben. Erkenntnis ist daher niemals abschließend oder umfassend.
2. Die Einsicht, daß Erkenntnis sich offenbar interaktiv vollzieht, setzt die Annahme der Existenz einer realen Welt voraus.
3. Jede Form der Aktion ist zielgerichtet, d. h. mit jeder Handlung wird ein subjektiver Zweck verfolgt, und sei es nur derjenige der Erkenntnis. Zielgerichtetes Handeln aber setzt die Existenz natürlicher Regel- bzw. Gesetzmäßigkeiten voraus, die das Ergebnis einer Handlung kalkulierbar machen.

Die Erkenntnis dieser Regelmäßigkeiten erklärt die Realität, weil sie im scheinbaren Chaos zielgerichtetes Handeln ermöglicht.

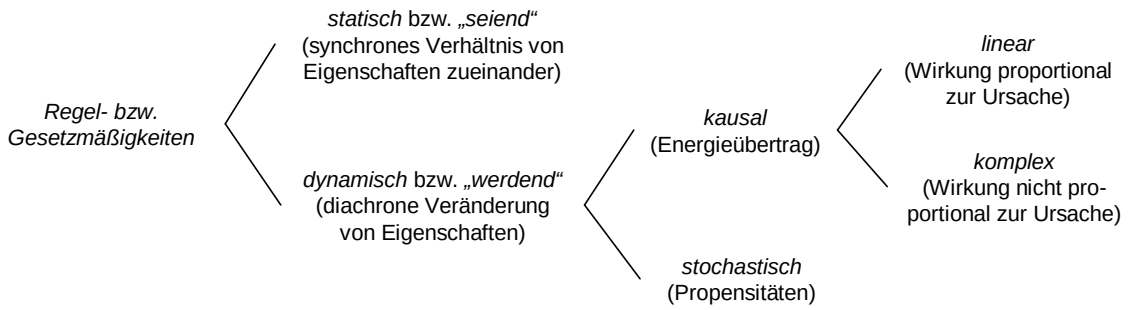
4. Jeder Kognitionsapparat muß, um mit der Realität interagieren zu können, selbst Teil dieser sein. Er kann sie daher nur symbolisch-abstrakt und partiell beschreiben. Das zugrundeliegende symbolische Begriffsnetz organisiert sich autopoietisch, da es seine Struktur aus sich heraus konstruieren und aufrecht erhalten muß. Zugleich aber besteht durch Interaktion eine permanente Rückkopplung an die Realität. Kognitive Dissonanzen führen zu Restrukturierungsprozessen.

Unter Berücksichtigung dieser Kriterien wird als basale Theorie zunächst eine materialistische Ontologie in Anlehnung an Bunge u. Mahner (2004) herangezogen (vgl. auch Schneider 2006). Diese setzt – aus der aristotelischen Metaphysik bereits bekannte – Entitäten[15] voraus, die ihrer Substanz nach als materiell existent und somit real gegeben angesehen werden. Diesen Entitäten kommen sodann essentielle Eigenschaften zu, welche deren artspezifischen Charakter konstituieren. Bei einer Veränderung oder einem Wegfall dieser Eigenschaften hört eine Entität auf als solche zu existieren. Darüber hinaus können Entitäten über eine Reihe weiterer, akzidentieller Eigenschaften verfügen, deren Veränderung oder Wegfall ohne Bedeutung für ihre Existenz an sich ist. Eigenschaften können einer bestimmten Entität intrinsisch – unabhängig von anderen Entitäten – zu eigen sein, oder aber aus der Relation mehrerer Entitäten zueinander resultieren.

Energie wird als universelle Eigenschaft aller Dinge aufgefaßt und mit deren prinzipieller Fähigkeit zur Veränderung ihrer Eigenschaften gleichgesetzt. Eigenschaften sind vor diesem Hintergrund potentiell kontingent und damit eine variable Größe. Unter dem Zustand einer Entität wird der Vektor all ihrer Eigenschaften zu einem bestimmten Zeitpunkt verstanden. Zustandsänderungen (Ereignisse) können quantitativ oder qualitativ sein. Im ersten Falle handelt es sich um eine Variation bzw. Transformation des Zustandsvektors, im zweiten hingegen um das Hinzutreten neuer bzw. das Wegfallen bestehender Eigenschaften und damit eine Redimensionierung des Zustandsraumes. Raum und Zeit ergeben sich sekundär aus der synchronen Ordnung des Universums aller Dinge, sowie aus der diachronen Abfolge ihrer Zustände.

Die Geschichte einer Entität entspricht einer Kette von Ereignissen – einem Prozeß – und läßt sich als geometrische Verhaltenskurve (Trajektorie) in einem multidimensiona-

15 Im Folgenden wir dieser Begriff synonym zu *Ding* bzw. *Sache* verwandt.



Quelle: Eigene Darstellung in Anlehnung an Bunge u. Mahner (2004).

Abbildung 2.2: *Typologie ontischer Regel- bzw. Gesetzmäßigkeiten*

len Zustandsraum darstellen. Jeder Punkt dieses Raumes entspricht einem bestimmten Zustandsvektor, d. h. einem Tupel konkreter Eigenschaften. Alle Zustandsänderungen folgen kausalen oder stochastischen Regel- bzw. Gesetzmäßigkeiten (vgl. hierzu Abbildung 2.2), so daß Ereignisse in einem weiteren Sinne determiniert sind. Da stochastische Prozesse im Gegensatz zu Kausalketten jedoch nicht auf einem Energieübertrag zwischen zwei Entitäten, sondern auf zufälligen Neigungen (Propensitäten) einzelner Entitäten beruhen, sind sie nicht streng deterministisch und daher irreversibel. Hierin liegt zugleich der Grund für die Gerichtetheit der Zeit. Gesetzmäßigkeiten sind selbst Eigenschaften von Entitäten, existieren also nur durch und mit diesen. Sie erlauben innerhalb des allgemeinen Zustandsraumes einer Entität die Eingrenzung eines nomologischen Zustandsraumes, der die Untermenge aller real erreichbaren Zustände umfaßt. Die Erkenntnis kausaler und stochastischer Zusammenhänge ermöglicht in letzter Konsequenz deduktiv-nomologische Erklärungen nach dem von Hempel u. Oppenheim (1948) formalisierten Schema.

Neben einfachen Entitäten existieren solche, die selbst aus einem Aggregat oder einer Kombination anderen Entitäten bestehen. Sind Entitäten Kombinationen, so zeichnen sie sich durch eine eng gekoppelte Architektur ihrer Bestandteile aus, d. h. die sie konstituierenden Komponenten sind in eine kohäsive Struktur – ein System – eingebunden. Strukturen sind nach Bunge u. Mahner (2004: 72 ff.) bindende relationale Eigenschaften (Verknüpfungen), die sich unmittelbar auf den Zustand der durch sie verbundenen Dinge auswirken. Ein System als Ganzes definiert sich daher im Gegensatz zum Aggregat nicht allein durch die Menge seiner Komponenten, sondern vor allem durch seine innere Verbundenheit, seine Endostruktur. Der Zustandsvektor eines

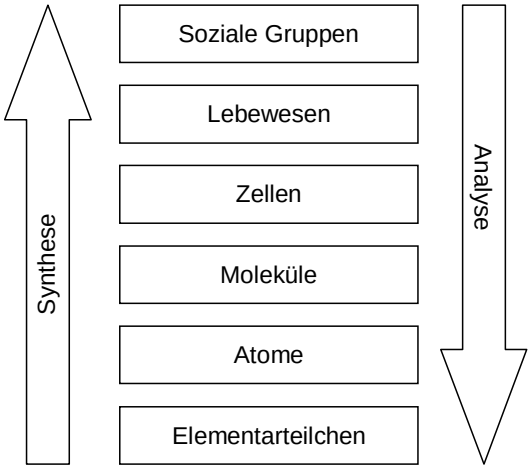
Systems umfaßt neben resultanten Eigenschaften, die sich unmittelbar aus den Zuständen seiner Komponenten ergeben, auch emergente Eigenschaften, die nur dem System als Ganzem zukommen.

Außer dem alles umfassenden System des Universums existieren de facto keine vollkommen isolierten Systeme,[16] so daß jedes System – mit Ausnahme des Universums – immer auch über Verbindungen zu Entitäten in seiner Umgebung und damit eine Exostruktur verfügt. Solchermaßen offene Systeme aber haben funktionalen Charakter. Sie nehmen Stimuli aus ihrer Umgebung auf und geben selbst Ereignisimpulse an diese ab. Mathematisch läßt sich dies als Abbildung einer Eingangs- auf eine Ausgangsgröße darstellen. Der zugrundeliegende Zusammenhang ist jedoch nicht zwangsläufig algebraischer Natur. Statische Systeme verändern ihren Zustand vor diesem Hintergrund ohne äußere Einwirkungen nicht; dynamische hingegen durchlaufen aus sich heraus kontinuierliche Zustandsänderungen. Häufig handelt es sich bei dynamischen zugleich um komplexe Systeme, die aus einer Vielzahl hochgradig diversifizierter, vielfältig vernetzter Komponenten bestehen. Komplexe Systeme sind aufgrund interner Wechselwirkungen i. d. R. nicht linear, d. h. Ein- und Ausgangsgrößen verhalten sich nicht proportional zueinander. Die Grenze zwischen System und Umwelt ist nicht immer eindeutig definiert. Dynamische Systeme können im Laufe ihrer Ontogenese Komponenten aus ihrer Umwelt aufnehmen oder an diese abgeben. Auch können Komponenten in bestimmten Fällen gleichzeitig Teil verschiedener Systeme sein.

Als zusammengesetzte Entitäten können Systeme per definitionem ineinander verschachtelt sein. Faktisch ist daher jedes Ding entweder selbst ein System und/oder Teil eines Systems. Diese Omnipräsenz funktionaler, systemischer Strukturen begründet den integrativen Charakter, den die formalen Strukturwissenschaften der Mathematik sowie der Allgemeinen Systemtheorie (vgl. von Bertalanffy 1956, 1968) als interdisziplinäres Fundament sämtlicher Realwissenschaften entfalten.[17] Darüber hinaus legt sie eine Untergliederung des Universums aller Dinge in ontische Systemschichten nahe, wie sie bspw. Oppenheim u. Putnam (1958) vornehmen (vgl. Abbildung 2.3), wobei sich ebe-

16 Gäbe es sie, so wären sie aufgrund ihrer Isoliertheit für den Rest des Universums gleichwohl irrelevant. Sie entzögen sich per definitionem jeder Wechselwirkung mit der Außenwelt und könnten aus dieser heraus daher auch nicht erkannt werden. Sollte der Betrachter aber selbst Teil eines isolierten Systems sein, so erschiene ihm dieses als eigentliches Universum.

17 Zugleich veranlaßt sie etwa Schwegler (1992) zum Versuch einer nicht substantialistischen Ontologie, die statt substantieller Entitäten Relationen zum Ausgangspunkt nimmt.



Quelle: Oppenheim u. Putnam (1958).
Eigene Darstellung.

Abbildung 2.3: *Ontische Schichten bzw. Entitätsebenen im Physikalismus*

nenübergreifend strukturelle Isomorphien abzeichnen. Ein solches Modell verleitet zu der Annahme, jede Ebene ließe sich auf die jeweils darunter liegende zurückführen, alle Entitäten seien also letztlich mit Hilfe physikalischer Gesetzmäßigkeiten zu erklären. Ein derartiger, reduktionistischer Physikalismus vernachlässigt allerdings die Existenz emergenter Systemeigenschaften. Da diese nur einem System als Ganzem zukommen, lassen sie sich nicht allein auf dessen Bestandteile zurückführen. Vielmehr ist Emergenz gleichbedeutend mit der Bildung einer höheren systemischen Ordnung, die zu qualitativ völlig neuen Eigenschaften führt (vgl. hierzu bspw. Krohn u. Küppers 1992). Daraus folgt, daß auf jeder ontischen Systemebene neue Gesetzmäßigkeiten auftreten, welche sich aus denen der darunter liegenden Ebenen nicht unmittelbar herleiten lassen.

Ordnung kann mit der Regelmäßigkeit von Ereignissen gleich gesetzt werden. Sie geht daher immer mit einer Einengung des nomologischen Zustandsraumes einer Entität einher. Umgekehrt entspricht Unordnung dessen Ausweitung. Ordnung entsteht durch kausale Determination, Unordnung durch stochastisches Chaos bzw. Propensitäten. Weil Kausalität jedoch einen Energieübertrag voraussetzt, ist eine globale Zunahme von Ordnung in isolierten Systemen – in Übereinstimmung mit dem zweiten Hauptsatz der Thermodynamik – nicht zu erwarten. Ganz im Gegenteil strebt ein solches System – und damit auch das Universum als Ganzes – aufgrund der Akkumulation stochastischer Prozesse aller Wahrscheinlichkeit nach einer maximalen Entropie und damit Unordnung

zu. Ordnungsbildung ist dabei nur lokal möglich, indem sich komplexe Subsysteme herausbilden, die selbst Energie und/oder Entropie exportieren und damit zu Lasten ihrer Umwelt einen höheren Ordnungsgrad erreichen.

Die Selbstorganisation komplexer Systeme kann entweder auf konservativer (reversibler) oder dissipativer (irreversibler) Basis erfolgen (vgl. Mainzer 2004: 59 ff.). Im ersten Falle ist Ordnung typischer Weise das Ergebnis eines energiearmen Gleichgewichts, d. h. ein System verliert so lange Energie an seine Umwelt, bis es selbst zu keinerlei Veränderung mehr fähig ist und damit in einen statischen Zustand übergeht. Sofern ihm von außen keine weitere Energie zugeführt wird, verharrt dieses System dann in einem stabilen thermodynamischen Gleichgewicht stationär auf einem Fixpunkt seines Zustandsraumes. Beispiele sind etwa kristalline oder auch virale Strukturen. In dissipativen Systemen hingegen findet ein kontinuierlicher Austausch von Energie und/oder Komponenten zwischen System und Umwelt statt. Hierbei kompensiert das System im Rahmen eines Fließgleichgewichts permanent interne Verfallsprozesse und externe Störungen, wie das bspw. in Metabolismen der Fall ist.

In der Chaostheorie wird eine Teilregion im Zustandsraum eines Systems, aus der keine Trajektorien hinausführen, die also ohne äußere Einwirkung nicht wieder verlassen wird, als Attraktor bezeichnet (vgl. Kauffman 1993: 175 ff.). Da solche Attraktoren offenbar eine Einengung des nomologischen Zustandsraumes zur Folge haben, wirken sie ordnungsbildend. Alle Trajektorien, die gegen einen Attraktor konvergieren, gehören dabei zu dessen Einzugs- bzw. Attraktionsbereich. Je mehr Ausgangszustände im Einzugsbereich eines Attraktors liegen, desto stabiler ist die mit ihm verbundene Ordnung, da sich das System auch nach einer Störung mit hoher Wahrscheinlichkeit noch immer im Einzugsbereich des selben Attraktors befindet. Attraktoren können sowohl aus einem stationären Fixpunkt als auch aus einer oder mehreren Trajektorien bestehen. Häufig bilden diese Trajektorien periodische Zyklen. Es existieren aber auch seltsame Attraktoren, die aperiodische Trajektorien aufweisen. Diese Trajektorien bilden fraktale Geometrien, i. e. sie falten sich auf engstem Raum zusammen. Trotz ihrer Beschränkung auf eine Teilregion des Zustandsraumes können sie daher eine Vielzahl von Zuständen umfassen. Innerhalb dieser entfernen sich anfänglich benachbarte Trajektorien zugleich exponentiell voneinander, wodurch ein deterministisches Chaos nichtlinearer Zustandsänderungen entsteht (vgl. Kappelhoff 2003a).

Je kleiner ein Attraktor ist, je weniger Zustände er also umfaßt, umso höher ist der Grad an erreichter Ordnung. Die Dynamik komplexer Systeme läßt sich somit

zwischen den Polen einer absoluten Ordnung und eines deterministischen Chaoses verorten. Der absoluten Ordnung entspricht ein minimaler Attraktor (Fixpunkt), dem deterministischen Chaos hingegen ein seltsamer Attraktor. Eine Reihe herausgehobener Systemvariablen beeinflußt unmittelbar die Charakteristik der Attraktoren eines Systems und damit auch dessen Ordnung und Stabilität. Zu diesen essentiellen Eigenschaften, die im Folgenden als Parameter bezeichnet werden, gehören auf abstraktester Modellebene bspw. Zahl, Art und Diversifikation der Komponenten; der Grad der internen Vernetzung sowie der spezifische Modus der Verknüpfungen. Spannt man über diesen Parametern einen multidimensionalen Raum auf, so entspricht jeder Punkt in diesem Parameterraum genau einem konkreten Parametervektor und damit zugleich einer spezifischen Ordnung des zugehörigen Systems. Der Parameterraum selbst zerfällt hierbei in diskrete Partitionen, an deren Grenzen Bifurkationen in dieser Ordnung – Phasenübergänge von Chaos zu stabiler Ordnung und umgekehrt – auftreten.

Ordnung ist demnach nicht nur eine emergente Systemeigenschaft, sondern zugleich auch Conditio sine qua non einer dauerhaften Existenz des Systems. Wird dieses durch eine extern induzierte Änderung (Störung) seiner Parameter in nicht-deterministisches Chaos abgedrängt, so hört es auf als integrierte, funktionale Entität zu existieren. Faktisch unterliegen daher alle komplex-dynamischen Systeme einem permanenten Streß durch externe Störungen, der sich unmittelbar aus ihrer Einbettung in eine Ökologie weiterer Systeme und einer daraus resultierenden Dynamik externer Ereignisse ergibt. Die Überlebenschance (Fitneß) eines Systems wird vor diesem Hintergrund wesentlich von der Fähigkeit seiner Ordnung bestimmt, äußere Einflüsse so zu verarbeiten, daß eben diese Ordnung möglichst wenig gefährdet wird.

Komplexe dynamische Systeme sind somit gezwungen ihre Ordnung weitgehend an die Erfordernisse ihrer Umgebung anzupassen. Als komplex-adaptive Systeme wandern sie – getrieben durch den Druck der Selektion – auf der Suche nach immer höherer Fitneß durch ihren Parameterraum (vgl. Ashby 1960). Gewichtet man nun jeden Punkt im Parameterraum eines Systems mit dem spezifischen Fitneßwert seiner korrespondierenden Ordnung, so ergibt sich das Bild einer Fitneßlandschaft, in der komplex-adaptive Systeme jeweils angrenzenden Orten höherer Fitneß zustreben. Ob ein solches Vorgehen jedoch zum Erreichen des globalen Fitneßgipfels führt, hängt wesentlich von der Topologie der jeweiligen Fitneßlandschaft ab. Ist diese stark zerklüftet, so können Systeme in einem lokalen Optimum eingeschlossen bleiben; ist sie hingegen weitgehend flach, so findet die Selektion nicht genügend Ansatzpunkte und es kann eine Fehlerkatastrophe

eintreten (Kauffman 1993: 209 ff.).

Der Prozeß der Evolution eines Systems ist also offenbar gleichbedeutend mit der Erkundung seiner Fitneßlandschaft. Weil die Topologie dieser Landschaft jedoch nicht stabil ist, sondern wesentlich von der Entwicklung anderer Entitäten in der Umgebung des Systems abhängt, ist Evolution immer auch Koevolution im Rahmen eines umfassenderen Ökosystems. Betrachtet man dieses – wie etwa Holland (1995) – als komplexes System höherer Ordnung bzw. als Kollektiv dynamisch interagierender, adaptiver Komponenten, so wird deutlich, daß dessen Fitneßoptimum sich nicht automatisch aus der Summe der Optima seiner Komponenten ergibt. Dem Gesamtoptimum des Systems auf der Makroebene entsprechen hier oftmals nur Suboptima der auf der Mikroebene koevoluierenden Komponenten. Zugleich korrespondiert eine konkrete Systemordnung aufgrund einer sich dynamisch verändernden Umgebung zumeist nur temporär mit einem globalen Fitneßoptimum.

Um sich innerhalb seiner Fitneßlandschaft bewegen zu können, muß ein System inkrementelle Änderungen seiner Parameter vornehmen. Besondere Bedeutung kommt in diesem Zusammenhang dem Prozeß der Reproduktion zu, bietet doch jede weitgehend baugleiche Kopie eines Systems die Chance, durch eine minimale Variation einzelner Parameter benachbarte Regionen in der Fitneßlandschaft zu besiedeln. Zudem ermöglicht die Reproduktion eine phylogenetische Evolution über mehrere Generationen hinweg, so daß ein einmal erreichtes Anpassungsniveau über die Lebensdauer eines einzelnen Systems hinaus bewahrt werden kann. Auf lange Sicht sorgt dann die natürliche Selektion für eine Verschiebung der gesamten Population einer spezifischen Systemklasse hin zu höherer Fitneß. Prinzipiell ist dabei zunächst unerheblich, ob die Reproduktion eines Systems autopoietisch oder extern erfolgt. Über die Fähigkeit zur Selbstreproduktion verfügen jedoch im allgemeinen nur biologische Systeme.

Kauffman (1993: 232 ff.) formuliert die Hypothese, daß der Evolutionsprozeß komplex-adaptive Systeme – unabhängig davon ob ihr Ausgangszustand in einem chaotischen oder einem geordneten Regime liegt – generell an den Phasenübergang von Chaos und stabiler Ordnung dränge, da nur hier ein optimales Verhältnis von Flexibilität und Stabilität – Variation und Retention – gegeben sei. Zugleich werde an diesem Punkt die maximal mögliche Komplexität in der Dynamik des Systems erreicht. Die Emergenz neuer ontischer Systemschichten wäre damit nur zum Teil das – mehr oder weniger zufällige – Ergebnis eines langfristigen Selektionsprozesses. Vielmehr setzt nach Kauffman ab einer bestimmten Diversität potentieller Systemkomponenten mit hoher

Wahrscheinlichkeit ein Automatismus ein, der zur Selbstorganisation komplexerer, autokatalytischer Systeme führt.

2.1.3 Kybernetische Systeme

Es liegt vor diesem Hintergrund nahe, daß die auf dem Prinzip der zufälligen Mutation beruhende Strategie von Versuch und Irrtum bei der Erkundung von Fitneßlandschaften auf höheren Entitätsebenen um die Fähigkeit einer zielgerichteten und damit gesteuerten Anpassung komplexer Systeme ergänzt wird. Diese jedoch setzt voraus, daß ein System prinzipiell in der Lage ist, seine eigene Fitneßlandschaft zu reflektieren, d. h. seine Umgebung kognitiv zu rezipieren. Die hierzu notwendigen Mechanismen sind Gegenstand der Informations- und Kommunikationstheorie (Shannon 1948; Shannon u. Weaver 1949) sowie der Kybernetik (Wiener 1962; Ashby 1974).

Wie bereits gezeigt, handelt es sich bei komplexen Systemen um funktionale Entitäten. Da ihre Ordnung spezifische Trajektorien präjudiziert, implementieren sie faktisch zugleich einen konkreten Transformationsmechanismus. Über Komponenten mit eingehenden Verknüpfungen (Sensoren) werden aus der Umgebung Zustandsänderungen (Eingangswerte) in das System induziert, die dann entlang einer vorgezeichneten Trajektorie kaskadieren und schließlich zu bestimmten Endzuständen (Ausgangswerten) führen, die über Komponenten mit ausgehenden Verknüpfungen (Effektoren) in die Umgebung des Systems zurückwirken können. Ein solcher Mechanismus, den wir etwa bei Holland (1995) als „internes Modell“ und bei Gell-Mann (1995a,b) als „Schema“ wiederfinden, beinhaltet bereits Wissen bzw. Information über die Umgebung eines Systems, weil eine interne Zuordnung von eingangsseitigen zu ausgangsseitigen Zuständen immer auch die Annahme einer externen Ordnung impliziert. Erst durch die Existenz einer extern vorgegebenen Ordnung – von Regelmäßigkeiten in der Umgebung eines Systems respektive im übergeordneten Supersystem – können Systeme durch interne Ordnung adaptive Fitneßvorteile erzielen. Insofern die Evolution dabei eine funktionale Anpassung der inneren an die äußere Ordnung bewirkt, kann diese daher auch als repräsentatives Modell für jene betrachtet werden.

Ganz allgemein wird unter „In-Formation“[18] zunächst der konkrete Zustand eines Systems verstanden, sofern dieser prinzipiell kontingent ist. Nur wenn diese Bedingung zutrifft, der Zustand eines Systems also potentiell variabel ist, kann dieses wörtlich

18 Zu einer ausführlichen Behandlung des Begriffs der Information vgl. Abschnitt 3.1.

„in-formiert“ werden. Der quantitative Informationsgehalt des Systems steht dabei in direktem Zusammenhang mit der Varianz seiner möglichen Zustände. Er verhält sich reziprok zum Ordnungsgrad des Systems, weshalb er sich nach Shannon (1948) zugleich über ein Entropiemaß quantifizieren läßt. Folglich beinhaltet ein System absoluter Ordnung – also mit nur einem möglichen Zustand – keine Information.

Information kann zwischen zwei Systemen A und B transferiert werden, wenn beide derart gekoppelt sind, daß Effektoren des ersten unmittelbar Sensoren des zweiten beeinflussen: $A \rightarrow B$. Notabene muß die von B durchlaufene Veränderung nicht notwendiger Weise von der selben Art wie jene von A sein. Vielmehr ist es vollkommen ausreichend, daß die Veränderung in A überhaupt eine bestimmte Änderung in B zur Folge hat. In einer Kopplungsarchitektur der Form $Q_1 \rightarrow K \rightarrow S$ fungiert dann K als Kommunikationskanal zwischen einer Informationsquelle Q_1 und einer Informationssenke S. Implementiert der interne Transformationsmechanismus von K eine umkehrbar-eindeutige Zuordnung von Ein- zu Ausgangswerten, so ist ein verlustfreier Informationsfluß möglich. In diesem Falle sind Ein- und Ausgangsvarianz von K gleich groß. Wirkt nun die ursprünglich von Q_1 stammende Information nach Durchsatz durch K so auf Parameter von S ein, daß dieses in nicht-deterministisches Chaos abgedrängt wird, so stellt diese Information für S eine existenzbedrohende Störung und damit ein Problem dar. Um seinen Fortbestand zu sichern, muß S vor dieser kritischen Information geschützt werden, indem der auf S einwirkende Ist-Zustand von K in einen für S unschädlichen Soll-Zustand transformiert wird.

Ein passiver Schutz für S ergibt sich immer dann, wenn K aufgrund seiner internen Struktur kritische Information ohnehin blockiert, also kein vollständiger Kommunikationskanal ist. Hierzu muß K einen genügend hohen Ordnungsgrad aufweisen, um eine Entropie- und damit Informationsreduktion herbeizuführen, die seine Ausgangsvarianz auf solche Werte beschränkt, die für die Ordnung von S unkritisch sind. Ist dies nicht der Fall, so muß S aktiv mit Hilfe eines zusätzlichen Reglers R geschützt werden (Abbildung 2.4 a). Aufgabe von R ist es dann, die Parameter von K so zu regulieren, daß die für S kritische Ausgangsvarianz von K auf eine bestimmte Bandbreite reduziert wird. Zur Beeinflussung der für S kritischen Zielgröße muß R fortwährend auf Veränderungen von Q_1 reagieren. R muß daher ein hohes Maß an Kontingenz aufweisen, d. h. seine Ausgangsvarianz muß für eine vollständige Regelung mindestens der von Q_1 entsprechen, da die Information von R jene von Q_1 in K kompensieren muß.

Entscheidend ist ferner, daß die Geschwindigkeit des Informationsflusses von Q_1

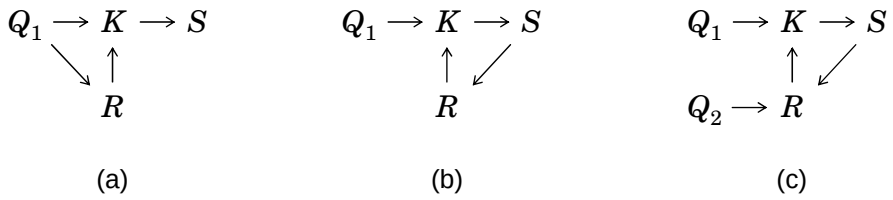


ABBILDUNG 2.4: *Regulierung in kybernetischen Systemen*

zu R schneller ist, als jene von Q_1 zu K, da nur so R die Parameter von K rechtzeitig beeinflussen kann. Oft ist dies nicht der Fall, so daß zur Stabilisierung auf eine unvollständige Regelung durch negative Rückkopplung ausgewichen werden muß (Abbildung 2.4 b). Eine solche Rückkopplung ist nur dann erfolgreich, wenn sich die von Q_1 induzierte Information nicht sprunghaft sondern kontinuierlich verändert. In diesem Falle wirken zunächst marginale Veränderungen auf die Parameter von S ein. Eine daraus resultierende Veränderung im Verhalten von S wird dann von R registriert und in gegenläufige Information an K umgesetzt, so daß ein übermäßiges Anwachsen störender Einflüsse auf S vermieden wird. Es entsteht ein homöostatisches Gleichgewicht, das sich nach von Q_1 verursachten Auslenkungen (Störungen) autonom wieder auf die von R vorgegebenen Parameterwerte für S einpendelt.

Existiert in einer solchen Architektur eine weitere Informationsquelle Q_2, die ihrerseits die Parameter von R determiniert und damit zugleich dessen Ordnung selektiert, so ist Q_2 in der Lage – unabhängig von der Störquelle Q_1 – indirekt auch die Ordnung von S zu dominieren, dieses also in seinem Verhalten zu steuern (Abbildung 2.4 c). Ordnung kann somit von Q_2 nach S diffundieren, weil Mechanismen der Regelung bzw. Steuerung eine effektive Einengung des nomologischen Zustandsraumes von S bewirken. Sind Q_2, R und S Subsysteme eines komplexen Systems A, K aber dessen Umgebung, so handelt es sich bei A um ein kybernetisches[19] System, das über die emergente Fähigkeit zur Selbststeuerung verfügt. Man beachte ferner, daß die Steuerungskapazität von A wesentlich von der Ausgangsvarianz seines Subsystems R abhängt, die wiederum für K eine Störung ist. Damit stellt sich die Komplexität von A für K als Kontingenz dar (vgl. hierzu auch Willke 2000: 29 f.). Die Ordnung in A wird also durch vermehrte

19 Norbert Wiener wählte den Begriff der „Kybernetik“ als Bezeichnung für eine allgemeine Wissenschaft der Regelung. Hierbei handelt es sich um einen vom altgriechischen Wort für „Steuermann“ – $\kappa\upsilon\beta\epsilon\rho\nu\eta\tau\eta\varsigma$ (*kybernetes*) – abgeleiteten Neologismus (vgl. hierzu Wiener 1966: 20).

Unordnung in seiner Umgebung erkauft.

Selbstverständlich können auch mehrere kybernetische Systeme zu einem kybernetischen System höherer Ordnung kombiniert sein, indem S seinerseits als Regler eines weiteren Systems fungiert. Wesentlicher Vorteil eines mehrstufigen Regelungsprozesses ist, daß Mechanismen der Problemlösung nicht von vornherein fest in der Systemstruktur verankert sein müssen, sondern ad hoc generiert werden können. Durch die Emergenz von Regelungseffekten kann dabei von Systemebene zu Systemebene jeweils eine detailliertere und somit zugleich komplexere Steuerungskapazität ausdifferenziert werden. Ferner können die Parameter einzelner Regler gegenüber mehr als einer Informationsquelle Sensibilität aufweisen, so daß nicht nur hierarchische, sondern auch dezentrale bzw. polyzentrische – auf Parallelprozessen basierende – Steuerungsnetzwerke denkbar sind, deren Knoten selbst wiederum aus kybernetischen Systemen bestehen. Je nachdem ob in einem solchen Netzwerk negative (ausgleichende) oder positive (selbstverstärkende) Rückkopplungsmechanismen überwiegen, kann es dann zu tendenziell systemstabilisierenden oder -zerstörenden Effekten kommen.

In Anlehnung an Gell-Mann (1995b: 14 f.) können zusammenfassend drei Arten der Adaption komplexer Systeme identifiziert werden, die sich jeweils unterschiedlichen Zeithorizonten zuordnen lassen: (1) Die sich aus seiner Ordnung unmittelbar ergebende kurzfristige Anpassung eines Systems durch direkte Transformation von Eingangs- zu Ausgangsgrößen. (2) Die mittelfristige Anpassung durch kybernetische Regelung seiner Parameter. Dies entspricht einer Anpassung der zugrundeliegenden Systemordnung und damit einer Transformation des Transformationsmechanismus, also einer Transformation zweiter Ordnung. (3) Die langfristige Anpassung der gesamten Population einer Systemklasse durch die evolutionären Kräfte von Mutation und Selektion, i. e. durch die Elimination nicht ausreichend angepaßter bzw. anpassungsfähiger Systeme.

Es liegt auf der Hand, daß auf den unteren Entitätsebenen, auf denen Systeme nur von geringer Komplexität und Diversität sind, hauptsächlich die dritte Art der Anpassung zum Tragen kommt. Auf den mittleren Ebenen hingegen gewinnt – parallel zur zunehmenden Komplexität der Systeme – die erste Art der Anpassung an Bedeutung, da komplexere Transformationsmechanismen hier zugleich die Bewältigung vielfältiger Stimuli ermöglichen. In den oberen Ebenen schließlich dominiert die zweite Art der Anpassung, also eine gezielte Problembewältigung durch komplexe Steuerungsmechanismen. Diese Steuerungsmechanismen beruhen, wie bereits erwähnt, auf Transformationen zweiter Ordnung. Sie passen die internen Schemata eines Systems im Wege einer

negativen Rückkopplung inkrementell an dessen Umgebung an. Genau diese Anpassung aber entspricht der kognitiven Fähigkeit des Lernens. Aufgrund der zentralen Rolle, die die Rückkopplungsschleife in diesem Zusammenhang einnimmt, ist Lernen dabei wesentlich ein iterativer Prozeß. Als solcher ist es immer auch selbstreferentiell, weil es notwendiger Weise auf den jeweils vorhergehenden Systemzustand Bezug nimmt. Dennoch ist dieser Prozeß nicht hermetisch abgeschlossen, da die zirkulierende Information über den Umweg der Systemumgebung in dieses zurückgekoppelt wird. In jedem Falle aber gewinnen Systeme durch Regelungsmechanismen eine höhere Unabhängigkeit gegenüber Veränderungen in ihrer Umgebung.

Die kritischen Entitäten in der Umgebung eines lernfähigen Systems aber sind zumeist ebenfalls komplex-adaptive Systeme. In einer solchen Ökologie koevoluierender komplex-adaptiver Systeme tritt das Problem der doppelten Kontingenz (vgl. Luhmann 1975: 171) auf, weil sich jedes System an das komplexe und damit kontingente Verhalten der anderen Systeme anpassen muß. Das hieraus resultierende Entscheidungsproblem ist Gegenstand der Spieltheorie. Axelrod (1984) zeigt, wie es vor dem Hintergrund wiederholter Interaktion durch eine Strategie wechselseitiger Nachahmung gleichwohl zu einem kollektiven Lernprozeß und in der Folge zu einer ordnungsbildenden Koordination im ökologischen Gesamtsystem kommen kann. Wesentliche Voraussetzung hierfür ist allerdings nach Holland (1995) die Fähigkeit komplex-adaptiver Systeme, sich anhand von individuellen und klassifikatorischen Merkmalen gegenseitig identifizieren und entsprechend aufeinander reagieren zu können. Systempopulationen, die diese Besonderheit aufweisen, werden daher von der Evolution begünstigt.

Innerhalb der Klasse aller biologischen Systeme kann eine Ausdifferenzierung kognitiver Subsysteme beobachtet werden, deren mentale Fähigkeit auf dem kybernetischen System eines dezentralen neuronalen Netzwerkes beruht (vgl. etwa Roth u. Schwegler 1995). Solche Systeme weisen ein Bewußtsein auf, welches sie in die Lage versetzt, andere Entitäten in ihrer Umgebung aufgrund ihrer Informationssignatur – also der von ihnen im kognitiven System selbst ausgelösten spezifischen Zustandsänderung – (wieder) zu erkennen. Der Prozeß des Erkennens besteht dabei wesentlich in einer Zuordnung der wahrgenommenen Information zu jener eines zuvor gelernten Prototyps (vgl. Mainzer 2004: 165 ff.). Solche Prototypen sind Attraktoren des kognitiven Systems. Sie verdichten alle in ihrem Einzugsbereich liegenden Informationen zu einem bestimmten Zustand und erlauben so, trotz perspektivisch bedingter Verzerrungen der Informationssignatur, eine zuverlässige Identifikation bzw. Klassifikation und mithin

differenzierte Reflektion wahrgenommener Entitäten in Form einer mentalen Repräsentanz. Das hochentwicklete kognitive System des menschlichen Gehirns ermöglicht gar die Herausbildung einer mentalen Repräsentanz seiner selbst, so daß eine rekursive Selbst-Reflektion und somit ein subjektives Selbst-Bewußtsein entstehen kann.

Als konstruiertes Ergebnis eines individuellen Lernprozesses differieren die mentalen Repräsentanzen für ein und dieselbe Entität jedoch höchst wahrscheinlich zwischen verschiedenen kognitiven Systemen, vor allem wenn diese von hoher Komplexität sind, was deren Subjektivität zusätzlich unterstreicht. Zugleich aber steuern diese Repräsentanzen indirekt die Interaktion von System und Umgebung und tragen so wesentlich zu dessen (Überlebens-)Erfolg bei. Weil ihre Funktionalität bzw. Dysfunktionalität in diesem Kontext reale Wirkungen entfaltet und daher eine objektiv meßbare Größe darstellt, lassen sich subjektive Repräsentanzen somit unter objektive Klassen funktionaler Äquivalenz subsumieren. Allein aufgrund dieser Äquivalenz zwischen bestimmten mentalen Repräsentanzen ist eine Kommunikation und Kooperation zwischen unterschiedlichen kognitiven Systemen überhaupt möglich. Einer solchen Äquivalenzklasse und der mit ihr konstruierten Begrifflichkeit schreibt Bunge (2001) daher eine Existenz als fiktionale bzw. konzeptuelle Entität zu. Deren Eigenschaften sind – im Gegensatz zu denen realer Objekte – nicht veränderbar und werden von Bunge im Unterschied zu diesen als Prädikate apostrophiert.

2.2 Governance in sozio-technischen Systemen

2.2.1 Elemente und Strukturen sozio-technischer Systeme

In den letzten Jahren nehmen Governance-Ansätze in der Literatur vieler Disziplinen, so auch der Wirtschafts- und Sozialwissenschaften, eine zentrale Rolle als „transdisziplinäres Brückenkonzept“ (Blatter 2006) ein. Eine große Stärke und zugleich Schwäche liegt dabei in der allgemeinen semantischen Unschärfe des Begriffs „Governance“. So kommt etwa Kooiman (2002: 72) allein im Bereich der Politikwissenschaft auf eine Klassifikation von wenigstens zwölf Konzepten. Einen umfassenden Überblick über Entwicklungsgeschichte und -stand der Governance-Forschung aus dem theoretischen Blickwinkel der Neuen Politischen Ökonomie vermittelt insbesondere Lütz (2003).

Sprachgeschichtlich ist der Begriff eng verwandt mit dem altgriechischen Wort für Steuermann ($\kappa\upsilon\beta\epsilon\rho\nu\eta\tau\eta\varsigma$ – *kybernetes*), auf das sich, wie oben bereits erwähnt, auch

der Begriff der „Kybernetik“ bezieht (vgl. Schneider 2004c). Diese kybernetische Begriffsdimension ist Grundlage der vorliegenden Arbeit. Governance wird somit als übergreifendes theoretisches Konzept zur Analyse kybernetischer Regelungs- und Steuerungsstrukturen auf der ontischen Ebene komplexer sozio-technischer Handlungssysteme verstanden. Steuerung bzw. Regelung wird als ordnungsbildender Mechanismus interpretiert, der in kollektiven Handlungssystemen wesentlich auf der emergenten Eigenschaft institutioneller Arrangements beruht (vgl. hierzu Mayntz 2004). Entsprechend übersetzen bspw. Schneider u. Kenis (1996) *Governance* als „institutionelle Steuerung“ (vgl. auch Schneider 2004b).

Soll die einseitig holistische Perspektive struktur-funktionalistischer Systemtheorien (Parsons 1951, 1971; Easton 1965) vermieden werden, so bedarf eine Analyse sozialer Handlungssysteme jedoch neben einer Betrachtung des institutionellen Gefüges immer auch einer Berücksichtigung ihrer wesentlichen Akteure und Ressourcen. Nur unter Einbezug dieser Systemkomponenten lassen sich gesellschaftliche Steuerungsprozesse, und damit auch gesellschaftliche Ordnungsbildung, mikrofundieren[20] und mithin umfassend analysieren. Dieser Sichtweise wird wohl am ehesten das analytische Raster des „akteurzentrierten Institutionalismus“ (Mayntz u. Scharpf 1995a; Schneider u. Mayntz 1995; Scharpf 2000) mit seiner konzeptionellen Synthese von Ansätzen des Neo-Institutionalismus und der Rational-Choice-Theorie gerecht. Es dient daher als zentraler Referenzpunkt des im Folgenden dargelegten Analyserahmens.

Der Organismus des Menschen ist, wie alle biologischen Systeme, ein dissipatives System, welches die (labile) Ordnung seines homöostatischen Fließgleichgewichts nur im Rahmen eines Metabolismus dauerhaft aufrechterhalten kann. So reguliert etwa das vegetative Nervensystem die permanente Kompensation interner Zerfallsprozesse des Organismus sowie extern einwirkender Störfaktoren. Die hierzu notwendige Veränderung setzt allerdings eine kontinuierliche Zufuhr von Energie und Materie voraus, so daß jeder Organismus in regelmäßigen Abständen Entitäten aus seiner Umgebung aufnehmen muß. Bedingt durch die negative Rückkopplungsstrukur zentraler biologischer Regulierungsprozesse tritt ein Mangel an – bzw. ein *Bedürfnis* nach – solchen Entitäten zumeist periodisch auf. Selbstverständlich erstreckt sich das komplexe System des menschlichen Organismus jedoch auch auf höhere ontische Ebenen, so daß sich über

20 Zur Mikrofundierung sozialer Steuerungsprozesse vgl. das Schema der *Boudon-Coleman-Erklärung* bei Schneider u. Janning (2006: 38 f.).

die rein physischen Bedürfnisse hinaus zusätzlich ein individuelles Ensemble psychischer und sozialer Bedürfnisse ergibt. Diese komplexe Bedürfnisstruktur motiviert das Individuum hinsichtlich einer Bedürfnisbefriedigung tätig zu werden.

Da die meisten Bedürfnisse nicht abschließend befriedigt werden können, sondern periodisch wiederkehren, stellen sie den Menschen vor eine dauerhafte Herausforderung, die eine aktive Teilhabe am Geschehen in seiner Umgebung begründet. Hieraus leitet sich ein natürliches *Interesse*[21] an langfristig günstigen Umweltbedingungen ab, welche eine regelmäßige und möglichst umfassende Bedürfnisbefriedigung erlauben. Der Begriff des „Interesses" kann dabei auf eine etymologisch durchaus wechselvolle Geschichte zurückblicken (vgl. Hirschman 1986, 2002). Im ausgehenden Mittelalter wurde er, wie heute noch im englischsprachigen Raum, zunächst auch und vor allem ganz allgemein im Sinne eines finanziellen An- oder Vorteils bzw. eines Zinses verwandt, was ihm eine zunehmend negative Konnotation eintrug. Während der Aufklärung galt ein rational reflektiertes Eigeninteresse hingegen als Garant der Zügelung animalischer Triebe und damit auch als (gesamt-)gesellschaftlich erstrebenswert. Man hoffte gar, daß als irrational erlebte, tradierte Moralvorstellungen durch einen rationalen Interessenbegriff weitgehend obsolet würden.

Voraussetzung einer mittelbaren oder unmittelbaren Befriedigung spezifischer Bedürfnisse im engeren bzw. einer Interessenwahrung im weiteren Sinne sind jeweils bestimmte Objekte und/oder Zustände. Diese weisen als *Güter* einen subjektbezogenen Nutzenwert auf, der jedoch aufgrund individuell differierender Präferenzen objektiv (interpersonal) nur schwer vergleichbar ist. Der multidimensionale Raum der spezifischen Nutzungseigenschaften solcher Güter spannt ein klassifikatorisches Spektrum möglicher Güterarten auf (vgl. Coleman 1990; Esser 1999b). Die wichtigsten Kriterien sind hierbei üblicherweise *Exklusivität* (Musgrave 1959) und *Rivalität* (Samuelson 1954) eines Gutes (vgl. hierzu auch Ostrom 2002). Individualgüter zeichnen sich durch eine Exklusivität im Konsum aus, d. h. sie lassen bezüglich ihrer Nutznießung einen Ausschluß Dritter ohne wesentlichen Aufwand zu. Im Gegensatz hierzu ist ein solcher Ausschluß bei Kollektivgütern nicht oder nur unter erheblichem zusätzlichen Aufwand möglich. Rivalisierende Güter haben die Eigenschaft, daß ihr individueller Nutzwert mit jedem weiteren Konsumenten abnimmt. Bei nicht-rivalisierenden Gütern bleibt dieser hingegen auch mit steigender Konsumentenzahl gleich.

21 Der lateinische Ausdruck *inter esse* bedeutet wörtlich „dazwischen sein", „teilhaben".

Ist ein Gut sowohl rivalisierend als auch exklusiv, wird es als reines *Privatgut*, ist es weder rivalisierend noch exklusiv, als reines *öffentliches Gut* bezeichnet.[22] Im Falle rivalisierender Kollektivgüter handelt es sich ferner um sog. *Allmende-Güter* (vgl. Hardin 1968), im Falle nicht-rivalisierender Individualgüter um sog. *Club-Güter* (vgl. Buchanan 1965). Oftmals sind Güter jedoch weit komplexere Mischformen, bei denen es von analytischer Bedeutung sein kann, ob sie durch eine Nutzung lediglich ge- oder auch verbraucht werden, ob sie während der Nutzung nur einem oder mehreren Konsumenten zur Verfügung stehen können, und ob sie übertragbar oder individuell gebunden sind. Auch die Frage einer freien Verfügbarkeit oder aber Knappheit kann ein wichtiges Kriterium sein.

Stehen die zur Befriedigung gegebener Bedürfnisse benötigten spezifischen Güter nicht unmittelbar zur freien Verfügung, so stellt sich das Problem ihrer Erzeugung. Weil dies der Regelfall ist, bedeutet Leben fortgesetztes Problemlösen (Popper 1994). Daher müssen Menschen produktiv handeln indem sie intentional auf ihre Umgebung einwirken. Ein solches Handeln zielt dann auf einen Nutzengewinn, der sich sich aus der Befriedigung individueller Bedürfnisse durch den Konsum spezifischer Güter ergibt. Der Nutzen selbst kann zugleich auf einer höheren Abstraktionsebene als superiores Konsumgut begriffen werden, in dessen Produktion letztlich alle anderen Güter als Zwischenprodukte bzw. *Ressourcen* einfließen. Nutzen stellt sich so als Funktion des Konsums und dieser umgekehrt als Produktion von Nutzen dar (Esser 1999a,c).

In der klassischen Wirtschaftstheorie ist jedes Produkt das Ergebnis einer spezifischen Kombination der Produktionsfaktoren Boden, Arbeit und Kapital. Unter dem Faktor Boden werden sämtliche natürlichen Ressourcen, unter Arbeit alle menschlichen Tätigkeiten mit dem Ziel einer Wertschöpfung subsumiert. Der derivative Faktor Kapital hingegen leitet sich aus einer Akkumulation der beiden anderen, originären Faktoren ab. Er stellt das Ergebnis eines vorangegangenen Produktionsprozesses dar und umfaßt als solches vor allem Werkzeuge und Produktionsanlagen sowie – in neuerer Definition – ebenfalls Wissen und individuelle Fähigkeiten (Humankapital). Die Betriebswirtschaftslehre unterscheidet daneben noch einen dispositiven Faktor, der sich auf die im Produktionsprozeß anfallenden Steuerungs- und Koordinationsleistungen bezieht. Allerdings handelt es sich hierbei im volkswirtschaftlichen Sinne eher um eine

22 Zu einer weitergehenden, historisch fundierten Differenzierung öffentlicher und privater Güter vgl. Geuss (2003).

weitergehende Ausdifferenzierung des Faktors Arbeit. Die Ressourcen aller drei Faktorarten stehen, abgesehen von wenigen Ausnahmen im Bereich natürlicher Ressourcen, in nur begrenztem Umfang zur Verfügung, weshalb ihr Ge- und Verbrauch im Produktionsprozeß Opportunitätskosten verursacht, da er den Verzicht auf die Realisierung alternativer Produktionsoptionen impliziert. Solche Kosten repräsentieren dann einen negativen, weil entgangenen Nutzen.

Die Rational-Choice-Theorie unterstellt hier, daß Akteure ferner bestrebt sind rational zu wirtschaften, d. h. neben einer effektiven (erfolgreichen) Nutzenproduktion zugleich immer auch an einem effizienten (optimalen) Kosten-Nutzen-Verhältnis ihres Handelns interessiert sind, um so ihre individuelle Nutzenfunktion zu maximieren. Unter alternativen Produktionsoptionen wählen sie daher diejenige, welche ihnen einen optimalen Nutzen verspricht und entsprechen insofern dem Paradigma des *homo oeconomicus*. Dennoch gelingt es rationalen Akteuren in der Praxis gleichwohl nur in den seltensten Fällen, sich unter alternativen Handlungsoptionen für die objektiv rationalste Lösung zu entscheiden. Ursächlich hierfür ist, daß jede im Produktionsprozeß anfallende Dispositionsentscheidung Informationsressourcen[23] voraussetzt. Diese Informationen aber sind aufgrund kognitiver Begrenzungen (vgl. March u. Simon 1958; Conlisk 1996) knapp und verursachen daher ebenfalls Kosten. Entscheidungen fallen so zumeist unter Unsicherheit und führen damit i. d. R. zwar zu suboptimalen, aber im Einzelfall dennoch zufriedenstellenden bzw. hinreichenden Lösungen.

Das lateinische Verb *agere*, von dem sich der Begriff des „Akteurs“ ableitet, deutet mit seinen beiden Konnotationen „handeln“ und „verhandeln“ bereits an, daß Handeln kaum ohne soziale Komponente (vgl. Granovetter 1985) und damit Verhandeln denkbar ist. Schon Aristoteles[24] und später Cicero[25] charakterisierten den Menschen als ein seiner Natur nach soziales Wesen, als $\zeta\omega o\nu\ \pi o\lambda\iota\tau\iota\kappa o\nu$ (*zòon politikon*) bzw. *ens sociale*, und Dahrendorf (1974) prägte als Pendant zum Begriff des bereits erwähnten *homo oeconomicus* jenen des *homo sociologicus*. Eine solche Sozialität – „also die Faktizität sozialer Strukturen und anderer Akteure“ (Schimank 1992: 182) – aber bleibt nicht ohne Bedeutung für das Handeln eines begrenzt-rationalen Akteurs, denn in sozialen, aus einer Vielzahl von Akteuren bestehenden Handlungssystemen verteilt sich die Kontrolle

23 Zu einer ausführlichen Definition des Begriffs der Information vgl. Abschnitt 3.1.

24 Aristoteles: *Politik*, I 2 1252b; III 6 1278b

25 Cicero: *De re publica*, I 25, 39

über verschiedene Ressourcen zwangsläufig mit hoher Wahrscheinlichkeit auf mehr als einen Akteur.

Dieser Umstand macht einen Austausch von Ressourcen oder Verfügungsrechten notwendig, um die Erstellung bestimmter Güter überhaupt erst zu ermöglichen. Neben die Produktion als Aktion tritt daher der Austausch, die Transaktion (vgl. Coleman 1990). Beide Aspekte spiegeln sich auch in den Bedeutungen des Wortes „Handeln“ als „tätig werden“ einerseits und als „Kauf“ und „Verkauf“ von Gütern andererseits wider.[26] Ein solcher Austausch bedingt soziale Beziehungen in Form mehr oder weniger dauerhafter Trans- und Interaktionskontakte zwischen den Akteuren und setzt wechselseitige Erwartungssicherheit bezüglich der Verhaltensweisen des Interaktionspartners und damit ein Mindestmaß an sozialer Ordnung voraus. Gäbe es diese Erwartungssicherheit nicht, so wäre das Zustandekommen einer sinnhaft aufeinander bezogenen Interaktion nahezu unmöglich (vgl. Luhmann 1993b).

Dem Menschen als primär vernunftbegabtem Wesen allerdings fehlen weitgehend jene animalischen Instinkte, die sein Verhalten in engen, genetisch programmierten Schemata halten und damit sozial berechenbar machen. Der an und für sich immense Vorteil der Fähigkeit reflektierten Handelns zwingt ihn daher zugleich, sich in seiner Handlungsfreiheit sozialen Konventionen zu unterwerfen, sozial geteilte Handlungs- und Interpretationsmuster zu adaptieren. Medium der Herstellung von Erwartungssicherheit im sozialen Interaktionsfeld ist eine Institutionalisierung von Handlungen im Sinne einer generalisierenden und typisierenden Habitualisierung, wodurch die Reaktionsmuster potentieller Interaktionspartner situativ weitgehend antizipationsfähig werden. Aus anthropologischer Sicht bilden derart geronnene Handlungsmuster das rationale Komplement instinktiver Verhaltensweisen (Gehlen 1975). Sie strukturieren als formelle und informelle Regelsysteme die Handlungsmöglichkeiten der Akteure eines sozialen Handlungssystems, indem sie bestimmte Handlungsweisen gratifizieren oder sanktionieren und deren Eintrittswahrscheinlichkeit damit erhöhen oder verringern (North 1991; Scharpf 2000). Die Folge ist eine Kontingenzreduktion, welche die soziale Umwelt weitgehend berechenbar macht und so zur kognitiven Entlastung der Akteure beiträgt (March u. Simon 1958). Aus ökonomischer Perspektive senken sie damit wesentlich die (Informations-)Kosten einer Transaktion (Coase 1960).

26 Die Betriebswirtschaftslehre spricht in diesem Zusammenhang auch vom Entscheidungsproblem des „Make-or-Buy“ bzw. der Alternative von Eigenfertigung und Fremdbezug.

Zugleich sind Institutionen in der Lage soziale Handlungssysteme auszudifferenzieren, indem sie eine funktional spezialisierte Rollenverteilung vornehmen und über einen damit verbundenen kollektiven Erwartungshorizont das Verhalten einzelner Akteure, wenn nicht abschließend determinieren, so doch zumindest einschränkend kanalisieren und somit steuern. Über die soziale Definition spezifischer Identitäten wird eine interpersonale Schnittstelle eröffnet, die interaktives Handeln prinzipiell erst ermöglicht (Mead 1998). Parallel dazu entsteht eine kollektive Identität, ein gemeinschaftlich geschaffener und geteilter Sinnzusammenhang, welcher mittels einer inter-subjektiv konstruierten Wirklichkeitssemantik eine kommunikative Koordination der Akteure und damit ihre Integration in komplexe Handlungszusammenhänge erlaubt, wodurch eine umfassende Innendifferenzierung sozialer Handlungssysteme in immer filigranere funktionelle Subsysteme möglich wird (Mayntz et al. 1988; Mayntz 1997a).

Nach Berger u. Luckmann (2003) lassen sich Institutionen als Ergebnis eines sozialen Konstruktionsprozesses begreifen. Sie können sowohl aus dynamischen Prozessen spontaner bzw. „transintentionaler“ (Schimank 2003) Selbstordnung als auch aus einer bewußten Organisationsanstrengung, der eine intentionale Gestaltungsabsicht zu Grunde liegt, resultieren. Sie bilden dabei immer auch selbst Ausgangspunkt und Grundlage solcher Prozesse. Beide Arten der Ordnungsbildung gehen oftmals Hand in Hand und sind nicht immer klar voneinander zu trennen (Czada u. Schimank 2000).

Eine spontane Institutionenbildung läßt sich auf koevolutionäre Handlungsprozesse zurückführen, in deren Verlauf sich durch interaktive Erfahrung erlernte Verhaltens- und Interpretationsmuster der Akteure über positive Rückkopplungseffekte inter-subjektiv verfestigen und schließlich in ein institutionelles Fließgleichgewicht münden.[27] Dieses bildet dann ein aus Makroperspektive unintendiertes Aggregat einer Vielzahl individueller Handlungen auf der Mikroebene. Die Entstehung von Sprache als grundlegender Institution der Kommunikation zur Überwindung des existenziellen Problems der doppelten Kontingenz ist beispielhaft für einen solchen Prozeß evolutionärer Selbstordnung. Weil Akteure jedoch nicht ausschließlich, wie etwa von Luhmann durch die Annahme autopoietischer Systeme unterstellt, institutionell fremdgesteuert, sondern zugleich auch an einer aktiven Maximierung ihres individuell definierten Nutzens interessiert sind, bleiben Institutionen als Handlungsrestriktionen selbstverständlich immer

27 Vgl. hierzu Axelrod (1984), der für den Spezialfall eines iterativen Gefangenendilemmas die Entstehung kooperativer Strukturen durch eine Strategie des „Tit-for-Tat“ erklärt.

auch Gegenstand bewußter Reflexion sowie eines sich daraus ableitenden intentionalen Gestaltungswillens (Schneider u. Kenis 1996).

Die Existenz einer institutionellen Ordnung liegt aufgrund der durch sie erzielten Kontingenzreduktion, sowie einer damit verbundenen Senkung der Transaktionskosten, letztlich im kollektiven Interesse aller Akteure. Institutionen wirken auf diese Weise nicht ausschließlich restriktiv, sondern eröffnen auch neue Handlungsspielräume und gewinnen damit Gutscharakter. Schimank (1992) klassifiziert daher soziale Strukturen im weiteren Sinne als öffentliche Güter und diskutiert aus einer solchen Perspektive die Bedingungen ihrer Aufrechterhaltung und Neugestaltung im Rahmen spieltheoretisch modellierter Konstellationen. Er zeigt, daß einzelne, rational handelnde Akteure unter bestimmten Bedingungen bestrebt sein können, sich strukturellen Regeln, bei gleichzeitiger Fortgeltung derselben für alle anderen, selbst zu entziehen, wodurch eine natürliche Tendenz zur Erosion dieser Regeln entsteht. Die Akteure sehen sich mit dem Problem des Gefangenendilemmas konfrontiert.

Umgekehrt befinden sich die Akteure hinsichtlich der Gestaltung neuer Sozialstrukturen in einem, durch divergierende Interessen gekennzeichneten Koordinationsspiel (Geschlechterkampf), da jeder Akteur versucht ist, ihn besonders begünstigende Strukturen zu etablieren, wobei jedoch alle das grundlegende Interesse am Zustandekommen einer allgemeinverbindlichen Ordnung teilen. Allerdings ist die diesen Überlegungen zugrunde liegende Interpretation sozialer Strukturen als öffentliches Gut wohl nur auf Fälle bewußt intendierter institutioneller Ordnungsbildung anwendbar. Transintentionale Institutionen, wie die als Beispiel bereits bemühte Sprache, gehören hingegen eher zur Kategorie der Kommunalgüter[28], was sowohl ihr Zustandekommen als auch ihre Aufrechterhaltung im Kontext eines Koordinationsspiels mit konvergierenden Interessen verortet und deshalb aus spieltheoretischer Perspektive prinzipiell unproblematischer erscheinen läßt.

Eine spezifische Form der Institutionalisierung von Handlungsabläufen stellt die Technik dar. Der Begriff der „Technik“, oder allgemeiner der „Technologie“,[29] geht auf das altgriechische $\tau\varepsilon\chi\nu\eta$ (*techne*) zurück, was „Kunstfertigkeit“ oder „handwerkliche Fähigkeit“ bedeutet (Rammert 1999, 2000). Seine moderne Konnotation erschließt sich anhand mehrerer Dimensionen (vgl. Hyner 2000). Aus anthropologischer Sichtweise ist

28 Zu den spezifischen Eigenschaften von Kommunalgütern vgl. Esser (1999b).

29 Zu einer expliziten Differenzierung der Begriffe vgl. Wersig (2000).

Technik zunächst ein Organersatz (Gehlen 1966), durch welchen der Mensch im Unterschied zum Tier die vorgefundene natürliche Umgebung tiefgreifend verändern und zu einer, seinen Bedürfnissen angepaßten „Übernatur“ (Ortega y Gasset 1978: 15) formen kann. Oft werden unter Technik im engeren Sinne daher jene materiellen Artefakte[30] verstanden, die im Hinblick auf die Erreichung eines bestimmten Zieles instrumentellen Charakter haben.

Die Soziologie kennt allerdings eine weitere, umfassendere Definition, in welcher Technik geronnenes Wissen über bereits erprobte Handlungsstrategien verkörpert, welche für Klassen ähnlicher Probleme erfolgreiche Lösungen implementieren und daher bei wiederkehrenden Problemstellungen eine kognitive Entlastung der Akteure ermöglichen. So schreibt Max Weber (1980: 32):

> „Technik“ eines Handelns bedeutet uns den Inbegriff der verwendeten *Mittel* desselben im *Gegensatz* zu jenem Sinn oder Zweck, an dem es letztlich (in concreto) orientiert ist, „rationale“ Technik eine Verwendung von Mitteln, welche bewußt und planvoll orientiert ist an Erfahrungen und Nachdenken, im Höchstfall der Rationalität: an wissenschaftlichem Denken.

Technik dient aus einer solchen Perspektive dem Zwecke einer Handlungsoptimierung bzw. Effizienzsteigerung und bildet damit eine wichtige Grundlage komplexer Wirtschaften und eine notwendige Voraussetzung gesellschaftlicher Entwicklung (Joerges 1988; Esser 1999a).

Bei Ortega y Gasset (1978) findet sich das Modell einer, historisch veranschaulichten, dreistufigen Technikgenese: In den *primitiven Gesellschaften* der Vor- und Frühzeit wurden noch mehr oder weniger natürliche Hilfsmittel, wie Steine und Keulen, verwandt. Die einzelnen Akteure versorgten sich weitgehend selbst. Spezialisierung und Arbeitsteilung gab es meist nur im Familienverband, Handel und Warentausch finden sich, wenn überhaupt, so nur lokal. In den fortgeschrittenen *Handwerksgesellschaften* der Antike und des Mittelalters hingegen existierten bereits hoch spezialisierte Handwerker, die sich komplizierter Werkzeuge und Methoden bedienten. Technisches Wissen wird von Generation zu Generation weitergeben und verfeinert. Ausgedehnte Handelswege erstreckten sich von Zentraleuropa bis Asien. Der „Übergang des bloßen Werkzeugs zur Maschine, das heißt, zum selbsttätigen Apparat“ (Ortega y Gasset 1978: 62)

30 Der Begriff „Artefakt“ setzt sich aus lateinisch *ars* (Kunst) und *factum* (geschaffen) zusammen und verweist daher auf etwas Künstliches in Abgrenzung zum Natürlichen.

schließlich bereitete den Weg zur *industriellen Gesellschaft*, in der sich Technik „in automatisierten Prozessen, zumindest teilweise, von ihren menschlichen Trägern lösen“ (Hyner 2000: 15) kann.

Vorbedingung einer solchen Automatisierung ist fast immer eine hohe Ausdifferenzierung einzelner Prozeßschritte, deren menschliche Träger dann sukzessive durch geeignete Maschinen substituiert werden (Schmidt u. Werle 1992). In der Folge entstehen Prozeßketten, die sich aus einer Vielzahl von Akteuren, technischen Artefakten und institutionellen Steuerungsarrangements zusammensetzen, welche funktional aufeinander bezogen und architektonisch zu einem übergreifenden Gesamtsystem integriert sind. Soweit Technik dabei aus soziologischer Perspektive nicht einfach als Umwelt eines eingebetteten sozialen Systems, sondern vielmehr als integraler Bestandteil desselben aufgefaßt wird, kann mit einiger Berechtigung von sozio-technischen Systemen gesprochen werden (Mayntz 1988b). Oft sind solche Systeme von bedeutendem Umfang und zugleich hoher Kritizität für eine Gesellschaft, weil sie infrastrukturelle Aufgaben wahrnehmen. In der sozialwissenschaftlichen Literatur wurden diese Systeme vor allem in den 1990er Jahren als „großtechnische Systeme“ (Large Technical Systems) thematisiert, so etwa bei Hughes (1987), Mayntz u. Hughes (1988), Mayntz (1993), Schneider (1991, 1993), Joerges u. Braun (1994), Joerges (1996) und Coutard (1999).

2.2.2 Basale Modi institutioneller Steuerung

Sozio-technische Systeme werfen, wie jedes Interaktionssystem, Koordinationsprobleme auf, da eine effektive und effiziente Kooperation der in ihren Handlungen und Entscheidungen interdependenten Akteure nicht a priori vorausgesetzt werden kann. Scharpf (2000: 204 ff.) unterscheidet hier in Anlehnung an Lax u. Sebenius (1986) zwischen den beiden Dimensionen der Produktion einerseits sowie der Verteilung andererseits. Während es hinsichtlich der Produktionsdimension um eine Maximierung der allgemeinen Wohlfahrt durch eine möglichst optimale Allokation der verfügbaren Ressourcen und damit letztlich eine Minimierung der (Opportunitäts-)Kosten geht, verweist die Verteilungsproblematik auf die normative Frage nach der Distribution eines solchermaßen erwirtschafteten Gesamtnutzens.

Die traditionelle Wohlfahrtstheorie bemißt die allokative Effizienz einer Ökonomie zunächst aus dem Blickwinkel der Produktionsdimension utilitaristisch und eindimensional in Relation zum aggregierten Gesamtnutzen aller Akteure. Aufgrund konzep-

tioneller Schwierigkeiten hinsichtlich der Quantifizierbarkeit sowie interpersonalen Vergleichbarkeit von Nutzen erscheint eine solche Definition heute allerdings fragwürdig (Scharpf 2000: 159 f.; Breyer u. Kolmar 2001: 49 ff.; Mayntz 2002a). Die neuere Wohlfahrtsökonomie tendiert daher zu einer Bewertung nach dem sog. Pareto-Kriterium, d. h. sie betrachtet eine Ressourcenallokation genau dann als wohlfahrtsmaximierend, wenn keiner der beteiligten Akteure besser gestellt werden könnte, ohne zugleich einen anderen Akteur in seinem Nutzen zu schmälern und bezieht so auch die Verteilungsdimension ein (Weimann 2004: 73 ff.). Diese Definition gewährleistet eine vollständig nutzbringende Verwertung aller zu Verfügung stehenden Ressourcen und läuft auf eine Maximierung der allgemeinen Konsumfunktion in einem n-dimensionalen Nutzenraum hinaus, wobei n der Anzahl der beteiligten Akteure entspricht. Der Pareto-effiziente Raum selbst umfaßt dann $n - 1$ Dimensionen.

Sobald jedoch $n > 1$ ist, also in jedem sozialen Handlungssystem, erhält man statt eines eindeutigen Pareto-Optimums zumeist einen unter allokativen Effizienzgesichtspunkten indifferenten Pareto-optimalen Raum, in welchem verschiedene wohlfahrtsmaximierende Ressourcenallokationen möglich sind, wobei die Nutzenverteilung unter den Akteuren stark variieren kann und nach dem zweiten Hauptsatz der Wohlfahrtsökonomie letztlich nur von der Ausgangsverteilung der Ressourcen abhängig ist. Hier sind Konstellationen, in denen bestimmte allokative Optima ein Distributionsergebnis mit sich bringen, aus welchem einige Akteure überproportionalen Nutzen ziehen, nicht nur denkbar sondern auch wahrscheinlich. In solchen Konstellationen haben dann nicht alle Akteure per se ein gleich starkes Interesse an diesem Optimum, es sei denn, das Verteilungsergebnis kann, wie etwa vom Coase-Theorem gefordert, nachträglich durch Kompensationszahlungen revidiert werden.

Aufgrund der skizzierten Problematik benötigt jedes Interaktionssystem hinsichtlich einer Maximierung der allgemeinen Wohlfahrt einen institutionellen Rahmen, der es in die Lage versetzt, über einen geeigneten Regelungsmechanismus einen problematischen Ist-Zustand in einen angestrebten Soll-Zustand zu transformieren, der also eine Koordination der Akteure gewährleistet und so eine optimale Ressourcenallokation herbeiführt. Wesentliche Voraussetzungen für das Erreichen einer Pareto-optimalen Allokation ergeben sich dabei aus der Transaktionskostentheorie. Ihr liegt die Annahme zugrunde, daß der Austausch jeglicher Ressourcen Reibungsverluste in Form von Transaktionskosten verursacht, welche sich wiederum auf die Kosten fehlender Information hinsichtlich der Randbedingungen des Handelns reduzieren lassen (Dahlman 1979: 148).

Je höher die Informationskosten einer Transaktion sind, desto unwahrscheinlicher ist ihr Zustandekommen, da ein Tauschgeschäft nur dann rentabel erscheint, wenn die anfallenden Kosten den erzielten Nutzen nicht übersteigen.

Gäbe es keinerlei Transaktionskosten, also im Falle einer idealen Walrasianischen Informationstransparenz, stellte sich unter den Voraussetzungen des ersten Hauptsatzes der Wohlfahrtsökonomie sowie der Möglichkeit von Ausgleichszahlungen ein autonomes Pareto-effizientes Gleichgewicht ein, da jeder weitere Ressourcentausch, der eine Pareto-superiore Allokation nach sich zöge, immer zugleich auch im bilateralen Interesse der potentiellen Transaktionspartner läge. Bleibt der Ressourcenfluß jedoch durch den Reibungsverlust der Transaktionskosten vor Erreichen jenes äquilibren Optimums stecken, so ergibt sich eine ineffiziente Ressourcenallokation. Das Erreichen einer Pareto-effizienten Allokation ist demnach vor allem eine Frage der Minimierung anfallender Transaktionskosten.

Folglich wird in der Neuen Politischen Ökonomie das Konstrukt des Marktes als Komplex jener Institutionen begriffen, „that exist to facilitate exchange, that is, they exist in order to reduce the cost of carrying out exchange transactions“ (Coase 1988: 7). Der Markt stellt aus einer solchen Perspektive die einfachste Form eines dezentralen institutionellen Regelungsmechanismus dar (Lindblom 2001). Akteure gehen hier nur punktuell und temporär Austauschbeziehungen ein, unterhalten darüber hinaus aber keine dauerhafte Beziehungsstruktur, sondern stehen in nahezu vollkommener Konkurrenz zueinander (Wiesenthal 2000: 50 ff.). Der Ausstieg aus einer Transaktionsbeziehung (*exit*) ist so im Idealfall mit keinerlei Kosten verbunden (Hirschman 1970). Transaktionen sind dann prinzipiell in jeder Akteursdyade möglich, wodurch ein Maximum an Wettbewerb und Flexibilität hinsichtlich des gesamten Tauschflusses erreicht wird.

Zu den institutionellen Voraussetzungen eines idealen Marktes gehören u. a. ein funktionierendes Preissystem sowie ein vertragliche Rechte und Pflichten garantierendes Rechtssystem. Beide können daher auch als öffentliche Güter betrachtet werden (vgl. Kaul et al. 2003). Ersteres beruht im Allgemeinen auf einem abstrakten und generalisierten Tauschmedium, das die zentrale Funktion eines Mangelindikators bzw. Mittlers zwischen Angebot und Nachfrage erfüllt. Letzteres gewährleistet die Erfüllung eingegangener Transaktionsverpflichtungen und macht daher eine bestehende Vertrauensbeziehung und damit längerfristige Bindung zwischen potentiellen Transaktionspartnern unnötig. Beide tragen so zu einer Minimierung der anfallenden Informationskosten bei. Der vollkommene Markt stellt mithin eine „Arena dar, in der jede Partei

die selbstdefinierten Ziele und Bedürfnisse realisieren kann“ (Powell 1996: 223). Sein Allokationsergebnis entspricht einer spontanen Ordnung im Sinne Hayeks (2003).

Gleichwohl ist der Mechanismus des Marktes nicht in jedem Fall a priori Garant einer Pareto-effizienten Allokation (vgl. Richter u. Wiegard 1993), sondern versagt vor allem im Falle von Externalitäten. Solche externen Effekte entstehen immer dann, wenn Produktion oder Konsum eines Gutes zugleich den Nutzen Dritter tangiert, Kosten oder Nutzen einer Handlung also nicht mehr individuell zurechenbar und damit privat, sondern von kollektivem bzw. sozialem Charakter sind. Externalitäten können in ihrer Qualität positiv oder negativ sein, je nachdem ob sie sozialen Zusatznutzen oder soziale Zusatzkosten implizieren. Ihre Ursache liegt „in nicht vollständig definierten Eigentumsrechten bzw. in einem Versagen des Ausschlussprinzips“ (Weimann 2004: 133). Externe Effekte ziehen zusätzliche Informations- und damit Transaktionskosten nach sich, da das Kosten-Nutzen-Verhältnis der ihnen zugrundeliegenden Handlung nicht vollständig über das Preissystem des Marktes abgebildet werden kann (Dahlman 1979: 150 ff.). Sie haben daher im allgemeinen eine ineffiziente Ressourcenallokation zur Folge.

Externe Effekte stehen in engem Bezug zur Kategorie der kollektiven Güter. So kann man positive Externalitäten in gewisser Hinsicht als Produktion eines öffentlichen Gutes, negative hingegen als (Über-)Nutzung eines Allmende-Gutes interpretieren. In beiden Fällen werden jeweils die Interessen mehrerer Akteure tangiert. Dieser Umstand impliziert eine strategische Interaktionsdimension im Sinne der Spieltheorie, da die beteiligten Akteure gezwungen sind, hinsichtlich ihres individuellen Kosten-Nutzen-Verhältnisses neben dem eigenen Handeln auch die Konsequenzen möglicher Handlungen Dritter zu berücksichtigen. Häufig verhindert dabei eine Rationalitätenfalle, i. e. das Auseinanderfallen von individueller und kollektiver Rationalität, eine optimale Ressourcenallokation bzw. Nutzendistribution auf Basis eines reinen Marktmechanismus. Es ergibt sich das Problem, die individuellen Handlungen der Akteure so zu koordinieren, daß ein wohlfahrtsmaximierendes Ergebnis erreicht wird.

Geht man aus Gründen der Vereinfachung zunächst von einem minimalen Interaktionssystem mit nur zwei Akteuren und zwei Handlungsalternativen bzw. -strategien (Kooperation und Defektion) aus, so lassen sich drei archetypische Klassen strategischer Problemkonstellationen unterscheiden (Zürn 1992: 153; Scharpf 2000: 129 ff.):

1. *Reine Koordinations- bzw. Normierungsprobleme*: Hier konvergieren die Interessen beider Akteure. Es existieren zwei Nash-Gleichgewichte, von denen jedoch eines Pareto-superior ist, so daß sich das Koordinationsproblem auf

ein Kommunikationsproblem reduziert.

2. *Reine Konflikt- bzw. Wettbewerbsprobleme*: Hier divergieren die Interessen beider Akteure diametral. Aufgrund eines fehlenden Nash-Gleichgewichts kann es nur konfliktäre und damit labile Lösungen geben. Stabilität läßt sich nur durch die Machtprojektion eines externen Regelungsapparates erreichen, der durch Gratifikation und/oder Sanktion die Nutzenfunktion der beteiligten Akteure modifiziert.
3. *Mixed-Motive-Probleme*: Hier divergieren die Interessen beider Akteure orthogonal, wodurch sich sowohl Konflikte als auch Gemeinsamkeiten ergeben können. Es entsteht eine komplexe Interdependenz. Typische Konstellationen sind Versicherungsspiel, Geschlechterkampf, Gefangenendilemma oder das Spiel mit dem Untergang.

Der Produktion öffentlicher Güter liegt zumeist ein Mixed-Motive-Problem zugrunde. Zwar sind prinzipiell alle Akteure an der Bereitstellung dieser Güter interessiert, jedoch streben sie zugleich danach ihren individuellen Produktionskostenanteil zu minimieren. Nach Olson (1965) läßt sich diese strategische Konstellation im allgemeinen als spieltheoretisches Gefangenendilemma modellieren. Es handelt sich dann um ein Variabelsummenspiel mit dominanter Strategie, gemäß derer defektierende Akteure aufgrund einer „Trittbrettfahrer-Problematik“ in jedem Fall höhere Auszahlungen erzielen, als jene, die kooperieren. Es existiert folglich nur ein Nash-Gleichgewicht (Nash 1951), in welchem alle rational handelnden Akteure defektieren, wodurch es zu einer Unterversorgung an öffentlichen Gütern kommt. Gleichwohl ließe sich durch beidseitige Kooperation sowohl die Gesamtauszahlung, d. h. die allgemeine Wohlfahrt, als auch der individuelle Nutzen jedes einzelnen Akteurs steigern, also eine Pareto-superiore Allokation herbeiführen.

Die Produktion öffentlicher Güter kann allerdings auch durch andere Konstellationen strukturiert sein (Cornes u. Sandler 1996; Sandler 2004: 25 ff.). Von besonderer Bedeutung für die Art der Konstellation ist hier insbesondere die spezifische Aggregationstechnologie des jeweiligen Gutes (vgl. Cornes 1993; Holzinger 2001). Bereits Hirshleifer (1983, 1985) weist darauf hin, daß sich der Gesamtnutzen eines öffentlichen Gutes nicht zwangsläufig additiv aus den Beiträgen aller am Produktionsprozeß beteiligten Akteure ergibt. Stattdessen kann der Gesamtnutzen auch ausschließlich durch den niedrigsten (*weakest-link*) oder höchsten (*best-shot*) Einzelbeitrag bestimmt sein. Im ersten Falle handelt es sich dann um ein Versicherungsspiel, im letzteren um ein Spiel mit dem Untergang. In beiden Spielen gibt es keine dominante Strategie und es

existieren jeweils zwei Nash-Gleichgewichte. Problematisch ist hier, daß im Versicherungsspiel nur ein Nash-Gleichgewicht, im Spiel mit dem Untergang sogar keines der beiden Nash-Gleichgewichte, einer wohlfahrtsmaximierenden Lösung entspricht.

Auch die Distribution eines Allmende-Gutes ist mit einer Mixed-Motive-Problematik verbunden, die oftmals zu einer „Tragik der Allmende“ (Hardin 1968; Ostrom 1993) führt. Da Allmende-Güter zwar prinzipiell von jedem genutzt werden können, jedoch zugleich erschöpfbar sind, sehen sich die Akteure hinsichtlich ihrer Verteilung ebenfalls mit einem Gefangenendilemma konfrontiert. Aufgrund der Konkurrenzsituation defektieren im Nash-Gleichgewicht alle Akteure, so daß es zu einer Übernutzung des Gutes und damit zu einem Wohlfahrtsverlust kommt. Nach dem Coase-Theorem ergibt sich hier ausschließlich dann eine optimale Verteilung des Nutzens, wenn die Möglichkeit transaktionskostenfreier Verhandlungen und Ausgleichszahlungen zwischen den konkurrierenden Akteuren gegeben ist (Coase 1960).

Das Versagen des Marktes bezüglich der Produktion und Distribution kollektiver Güter begründet offensichtlich die Notwendigkeit weiterer, marktalternativer Regelungsformen. So schreibt Arrow (1963: 947):

> I propose here the view that, when the market fails to achieve an optimal state, society will, to some extent at least, recognize the gap, and nonmarket social institutions will arise attempting to bridge it.

Spieltheoretisch betrachtet bringen diese Regelungsmechanismen individuelle und kollektive Rationalität über eine Regeländerung und damit eine Modifikation der individuellen Nutzenfunktion der Akteure in Einklang. An die Stelle des konkurrenzorientierten und anonymen Mechanismus des Marktes treten in einigen Bereichen dauerhaft marktalternative Steuerungsstrukturen, Inseln intentionaler exogener Ordnungsinduktion – „islands of planned co-ordination in a sea of market relations“, wie Richardson (1972: 883) treffend formuliert.

Allgemein kennzeichnend für marktalternative Mechanismen ist, daß Akteure in ihrem Rahmen teil- und/oder zeitweise, freiwillig oder oktroyiert, auf ihre *Exit*-Option und damit auf einen wesentlichen Teil ihrer autonomen Handlungsfreiheit verzichten (Hirschman 1970). Oft sind die beteiligten Akteure dann dauerhaft in einem eng gekoppelten institutionellen Geflecht organisiert, in dessen Gefüge sie ihre Handlungen an vordefinierten Rollen orientieren. Zugleich übertragen sie einer solchen systemischen Organisation als Ganzer die Kontrolle über Teile ihrer individuellen Ressourcen und

handeln selbst nurmehr als Agenten in deren Auftrag, wodurch diese über eine souveräne Handlungs- und Entscheidungsmacht nach innen und außen verfügt und damit die Qualität eines eigenständigen Handlungssubjekts – eines korporativen Akteurs – erhält (vgl. Coleman 1974; Scharpf 2000: 101 ff.; Schimank 2002). Korporative Akteure können dann in bestimmten Kontexten gegenüber einem nur kollektiv operierenden Akteursaggregat neben Größen- und Verbundvorteilen eine Reihe weiterer Vorteile realisieren, zu deren wichtigsten eine weitgehende Spezialisierung durch Arbeitsteilung, eine dauerhafte Interessenverfolgung sowie die Fähigkeit zur erhöhten Komplexitätsbewältigung zählen (Schneider 2000a: 247).

Dem stehen allerdings im Soll die anfallenden Kosten für eine nunmehr notwendige intentionale Steuerung der Ressourcenallokation entgegen. Ergibt sich durch den Mechanismus des Marktes, in Abhängigkeit von dessen Grad an Walrasianischer Vollkommenheit, eine mehr oder weniger effektive Ressourcenallokation durch Smith' (1991) „unsichtbare Hand" spontan, so muß diese innerhalb einer Organisation von einer „sichtbaren Hand" (Chandler 1977) intentional herbeigeführt werden (vgl. Williamson 1996: 145 ff.). Dispositionsentscheidungen fallen hier im Gegensatz zum Markt nicht dezentral sondern zentral, d. h. hierarchisch koordiniert, und liegen daher nicht immer auch im individuellen Interesse der Organisationsmitglieder, woraus sich eine besondere Motivations- und Kontrollproblematik ergibt. Zugleich können die Mitglieder ihren Individualinteressen nicht mehr durch Abwanderung (*exit*) sondern nurmehr durch Widerspruch (*voice*) Gehör verschaffen (vgl. Hirschman 1970).

Die Folge sind informationelle Asymmetrien, die eine besondere Steuerungsproblematik implizieren und vor allem von der Agenturtheorie thematisiert werden. Innerhalb eines hierarchischen Kontexts spielen daher Autorität und Loyalität eine zentrale Rolle (vgl. Simon 1996). Einerseits senken hierarchische Organisationen auf diese Weise zwar Transaktionskosten, weil sie umfangreiche Ressourcen von vorn herein einer zentralen Dispositionsinstanz unterstellen und gleichzeitig das Eigeninteresse einzelner Mitglieder zumindest partiell hinter ein aggregiertes Gemeininteresse zurücktreten lassen. Andererseits können informationelle Engpässe zwischen den Ebenen einer Hierarchie aber auch zusätzliche Informationskosten nach sich ziehen und daher zu einer Fehlallokation bzw. einem Organisationsversagen führen.

In Anbetracht dessen kommt der Inklusivität einer Organisation, verstanden als Ausmaß der Partizipationsmöglichkeiten ihrer Mitglieder am Prozeß der korporativen Ressourcen-Disposition insofern besondere Bedeutung zu, als eine möglichst umfassen-

de Berücksichtigung aller Individualinteressen und damit eine möglichst breite Interessenaggregation entscheidend zur rationalen Legitimation des letztlich erzielten Distributionsergebnisses beiträgt (vgl. Habermas 1999: 166). Je geringer diese Legitimation ausfällt, desto weniger kann die Loyalität und damit eine intrinsische Motivation der Organisationsmitglieder vorausgesetzt werden und desto stärker müssen diese über zusätzliche Gratifikationen und/oder Sanktionen zu kooperativem Verhalten extrinsisch angehalten werden. Coleman (1990: 72 ff.) spricht in diesem Zusammenhang auch von konjunkten (hohe Partizipation) und disjunkten (geringe Partizipation) Organisationsstrukturen.

Aufgrund von Rationalisierungseffekten neigen einmal existente Organisationen häufig zur horizontalen Integration funktional äquivalenter Strukturen und damit letztlich zu einer Monopolbildung. Elias (1939: 123 ff.) unterstreicht die Bedeutung eines solchen „Monopolmechanismus“ im Rahmen der organisationsgeschichtlichen Herausbildung zentraler Fürstentümer während der europäischen Feudalzeit. Im Zeitalter der Renaissance verschärften sich deren gegenseitige Machtkämpfe dann zunehmend. Stehende Heere sowie eine dauerhafte Militär- und Steuerverwaltung zu ihrem Unterhalt wurden erforderlich. Eine hieraus resultierende monopolisierte Zentralgewalt schuf schließlich die Voraussetzungen für den modernen europäischen Nationalstaat (Mayntz 1997b; van Creveld 2004). Mit einem aus verschiedenen Kämpfen hervorgegangenen Staatsterritorium sowie einem kulturell zumeist homogenen Staatsvolk umfaßt dieser einen nach außen hin weitgehend abgeschlossenen Raum, „in dem sich gesellschaftliche Austauschbeziehungen und Handlungszusammenhänge verdichtet“ (Zürn 2001: 222) haben.

Der Staat ist demnach jene öffentliche – weil omnipräsente – idealtypische Organisation, die alle innerhalb eines eingegrenzten geographischen Territoriums lebenden Personen obligatorisch inkorporiert. Durch den Anspruch des Gewaltmonopols behält er sich potentiell und exklusiv die absolute und letztinstanzliche Dispositionsgewalt über alle auf seinem Territorium verfügbaren Ressourcen als Grundlage einer souveränen Handlungs- bzw. Interventionsmacht nach innen wie außen vor. Diese Handlungsmacht ist jedoch nach innen und außen *de facto*, in konstitutionellen Staaten nach innen auch *de jure*, beschränkt, so daß partielle Räume individueller Verfügungsgewalt existieren, in denen private Formen institutioneller Steuerung – seien es private Hierarchien oder Marktarrangements – bestehen können.

Legitimiert wird das staatliche Gewaltmonopol über die Gewährleistung einer ausreichenden Versorgung mit kollektiven Gütern, zu denen traditionell innere wie äuße-

re Sicherheit gehören (vgl. Desai 2003). Diese Kollektivgüter sind zugleich notwendige Voraussetzung einer dauerhaften Aufrechterhaltung sozio-ökonomischer Ordnung.[31] Ihre Produktion und Distribution wird über die Formulierung und Implementation politischer[32] Programme (Politiken) reguliert, die eine Koordination kollektiven Handelns sicherstellen (vgl. Francis 1993). Der Staat nimmt dabei idealtypisch die Funktion einer zentralen Steuerungsinstanz, eines kybernetischen Reglers, innerhalb der Gesellschaft wahr, wohingegen private Akteure als Steuerungsobjekte den Gegenstand öffentlicher (Fremd-)Regulierung bilden (vgl. Mayntz 1987). Regulierung umfaßt dann „nicht nur die Regelbildung (*rule-building*), sondern auch die Regelüberwachung (*monitoring*) und Sanktionierung von Regelverstößen (*enforcement*)“ (Czada et al. 2003: 15). Schneider (2000c) weist jedoch darauf hin, daß der Staat als öffentlicher Sektor keine „unitarische Handlungseinheit“ (a. a. O.: 246) bzw. „singulär-integrierte Hierarchie“ (a. a. O.: 245), sondern vielmehr ein komplexes „Organisationsfeld korporativer Akteure“ (a. a. O.: 245) darstellt, welches „aus einer Pluralität von weitgehend selbständigen Organisationen besteht, die ihre Handlungsziele relativ autonom bestimmen“ (a. a. O.: 245).

Der Bogen institutioneller Steuerungsmechanismen spannt sich somit von dezentralen Strukturen des Marktes einerseits bis zu hierarchischen Organisationsstrukturen andererseits. Im Kontext dezentraler Marktmechanismen werden die Akteure primär intrinsisch durch individuelle Interessen motiviert, während sich hierarchische Strukturen an einem übergeordneten Kollektivinteresse orientieren und daher extrinsischer Anreize bedürfen. Die Sphäre des Handelns ist im ersten Falle eher privater, im zweiten eher öffentlicher Natur. Je nach Art des dominierenden Steuerungsrahmens können Akteure entsprechend klassifiziert werden. Für die vorliegende Untersuchung wurde hierzu eine Ordinalskala möglicher Organisations-*Status* gewählt, die von *öffentlichen* über *gemischte* bis hin zu *nicht-gewinnorientierten* und *gewinnorientierten privaten* Akteuren reicht. Entscheidend für die Klassifizierung sind jedoch nicht die internen Steuerungsmechanismen eines korporativen Akteurs, die ja per definitionem immer hierarchisch sind, sondern vielmehr dessen externer Koordinationsmodus im Zusammenspiel mit

31 Auf die primär ordnungswahrende Funktion des Staates verweist bereits die Etymologie des Begriffs, der sich vom lateinischen Wort *status* ableitet und damit auf Lage, Verfassung und Zustand eines sozio-ökonomischen Systems Bezug nimmt.

32 Der Begriff des „Politischen“ leitet sich bekanntlich wortgeschichtlich vom altgriechischen $\pi o \lambda \iota \varsigma$ (*polis*) her und verweist damit per se auf einen, die (stadtstaatliche) Gemeinschaft als Ganzes betreffenden, öffentlichen Zusammenhang.

anderen Akteuren.

2.2.3 Governance-Konfigurationen im globalen Kontext

Die Fähigkeit öffentlicher Akteure politische Programme effektiv und effizient umsetzen zu können wird wesentlich durch deren (Handlungs-)Macht determiniert. Diese wiederum ist eine Funktion der jeweils zur Verfügung stehenden Ressourcen. Sozioökonomische Prozesse der Industriealisierung und Globalisierung führen dabei offenbar zu einer Erosion staatlicher Handlungssouveränität nach innen wie außen. Ein damit verbundener Verlust an öffentlicher Steuerungskapazität wirft hinsichtlich der Produktion und Distribution kollektiver Güter die Frage nach neuen, alternativen Governance-Konfigurationen jenseits der traditionellen Steuerungsmechanismen des reinen Marktes einerseits, sowie eines klassischen Etatismus andererseits, auf (vgl. Rosenau u. Czempiel 1992; Kooiman 1993; Rhodes 1996, 1997; Ronit u. Schneider 1999, 2000a; Schneider 2004c). Die theoretische Perspektive auf die skizzierte Problematik variiert dabei je nach disziplinärem Kontext mitunter erheblich (vgl. Mayntz 2005).

Im Zuge der Industriealisierung ermöglichte eine zunehmende technische Automatisierung im Verbund mit einer sowohl vertikalen als auch horizontalen Integration umfangreicher Produktionsprozesse zunächst Skalen- und Verbundvorteile, deren Realisierung allerdings eine Bündelung größerer Ressourcenmengen sowie eine weitgehende funktionale Ausdifferenzierung einzelner Arbeitsschritte – und damit zugleich den hohen Organisationsgrad privater Hierarchien – voraussetzte (vgl. Mayntz 1997a).[33] Ferner tendiert eine industrielle Massengesellschaft zu großen Akteursgruppen mit strukturell homogenen Interessen und daher zur Ausbildung verbandlicher Strukturen. Direkte Folge ist eine signifikante Zunahme der Anzahl und Größe korporativer Akteure auch im privaten Sektor (Coleman 1974; Judge 1995; Hollingsworth 1996; Perrow 1996, 2002; Ronit u. Schneider 2000a; Schneider 2000c).

Bezüglich moderner Gesellschaften kann somit nicht allein von Markt- sondern auch und vor allem von komplexen Organisationswirtschaften gesprochen werden, in denen der größte Teil des Transaktionsaufkommens nicht am freien Markt, sondern innerhalb geschlossener Organisationen abgewickelt wird (Chandler 1977; Simon 1996). Ei-

33 Vorbedingung eines solchen hohen Organisationsgrades ist zunächst ein hinreichendes infrastrukturelles Niveau, zu dem etwa fortgeschrittene Transport-, Kommunikations- und Energieversorgungssysteme gehören (vgl. hierzu Abschnitt 4.1).

ne zunehmende Akkumulation von Ressourcen im Einflußbereich privater Akteure aber stärkt deren Handlungsmacht und führt so zu einem relativen Verlust des Staates an innerer Souveränität (Schneider 2004d). Scharpf (1991: 622) spricht in diesem Kontext von einer „Enthierarchisierung der Beziehungen zwischen Staat und Gesellschaft".

Zugleich schaffte die Industriealisierung durch fortgeschrittene Logistiksysteme die Voraussetzung für eine erste Welle der Globalisierung[34] bzw. Internationalisierung, indem sie eine signifikante Ausweitung sozio-ökonomischer Handlungs- und Transaktionsbeziehungen über nationale Grenzen hinweg erlaubte. Es entstanden grenzüberschreitende Ressourceninterdependenzen, die die äußere Souveränität des Staates im Verhältnis zu anderen Staaten einschränken und neue Formen internationaler Kooperation erfordern (Keohane u. Nye 1977, 2000a; Held et al. 1999; Held 2000; Held u. McGrew 2003; Keohane 2002, 2005; Zürn 2001; Nye 2004). Darüber hinaus führte eine zunehmende Ausdehnung von Produktions- und Transaktionsketten über nationalstaatliche Grenzen hinweg auch zu grenzüberschreitenden Externalitäten und damit zu einer internationalen Bereitstellungs- bzw. Verteilungsproblematik hinsichtlich globaler Kollektivgüter (Cerny 1995; Nordhaus 2000; Sandmo 2003). Die Folge ist eine geographische Inkongruenz von sozio-ökonomischer Steuerungsproblematik und staatlicher (politischer) Regulierungsfähigkeit (Reinicke 1998a; Zürn 1998, 2001).

Eine weitere Welle der Globalisierung bzw. „Transnationalisierung" (vgl. Kaiser 1969) geht auf die Entwicklung leistungsfähiger Informations- und Kommunikationssysteme zurück (Marsden 2000a; Schneider 2004d). Diese senken Informations- und Transaktionskosten in nennenswertem Umfang und ermöglichen privaten Akteuren eine transnationale Reorganisation interner Produktionsabläufe. Flankiert von einer umfassenden Liberalisierung und Deregulierung nationaler Märkte entsteht so eine global immer enger verflochtene Ökonomie (Kahler u. Lake 2003; Schneider u. Tenbücken 2004). In dieser gewinnen transnational operierende private Akteure als „Global-Player" deutlich an Handlungsmacht, da sie sich territorial gebundener staatlicher Intervention oftmals leicht entziehen können. Das klassische Instrumentarium staatlicher Intervention stellt öffentliche Akteure dann vor die Wahl zwischen einem defensiven Protektionismus und einem offensiven, inter-staatlichen Deregulierungswettbewerb (Reinicke

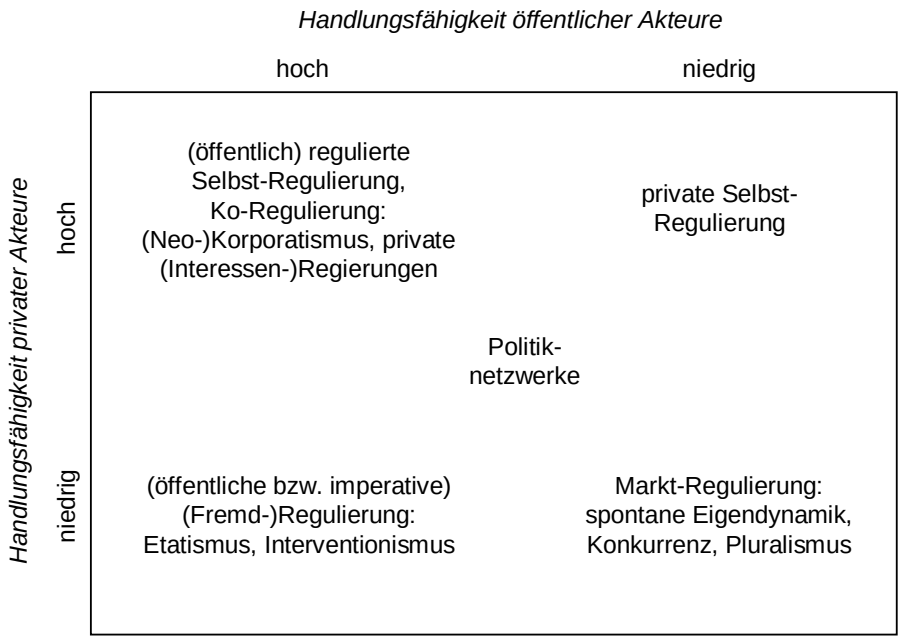
34 Held u. McGrew (1999, 2003) interpretieren das Phänomen der Globalisierung als lang anhaltenden Prozeß, der sich schubweise ausbreitet. Sie gehen historisch noch weiter zurück und sehen vorhergehende Wellen der Globalisierung bereits im Zeitalter der Entdeckungen sowie des Imperialismus.

1998a: 75 ff.). Beide Strategien sind jedoch mit schwerwiegenden Nachteilen verbunden, da protektionistische Lösungen zumeist Wohlfahrtsverluste implizieren, während ein Deregulierungswettbewerb staatliche Steuerungsmöglichkeiten per se stark einschränkt und so zu einer Unterversorgung an kollektiven Gütern führen kann.

Einige Autoren sehen einen Ausweg aus diesem Dilemma vor allem in transgouvernementalen Netzwerken des politisch-administrativen Sektors (vgl. Slaughter 2004; Thurner et al. 2005; Eberlein u. Newman 2008). Angesichts des komplexen Umfeldes einer global verflochtenen Ökonomie erscheint eine exklusive Steuerung der Produktion und Distribution globaler Kollektivgüter durch öffentliche Akteure allein jedoch nahezu unmöglich. Vielmehr erstreckt sich das mit der Formulierung und Implementation globaler Politiken befaßte Politikfeld notwendiger Weise auch auf private Akteure (Bagnoli u. Lipman 1989; Risse-Kappen 1995; Powell u. Clemens 1998; Holitscher 1999; Schneider u. Ronit 1999; Ronit u. Schneider 1999, 2000b; Börzel 2000, 2002; Schneider 2000b, 2002; Knill u. Lehmkuhl 2002a,b; Edwards u. Zadek 2003; Hertel 2003; Börzel u. Risse 2005; Pattberg 2005; Arts 2006). Insofern diese dann nicht ausschließlich durch staatliche Intervention fremdgesteuert werden, sondern Steuerungssubjekt und -objekt zumindest teilweise zusammenfallen, entstehen spezifische Arten der Selbst-Regulierung. Solche Arten kybernetischer Selbst-Regulierung erscheinen etwa bei Dunsire (1993) als eigenständige Governance-Form neben Staat und Markt.

Abbildung 2.5 strukturiert das in der Theorie diskutierte Spektrum idealtypischer Governance-Konfigurationen entlang der Handlungsmacht bzw. -fähigkeit der am Regulierungsprozeß beteiligten öffentlichen (staatlichen) und privaten (gesellschaftlichen) Akteure. Jede Form der Selbst-Regulierung setzt dabei zunächst eine ausreichende kollektive Handlungsfähigkeit auf Seiten privater Akteure voraus. Trifft diese zugleich auf eine hohe Handlungsmacht öffentlicher Akteure, so ergeben sich häufig Arrangements einer regulierten Selbst-Regulierung (vgl. Schulz u. Held 2002) bzw. Ko-Regulierung (vgl. Latzer et al. 2002), innerhalb derer private Akteure im Rahmen öffentlicher Vorgaben zu quasi-staatlichen Funktionsträgern aufsteigen können. Im Bereich innenpolitischer Theorien werden diese Arrangements zumeist unter dem Stichwort des *(Neo-) Korporatismus* bzw. *privater (Interessen-)Regierungen* thematisiert (Lehmbruch 1967; Schmitter 1977, 1979; Streeck 1983, 2006; Streeck u. Schmitter 1985, 1996; Coleman 1999).

Insbesondere Interessenverbände nehmen hier eine Schlüsselfunktion als janusgleiches Scharnier zwischen individueller und kollektiver Handlungsrationalität wahr. Ei-



Quelle: In Anlehnung an Mayntz u. Scharpf (1995b: 25) sowie Knill u. Lehmkuhl (2002b: 49).

Abbildung 2.5: *Idealtypische Governance-Konfigurationen*

nerseits vertreten sie nach außen gegenüber staatlichen Akteuren die aggregierten Partikularinteressen ihrer privaten Mitglieder im Prozeß der Politik-Formulierung (Mitgliedschaftslogik), andererseits koordinieren sie diese Mitglieder nach innen im Prozeß der Politik-Implementierung in Übereinstimmung mit öffentlichen, an einem kollektiven Handlungsziel orientierten Vorgaben (Einflußlogik) (Streeck 1983; Streeck u. Schmitter 1985, 1996). Eine zentrale Ressource, die Verbände dem Staat hierbei im Tausch gegen eine Berücksichtigung ihrer Interessen zur Verfügung stellen, ist jener relative Wissens- bzw. Informationsvorsprung, den private Akteure als Regulierungsobjekte gegenüber öffentlichen Akteuren als Regulierungssubjekten der Sache nach haben. Gerade in komplexen Regulierungszusammenhängen kann dieser von kritischer Bedeutung für den Erfolg einer Politik sein.

Darüber hinaus haben Verbände oftmals die Fähigkeit, politische Programme partiell auch gegen die Partikularinteressen der eigenen Mitgliederklientel durchsetzen zu können. Dies setzt allerdings den hohen Organisationsgrad monopolisierter Interessenvertretungen voraus. Gerade hier zeigen sich bedeutende Unterschiede zwischen US-amerikanischen und kontinentaleuropäischen Interessenverbänden. Während in Euro-

pa mit den Zünften korporatistische Formen zentraler Interessenvertretung bereits im Mittelalter, also weit vor der dem Aufkommen der Nationalstaaten, existierten, entstanden Interessenverbände in den USA erst im Zuge der Industriealisierung. Ferner behindert in den USA eine strikte Kartellgesetzgebung weitgehend die Herausbildung monopolisierter Interessenvertretungen (vgl. Kagan 2001), wohingegen diese in Europa durch Zwangsmitgliedschaften – so etwa im berufsständischen Kammernsystem – oftmals staatlich gefördert wird. Hieraus ergeben sich zwei grundlegend verschiedene Modi der Ko-Regulierung in den USA und Europa, die Newman u. Bach (2004) als „legalistische“ und „koordinierte“ Selbst-Regulierung bezeichnen. Die Selbst-Regulierung privater Akteure beruht demnach in den USA vor allem auf der präventiven Vermeidung staatlicher Intervention, während sie in Europa das Ergebnis eines koordinierten Aushandlungsprozesses ist. Wichtigste Ressource öffentlicher Akteure zur Durchsetzung politischer Programme ist in den USA die Androhung einer gesetzlichen (Fremd-) Regulierung, in Europa jedoch die Delegation staatlicher Autorität.

Im komplexen Umfeld einer global verflochtenen Ökonomie spricht, wie bereits erwähnt, allerdings vieles dafür, daß weder öffentliche noch private Akteure für sich genommen über eine ausreichende Handlungsfähigkeit zur Produktion und Distribution globaler Kollektivgüter verfügen. Vielmehr ergänzen sich ihre jeweiligen Ressourcen – und damit auch ihre Handlungsmöglichkeiten – oftmals komplementär, so daß eine wechselseitige Kooperation erforderlich ist. Zur Mobilisierung verstreuter Ressourcen aber eignen sich insbesondere jene Governance-Konfigurationen, die in der Theorie als *(Politik-)Netzwerke* diskutiert werden (vgl. u. a. Kenis u. Schneider 1991; Scharpf 1994a,b; Schneider et al. 1994; Jansen u. Schubert 1995; Mayntz 1996; Powell 1996; Börzel 1998; Thatcher 1998; Benner u. Reinicke 1999; Reinicke 1999; Kappelhoff 2000b; Witte et al. 2000; Reinicke et al. 2001; Benner et al. 2002, 2003, 2004; Schneider 2003, 2004a, 2005).

Aus der abstrakten Perspektive der mathematischen Graphentheorie handelt es sich bei Netzwerken zunächst ganz allgemein um eine Ansammlung von Knoten (Akteuren) und Kanten (Beziehungen). Zieht man diese Definition als Grundlage eines steuerungstheoretischen Netzwerkkonzeptes heran, so läßt sich prinzipiell jedes komplexe sozioökonomische System als Netzwerk interpretieren. Allerdings verliert das Netzwerkkonzept durch eine derart umfassende Auslegung bedeutend an analytischer Schärfe (vgl. Kenis u. Schneider 1991: 40). Es scheint daher sinnvoll, eine engere Begriffsdefinition zu wählen. So werden Netzwerke in der institutionellen Ökonomie zumeist als alternative

TABELLE 2.1: *Typologie diskreter Steuerungsformen*

	Markt	*Netzwerk*	*Hierarchie*
Kopplungsstruktur	atomistisch, anonym	horizontal, reziprok, informell, variabel	vertikal integriert, formal organisiert
Interessen	individuell	interdependent, konjunkt	kollektiv, aggregiert
Handlung	individuell, kompetitiv	konzertiert, kooperativ	korporativ, delegiert
Sphäre	privat	hybrid	öffentlich
Motivation	intrinsisch	hybrid	extrinsisch
Ressourcen	individuell	komplementär	kollektiv gepoolt
Allokation	spontane Tauschdyaden	generalisierter Tausch	autoritäre Disposition
Koordination	dezentral	polyzentral	zentral
Steuerungsmedium	Preise	Vertrauen, Sozialkapital	Anweisungen
Rückkopplung	Abwanderung	Verhandlung	Widerspruch

Hybridform aufgefaßt, die in einem Kontinuum zwischen den extremen Polen eines dezentralen Marktes und einer zentralen Hierarchie angesiedelt ist und gegenüber diesen Extrema besondere, kontextspezifische Transaktionskostenvorteile aufweist (vgl. etwa Williamson 1985, 1996; Wolff u. Neuburger 1995; Jones et al. 1997).

Allerdings verengt eine solche Betrachtung die Analyse von Governance-Konfigurationen einseitig auf das Merkmal der jeweiligen Kopplungsstruktur (vgl. Mayntz 1996: 477). Netzwerke unterscheiden sich jedoch nicht nur durch die Art ihrer Kopplung, sondern auch durch eine Reihe weiterer Charakteristika von den Mechanismen des Marktes und der Hierarchie (vgl. Tabelle 2.1). Powell (1996) argumentiert deshalb, bei Netzwerken handle es sich weniger um eine Hybridform, als vielmehr um eine diskrete Steuerungsform jenseits von Markt und Hierarchie mit gänzlich neuen Qualitäten. Die Akteure gehen in dieser freiwillig informelle – oftmals themenspezifisch orientierte (vgl. Heclo 1978) – Austauschbeziehungen ein, deren längerfristiger Unterhalt dann wechselseitiges Vertrauen schafft. Vor dem Hintergrund eines durch Iteration und Interdependenz gekennzeichneten Handlungskontextes (vgl. Axelrod 1984) wird eine neue Form polyzentraler Koordination möglich, in welcher sich die Ressourcenallokation weder spontan noch autoritär vollzieht, sondern auf einem generalisierten – möglicherweise

transitiven – Tausch beruht (vgl. Marin 1990a,b). Steuerungsmedium ist hierbei vertrauensbasiertes Sozialkapital, welches als zentrale „Meta-Ressource" die Mobilisierung weiterer Ressourcen im Netzwerk erst ermöglicht (vgl. Bourdieu 1983, 1985; Coleman 1988, 1990).[35]

Im Gegensatz zu hierarchischen Formen der Koordination verfügen Netzwerke nicht über eine vertikal integrierte und formal organisierte Kopplungsstruktur. Ihre Stärke liegt vielmehr in einer großen Zahl informeller und loser Verbindungen (vgl. Granovetter 1973). Diese „variable Geometrie" (Castells 2000a: 1) eröffnet die Möglichkeit einer permanenten Rekonfiguration. Durch ihre Polyzentralität implementieren Netzwerke eine komplexe, mehrstufige Steuerungsarchitektur. Sie besitzen keinen unmittelbaren Problemlösungsmechanismus, sondern institutionalisieren stattdessen einen Algorithmus zur Auffindung und Umsetzung einer singulären Lösung im Wege der Verhandlung. Diese Eigenschaft versetzt sie in die Lage, Ressourcen ähnlich dem Markt punktuell und problemspezifisch zu mobilisieren, wobei die Akteure gleichzeitig konzertiert kooperieren und so Konflikte zwischen kollektiver und individueller Handlungsrationalität weitgehend vermeiden. Ihre Organisationskapazität ist virtuell insofern, als sie nur der Möglichkeit nach vorgehalten und lediglich im konkreten Problemfall temporär realisiert wird.

In stabilen Umgebungen, in denen große Klassen strukturell ähnlicher Standardprobleme vorherrschen, sind Netzwerke hierarchischen Formen der Koordination unter Transaktionskostengesichtspunkten aufgrund dieser Eigenschaften unterlegen, da sie immer auch aufwendige Verhandlungsprozesse implizieren. In komplexen, hoch variablen Umgebungen mit hoher Problemvarianz hingegen stellt die strukturell bedingte Flexibilität eines Netzwerkes einen gewichtigen Vorteil dar. Sie ermöglicht einen Anpassungsprozeß, der in der Theorie organisationalen Lernens durch Argyris u. Schön (1978) als „Double-Loop-Learning" charakterisiert wurde und letztlich auf Selbstreflexion beruht. Netzwerke reagieren auf Probleme im Unterschied zu Hierarchien nicht in Form eines starren, mechanischen *Input-Output*-Schemas mit strukturell implementierter Steuerungslogik, sondern vielmehr im Wege dynamischer Restrukturierungsprozesse, wie sie auch Gegenstand der Theorie komplex-adaptiver Systeme sind (vgl. Gell-

35 Nach Putnam (1993: 169) weist soziales Kapital Charakteristika einer „moral resource" (Hirschman 1984: 93) auf. Solche „moralischen Güter" sind nicht nur nicht-rivalisierend, sondern ihr Gebrauch erhöht ihren Nutzwert darüber hinaus zusätzlich. Umgekehrt verringert sich ihr Nutzwert mit abnehmendem Gebrauch.

Mann 1994, 1995a,b; Kauffman 1993, 1995; Kappelhoff 2000a). Im komplexen Umfeld einer global verflochtenen Ökonomie, in dem permanent qualitativ neue Probleme auftreten, ist diese Fähigkeit von zentraler Bedeutung. Im Sinne einer „horizontalen Subsidiarität“ (Reinicke 1998b: 89) werden kollektive Güter dabei idealiter von jenen Akteuren bereitgestellt, die über die geeignetsten Ressourcen hierzu verfügen.

Die Hauptaufgaben globaler Politiknetzwerke liegen Reinicke et al. (2001: 270 ff.) zufolge im Agendasetting, der Verhandlung globaler Standards, der Aggregation und Distribution problemspezifischer Informationsressourcen, der Ressourcenmobilisation zum Zwecke der Produktion kollektiver Güter sowie der Implementation gemeinsam ausgehandelter Politiken. Entsprechend identifizieren Benner et al. (2002) drei funktionale Typen globaler Politiknetzwerke:

1. *Verhandlungsnetzwerke* binden alle in einem spezifischen Politikfeld relevanten Akteure ein. Häufig dienen sie einer transparenten Aushandlung globaler Standards und Normen.
2. *Koordinationsnetzwerke* dienen als Informationsplattform. Sie ermöglichen die Abstimmung konzertierter Handlungsstrategien zur Produktion kollektiver Güter.
3. *Implementationsnetzwerke* unterstützen eine effektive Umsetzung internationaler Verträge.

Im Rahmen der vorliegenden Untersuchung ist neben dem *Status* der Akteure auch deren *Scope*, i. e. deren Aktionsradius von Interesse. Als ordinale Kategorien wurden hier die Aktionsebenen *national*, *regional* und *global* gewählt. Der regionale Aktionsradius entspricht dabei nicht einer sub-staatlichen Ebene, sondern einer geographisch eingegrenzten supra- bzw. internationalen Zwischenebene.

3 Die globale Informationsgesellschaft als Kontext

3.1 Information und Kommunikation

3.1.1 Zur Wort- und Ideengeschichte

Der Begriff der „Information“ ist zentraler Bestandteil einer Reihe wissenschaftlicher Disziplinen. Für die Informationswissenschaft ist das Phänomen der Information selbst primäres Erkenntnisobjekt, während die Informatik sich insbesondere mit den technischen Fragen ihrer Verarbeitung befaßt. Die Nachrichtentechnik beschäftigt sich mit den physischen Möglichkeiten der Übertragung von Information, wohingegen Medien- und Kommunikationswissenschaft den sozio-kulturellen Rahmen ihres Austausches beleuchten. Die Wirtschaftswissenschaft wiederum untersucht u. a. die Rolle von Information im Prozeß der Güterproduktion und für die Kybernetik schließlich ist Information Mittel biologischer, technischer und sozialer Steuerung. Angesichts einer derart breiten Streuung des Begriffs erscheint zunächst dessen nähere, etymologische wie inhaltliche Bestimmung sinnvoll.

Capurro (1978), der einen ausführlicher Überblick zur historischen Entstehung des Begriffs der Information gibt, ordnet diesen ideengeschichtlich in dasselbe Wortfeld wie die altgriechischen Begriffe $\varepsilon\iota\delta o\varsigma$ (*eidos*), $\iota\delta\varepsilon\alpha$ (*idea*) und $\tau\upsilon\pi o\varsigma$ (*typos*) ein, wodurch sowohl ein Bezug zum Begriff der Form in der Platonischen Ideenlehre als auch in der Aristotelischen Kategorienlehre hergestellt wird. Etymologisch geht Information auf das lateinische *informatio* zurück, welches sich seinerseits aus dem Präfix „in-“ und dem Hauptwort *formatio*, einer Substantivierung des Verbs *formare* (formen, gestalten) zusammensetzt. Im Gegensatz zum ursprünglichen Substantiv *forma*, das Form, Aussehen, Gestalt oder Archetypus meint, hebt das mittels der Endung „-tio“ substantivierte *formatio* allerdings die Handlung selbst oder aber deren Ergebnis hervor, beschreibt also das Formen, Gestalten, Bilden oder das Geformte, Gestaltete, Gebildete. Die Vorsilbe „in-“ apostrophiert dabei einerseits die beschriebene Handlung und charakterisiert diese andererseits als in etwas hineinwirkend. Unter *informatio* versteht der Lateiner demnach eine „Belehrung und Unterweisung“ im Sinne „einer Formung des Intellekts“

(Lyre 2002: 12) oder aber die Bildung selbst als deren Produkt. Im Lateinisch-Deutschen Wörterbuch findet sich *informatio* denn auch in der Übersetzung als (geistige) Vorstellung bzw. Idee.

Wie Capurro (1978) zeigt, behielt der Begriff der Information während des gesamten Mittelalters die antike Konnotation des pädagogischen Unterweisens im Sinne eines Wissenstransfers bei. In dieser Bedeutung wurde er in fast alle europäischen Sprachen, seit dem 15. Jahrhundert auch ins Deutsche, übernommen. Gleichzeitig erfährt er in den romanischen Sprachen sowie im Englischen bereits im ausgehenden Mittelalter, im Deutschen hingegen erst während der Aufklärung und im Humanismus, durch Übernahme in die Alltagssprache eine pragmatische Bedeutungserweiterung, in deren Folge man unter dem Vorgang des Informierens nun nicht mehr nur eine pädagogische Wissensvermittlung, sondern vielmehr auch das Erteilen einer – in einem konkreten Handlungszusammenhang relevanten – Benachrichtigung, Mitteilung oder Auskunft oder aber, reflexiv gebraucht, das Einholen einer solchen versteht. Diese pragmatische Konnotation des Informationsbegriffs ist die bis heute umgangssprachlich vorherrschende. Angelehnt an die Semiotik[36] wird ein allgemeiner Informationsbegriff im folgenden entlang dreier Dimensionen erschlossen: der *Semantik*, der *Syntaktik* sowie der *Pragmatik*. Je nach dominanter Sichtweise stellt sich Information dabei als *Bedeutung*, als *Datum* oder als *Ressource* dar.

3.1.2 Die semantische Dimension

Beginnen wir mit der Betrachtung von Information aus semantischer Perspektive in deren Eigenschaft als den Intellekt exogen Formendes, Bildendes, Gestaltendes. Wir befinden uns dann zugleich am unmittelbaren Übergang von objektiver Informationsrepräsentation zu subjektiver Informationsperzeption und -kognition. Dabei nimmt das Subjekt einen physischen Zustand A seiner Umwelt als etwas objektiv Gegebenes, als *Datum*[37], wahr. Information steht hier notabene zunächst nur für objektiv gegebene Datenstrukturen, unabhängig von deren Entstehungszusammenhang. Im anschließenden Erkenntnisprozeß wird das Wahrgenommene in Form einer neuen subjektiv-mentalen Repräsentanz A' abgebildet, oder aber ggf. als zu einer solchen, bereits bestehenden Re-

36 Diese geht im Wesentlichen auf die grundlegenden Arbeiten von Peirce (1998a), de Saussure (1931) und Morris (1966) zurück.

37 Das lateinische *datum* meint wörtlich etwas „Gegebenes“.

präsentanz gehörig (wieder-)erkannt. Wahrgenommenes wird so in die eigene, kognitive „Landkarte“ integriert und damit gedanklich (be-)greifbar gemacht.

Um jedoch in der allgegenwärtigen Flut von Daten, die durch eine Vielzahl scheinbar chaotischer Ereignisse in komplexen Umwelten ausgelöst wird, kausale Zusammenhänge erkennen zu können, müssen wahrgenommene Daten durch Abstraktion und Interpretation zudem mental verdichtet und strukturiert werden. So schreibt Nichols (1987: 7):

> Man is confronted with a wide and varied environment. To reduce the diversity of his environment to manageable order, man resorts to classification and to the information of general ideas about groups of things—that is, man simplifies to aid comprehension.

Jede Form mentaler Komplexitätsreduktion beruht, neben einer Klassifikation ähnlicher Ereignisse, vor allem auf dem Erkennen von Regelmäßigkeiten, die sich in der Korrelation wahrgenommener Zustände ausdrücken. Diese lassen die Konstruktion abstrakter, relationaler Modelle und damit die Neubildung von Wissen zu (vgl. Abschnitt 2.1.1). Der Gedanke einer maximalen Datenreduktion ohne Informationsverlust durch Aufdeckung struktureller Regelmäßigkeiten liegt ebenfalls dem Konzept der Kolmogorow-Komplexität[38] zugrunde, die daher auch als Maß des algorithmischen Informationsgehaltes einer Folge von Daten aufgefaßt werden kann (vgl. Li u. Vitanyi 1993).

Wenn also gilt, daß der Zustand A eines bestimmten Objektes regelmäßig den Zustand B eines weiteren Objektes impliziert, so ist es denkbar, A als Symbol, als sinnbildlich für B stehendes Zeichen, zu interpretieren, das es als solches zu deuten gilt. Der Deutung selbst liegt dabei jedoch nicht notwendigerweise eine objektive (Kausal-) Relation zwischen A und B zugrunde. Eine Deutung vollzieht sich vielmehr ganz wesentlich als subjektive Zuordnung von A zu B'. Saussure unterscheidet daher zwischen A, B und B' als „signifiant“, „signification“ und „signifié“; Peirce als „sign“, „object“ und „interpretant“. Peirce (1998b) differenziert ferner nach dem Zusammenhang von Bezeichner („sign“) und Bezeichnetem („object“) zwischen „icons“, „indices“ und „symbols“. „Icons“ sind Bezeichner, bei denen eine augenfällige Ähnlichkeit zwischen A und B besteht; „indices“ solche, bei denen ein tatsächlicher Zusammenhang vorliegt; während bei „symbols“ eine Relation allein aufgrund von Konventionen besteht.

Die Interpretation wahrgenommener Daten bewegt sich vor diesem Hintergrund immer im Spannungsfeld von intensionaler (Be-)Deutung und extensionalem, referen-

38 Dieses Komplexitätsmaß wurde nach dem russischen Mathematiker Andrej N. Kolmogorow benannt, der als dessen Entdecker gilt.

ziertem Objektbereich. Information kann somit als Prozeß der Transformation objektiv-physischer Datenstrukturen in subjektiv-mentale Repräsentanzen, als Rekonstruktion der äußeren physischen Welt in jener inneren begrifflicher Ideen, betrachtet werden. Information wirkt dann als solche induktiv, sie ergänzt, verändert und formt bestehende Wissensstrukturen und sedimentiert selbst zu neuem Wissen (vgl. hierzu Abschnitt 2.1.1). Nicht zuletzt die Erkenntnisse der analytischen (Sprach-)Philosophie seit dem *Linguistic Turn* lehren, daß sich dieser Prozeß im Kontext einer Einordnung des Wahrgenommenen in das logisch deduktive System eines dem Subjekt eigenen Begriffsnetzes vollzieht. Die kognitiven Strukturen eines solchen Netzes entstehen im definitorischen Wechselspiel begrifflicher Differenzierung durch Abgrenzung einerseits, sowie Integration durch Subsumption andererseits und haben prinzipiell autopoitischen Charakter. Erst diese Strukturierung des Wahrgenommenen in Form mentaler Repräsentanzen ermöglicht dessen kausale oder stochastische und damit verstehende – weil erklärende – Modellierung.

Problematisch aber bleibt die Frage, wie ein solchermaßen gebildetes, subjektives Begriffsnetz inter-subjektiv anschlußfähig wird, denn diese Anschlußfähigkeit ist notwendige Voraussetzung einer (Mit-)Teilbarkeit, i. e. Kommunikation[39] bestehenden Wissens. Im Laufe der Menschheitsgeschichte hat sich zu diesem Zwecke eine Reihe von Kommunikationssystemen herausgebildet, von denen die Sprache ohne Zweifel das bedeutendste ist. All diesen Kommunikationssystemen ist gemein, daß sie subjektive Begrifflichkeiten mit einem inter-subjektiv konstruierten Zeichensatz objektiver Zustände verknüpfen, um so die Möglichkeit des Informationsaustauschs zu eröffnen. Dieser gemeinsame semantische Wahrnehmungshorizont muß allerdings zunächst durch Interaktion mit der künstlich geschaffenen Welt des Zeichensystems erlernt werden (vgl. hierzu auch Abschnitt 2.1.1 und 2.1.3). Dieses Lernen erfolgt als interaktiver und iterativer Anpassungsprozeß im Wege von Versuch und Irrtum. Nur so wird eine Überwindung der Luhmannschen Problematik einer „doppelten Kontingenz“ möglich.

3.1.3 Die syntaktische Dimension

Betrachten wir das Subjekt als „informationsverarbeitendes System“, das Daten aus seiner Umwelt nicht nur aufnimmt und in mentale Repräsentanzen umformt, sondern solchermaßen gewonnenes Wissen auch mit anderen Subjekten auszutauschen sucht,

39 Das lateinische *communicare* bedeutet „teilen“ bzw. „mitteilen“.

so führt uns das zu der unmittelbaren Frage nach den syntaktischen Eigenschaften eines hierfür notwendigen Zeichensystems. Das Formen von Zeichen ist dabei als zur Datenrezeption komplementärer Prozeß der Produktion von Daten zu verstehen. Information bedeutet in diesem Sinne das Gestalten eines materiellen Trägermediums, durch welches diese für Dritte physisch faß- und damit zugleich wahrnehmbar wird. Es ergibt sich ein einfaches nachrichtentechnisches Modell des Datentransfers zwischen Informationsquelle und -senke. Das zwischengeschaltete physische Kommunikationssystem besteht aus einem Übertragungskanal sowie, jeweils an dessen Enden, einem zur Kodierung/Dekodierung geeigneten Sender/Empfänger. Als Zeichen finden in einem solchen System die Zustände bestimmter materieller Objekte Verwendung. Ein Zustand kann dabei allerdings nur dann als Informationsträger fungieren, wenn er für den Rezipienten nicht vorhersehbar ist. Wüßte dieser bereits mit absoluter Sicherheit in welchem Zustand sich ein Objekt befindet, so hätte dieses für ihn keinerlei Neuigkeitswert mehr. Ein sicherer Zustand kann daher auch keine Information repräsentieren. Anders ausgedrückt tritt Information immer nur dann auf, wenn etwas Unerwartetes wahrgenommen wird.

Das Kriterium des Neuigkeits- bzw. Überraschungswertes von Information ist zentral für die nachrichtentechnische Informationstheorie, die auf Überlegungen von Shannon (1948) sowie Shannon u. Weaver (1949) basiert. Ihr liegt eine mathematische Betrachtung von Informationsstrukturen zugrunde, welche sich des aus der Physik entlehnten Begriffs der *Entropie* bedient und diesen als stochastisches Maß der Zufälligkeit und damit Unbestimmtheit eines Elementarereignisses a versteht. Dies ist gleichbedeutend mit einer subjektiv nicht vorhersagbaren Zustandsänderung eines bestimmten Objektes. Die Wahrscheinlichkeit $P(a_i)$, mit der das i-te Element a_i der Ergebnismenge Ω auftritt, wird dabei durch Bildung des dualen Logarithmus per definitionem auf die binäre Einheit des Bit[40] bezogen, wie sie in der Wissenschaft technischer Informationsverarbeitung, der Informatik, allgemein üblich ist. Die Logarithmierung bietet den Vorteil, daß nunmehr der Informationsgehalt mehrerer Symbole additiv anstatt multiplikativ bestimmt werden kann. Der in Bit gemessene Informationsgehalt der Ausprägung $a_i \in \Omega$ mit der Wahrscheinlichkeit $P(a_i)$ berechnet sich folglich als: $I_i = -log_2\, P(a_i)$. Bildet man hierauf basierend den Erwartungswert für a, so erhält man die bekannte Shann-

40 *Bit* steht als Abkürzung für „Binary Digit“, der kleinsten Speicher- und Übertragungseinheit elektronischer Rechenanlagen. Ein Bit entspricht einem basalen Elementarereignis, dessen Ergebnismenge Ω zwei, genau gleich wahrscheinliche Elemente umfaßt.

onsche Formel:

$$H(a) = -\sum_i P(a_i) \cdot log_2\, P(a_i) \tag{3.1}$$

H entspricht dann der Informationsentropie von a. Diese ist um so höher, desto unbestimmter das Elementarereignis a ist. Bei absolut gleichmäßiger Verteilung der Wahrscheinlichkeiten auf die Elemente der Ergebnismenge Ω wird die maximale Entropie H_{max} erreicht. Daher weisen Elementarereignisse mit stark variierender Wahrscheinlichkeitsverteilung eine entsprechend geringere Entropie und damit zugleich höhere Redundanz $R = H_{max} - H$ auf. Aus nachrichtentechnischer Perspektive ist die Informationsentropie H von besonderem Interesse, weil ein als Zeichen fungierendes Elementarereignis a genau $H(a)$ Bit Informationsgehalt repräsentieren kann. Vice versa benötigt man genau $H(a)$ Bit, um umfassend über das Elementarereignis a zu informieren. Um a als Zeichen für b zu verwenden, muß also gelten: $H(a) \geq H(b)$.

3.1.4 Die pragmatische Dimension

Ob und welchen Informationsgehalt ein übermitteltes Zeichen für einen bestimmten Empfänger tatsächlich hat, hängt aus einem pragmatischen Verständnis allerdings nicht allein von dessen Neuigkeitswert ab, sondern ergibt sich vor allem aus dem spezifischen Situationskontext des Rezipienten. Besonders deutlich wird dies, wenn man bedenkt, daß eine Kette rein zufälliger Ereignisse nach der Formel 3.1 einen sehr hohen Entropie- und damit auch Informationsgehalt aufweist, für einen potentiellen Empfänger aber wohl kaum von Nutzen sein dürfte. Um in einer konkreten Situation einen praktischen Nutzwert zu entfalten, müssen Daten vielmehr handlungsrelevantes Wissen, also solches, das zur Lösung aktueller Probleme beiträgt, repräsentieren. Nur wenn sie diese Anforderung erfüllen, können sie als Information in einem Handlungskontext tatsächlich gestaltend wirken. Die Informationswissenschaft spricht daher vom „pragmatischen Primat" der Information und definiert diese plakativ als „Wissen in Aktion". Die Transformation allgemeinen Wissens in spezifische, lösungsrelevante Information führt so zur Genese informationeller Mehrwerte (Kuhlen 1995: 34 – 43).

Daß handlungsrelevantes Wissen auch (Gestaltungs-)Macht sein kann, erkannte schon Francis Bacon[41], denn der Zugriff auf relevantes Wissen zum richtigen Zeitpunkt erhöht die Chance einer erfolgreichen Interessenwahrung signifikant (vgl. Stehr

41 In den *Meditationes Sacrae* schrieb Francis Bacon 1597: „Nam et ipsa scientia potestas est."

2000: 81 ff.). Zugleich kann zu viel Wissen aufgrund eingeschränkter kognitiver Verarbeitungskapazitäten jedoch auch Orientierungslosigkeit und damit Ohnmacht bedeuten, weshalb einer situationsbezogenen Aufbereitung von Wissen als konkret handlungsrelevanter Information zentrale Bedeutung zukommt. Dies gilt umso mehr in Gesellschaften mit stark wachsendem Wissenspool, in denen Universalgelehrte, wie es noch ein Gottfried Wilhelm Leibniz war, nicht mehr vorstellbar sind. Eine verteilte Informationsverarbeitung unter Zuhilfenahme kybernetischer Technologien wird hier zur Conditio sine qua non technischer wie gesellschaftlicher Steuerungsfähigkeit (vgl. Wiener 1962; Beniger 1986; Schneider u. Kenis 1996; Stehr 2001a).

Es liegt auf der Hand, daß Information unter diesen Bedingungen für Handlungsentscheidungen in komplexen Systemen eine nicht zu vernachlässigende Ressource darstellt. Ihre essentielle Funktion besteht aus Sicht ökonomischer Entscheidungstheorien vor allem in einer Reduktion von Unsicherheit bezüglich eines für den Handlungserfolg und damit Nutzengewinn kritischen Ereignisses, dessen objektive (frequentistische) Wahrscheinlichkeitsverteilung dem Akteur unbekannt ist. Wir wollen dieses Ereignis gemäß der oben eingeführten Nomenklatur hier als B, dessen objektive Wahrscheinlichkeiten als $P(B_j)$, bezeichnen. Der Akteur verfügt aufgrund seines bisherigen Wissensstandes jedoch über eine, mehr oder weniger treffende, subjektive Vorstellung bezüglich der Wahrscheinlichkeitsverteilung von B. Diese subjektiven *A-priori*-Wahrscheinlichkeiten $P'(B_j)$ gilt es durch den Konsum einer – sich in einem Ereignis A manifestierenden – Information zu verfeinern. Die entsprechenden bedingten *A-posteriori*-Wahrscheinlichkeiten $P'(B_j|A_i)$ berechnen sich dann nach dem *Bayes-Theorem* als:

$$P'(B_j|A_i) = \frac{P'(B_j) \cdot P(A_i|B_j)}{\sum_j P'(B_j) \cdot P(A_i|B_j)} \tag{3.2}$$

Die bedingten objektiven Wahrscheinlichkeiten $P(A_i|B_j)$, auch als *Likelihood* bezeichnet, stehen hierbei für die Qualität des Informationsgehaltes von A, i. e. sie geben an, wie gut das Ereignis B durch die Kenntnis von A vorhergesagt werden kann. Je höher diese Informationsqualität ist, desto weniger fallen nach Formel 3.2 die subjektiven *A-priori*-Wahrscheinlichkeiten $P'(B_j)$ ins Gewicht, desto mehr „formt“ also A die *A-posteriori*-Wahrscheinlichkeiten und damit letztlich die Entscheidungsgrundlage für ein erfolgreiches Handeln.

Brandes et al. (1997: 323 ff.) weisen darauf hin, daß das Ausmaß der Informations-

qualität jedoch häufig eine *ex ante* ebenfalls unbekannte Größe ist. Dieser Umstand zwingt die Akteure anstelle der objektiven Wahrscheinlichkeiten $P(A_i|B_j)$ ebenfalls subjektive Wahrscheinlichkeiten $P'(A_i|B_j)$ anzunehmen. Der Prozeß des Informierens hat damit tendenziell den Charakter eines infiniten Regresses, da er selbst bereits Information bezüglich $P'(B_j)$ bzw. $P'(A_i|B_j)$ voraussetzt. Dieser Kreis läßt sich offenbar nur durch wiederholte *Ex-post*-Revision der gewonnenen Erkenntnisse und angewandten Methoden der Informationsbeschaffung – also im Wege evolutorischen Lernens – durchbrechen, weshalb Versuch und Irrtum wesentlich zu den Randbedingungen menschlicher Existenz gehören.

Dabei kann, wie bei jeder anderen Ressource auch, zunächst von einem Abnehmendem Grenznutzen der Information ausgegangen werden. Dies zumindest legt das von Kauffman (1995: 203 – 206) und anderen beschriebene Phänomen der Lernkurven nahe. Da der (Gebrauchs-)Wert der Ressource Information aufgrund ihres besonderen Charakters aber im Vorhinein oftmals nicht eindeutig feststeht, kann als Kriterium zur Bestimmung des Informationsoptimums allerdings nicht wie sonst üblich das Gleichgewicht von marginalen Kosten und marginalem Nutzen herangezogen werden. Im Mittelpunkt der Informationsökonomik steht daher seit der grundlegenden Arbeit von Stigler (1961) vor allem die Frage nach geeigneten alternativen Suchalgorithmen bzw. Abbruchkriterien der Informationsbeschaffung. Daneben ist die Frage nach dem Gutscharakter von Information ganz allgemein seit längerem Gegenstand theoretischer Diskussionen (vgl. Arrow 1969, 1974, 1979; Samuelson 1954).

3.2 Eine informationstechnische Genealogie

3.2.1 Von der Oralität zur Literalität

Weil Informationen und deren Austausch im Wege der Kommunikation zu den elementaren Voraussetzungen koordinierten Handelns gehören, sind Systeme zur Verarbeitung, Speicherung, Übertragung und Verteilung von Information seit Anbeginn Begleiterscheinungen menschlicher Zivilisation. Als gesellschaftliche Basissysteme sind sie selbstverständlich auch Gegenstand technologischer Effizienzsteigerung, weshalb sie neben Akteuren in zunehmendem Maße auch technische Artefakte umfassen. In einem Prozeß der Koevolution entwickeln sich diese sozio-technischen Systeme parallel zur Ausdifferenzierung ihrer Trägergesellschaften und bilden für deren Kultur Grundlage

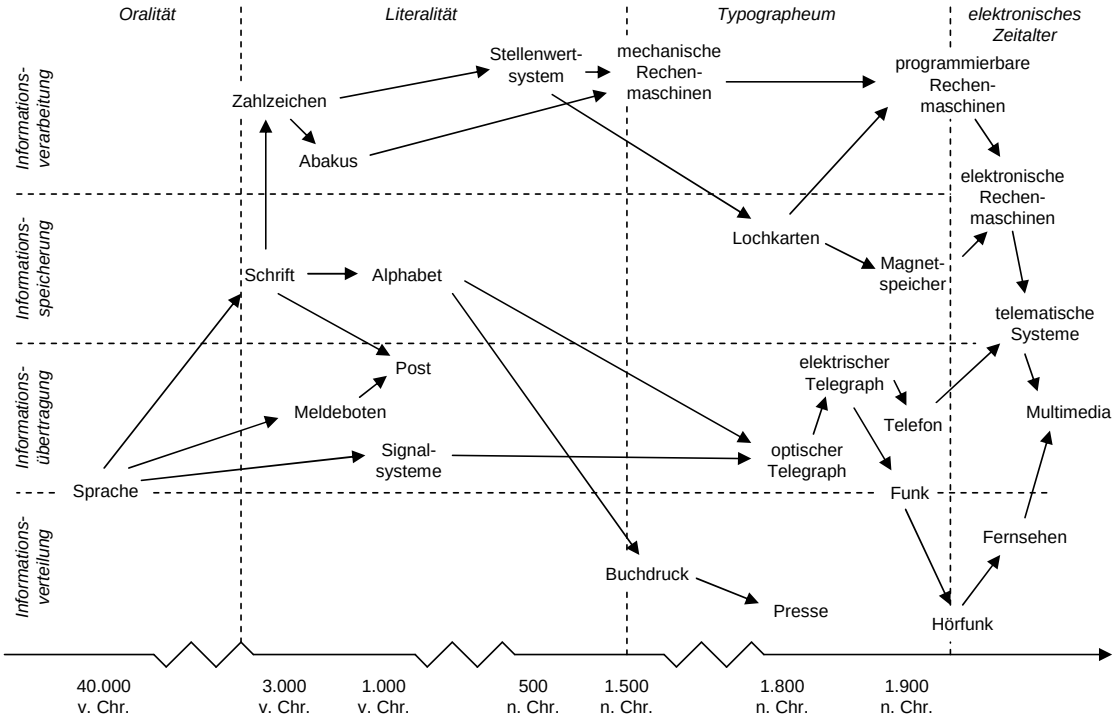


ABBILDUNG 3.1: *Divergenz und Konvergenz von Informationstechnologien*

und Implikation zugleich (Mayntz 1988b, 1995).

Im folgenden werden hier die wichtigsten technischen Entwicklungsschritte hervorgehoben (für einen groben schematischen Überblick vgl. Abbildung 3.1) und in einen evolutionsgeschichtlichen Zusammenhang gebracht. Ein ausführlicher Überblick zur Geschichte der Entwicklung sozio-technischer Kommunikationssysteme findet sich bei Schneider (1999) sowie in den Beiträgen des Sammelbandes von Teuteberg u. Neutsch (1998), eine umfangreiche Beschreibung der historischen Entstehung von Systemen der Informationsverarbeitung u. a. bei Williams (1997) und Ceruzzi (2000). Zu den Details der geschichtlichen Entwicklung der Konvergenztechnologie des Internet aus technisch-historischer Sicht sei Abbate (1999b), aus institutioneller Perspektive Werle (1999) und Leib (2002) empfohlen. Broß u. Garbes (2006) schließlich befassen sich mit den Folgen digitaler Konvergenz.

Der bedeutendste, die Hominisation vermutlich erst auslösende Meilenstein in der Geschichte menschlicher Kommunikation ist ohne Zweifel die Entwicklung des akustischen Zeichensystems der Sprache vor über 40.000 Jahren. Schon für Aristoteles unterschied bekanntermaßen der Gebrauch derselben den Menschen vom Tier, denn

Sprache ermöglicht die begriffliche Abstraktion vom Konkreten und damit eine vorausschauende und vernunftmäßige Planung und Koordination des Handelns. Sprache fördert Arbeitsteilung in der Gemeinschaft und vereinfacht wesentlich die horizontale (interpersonale) Weitergabe von Fähigkeiten und Wissen im Gegensatz zu deren bloß genetischer Vererbung. Die evolutionären Mechanismen der Variation und Retention entfalten so eine weit effektivere Wirksamkeit, als dies im Tierreich möglich ist. Die Erfindung der Sprache zählt daher zu den auslösenden Momenten einer – bis heute anhaltenden – exponentiellen Vervielfachung menschlicher Fähigkeiten.

Direkte mündliche Verständigung blieb für Jahrtausende die wichtigste Kommunikationsform und ist es in primitiven Gesellschaften teilweise noch heute.[42] Eine weitere, bahnbrechende Neuerung brachte erst die Einführung eines ausdifferenzierten optischen Zeichensystems, das nicht nur zur unmittelbaren Weitergabe von Informationen, sondern auch zu deren längerfristiger Speicherung und mediatisierten Übertragung geeignet war. Die bisher ältesten Anzeichen für eine, über sakrale Höhlenmalereien hinausgehende Schrift mit praktischem Gebrauchswert finden sich auf Tontafeln, die bei archäologischen Ausgrabungen in der Gegend der frühzeitlichen Stadt Uruk entdeckt und auf das Ende des vierten Jahrtausends v. Chr. datiert wurden. Diese frühe Keilschrift revolutionierte nach Nissen et al. (2004) im Laufe ihrer weiteren Perfektionierung Buchhaltung und Ressourcenverwaltung in den Stadtstaaten Mesopotamiens und schuf so eine wesentliche Voraussetzung für die Entstehung des ersten sumerischen Flächenstaates etwa eintausend Jahre später.

Die Technik der schriftlichen Fixierung von Information entstand offenbar als Form der nicht-mentalen Wissensaufbewahrung im Umfeld der Verwaltung größerer Ressourcenansammlungen, wie sie sich bspw. in Tempelanlagen oder an Fürstenhöfen fanden. Vermutlich waren die ersten Schriftzeichen, wie etwa altägyptische Hieroglyphen, zunächst nur eine direkte bildlich-analoge Darstellung des Gemeinten. Durch entsprechende Wiederholung der Symbole wurden die zu verwaltenden Ressourcen 1:1 aufgelistet, um so einen besseren Überblick zu erhalten. Im Falle großer darzustellender Mengen liegt dann die Verwendung besonderer Abkürzungen und damit die Entwicklung von Zahlzeichen nahe, womit zugleich ein erster Abstraktionsschritt erfolgt und eine rechne-

42 Vermutlich wurde diese zur Überwindung größerer Distanzen vereinzelt um Rauch- und Feuerzeichen sowie Horn-, Pfeifen- oder Trommelsignale ergänzt. Allerdings sind solche rudimentären Signalsysteme aufgrund ihres stark eingeschränkten Zeichensatzes bestenfalls zur Übermittlung einfachster Nachrichten geeignet.

rische Verarbeitung von Information, mithin die deduktive Gewinnung neuer Information, in besonderer Weise begünstigt wird. Weil Information hierbei erstmals in Form diskreter Symbole kodiert wird, deren Inhalt sich nicht mehr unmittelbar aus ihrer bildlichen Analogie erschließt, handelt es sich faktisch zugleich um eine Art frühzeitlicher Digitalisierung von Wissen, deren Entzifferung nun ihrerseits bestimmte Vorkenntnisse voraussetzt, also einer gewissen Intelligenz bedarf. Additive Zahlensysteme und einfache technische Artefakte wie der Abakus sind in diesem Stadium typische Instrumente der Informationsverarbeitung.

Gesellschaftlich eröffnen sich durch die Erfindung von Schrift und Zahlen eine Reihe neuer Entwicklungspotentiale. So erlauben etwa astronomische Berechnungen eine genauere Bestimmung der kalendarischen Jahreszeiten und somit die Optimierung von Aussaat und Ernte sowie die Einrichtung einer zentralisierten Vorratsverwaltung. Die schwierige Erlernbarkeit früher Schriftformen beschränkte deren Anwendung jedoch zugleich auf eine kleine Klasse hauptberuflicher Priester und Schreiber, die so zur ersten Beamtenelite der Geschichte aufsteigen und durch eine Monopolisierung von Wissen bedeutende Macht erlangen konnte. Auf der Grundlage ihrer Planung entstanden kulturelle Höchstleistungen wie die monumentalen Bauwerke der Pyramiden und Zikkurate, aber auch erste Bewässerungssysteme. Nicht zuletzt Wittfogel (1962) verortete ja die Entstehung früher Staatlichkeit in diesem Kontext.

Einen bedeutenden Entwicklungssprung stellt zweifellos auch die Koppelung einzelner Schriftzeichen an die Phoneme der Sprache dar, weil sie, im Gegensatz zu piktographischen Schriftsystemen, trotz eines minimalen Zeichensatzes eine schriftliche Fixierung von Sprache in der gesamten Breite ihrer begrifflichen Differenzierung und Abstraktionstiefe zuläßt. Dies geschah wohl erstmalig im phönizischen Alphabet und wurde sehr bald von Griechen, Römern und anderen Kulturvölkern übernommen. Erst die hieraus resultierende Vereinfachung der Erlern- und Anwendbarkeit von Schrift macht die kulturelle Blüte eines Bildungsbürgertums, wie sie uns aus der klassischen Antike vertraut ist, überhaupt denkbar. Die Diffusion von Information wurde in der Folge nicht mehr hauptsächlich durch die Komplexität der Schrift, sondern vielmehr durch die technischen Möglichkeiten ihrer Vervielfältigung beschränkt.

Auf dem Gebiet der Informationsübertragung ermöglichte die Erfindung der Schrift neue Formen indirekter (Tele-)Kommunikation. Schriftlich überbrachte Nachrichten können umfangreicher als mündliche Botschaften ausfallen und lassen sich, bspw. mittels eines Siegels, leichter authentifizieren. Bereits die Großreiche der Antike hatten

daher umfangreiche Boten- und Meldesysteme etabliert, die einen Austausch von Depeschen über weite Distanzen hinweg ermöglichten. Das bekannteste und am besten dokumentierte dieser Nachrichtensysteme ist wohl der *cursus publicus* des römischen Kaiserreichs (vgl. Riepl 1913; Kolb 2000). Diese Systeme waren jedoch der Allgemeinheit nicht zugänglich, sondern blieben Verwaltung und Militär vorbehalten. Ein großer Nachteil lag in ihrer vergleichsweise geringen Übertragungsgeschwindigkeit, die vor allem in der „Geschwindigkeit der schnellsten Transportmittel" (Schneider 1999: 55) an ihre Grenzen stieß. Unter diesen Bedingungen stellte der Ausbau eines infrastrukturellen Netzes von Relaisstationen zur Versorgung von Stafettenkurieren über Jahrhunderte das Optimum der Nachrichtentechnik dar.

Vermutlich im Laufe des fünften Jahrhunderts n. Chr. ergab sich im Bereich der Informationsverarbeitung eine weitere, nicht minder bedeutsame Neuerung: Die Entwicklung eines durchgehend positionalen Zahlensystems, welches das bisher gebräuchliche Additionssystem zu verdrängen begann. Möglich wurde diese Innovation durch die Einführung der Ziffer Null im indischen Kulturraum. Nach Williams (1997) hatte es zwar bereits im Altertum vereinzelte Ansätze rudimentärer Positionssysteme gegeben, so etwa in Babylon um 200 v. Chr.; allerdings wurde in diesen Varianten das funktional der Null entsprechende Zeichen lediglich als Platzhalter und nicht als eigenständige Ziffer aufgefaßt und daher bei schließenden Nullstellen, wie sie etwa bei der Zahl 1.000 auftreten, nicht konsequent verwandt. Daß es sich bei der Null um eine eigenständige Zahl handeln könnte, rückte offenbar erst im kulturellen Kontext einer buddhistisch inspirierten Vorstellung vom absoluten Nichts in den Bereich des Denkbaren.

3.2.2 Vom Typographeum zum elektronischen Zeitalter

Ein auf dieser Neuerung basierendes Stellenwertsystem aber erlaubt nicht nur die Darstellung nahezu beliebig großer Zahlen mittels nur weniger Ziffern, sondern vereinfacht vor allem die Arithmetik in bedeutendem Maße. Ohne ein solches positionales System wäre die Entwicklung erster mechanischer Rechenmaschinen durch Wilhelm Schickard 1623, Blaise Pascal 1642 und Gottfried Wilhelm Leibniz 1672 kaum vorstellbar gewesen. Im 19. Jahrhundert entwarf dann schließlich der britische Mathematiker und Philosoph Charles Babbage auf Grundlage dieser Vorarbeiten und unter dem Eindruck der industriellen Revolution Pläne für eine dampfgetriebene Rechenmaschine, die – parallel zu den damals verbreiteten Webstühlen – erstmals mit Lochkarten programmgesteuert

und damit zur automatisierten Berechnung mathematischer Funktionen geeignet sein sollte, aus Geldmangel allerdings nie zur Konstruktion gelangte.

Auf dem Weg dorthin sollte aber zunächst die Erfindung des Buchdrucks durch Johannes Gutenberg Mitte des 15. Jahrhunderts das Problem der Vervielfältigung schriftlicher Informationen in eleganter Weise lösen und damit wesentlich zur Diffusion von Wissen beitragen.[43] In der Folge erleichterten gedruckte Massenpublikationen breiten Gesellschaftsschichten den Zugang zu Information, was tiefgreifende gesellschaftliche Veränderungen im Zeichen der Aufklärung nach sich zog (vgl. McLuhan 1962). Ein größerer Durchbruch ergab sich ferner in der Telekommunikationstechnik Ende des 18. Jahrhunderts, als die Erfindung des optischen Flügeltelegraphen durch die Gebrüder Chappe erstmals die Übermittlung von Nachrichten in nur wenigen Stunden auch über große Distanzen hinweg ermöglichte (Beyrer 1998).[44]

Im 19. Jahrhundert löste das Aufkommen der Elektrotechnik als neuer Basistechnologie dann einen weiteren Entwicklungsschub in fast allen Bereichen der Informationstechnik aus. Das Phänomen der Elektrizität bzw. elektrostatischen Aufladung war zwar bereits in der Antike bekannt, wurde aber erst im Laufe des 18. und 19. Jahrhunderts durch eine Reihe bedeutender Erfindungen technisch beherrsch- und nutzbar. Angesichts dieser Fortschritte war die Konstruktion eines elektrischen Telegraphen nurmehr eine Frage der Zeit (vgl. Reindl 1998). Die elektrische Telegraphie sollte sich der optischen dabei in zweifacher Weise überlegen erweisen: Zum einen ist sie unabhängig von den auf Witterung, Tageszeit und Krümmung der Erdoberfläche beruhenden Sichtbedingungen; zum anderen wurde neben einer nochmaligen Steigerung der Übertragungsgeschwindigkeit durch eine bedeutende Reduktion und zunehmende Automatisierung der Relaisstationen auch die Ausschaltung einer Vielzahl fehlerträchtiger Mensch-Maschine-Schnittstellen und damit eine verbesserte Zuverlässigkeit des Gesamtsystems erreicht (Schneider 1999). Letztlich konnten nur so auch interkontinentale Distanzen überwunden werden.

Trotz des gewaltigen Fortschritts bei der Übermittlung von Information hatte aber

43 Dies gilt zumindest für den europäischen Kulturraum. In Asien wurde die Technik des Buchdrucks bereits sehr viel früher, so etwa in China seit dem 9. und in Japan seit dem 11. Jahrhundert, angewandt (Mitterauer 1998).

44 Zwar berichtet schon Homer in der Ilias von Feuerzeichen und anderen optischen Signalsystemen der Griechen (Riepl 1913), allerdings waren diese in ihrem Zeichensatz äußerst eingeschränkt und daher zur Übermittlung komplexer Nachrichten kaum geeignet.

auch die Telegraphie noch einen schwerwiegenden Nachteil, den seit der Erfindung der ersten Schriftsysteme – mit Ausnahme mündlicher Meldesysteme – eigentlich alle Informationstechniken geerbt hatten: Ihre Anwendung war mit dem Erlernen eines spezifischen, digitalen Zeichencodes verbunden, weshalb die Bedienung des optischen wie elektrischen Telegraphen durch besonders spezialisiertes Fachpersonal erfolgen mußte. Zudem blieb die Übertragungskapazität, gemessen am Durchsatz des Informationsgehaltes je Zeiteinheit, durch die jeweils notwendige und von Menschen zu versehende Kodierung/Dekodierung stark eingeschränkt. Erst die, durch die Erfindung des Telefons mögliche gewordene, analoge Übertragung akustischer Schallwellen vereinfachte die Anwendung der Telekommunikationstechnologie unter ergonomischen Gesichtspunkten soweit, daß eine engmaschige kommunikationstechnische Vernetzung und damit zugleich ein bisher unbekanntes Maß sozialer Konnektivität erreicht werden konnte.

Die Entwicklung der Funktechnik ließ ab Anfang des 19. Jahrhunderts eine drahtlose Übermittlung von Sprache auch auf weite Entfernungen zu, wodurch neben der Punkt-zu-Punkt-Kommunikation des Telefons prinzipiell auch eine Punkt-zu-Multipunkt-Kommunikation realisierbar wurde. Mit dem Aufkommen der Massenmedien des Hörfunks und Fernsehens können analoge auditive und visuelle Informationen nun erstmals in Echtzeit Distanzen überwinden, die einem vielfachen der Ruf- und Sehweite entsprechen und dabei ein nahezu beliebig großes Publikum erreichen. Hörfunk und Fernsehen sind so in der Lage im Rahmen einer zeitnahen Informationsdiffusion breite Bevölkerungskreise zu durchdringen und über unterschiedlichste Gesellschaftsschichten hinweg eine integrative Wirkung zu entfalten, indem sie einen gemeinsamen Informationshorizont vermitteln. Problematisch ist hierbei jedoch vor allem die Asymmetrie der zugrundeliegenden 1:n-Kommunikation, die lediglich einen einseitig gerichteten Informationsfluß ohne Rückkanal zuläßt.

Die technischen Neuerungen der elektromagnetischen Informationsübertragung und -verbreitung machten allerdings zugleich auch die Entwicklung neuer Technologien der Informationsspeicherung erforderlich, da durch elektromagnetische Wellen oder Spannungen repräsentierte Information per se flüchtig ist. Eine bereits gängige Form der Informationsspeicherung war die Lochkarte, die schon während der Industriealisierung zur Steuerung automatischer Webstühle eingesetzt worden war und sich als digitales Trägermedium problemlos mit dem elektrischen Telegraphen kombinieren ließ. Zur Aufzeichnung und Wiedergabe analoger Informationen war sie jedoch gänzlich ungeeignet. Die Entwicklung von Phonograph, Grammophon und später magnetischen Speicher-

medien kann vor diesem Hintergrund als Reaktion auf die besondere Herausforderung der Aufbewahrung analoger Information gesehen werden (vgl. auch Wersig 2000).

Wir wollen den Blick an dieser Stelle noch einmal auf die bis dahin weitgehend isoliert verlaufende Entwicklung von Technologien der Informationsverarbeitung lenken. Wie oben bereits angedeutet ist Informationsverarbeitung vor allem als Prozeß der deduktiven Gewinnung neuer Information aus bereits vorhandener zu verstehen, was keinesfalls mit einem Zugewinn an Wissen gleichzusetzen ist. Da es sich bei der Verarbeitung von Information also letztlich um eine Abbildung bestehender auf neue Symbolstrukturen handelt, kann diese auch als mathematische Funktion umschrieben werden. Insofern sich Information digital – also diskret – symbolisieren läßt, kann sie dann ebenfalls in Zahlen codiert und folglich rechnerisch verarbeitet werden.[45]

Im Kontext einer umkehrbaren Zuordnung von Zahlen zu Informationsinhalten ist hier insbesondere ein von Kurt Gödel erstmals beschriebener und daher nach ihm benannter mathematischer Isomorphismus von herausgehobener Bedeutung. Die Frage der Verarbeitung von Information ist damit vor allem eine Frage der Verfügbarkeit leistungsfähiger Rechentechnologien sowie geeigneter Verfahren bzw. Algorithmen zur Abbildung berechenbarer Funktionen der Informationstransformation. Bereits 1937 hatte Alan M. Turing das mathematisch-formale Modell eines universellen Rechenautomaten entwickelt (Turing 1937). Dieser sollte, gemäß einer von Alonzo Church und Turing formulierten und heute weitgehend unbestrittenen, letztlich aber nicht beweisbaren These auf die Klasse aller berechenbaren Funktionen anwendbar sein. Diese Turing-Maschine legte die theoretische Grundlage für jene automatisierte Verarbeitung von Information, die heute allgemein als Informatik bezeichnet wird.

Ab 1936 arbeitete in Berlin Konrad Zuse an der Entwicklung eines elektromechanischen Rechenautomaten, der im Gegensatz zu den üblicherweise gebräuchlichen Tischrechnern der einfacheren Realisierbarkeit halber auf dem Dual- anstelle des Dezimalsystems beruhen und wie die Rechenmaschine von Charles Babbage programmgesteuert sein sollte. Im Jahr 1941 schaffte Zuse mit einem Nachfolgemodell den Durchbruch zur Konstruktion des ersten voll funktionsfähigen, frei programmierbaren Rechenautomaten, den er dann später „Z3“ taufte. Nach Williams (1997) lassen sich neben den von

45 Prinzipiell sind zwar auch analoge – bspw. auf kontinuierlichen Spannungsschwankungen basierende – Rechenmaschinen denkbar, allerdings stoßen diese, vor dem heutigen Stand der Technik, hinsichtlich ihrer Genauigkeit sehr schnell an ihre Grenzen, so daß sich das digitale Prinzip in der Rechnertechnologie weitgehend durchgesetzt hat (vgl. Williams 1997).

Zuse gebauten Maschinen noch mindestens drei weitere Entwicklungslinien ähnlicher Rechenautomaten ausmachen, die Ende der 1930er Jahre in etwa zeitgleich bei den Bell Thelephone Laboratories, bei International Business Machines (IBM) sowie von Howard Aiken in Harvard entwickelt wurden.

Der Ausbruch des zweiten Weltkrieges isolierte zwar einerseits die Entwicklungen des Deutschen Konrad Zuse von denen auf Seiten der Alliierten, führte aber andererseits auch zu intensivierten Innovationsbemühungen auf beiden Seiten. Besonders die Briten waren zur Entschlüsselung der deutschen Chiffriermaschine „Enigma“ an der Entwicklung von Anlagen mit enormer Rechenleistung interessiert. Diese stellte ab 1943 ein Großrechner von gigantischem Ausmaß unter dem bezeichnenden Decknamen „Colossus“ zur Verfügung, der ausschließlich auf Elektronenröhren basierte und daher als erster elektronischer Rechner der Welt gilt. Colossus operierte, wie von nun an fast alle Rechner, ebenfalls auf binärer Basis. Im Gegensatz zur Z3 konnte er neben den Daten auch das Programm selbst im Hauptspeicher aufnehmen.

Die Computertechnologie insgesamt ist in der Frühphase offenbar stark durch ihr militärisches Nutzenpotential dominiert (vgl. Werle 1999). Dies hat seine Ursache zum einen in der spezifischen Kostenstruktur, die Anschaffung und Unterhalt aufgrund teurer Komponenten, einer hohen Leistungsaufnahme sowie eines enormen Platzbedarfs privat kaum finanzierbar machte. Zum anderen ist eine schnelle Informationsgewinnung, -verarbeitung und -verteilung gerade in der Kriegsführung von beachtlichem strategischen Nutzen, weshalb ein möglichst hoher Vernetzungsgrad der eigenen Truppen (*Network Centric Warfare*) sowie deren Informationsüberlegenheit (*Information Warfare*) im Zentrum jeder modernen Militärdoktrin stehen (vgl. Arquilla u. Ronfeldt 1996; Molander et al. 1996; Libicki 2007).

Die neue Rechnertechnologie wurde nur langsam von zivilen Einrichtungen adaptiert. Ein wesentlicher Schritt war die Entwicklung des *Time-Sharing* 1957, das den parallelen Zugang mehrerer Nutzer zu einem Großrechner ermöglichte und so dessen Auslastung und damit Wirtschaftlichkeit deutlich verbesserte. Die Bedienung erfolgte durch Terminals, die über eine Standleitung mit einem Rechenzentrum verbunden waren. Diese, zumeist nur aus einem Bildschirm und/oder Drucker sowie einer Tastatur bestehenden, alphanumerischen Ein- und Ausgabegeräte eröffneten, im Gegensatz zur bis dahin üblichen sequentiellen Stapelverarbeitung, eine interaktive Schnittstelle zwischen Mensch und Maschine. In den 1960er Jahren waren Rechenzentren aufgrund dieser Neuerungen bereits in der öffentlichen Verwaltung, an Hochschulen und in Großun-

ternehmen anzutreffen. Daß ein derart zentralisiertes technisches System eine extrem hohe Verwundbarkeit aufweist, bedarf hier keiner weiteren Ausführung. Tatsächlich waren es wiederum militärisch-sicherheitspolitische Erwägungen, die Ende der 1960er Jahre den Anstoß zu einer weiteren technischen Errungenschaft gaben, die schließlich den Weg für eine verteilte Netztopologie ebnen sollte.

3.2.3 Ein Netz aus Netzwerken entsteht

Im Jahr 1958 war, unter dem Eindruck der sowjetischen Erfolge in der Militär- und Raumfahrttechnik,[46] im Verantwortungsbereich des US-Verteidigungsministeriums die Advanced Research Projects Agency (ARPA)[47] gegründet worden. ARPA sollte den Vereinigten Staaten durch eine gezielte Koordination und Förderung von Forschungsprojekten erneut zu technologischer Führung verhelfen und diese nach Möglichkeit dauerhaft ausbauen. Zu diesem Zweck wurde eine Reihe von Projekten finanziert, die sich auf verschiedene Universitäten und Forschungseinrichtungen in den USA verteilten. Mitte der 1960er Jahre stand man bei ARPA schließlich vor der Herausforderung, diese über das ganze Land verstreuten Projekte informationstechnisch zuverlässig so zu vernetzen, daß ein gemeinsamer Zugriff auf Informationsressourcen möglich wurde. Nicht zuletzt wegen der hohen Kosten einer herkömmlichen Datenübertragung im Telefonnetz sollte diese Aufgabe ein neues, ARPANET genanntes Netzwerk übernehmen, gestützt auf die spezielle Technologie des *Packet-Switching*. Im Jahr 1971 umfaßte das ARPANET fünfzehn Knoten, unter ihnen SRI, RAND Corporation, UCLA, Stanford, Harvard, das MIT sowie die Carnegie Mellon University. Ein Jahr später wurde das neue Netzwerk dann offiziell auf der Internationalen Konferenz für Computerkommunikation in Washington vorgestellt (vgl. Abbate 1999b).

Die Technik des *Packet-Switching* geht im Wesentlichen auf die Arbeiten von Paul Baran und Donald Watts Davies zurück. Baran hatte bei RAND an einem Kommunikationssystem gearbeitet, das auch im Falle schwerster Schäden weitgehend ausfallsicher sein sollte. Vor allem die US Air Force war, hinsichtlich der Aufrechterhaltung ihrer

46 Ein Jahr zuvor hatte die Sowjetunion mit dem erfolgreichen Start des *Sputnik 1* überraschend das Wettrennen um den ersten künstlichen Satelliten in einer Erdumlaufbahn gewonnen. In den USA löste dieser unerwartete technische Vorsprung Bedrohungsängste aus und führte u. a. zur Gründung der National Aeronautics and Space Administration (NASA).

47 ARPA wurde zwischenzeitlich in Defense Advanced Research Projects Agency (DARPA) umbenannt.

Kommandostruktur im Falle eines Atomkrieges, an einem solchen System interessiert. Barans Konzept sah ein verteiltes, dezentrales Kommunikationsnetz auf Basis eines paketorientierten Vermittlungsverfahrens vor. Ähnliche Gedanken entwickelte etwa zur selben Zeit Davies am National Physical Laboratory in England und auch in Frankreich und Deutschland beschäftigten sich verschiedene Forschungseinrichtungen mit paketvermittelten Netzen. Ein paketvermitteltes Verfahren fragmentiert, im Unterschied zum herkömmlichen *Circuit-Switching*, bei dem eine durchgehende Übertragungsleitung geschaltet wird, die zu übermittelnden Daten in einzelne Pakete (*Datagramme*), die dann unabhängig voneinander von Knoten zu Knoten durch ein teilvermaschtes Netzwerk weitergereicht werden. Ein solches Verfahren gewährleistet eine weitgehende Ausfallsicherheit, da die einzelnen Pakete i. d. R. über alternative Wege zum Ziel gelangen können. Gleichzeitig kommt das *Packet-Switching* aufgrund einer dezentralen Netzwerktopologie ohne die potentielle Schwachstelle einer zentralen Steuerungsinstanz aus. Zudem steht ein und derselbe Übertragungskanal für mehrere Kommunikationsverbindungen zur selben Zeit zur Verfügung, wodurch ein optimaler Auslastungsgrad der Übertragungskapazitäten im Netzwerk erreicht wird (Baran 1964).

Weil ein paketvermitteltes Verfahren der Informationsübermittlung auf einer Fragmentierung der Daten beruht, ist es jedoch nur im Umfeld digitaler Information vorstellbar. Nur diskrete Daten lassen sich in Datagramme partitioniert verschicken, wohingegen die Übermittlung analoger Daten einen kontinuierlichen Verbindungskanal voraussetzt. Ferner bedarf ein paketorientiertes Verfahren einer intelligenten Weiterleitung der Datagramme an den zu durchlaufenden Vermittlungsstellen, bedingt also die Fähigkeit zur automatisierten Datenverarbeitung. Die einzelnen Netzknoten müssen in der Lage sein, die Adressierung der Datagramme auszulesen und diese mit ihren jeweils lokal gespeicherten Informationen zur Topologie des Netzwerkes derart zu verknüpfen, daß eine sinnvolle Entscheidung über die Weiterleitung der Pakete möglich wird. Auch müssen die Datenpakete ggf. zwischengespeichert und beim Empfänger schließlich wieder in ihrer ursprünglichen Reihenfolge zusammengesetzt werden können. *Packet-Switching* setzt daher verteilte Intelligenz voraus und ist nur im Kontext einer Konvergenz von Technologien der Informationsübertragung und -verarbeitung auf digitaler Basis denkbar.

Genau diese Konvergenz von Informations- und Kommunikationstechniken ist kennzeichnend für die nun folgende Dekade. Fortschritte in der Mikroelektronik, vor allem im Transistor- und Halbleiterbau sowie bei der Integration elektronischer Schaltkreise

(vgl. Noyce 1980), hatten Größe und Herstellungskosten von Computern inzwischen deutlich reduziert,[48] und damit deren Diffusion begünstigt. Die automatische Steuerung von Prozessen, nach Wiener (1962) auch als Kybernetik bezeichnet, wurde zum vorherrschenden Paradigma in Technik und Wissenschaft. Die fortschreitende Automatisierung der Produktionsprozesse selbst wiederum erhöhte die Produktivität nachhaltig und verstärkte im Wege positiver Rückkopplungseffekte die Spirale sinkender Elektronikpreise zusätzlich. Eine umfassende Vernetzung von Rechnern, die letztlich in einer Verschmelzung von Informations- und Kommunikationstechnologien kulminierte, schien logische Folge dieser Entwicklung zu sein, die nun auch in ihrer wirtschafts- und gesellschaftspolitischen Dimension als Umbruch, Herausforderung und Chance begriffen wurde. So beschäftigte man sich zum Ende des Jahrzehnts etwa in Frankreich verstärkt unter industriepolitischen Gesichtspunkten mit der „Informatisierung der Gesellschaft“ (Nora u. Minc 1979) und prägte dabei den Begriff der „Telematik“[49].

Bei ARPA entwickelte man inzwischen eine neue Generation paketvermittelter Netzwerke. Aufgrund militärischer Erfordernisse sollten sich diese u. a. zur Datenübertragung via Funk und Satellit eignen. An der Universität von Hawaii[50] wurde hierzu das *Alohanet* konzipiert, das Robert Metcalfe[51] dann Mitte der 1970er zum *Ethernet* weiterentwickelte. Bei der Ethernet-Technologie kommunizieren mehrere Teilnehmer über einen gemeinsamen Kanal, im Falle eines funkbasierten Netzes den „Äther“ – daher der Name, wobei keine Mechanismen zentraler Koordination vorgesehen sind. Versuchen

48 Gordon E. Moore publizierte 1965 die Annahme, daß sich die Dichte der Transistoren in integrierten Schaltkreisen, mithin deren Rechenleistung und Speicherkapazität, etwa alle 24 Monate verdopple, während die Herstellungskosten im selben Maße zurückgingen (Moore 1965); eine offenbar weitgehend zutreffende Beobachtung, die seitdem auch als „Mooresches Gesetz“ bekannt ist.

49 Simon Nora und Alain Minc verwendeten in ihrem 1978 im Auftrag des französischen Staatspräsidenten verfaßten Bericht *L'informatisation de la société* erstmalig den Begriff *télématique*. Diese Wortschöpfung, zu deutsch „Telematik“, setzt sich aus den Begriffen „Telekommunikation“, „Automation“ und „Informatik“ zusammen.

50 Die Institute der University of Hawaii sind über verschiedene Inseln verstreut. Daher erschien hier eine Funkverbindung besonders nützlich.

51 Metcalfe gilt als Vater des „Metcalfeschen Gesetzes“, demzufolge der Nutzen eines Netzwerkes im Quadrat zur Anzahl seiner Knoten ansteigt, weil insgesamt mehr Ressourcen zur Verfügung stehen. So sind bei n Teilnehmern $\frac{n\cdot(n-1)}{2}$ potentielle Verbindungen denkbar. Es ist unmittelbar einsichtig, daß dieser Term bei hohen Werten für n gegen $n^2 : 2$ tendiert. Der Grundgedanke des Metcalfeschen Gesetzes findet in der sozialwissenschaftlichen Literatur unter dem Begriff der (positiven) Netzwerkexternalitäten Beachtung (vgl. etwa Schneider 1989; Liebowitz u. Margolis 1995).

zwei oder mehr Teilnehmer zur gleichen Zeit zu senden, kommt es zu einer Signalkollision und dem Verlust der gesendeten Daten. Um dennoch sicherzustellen, daß alle Daten ihr Ziel erreichen, wartet der Sender jeweils auf deren Quittierung durch den Empfänger. Erfolgt diese nicht innerhalb eines bestimmten Zeitrahmens, so werden die Daten erneut versandt, wobei eine zufällige Zeitverzögerung vorgeschaltet ist, um eine dauerhafte gegenseitige Blockade zu verhindern. Das Ethernet hat damit de facto eine sternförmige Netztopologie, deren logischen Mittelpunkt das Übertragungsmedium, welches selbstverständlich auch ein Kabel sein kann, bildet.

Nach der erfolgreichen Inbetriebnahme funk- und satellitengestützter Kommunikationsnetze verfügte ARPA Anfang der 1970er Jahre über eine Reihe heterogener Netzwerkarchitekturen, die es untereinander in Form eines netzwerkübergreifenden Netzes von Netzen zu verknüpfen galt. Die Idee des „Internet“[52] war geboren, wenngleich diese Bezeichnung erst Anfang der 1980er Jahre allgemein üblich wurde. Bis dahin sprach man u. a. von „Virtual Network“, „Multinetwork Environment“ oder „Concatenated Network“. Im Auftrag von ARPA begannen Robert Kahn und Vinton Cerf 1973 im Hinblick auf ein solches „Metanetz“ mit der Entwicklung eines, zur nahtlosen Datenübertragung zwischen heterogenen Netzwerken geeigneten, neuen Protokolls[53]. Um eine möglichst breite Akzeptanz und Kompatibilität dieses neuen Übertragungsprotokolls zu erreichen, stellten Kahn und Cerf ihre Überlegungen zunächst im Rahmen der International Network Working Group (INWG)[54] vor einem globalen Expertenpublikum zur Diskussion. Ziel war ein Standard, der eine weltumspannende Vernetzung bereits bestehender, lokaler Netzwerke ermöglichte. Am Ende des nun folgenden Diskussionsprozesses stand schließlich die Spezifikation eines – *Transmission Control Protocol* (TCP) genannten – offenen Übertragungsprotokolls, das eine Ende-zu-Ende-Verbindung zweier *Hosts*[55] über verschiedene Netze hinweg erlaubt (Salus 1995; Abbate 1999b).

Die einzelnen lokalen Netze werden dabei über *Gateways*[56] untereinander verbun-

52 Die Bezeichnung „Internet“ entstand als Kontamination für „Interconnected Networks“.

53 Ein Übertragungsprotokoll spezifiziert die genauen Modalitäten des Datenaustauschs zwischen mehreren Computern.

54 Die INWG wurde auf der Internationalen Konferenz für Computerkommunikation 1972 gegründet und schloß sich bald darauf der International Federation for Information Processing (IFIP) an.

55 Als Host werden Rechner bezeichnet, die als Server fungieren, d. h. in einem Netzwerk dauerhaft Ressourcen zur Verfügung stellen.

56 Als Gateway werden Rechner bezeichnet, die an zwei oder mehr Netze zugleich angeschlossen sind.

den und konstituieren in ihrer Gesamtheit das Internet. Um die Engpaßstellen der Gateways von den Aufgaben der eigentlichen Verbindungssicherung zu entlasten, wurde TCP bereits sehr früh um ein zusätzliches – *Internet Protocol* (IP) genanntes – Protokoll erweitert. Während letzteres für Weiterleitung (*Routing*) und Umwandlung der Datagramme in das jeweilige, netzwerkspezifische Format zuständig ist und daher sowohl auf Hosts als auch Gateways laufen muß, setzt TCP auf IP auf und übernimmt die Gewährleistung einer verläßlichen Ende-zu-Ende-Verbindung, wird also nur auf den Hosts selbst benötigt. Auf TCP/IP wiederum basieren dann weitere Protokolle, die bestimmte Funktionalitäten – sog. Dienste – wie bspw. die Übertragung von Dateien (FTP), den Austausch von Nachrichten (SMTP) oder die Emulation eines Terminals (Telnet) bereitstellen (Kubicek 1997).

Um die Kommunikation zwischen heterogenen Systemarchitekturen zu erleichtern, werden die bei einer Datenübertragung im Netzwerk anfallenden technischen Aufgaben üblicher Weise in funktionale Schichten unterteilt, die aufeinander aufbauen. Diese Schichten wurden von der International Organization for Standardization (ISO) Ende der 1970er Jahre im Rahmen des „Open Systems Interconnection Reference Model“ wie folgt standardisiert (vgl. Fuhrberg et al. 2001: 7 f.): (1) physische Bitübertragung, (2) Sicherstellung einer fehlerfreien Verbindung, (3) Paketvermittlung, (4) Sicherstellung des Datentransportes im Rahmen einer Ende-zu-Ende-Verbindung, (5) Sitzungsverwaltung, (6) Darstellung rechnerunabhängiger Datenformate, (7) Anwendung. Die Schichten eins bis drei sind hardwarenah, vier bis sieben hingegen anwendungsbezogen. Im Falle von TCP/IP entsprechen die erste und zweite Schicht dem lokalen Netzwerk (bspw. Ethernet), während die dritte das IP-Protokoll umfaßt. Schicht vier ist dann das TCP-Protokoll und fünf bis sieben die jeweilige Anwendung.

Im Jahr 1975 war die experimentelle Phase des ARPANET weitgehend abgeschlossen. Es wurde nun verstärkt zur Vernetzung militärischer Einrichtungen herangezogen und bis 1983 komplett auf das TCP/IP-Protokoll umgestellt. Schließlich wurde 1983 aus Gründen der Sicherheit und Geheimhaltung der militärisch genutzte Teil als MILNET gänzlich ausgegliedert, während das restliche ARPANET weiterhin zu Forschungs- und Entwicklungszwecken zur Verfügung stand. Zur selben Zeit bemühte sich die National Science Foundation (NSF) alle amerikanische Forschungseinrichtungen für Informatik, die nicht an ARPA-Projekten beteiligt waren, im Rahmen eines neuen *Computer Science Network* (CSNET) zu vernetzen. Das CSNET wurde ebenfalls auf TCP/IP-Basis konzipiert und mit dem ARPANET gekoppelt. Es erlaubte erstmals auch Verbindun-

gen zu ähnlichen Wissenschaftsnetzen in Deutschland, Frankreich, Japan, Korea, Finnland, Schweden, Australien, Israel und Großbritannien und war gegen Gebühr für alle computerwissenschaftlichen Einrichtungen aus Forschung, Wirtschaft und Verwaltung zugänglich.

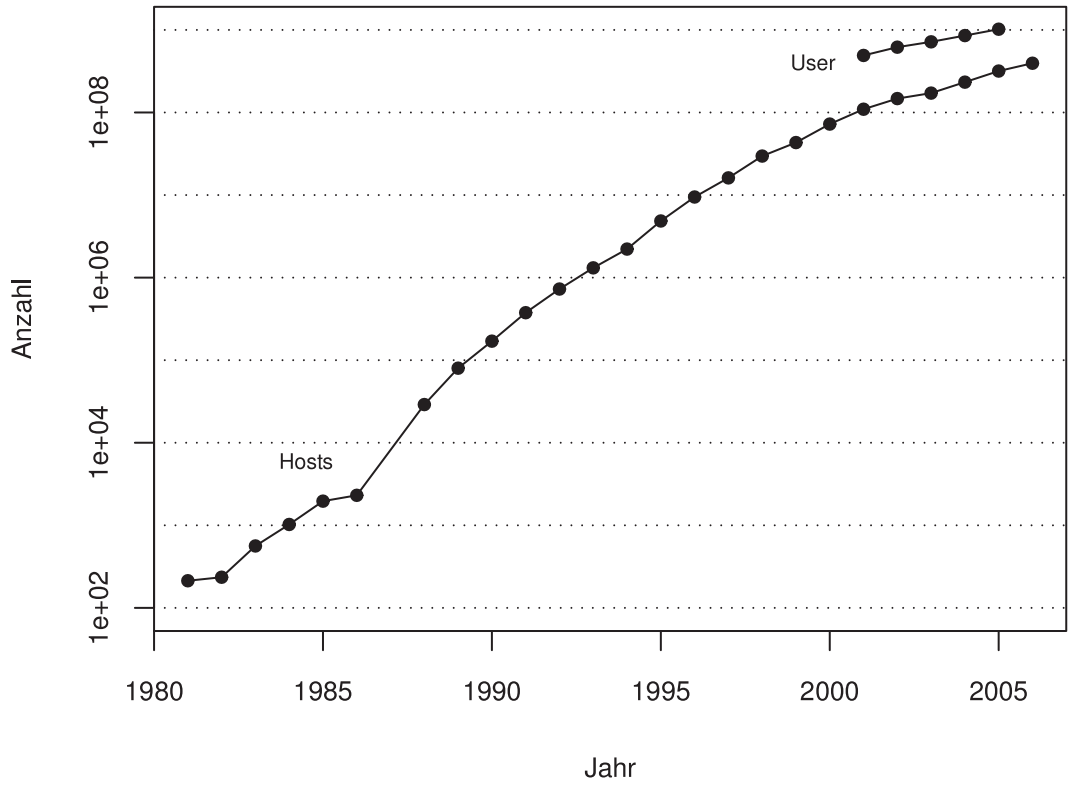
Mitte der 1980er Jahre stattete die NSF mehrere Rechenzentren mit neuen Supercomputern aus, deren Kapazität möglichst vielen wissenschaftlichen Einrichtungen nunmehr aller Disziplinen zur Verfügung stehen sollte. Hierzu wurden die lokalen Rechenzentren an ein regionales Netzwerk und dieses wiederum an ein landesweites Hochleistungsnetz angeschlossen, welches das Rückgrat (*Backbone*) des neuen NSFNET bildete, das 1986 als Nachfolger des CSNET in Betrieb genommenen wurde. Das NSFNET trug wesentlich zu einer raschen Ausbreitung der Internet-Technologie bei und drängte das ARPANET in seiner Bedeutung zunehmend in den Hintergrund, so daß dieses schließlich 1990 ganz eingestellt wurde (Abbate 1999b; Werle 1999).

Die in Abbildung 3.2 dargestellte Zeitreihe gibt eine ungefähre Vorstellung der quantitativen Entwicklung des Internet und verdeutlicht anschaulich dessen exponentielles Wachstum auf mittlerweile über 300 Mio. angeschlossene Host-Rechner.[57] Möglich wurde ein solch explosiver Diffusionsprozeß durch das Zusammentreffen einer Reihe günstiger Rahmenbedingungen, die sich auf verschiedene technische, ökonomische und organisatorische Faktoren zurückführen lassen. Neben dem offenen und flexiblen TCP/IP-Protokoll, das eine umfassende Integration heterogener physischer Netzwerkarchitekturen in einem logischen „Netz der Netze“ technisch erst ermöglichte, ist hier zunächst der enorme Fortschritt im Bereich der Datenübertragungsraten zu nennen. Vor allem die Techniken der optischen Datenübertragung mittels Glasfaserkabel sowie der extraterrestrischen Datenübertragung via geostationärem Satelliten trugen wesentlich zur Bewältigung des rapide ansteigenden Datenverkehrs bei (vgl. Gilder 2000).[58] Stetig wachsende Bandbreiten wurden über leistungsstarke Modems, ISDN-Anschlüsse und schließlich DSL bis in den privaten Bereich hinein verfügbar. Parallel sanken die Kosten für mikroelektronische Bauteile seit den 1980er Jahren noch einmal deutlich. Ursächlich hierfür ist neben dem technischen Fortschritt[59] vor allem eine zeitgleich stattfindende

57 Zur automatisierten Erhebungsmethode der zugrundeliegenden Daten vgl. <`http://www.isc.org/index.pl?/ops/ds/new-survey.php`>.

58 Gemäß des „Gilderschen Gesetzes“, das auf den amerikanischen Technik-Philosophen George F. Gilder zurückgeht, verdreifacht sich die Bandbreite der Datenübertragung in etwa jährlich.

59 Vgl. hierzu das bereits in Fußnote 48 erwähnte Mooresche Gesetz.



Datenquelle: Internet Software Consortium < `http://www.isc.org` >, UNCTAD (2006: 7).
Anmerkung: Die Ordinate wurde aufgrund des exponentiellen Verlaufs logarithmisch skaliert.

Abbildung 3.2: *Anzahl der Hosts und User im Internet nach Jahren*

Privatisierung, Liberaliserung und Deregulierung nationaler Telekommunikationssektoren, die auch für stetig fallende Verbindungspreise im Fernmeldenetz sorgte (vgl. Humphreys 1990; Schneider 1999; Schneider u. Tenbücken 2004).

Sogenannte Heim-Computer sind seitdem auch in privaten Haushalten finanzierbar und erfreuen sich, nicht zuletzt aufgrund der Einführung grafischer Benutzeroberflächen[60], die eine vereinfachte weil intuitive Bedienung ermöglichen, zunehmender Beliebtheit. Während der 1960er Jahre, als *Time-Sharing* und Datenfernverarbeitung in Rechenzentren dominierten, galt es dagegen noch als Verschwendung, „to devote time and money to the user interface, because computer cycles were so precious and had

60 Die Entwicklung des *Graphical User Interface* (GUI), das den bisherigen Kommandozeilen-Modus ablöste, folgte der Erfindung der Computermaus als neuem Eingabegerät. Einer der ersten Heim-Computer mit GUI war der ab 1984 von der Firma Apple gebaute Macintosh.

to be expended on the problem, not the person“ (Negroponte 1995: 89 f.). Das änderte sich erst als die Entwicklung des Mikroprozessors Anfang der 1970er Jahre den Bau individueller Arbeitsplatzrechner[61] zuließ. Die ungeteilte Rechenkapazität eines nur von Einzelpersonen genutzten Computers stand damit erstmals auch für eine grafisch orientierte Oberfläche zur Verfügung.

Bis Ende der 1980er Jahre existierten auf der Plattform des Internet gleichwohl so gut wie keinerlei grafische Anwendungen. Stattdessen gab es ein Ensemble kommandozeilenorientierter Dienste zum Austausch (FTP) und Auffinden von Dateien (Gopher, Archie) im Netz sowie zum Versenden von Nachrichten (eMail). Deren Bedienung aber war umständlich und setzte fundierte Kenntnisse voraus. Die Nutzung des Internet blieb daher zunächst einem exklusiven Kreis technisch versierter Anwender aus Wissenschaft und Forschung vorbehalten. Für den Durchbruch zu einem Massenmedium fehlte dem neuen Informations- und Kommunikationssystem trotz gesunkener Zugangskosten und umfangreicher Leistungskapazitäten noch immer der entscheidende Baustein einer ergonomischen Schnittstelle zwischen Mensch und Maschine.

Im Jahr 1989 initiierte Timothy Berners-Lee am *Conseil Européen pour la Recherche Nucléaire* (CERN) in Genf ein Projekt mit dem Ziel der Umsetzung des bereits seit längerem bekannten Hypertextprinzips[62] in ein internetbasiertes System zur vernetzen Publikation wissenschaftlicher Arbeiten. Aus diesem Projekt ging später die formale Deskriptionssprache *Hypertext Markup Language* (HTML) samt dem zugehörigen *Hypertext Transfer Protocol* (HTTP) hervor, auf deren Basis sich schließlich ein weltumspannendes Netz untereinander verknüpfter Hypertextdateien – das *World Wide Web* (WWW) – etablieren sollte. In idealer Weise kombiniert das WWW die Suche nach Informationen mit deren Präsentation im Rahmen einer grafischen Benutzeroberfläche. Hierbei können mittlerweile neben Texten auch Bilder und Töne und damit multimediale Inhalte dargestellt werden, weshalb in der Literatur teilweise auch von *Hypermedia* (Kuhlen 1997) oder *Mediamatik*[63] (Latzer 1997; Latzer et al. 2002) die Rede ist. Durch die Möglichkeit der einfachen Darstellung und Verknüpfung von Daten

61 Diese sind nach einer Typ-Bezeichnung von IBM vor allem als „Personal Computer“ (PC) bekannt.

62 Hypertext durchbricht die sequentielle Darstellung von Texten durch eine nicht-lineare Vernetzung einzelner Textbausteine mittels logischer Verweise. Der Leser „navigiert“ sich dabei auf einem individuell gewählten Pfad durch den Text, liest also gewissermaßen interaktiv (Bolter 1997; Kuhlen 1997; Wilde 1999).

63 Der Begriff „Mediamatik“ ist offensichtlich eine Verknüpfung von Multimedia und Telematik.

im Internet wurde mit dem auf HTML beruhenden WWW so die Grundlage für ein weltumspannendes, logisches Informationsnetz gelegt, das aufgrund seiner komfortablen Bedienbarkeit den Weg zu einer Nutzung auch für Laien ebnete.[64]

In der Folge stieg die Zahl der weltweiten Internet-Nutzer auf über eine Milliarde an (vgl. Abbildung 3.2). Für die rasche Ausbreitung des Internet zeichnet dabei noch ein weiterer Mechanismus verantwortlich, der sich ursächlich aus dem spezifischen Strukturcharakter eines jeden Netzwerkes ergibt. Gemäß dem bereits erwähnten Metcalfeschen Gesetz[65] korreliert der Individualnutzen eines jeden Netzwerkteilnehmers bekanntlich unmittelbar mit der Gesamtzahl aller Teilnehmer, wobei durchaus ein exponentieller Zusammenhang unterstellt werden kann. Dieser Umstand erklärt sich aus der Tatsache, daß der Zweck eines Netzwerkes ja gerade im Austausch von Informationen oder anderen Ressourcen besteht. Je mehr Teilnehmer aber Ressourcen in ein solches Netzwerk einbringen, desto größer ist folglich dessen Nutzen. Da jeder weitere Teilnehmer somit per se positive Netzwerkexternalitäten erzeugt, die letztlich allen Beteiligten zugute kommen, gibt es für jedes Netzwerk eine kritische Masse an Partizipanden, oberhalb derer der Individualnutzen eines jeden Teilnehmers die Individualkosten der Teilnahme übersteigt. Ist dieser Punkt erreicht, so beginnt ein positiver Rückkopplungsmechanismus zu greifen, der ein diskontinuierliches, exponentielles Wachstum des Netzes in Gang setzt (vgl. hierzu Mayntz 1988a). Nach anfänglich staatlicher Subventionierung durch die US-Regierung ist das Internet daher heute in der Lage, sich größtenteils privatwirtschaftlich zu finanzieren.

Aufgrund seines besonderen technischen Designs, das wesentlich auf offenen Standards und einem hohen Maß an Interoperabilität unterschiedlicher Hardware-Architekturen beruht, ist das Internet strukturell heterarchisch und von hoher Inklusivität. Die Grundzüge einer solchen Organisationsphilosophie reflektiert auch der logische Aufbau des WWW, in dem das Publizieren von Informationen polyzentral und deren Präsentation im Rahmen des Hypertext-Konzepts vernetzt statt hierarchisch erfolgt. Gerade die Implementation wesentlicher Prinzipien der Selbststeuerung (vgl. Eisner Gillett u.

64 Eine weitere Absenkung der Publikationsschwelle bringt gegenwärtig das sog. *Wiki*-Konzept, dessen bekannteste Anwendung die freie Online-Enzyklopädie `wikipedia.org` ist. „Wiki“ leitet sich von dem auf Hawai für „schnell“ gebräuchlichen Begriff „wikiwiki“ ab. Anwendungen auf Basis des *Wiki*-Konzepts erlauben die unmittelbare Online-Bearbeitung von WWW-Seiten nicht nur durch deren Autor, sondern durch jedermann. Sie finden daher insbesondere im Rahmen des Wissensmanagements Verwendung.

65 Vgl. Fußnote 51.

Kapor 1997; Christiansen 2000; Price u. Verhulst 2000) versetzt das Internet dabei offenbar in die Lage, den mit einem raschen Wachstum verbundenen hohen Grad an Komplexität bei gleichzeitig permanentem Wandel erfolgreich zu bewältigen.

Nur sehr wenige Aufgabenbereiche, so etwa die Verwaltung des Adreß- und Namensraumes sowie die Weiterentwicklung technischer Standards, benötigen eine zentrale Koordinationsinstanz. Zum hiermit befaßten institutionellen Kern des Systems gehören dabei sowohl formelle als auch informelle Organisationen, wie etwa das Network Management Center (NMC), das Network Information Center (NIC) sowie das Internet Configuration Control Board (ICCB), heute Internet Architecture Board (IAB) (vgl. Kahin u. Keller 1997; Werle 1999; Gould 2000; Cave u. Mason 2001; Baird 2002; Leib 2002). Eine zentrale Rolle spielte ferner von Anfang an die Internet Assigned Numbers Authority (IANA), deren heutiger Nachfolger die Internet Corporation for Assigned Names and Numbers (ICANN) ist. Doch selbst die Vergabe der IP-Adressen erfolgt blockweise, wodurch deren weitere Zuteilung den jeweils lokalen Netzwerkbetreibern im Wege der Delegation überlassen bleibt. Ein strukturiertes *Domain Name System* (DNS), das 1983 an der University of Southern California im Wesentlichen von Paul Mockapetris entworfen wurde, ermöglicht flankierend die Zuordnung eindeutiger Host-Namen mittels einer hierarchischen Baumstruktur. Diese unterteilt den Namensraum in verschachtelte Domänen und läßt daher ebenfalls eine weitgehend dezentrale Namensverwaltung unterhalb der obersten Ebene der *Top-Level-Domains* zu.

Differentia specifica von Computernetzwerken ist ferner, daß deren Knoten per definitionem aus intelligenten[66] Maschinen bestehen, die untereinander digital codierte Daten austauschen (vgl. Coy 1996). Maschinelle Kommunikation verläuft dabei auf Basis von *Binary Digits*, in Kontamination auch „Bits“ genannt, als universeller digitaler „lingua franca“ (Negroponte 1995: 63), und damit in weitgehender Abstraktion von den jeweilig referenzierten Inhalten. Erst auf Grundlage entsprechender Metainformationen werden einzelne Bits an ihrem Bestimmungsort rechnergestützt zu – im jeweiligen Handlungskontext relevantem – Wissen und damit Information in Form von Bildern, Tönen, Texten etc. aufbereitet. Der hohe Abstraktionsgrad digitalisierter Daten erlaubt nicht nur deren umfangreiche maschinelle Verarbeitung, sondern auch eine Integration bislang getrennter Analogtechniken der Informationsübertragung und -speicherung zu einem qualitativ neuen Medium in bisher nicht gekanntem Maße. Computertechnologie

66 Intelligenz meint hier im engeren Sinne die Fähigkeit zu interpretativer Symbolverarbeitung.

fungiert dabei als Mittler zwischen der konkreten, analog-kontinuierlichen Vorstellungs- und Lebenswelt der Nutzer und einem stetig expandierenden, abstrakten Universum diskreter, digital mediatisierter Daten. Im Ergebnis bilden Netzwerke wie das Internet ein Medium, welches sowohl Aspekte der Individual- als auch der Massenkommunikation umfaßt (vgl. Kubicek 1997).

Als technische Plattform für unterschiedlichste multimediale Inhalte ist dieses Medium in der Lage nahezu alle modernen Lebensbereiche in immer stärkerem Maße zu durchdringen. Bereits auf proprietärer Basis existierende IuK-Dienste migrieren aller Voraussicht nach zunehmend in die Welt der Internet-Technologie oder schaffen zumindest Schnittstellen zu dieser. So gibt es etwa im Bereich des Mobilfunks, in dem digitale Techniken und eine Partitionierung in Zellen inzwischen die zeitgleiche Nutzung des zur Verfügung stehenden Frequenzspektrums durch eine Vielzahl von Teilnehmern ermöglichen, Bestrebungen Informationen aus dem Internet über das *Wireless Application Protocol* (WAP) mobil verfügbar zu machen. Auch kann mittels *Voice over IP* bereits über Computernetzwerke telefoniert werden, während *Media Streaming* den Empfang von Audio- und Video-Inhalten per Internet zuläßt. Höchstwahrscheinlich ist die einfache Portierung traditioneller Technologien jedoch nur der Anfang völlig neuer Nutzungsmöglichkeiten, die sich vor allem durch ein Zurückdrängen des passiven *Push*-Prinzips herkömmlicher Massenmedien zugunsten der (inter-)aktiven *Pull*-Technologie des WWW ergeben. Informationen werden nicht mehr zentral er- und verarbeitet, um dann anschließend nach dem „Gießkannenprinzip“ breit gestreut zu werden, sondern können im Prinzip von jedermann im WWW zur Verfügung gestellt und entsprechend dem individuellem Bedarf abgerufen werden. Computerbasierte, künstliche Agenten schließlich unterstützen den Nutzer bei einer differenzierten Informationssuche und -aufbereitung, wodurch eine Fülle neuer Möglichkeiten entsteht (vgl. Kuhlen 1999).

3.3 Die globale Informationsgesellschaft

3.3.1 Makroökonomische Strukturverschiebungen

Ausgehend von der Annahme eines koevolutionären Zusammenhangs von Technologie und Gesellschaft sind aus soziologischer Perspektive moderne Informationstechnologien in doppelter Weise von Interesse, da sie zugleich Determinante und Resultat moderner Informationsgesellschaften sind (vgl. Weingart 1989; Rammert 2000: 59 ff.). Es stellt

sich somit zum einen die Frage nach jenen gesellschaftlichen – insbesondere ökonomischen, institutionellen und kulturellen – Rahmenbedingungen, die eine bestimmte Informationstechnologie erst ermöglichen und erfordern; zum anderen richtet sich das Augenmerk auf diejenigen gesellschaftlichen Veränderungen, die eine solche Technologie selbst nach sich zieht. Aus Makroperspektive ergibt sich auf einer höheren Abstraktionsebene das Bild eines zwischen gesellschaftlichen und technologischen Triebkräften oszillierenden Entwicklungspfades, der als dialektischer Prozeß wechselseitiger „schöpferischer Zerstörung“ im Sinne Schumpeters (1942) begriffen werden kann, welcher bestehende Strukturen durch Veränderungen im jeweils anderen Bereich einem evolutionären Anpassungsdruck unterwirft und sich selbst dabei gleich einem Perpetuum mobile dauerhaft fortschreibt. Castells (2001a: 6 ff.) erkennt hier gar einen Prozeß positiver Rückkopplung von technologischer Innovation und gesellschaftlicher Anwendung, der zu einer Beschleunigung des allgemeinen Wandels führe. Andererseits kann aus einer übergreifenden Perspektive mit Schmidt u. Werle (1992: 6) ebenfalls konstatiert werden:

> Technische Systemarchitekturen und soziale Koordinationsmuster stabilisieren sich wechselseitig und schaffen so einen Korridor, der die weitere technische Entwicklung strukturiert.

Katalytisch wirken in komplexen sozio-technischen Systemen vermutlich insbesondere jene Konstellationen, die Hughes (1987) als „reverse salients“ bezeichnet. Derartige „Schwachstellen“ entstehen, wenn ein System im Zuge seiner Ausdehnung oder Anpassung um fortgeschrittene Komponenten – seien es technische oder soziale Artefakte – erweitert wird, die aufgrund ihrer verbesserten Effizienz bestehende Komponenten deklassieren und daher sukzessive auch deren Erneuerung erforderlich machen. Jeder Innovationszyklus trägt so bereits den Keim des folgenden in sich. Eine sich hieraus ergebende Eigendynamik des Entwicklungsprozesses tendiert offenbar zu immer schnelleren Zyklen – ein Sachverhalt, den der Schriftsteller Ernst Jünger einmal metaphorisch als „Akzelerationsprinzip“ zu umschreiben suchte. Evolutionäre Prozesse verlaufen aus Makroperspektive jedoch keineswegs immer stetig, sondern neigen häufig zu einem Wechsel von Stagnation und sprunghaftem Umbruch (Mayntz 1988a; Schneider 2000a). Dies hat seine Ursache u. a. darin, daß bestehende Technologien nicht ad infinitum verbessert werden, da i. d. R. einem fallenden Grenznutzen durch Optimierung steigende Grenzkosten für Forschung und Entwicklung gegenüberstehen (vgl. Frenken 2006: 50).

TABELLE 3.1: *Entwicklungstrends in der globalen Informationsgesellschaft*

Subsystem	*Entwicklungstrend*
Technik	Digitalisierung, Konvergenz
Organisation	Fusion, Deregulierung
Ökonomie	Privatisierung, Konzentration, Konkurrenz
Kultur	Internationalisierung, Amerikanisierung, Demokratisierung

Es ist herrschende Auffassung unserer Zeit, daß wir uns gegenwärtig in einem geschichtlichen Umbruch bedeutenden Ausmaßes befinden, der eng mit den in Abschnitt 3.2 erörterten Fortschritten im Bereich der Informations- und Kommunikationstechnologie verknüpft ist. Kennzeichnend für diesen Umbruch ist eine zunehmende informationstechnische Vernetzung auch über nationalstaatliche Grenzen hinweg, die – im Zusammenspiel mit einer technisch hoch entwickelten Logistik (vgl. Alt u. Schmid 2000) – eine Verdichtung von Raum und Zeit impliziert und so eine Ausweitung globaler Interdependenzen in wirtschaftlicher, politischer und kultureller Hinsicht nach sich zieht (vgl. Cairncross 1997). Im Kontext dieser Entwicklung wird eine globale Dispersion des Produktionsprozesses in bislang ungeahntem Ausmaß möglich, weil der integrative Faktor der Information dank technischer Mediatisierung nahezu ohne Zeitverzug an fast jedem Ort und zu jeder Zeit verfügbar ist.

Kulturell und wirtschaftlich eröffnet die Dimension der Globalisierung neue Spielräume, organisatorisch stellt sie eine zentrale Herausforderung für die Steuerungsfähigkeit herkömmlicher – wesentlich nationalstaatlich basierter – institutioneller Regelungsmechanismen dar (vgl. u. a.: Cerny 1995; Held et al. 1999; Held u. McGrew 1999; Held 2000; Held u. McGrew 2002; Keohane u. Nye 2000a,b; Keohane 2002; Marsden 2000a). Kennzeichnend für eine globalisierte Informationsgesellschaft sind dabei nach Hamelink (1994) und Boyd-Barrett (2004) die in Tabelle 3.1 zusammengefaßten Entwicklungstrends. Zu den interessanten Fragen unserer Zeit gehört damit auch, ob und in wie weit institutionelle Transformationen, wie etwa die Öffnung und Entgrenzung nationaler Märkte, notwendige Voraussetzung dieser Entwicklung waren und sind, oder ob sie lediglich als begleitende Reaktion des politischen Systems die Faktizität eines – zu einem gewissen Grade eigendynamischen – techno-ökonomischen Wandels nachvollziehen.

Als Fukuyama (1989) kurz nach dem Ende der Ost-West-Konfrontation das Ende der Geschichte konstatierte, begründete er dies mit dem Wegfall ideologischer Spannungen zwischen demokratischen und totalitären Gesellschaftsformen. Abgesehen von der Tatsache, daß diese Vermutung spätestens durch die New Yorker Terroranschläge des 11. Septembers 2001 offenbar von der Geschichte selbst überholt und widerlegt wurde, scheint es gleichwohl wenig sinnvoll, Geschichte als Projektion eines singulären Antagonismus zu begreifen, wenngleich eine solche Sichtweise auf eine umfangreiche Tradition der Auslegung und Fortführung Hegelscher Dialektik zurückblicken kann. Vielmehr besteht die Geschichte menschlicher Gesellschaften offenkundig aus mehreren, ineinander verflochtenen Entwicklungspfaden, die als Ketten sozialer Problemlösungsprozesse verstanden werden können (vgl. Popper 1994). Jede Problemlösung aber wirft die Frage nach der Verteilung von Kosten und Nutzen des Handelns auf und birgt daher, sofern es sich bei der zugrundeliegenden Situationslogik um ein Konstantsummenspiel handelt, zumeist auch einen Interessenkonflikt, dessen Austragung im Idealfall durch den institutionellen Rahmen einer Gesellschaft in friedliche Bahnen gelenkt wird.

Ein diachroner Vergleich der im Wandel der Zeit jeweils dominierenden Problemkonstellationen einer Gesellschaft, die wir bei Bell (1973) als deren „axiales Prinzip“[67] wiederfinden, lenkt den Blick auf fundamentale Veränderungen in der Sozialstruktur und erlaubt so eine geschichtliche Phasenbildung. Diese kann zu einer historischen Gesellschaftstypologie von heuristischem Wert beitragen, indem sie wesentliche Entwicklungstendenzen bzw. „Trajektorien“ (Bell 1998) verdeutlicht.

Zu den empirisch am besten faßbaren Indikatoren derartiger gesellschaftlicher Transformationsprozesse zählen makroökonomische Strukturverschiebungen (vgl. Latzer u. Schmitz 2002: 13 ff.). Um diese quantitativ meßbar zu machen bietet sich eine sektorale Differenzierung der Wirtschaft anhand von Dissimilaritäten im Prozeß der Produktion von Gütern an. Am bekanntesten ist hier sicher die Dreiteilung in extraktiven, transformativen sowie Dienstleistungssektor, die auf Fisher (1939) und Clark (1940) zurückgeht und später von Fourastié (1954) zu einer Gesellschaftstheorie verfeinert wurde, in der der technische Fortschritt die Grundlage stetig steigender Produktivität bildet und sich daher ein struktureller Wandel von der Agrar- zur Industrie- und schließlich Dienstleistungsgesellschaft abzeichnet. Ausdruck findet dieser Wandel in einer Verschiebung des

67 Bell (1973: 115) definiert das „axiale Prinzip“ einer Gesellschaft als „the major lines around which other institutions are draped, and which pose the major problems of solution for the society“.

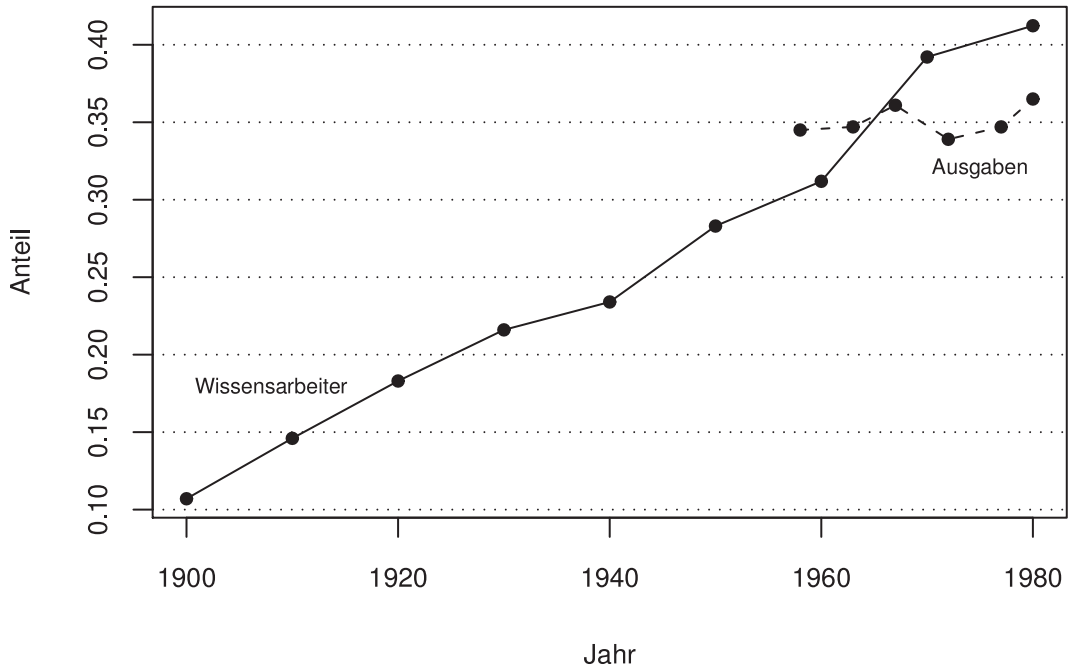
TABELLE 3.2: *Die Nachfragestruktur der US-Wissensindustrie nach Machlup, gemessen als prozentualer Anteil der Ausgaben zur Wissensproduktion am inflationsbereinigten BNE*

Jahr	1958	1963	1967	1972	1977	1980
Bildungswesen	16.6	16.8	17.4	14.8	13.4	12.0
Forschung und Entwicklung	2.2	2.6	2.7	2.2	2.1	2.2
Kommunikationsmedien	7.6	7.1	7.4	7.9	8.7	9.3
Informationsmaschinen	1.8	2.2	2.4	2.3	2.9	3.9
Informationsdienstleistungen	6.3	6.0	6.2	6.7	7.6	9.1
Summe	34.5	34.7	36.1	33.9	34.7	36.5

Quelle: Rubin u. Huber (1986: 24).

wirtschaftlichen Schwerpunktes einer Gesellschaft, gemessen sowohl an der Anzahl der Beschäftigten in den einzelnen Sektoren, als auch am relativen Anteil der Wertschöpfung der Sektoren am Bruttonationaleinkommen (BNE). Diese Konzeption impliziert eine inhärente natürliche Ordnung zwischen den Sektoren insofern, als der Ausbau eines jeden Sektors bereits eine hohe Produktivität der Sektoren niedererer Ordnung voraussetzt, da nur so genügend Arbeitskräfte für neue Aufgaben zur Verfügung stehen. Daher kann hier mit einigem Recht auch von primärem, sekundärem und tertiärem Sektor gesprochen werden.

Als einer der ersten erkannte Machlup (1962) die zentrale Bedeutung von Wissen als eigenständigem Wirtschaftsgut in modernen Dienstleistungsgesellschaften. Er prägte den Begriff der „Knowledge Industry“ und gliederte diese als eigenständigen vierten Sektor aus dem Dienstleistungssektor aus, um deren quantitative Entwicklung im Rahmen der volkswirtschaftlichen Gesamtrechnung statistisch zu analysieren. Machlup bedient sich dabei zweier Ansätze: während beim *Occupations Approach* der wissensindustrielle Sektor anhand spezifischer Berufsbilder abgegrenzt wird, orientiert sich der *Industry Approach* an den Gütereigenschaften der jeweiligen Produkte. Vor- und Nachteile beider Ansätze liegen auf der Hand. Im ersten Falle stellen sich Probleme hinsichtlich der Gewichtung des wissensbezogenen Anteils verschiedener Berufe sowohl in Relation zueinander als auch im Wandel der Zeit; im zweiten kann nur die Wertschöpfung derjenigen Wissensprodukte unmittelbar erfaßt werden, deren Distribution



Datenquelle: Machlup (1962: 384 f.), Rubin u. Huber (1986: 24, 196).

Abbildung 3.3: *Die Entwicklung der US-Wissensindustrie nach Machlup, gemessen als relativer Anteil der Wissensarbeiter an der Gesamtzahl aller Beschäftigten sowie der Ausgaben zur Wissensproduktion am inflationsbereinigten BNE*

am Markt erfolgt und die daher einen konkreten Preis realisieren, wohingegen die Wertschöpfung aller anderen wissensbezogenen Tätigkeiten entweder unberücksichtigt bleibt oder mittels empirisch nur mangelhaft fundierter Verfahren zu schätzen ist.

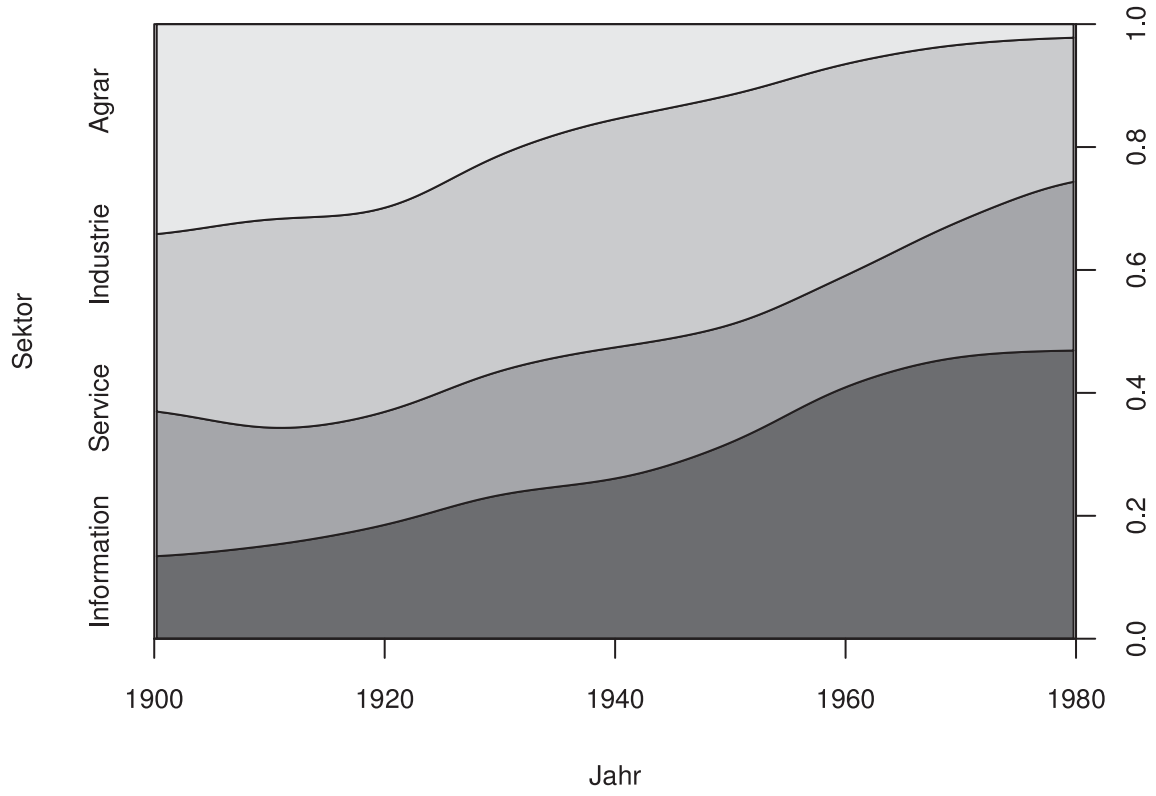
Obwohl Machlup beide Ansätze parallel verfolgt, liegt der Schwerpunkt seiner Arbeit nach eigenem Bekunden gleichwohl auf letzterem (Machlup 1962: 48). Machlups Berechnung des Anteils der Wissensindustrie am BNE der USA beruht hauptsächlich auf der Endnachfrage an wissensbezogenen Gütern, entspricht methodisch also im Wesentlichen der volkswirtschaftlichen Verwendungsrechnung. Bis zu seinem Tode 1983 arbeitete Machlup an einem Folgewerk zur Entwicklung der US-Wissensindustrie im Zeitraum von 1960 bis 1980, welches dann posthum von seinen Schülern Rubin u. Huber (1986) veröffentlicht wurde. Tabelle 3.2 schlüsselt für den genannten Zeitraum die von Machlup berechneten Daten zur wissensbezogenen Nachfragestruktur auf. Auf Basis dieser Daten läßt sich zwischen 1960 und 1980 ein deutlicher Trend zum Rückgang bzw. zur Stagnation der relativen Ausgaben für Bildung sowie Forschung und Entwick-

lung konstatieren, der allerdings durch steigende Aufwendungen für IuK-Technologien und -Dienstleistungen kompensiert wird. Insgesamt erhöht sich die Gesamtnachfrage nach Wissensprodukten in Relation zum BNE im untersuchten Zeitraum jedoch nur unwesentlich.

Interessant ist der Vergleich zur Entwicklung der Beschäftigungsstruktur. Abbildung 3.3 veranschaulicht beide Zeitreihen grafisch. Während der Anteil der Wissensproduktion am BNE nahezu konstant bleibt, steigt der Anteil der Wissensarbeiter an der Gesamtzahl aller Beschäftigten kontinuierlich an. Beide Kurven schneiden sich etwa Mitte der 1960er Jahre. Ab diesem Zeitpunkt sind im Verhältnis zur Gesamtnachfrage an Wissensgütern überproportional viele Wissensarbeiter zu verzeichnen. Auf den ersten Blick läßt dies eine sinkende – oder zumindest im Vergleich zur Gesamtwirtschaft nur unterproportional steigende – Produktivität der Wissensarbeit trotz technologischen Fortschritts vermuten. Ein solcher Schluß wäre allerdings voreilig, besteht doch auch die Möglichkeit, daß ein wachsender Teil der Wissensproduktion außerhalb der Märkte alloziert wird und sich damit einer statistischen Erfassung weitgehend entzieht.

Im Jahr 1976 legte Marc Uri Porat im Auftrag des US-Handelsministeriums eine Dissertation (Porat 1977) vor, in der er an Machlups empirische Analyse der Wissensindustrie, die Porat als „Information Economy“ bezeichnet, anknüpft, jedoch zugleich eine Reihe methodischer Modifikationen vornimmt. So orientiert Porat sich im Gegensatz zu Machlup, der eine Restrukturierung der volkswirtschaftlichen Gesamtrechnung vorgenommen hatte, strikt an den traditionell üblichen Kategorien (Rubin u. Huber 1986: 7), weshalb Porats Ansatz nicht immer die analytische Tiefenschärfe von Machlups Studie erreicht, dafür aber einen vereinfachten Rückgriff auf bestehendes statistisches Datenmaterial erlaubt. Als wesentliche Neuerung aber unterscheidet Porat zwischen primärem und sekundärem Informationssektor, je nachdem ob es sich bei den erstellten Informationsgütern und -dienstleistungen um Endprodukte der Informationsindustrie oder aber um Zwischenprodukte anderer Industrien handelt. Auf diese Weise soll auch diejenige Wertschöpfung erfaßt werden, die durch Vorleistungen für nicht informationsbezogene Güter entsteht, wie das etwa im Rechnungswesen klassischer Industriebetriebe der Fall ist.

Um auch den sekundären Informationssektor unmittelbar messen zu können, basiert Porats Verfahren nicht auf einer volkswirtschaftlichen Verwendungsrechnung, sondern auf einer Verteilungsrechnung, der Einkommen und Gewinne informationsbezogener Berufe und Unternehmen zugrundeliegen (Rubin u. Huber 1986: 13 – 15). Obwohl bei-



Datenquelle: Porat nach Katz (1988: 144).

Abbildung 3.4: *Der Anteil der Sektoren der US-Wirtschaft am BNE nach Porat*

de Berechnungsweisen im Ergebnis zum selben Gesamtbetrag des BNE führen, kann der gemessene Anteil des Informationssektors je nach Verfahren deutlich variieren. Abbildung 3.4 veranschaulicht die Entwicklung der US-Wirtschaft in einem Vier-Sektoren-Modell auf Grundlage der Poratschen Daten. Deutlich erkennbar ist hier die zunehmende Bedeutung des Informationssektors, der um 1980 bereits gute 45 Prozent des BNE umfaßt. Umgekehrt läßt sich konstatieren, daß nur noch etwa 25 Prozent aller Einkommen und Gewinne im Bereich der klassischen Sektoren der Industrie- und Agrarwirtschaft erzielt werden. Zu einem ähnlichen Bild kommt, angelehnt an die Poratsche Vorgehensweise, für Deutschland auch Dostal (1995).

3.3.2 Gesellschaftstheoretische Ansätze

Die in den Studien von Machlup und später Porat deutlich erkennbaren Strukturverschiebungen waren und sind, zusammen mit den ähnlich gelagerten Arbeiten des Japaners Youichi Ito, auch Gegenstand einer Reihe gesellschaftstheoretischer Überlegungen. Vor allem Machlups Studie dient bevorzugt als Referenzpunkt zur empirischen Fundierung theoretischer Ansätze der Wissens- bzw. Informationsgesellschaft. Porat hingegen wurde hinsichtlich seiner Fragestellung selbst von Bell und anderen inspiriert. Unter denjenigen Arbeiten, die die herausgehobene Bedeutung von Information und Wissen in modernen Gesellschaften in den Mittelpunkt ihrer Untersuchung stellen, sind – neben eher populärwissenschaftlichen Werken wie Toffler (1980) und Negroponte (1995) – vor allem Bell (1973, 1979, 1998), Drucker (1968, 1989, 1993) und Castells (2000b, 2001a,b) sowie für den deutschen Sprachraum Glotz (1999, 2001), Stehr (1994, 2000, 2001a,b) und Bühl (1996, 2000) zu nennen.

Befassen sich die meisten Autoren hauptsächlich mit den Auswirkungen der Informatisierung auf die Gesellschaft, so beleuchtet Beniger (1986) zunächst die Ursachen der Entstehung moderner Informationsgesellschaften, die seiner Meinung nach bis weit in das 19. Jahrhundert zurückreichen, als Technisierung und Automatisierung neue Steuerungs- und Koordinationsprobleme aufwarfen, zu deren Bewältigung eine bis heute anhaltende Weiterentwicklung von Kontroll- bzw. Steuerungs- und damit auch Informationstechnologien notwendig wurde. Aus einem solchen Blickwinkel erfordert die nahezu vollständige maschinelle Substitution menschlicher wie tierischer Muskelkraft im Zuge der Industriealisierung auch eine maschinelle Substitution der Steuerungsleistung des menschlichen Geistes. Industriealisierung und Informatisierung stellen sich damit als komplementäre Aspekte technologischen Fortschritts dar. Ist der kritische Rohstoff der Industriegesellschaft die zum Betrieb automatisierter Fertigungsanlagen unabdingbare Energie, so tritt neben diese in der Informationsgesellschaft zusätzlich der entscheidende Faktor (maschinell verarbeiteter) Information, auf deren Grundlage rationale Entscheidungen in einem durch automatisierte Prozesse drastisch erweiterten, zugleich aber zunehmend komplexen Handlungsraum erst möglich werden.

Weil jede Form von Technologie letztlich ein Mittel der Effizienz- und damit Produktivitätssteigerung ist, setzt ihre Implementation immer auch menschliche Arbeitskraft frei, die dann in der Folge zur Generierung additiven Wohlstandes zur Verfügung steht (vgl. Webster 2002: 38). Zugleich bewirkt technologischer Fortschritt einen zuneh-

menden Abstraktionsgrad menschlicher Arbeit, da diese ihre maximale Wertschöpfung vorzugsweise dort entfaltet, wo sie (noch) nicht durch eine konkrete Technik substituiert werden kann. Indem sich Technik zwischen Mensch und Natur schiebt, verändert sie so jene wirtschaftlichen und sozio-kulturellen Strukturen, die die Produktionsweise einer Gesellschaft bestimmen. In Erkenntnis dieses Umstandes kennzeichnet etwa Bell (1973: 126 ff.) die Handlungslogik prä-industrieller Gesellschaften als „game against nature", industrieller hingegen als „game against fabricated nature". Für post-industrielle Gesellschaften schließlich spricht er von einem „game between persons".

Da das niedrige Produktivitätsniveau einer prä-industriellen Gesellschaft gerade einmal die Befriedigung der Existenzbedürfnisse der überwiegenden Mehrheit ihrer Mitglieder ermöglicht, konzentriert sich diese auf die Probleme des täglichen Überlebens und wird vor allem durch traditionelle Produktions- und Verteilungsstrukturen dominiert, die sich über lange Zeiträume herausgebildet haben. Natürliche Rohstoffe und die Anwendung von Muskelkraft sind zentrale Produktionsfaktoren und die Basis von Macht, verstanden als Chance zur Durchsetzung eigener Interessen. Wandel vollzieht sich nur sehr langsam, da kaum Überkapazitäten für experimentelle Innovationen zur Verfügung stehen. In der industriellen Gesellschaft hingegen ist die Deckung der Existenzbedürfnisse durch den maschinell erzielten Produktivitätszuwachs weitestgehend gesichert. Zentrale Faktoren sind nun Kapital und Energie als Voraussetzung der Anschaffung und des Betriebes von Maschinen. Gesellschaftliche Konkurrenz besteht vor allem um Güter zur Deckung von Grundbedürfnissen. Axiales Prinzip ist nach Bell (1973: 117) ökonomisches Wachstum, induziert durch marktwirtschaftlich (privat) oder hierarchisch (staatlich) alloziertes Kapital. Wandel erfolgt größtenteils im Wege inkrementeller Rationalisierung, motiviert durch das Streben der Kapitaleigner nach Profit, wodurch sich eine kontinuierliche Produktivitätssteigerung einstellt.

Ein hieraus resultierender Zuwachs an gesamtgesellschaftlichem Wohlstand sorgt zwar zunächst für abnehmende Verteilungskonflikte im Bereich der Grundbedürfnisse, ruft andererseits aber auch sehr bald neue Luxusbedürfnisse hervor, deren Befriedigung schließlich den Strukturwandel zur post-industriellen Dienstleistungsgesellschaft einleitet. In dieser geht es, folgt man Bell (1973: 128), vor allem um die Bereitstellung von Gesundheits- und Bildungsgütern. Diese aber beruhen wesentlich auf dem Faktor Wissen, weshalb die post-industrielle Gesellschaft auch eine Informationsgesellschaft ist, in der kodifiziertes theoretisches Wissen zum Axialprinzip avanciert. Dementsprechend prognostiziert Bell für post-industrielle Gesellschaften eine herausgehobene Bedeutung

intellektueller – insbesondere wissenschaftlicher – Tätigkeiten, die auf die Entwicklung von Theorien zur Analyse und Simulation von – sowie zur Entscheidungsfindung in – komplexen Systemen abzielen.

Auch Drucker (1968, 1989, 1993) rezipierte bereits sehr früh Machlups Idee der Wissensindustrie als *Knowledge Economy*. Wurde jedoch im Zuge des auf Frederic W. Taylor zurückgehenden Scientific Management Wissen noch nahezu ausschließlich als Mittel zur technokratischen Optimierung industrieller Fertigungsprozesse begriffen, so betont Drucker für das Zeitalter einer von ihm als „post-kapitalistisch" bezeichneten, neuen Gesellschaft die zentrale Bedeutung von Wissen an sich. Post-kapitalistisch sei diese Gesellschaft dabei nicht etwa im marxistischen Sinne, und daher auch nicht zwangsweise von einem Rückgang bewährter und im Hinblick auf stetige Innovationsanreize notwendiger marktwirtschaftlicher Koordinationsmechanismen begleitet, sondern vielmehr allein aufgrund der Tatsache, daß Wissen das Kapital als grundlegende Ressource der industriellen Wirtschaftsform ablöse. Der Prozeß der Allokation des – in post-kapitalistischen Gesellschaften zum Großteil im Besitz von Kleinanlegern befindlichen – Kapitals hingegen ist weitgehend institutionalisiert und erfolgt daher unabhängig von Einzelpersonen, weshalb Drucker in diesem Zusammenhang auch von einem „Capitalism without capitalists" (Drucker 1993: 67) spricht.

Die wirtschaftliche und damit auch gesellschaftliche Hauptrolle spiele, so Drucker, künftig der Wissensarbeiter, der durch Allokation und Transformation von Wissen Innovation und damit Produktivitätszuwachs ermögliche. Im Unterschied zum Industriearbeiter verfüge der Wissensarbeiter jedoch nicht nur über seine Arbeitskraft, sondern mit dem ihm eigenen Wissen auch über einen Großteil der im Produktionsprozeß eingesetzten kritischen Ressourcen, wodurch er im Verhältnis zu seinem Auftraggeber weit größere Unabhängigkeit als jener genieße. Hieraus ergeben sich neue Probleme der Organisationsintegration, wie sie etwa in die Agenturtheorie thematisiert werden. Zweck moderner Organisationen ist dann in der Hauptsache eine Bündelung von Wissensressourcen sowie deren produktive Allokation. Management ist nicht mehr primär Prozeßoptimierung sondern im Schumpeterschen Sinne Forcierung des Wandels durch gezielte Innovation. Den vorrangigen Modus der Koordination bildet nicht die hierarchische Fremdsteuerung des Industriearbeiters, sondern die kooperative Selbststeuerung kreativer Wissensarbeiter (Drucker 1968: 188 ff.).

Wie in Abschnitt 3.2 bereits verdeutlicht, spielt Information und die Technologie ihrer Verarbeitung und Verteilung seit Urzeiten eine zentrale Rolle in menschlichen

TABELLE 3.3: *Schema einer Gesellschaftstypologie*

	Agrar-Gesellschaft	*Industrie-Gesellschaft*	*Informations-Gesellschaft*
Wertschöpfungsprinzip	Extraktion	Transformation	Innovation
Zentrale Berufsbilder	Bauern, Handwerker	angelernte Arbeiter	Wissensarbeiter, Manager
Kritische Produktions- und Machtfaktoren	natürliche Rohstoffe, Muskelkraft	Kapital, Energie	Wissen, Information
Konkurrenzfeld	Existenzbedürfnisse	Grundbedürfnisse	Luxusbedürfnisse
Logik des Handelns	Spiel gegen die Natur	Spiel gegen die technisierte Natur	Spiel zwischen Akteuren
Wirklichkeitszugang	Erfahrung, Tradition	Empirie, Induktion	Theorie, Deduktion
Konfliktlinien	Bauern vs. Adel	Arbeiter vs. Kapitalisten	gering Qualifizierte vs. Wissenselite
Koordinations-mechanismen	Familienbande, Feudalstrukturen	Hierarchie, Markt	Netzwerk, Heterarchie
Interdependenzen	lokal	national	global
kulturelle Bezugspunkte	Mythen, Religion	Massenmedien	individuelle und virtuelle Realitäten

Quelle: Eigene Zusammenstellung in Anlehnung an Bell, Drucker und Castells.

Gesellschaften. Castells (2000b) unterstreicht ferner, daß auch Netzwerke als flexible Organisationsform schon lange zum Repertoire sozialer Koordinationsmechanismen gehören. Liegt die Stärke polyzentraler Netzwerke vor allem in ihrer beachtlichen Fähigkeit zu einer vergleichsweise schnellen, selbstorganisierten Adaption an eine sich stetig wandelnde Umwelt, so steht diesem an sich gewichtigen Vorteil in der Bewältigung eines hohen Komplexitätsgrades allerdings zugleich der nicht unbedeutende Nachteil eines erhöhten Koordinations- und damit Informationsaufkommens entgegen, das die informationstechnischen Möglichkeiten vergangener Gesellschaften mit zunehmender Netzwerkgröße sehr bald überforderte.

Umfangreiche gesellschaftliche Strukturen tendierten daher in der Geschichte zu hierarchisch-zentralisierten Organisationsformen, wie etwa dem klassischen Nationalstaat, die mit ihren auf Dauer angelegten und damit inhärent nur wenig flexiblen Institutionen den Informationsfluß wesentlich reduzieren und kanalisieren. Erst die elektronische Informationstechnologie unserer Zeit erweitert – und das ist nach Castells (2001a: 75 ff.) das entscheidende Momentum – die Kapazität moderner Gesellschaften zur Informationsverarbeitung derart, daß Netzwerke nunmehr auch im großen Maßstab

zum dominierenden Koordinationsparadigma in fast allen gesellschaftlichen Teilbereichen aufsteigen können (vgl. Wellman et al. 1996). Dies gilt offenbar selbst für den Bereich der traditionell hierarchisch organisierten Kriegsführung (vgl. Arquilla u. Ronfeldt 1996, 2001). Da die Chance zur Ressourcenmobilisation und damit der Nutzen eines Netzwerks ferner, gemäß des Metcalfeschen Gesetzes (vgl. Fußnote 51), parallel zu dessen Größe exponentiell zunimmt, läßt sich hieraus auch eine – dem Netzwerkparadigma immanente – Tendenz zur globalen Ausdehnung vernetzter Strukturen herleiten.

Die außergewöhnliche Flexibilität von Netzwerken hinsichtlich Koordination und Ressourcenmobilisation in Verbindung mit ihrer globalen Ausdehnung generiert ein enormes Innovationspotential und induziert so neue Produktivitätszuwächse, die nach Castells (2001a: 19 ff.) ein Überleben des kapitalistischen Wirtschaftssystems nach der Krise des Keynesianismus Anfang der 1970er Jahre erst möglich machten, zugleich aber dessen grundlegende Restrukturierung in Form einer Netzwerkökonomie erzwangen. In dieser integrieren vernetzte Informationstechnologien global verteilte Produktions- und Distributionsprozesse, deren Differenzierung und Spezialisierung über nationalstaatliche Grenzen hinweg erfolgt. Die neuen sozio-kulturellen Konfliktlinien des „informationellen Kapitalismus“ gruppieren sich dabei um den Zugang zu diesen Netzwerken, allen voran dem Internet als zentraler informationstechnischer Infrastruktur der Informationsgesellschaft, denn dieser Zugang wird zur zentralen Voraussetzung der Mobilisation interessensrelevanter Ressourcen (vgl. Dutton 1999; Rifkin 2000; Castells 2001b).

3.3.3 Die virtuelle Welt elektronischer Räume

Moderne informationstechnische Netzwerke spannen aber auch einen qualitativ neuen „elektronischen Raum“ (Kuhlen 2005) sozialer Interaktion auf, der in der Literatur häufig als „virtuelle Realität“ charakterisiert wird (Rheingold 1995; Wellman et al. 1996; Münker 1997; Floyd 1999; Bühl 2000; Schuler u. Day 2004). Schon die Wahl eines solchen Oxymorons verdeutlicht, daß hierbei traditionelle raum-zeitliche Kategorien verschwimmen (vgl. Mihalache 2002). Es entsteht eine artifizielle, symbolische Welt, die, obwohl im eigentlichen Sinne nicht real da nicht physisch existent, sondern letztlich nur aus einem interpretationsoffenen digitalen Bit-Muster bestehend, so doch über das Medium intelligenter Rechenmaschinen indirekt erfahrbar wird (vgl. Benedikt 1992). Eo ipso kann diese potentiell in die reale Welt hineinwirken und gewinnt damit virtuellen Charakter. In einer solchen virtuellen Welt auf Basis vernetzter Informati-

onssysteme spielen die Erzählungen des kanadischen Science-Fiction-Autors William Gibson, dessen Roman-Trilogie „Neuromancer“ (Gibson 1984) den von ihm geprägten Neologismus „Cyberspace“[68] zu einer der populärsten Metaphern computergestützter Handlungsräume werden ließ. Gibson selbst umschreibt die virtuelle Welt des Cyberspace als „konsensuelle Halluzination“.

Weil in der virtuellen Welt elektronischer Räume nicht dieselben physikalischen Gesetzmäßigkeiten wie im euklidischen Raum der realen Erfahrungswelt herrschen, dient diese nicht nur als kollektive Projektionsfläche für Ideen und Gedanken sondern eröffnet auch der Phantasie neue Spielräume. In elektronischen Räumen etabliert sich eine partielle Parallelwelt, die einerseits reale Objekte referenziert, andererseits aber auch gänzlich irreale Konstrukte umfaßt. Nach der Immersion in die Welt vernetzter Computer kann der „Cybernaut“ nicht nur frei im Cyberspace navigieren, sondern zugleich als „Cyberstructor“ an der Gestaltung der virtuellen Welt einschließlich des eigenen Avatars mitwirken. In der Folge erodieren in elektronischen Räumen monolithische Identitäten zu Gunsten multipler Persönlichkeiten und fragmentierter Subjekte (vgl. Jameson 1993; Turkle 1997). Soziale Interaktion folgt dabei „online“ offenbar anderen Regeln, als dies „offline“ der Fall ist. Im Cyberspace entwickelt sich eine eigene Subkultur, wie das Beispiel der *Netiquette*[69], eines Kanons allgemein akzeptierter Verhaltensregeln, illustriert.

Aufgrund der dezentralen Struktur des Internet wird sowohl die Möglichkeit als auch die Notwendigkeit staatlicher Regulierung, in Sonderheit im Umfeld von Grassroot-Organisationen und Bürgerrechtsbewegungen wie etwa der Electronic Frontier Foundation (EFF), häufig prinzipiell in Abrede gestellt. So stammt bspw. vom EFF-Mitbegründer John Gilmore der oft zitierte Satz: „The net treats censorship like damage and routes around it.“[70] In der Konsequenz wird der Cyberspace aus einer solchen Perspektive als eigenständiger, von der materiellen Welt weitgehend unabhängiger Raum sozialer Interaktion aufgefaßt, in dem es eine neue, libertär-basisdemokratische Kultur zu etablieren gilt. John P. Barlow, ebenfalls Mitbegründer der EFF, schreibt daher in seiner

68 Der erste Wortteil ist ganz offensichtlich eine Anleihe bei Norbert Wieners „Cybernetics“ und damit eine Referenz an den Kontroll- und Steuerungscharakter vernetzter Informationssysteme, während sich der zweite Teil auf den lateinischen Begriff *spatium* zurückführen läßt, der – nota bene – neben einer räumlichen auch die Konnotation einer zeitlichen Dimension umfaßt.

69 Das Kunstwort ist eine Kontamination der Begriffe „net“ und „etiquette“.

70 Vgl. <`http://www.toad.com/gnu`>.

– an die Regierungen der industriealisierten Welt gerichteten – „Declaration of the Independence of Cyberspace“ aus dem Jahr 1996:[71]

> Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions. [...] You do not know our culture, our ethics, or the unwritten codes that already provide our society more order than could be obtained by any of your impositions. [...] Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live. [...] Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are based on matter, and there is no matter here. [...] We will create a civilization of the Mind in Cyberspace.

Genau diese hypothetische Unabhängigkeit des Cyberspace jedoch gilt es kritisch zu hinterfragen, denn – abgesehen von der unbestreitbaren kulturellen Eigendynamik des Cyberspace – bleibt das Internet zweifelsohne ein funktionales Subsystem der realen Welt. Als solches ist es selbstverständlich ebenso aus dieser heraus beeinflußbar wie es umgekehrt in sie hinein Rückwirkungen entfalten kann. Eine solche Rückwirkung aber begründet das Interesse realer Akteure an einer „Kolonialisierung“ des Cyberspace zum Zwecke der Beeinflussung eben dieser realen Auswirkungen. Lessig (1999) hebt hervor, wie sehr die Handlungsfreiheit des Einzelnen im Cyberspace vor einem solchen Hintergrund von dessen hard- und softwaretechnischer Architektur, die bei Lessig unter dem Überbegriff des „Code“ subsumiert wird, abhängig ist. Dieser technische Kontext aber ist durch Wirtschaft und Staat vielfältig manipulierbar, was eine mittelbare Steuerbarkeit des Handelns im Cyberspace impliziert.

Machte die ursprüngliche Architektur des Internet eine zentrale Regulierung de facto unmöglich, so perpetuiert sich dieser Umstand nach Lessig (1999) keineswegs zwangsläufig. Ganz im Gegenteil konstatiert Lessig im Zuge der architektonischen Weiterentwicklung eine zunehmende Implementation technischer Kontrollmechanismen, die eine immer weitergehende Einengung individueller Handlungsfreiheit im Cyberspace bedeute. Nicht zuletzt deshalb komme der Unabhängigkeit technischer Standardisierungsorganisationen wie ICANN besondere Bedeutung hinsichtlich der Wahrung von Freiheitsrechten zu. Die mit der Akkumulation privater Daten verbundene Erstellung

71 Vgl. <`http://homes.eff.org/~barlow/Declaration-Final.html`>, aufgerufen am 23.8.2005, zum vollständigen Wortlaut.

TABELLE 3.4: *Konfligierende Interessen im Cyberspace*

Anwender	↔	*Techno-Elite*
Privatsphäre	↔	Identifikation
Vertrauliche Kommunikation	↔	Kontrolle des Datenflusses
Freie Meinungsäußerung	↔	Kontrolle der Inhalte
Freiheit der Information	↔	Geistiges Eigentum

von Konsumentenprofilen durch Unternehmen, die Filterung des Datenverkehrs durch Provider und staatliche Institutionen sowie die Umsetzung neuer Mechanismen des Kopierschutzes exemplifizieren dabei aus Lessigs Sicht die These eines zunehmenden (technischen) Regulierungsniveaus im Cyberspace nachdrücklich.

Rückblickend läßt sich damit, neben dem Zugang zum Internet als basaler Conditio sine qua non der Überwindung „digitaler Obdachlosigkeit", innerhalb des Cyberspace selbst eine weitere Konfliktlinie identifizieren. Diese verläuft zwischen den Anwendern und jener Elite, die die technischen Rahmenbedingungen setzt und damit implizit die Handlungsmöglichkeiten der virtuellen Welt definiert. Beide Seiten präferieren eine libertäre Ideologie, da ein Vakuum staatlicher Regulierung einerseits der Ausübung individueller Freiheitsrechte der Anwender tatsächlich oder vermeintlich entgegenkommt, andererseits aber auch die bestehenden strukturellen Machtpositionen der Techno-Elite nicht gefährdet (Jordan 1999: 215).

Macht, im Weberschen Sinne verstanden als Chance zur Durchsetzung eigener Interessen, aber muß um Wirkung entfalten zu können auf einen konkreten Adressaten projezierbar sein.[72] Eine Identifikation einzelner Anwender liegt daher im natürlichen Bestreben der Techno-Elite.[73] Ferner ist diese zur Festigung ihrer Macht an verbindlichen Spielregeln interessiert, die eine Kontrolle von Informationsinhalten und Datenfluß im Cyberspace erfordern. Schließlich stützt sich Macht unmittelbar auf Ressourcen. Da Information und Wissen im Cyberspace zur zentralen Ressource avanciert, gewinnen in

72 Aus diesem Grund nimmt bei asymmetrischen Machtverhältnissen die unterlegene Seite häufig in einem verdeckten Guerilliakampf Zuflucht, dessen schärfste Waffe die Anonymität der Handelnden ist.

73 Dies gilt auch für staatliche Behörden, die zur Strafverfolgung in besonderer Weise auf Möglichkeiten der Identifikation angewiesen sind (Reitinger 2000).

diesem Zusammenhang geistige Eigentumsrechte als Garantie einer dauerhaften Verfügungsgewalt besondere Bedeutung. Die sich hieraus ableitenden Antagonismen im Spannungsfeld von Anwender und Techno-Elite sind abschließend noch einmal in Tabelle 3.4 zusammengefaßt.

4 Elektronische Sicherheit als soziales Problem

4.1 Elektronische Netze als kritische Informationsinfrastruktur

4.1.1 Zum Begriff der Infrastruktur

Die Wortgeschichte des Begriffes „Infrastruktur“ ist relativ jung. Gleichwohl sind die bezeichneten Strukturen weitaus älter als der Begriff selbst. Sie existieren in der Geschichte aller arbeitsteilig wirtschaftenden Gesellschaften, unabhängig von deren Grad an Ausdifferenzierung und technologischer Entwicklung. So gab es bereits in der Antike mit dem griechischen System der Signalfeuer oder den römischen Fernstraßen und Aquädukten bedeutende Infrastrukturen, wenngleich das Bewußtsein ihrer zentralen gesellschaftlichen und ökonomischen Bedeutung vermutlich noch nicht in entsprechendem Maße ausgeprägt war. Nach Frey (1972: 3 ff.) erkannte jedoch bereits der Merkantilismus die herausgehobene Bedeutung grundlegender infrastruktureller Einrichtungen, wie etwa des Verkehrs- und Postnetzes, aber auch des Schulsystems, für die allgemeine Wohlfahrt einer Volkswirtschaft.

Der heute geläufige Neologismus „Infrastruktur“ setzt sich aus den beiden lateinischen Bestandteilen „infra“ (unterhalb, unten, darunter) sowie „structura“ (Aufbau, Struktur) zusammen. Das korrespondierende Verb zu „structura“ ist „struere“, welches „schichten“ oder „stapeln“ bedeutet. Infrastruktur ließe sich also als „zugrundeliegende Schicht“ übersetzen. Bereits an dieser Übersetzung wird deutlich, daß die Bezeichnung Infrastruktur, über die von ihr unmittelbar bezeichnete Grundlage hinaus, immer auch auf eine weitere Entität verweist, deren notwendige Voraussetzung eben diese Grundlage bildet. Eine Infrastruktur ist niemals Selbstzweck sondern immer Fundament einer übergeordneten „Suprastruktur“, welche von ihr erst ermöglicht und damit zugleich beschränkt und mithin strukturiert wird.

Van Laak (1999: 280 ff.) zufolge entstand der Begriff der Infrastruktur im letzten Viertel des 19. Jahrhunderts im Rahmen eines Eisenbahnprojektes in Frankreich. Die früheste bekannte Verwendung datiert offenbar auf den 13. August 1875. Damals verfaßte ein Sekretär namens M. Aclocque einen Bericht für die Eisenbahnkommis-

sion der französischen Nationalversammlung, in welchem der Begriff erstmals in der heute geläufigen Form Verwendung fand. „Infrastructure“ wird dabei in Abgrenzung zur „superstructure“ (Gleiskörper, Bahnhöfe, Telegraphen etc.) zur Bezeichnung des Unterbaus (Dämme, Brücken, Geländeeinschnitte etc.) herangezogen. Dieses bautechnische Verständnis hält sich bis in die Mitte des 20. Jahrhunderts. Doch die eigentliche Karriere der Wortschöpfung beginnt erst 1950 als die NATO den Begriff in ihren militärischen Sprachgebrauch übernimmt. Vermutlich geschieht dies auf Veranlassung von Jean Monnet, „der für die französische Regierung die Idee zum Infrastruktur-Plan in die NATO eingebracht hatte“ (van Laak 1999: 282). Als Infrastruktur wurden nun unter dem strategischen Gesichtspunkt militärischer Handlungsfähigkeit vor allem die, für eine reibungslos funktionierende Logistik entscheidenden, ortsfesten Objekte verstanden, also

> die Gesamtheit derjenigen Gebäude, Anlagen und Kommunikationsnetze, die für das Nachschubwesen, insbesondere im Hinblick auf die Versendung von Gütern und Nachrichten, erforderlich sind. (Jochimsen 1966: 100)

Beabsichtigt war, vor dem Hintergrund des sich anbahnenden Ost-West-Konfliktes, die Errichtung einer standardisierten und länderübergreifenden militärischen Infrastruktur als zentraler Voraussetzung einer integrierten Verteidigung des Bündnisgebietes. In der Folge erwähnt „Der Große Brockhaus“ (Bd. 5) den Begriff der Infrastruktur bereits 1954 erstmals als

> Unterbau einer Organisation, neuerdings (bei der NATO) zusammenfassende Bezeichnung für militärische Anlagen wie Kasernen, Flughäfen, Tankstellen, Radarstationen u. a.

Im Anschluß diffundierte der Begriff dann im internationalen Sprachgebrauch. Sowohl Montanunion als auch EWG übernahmen ihn, wobei eine inhaltliche Verschiebung seiner Bedeutung erfolgte. Immer häufiger wurde Infrastruktur nun nicht nur aus militärisch-strategischer, sondern vor allem aus ordnungspolitischer Perspektive als Grundlage ökonomischer Prosperität gesehen. Deutlich wird das etwa im Sammelband von Simonis (1977) oder bei Jochimsen (1966) und Frey (1972). Zu Anfang der 1970er Jahre dominiert die wirtschaftliche Konnotation bereits deutlich. In „Meyers Enzyklopädischem Lexikon“ (Bd. 12) von 1974 finden wir Infrastruktur als

> notwendiger Unterbau, der zur wirtschaftl. Entwicklung eines Raumes unabdingbar ist, und zwar die Gesamtheit aller durch den Staat oder andere Gebietskör-

> perschaften des öffentlichen Rechts getragenen Einrichtungen der sog. Vorsorgeverwaltung (z. B. die der Allgemeinheit dienenden Einrichtungen für: Verkehr und Beförderung, Fernsprech- und Fernmeldewesen, Gas-, Wasser- und Elektrizitätsversorgung, Müllabfuhr, Abwasserbeseitigung, Bildung und Kultur, Krankheitsvorsorge und Krankenbehandlung, Totenbestattung).

Über diese Realdefinition hinaus gestaltet sich eine inhaltliche Abgrenzung des Begriffes jedoch schwierig. Gegenwärtig existieren in der wissenschaftlichen Literatur[74] eine Reihe konkurrierender Nominaldefinitionen, denen im Wesentlichen gemein ist, „daß mit Infrastruktur der Rahmen gemeint ist, innerhalb dessen sich das Wirtschaften vollzieht“ (Hedtkamp 1996: 2). Infrastruktur wird hier oftmals aus soziologischer Perspektive systemtheoretisch als funktional notwendiges Subsystem von Wirtschaft und Gesellschaft – gewissermaßen als deren Rückgrat – verstanden (Mayntz 1988b), da sie „die wachstums-, integrations- und versorgungsnotwendigen Basisfunktionen einer Gesamtwirtschaft“ (Jochimsen u. Gustafsson 1977: 38) übernehme. Eine leistungsfähige Infrastruktur ist dann Grundlage der (Privat-)Wirtschaft und damit von öffentlichem – weil gesamtgesellschaftlichem – Interesse. Hieraus erklärt sich, warum Infrastruktursysteme vielfach staatlich organisiert, zumindest jedoch reguliert werden.

Aus wirtschaftswissenschaftlicher Sicht werden Infrastrukturen hingegen vor allem im angelsächsischen Raum gerne als Social Overhead Capital aufgefaßt (Hirschman 1958). Als solches stellen sie ein gesamtgesellschaftlich genutztes Anlagekapital dar, welches eine notwendige Voraussetzung privater Investitionen bildet. Die Abwicklung von Geschäftsprozessen bedingt eben dieses öffentliche Anlagekapital zur Minimierung anfallender Transaktionskosten (Hedtkamp 1996: 11 ff.). Aus dieser Perspektive waren öffentliche Infrastrukturinvestitionen und ihre volkswirtschaftlichen Auswirkungen vor allem während der 1990er Jahre auch Gegenstand ökonometrischer Untersuchungen (Gramlich 1994).

Im Hinblick auf den Infrastrukturkomplex in seiner Gesamtheit kann demnach zwischen einem Kapitalstock und den mit seiner Hilfe bereitgestellten Gütern und Leistungen differenziert werden. Dem materiellen oder physischen Infrastrukturkapital werden dabei gewöhnlich jene Anlagen und Betriebsmittel, die der Energieversorgung, dem Transport und Verkehr, der Telekommunikation, der staatlichen Verwaltung, der

74 Vgl. u. a.: Hirschman (1958), Jochimsen (1966), Frey (1972), Jochimsen u. Gustafsson (1977), Simonis (1977), Frey (1988), Mayntz u. Hughes (1988), Gramlich (1994), Hammer (1995), Hedtkamp (1996), van Laak (1999).

Forschung und Bildung sowie dem Gesundheitswesen dienen, zugerechnet (Jochimsen 1966: 103). Oftmals haben diese Infrastruktureinrichtungen zugleich den Charakter großtechnisch vernetzter Systeme[75] und unterliegen aufgrund ihrer Intradependenz einer technischen Unteilbarkeit. Sie neigen zu Sprungkosten sowie einem hohen Fixkostenanteil, der ausgeprägte Skaleneffekte impliziert und hohe, extrem risikobehaftete Anfangsinvestitionen voraussetzt (Frey 1988: 201). Beides begünstigt die Herausbildung natürlicher Monopole und kann – muß jedoch nicht zwangsweise (vgl. Gans 2001) – zu einem Marktversagen hinsichtlich einer ausreichenden Bereitstellung infrastruktureller Güter führen. Das enge Verständnis von Infrastruktur als materiellem Sachkapital wird gelegentlich noch um ein Konzept des immateriellen Kapitals erweitert. Jochimsen u. Gustafsson (1977: 39) erwähnen hier etwa das Rechtssystem sowie kulturelle Traditionen, aber auch die Bevölkerungsstruktur und das Ausbildungs- bzw. Fähigkeitsniveau einer Gesellschaft (Human Capital).

Die mit Hilfe des Infrastrukturkapitals erzielten infrastrukturellen Güter sind zumeist ökonomisch nur schwer quantifizierbare Größen, die sich bspw. in einem erhöhten Sicherheitsniveau oder einer aus gut ausgebauten Verkehrswegen resultierenden Zeitersparnis manifestieren. Gleichwohl gehen sie als Vorleistungen und/oder relevante Rahmenbedingungen in den Produktionsprozeß fast aller Wertschöpfungsketten einer Volkswirtschaft ein. Der Infrastruktur kommt somit eine gesamtwirtschaftliche Querschnittsfunktion zu, wobei die einzelnen Infrastruktursysteme untereinander vielfach verflochten und teilweise interdependent sind.

Infrastrukturelle Güter können insofern als öffentlich charakterisiert werden, als ein allgemeiner Zugang zu ihnen von makroökonomischem und damit gesamtgesellschaftlichem Interesse ist. Es handelt sich jedoch nicht ohne weiteres auch um „öffentliche Gütern“ im engeren Sinne der Theorie der öffentlichen bzw. kollektiven Güter[76], da viele der infrastrukturellen Güter durchaus einer Zugangsbeschränkung unterliegen können und somit nicht das strenge Kriterium der Nicht-Ausschließbarkeit erfüllen. Auch eine Nicht-Rivalität im Konsum ist häufig nicht gegeben. Gerade bei der Energieversorgung

75 Zum Konzept großtechnischer Systeme sowie deren infrastrukturellen Eigenschaften vgl. insbesondere Mayntz (1988b), Mayntz u. Hughes (1988) und Mayntz (1993).

76 Nach Richter u. Wiegard (1993: 200) wird in Teilen der wirtschaftswissenschaftlichen Literatur zwischen öffentlichen und kollektiven Gütern insofern differenziert, als erstere öffentlich bereitgestellte Güter im allgemeinen, letztere aber nur solche mit den Eigenschaften der Nicht-Ausschließbarkeit und der Nicht-Rivalität im Konsum bezeichnen.

sowie im Transport- und Verkehrswesen sind Engpässe hinlänglich bekannt. Nur sehr wenige Infrastrukturleistungen, wie etwa innere und äußere Sicherheit, entsprechen der engen theoretischen Definition öffentlicher Güter beinahe vollkommen, die überwiegende Mehrzahl hingegen ist von meritorischem Charakter.[77] Diese Güter müssen keineswegs ausschließlich von der öffentlichen Hand bereitgestellt werden. Ihre Produktion bleibt vielmehr oft der Privatwirtschaft überlassen, so z. B. im Falle des Gesundheitswesens oder der Energieversorgung. Ein reines Marktgleichgewicht kann aber auch hier zu einer politisch oder normativ unerwünschten Allokation infrastruktureller Güter der allgemeinen Daseinsvorsorge führen, so daß häufig ein Interesse an staatlicher Intervention oder Regulierung besteht. Insgesamt gesehen zeichnet sich jedoch in jüngster Zeit ein deutlicher Trend zur umfassenden Privatisierung infrastruktureller Einrichtungen ab (vgl. Scheele 1993; Schneider u. Tenbücken 2004).

Infrastrukturen lassen sich somit zusammenfassend als komplex strukturierte Systeme charakterisieren, die einheitliche und im allgemeinen nicht substituierbare Güter und Leistungen dauerhaft für eine große Anzahl von Nutzern bereitstellen (vgl. Hammer 1995). Ein hochgradig ausdifferenzierter infrastruktureller Produktionsprozeß umfaßt dabei typischerweise eine Vielzahl eng gekoppelter Systemkomponenten. Der gesamte Infrastrukturkomplex einer Gesellschaft zerfällt in ein Ensemble sozio-technischer Subsysteme, die auf vielfache Weise physisch und/oder logisch interdependent sind. Aufgrund dieser Interdependenzen kann der Ausfall einzelner Komponenten direkt oder indirekt kaskadierende oder eskalierende Effekte hervorrufen (vgl. Rinaldi et al. 2001). Verläßlichkeit und Funktionssicherheit einer Infrastruktur sind daher für die auf ihr basierende Volkswirtschaft häufig von kritischer, oft sogar existentieller Bedeutung, da die zumeist beträchtlichen ökonomischen Potentiale, die auf der Grundlage infrastruktureller Vorleistungen realisiert werden, nur mit und durch diese Infrastruktur Bestand haben können. Zugleich sind moderne sozio-technische Infrastruktursysteme jedoch aufgrund ihres hohen Komplexitätsgrades oftmals durch ein erhebliches Störpotential sowie eine hieraus resultierende extreme Verwundbarkeit gekennzeichnet (vgl. Mayntz u. Hughes 1988: 235).

77 Meritorische Güter werden hier in Anlehnung an Musgrave (1957, 1959) als Impure Public Goods verstanden. Hedtkamp (1996: 3 f.) weist ferner darauf hin, daß die Zuordnung eines bestimmten Gutes zur Klasse der öffentlichen bzw. meritorischen Güter, bedingt durch technische Entwicklungen sowie sich wandelnde politische Wertvorstellungen, im Laufe der Zeit Verschiebungen unterworfen sein kann.

4.1.2 IuK-Systeme als kritische Querschnittsfunktion

Zu den kritischen[78] Infrastruktursektoren moderner Gesellschaften zählen vor allem die Systeme der Gesundheitsfürsorge (einschließlich der Nahrungs- und Wasserversorgung), der öffentlichen Verwaltung (einschließlich der Sicherheitsorgane), der Rettungs- und Notfalldienste (einschließlich des Katastrophenschutzes), des Transport- und Verkehrswesens, des Bank- und Finanzwesens sowie der Energieversorgung und der Telekommunikation bzw. Informationsverarbeitung.

Ein historischer Rückblick zeigt, daß Zahl und Umfang der für eine Gesellschaft kritischen Infrastruktursysteme offenbar proportional zu deren Komplexität und Entwicklungsniveau ansteigt (vgl. Abbildung 4.1). Basieren urzeitliche Gesellschaftsformen, wie Großfamilien oder Stammesverbände, lediglich auf der Infrastruktur einer gemeinsamen Gesundheitsfürsorge (Lagerplatz und Nahrungsmittelversorgung), so benötigen die ersten Stadtstaaten bereits eine funktionierende öffentliche Verwaltung (Krieger- und/oder Priesterkaste) sowie ein – wenn auch rudimentäres – Rettungswesen zur Brand- und Seuchenbekämpfung. In den territorial ausgedehnten antiken Großreichen kommen Einrichtungen zum Transport und Verkehr von Waren und Truppen hinzu. Gesellschaften mit weiter ausdifferenzierten Handwerkszweigen, wie wir sie aus dem Spätmittelalter und der Zeit des Merkantilismus kennen, verfügen ferner über ein – den Austausch einer Vielzahl von Gütern erleichterndes – Bank- und Finanzwesen. Industrielle Gesellschaften erfordern darüber hinaus ein umfangreiches System der Energieversorgung. Moderne Wissensgesellschaften schließlich wären ohne Informations- und Kommunikationssysteme undenkbar.

Für jede Entwicklungsstufe gilt dabei offenbar, daß das sie jeweils tragende Infrastruktursystem, samt aller Infrastruktursysteme der darunter liegenden Stufen, eine unabdingbare Voraussetzung der Erhaltung des jeweils erreichten Entwicklungsniveaus darstellt. Ferner beruhen in präindustriellen Gesellschaften sämtliche infrastrukturellen Produktionsprozesse zu einem wesentlichen Teil auf menschlicher und/oder tierischer Muskelkraft und bedingen sich daher nur zu einem geringen Grade wechselseitig. Nach der industriellen Revolution jedoch lassen selbsttätige Maschinen die Muskelkraft als zentralen Antriebsfaktor im Fertigungsprozeß in den Hintergrund treten. Weil diese Maschinen jedoch eine stetige Energiezufuhr benötigen, sind die neu

78 Zu den Begriffen der „Kritizität“ und „Kritikalität“ sowie zu einer möglichen Operationalisierung vgl. Reinermann u. Weber (2004).

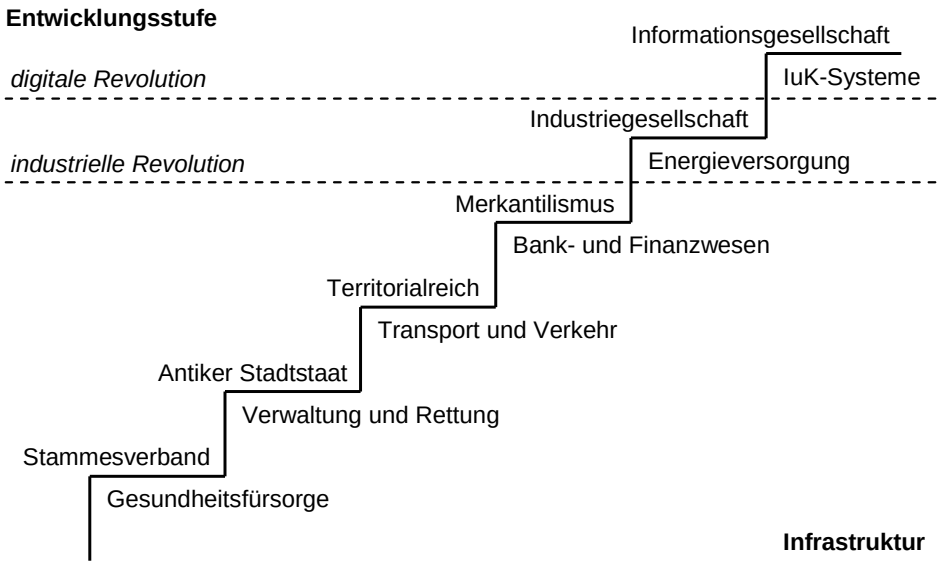


Abbildung 4.1: *Entwicklungsstufen und kritische Infrastruktursektoren*

hinzukommenden Systeme der Energieversorgung Infrastrukturen einer höheren Ordnung, da sie zur zentralen Voraussetzung aller anderen Infrastruktursysteme werden. Als „Meta-Infrastruktur" nehmen sie eine auch für alle anderen Infrastruktursysteme kritische Querschnittsfunktion wahr. Gleiches gilt für elektronische IuK-Systeme im Hinblick auf die Informationsgesellschaft. Diese automatisieren nun auch einen Großteil der bisher allein dem menschlichen Verstand vorbehaltenen intellektuellen Arbeit. In der Folge einer allgemeinen Informationalisierung, also einer zunehmenden informationstechnischen Durchdringung aller Lebensbereiche, wird die von IuK-Systemen als „‚intelligenten' Infrastrukturen" (Willke 2001: 306) erbrachte Steuerungsleistung damit auch zur Conditio sine qua non der Operabilität aller anderen Infrastrukturen (vgl. Abbildung 4.2).

Zugleich erhöht sich durch eine zunehmende informationstechnische- und logistische Vernetzung von Produktionsprozessen in modernen Gesellschaften ganz allgemein der Grad der Inter- und Intradependenz kritischer Infrastrukturen (Rinaldi et al. 2001; Rathmell 2001). Es liegt auf der Hand, daß den elektronischen Systemen der Information und Kommunikation hierbei eine besonders exponierte Querschnittsfunktion in der Architektur des Infrastrukturgefüges zukommt (vgl. Cerny 2000). Als Nervenbahnen der Informationsgesellschaft bilden sie buchstäblich den neuralgischen Punkt des gesamten Infrastrukturkomplexes und sind daher gesamtgesellschaftlich von stra-

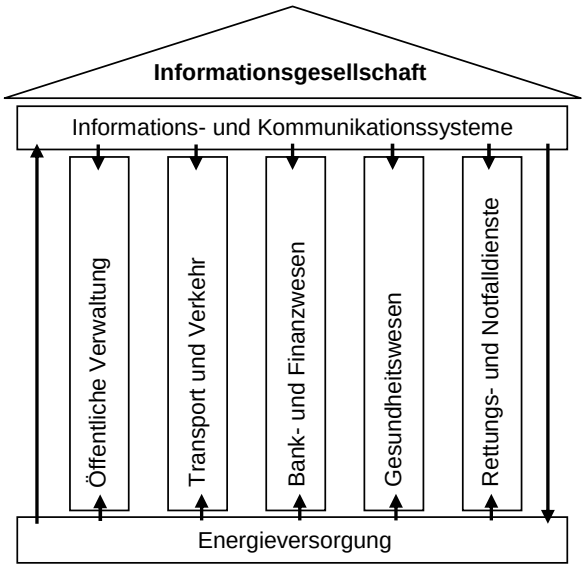


Abbildung 4.2: *Das Infrastrukturgefüge in der Informationsgesellschaft*

tegischem Interesse. Aufgrund der weitreichenden globalen Vernetzung dieser Systeme gewinnt das Problem ihres Schutzes vor diesem Hintergrund zugleich eine inter- bzw. transnationale Dimension (vgl. Sofaer u. Goodman 2001a; Beer 2004). Nicht zuletzt deshalb wird seit den 1990er Jahren der Ausbau und Schutz vernetzter IuK-Systeme nicht nur unter dem Stichwort der „Nationalen Informations-Infrastruktur“ (NII), sondern vermehrt auch unter den Gesichtspunkten einer „Globalen Informations-Infrastruktur“ (GII) in Wirtschaft, Politik und Wissenschaft diskutiert (Carbo u. Wallace 1997; James 2001; Hunker 2002).[79]

4.1.3 IuK-Systeme als Basis des eCommerce

Die fortschreitende Informationalisierung der Gesellschaft impliziert selbstverständlich nicht nur eine zunehmend kritische Rolle von IuK-Systemen im Rahmen des Infrastrukturgefüges, sondern auch eine verstärkte Verlagerung allgemeiner wirtschaftlicher

79 Den Anfang machten hier die USA mit dem unter der Clinton/Gore-Administration 1993 initierten „National Information Infrastructure Program“, in dessen Kontext vor allem Vizepräsident Albert Gore das Schlagwort vom „Information Superhighway“ prägte. Schon 1994 zog dann die Europäische Union mit einem Aktionsplan unter dem Titel „Europe and the Global Information Society“ nach. Dieser wurde von einer Arbeitsgruppe unter dem Vorsitz des Vizepräsidenten der Europäischen Kommission, Martin Bangemann, verfaßt und ist daher auch als „Bangemann-Report“ bekannt.

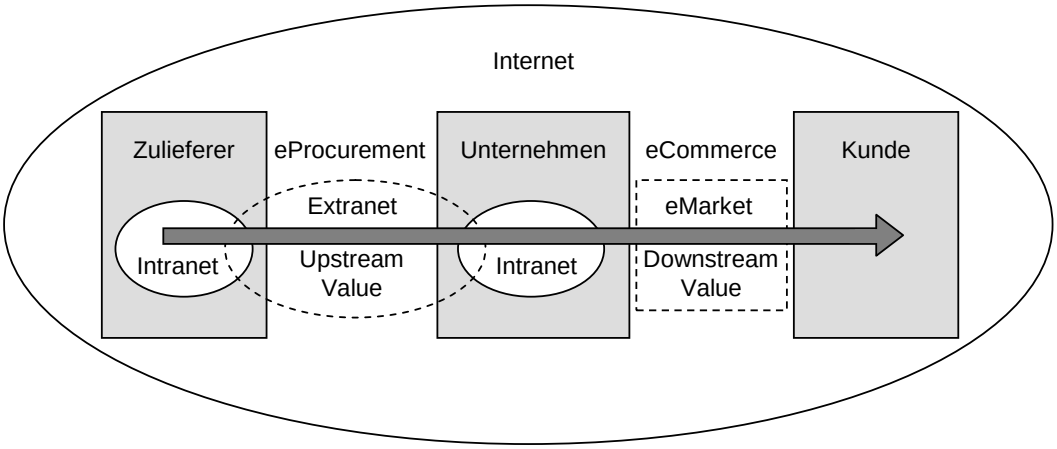


Abbildung 4.3: *Die Wertschöpfungskette im eBusiness*

(Trans-)Aktionen auf die Plattform kritischer Informationsinfrastrukturen. Dies gilt vor allem für das Internet. IuK-Systeme können dabei sowohl zur Unterstützung unternehmensinterner als auch -externer Prozesse herangezogen werden. Ihr Einsatz erhöht nicht nur die Markttransparenz und in der Folge den Druck zur Rationalisierung, sondern eröffnet auch neue Spielräume hinsichtlich der Aufbau- und Ablauforganisation in Unternehmen und zieht daher oftmals eine fundamentale Restrukturierung der gesamten Wertschöpfungskette nach sich. So ermöglicht die erweiterte Kontroll- und Steuerungskapazität von IuK-Systemen bspw. eine vermehrte Ausgliederung von Geschäftsprozessen, während durch die mit diesen Systemen einhergehende Verdichtung von Raum und Zeit zugleich neue Möglichkeiten des Direktvertriebes geschaffen werden (vgl. Greenstein u. Vasarhelyi 2002: 25 ff.). Beruhen Geschäftsprozesse auf elektronischen IuK-Systemen als integralem Bestandteil, so wird gemeinhin von „electronic Business“ (eBusiness) gesprochen. Abbildung 4.3 exemplifiziert den Aufbau einer allgemeinen Wertschöpfungskette im eBusiness.

Sofern unternehmensintern eingesetzte IuK-Systeme auf dem Internetprotokoll basieren, aber von außerhalb nicht frei zugänglich sind, werden diese als „Intranet“ bezeichnet. Sind zwei oder mehr Intranets exklusiv über das Internet derart miteinander verbunden[80], daß sie ein in sich geschlossenes, logisches Netz bilden, so spricht man von einem „Extranet“. Extranets spielen im Rahmen des eBusiness vor allem hinsichtlich

80 Eine solche Verbindung ist bspw. mittels einer Tunnelung über Virtual Private Networks (VPN) realisierbar.

elektronischer Beschaffungssysteme (eProcurement) eine zentrale Rolle. Im Unterschied hierzu werden unter „electronic Commerce“ (eCommerce) diejenigen wirtschaftlichen Transaktionen verstanden, die über einen elektronischen Markt (eMarket) abgewickelt werden. Kennzeichnend für elektronische Märkte ist dabei, daß die Koordinationsfunktionen des Marktes ganz oder teilweise über IuK-Systeme realisiert werden (Semar 2001: 13).

Nach Lincke (1998) sowie Latzer u. Schmitz (2002: 11 f.) lassen sich prinzipiell vier Phasen einer Transaktion am Markt unterscheiden:

1. *Information:* Anbieter werben für ihre Produkte und potentielle Kunden verschaffen sich einen Marktüberblick
2. *Vereinbarung:* Käufer und Verkäufer einigen sich vertraglich auf konkrete Konditionen
3. *Abwicklung:* Lieferung und Bezahlung der Ware
4. *After-Sales:* mittel- bis langfristige Kundenbetreuung

In jeder dieser Phasen können elektronische IuK-Systeme sowie auf ihnen basierende künstliche Agenten unterstützend eingesetzt werden. Je nachdem ob dies in allen Phasen der Fall ist, oder ob eine Unterstützung nur in einigen Phasen realisiert wird, kann dann von eCommerce im engeren bzw. weiteren Sinne gesprochen werden.

Der Sache nach eignen sind für den elektronischen Handel in Sonderheit Standardgüter, da ein potentieller Kunde diese in der Informationsphase aufgrund ihrer allgemein bekannten und gleichbleibenden Eigenschaften nicht unmittelbar in Augenschein zu nehmen braucht. Elektronische Produktkataloge und Suchmaschinen können hier die Funktion traditioneller Märkte hervorragend substituieren. Auch die in der Phase der Vereinbarung auftretende Kommunikationsbeziehung läßt sich dann problemlos in IuK-Systemen abbilden.

Handelt es sich bei der Ware zusätzlich um ein digitales Gut[81], im weiteren Sinne also um Information, so kann ferner auch deren Lieferung auf elektronischem Wege erfolgen. Aus dem selben Grunde bereitet auch eine elektronische Abwicklung des Bezahlvorgangs technisch keine Schwierigkeiten, da das in aller Regel verrechnete Giralgeld

81 Digitale – oder vielmehr digitalisierbare – Güter sind immaterielle Güter bzw. Dienstleistungen, die sich als Folge diskreter Symbole oder Zeichen darstellen lassen, wie das bspw. bei Texten, Musik, Bildern oder ganz allgemein jeder anderen Form von Information der Fall ist (vgl. Stelzer 2000).

ebenfalls die Eigenschaften eines digitalen Gutes aufweist. Zur Auslieferung physischer Güter hingegen muß in der Phase der Abwicklung auf logistische Kapazitäten zurückgegriffen werden. Nach Alt u. Schmid (2000) kann allerdings ein koevolutiver Gleichschritt von Informations- und Transporttechnologie vorausgesetzt werden, so daß das Niveau der Logistik einer Volkswirtschaft i. d. R. mit dem jeweiligen Entwicklungsstand ihrer IuK-Technologie korrespondiert. Schließlich sind auch Maßnahmen des After-Sales, wie etwa Reklamationen oder Support-Dienstleistungen, auf elektronischem Wege denkbar.

Selbstverständlich können elektronische Transaktionen nicht nur zwischen Unternehmen und Endverbraucher (Business-to-consumer; B2C) abgewickelt werden, sondern auch zwischen Unternehmen (Business-to-Business; B2B), Privatpersonen (Consumer-to-Consumer; C2C) sowie im Rahmen eines öffentlichen Verwaltungsaktes (Government-to-Constituent; G2C) (vgl. Belanger et al. 2002). Letzteres kann auch als Spezialfall des „electronic Government“ (eGovernment) betrachtet werden.

4.2 Das Bedrohungsszenario Cybercrime

4.2.1 Das Themenfeld

Kritische Informationsinfrastrukturen sind, angesichts ihres hohen Komplexitätsgrades, in vielfacher Weise verwundbar (Schmitz 2004; Geiger 2000: 156 ff.). Konkrete Gefährdungen für die Funktionssicherheit kritischer Informationsinfrastrukturen können ganz allgemein sowohl aus intendierten wie unintendierten Handlungen Dritter, als auch aus den Zufällen höherer Gewalt resultieren. Hinsichtlich intendierter Handlungen kann vor diesem Hintergrund ferner zwischen solchen Bedrohungen, die sich unmittelbar gegen die physischen Anlagen und Betriebsmittel der IuK-Systeme richten, und solchen, die sich innerhalb des virtuellen Interaktionsraumes des Cyberspace selbst auf einer rein logischen Ebene ergeben, differenziert werden. Während ersteren weitgehend mit den Mitteln des traditionellen Objektschutzes zu begegnen ist, stellen letztere eine qualitativ neue Herausforderung für den Schutz kritischer Informationsinfrastrukturen dar.

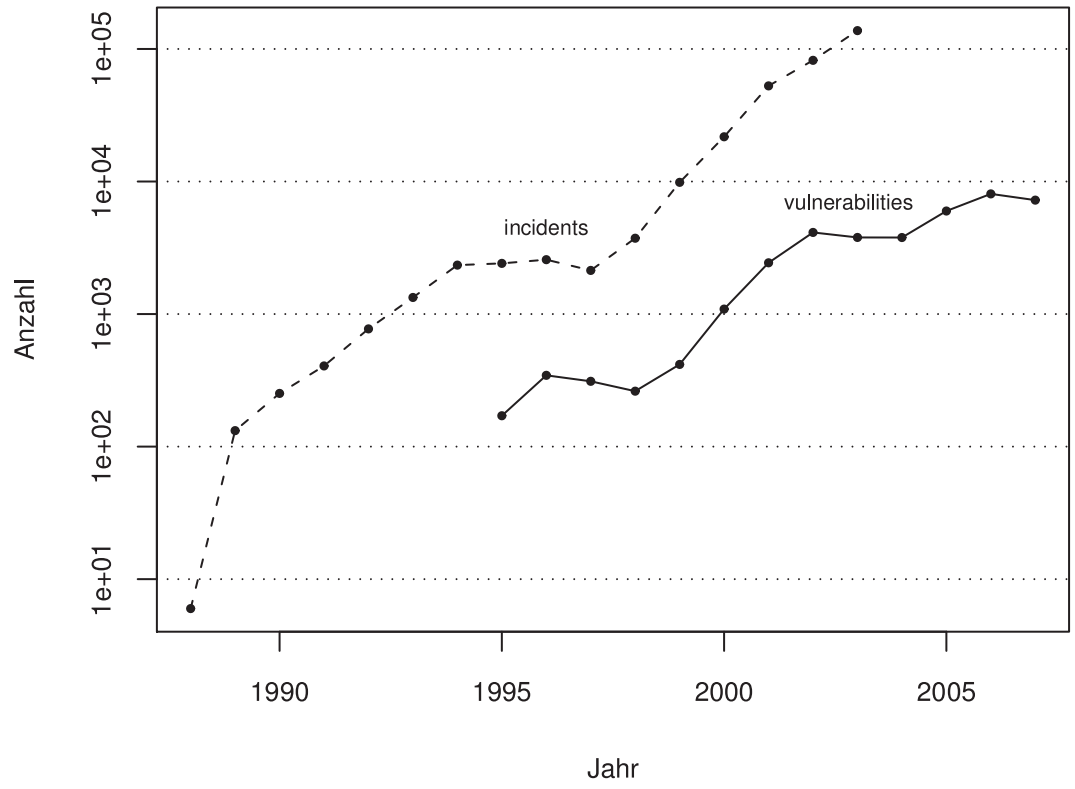
Zu den intendierten Bedrohungen im virtuellen Interaktionsraum gehören verschiedene Spielarten des „Cybercrime“, die oft auch synonym als Computer-, Internet- oder High-Tech-Kriminalität bezeichnet werden. Daneben existieren ferner in einer etwas anderen Konnotation die Begriffe des „Cyberterrorism“ sowie des „Cyberwar“. Obwohl sich diese Terminologie in den letzten Jahren im sicherheitspolitischen Diskurs weitge-

hend etablieren konnte, fehlt in der Literatur bislang dennoch eine allgemein anerkannte Definition des exakten Bedeutungsumfanges der einzelnen Begriffe.[82] Da sich die mit ihnen umschriebenen Formen krimineller – weil Dritte schädigender – Handlungen im Cyberspace zwar hinsichtlich ihrer Urheber und deren Motivationsstruktur deutlich unterscheiden mögen, bezüglich der angewandten Methoden und erzielten Auswirkungen jedoch ein hohes Maß an Übereinstimmung aufweisen, werden diese im Folgenden zusammenfassend unter dem einheitlichen Überbegriff des Cybercrime subsumiert. Eine solche Vorgehensweise erscheint nicht zuletzt deshalb gerechtfertigt, weil sich Urheber und Motiv eines Angriffs im Cyberspace oft nicht eindeutig ermitteln lassen (vgl. Thomas u. Loader 2000: 3). Gemein ist diesen kriminellen Handlungen jedoch in jedem Falle ihr Bezug zu vernetzten Computersystemen (Sieber 2008: 131).

In der Literatur gibt es, wie erwähnt, eine Vielzahl konkurrierender Definitionen des Begriffs Cybercrime (vgl. Groebel et al. 2001: 17 ff.; Yar 2006: 9 ff.). Unter Cybercrime im weiteren Sinne werden dabei ganz allgemein jene intendierten Handlungen bzw. Angriffe verstanden, die unter Zuhilfenahme von IuK-Systemen erfolgen und bewußt Dritte schädigen. Wall (2007: 49 f.) differenziert ferner zwischen „computer integrity crime“, „computer-assisted crime“ und „computer content crime“. Nur Straftaten gegen die Integrität eines IuK-Systems, also solche die auf einen unberechtigten Zugriff auf die Daten eines IuK-Systems oder dessen Funktionsstörung abzielen, sind jedoch kritisch für die Funktionssicherheit von Informationsinfrastrukturen. Kriminelle Handlungen, deren Auswirkungen sich hingegen nicht unmittelbar gegen diese Informations- und Kommunikationssysteme selbst richten, sondern diese nur als Mittel bzw. „Tatwerkzeug“ (Wiedemann 2000) zur Begehung einer herkömmlichen Straftat nutzen, sind für die Funktionssicherheit kritischer Infrastrukturen letztlich nicht von Bedeutung und spielen daher im Kontext der vorliegenden Untersuchung nur eine untergeordnete Rolle.

Die in Computernetzen verbreiteten kriminellen Techniken werden in der Literatur ausführlich behandelt, so etwa bei Kaufman et al. (1995: 18 – 19), Schwartau (2000), Felzmann (2000), Philippsohn (2001), Groebel et al. (2001), Furnell (2002: 143 ff.), Dornseif (2005), Yar (2006) und Wall (2007). Bei Kyas u. a Campo (2002: 43 ff.) findet sich eine Beschreibung ihrer Entstehungsgeschichte sowie eine umfangreiche Zusammenstellung bedeutender Vorfälle zwischen 1961 und 2001 (a. a. O.: 49 – 54). Aufgrund der hohen Flexibilität und Eigendynamik vernetzter IuK-Technologien sind die Mög-

82 Zu den unterschiedlichen Begriffsabgrenzungen vgl. bspw. Furnell (2002: 21 ff.).



Datenquelle: CERT/CC Statistics <http://www.cert.org/stats/>
Anmerkung: Die Ordinate ist aufgrund des stark exponentiellen Verlaufs logarithmisch skaliert.

Abbildung 4.4: *Anzahl der beim CERT/CC gemeldeten Sicherheitslücken und -vorfälle*

lichkeiten des Mißbrauchs allerdings tendenziell nahezu unbegrenzt.

Ein immer extensiverer und mit zunehmender Komplexität oftmals fehlerbehafteter Programmcode führt, bei gleichzeitiger Akzeleration der Innovationszyklen, permanent zum Auftreten neuer Vulnerabilitäten, die aufgrund vorherrschender Monokulturen in der Software-Landschaft einen hohen Verbreitungsgrad erreichen. Auf technischer Ebene erschwert dieser Umstand die Identifikation, Analyse und Behebung von Fehlerquellen im Design oder der Implementierung sowie bei der Installation und der Konfiguration einer neuen Anwendung, während er in sozialer bzw. organisatorischer Hinsicht ein umfassendes Verstehen und Beherrschen der oft umfangreichen Funktionalität eben dieser Anwendung durch deren Nutzer kaum noch zuläßt, so daß auch hier aus mangelndem Wissen und fehlerhafter Bedienung Sicherheitslücken resultieren (vgl. Winkel 2000; Hutter 2002). Ein dank weitgehender Automatisierung erreichtes, hohes Maß an

Abbildung 4.5: *Das Themenfeld*

Bedienkomfort ermöglicht dabei zwar einerseits einem immer umfangreicheren Kreis auch technisch nicht versierter Nutzer den Zugang zu hoch komplexen Anwendungen, entzieht jedoch andererseits dem Nutzer die direkte Kontrolle systemnaher Prozesse und eröffnet damit zusätzliche Sicherheitsrisiken.[83] Die in Abbildung 4.4 dargestellten Zeitreihen verdeutlichen, daß sowohl die Anzahl der Sicherheitslücken als auch -vorfälle hierbei drastisch ansteigt.

Unter Ausnutzung immer neuer Verwundbarkeiten ergibt sich so ein facettenreiches Spektrum möglicher Angriffsvektoren. Dieses unterliegt aufgrund der hohen Variabilität seiner Umwelt zugleich einem stetigen Wandel, da es das Schließen bekannter sowie das Entstehen neuer Sicherheitslücken beständig nachvollzieht, wodurch die Herausbildung einer allgemeinen Taxonomie krimineller Techniken im Cyberspace erschwert wird. Abbildung 4.5 strukturiert das Themenfeld Cybercrime als Momentaufnahme in Form einer Mindmap (vgl. Downs u. Stea 1977), um einen vorläufigen Überblick zu erhalten.

4.2.2 Angriffsvektoren in elektronischen Netzwerken

Abbildung 4.6 veranschaulicht die Häufigkeit verschiedener Arten des Angriffs in elektronischen Netzwerken im Laufe der letzten Jahre. Nicht selten wird bei solchen Angriffen versucht, Programmroutinen mit Schadensfunktion (Malware) auf den angegriffenen Rechnern zu etablieren. Eine zentrale Rolle kommt dabei dem selbst-replizierenden Code sog. Viren und Würmer zu:[84]

- Als nicht eigenständig lauffähiger Code „infizieren“ *Computerviren*[85] – in Analogie zu ihren biologischen Vorbildern – ein Wirtsprogramm durch Einbindung eigener Befehlssequenzen. Mit dessen Aufruf gelangt dann auch der Code des Virus zur Ausführung und kann auf diese Weise weitere Programme infizieren, sich also selbst reproduzieren. Verbreitet werden Viren durch die Weitergabe infizierter Programme. Neben den File-Viren, die normale Anwendungsprogramme infizieren, können die Spezialtypen der Boot- und Makro-Viren unterschieden werden. Erstere befallen jene basalen Programme eines Betriebssystems, die im Boot-Sektor eines Datenträgers liegen und

83 So bietet etwa das automatische Öffnen und Anzeigen von eMail-Anhängen einen zusätzlichen Bedienkomfort, dient jedoch zugleich als Einfallstor für Viren und Würmer.

84 Zur jeweils aktuellen Bedrohungslage vgl. <`http://www.trendmicro.com/map/`>.

85 Die Bezeichnung „Virus“ geht auf die 1984 von Fred Cohen veröffentlichte Arbeit „Computer Viruses – Theory and Experiments“ zurück (Felzmann 2000: 82).

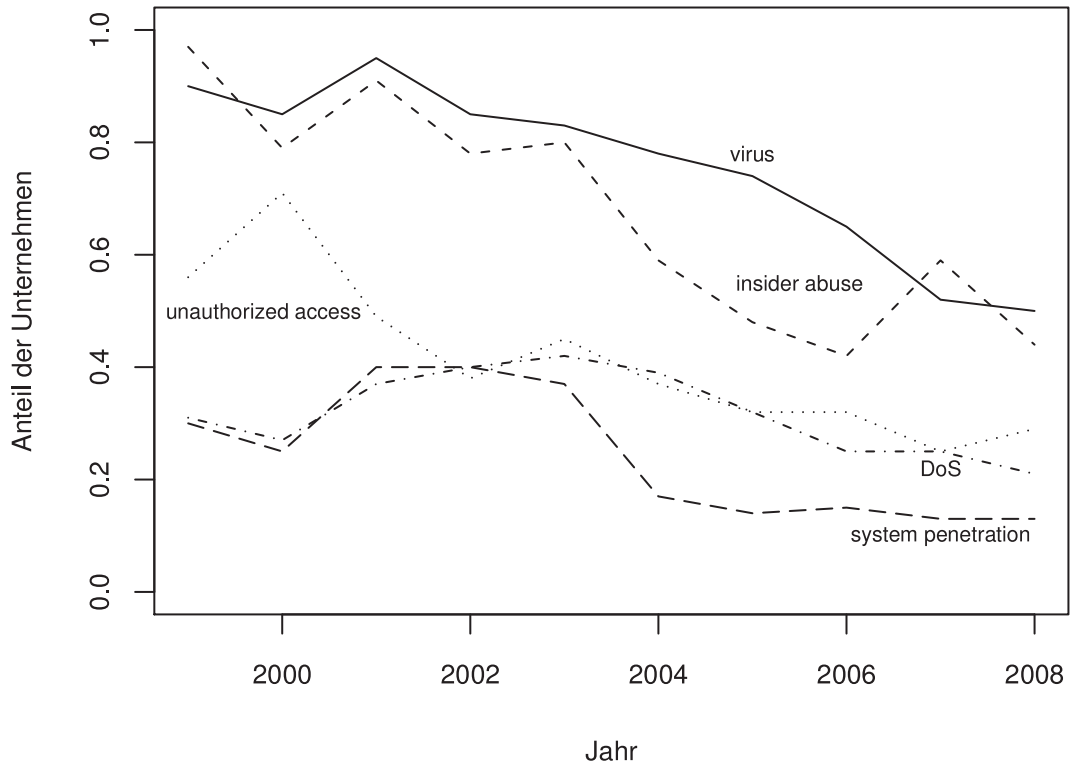
daher beim Systemstart automatisch aufgerufen werden und während der gesamten Laufzeit des Systems im Hintergrund aktiv sind, während letztere sich die mittlerweile in vielen Anwendungsprogrammen existierenden Makro- und Skript-Sprachen zu Nutze machen, um über – scheinbar harmlose – interpretierbare Datendateien zu diffundieren. Eine ausgesprochen raffinierte Variante sind ferner die sog. „polymorphen" Viren, die ihren eigenen Code unter Beibehaltung ihrer Kernfunktionalität permanent restrukturieren. Ähnlich dem biologischen AIDS-Virus wird durch die anhaltende Veränderung des „Phänotyps" so eine verbesserte Camouflage erreicht. Häufig steht der Begriff des Computervirus allerdings auch ganz allgemein Pars pro toto für sämtliche Arten schädlicher Programmroutinen.

- Im Unterschied zu Viren sind *Würmer* eigenständige Programme, die sich selbständig über Computernetzwerke verbreiten. Dies geschieht bspw. über automatisch versandte eMail-Anhänge, die vom ahnungslosen Empfänger geöffnet und damit zur Ausführung gebracht werden. Nach seiner Aktivierung nutzt der Wurm dann das infizierte System als Plattform zur weiteren Diffusion im Netzwerk. Mit der zunehmenden Vernetzung von Rechnern gewinnen Würmer im Vergleich zu Viren an Bedeutung.

Selbst wenn Viren und Würmer außer ihrem Reproduktionsmechanismus keine weiteren unmittelbaren Schadensfunktionen implementieren, so entfalten sie dennoch schon allein aufgrund ihres Ressourcenverbrauchs an Rechen-, Speicher- und/oder Übertragungskapazitäten mittelbar negative Wirkungen.[86] Oftmals dienen sie allerdings zugleich als Träger spezifischer Schadensfunktionen. Solche Schadensfunktionen können auch bereits von vornherein intentionaler Bestandteil einer Software sein:

- Implementieren scheinbar oder tatsächlich nützliche Programme zusätzlich verdeckte Schadensfunktionen, so werden diese – in offensichtlicher Anspielung auf die griechische Mythologie – als *Trojanisches Pferd* bezeichnet. Anders als Viren und Würmer werden Trojanische Pferde vom Nutzer in Unkenntnis dieser Funktionen absichtlich und bewußt auf dem Ziel-System zur Ausführung gebracht.

86 Bekanntestes Beispiel ist hier wohl der sog. Morris- bzw. Internet-Wurm, dessen Urheber Robert T. Morris damals Student an der Cornell University war. Obwohl der Wurm von Morris ursprünglich lediglich zu Versuchszwecken und ohne intendierte Schadensfunktion entworfen worden war, geriet er aufgrund eines logischen Programmierfehlers außer Kontrolle. Anstatt sich auf jedem System nur ein einziges Mal zu replizieren, befiel der Wurm auch bereits infizierte Server solange erneut, bis diese unter der Last des sich akkumulierenden Ressourcenverbrauchs zusammenbrachen. Im November 1988 wurden so innerhalb kürzester Zeit mehrere Tausend UNIX-Server lahmgelegt, wobei ein Schaden in Millionenhöhe entstand. Dieser bis dahin ungewöhnlich hohe Schaden wurde schließlich zum auslösenden Momentum für die Gründung des CERT/CC. Zu den technischen Spezifika dieses Wurms vgl. Spafford (1991).



Quelle: In Anlehnung an Computer Security Institute (2008: 15).

ABBILDUNG 4.6: *Entdeckte Angriffe in US-Unternehmen nach dem CSI-Survey*

- Eine besondere Form des Trojanischen Pferdes ist sog. *Spyware*, mittels derer sich Dritte Daten über das individuelle Nutzungsverhalten eines Anwenders verschaffen. Dies geschieht i. d. R. zum Zwecke einer spezifischen Bewerbung.

Zu den verschiedenen Typen von Schadensfunktionen, die u. a. mittels Viren, Würmern oder Trojanischen Pferden auf einem System etabliert werden können, zählen vor allem *Backdoors*, *Logic Bombs*, *Sniffer* sowie *Bots*[87]:

- Eine *Backdoor* ermöglicht Dritten den unbefugten Fernzugriff auf ein System oder dessen Funktionen zu einem beliebigen Zeitpunkt, indem gezielt eine technische Sicherheitslücke eröffnet wird.
- Bei *Logic Bombs* handelt es sich um eine Schadensfunktion, die in Abhängigkeit vom Eintreten eines bestimmten (logischen) Ereignisses ausgelöst

87 *Bot* steht als Kurzform für *Robot*.

wird. Häufig ist dieses Ereignis ein spezifisches Datum oder ein spezifischer Systemzustand.

- *Sniffer* sind Schnüffelprogramme, die ein verdecktes Mitlesen bzw. Aufzeichnen ein- und/oder ausgehender Daten an den Schnittstellen eines Systems erlauben. Meist werden sie verwandt, um in den Besitz geheimer Zugangscodes zu gelangen.
- *Bots*, im Hacker-Jargon teilweise auch als *Zombies* oder *Drones* bezeichnet, sind Programme, die selbsttätig Aufgaben im Netzwerk erledigen. Oft implementieren sie Ansätze adaptiver Intelligenz, die ihnen in begrenztem Umfang eine autonome Entscheidungsoptimierung ermöglichen. Gewöhnlich werden *Bots* eingesetzt, um das Internet automatisch nach bestimmten Informationen zu durchforsten. Allerdings können sie auch zum illegalen Abschöpfen von Informationen oder zur Durchführung eines Angriffs auf Dritte mißbraucht werden.

Alle bisher genannten Angriffsmethoden beruhen ganz wesentlich darauf, daß es gelingt, Programmcode mit integrierter Schadensfunktion (*Malware*) auf dem angegriffenen System zu etablieren. Allerdings ist es auch möglich, sich ohne die vorherige Platzierung solcher Schadensroutinen Zugang zu einem fremden System zu verschaffen:

- Beim *Password Cracking* wird versucht, einen bestehenden Paßwortschutz mit technischen Mitteln zu knacken. Hierzu werden systematisch alle möglichen Zeichenkombinationen erprobt (*Brute Force Attack*). Ein Blick in die Kombinatorik lehrt allerdings, daß bei einem solchen Vorgehen mit zunehmender Paßwortlänge die durchschnittlich benötigte Zeit exponentiell ansteigt. Selbst bei hoher Rechenkapazität stößt ein solches Verfahren bei ausreichender Länge des Paßwortes schnell an seine Grenzen. Um dieses Problem zu umgehen, verwenden Angreifer oftmals alternative Listen häufig vorkommender Zeichenkombinationen (lexikalischer Angriff).
- Beim *Spoofing* versucht der Angreifer, unter technischer Vortäuschung einer falschen Identität (Maskerade), Zugang zu einem System zu erhalten. Hierzu wird bspw. die IP-Quelladresse der eigenen Datenpakete so verändert, daß das angegriffene System diese irrtümlich einem vertrauenswürdigen Absender zuordnet (vgl. Fuhrberg et al. 2001: 59 ff.).
- Dem *Spoofing* eng verwandt ist das *Mis-* bzw. *Rerouting*. Der ausgehende Datenverkehr des angegriffenen Systems wird ganz oder teilweise so umgeleitet, daß er anstelle des ursprünglichen Bestimmungsortes im Rechner eines Dritten aufläuft oder vollkommen im Netz verloren geht. Möglich wird dies zumeist durch Manipulationen an der Software jener Vermittlungsrechner (*Router*), die für die Weiterleitung von Datagrammen im Netz verantwortlich sind.

- Beim *Pharming*[88] surft der Nutzer eines angegriffenen Systems nur scheinbar auf der von ihm aufgerufenen originären WWW-Seite, tatsächlich aber wird er auf eine täuschend echte Kopie dieser Seite in einem vom Angreifer kontrollierten Pool von Servern – einer „Server-Farm" – umgeleitet, wodurch der Angreifer in den Besitz der eingegebenen Daten gelangt. Hierzu werden die vom WWW-Browser des angegriffenen Systems aufgerufenen DNS-Adressen nicht in ihre eigentlich korrespondierenden IP-Adressen, sondern in die der „Server-Farm" aufgelöst. Möglich wird dies durch eine Manipulation des DNS-Servers oder des WWW-Browsers. Letzteres kann bspw. durch Viren und Würmer erfolgen.
- Im Falle eines *Exploits* nutzt der Angreifer bekannte Schwächen, Fehlfunktionen und Sicherheitslücken der auf einem Ziel-System installierten Programme, die die Ausführung schädlicher Funktionen ermöglichen. Häufig beruht dieses Vorgehen auf dem absichtlichen Auslösen eines Speicherüberlaufs. Ein solcher Überlauf entsteht, wenn der von einem Programm zur Ablage seiner Daten vorgesehene Speicherplatz durch große Datenmengen überschritten wird. Die überschüssigen Daten werden dann bei fehlerhaftem Speichermanagement in nicht dafür vorgesehene Speicherbereiche geschrieben und können dort die Ausführung des Programms in einem vom Angreifer beabsichtigten Sinne beeinflussen (vgl. Fuhrberg 2000: 95).

Neben diesen rein technischen Methoden des nicht autorisierten Zugriffs auf ein System oder dessen Daten gibt es noch eine Reihe weiterer Angriffstechniken, die sich primär auf das soziale bzw. organisatorische Umfeld eines IuK-Systems konzentrieren und dementsprechend als *Social Engineering* bezeichnet werden (vgl. Rustemeyer 2004):

- In seinen Ausmaßen häufig unterschätzt wird der *Interne Mißbrauch* von IuK-Systemen durch zugangsberechtigte Mitarbeiter bzw. Innentäter (vgl. Randazzo et al. 2004).[89] Typische Beweggründe sind private Bereicherung, Bestechlichkeit und persönliche Rache.
- *Impersonation*: Durch Vorspiegelung einer falschen Identität (*Maskerade*) werden zugangsberechtigte Personen unter Ausnutzung ihrer Gutgläubigkeit vom Angreifer zur Herausgabe vertraulicher Authentifizierungsdaten veranlaßt.
- Eine in letzter Zeit vermehrt auftretende, spezielle Form der Impersonati-

88 *Pharming* ist ein Kunstwort, das sich aus den Begriffen „Password" und „Farming" zusammensetzt.

89 Kyas u. a Campo (2002: 34 f.) verweisen in diesem Zusammenhang auch auf eine erhöhte Verwundbarkeit durch die zunehmende Verbreitung von Heimarbeitsplätzen, an denen IuK-Systeme für Dritte besonders leicht zugänglich sind.

on ist das sogenannte *Phishing*[90]. Über eine eMail mit falscher Absender-Identität wird der Empfänger auf eine von Dritten betriebene Internetseite gelockt und dort zur Eingabe seiner Authentifizierungsdaten veranlaßt.

- Darüber hinaus existieren noch weitere Formen des unberechtigten Zugriffs auf Authentifizierungsdaten. Zu nennen ist hier etwa das Durchsuchen von Büroabfällen nach nicht sachgemäß vernichteten Zugangsdaten (*Dumpster Diving*) sowie die *Bestechung* und/oder *Erpressung* zugangsberechtigter Personen.

Die mit einem unberechtigten Zugriff auf fremde Daten verbundenen Absichten des Angreifers sind oft vielfältig und können von Spionage bzw. Diebstahl über Manipulation und Fälschung bis zur Vernichtung von Daten reichen. Häufig wird allerdings auch die vorübergehende Störung der Leistungserbringung eines IuK-Systems bezweckt:

- Bei einem *Denial-of-Service*-Angriff (DoS-Attack) versucht der Angreifer die Funktion eines IuK-Systems ganz oder teilweise zum Erliegen zu bringen, indem er bspw. einen Systemabsturz oder eine Endlosschleife herbeiführt. Eine weitere Möglichkeit ist die Überlastung eines Systems durch eine Vielzahl gleichzeitiger Anfragen. Kommen diese konzertiert von mehreren Rechnern, so handelt es sich um einen *Distributed-Denial-of-Service*-Angriff (DDoS-Attack). Einem solchen verteilten Angriff geht i. d. R. die Übernahme einer großen Anzahl von Rechnern im Netzwerk, etwa mit Hilfe von Viren, Würmern oder Trojanischen Pferden, voraus. Von diesen kompromittierten Plattformen aus wird dann, zumeist ohne Wissen der Betreiber, der DDoS-Angriff auf das eigentliche Ziel gestartet (vgl. Campbell 2005; Bless et al. 2005: 339 ff.).

Selbstverständlich können und werden die hier beschriebenen Angriffstechniken auch in vielfältiger Weise kombiniert zum Einsatz gebracht. Eine gängige Methode zur Verschleierung der Identität des Angreifers ist dabei das sogenannte *Looping*:

- Beim *Looping* erfolgt der Angriff auf das eigentliche Ziel über eine vorgeschaltete Kette kompromittierter Systeme Dritter. Soll bspw. ein Angriff auf einen Rechner R_n erfolgen, so geschieht dies nicht unmittelbar vom Rechner R_1 des Angreifers aus. Stattdessen wird von R_1 zunächst in ein drittes System R_2 und von diesem dann in R_3 usw. eingedrungen. Nach $n-1$ Schritten wird schließlich das eigentliche Ziel R_n erreicht. Die Rückverfolgung eines solchen Angriffs zu seinem Ursprung setzt den Zugang zu sämtlichen Systemen R_2 bis R_n voraus, wodurch der Angreifer nur sehr schwer identifizierbar ist.

90 Der Begriff *Phishing* entstand durch Zusammenziehen der Wörter „Password“ und „Fishing“.

4.2.3 Charakteristika elektronischer Kriminalität

Ein Angriff in elektronischen Netzwerken bietet dem Täter, im Vergleich zu traditioneller Kriminalität, eine Reihe gewichtiger Vorteile, zu denen eine niedrige Zugangsschwelle sowie minimale Kosten der Vorbereitung und Durchführung bei gleichzeitig hohen Erfolgschancen gehören (vgl. Harbort 1996). Sowohl das Wissen über einschlägige kriminelle Techniken als auch spezielle Werkzeuge zu deren Umsetzung sind im Internet frei verfügbar. Diese Techniken können daher bereits mit geringem Aufwand und minimalen Vorkenntnissen angewandt werden. Auch werden neue Techniken permanent in Internet-Foren zur Diskussion gestellt und fortentwickelt.

In elektronischen Netzwerken geht der Täter ferner ein verhältnismäßig geringes persönliches Risiko ein, dem ein vergleichsweise hoher Schaden auf Seiten der Opfer gegenübersteht. So belaufen sich nach dem vom Computer Security Institute (CSI) im Auftrag der US-Bundespolizei FBI jährlich erstellten Computer Crime and Security Survey die geschätzten Verluste von 313 ausgewählten amerikanischen Unternehmen im Jahr 2006 auf über 52 Mio. US-Dollar (CSI/FBI 2006: 15).[91] Tatsächlich muß jedoch von einem weit höheren Gesamtschaden ausgegangen werden, da nur rund die Hälfte aller befragten Unternehmen (313 von 616) überhaupt Angaben zu ihren geschätzten Verlusten machte (CSI/FBI 2006: 12). Offenbar existiert aufgrund befürchteter Imageschäden innerhalb der Wirtschaft eine Tendenz zur Tabuisierung von Cyberkriminalität, die in einer hohen Dunkelziffer resultiert (vgl. Sofaer u. Goodman 2001a: 21 ff.).

Da der Täter selbst – von internem Mißbrauch einmal abgesehen – am Tatort physisch nicht präsent zu sein braucht, sondern seinen Angriff aus sicherer räumlicher und zeitlicher Distanz planen und umsetzen kann, ist er trotz der teilweise immensen Schäden zugleich nur einem verhältnismäßig geringen Verfolgungsdruck ausgesetzt (vgl. Yar 2006: 54 f.). Zusätzlich kann er sich eines umfangreichen Repertoires an Techniken zur Verschleierung der eigenen Identität und zur Vernichtung von Spuren bedienen (vgl. Denning u. Baugh 2000). Es ist Opfer und Strafverfolgungsbehörden somit oft nicht möglich, einen Angriff sowie dessen Ausmaß unmittelbar und zeitnah zu erkennen, noch den Urheber und dessen Intention zweifelsfrei zu identifizieren. Häufig bleibt im Unklaren, ob sich hinter einem Angriff gewöhnliche Kriminalität oder aber politische bzw.

91 Es sei hier kritisch vermerkt, daß das CSI-Survey wissenschaftlichen Anforderungen an eine repräsentative Stichprobe kaum genügen dürfte (vgl. hierzu auch Berkowitz u. Hahn 2003). Dies liegt nicht zuletzt an einer teilweise geringen Rücklaufquote.

strategische Ziele verbergen.

Nach Thomas u. Loader (2000: 6 – 8) können, je nach Motivation, grundsätzlich drei Täter-Kategorien unterschieden werden (vgl. hierzu auch Ratzel 2004: 140):

1. *Hacker*, nicht selten im minderjährigen Alter, dringen zumeist aus spielerischer Neugierde oder zur Profilierung illegal in fremde IuK-Systeme ein. Ihr Angriff zielt nicht primär auf eine finanzielle Bereicherung oder eine anderweitige absichtliche Schädigung Dritter, sondern häufig auf einen publikumswirksamen Coup, wie etwa das scherzhafte Verändern von WWW-Inhalten. Viele Hacker folgen dabei einem selbst auferlegten Ehrenkodex.[92] Die wissentlich oder unwissentlich in Kauf genommenen Kollateralschäden können gleichwohl beträchtlich sein.
2. *Datendiebe* und *-saboteure* bedienen sich ähnlicher Methoden wie Hacker, verschaffen sich jedoch gezielt illegalen Zugang zu Daten, um diese gewinnbringend weiter zu verwerten oder zu veräußern. Hierzu zählt bspw. Wirtschaftsspionage und -sabotage, aber auch der Diebstahl von Identifikationsdaten, wie etwa Kreditkartennummern. Nicht selten handelt es sich hier um professionelle, gewerbsmäßig ausgeübte Auftragskriminalität.
3. *Terroristen*, *Extremisten* und *Sozialstraftäter* nutzen IuK-Systeme für illegale politische und/oder soziale Aktivitäten. Hierunter fällt etwa die Weitergabe von Anleitungen zum Bau von Bomben oder die Verbreitung von illegalen politischen Hetzschriften (vgl. Whine 2000), aber auch von Kinderpornographie. Als Begleiterscheinung herkömmlicher politischer Konflikte läßt sich in diesem Umfeld auch ein verstärkter Aktivismus (Hacktivism) feststellen, der sich bspw. in der Übernahme und Verunstaltung gegnerischer WWW-Seiten sowie in Online-Demonstrationen (Web Sit-ins) manifestiert (vgl. Denning 2001).

Straftaten im Cyberspace haben aufgrund der in vernetzten IuK-Systemen entstehenden spezifischen Externalitäten oftmals besondere Negativeffekte, die eng mit den sog. Netzwerk-, Spillover- oder Knock-on-Effekten (vgl. Borg 2005) moderner, informationstechnisch basierter Volkswirtschaften verknüpft sind. So kommt es im einfachsten Fall allein aufgrund der hohen Konnektivität dieser IuK-Systeme zu negativen Netzwerkexternalitäten, bspw. bei der Verbreitung unerwünschter und unseriöser Werbung (Spam) oder bei der unkontrollierten Ausbreitung von Viren und Würmern. Umgekehrt kommen negative Netzwerkeffekte auch und gerade bei der Verbreitung neuer Angriffstechniken zum Tragen, deren Diffusion sie eo ipso wesentlich beschleunigen.

92 Vgl. hierzu etwa die „Hackerethik“ des Chaos Computer Club (CCC) <`http://www.ccc.de`>.

DDoS-Angriffe sind dann eine bereits fortgeschrittene Form der kriminellen Ausnutzung externer Netzeffekte, da hier bestehende Sicherheitslücken im System eines Dritten zu einem Folgeangriff auf das eigentliche Ziel mißbraucht werden. Auf diese Weise werden in einem Computernetzwerk die Sicherheitslücken jedes einzelnen Teilnehmers zur potentiellen Risikoquelle und damit zum Kostenfaktor aller anderen Teilnehmer. Bei verbreiteten Sicherheitslücken, etwa im Falle von Software-Monokulturen, kann der Angreifer so eine kaskadierende Hebelwirkung erzielen.

Aufgrund dieser Eigenheiten können in einem globalen elektronischen Netzwerk sowohl Opfer wie Angreifer, als auch die zum Angriff mißbrauchten Systeme, in jeweils unterschiedlichen Staaten und damit zumeist fragmentierten Rechtsräumen dislozierd sein,[93] wodurch eine kriminaltechnische Aufklärung und Beweissicherung sowie strafrechtliche Verfolgung deutlich erschwert werden (vgl. Wall 2007: 159 ff.; Sieber u. Nolde 2008; Sieber 2008). Selbst wenn der Angreifer genügend Spuren hinterläßt,[94] schützen ihn Differenzen in der nationalen Gesetzgebung dann oftmals dennoch vor Strafverfolgung (vgl. Wiedemann 2000; Sprinkel 2002).[95] Es ist daher kaum verwunderlich, daß Cybercrime auch und vor allem ein transnationales Phänomen ist, wie eine Reihe einschlägiger Vorfälle illustriert (Sofaer u. Goodman 2001a; Brenner u. Schwerha 2002), dessen wesentliche Ursachen u. a. in

> widespread disparities among states, in the legal, regulatory, or policy environment [...], and the lack of a sufficiently high degree of international cooperation in prosecuting and deterring such crime (Sofaer u. Goodman 2001a: 6 f.)

zu suchen sind. Die situative Überlagerung technischer Spezifika – primär in Form negativer Netzwerkexternalitäten – bei gleichzeitiger Ermangelung eines einheitlichen normativ-institutionellen Regulierungsrahmens auf globaler Ebene ist somit gegenwärtig charakteristisch für kriminelle Handlungen im Umfeld globaler, sozio-technischer Informations- und Kommunikationssysteme.

---

93 Exemplarisch sei hier auf einen Fall verwiesen, in dem das BKA in den Jahren 2001 und 2002 ermittelte (Ratzel 2004: 141). Dabei hatte ein Student von der Universität Umea in Schweden aus ein Trojanisches Pferd auf einem Rechner der Universität Kaiserslautern installiert, mittels dessen er in Computersysteme der US-Marine eindrang, um von dort Quellcode-Dateien herunterzuladen.

94 Zu den Möglichkeiten der Spurensicherung im Internet vgl. Köhntopp u. Köhntopp (2000).

95 Prominentestes Beispiel ist hier wohl der sog. „I love you"-Wurm, der im Mai 2000 einen Gesamtschaden von über 7 Mrd. US-Dollar verursachte. Obwohl ein Informatik-Student in Manila als Urheber des Wurms ermittelt werden konnte, war eine strafrechtliche Ahndung angesichts bis dahin lückenhafter philippinischer Gesetze dennoch nicht möglich (vgl. Sprinkel 2002).

4.2.4 Cybercrime und eCommerce

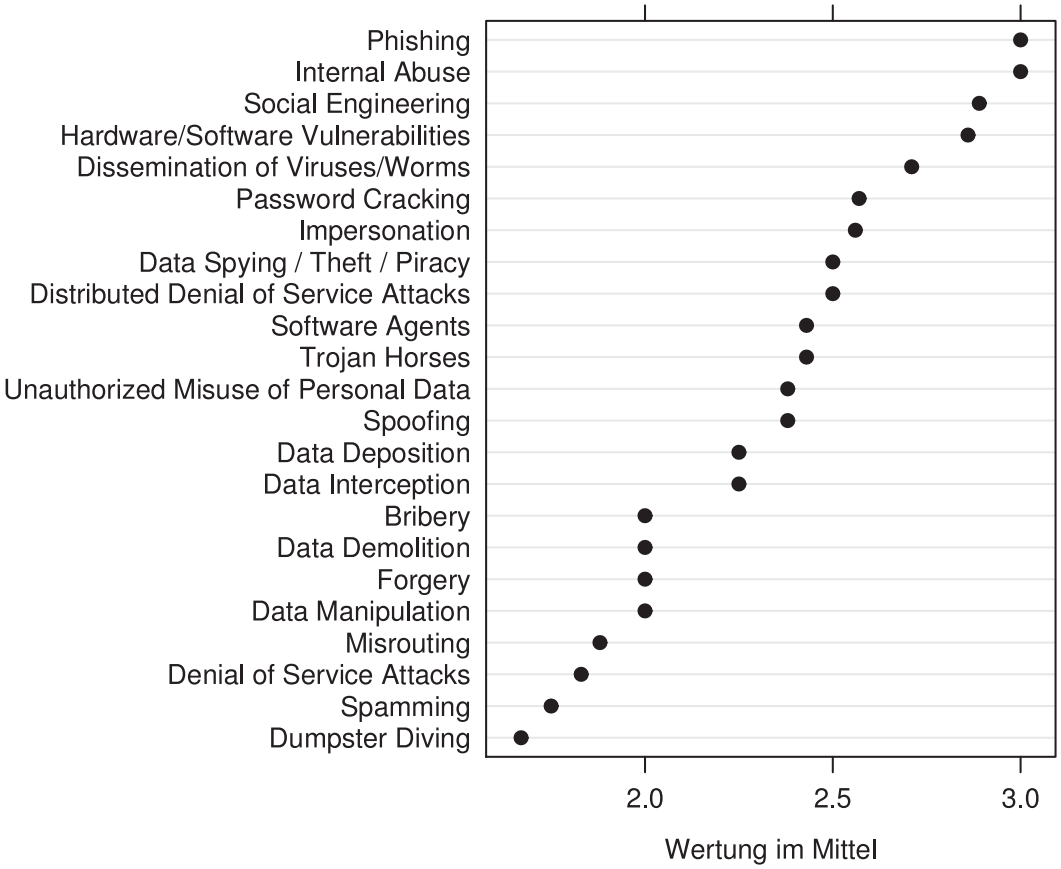
Selbstverständlich werfen die beschriebenen Formen elektronischer Kriminalität auch und gerade im Rahmen elektronischer Transaktionen – respektive des eCommerce – erhebliche Sicherheitsprobleme auf (vgl. BKA 1999; Hey 2001; Koch 2001). So richtete sich etwa nach einer sechsmonatigen Studie des Online-Sicherheitsunternehmens Riptech[96] (vgl. Fishman et al. 2002, hier zitiert nach Smith 2004: 224 f.) die überwiegende Mehrzahl aller Angriffe gegen Wirtschaftsunternehmen, wobei rund 40 Prozent ihren Ursprung in den USA und weitere 40 Prozent in China, Deutschland, Großbritannien, Italien, Japan, Südkorea, Kanada und Taiwan hatten. Einer Analyse des Medienkonzerns VNU[97] zufolge zeichnet sich hier jedoch neuerdings ein Trend zu einer stärker organisierten Form der Online-Kriminalität ab, die hauptsächlich in den Nachfolgestaaten der ehemaligen Sowjetunion beheimatet ist (vgl. auch Voiskounsky et al. 2000).

Neben den durch einen Angriff unmittelbar verursachten Schäden sind vor allem die durch einen eventuellen Vertrauensverlust potentieller Geschäftspartner mittelbar entstehenden Verluste ein nicht zu vernachlässigender Faktor (vgl. Smith 2004), da Vertrauen eine wesentliche Voraussetzung jeder Transaktion bildet. Dies gilt umso mehr in der immateriellen Welt informationsbezogener Produkte und Dienstleistungen, in der neue Mechanismen der Vertrauensbilung von herausgehobener Bedeutung sind (Sydow 1996; Belanger et al. 2002; Petrovic et al. 2003). Aus Angst vor einem Vertrauensverlust werden sicherheitsrelevante Vorfälle von Unternehmen daher sehr häufig nicht zur Anzeige gebracht (vgl. Hey 2001).

Aus der Befragung der Interviewpartner in den für die zehn Fallstudien ausgewählten Organisationen ergab sich hinsichtlich des Gefährdungspotentials verschiedener Angriffstechniken für elektronische Transaktionen das in Abbildung 4.7 dargestellte Bild. Deutlich erkennbar ist, daß der Bedrohung durch internen Mißbrauch eine herausgehobene Bedeutung beigemessen wird. Ebenfalls hoch bewertet werden Formen der Impersonation im allgemeinen sowie das Phishing im besonderen. Letzteres mag dem Umstand geschuldet sein, daß die Technik des Phishing zum Zeitpunkt der Befragung (Oktober 2004) in den Medien besondere Beachtung fand. Da jedoch sämtliche Techniken des sog. Social Engineering als überdurchschnittlich hohe Bedrohung be-

96 Riptech wurde zwischenzeitlich von Symantec übernommen.

97 Vgl. <`http://www.vnunet.com/computing/analysis/2076013/russia-malice`>.



Datenquelle: Interviews. *Codierung*: 1 "less dangerous", 2 "dangerous", 3 "very dangerous".

Abbildung 4.7: *Bedrohungspotential für eCommerce in der Expertenwertung*

wertet wurden, liegt der Schluß nahe, daß Angriffe aufgrund verbesserter technischer Schutzmaßnahmen vermehrt auf soziale und organisatorische Schwächen im Umfeld elektronischer IuK-Systeme zielen (vgl. Rustemeyer 2004).

Interessant ist ferner, daß in DDoS-Angriffen ein deutlich höheres Gefährdungspotential gesehen wird, als dies bei einfachen DoS-Angriffen der Fall ist. Stellt man allerdings in Rechnung, daß DDoS-Angriffe sich negative Netzwerkexternalitäten in besonderer Weise zu Nutze machen, so erscheint dies kaum verwunderlich. Ein autonomer Schutz gegen diese Form der Bedrohung ist aus Sicht einzelner Netzteilnehmer so gut wie unmöglich.

4.3 Sicherheit in elektronischen Netzen

4.3.1 Elektronische Sicherheit als globales Kollektivgut

Wohl kaum ein Begriff wird im Deutschen so vielschichtig und daher unscharf gebraucht wie jener der „Sicherheit“. Kaufmann (1973: 50 – 51) identifiziert nicht weniger als zwölf nuancierte Konnotationen. So kann Sicherheit nicht allein den Zustand eines relativen Geschütztseins bezüglich einer konkreten Gefährdung bedeuten, sondern auch auf die Zuverlässigkeit eines (technischen) Prozesses, die Routine einer Tätigkeit, den Wahrheitsgehaltes einer Aussage, die Bestimmtheit einer Überzeugung, die Wahrscheinlichkeit des Eintretens eines Ereignisses oder die Selbstdarstellung einer Person verweisen. Angesichts dieser Bedeutungsvielfalt differenziert etwa der Lateiner dort, wo im Deutschen oftmals schlicht das Adjektiv „sicher“ verwandt wird, zwischen „tutus“, „securus“, „certus“ und „firmus“; während das Englische mit „sure“, „safe“, „secure“, „firm“ und „certain“ gar fünf verschiedene Bezeichnungen für die Eigenschaft des Sicher-Seins kennt.

Im folgenden wird unter Sicherheit im engeren Sinne jenes Maß an Immunität verstanden, welches ein bestimmtes Gut hinsichtlich möglicher Schäden (einer Nutzenminderung) aufweist. Sicherheit ist damit zunächst und vor allem ein relativer Begriff, der sich in seinem Bedeutungsgehalt als Sicherheit eines Gutes vor einer mehr oder weniger konkreten Gefährdung bestimmt. Diese Gefährdung muß keineswegs objektiv existieren, sondern kann auch lediglich (inter-)subjektiv als solche empfunden bzw. konstruiert – damit aber auch verkannt – werden.[98] Subjektives Sicherheitsbewußtsein und objektive Sicherheitslage korrespondieren also nicht zwangsläufig, wenngleich subjektives Sicherheitsempfinden zumeist auf Vertrauen in ein gewisses Maß an objektiver Sicherheit gründet. Objektive Sicherheit aber ist keine absolute, sondern vielmehr eine graduelle Modalität, die sich am Grad ausgeschlossener Unsicherheit bemißt. Subjektive und kollektive Sicherheitsbegriffe hingegen unterliegen im Wandel der Zeit stetigen Veränderungen (vgl. Krause u. Williams 1996: 49; Deibert 2002: 117 ff.).

Eine mögliche Gefährdung der objektiven Sicherheit eines Gutes kann sowohl aus höherer Gewalt resultieren, als auch beabsichtigte oder unbeabsichtigte Folge der Hand-

98 Aus einer poststrukturalistischen Perspektive, wie sie bspw. Huysmans (1998) einnimmt, erschließt sich der Bedeutungsgehalt des Begriffs „Sicherheit“ dann gar ausschließlich als diskursive Formation im Spannungsfeld fundamentaler Gegensätze, kollektiv konstruiert als Mittel eines rationalen Umgangs mit der Endlichkeit des Subjekts.

lungen Dritter und damit Ausfluß negativer Externalitäten sein. Im letzteren Falle entziehen sich potentielle Gefahrenquellen dann ganz oder teilweise dem unmittelbaren Einfluß eines, an der Sicherheit eben dieses Gutes interessierten Akteurs. Aus dessen Sicht ergeben sich prinzipiell drei, nicht immer in gleichem Maße effektive Strategien zur Erhöhung der Sicherheit eines Gutes: (1) falls möglich eine proaktive, d. h. vorbeugende Einwirkung auf potentielle Gefahrenquellen (*Prävention*), (2) eine unmittelbare Abwehr akuter Bedrohungen zur Schadensverhinderung bzw. -minderung (*Reaktion*) sowie (3) ein nachträglicher Ausgleich bereits eingetretener Schäden (*Kompensation*). Je nach Art und Umfang einer Bedrohung kann der optimale Mix an präventiven, reaktiven und kompensatorischen Maßnahmen variieren. Präventive Maßnahmen implizieren hierbei eher eine langfristige, strategische Perspektive, während reaktive und kompensatorische Maßnahmen eher kurzfristigen Charakter haben und daher primär auf einer operativen Ebene angesiedelt sind.

Solche Schutz- und Sicherheitsmaßnahmen sind jedoch i. d. R. mit erheblichen Kosten verbunden, während ihre Wirksamkeit in einer komplexen Umwelt, die in ständigem Wandel – nicht zuletzt durch den Fortschritt der Technik selbst (vgl. Beck 2003) – neue Gefahrenpotentiale hervorbringt, oft nur von kurzer Dauer ist. Es ist offensichtlich, daß dies insbesondere auch für Schutz- und Sicherheitsmaßnahmen in der Umgebung elektronischer Netze gilt. Sicherheit ist folglich selbst „ein knappes Gut, das unter sich stetig wandelnden Umweltbedingungen immer wieder neu erzeugt und zugeteilt werden muss“ (Winkel 2000: 21). Es stellt sich somit zugleich die Frage, welche institutionellen Mechanismen eine ausreichende Bereitstellung des Gutes Sicherheit gewährleisten können. Hierzu ist zunächst zu klären, ob dem knappen Gut Sicherheit der Charakter eines Individual- oder eines Kollektivgutes zukommt.

Wäre Sicherheit ein Individualgut, so müßte sie sich in exklusiver Weise bereitstellen lassen. Soweit sich Sicherheit durch reaktive und/oder kompensatorische Maßnahmen gewährleisten läßt, trifft dies ohne Zweifel zu. Der Nutzen reaktiver Maßnahmen des Objekt- und Personenschutzes ist bereits per definitionem exklusiv und auch kompensatorische Maßnahmen des Schadensersatzes beziehen sich zwangsläufig in exklusiver Weise auf individuelle Schäden. Mit Unternehmen der Sicherheits- sowie Versicherungsbranche finden sich daher für beide Dienstleistungen im Rahmen eines reinen Marktmechanismus ausreichend Anbieter. Unklarer ist die Lage hinsichtlich präventiver Maßnahmen, da die von einer Gefahrenquelle ausgehende Bedrohung selbst möglicherweise nicht auf ein einzelnes Gut beschränkt ist. In einem solchen Falle kann dann der Nutzen

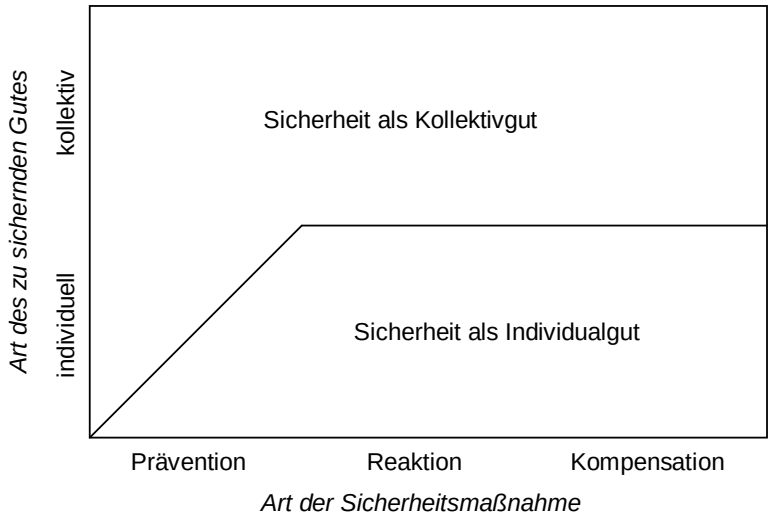


ABBILDUNG 4.8: *Der Charakter des Gutes Sicherheit*

einer präventiven Maßnahme eventuell auch Güter dritter Akteure betreffen und daher nicht exklusiv sein. Klassisches Beispiel ist hier die Landesverteidigung, welche zu einem nicht geringen Teil auf Abschreckung und Prävention beruht und deren Nutzen nicht exklusiv ist.

Da das Gut Sicherheit sich nach obiger Definition immer auf ein weiteres zu sicherndes Gut bezieht, ist ihr Gutscharakter darüber hinaus wesentlich durch den Charakter eben dieses zu sichernden Gutes bedingt. So ist die Sicherheit eines kollektiven Gutes zwangsläufig auch immer selbst ein kollektives Gut, weil von kollektivem Interesse. Umgekehrt kann jedoch auch die Sicherheit eines individuellen Gutes – wie gezeigt – dann kollektiven Charakter annehmen, wenn die hierfür benötigten präventiven Maßnahmen zugleich der Sicherheit anderer Güter dienen. Abbildung 4.8 verdeutlicht diesen Zusammenhang schematisch.

Wie in Abschnitt 4.1 dargestellt, handelt es sich bei elektronischen Netzen um kritische Infrastrukturen und daher um öffentliche, zumindest aber meritorische, mithin „quasi-öffentliche“ Güter. Gleiches gilt folglich auch für die Sicherheit dieser Güter.[99] Der meritorische Gutscharakter von Sicherheit in elektronischen Netzen wird ferner durch den Umstand unterstrichen, daß auch der individuelle Nutzen konkreter Sicherheits- und Schutzmaßnahmen von einzelnen Akteuren, bedingt durch deren

99 Zum Charakter von Sicherheit als öffentlichem Gut vgl. auch Desai (2003).

begrenzte Rationalität sowie einen daraus resultierenden verzerrten subjektiven Sicherheitsbegriff, verkannt werden kann. Zugleich besteht jedoch in jedem Gemeinwesen ein grundlegendes Interesse an einem Mindestmaß allgemeiner Sicherheit im öffentlichen Raum, nicht zuletzt weil diese Prosperität durch Handel und diesen durch Vertrauen erst ermöglicht, also wohlfahrtssteigernd wirkt.[100] Dies gilt selbstverständlich auch hinsichtlich elektronischer Interaktionsräume bzw. Netze sowie des in ihnen abgewickelten Handels (eCommerce). Da diese Interaktionsräume sich global erstrecken, stellt deren Sicherheit folglich ein globales Kollektivgut dar.

Betrachtet man die Bereitstellung des Gutes Sicherheit unter ökonomischen Gesichtspunkten, so wird eine Entscheidung für oder wider ihrer Produktion im Wesentlichen auf einem Kosten-/Nutzenvergleich beruhen. Während sich jedoch die Kosten konkreter Sicherheitsmaßnahmen anhand der in den Produktionsprozeß einfließenden Ressourcen i. d. R. ohne große Schwierigkeiten ermitteln lassen, ist eine Bewertung des erzielten Nutzens der Sache nach oftmals mit Problemen verbunden, denn gerade präventive Sicherheitsmaßnahmen zielen ja auf eine Vermeidung potentieller Schäden. Im Erfolgsfalle ist somit keineswegs immer klar ersichtlich, ob und in welcher Höhe ein Verzicht auf diese Sicherheitsmaßnahmen zum Eintreten eines Schadens geführt hätte, in wie weit eine Nicht-Schädigung also als unmittelbarer Nutzen dieser Maßnahmen zu werten ist.

Die Wirtschaftswissenschaft umgeht dieses Problem, indem sie Sicherheit nicht allein als Zustand der Schadensimmunität, sondern ganz allgemein als das Maß der Berechenbarkeit einer – die Interessen der beteiligten Akteure tangierenden – Entwicklung definiert und damit als kalkulatorische Modalität zukunftsgerichteter (Investitions-)Entscheidungen begreift. Unsicherheit als komplementärer Begriff ist dann das Resultat jeden nicht vorhersehbaren Ereignisses, sofern es eben diese Entwicklung tendenziell beeinflußt, ganz gleich ob es dabei summa summarum positive oder negative Rückwirkungen hinsichtlich der Interessen der betroffenen Akteure entfaltet.

Zur kalkulatorischen Bewältigung von Unsicherheiten greift die Wirtschaftswissenschaft auf den Begriff des *Risikos*[101] zurück. Aus Abbildung 4.9 wird ersichtlich, daß

100 Die Gewährleistung öffentlicher Sicherheit zählte bereits in der Antike zu den Kernaufgaben staatlicher Strukturen und Funktionsträger. So ließ etwa Kaiser Nero in Anerkennung dieses Umstandes Münzgeld mit dem Bild der personifizierten *Securitas* als allegorischer Frauengestalt mit Zepter und Füllhorn, den Symbolen staatlicher Macht und ökonomischen Wohlergehens, prägen.

101 Nach Rammstedt (1992) leitet sich der Begriff vom italienischen „risco“ ab, das in der Bedeutung

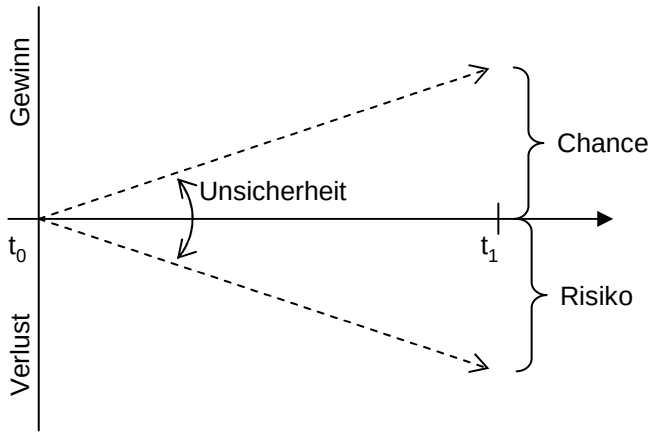


Abbildung 4.9: *Risiko und Chance in der BWL*

das, aus der Unsicherheit über eine zwischen zwei Zeitpunkten t_0 und t_1 stattfindende Entwicklung resultierende Risiko, hierbei als quantifizierbare Größe einer negativen Abweichung vom erwarteten Entwicklungsverlauf aufgefaßt wird. Diesem Risiko steht eine Chance in nicht notwendigerweise gleicher Höhe entgegen, um derentwillen jenes letztlich – mehr oder weniger freiwillig – in Kauf genommen wird. Das konkrete Risiko errechnet sich dabei aus Eintrittswahrscheinlichkeit und Ausmaß potentieller Schäden bzw. Verluste (Bedford u. Cooke 2001). Abbildung 4.10 verdeutlicht den entsprechenden Zusammenhang schematisch anhand einer Vierfeldermatrix.

Hinsichtlich geeigneter Maßnahmen zu einer Risikoreduktion – und damit indirekt Produktion von Sicherheit – lassen sich in Anlehnung an Schaumüller-Bichl (1992: 33–34) dann zusammenfassend vier mögliche Ansatzpunkte ausmachen: (1) Risikovermeidung bei gleichzeitigem Verzicht auf mögliche Chancen, (2) mit Opportunitätskosten belastete präventive Schutz- bzw. Abwehrmaßnahmen, (3) nachträgliche (reaktive) Schadensbegrenzung sowie (4) Überwälzung durch Rückversicherung[102]. Mittels geeigneter Maßnahmen kann so ein anfänglich hohes Risiko sukzessive auf ein letztlich unvermeidbares Restrisiko zurückgeführt werden.

möglicher finanzieller Unwägbarkeiten zunächst im Seehandel der norditalienischen Stadtstaaten der Renaissance Verwendung fand. Das italienische Wort selbst habe seinen Ursprung vermutlich im altgriechischen $\rho\iota\zeta\alpha$ (rhiza), was „Wurzel“ oder auch „Klippe“ bedeute.

102 Es liegt auf der Hand, daß eine Risikoüberwälzung nur in soweit möglich ist, als es sich um einen pekuniär kompensierbaren Schaden handelt und falls sich ein Dritter zur Übernahme bereit erklärt. Gerade bei existentiellen Risiken ist dies jedoch häufig nicht der Fall.

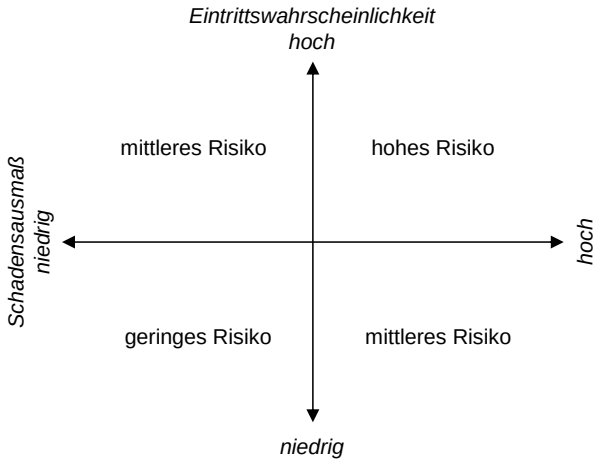


Abbildung 4.10: *Allgemeines Schema einer Risikoklassifikation*

Die ökonomische Betrachtungsweise des Risikos führt in der Soziologie – und hier vor allem bei Luhmann (1990, 1991) – zu einer begrifflichen Trennung zwischen Risiko einerseits und Gefahr andererseits, wobei ersteres als Folge von Unsicherheiten, denen sich das Subjekt in freier Entscheidung trotz möglicher Handlungsalternativen aussetzt, letztere aber als nicht von der subjektiven Entscheidung des Einzelnen abhängig und daher schicksalhaft unvermeidbar erachtet wird. Nach Luhmann (1993a) transformiert jedoch der technische Fortschritt im gleichen Maße, in dem er dem Subjekt die zunehmende Kontrolle seiner Umwelt erlaubt – in Luhmannscher Diktion also die allgemeine Kontingenz reduziert – Gefahren in Risiken, da ein potentieller Schaden unter Inkaufnahme entsprechender Opportunitätskosten durch technische Maßnahmen abwendbar wird. Allerdings können dieselben technischen Maßnahmen zugleich zum Auftauchen gänzlich neuer Risiken führen (vgl. Beck 2003).

4.3.2 Technische Schutzmaßnahmen

Diese Überlegung führt zu der Frage nach den technischen Möglichkeiten des Schutzes in elektronischen Netzwerken. Da hier auf den Schutz vor den Risiken elektronischer Kriminalität in Sonderheit fokussiert wird, können Maßnahmen des physischen Schutzes sowie solche vor den Folgen höherer Gewalt weitgehend außer Acht bleiben, wenngleich diese in einem umfassenden Sicherheitskonzept selbstverständlich nicht zu vernachlässigen sind.

Üblicherweise bemißt sich der Grad der Sicherheit elektronischer Informationen ent-

lang der Kriterien *Vertraulichkeit*, *Integrität* und *Verfügbarkeit* (Winkel 2000; Furnell 2002: 17 ff.).[103] Die Vertraulichkeit einer Information ist gewährleistet, wenn diese ausschließlich für autorisierte Nutzer zugänglich ist. Ihre Integrität ergibt sich aus ihrer Vollständigkeit und Richtigkeit. Manipulationen durch Dritte sowie Fehler bei der Übertragung und Speicherung müssen demnach auszuschließen sein. Oft bedingt die Überprüfung der Integrität einer Information zugleich die Möglichkeit ihrer Zuordnung zu einer konkreten Quelle (Authentizität). Ihre Verfügbarkeit schließlich setzt voraus, daß ein Zugriff für berechtigte Nutzer immer dann möglich ist, wenn diese eine Information aktuell benötigen.

Es ist unmittelbar einsichtig, daß die genannten Eigenschaften letztlich den Wert einer Information als Ressource ausmachen. Im Kontext elektronischer Transaktionen ist zudem die *Verbindlichkeit* bzw. *Nachweisbarkeit* (Accountability) einer Information von Bedeutung. Verbindlich ist eine Information genau dann, wenn weder Absender (Produzent) noch Empfänger (Konsument) ihren Austausch mit Aussicht auf Erfolg bestreiten können. Dem steht allerdings teilweise ein Interesse der Kommunikationspartner an der eigenen Privatsphäre, d. h. auf Kontrolle der Informationen über die eigene Identität (Datenschutz), entgegen (vgl. Hinde 2002; Phillips 2002). So kann bei manchen Transaktionen die *Anonymität* – oder zumindest *Pseudonymität* – eines oder beider Partner durchaus erwünscht sein.

Maßnahmen zum Schutz von Informationen in elektronischen Netzwerken müssen folglich geeignet sein, das Sicherheitsniveau entlang dieser Dimensionen umfassend zu erhöhen. Hierzu steht eine Reihe technischer Schutzmethoden zur Verfügung, die in der Literatur ausführlich behandelt werden, so etwa bei: Kaufman et al. (1995); Northcutt u. Novak (2001); Fuhrberg et al. (2001); Raepple (2001); Greenstein u. Vasarhelyi (2002); Schäfer (2003); Bless et al. (2005). Prinzipiell kann dabei zwischen passiven und aktiven Schutzmaßnahmen unterschieden werden. Während erstere einen unbefugten Zugriff auf Informationen über eine Transformation der sie repräsentierenden Daten erschweren, schränken letztere den Zugriff auf diese Daten selbst durch technische Kontrollmechanismen von vorn herein ein. Gängige Methoden des passiven Schutzes sind *Steganographie* und *Kryptographie* in Verbindung mit *Streuwertfunktionen*; solche des aktiven Schutzes *Viren-Scanner*, *Firewalls*, *Intrusion-Detection-Systeme* (IDS) sowie

103 Gemäß der Anfangsbuchstaben der englischen Bezeichnungen Confidentiality, Integrity, Availability) wird dies auch kurz als CIA-Model bezeichnet. Diese Kriterien finden u. a. in den *Guidelines for the Security of Information Systems* der OECD von 1992 Erwähnung (vgl. Jackson 2000).

verschiedene Verfahren der *Zugriffskontrolle*.

Zur Überprüfung der Integrität von Daten werden insbesondere Streuwertfunktionen (Hash-Algorithmen) herangezogen, die aus großen Datenmengen relativ kurze Prüfsummen (Hash-Werte) errechnen. Durch Abgleich der vor und nach einer Datenübertragung ermittelten Hash-Werte lassen sich dann Übertragungsfehler oder Manipulationen durch Dritte erkennen. Im Gegensatz zu normalen Prüfsummenfunktionen müssen Hash-Funktionen allerdings besonderen Kriterien genügen, zu denen die Unumkehrbarkeit (Urbildresistenz) sowie eine weitgehende Kollisionsresistenz gehören (Schwenk 2002: 11; Bless et al. 2005: 57 f.). Zudem wird zur Übermittlung des Hash-Wertes ein sicherer Übertragungskanal benötigt.

Ist die Gewährleistung der Integrität bestimmter Daten alleine nicht hinreichend, sondern soll darüber hinaus auch deren Vertraulichkeit geschützt werden, so bedarf es weiterer Maßnahmen. Naheliegend ist hier zunächst, die Existenz der Daten selbst zu verbergen. Die Geschichte kennt eine Reihe einschlägiger Beispiele: So berichtet Herodot, daß der Spartaner-König Demaratos aus dem Exil in Susa die Griechen mittels einer Wachstafel, bei der die eigentliche Nachricht nicht in die Wachsschicht sondern in das darunter liegende Holz geritzt war, vor dem Angriff der persischen Flotte warnte (vgl. Singh 2000); und von Plinius dem Älteren ist überliefert, daß dieser unsichtbare Tinte für Nachrichten zwischen den Zeilen seiner Briefe nutzte. Heute werden Informationen vor allem in größeren, unverfänglichen Datenmengen verborgen. In einem Bild mit der Auflösung von 1024×768 Punkten und einer Farbtiefe von 8 Bit je Punkt bspw. können durch eine Reduzierung der Farbtiefe um das niederwertigste Bit bis zu 96 KB an Daten versteckt werden (Raepple 2001: 163). Das durch diese Farbveränderungen auftretende Rauschen ist so minimal, daß es bei einem Bild mit ohnehin unscharfem Farbverlauf, bspw. einer gewöhnlichen Photographie, für das bloße Auge kaum erkennbar ist. Nachteilig wirkt sich bei solchen Verfahren der *Steganographie* allerdings ein vergleichsweise hohes Datenaufkommen aus. So wird im genannten Beispiel immerhin das achtfache der eigentlich zu schützenden Datenmenge benötigt. Für einen guten Schutz kann man gar vom etwa zwanzigfachen ausgehen (Fuhrberg et al. 2001: 136).

Zum Schutz der Vertraulichkeit von Daten kommen daher sehr viel häufiger *kryptographische* Verfahren zum Einsatz. Diese bilden die einzelnen Zeichen eines Klartextes[104] mittels einer umkehrbaren (bijektiven) mathematischen Funktion, der neben

104 Der Begriff „Text“ meint hier einen Datenstrom, verstanden als endliche Folge von Zeichen, in-

dem Argument der unverschlüsselten Zeichen ein Schlüssel bzw. Paßwort als Parameter übergeben wird, in chiffrierter Form ab. Die Zeichen des Klartextes können dabei sowohl durch Permutation transponiert als auch durch die Elemente eines Chiffrealphabets substituiert werden. Beide Methoden vollziehen sich jeweils in Abhängigkeit vom gewählten Schlüssel. Um eine stochastische Kryptoanalyse zu erschweren, wird eine möglichst gleichmäßige Verteilung der Zeichen im chiffrierten Text angestrebt. Das Optimum stellt eine Zeichenverteilung dar, die ein hohes Maß an Entropie aufweist, sich also kaum von einer rein zufälligen Anordnung unterscheidet.

Wird zur Ver- wie Entschlüsselung ein und derselbe Schlüssel benötigt, so handelt es sich um ein symmetrisches, andernfalls um ein asymmetrisches Kryptographieverfahren. Symmetrische Chiffrierverfahren sind historisch sehr alt (vgl. Kahn 1996). So ist bekannt, daß schon Caesar ein solches Verfahren zur Verschlüsselung wichtiger Nachrichten verwandte. Nachteilig wirkt sich hier allerdings aus, daß sowohl Sender als auch Empfänger einer Nachricht bereits a priori im Besitz eines geheimen Schlüssels (Secret Key) sein müssen. Andernfalls muß ein zusätzlicher sicherer Kanal zum Austausch dieses Schlüssels verfügbar sein (Problem der Schlüsselvereinbarung). Gängige Algorithmen der symmetrischen Verschlüsselung sind gegenwärtig:

- *Advanced Encryption Standard* (AES): Als Nachfolger des Data Encryption Standard (DES) wurde AES im Jahr 2000 vom National Institute of Standards and Technology (NIST) offiziell für alle US-Behörden zur Verschlüsselung von Dokumenten der höchsten Geheimhaltungsstufe freigegeben. Der Algorithmus ist frei zugänglich und wird auch außerhalb der öffentlichen Verwaltung in zahlreichen Anwendungen, wie etwa dem VoIP-Programm Skype, eingesetzt.
- *International Data Encryption Algorithm* (IDEA): Dieser Algorithmus wurde Anfang der 1990er Jahre an der ETH Zürich in Zusammenarbeit mit der Ascom AG entwickelt, deren Tochter Mediacrypt zur Zeit die Patente für das Verfahren hält.[105]
- *Blowfish*: Ein ebenfalls nicht patentiertes, frei zugängliches Verfahren, das Anfang der 1990er Jahre von dem Mathematiker und Kryptologen Bruce Schneier entwickelt wurde und sich besonders durch seine Schnelligkeit auszeichnet. Nachfolger ist der sog. „Twofish-Algorithmus“.

kludiert also auch digital repräsentierte Bilder und Töne.

105 Vgl. <`http://www.mediacrypt.com`>.

Geschichtlich wesentlich jünger als symmetrische sind asymmetrische Algorithmen. Möglich wurden diese erst durch die bahnbrechenden Überlegungen von Diffie u. Hellman (1976). Das heute übliche Verfahren wurde 1977 von den Mathematikern Ronald L. Rivest, Adi Shamir und Leonard Adleman entwickelt. Aufgrund der Initialen der Nachnamen seiner Erfinder wird es auch kurz als „RSA-Algorithmus“ bezeichnet. Asymmetrische Verfahren sind einem Einwegmechanismus vergleichbar, da zur Ver- und Entschlüsselung jeweils unterschiedliche Schlüssel benötigt werden. Voraussetzung hierfür ist eine mathematische Chiffrierfunktion, die zwar im Prinzip bijektiv ist, deren Umkehr jedoch ohne die zusätzliche Information eines zweiten Schlüssels gleichwohl äußerst aufwendig und somit de facto unmöglich ist (Einwegfunktion mit Falltür; vgl. Kesdogan 2000: 22 f.). Der RSA-Algorithmus macht sich hier den Umstand zu Nutze, daß nach dem gegenwärtigen Stand der mathematischen Forschung eine Primfaktorzerlegung im Bereich sehr großer Zahlen selbst unter Einsatz leistungsfähigster Rechenprozessoren extrem zeitraubend ist. Durch Multiplikation zweier hinreichend großer Primzahlen kann daher eine Zahl ermittelt werden, deren Zerlegung selbst unter Berücksichtigung der steigenden Rechenkapazitäten zukünftiger Computergenerationen auf absehbare Zeit ausgeschlossen erscheint, deren Primfaktoren also nur ihrem Urheber bekannt sind. Eine große Schwäche liegt dabei allerdings in der bisher mathematisch nicht bewiesenen Annahme, daß kein – bis jetzt möglicherweise noch unentdecktes – Verfahren einer vereinfachten Primfaktorzerlegung existiert.

Aufbauend auf dieser Annahme wird beim RSA-Verfahren zunächst unter Verwendung sehr großer Primzahlen und im Rückgriff auf den Satz von Euler ein Schlüsselpaar generiert, das aller Wahrscheinlichkeit nach nicht wechselseitig ableitbar ist, sich jedoch gleichwohl gegenseitig zur Ver- und Entschlüsselung bedingt.[106] Einer dieser bei-

106 Zu einer detaillierten Beschreibung des RSA-Algorithmus vgl. Burnett u. Paine (2001). Der Satz von Euler lautet in der allgemeinen Form für $a \in \mathbb{Z}$, $n \in \mathbb{N}$ und unter der Bedingung, daß a und n teilerfremd sind: $a^{\phi(n)} \equiv 1 \pmod{n}$. Die Eulersche Funktion ϕ ordnet ihrem Argument die Anzahl aller natürlichen Zahlen zu, die zu diesem teilerfremd und kleiner als es selbst sind. Falls das Argument n das Produkt zweier Primzahlen p und q ist, gilt daher: $\phi(n) = (p-1) \cdot (q-1)$. Zusammen mit einer zufällig gewählten natürlichen Zahl e, die zu n teilerfremd und kleiner als $\phi(n)$ sein muß, bildet n als geordnetes Zahlenpaar (n, e) den öffentlichen Schlüssel. Nun ist d so zu wählen, daß gilt: $e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$. Die Zahl d ergibt dann – ebenfalls zusammen mit n – den Tupel (n, d) des korrespondierenden privaten Schlüssels. Durch $y \equiv x^e \pmod{n}$ läßt sich nun ein beliebiger Wert x in y überführen, wobei dies nur durch $x \equiv y^d \pmod{n}$ umkehrbar ist. Gleiches gilt auch vice versa. Da zugleich d aus e bei hinreichend großem n nur unter Kenntnis von p und q, nicht aber von n allein, hergeleitet werden kann, erfüllt der Algorithmus alle für eine asymmetrische Verschlüsselung notwendigen Kriterien.

den Schlüssel wird öffentlich zugänglich gemacht (Public Key), der andere privat und vertraulich verwahrt (Private Key). Weil mittels des öffentlichen Schlüssels chiffrierte Daten nurmehr mit dem privaten Schlüssel dechiffriert werden können und umgekehrt, erweist sich das asymmetrische Verfahren dem symmetrischen hinsichtlich des Schutzes von Informationen in offenen IuK-Systemen an Praktikabilität vielfach überlegen. Da asymmetrische Algorithmen allerdings mit extrem großen Zahlen und Logarithmen operieren, sind sie im Vergleich zu symmetrischen äußerst rechen- und damit zeitintensiv, weshalb beide nicht selten zu hybriden Verfahren kombiniert werden (Bless et al. 2005: 87 ff.). Die eigentliche Verschlüsselung der Daten erfolgt dabei symmetrisch mittels eines zufällig erzeugten Secret Key. Dieser Secret Key wird dann asymmetrisch verschlüsselt an den symmetrisch chiffrierten Text angehängt.

Durch den Einsatz asymmetrischer Verfahren wird die geschützte Übermittlung vertraulicher Daten auch ohne exklusiven Austausch eines geheimen Schlüssels möglich. Um sicherzustellen, daß eine Nachricht nurmehr von ihrem Adressaten entziffert werden kann, chiffriert der Absender diese dazu lediglich mit dessen allgemein zugänglichem öffentlichen Schlüssel. Vice versa läßt sich eine Nachricht elektronisch signieren und damit zweifelsfrei einem bestimmten Absender zuordnen, indem dieser die Daten mit seinem privaten Schlüssel chiffriert. Weil ein Dechiffrieren ausschließlich mit dem korrespondierenden öffentlichen Schlüssel möglich ist, ist die Authentizität der Nachricht bzw. die Identität des Absenders folglich für jedermann überprüfbar. Bei großen Datenmengen wird aus Zeit- und Platzgründen allerdings auch hier nicht die gesamte Nachricht, sondern lediglich deren Hash-Wert asymmetrisch verschlüsselt (vgl. Fuhrberg et al. 2001: 96 ff.; Schäfer 2003: 91 ff.). Zusätzlich können weitere Modalitäten einer Kommunikationsbeziehung – etwa ein Zeitstempel oder die IP-Adressen von Sender und Empfänger – in die elektronische Signatur einfließen, um eine spätere Nachweisbarkeit zu erleichtern. Zeichnen beide Kommunikationspartner eine Nachricht auf diese Weise jeweils mit ihrer elektronischen Signatur gegen, so ist zugleich die Verbindlichkeit des Informationsaustauschs gewährleistet.

Obwohl sie das Problem der Schlüsselvereinbarung elegant umgehen, werfen asymmetrische Verfahren jedoch zugleich das Problem einer vertrauenswürdigen Generierung und Distribution öffentlicher Schlüssel im Rahmen einer Public Key Infrastructure (PKI) auf, da diese eine wesentliche Voraussetzung einer zuverlässigen Authentifikation der Kommunikationspartner bildet. Eine Lösung ist hier sowohl in der verteilten Form eines sog. Vertrauensnetzwerkes (Web of Trust), als auch über ein hierarchi-

sches System zentraler Zertifizierungsstellen (Certification Authority) denkbar (vgl. Lipp 2003: 248 ff.). In beiden Fällen beruht die Akzeptanz eines neu eingeführten öffentlichen Schlüssels jeweils wesentlich auf der Autorität eines bereits bekannten und als vertrauenswürdig eingestuften Dritten, der diesen Schlüssel mit seiner eigenen Signatur beglaubigt und damit zugleich für dessen Authentizität, d. h. für die verbindliche Zuordnung des einzuführenden Schlüssels zu einem bestimmten Kommunikationspartner, bürgt.

Die Theorie der Small Worlds (Watts 1999) legt nahe, daß sich über transitive Vertrauensketten jeder neue Schlüssel in einem Netzwerk gegenseitiger Beglaubigungen potentiell innerhalb weniger Schritte authentifizieren läßt. Diese Überlegung liegt dezentralen Vertrauensnetzwerken – wie sie sich etwa PGP[107] zu Nutze macht – zugrunde. Hierbei wird ein Initial-Vertrauen über persönliche – i. d. R. auf sog. Key Signing Partys erworbene – Kontakte hergestellt. Durch reziprokes Signieren wird dieses Vertrauen sodann systematisch auf neue Public Keys ausgeweitet, wobei jeder Teilnehmer selbst die Tiefe seiner transitiven Vertrauensbeziehungen festlegt. Im Gegensatz hierzu beruht das Modell des von der internationalen Fernmeldeunion (ITU) 1988 verabschiedeten X.509-Standards auf einer exklusiven PKI, die aus einer zentralen Hierarchie von Zertifizierungsstellen besteht (Nash et al. 2002: 489 ff.). Diese beglaubigen die Authentizität öffentlicher Schlüssel, wobei die einzelnen Zertifizierungsstellen von der jeweils nächst höheren Hierarchieebene zertifiziert sein müssen, so daß alle Zertifizierungsstränge letztlich bei einer Root Authority zusammenlaufen.[108] Für eine Anwendung im Bereich des Internet wurde der X.509-Standard von der Internet Engineering Task Force (IETF)[109] im RFC 3280 noch einmal näher spezifiziert.

Aufbauend auf Kryptographieverfahren läßt sich eine ganze Reihe weiterer Schutzmaßnahmen realisieren. So wurde etwa für Übertragungen im Internet ein Secure Socket Layer (SSL) zwischen Transportschicht (TCP/IP) und Anwendungsebene (HTTP, FTP etc.) eingefügt, um eine verschlüsselte und damit sichere Ende-zu-Ende-Verbindung zu ermöglichen (Schwenk 2002: 80 ff.; Schäfer 2003: 269 ff.). Alternativ entwarf die IETF

107 PGP steht für „Pretty Good Privacy“, ein Programm zur hybriden Verschlüsselung von Nachrichten, das aufgrund seiner freien Verfügbarkeit, seines offenen Quellcodes sowie eines starken Kryptographiealgorithmus vor allem bei Privatanwendern und Bürgerrechtsbewegungen einen hohen Verbreitungsgrad erreicht hat.

108 Eine Online-Liste von Zertifizierungsstellen findet sich unter <`http://www.pki-page.org`>.

109 Vgl. hierzu den Eintrag im Organisationsglossar im Appendix.

mit IPSec einen Standard zur Verschlüsselung der Datagramme bereits auf IP-Ebene, der hauptsächlich im RFC 2401 spezifiziert ist (Schwenk 2002: 112 ff.). Allgemein können durch öffentliche Kommunikationsnetze getunnelte private Netzwerke, sog. Virtual Private Networks (VPN), die zumeist nicht gegen Abstrahlung und technische Manipulationen zu sichern sind, hinsichtlich der Integrität und Vertraulichkeit der übertragenen Daten mittels Verschlüsselung hervorragend geschützt werden (Raepple 2001: 224 ff.). Gleiches gilt selbstverständlich auch für Funkverbindungen. Von besonderem Interesse sind kryptographische Methoden auch und besonders im Bereich des eCommerce. Neben der durch elektronische Signaturen eröffneten Möglichkeit verbindlicher Transaktionen erlauben sie im Rahmen des Digital Rights Management auch einen Schutz geistigen Eigentums (Schwenk 2002: 186 ff.). Darüber hinaus sind sie wesentliche Voraussetzung zur Realisierung elektronischer Zahlungssysteme (BSI 1999: 30 ff.; Lepschies 2000: 103 ff.; Fuhrberg et al. 2001: 401 ff.).

Im Gegensatz zu einer Übertragung durch ein offenes und damit tendenziell unsicheres Netzwerk wie das Internet lassen sich Daten auf einzelnen Rechnern oder in abgeschlossenen Teilnetzwerken nicht nur über kryptographische Methoden passiv, sondern durch Verfahren der Zugriffskontrolle auch aktiv schützen. Hierzu muß sich der Nutzer vor Beginn einer Sitzung zunächst authentisieren, d. h. seine Identität gegenüber dem System zweifelsfrei nachweisen (Kaufman et al. 1995: 205 ff.). Gängige Verfahren der Authentifikation beruhen zumeist auf exklusivem Wissen (Paßwort, Geheimzahl) oder Besitz (Chip- oder Magnetstreifenkarte). Zunehmend gewinnen aber auch biometrische Merkmale an Bedeutung (vgl. Vielhauer u. Steinmetz 2001). In Netzwerken mit ungeschütztem TCP/IP-Protokoll kann die Authentifikation zusätzlich durch einen zentralen Kerberos-Server unterstützt werden (Kaufman et al. 1995: 265 ff.). Jeder Nutzer muß sich dann gegenüber diesem für die Dauer einer Sitzung nur einmal authentisieren und kann anschließend auf alle Netzwerkdienste zugreifen, wobei der Kerberos-Dienst jeweils Client und Server wechselseitig authentifiziert.

Im Allgemeinen werden jedem authentisierten Nutzer im Rahmen eines Discretionary Access Control (DAC) Zugriffsrechte auf bestimmter Ressourcen und Daten eines IuK-Systems eingeräumt. Ausmaß und Umfang dieser Rechte kann von dessen Administrator für einzelne Nutzer oder Klassen von Nutzern frei definiert werden. Die Autorisation erfolgt damit allein in Abhängigkeit von der Identität des jeweiligen Nutzers, wodurch Probleme hinsichtlich einer Datenflußkontrolle entstehen können (vgl. Murauer 2001). Besonders in militärischen IuK-Systemen werden deshalb Modelle des

Mandatory Access Control (MAC) bevorzugt (Kaufman et al. 1995: 26 ff.). Bei dieser Art der Zugriffskontrolle überwacht das IuK-System aktiv die Einhaltung festgelegter Regeln, die die Integrität und Vertraulichkeit der Daten gewährleisten sollen. Zu diesem Zweck können Informationen sowohl nach Sachgebieten als auch Geheimhaltungsstufen klassifiziert werden. Ein Zugriff ist dann nur durch Nutzer mit der jeweiligen Berechtigungsstufe und Fachrichtung sowie nur innerhalb der jeweiligen Sicherheitsumgebung möglich, so daß ein Abfluß von Daten in andere Bereiche verhindert wird.

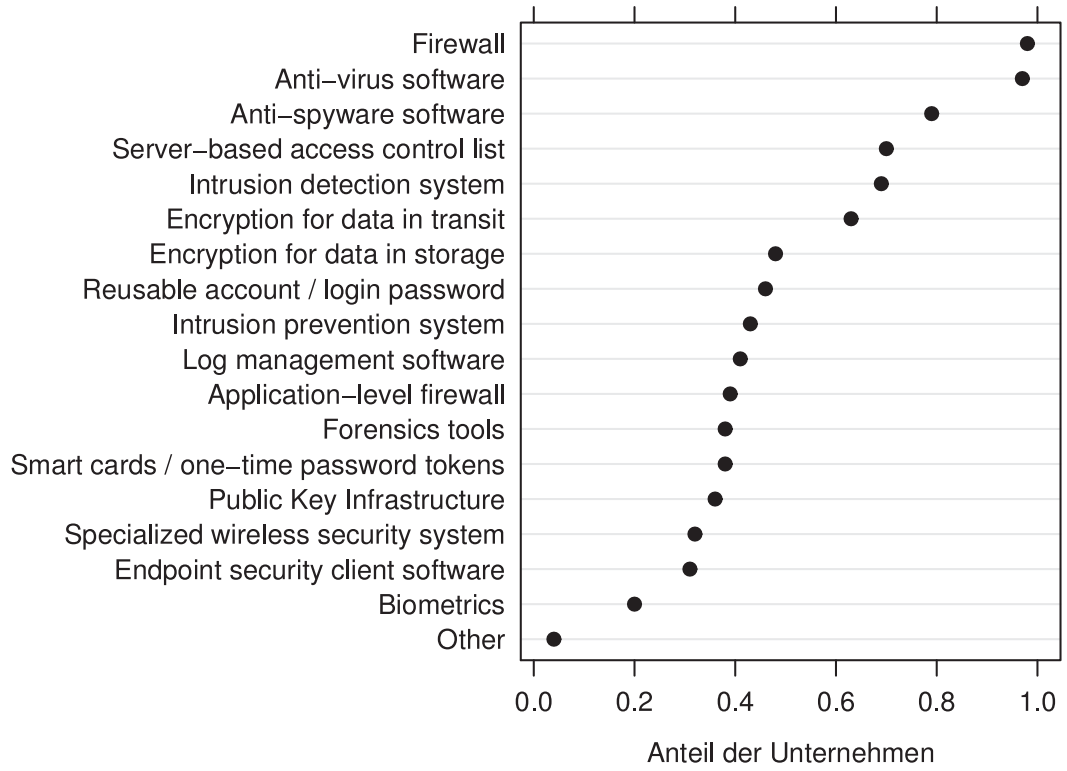
Eine Gatekeeper-Funktion an der Schnittstelle von abgeschlossenen Teilnetzwerken und dem Internet nehmen *Firewalls* ein (Fuhrberg et al. 2001: 137 ff.). Sie dienen der Überwachung und Filterung sowie ggf. Protokollierung des ein- und ausgehenden Datenverkehrs. Da sie die äußerste Bastion eines Teilnetzwerkes bildet, wird eine Firewall i. d. R. auf einem eigenen Rechner installiert, dessen Funktionalität auf das für ihren Betrieb unabdingbare Niveau zurückgeführt wurde, um potentielle Angriffsflächen so gering wie möglich zu halten. Zu einer Firewall gehören für gewöhnlich Paketfilter, die die kommenden und gehenden Datagramme auf der Übertragungsschicht überwachen. Sie erlauben u. a. Einschränkungen des zulässigen IP-Adreßraumes. Auch ist es möglich Datenverkehr von außerhalb prinzipiell zu unterbinden und Antworten auf zuvor aus dem Teilnetzwerk heraus erfolgte Anfragen nur innerhalb eines bestimmten Zeitfensters zuzulassen. Ferner kann ein Application-Gateway bzw. Proxy-Server eingesetzt werden, der als intermediäre Instanz auf der Anwendungsebene fungiert. Den einzelnen Anwendungen ist dann jeweils ein entsprechender Proxy-Prozeß auf dem Application-Gateway zugeordnet, über den sämtliche Verbindungen nach außen abgewickelt werden. Wird von einer Anwendung auf einem Client innerhalb des Teilnetzwerkes eine Anfrage an einen Server außerhalb desselben gerichtet, so nimmt der zugehörige Proxy diese zunächst entgegen, überprüft sie auf Zulässigkeit und leitet sie dann unter der eigenen Netzadresse an den Server weiter, fungiert also gegenüber diesem selbst als Client. Mit der Antwort wird im umgekehrten Sinne verfahren. Diese Vermittlerrolle erlaubt eine äußerst effektive Kontrolle des Datenflusses auf der Anwendungsebene.

Ergänzend zu einer Firewall können Intrusion Detection Systems (IDS) zum Einsatz kommen (vgl. Northcutt u. Novak 2001). IDS protokollieren und sammeln Informationen über Nutzungsverhalten und Datenflüsse und analysieren diese im Hinblick auf Anomalien sowie bekannte Angriffsmuster, wodurch ein frühzeitiges Erkennen potentieller Angriffe möglich wird. IDS können Host- oder Netz-basiert sein, je nachdem ob ein einzelner Rechner oder der Datenverkehr eines Netzwerkes überwacht werden soll. Die

Monitore Netz-basierter IDS können sowohl vor als auch hinter einer Firewall platziert werden oder aber in diese integriert sein, wobei jede dieser Lösungen jeweils spezifische Vor- und Nachteile aufweist (Fuhrberg et al. 2001: 187 f.). Bei einer Platzierung vor der Firewall können zwar Angriffe aus dem Internet in ihrer vollen Bandbreite erfaßt werden, allerdings ist das IDS dabei selbst verwundbar und kann zudem keine Innentäter erkennen. Eine Integration in die Firewall belastet diese mit zusätzlichen Funktionalitäten und steigert deren Anfälligkeit für Angriffe. Auch hier ist das Erkennen von internem Mißbrauch nicht möglich. Bei einer Platzierung hinter der Firewall ist das IDS gegen Angriffe geschützt und überwacht auch den internen Datenverkehr, jedoch werden zugleich nur noch diejenigen äußeren Angriffe, die durch die Firewall vordringen, registriert. Teilweise werden IDS als sog. Intrusion Response Systems (IRS) auch um reaktive Komponenten erweitert, die automatisierte Gegenmaßnahmen – wie etwa einen Gegenangriff oder eine Rekonfiguration der Firewall – erlauben. Allerdings sind beide Ansätze problematisch, da Angriffe oft über kompromittierte Systeme Dritter erfolgen, ein Gegenangriff also zumeist nur diese trifft. Eine automatische Rekonfigurierbarkeit der Firewall hingegen kann zusätzliche Sicherheitslücken eröffnen.

Schließlich gibt es technische Schutzmaßnahmen, die auf jedem Einzelrechner vorzunehmen sind. Hierzu gehört vor allem die Installation einer Personal Firewall sowie eines Viren-Scanners. Eine Personal Firewall übernimmt gleich einer Gateway-Firewall ebenfalls die Filterung des aus- und eingehenden Datenverkehrs. Sie implementiert einen Paketfilter und überwacht darüber hinaus, welche Anwendungen eine Verbindung zum Internet herstellen (Application Control). Zwar läßt sich eine Personal Firewall explizit auf das jeweilige Nutzungsverhalten abstellen, gleichwohl bietet sie aufgrund ihres geringeren Umfangs und der lokalen Installation auf einem normalen Arbeitsrechner dennoch einen geringeren Schutz als eine separate Gateway-Firewall. Viren-Scanner überprüfen ausführbare Dateien mit Hilfe einer Bibliothek bekannter Malware-Signaturen auf mögliche Schadensroutinen. Sie verhindern das Ausführen befallener Dateien und erlauben darüber hinaus in vielen Fällen deren Reparatur. Da ständig neue Schadensroutinen entwickelt werden (vgl. Abschnitt 4.2.2), muß die Signaturbibliothek allerdings laufend aktualisiert werden.

Zum Schutz von Informationen in elektronischen Netzwerken steht mit den aufgezeigten Techniken ein umfangreiches Spektrum an Maßnahmen zur Verfügung. Teilweise schließen sich diese allerdings auch gegenseitig aus. So hat etwa die Verschlüsselung des Datenverkehrs zur Folge, daß Firewall und Viren-Scanner Malware nur mehr bedingt



Datenquelle: CSI/FBI (2006: 16).

Abbildung 4.11: *Eingesetzte Sicherheitstechnologie nach dem CSI/FBI-Survey 2006*

identifizieren können. Diverse Viren nutzen diesen Umstand gezielt aus, indem sie sich selbst mit wechselndem Schlüssel chiffrieren. Abbildung 4.11 zeigt den Verbreitungsgrad der einzelnen Sicherheitstechnologien in jenen Unternehmen, die im Rahmen der in Abschnitt 4.2.3 bereits zitierten CSI/FBI-Studie von 2006 befragt wurden. Im Gegensatz zur Frage nach den Verlusten lag hier die Rücklaufquote allerdings bei 100 Prozent. Erkennbar ist, daß nahezu alle Unternehmen über Firewalls und Viren-Scanner verfügen. Allerdings setzten nur etwa zwei Drittel IDS ein. Fast zwei Drittel aller Unternehmen nutzen jedoch keinerlei PKI und über ein Drittel versendet Daten sogar gänzlich unverschlüsselt. Schwächen zeigen sich also insbesondere im Bereich des passiven Schutzes von Daten.

5 Die Produktion elektronischer Sicherheit

5.1 Institutioneller Rahmen

5.1.1 Rechtlich-formale Regulierung

Da es sich bei vernetzten Informationsinfrastrukturen um sozio-technische Systeme handelt, die neben technischen Artefakten auch Akteure und soziale Artefakte als kritische Komponenten umfassen, sind technische Maßnahmen zu ihrem Schutz alleine nicht hinreichend. Vielmehr bedarf es zur Gewährleistung der Sicherheit des Gesamtsystems einer flankierenden rechtlich-institutionellen Regulierung, wenngleich deren effektives Steuerungspotential in einem durch hohe Komplexität und globale Interdependenzen gekennzeichneten Umfeld nicht unumstritten ist (vgl. Fallenböck 2003: 155 ff.). Soll im globalen Wirtschafts- bzw. Handlungsraum ein bloßes Ausweichen der Adressaten einer Regulierung in andere Rechtsräume vermieden werden, so müssen nationale Politiken in diesem Bereich offenkundig konvergieren (vgl. Sofaer 2001). Verstärkte Bemühungen zur Harmonisierung konstatieren bspw. Bennett (1988), Putnam u. Elliott (2001) und Chang et al. (2003) sowie – aus juristischer Perspektive – Sieber (2008).

Auf globaler Ebene hat die Vollversammlung der Vereinten Nationen (UN) seit 1998 eine Reihe einschlägiger Resolutionen verabschiedet (vgl. Tabelle 5.1). Jährlich wiederkehrend werden die Mitgliedsstaaten der UN aufgefordert, Entwicklungen im Bereich der Informations- und Kommunikationstechnologie hinsichtlich möglicher Bedrohungen für die internationale Sicherheit zu prüfen und auf multinationaler Ebene Maßnahmen zum Schutz der Informationsinfrastruktur abzustimmen. Ferner sind die Mitgliedsstaaten aufgerufen den Generalsekretär der Vereinten Nationen über die von ihnen im nationalen wie internationalen Rahmen ergriffenen Maßnahmen zu informieren.

Die Resolutionen 55/63 von 2000 und 56/121 von 2001 adressieren explizit einen Maßnahmenkatalog zur Bekämpfung des kriminellen Mißbrauches der Informations- und Kommunikationstechnologie. Die Mitgliedsstaaten werden darin aufgefordert, ihr nationales Strafrecht an die entsprechenden Gegebenheiten anzupassen, ihre Bevölkerung hinsichtlich der neuen Gefahren zu sensibilisieren sowie international in der

TABELLE 5.1: *Einschlägige Resolutionen der Vollversammlung der Vereinten Nationen*

Jahr	*Sitzung*	*Nr.*	*Thema*
1998	53	70	Developments in telecommunications and information in the context of international security
1999	54	49	Developments in the field of information and telecommunications in the context of international security
2000	55	28	Developments in the field of information and telecommunications
2000	55	59	Vienna Declaration on Crime and Justice
2000	55	63	Combating the criminal misuse of information technologies
2001	56	19	Developments in the field of information and telecommunications in the context of international security
2001	56	121	Combating the criminal misuse of information technologies
2002	56	261	Plans of action for the implementation of the Vienna Declaration on Crime and Justice
2002	57	53	Developments in the field of information and telecommunications in the context of international security
2002	57	239	Creation of a global culture of cybersecurity
2003	57	304	Information and communication technology strategy
2003	58	32	Developments in the field of information and telecommunications in the context of international security
2003	58	199	Creation of a global culture of cybersecurity and the protection of critical information infrastructures
2004	59	61	Developments in the field of information and telecommunications in the context of international security
2005	60	45	Developments in the field of information and telecommunications in the context of international security
2006	60	252	World Summit on the Information Society
2006	61	54	Developments in the field of information and telecommunications in the context of international security
2007	62	17	Developments in the field of information and telecommunications in the context of international security
2008	63	37	Developments in the field of information and telecommunications in the context of international security
2009	64	25	Developments in the field of information and telecommunications in the context of international security
2009	64	211	Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures
2010	65	41	Developments in the field of information and telecommunications in the context of international security
2011	66	24	Developments in the field of information and telecommunications in the context of international security
2012	67	27	Developments in the field of information and telecommunications in the context of international security

Strafverfolgung zu kooperieren. Ähnliche Forderungen finden sich auch im Annex der Resolution 56/261 von 2002 unter der Überschrift „Action against high-technology and computer-related crime“. Im Auftrag der Vereinten Nationen organisierte die International Telecommunication Union (ITU) in den Jahren 2003 und 2005 zwei konsekutive World Summit on the Information Society (WSIS), in deren Folge die Resolution 60/252 von 2006 den Generalsekretär der UN aufforderte, ein Internet Governance Forum (IGF) zu etablieren. Dieses Forum dient u. a. ebenfalls dem Informationsaustausch sowie der Diskussion von Themen der Sicherheit im Internet.

Auf regionaler Ebene wurde insbesondere innerhalb der EU bereits eine fortgeschrittene länderübergreifende Harmonisierung der Gesetzgebung im Hinblick auf die Sicherheit kritischer Informationsinfrastrukturen erreicht (vgl. hierzu etwa Bendiek 2012: 19 ff.). Die Europäische Kommission verabschiedete 2006 eine *Strategie für eine sichere Informationsgesellschaft*[110], in der eine enge partnerschaftliche Koordination aller beteiligten Akteure sowie eine dezentrale Wahrnehmung der Verantwortung als wesentliche Voraussetzung eines effektiven Schutzes kritischer Informationsinfrastrukturen genannt werden. Parallel zu dieser Strategie wurde ein *Europäisches Programm für den Schutz kritischer Infrastrukturen*[111] (EPSKI) initiiert, welches u. a. den Aufbau eines *Warn- und Informationsnetzes für kritische Infrastrukturen* (WINKI) vorsieht.

Ergänzend verabschiedete der Europäische Rat 2008 dann eine Richtlinie über die *Ermittlung und Ausweisung kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern*[112]. Ein Aktionsplan der Europäischen Kommission zum *Schutz kritischer Informationsinfrastrukturen*[113] von 2009 identifiziert darüber hinaus fünf künftig zentrale Handlungsfelder europäischer Politik: (1) Prävention und Abwehrbereitschaft, (2) Erkennung durch Frühwarnsysteme, (3) Folgenminderung und Wiederherstellung, (4) internationale Zusammenarbeit und (5) Kriterien für kritische Informationsinfrastrukturen. Erste Erfolge dieses Aktionsplanes bilanziert die Komission 2011.[114] Der Aktionsplan hatte u. a. die Gründung der European Public-Private Partnership for Resilience (EP3R) zur Folge, die einen engen europaweiten Informationsaustausch zentraler Akteure fördern soll und sich in diverse Arbeitsgruppen gliedert.

110 Vgl. Mitteilung der Kommission KOM(2006) 251 vom 31. Mai 2006.

111 Vgl. Mitteilung der Kommission KOM(2006) 786 vom 12. Dezember 2006.

112 Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008.

113 Vgl. Mitteilung der Kommission KOM(2009) 149 vom 30. März 2009.

114 Vgl. Mitteilung der Kommission KOM(2011) 163 vom 31. März 2011.

Anfang 2013 schließlich veröffentlichte die Komission gemeinsam mit der Hohen Vertreterin für Außen- und Sicherheitspolitik eine *Cybersicherheitsstrategie*.[115] Als wesentliche Ziele werden hierin u. a. genannt: (1) eine verbesserte Widerstandsfähigkeit gegen Angriffe im Cyberspace, (2) eine Verringerung der Kriminalität im Cyberspace, (3) die Entwicklung von Kapazitäten zur Verteidigung des Cyberspace im Rahmen der Gemeimsamen Sicherheits- und Verteidigungspolitik sowie (4) die Entwicklung industrieller und technischer Grundlagen zur Verbesserung der Sicherheit im Cyberspace. Verbunden hiermit ist ein Vorschlag für eine Richtlinie über *Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union*[116].

Im folgenden wird lediglich paradigmatisch auf die rechtliche Situation in Deutschland sowie einschlägige inter- bzw. supranationale Vereinbarungen vertiefend eingegangen (vgl. Tabelle 5.2). Für einen entsprechenden Überblick hinsichtlich der USA sei darüber hinaus auf Burstein (2003) verwiesen. Ein analytischer Vergleich der Regulierung des eCommerce in beiden Rechtsräumen findet sich bei Schulzki-Haddouti (2000). Die Dissertation von Pfister (2007) vergleicht einschlägige Strafrechtsnormen in der Schweiz, Deutschland und Österreich. Sieber (1996, 1998, 2008) gibt einen grundlegenden Überblick zur deutschen sowie europäischen Rechtslage, während die Dissertation von Beukelmann (2001) juristische Aspekte und Möglichkeiten der Prävention elektronischer Kriminalität im allgemeinen aufzeigt. Die Dissertation von Koch (2008) beleuchtet strafrechtliche Probleme des Angriffs sowie der Verteidigung in Computernetzen. Der Sammelband von Hilgendorf (2004) sowie die Monographie von Hilgendorf et al. (2005) befassen sich mit dem deutschen Computer- und Internetstrafrecht. Insbesondere Frank (2004a) geht hier vertiefend auf strafrechtliche Instrumentarien gegen Software mit Schadensfunktionen ein. In seiner Dissertation untersucht Frank (2004b) ferner strafrechtliche Möglichkeiten zur Bekämpfung unseriöser Werbung (Spam). Wennerström (2004) schließlich beschäftigt sich mit der legislativen Regulierung elektronischer Kriminalität auf europäischer Ebene.

Zusammenfassend läßt sich eine Reihe zentraler Stationen in Gesetzgebung und Jurisdiktion auf fast allen Rechtsgebieten ausmachen. Schwerpunkte liegen dabei im Datenschutz (Grund- und Persönlichkeitsrechte), im Strafrecht (computerspezifische

115 Vgl. gemeinsame Mitteilung der Kommission und der Hohen Vertreterin für Außen- und Sicherheitspolitik JOIN(2013) 1 vom 7. Februar 2013.

116 Vgl. Mitteilung der Kommission KOM(2013) 48 vom 7. Februar 2013.

TABELLE 5.2: *Meilensteine inter- und supranationaler Harmonisierung*

Fokus	*Regime*	*Jahr*
Datenschutz	OECD-Richtlinien	1980
	Konvention des Europarates	1981
	UN-Richtlinien	1990
	EU-Richtlinie 95/46/EG	1995
	USA/EU-"Safe Harbor"-Vereinbarung	2000
	EU-Richtlinie 2002/58/EG	2002
Strafrecht	OECD-Empfehlungen	1986
	Empfehlungen des Europarates Nr. R (89) 9	1989
	OECD-Richtlinien	1992
	UN-Resolution 55/63	2000
	EU-Rahmenbeschluß 2001/413/JI	2001
	Cybercrime-Konvention des Europarates	2001
	UN-Resolution 56/121	2001
	UN-Resolution 56/261	2002
	erneuerte OECD-Richtlinien	2002
	EU-Rahmenbeschluß 2004/68/JI	2004
	EU-Rahmenbeschluß 2005/222/JI	2005
	EU-Richtlinie 2006/24/EG	2006
	EU-Richtlinie 2013/40/EU	2013
Geistiges Eigentum	EU-Richtlinie 91/250/EWG	1991
	WTO-TRIPS	1994
	UN/WIPO-Vertrag	1996
	EU-Richtlinie 96/9/EG	1996
	EU-Richtlinie 98/84/EG	1998
	EU-Richtlinie 2001/29/EG	2001
	Konvention des Europarates	2001
	EU-Richtlinie 2004/48/EG	2004
Vertragsrecht	EU-Richtlinie 1999/93/EG	1999
	EU-Richtlinie 2000/31/EG	2000

Kriminalität), im Urheberrecht (geistiges Eigentum) sowie im Vertragsrecht (elektronische Signatur).

5.1.1.1 Datenschutz

Zunächst gelangte Ende der 1960er Jahre das Thema des Datenschutzes[117] auf die politische Agenda. Der zunehmende Einsatz elektronischer Großrechenanlagen in Wirtschaft und Verwaltung ermöglichte seit den 1960er Jahren in umfassendem Maße die Speicherung und Verarbeitung personenbezogener Daten und stellte damit neue Herausforderungen an den Schutz der Persönlichkeitsrechte. Als erstes deutsches Bundesland reagierte 1970 Hessen mit einem Datenschutzgesetz (HDSG[118]). Schon bald folgten weitere Bundesländer und 1977 der Bund (BDSG[119]) mit eigenen Datenschutzgesetzen, die den Umgang mit personenbezogenen Daten sowohl für den privaten als auch öffentlichen Sektor regeln. Anläßlich einer Klage gegen das Volkszählungsgesetz von 1983 leitete schließlich das Bundesverfassungsgericht in seinem Urteil[120] vom Dezember 1983 aus Art. 2 Abs. 1 des Grundgesetzes in Verbindung mit Art. 1 Abs. 1 ein allgemeines Grundrecht auf „informationelle Selbstbestimmung“ ab. Novellierungen des BDSG folgten 1990, 2001 und 2009.

Auch in anderen Ländern wurden ähnliche Gesetze verabschiedet (vgl. Abbildung 5.1), wobei im Kern jeweils folgende Prinzipien zugrundeliegen: (1) die Vermeidung unnötiger Daten, (2) die Zweckgebundenheit von Daten, (3) der Schutz von Daten gegen unbefugten Zugriff, (4) ein Auskunftsrecht Betroffener. Parallel dazu kam es auf inter- bzw. supranationaler Ebene zu ersten Harmonisierungsbemühungen: Im Jahr 1980 einigten sich die Staaten der OECD auf *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*; 1981 verabschiedete der Europarat das *Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten*[121] und 1990 beschlossen die Vereinten Nationen die *Guidelines for the Regulation of Computerized Personal Data Files*[122]. Innerhalb der Europäi-

117 Der Begriff des Datenschutzes im engeren Sinne bezieht sich ausschließlich auf den Schutz personenbezogener Daten. Er ist jedoch nur im Kontext eines umfassenderen Konzeptes der Privatsphäre (Privacy) als Gegenbegriff und damit Ausschluß von Öffentlichkeit zu verstehen, dessen Teil er bildet. In diesem Sinne ist Datenschutz in elektronischen IuK-Systemen mit der Privatsphäre der Person gleichzusetzen, während sich das Fernmeldegeheimnis auf die Privatsphäre der Kommunikation bezieht.

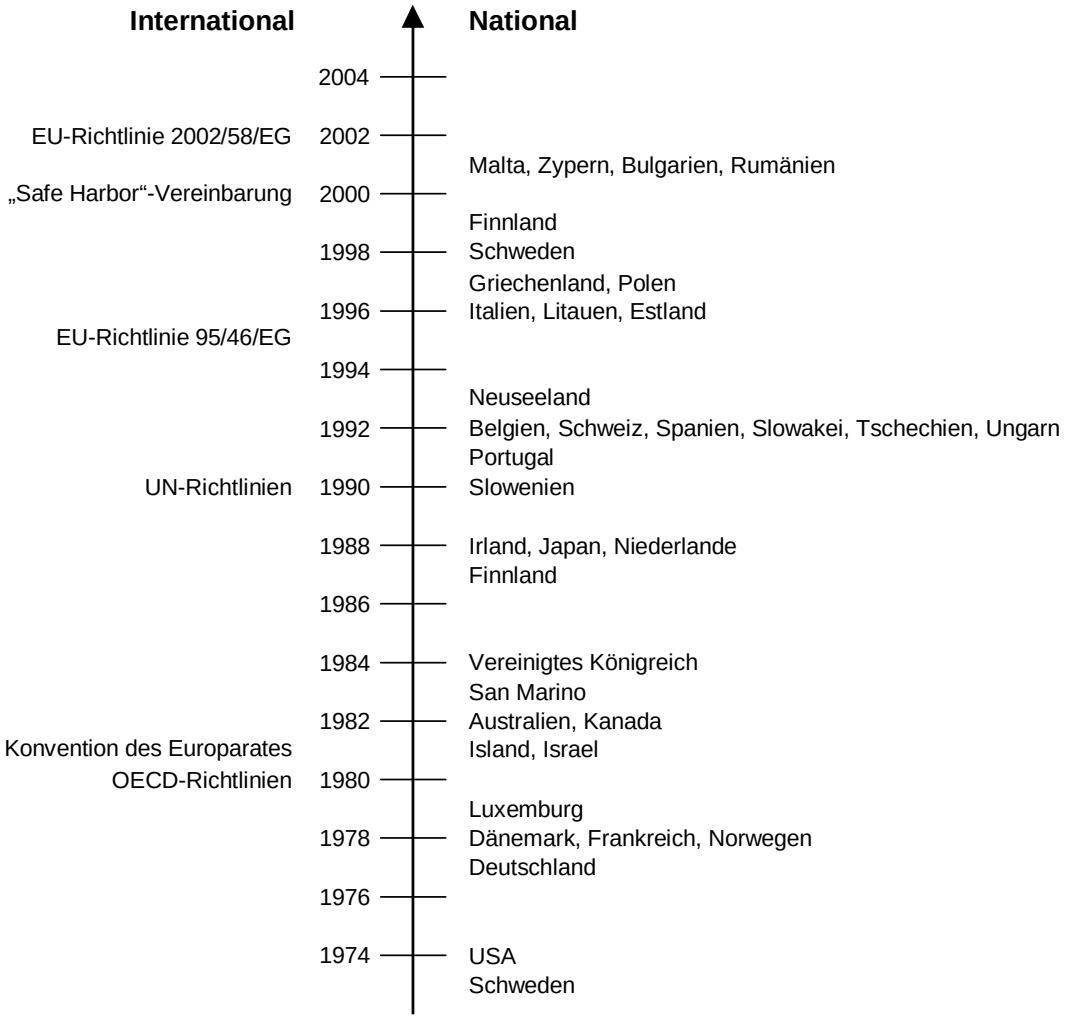
118 Hessisches Datenschutzgesetz vom 7. Oktober 1970, GVBl. I 625.

119 Bundesdatenschutzgesetz (BDSG) vom 27. Januar 1977, BGBl. I 201.

120 BVerfGE 65, 1 vom 15. Dezember 1983.

121 Konvention Nr. 108 des Europarates vom 28. Januar 1981, in Kraft getreten am 1. Oktober 1985.

122 Resolution 45/95 der UN-Vollversammlung vom 14. Dezember 1990.



Quelle: Sieber (1998: 33). Modifiziert, ergänzt und aktualisiert.

Abbildung 5.1: *Anpassungen im Datenschutz*

schen Union wurde die gesetzliche Regulierung des Datenschutzes über die *Richtlinien zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr*[123] von 1995 sowie über *den Datenschutz in der elektronischen Kommunikation*[124] von 2002 harmonisiert.

Im Gegensatz zu den meisten anderen Staaten blieb eine proaktive Regulierung

123 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995.

124 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002.

des Datenschutzes in den USA zumeist auf den öffentlichen Sektor beschränkt. Ausnahmen sind etwa der *Health Insurance Portability and Accountability Act*[125], welcher u. a. persönliche Gesundheitsdaten schützt sowie der *Gramm-Leach-Bliley Act*[126], welcher datenschutzrechtliche Bestimmungen für den Finanzsektor enthält (vgl. Buchner 2006: 16 f.). Hinsichtlich des privaten Sektors präferierten die USA ansonsten eine Selbstregulierung. Die von Seiten der Wirtschaft selbst auferlegten Verfahrensregeln lassen sich dabei allenfalls privatrechtlich einklagen. Vor allem in der EU – aber auch in vielen Staaten Mittel- und Osteuropas sowie in Kanada, Australien und Neuseeland – wurde Datenschutz hingegen als ein durch die öffentliche Hand zu gewährleistendes Grundrecht begriffen. Dementsprechend existieren hier umfangreiche gesetzliche Regelungen auch für den privaten Sektor (vgl. Drozdova 2001). Das damit zwischen der EU und den USA entstehende Regulierungsgefälle führte nach zweijährigen Verhandlungen im Jahr 2000 mit der sog. *Safe-Harbor*-Vereinbarung zu einer spezifischen Sonderlösung. Personenbezogene Daten dürfen demnach aus der EU heraus nur an solche US-Unternehmen transferiert werden, die sich freiwillig gegenüber dem US-Handelsministerium zur Einhaltung bestimmter Sicherheitsrichtlinien verpflichten, die ein den europäischen Bestimmungen entsprechendes Datenschutzniveau gewährleisten sollen (vgl. Fink 2002; Long u. Quek 2002; Farrell 2002, 2003).

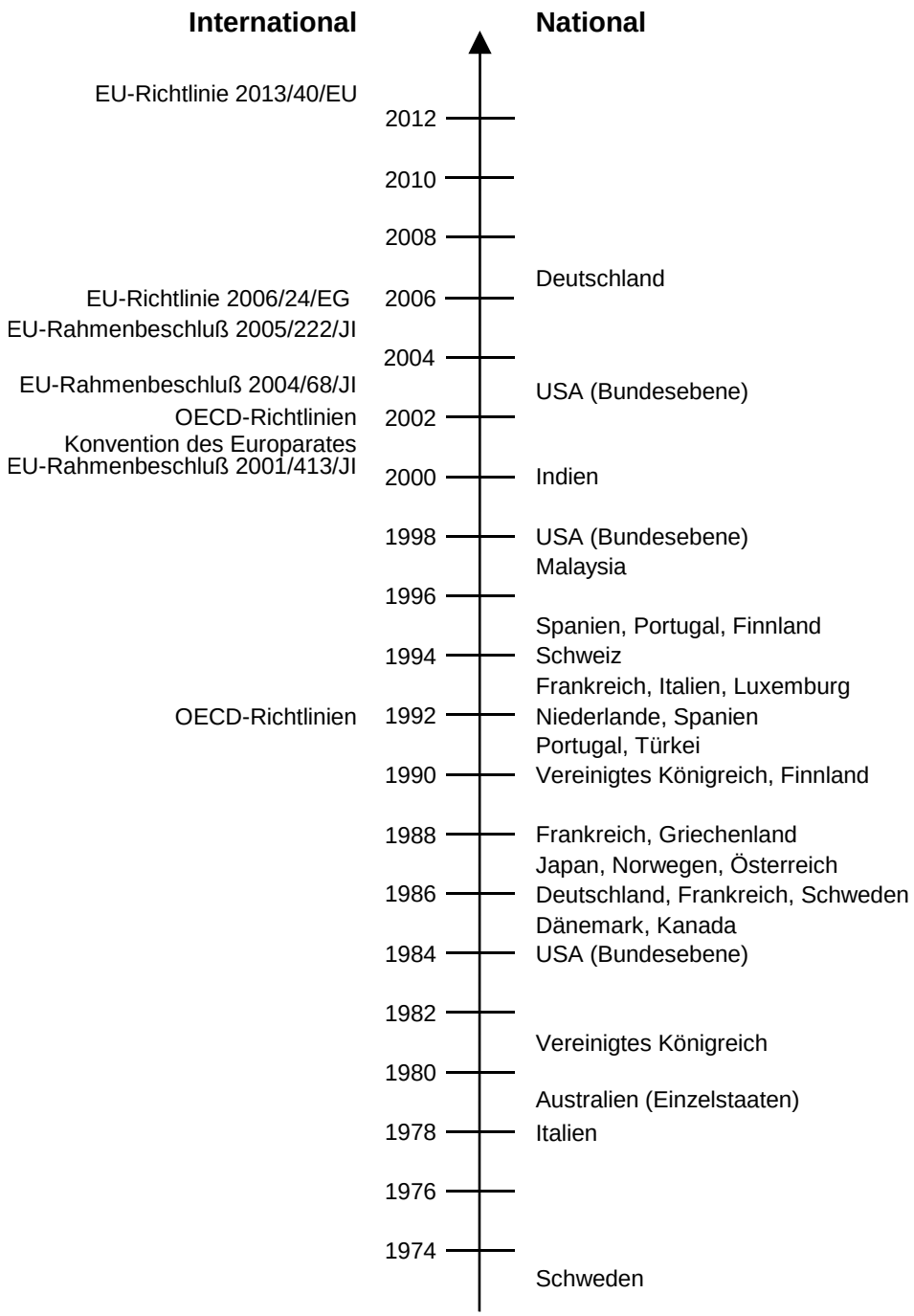
5.1.1.2 Strafrecht

Nach dem Datenschutz rückten vermehrt Fragen der Wirtschaftskriminalität in den Mittelpunkt öffentlicher Aufmerksamkeit. In den 1970er Jahren traten vor allem im Zusammenhang mit Bankomaten – aber auch in betrieblich genutzten Großrechenanlagen – gehäuft Fälle von Computermanipulation, -sabotage und -spionage auf, die sich nur bedingt unter geltendes Recht subsumieren ließen. In fast allen wichtigen Industriestaaten kam es in der Folge zu einer Reformwelle im nationalen Strafrecht (vgl. Abbildung 5.2). In Deutschland wurde nach mehrmaliger Verzögerung – zuletzt durch die verkürzte Legislaturperiode des neunten Deutschen Bundestages – 1986 das *2. WiKG*[127] verabschiedet. Dieses ergänzte u. a. das Strafgesetzbuch (StGB) um die Straftatbestände des „Ausspähens von Daten“ (§ 202a), der „Veränderung oder Vernichtung von Daten“

125 Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. §§ 201 f.

126 Gramm-Leach-Bliley Financial Services Modernization Act of 1999 (GLBA), 15 U.S.C. §§ 501 ff.

127 Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität vom 15. Mai 1986, BGBl. I 721.



Quelle: Sieber (1998: 33). Modifiziert, ergänzt und aktualisiert.

ABBILDUNG 5.2: *Anpassungen im Strafrecht*

(§ 303a) und der „Fälschung oder Veränderung beweiserheblicher Daten“ (§ 269) sowie der „Computersabotage“ (§ 303b), des „Computerbetruges“ (§ 263a) und der „Beeinflussung einer Datenverarbeitung im Rechtsverkehr“ (§ 270). Durch das 41. *StrÄndG*[128] kamen 2007 ferner die Straftatbestände „Abfangen von Daten“ (§ 202b) und „Vorbereiten des Ausspähens und Abfangens von Daten“ (§ 202c) hinzu. In den USA finden sich entsprechende Strafrechtsnormen im *Computer Fraud and Abuse Act*[129] von 1984, dessen Bestimmungen jeweils 1994, 1996 und 2001 ergänzt und erweitert wurden. Die Änderung von 2001 dehnt den Schutz des Gesetztes erstmals explizit auch auf Computer außerhalb der USA aus, sofern deren Anwendung Handel oder Kommunikation der USA im Innern oder Äußern betreffen.

Ein erster rudimentärer Schritt in Richtung einer internationalen Harmonisierung des Strafrechts waren die Empfehlungen der OECD aus dem Jahre 1986, betreffend die Manipulation von Computer-Systemen, computerbezogene Fälschung, die Störung von Computer-Systemen und -Daten, die Verletzung von Urheberrechten an Computer-Programmen sowie den illegalen Zugriff auf Compter-Systeme und -Netzwerke.[130] Hieran schließen im Jahre 1992 *Richtlinien zur Sicherheit von Informationssystemen* an (vgl. Jackson 2000). Diese haben den unverbindlichen Charakter einer allgemein gehaltenen Empfehlung, welche neun Prinzipien zur Gewährleistung von Sicherheit in IuK-Systemen umfaßt: (1) die Verantwortlichkeit von Eigentümern, Betreibern und Nutzern von IuK-Systemen für deren Sicherheit; (2) deren Sensibilisierung hinsichtlich der Umsetzung von Sicherheitsmaßnahmen; (3) die Befolgung ethischer Richtlinien, insbesondere die Berücksichtigung der Rechte Dritter; (4) eine multidisziplinäre Herangehensweise bei der Entwicklung von Sicherheitsmaßnahmen; (5) die Ausgewogenheit von Sicherheitsmaßnahmen und Risiken; (6) internationale Zusammenarbeit zur Entwicklung eines kohärenten Sicherheitssystems; (7) eine zeitnahe Reaktion auf Sicherheitsvorfälle; (8) eine ständige Neubewertung der Sicherheitslage; (9) die Berücksichtigung demokratischer Werte. Im Jahr 2002 wurden diese Richtlinien durch eine leicht veränderte Version abgelöst. Deren Prinzipien lauten nunmehr: (1) eine allgemeine Sensibilisierung; (2) die Verantwortung aller für die Sicherheit von IuK-Systemen;

128 Einundvierzigstes Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (41. StrÄndG) vom 7. August 2007, BGBl. I 1786.

129 Computer Fraud and Abuse Act of 1984 (CFAA), 18 U.S.C. § 1030 f.

130 Vgl. Schlußbericht der OECD DSTI/ICCP 84.22 vom 18. April 1986: „Computer-Related Criminality: Analysis of Legal Policy in the OECD-Area“.

(3) eine gegenseitige Unterstützung bei der Bewältigung von Sicherheitsvorfällen; (4) die Anerkennung gegenseitiger Interessen; (5) die Berücksichtigung demokratischer Werte; (6) eine Risikoeinschätzung unter Berücksichtigung internationaler Interdependenzen; (7) die besondere Beachtung von Sicherheitskriterien beim Technik-Design; (8) ein umfassendes Sicherheitsmanagement; (9) eine ständige Neubewertung der Sicherheitslage.

Bereits im Jahre 1989 hatte der Europarat in seiner Empfehlung Nr. R(89) 9 den Mitgliedsstaaten nahegelegt, Computer-Betrug, Computer-Fälschung, Beschädigung von Computerdaten, Computer-Sabotage sowie die nicht-authorisierte Vervielfältigung von Computerprogrammen unter Strafe zu stellen. Als Durchbruch hinsichtlich einer grenzüberschreitenden Verfolgung und Ahndung computerspezifischer Straftaten gilt dann die im Jahre 2001 folgende *Budapester Konvention*[131], auch bekannt als *Cybercrime-Konvention* (vgl. Kaspersen 2003; Lewis 2003c). Dieses Übereinkommen ist der erste internationale Vertrag zur Bekämpfung von Kriminalität in elektronischen Netzwerken unter besonderer Berücksichtigung von Angriffen auf die Netz- und Datensicherheit, des Betruges und der Fälschung, der Verbreitung von Kinderpornographie sowie der Verletzung geistiger Eigentumsrechte. Die Konvention steht neben den Mitgliedern des Europarates auch anderen Staaten offen und wurde bisher zusätzlich von Kanada, Japan, Südafrika und den USA unterzeichnet. Inhalt der Konvention sind u. a. Fragen der Strafbarkeit und Haftung, der gegenseitigen Rechtshilfe und Auslieferung Verdächtiger, des Informationsaustauschs sowie der Sicherstellung elektronischer Beweise.

Letzteres erfordert – neben der Möglichkeit des Abhörens und Aufzeichnens von Telekommunikationsverbindungen[132] – vor allem eine längerfristige Aufbewahrung (bis zu 90 Tage) sowie ggf. Offenlegung von Verbindungsdaten und kollidiert daher tendenziell mit den Grundrechten des Datenschutzes und des Fernmeldegeheimnisses (vgl. hierzu Yar 2006: 148 ff.). Für Deutschland finden sich entsprechende Normen zur sog. Vorratsdatenspeicherung im *Telekommunikationsgesetz* (TKG)[133] von 2004. Die europäische *Richtlinie über die Vorratsspeicherung von Daten*[134] aus dem Jahr 2006 sieht im Vergleich zu den Vorgaben der Budapester Konvention sogar nochmals erweiterte Fristen (6 bis 24 Monate) der Vorratsdatenspeicherung vor. Zudem wird der Katalog der zu

131 Konvention Nr. 185 des Europarates vom 23. November 2001, in Kraft getreten am 1. Juli 2004.

132 Diese ist in Deutschland in der Telekommunikations-Überwachungsverordnung (TKÜV) geregelt.

133 Telekommunikationsgesetz in der Neufassung vom 22. Juni 2004, BGBl. I 1190.

134 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006.

erfassenden Verbindungsdaten erheblich ausgeweitet. Die Umsetzung dieser Richtlinie erfolgte in Deutschland Ende 2007 durch eine Novellierung des TKG.[135] Anfang 2010 urteilte jedoch das Bundesverfassungsgericht, daß die derzeitige Regelung der Vorratsdatenspeicherung in Deutschland verfassungswidrig und somit nichtig sei.[136] Dennoch sei eine neue Regelung, welche eine höhere Datensicherheit sowie eine enger gefaßte Begrenzung der Verwendungszwecke gespeicherter Daten beinhalte, grundsätzlich zulässig. Darüber hinaus hat Irland vor dem Europäischen Gerichtshof aus formellen Gründen Klage gegen die Richtlinie 2006/24/EG erhoben, die jedoch Anfang 2009 abgewiesen wurde.[137]

Der traditionelle Zielkonflikt zwischen den bürgerlichen Persönlichkeits- und Freiheitsrechten (Privatsphäre) des Einzelnen einerseits, sowie einem kollektiven, öffentlichen Sicherheitsinteresse an der Repression von Straftaten andererseits, setzt sich damit im elektronischen Handlungsraum fort (vgl. Poullet 2004). Reitinger (2000) argumentiert, daß sich bei einer rein marktgesteuerten Entwicklung das Gleichgewicht stark zuungunsten einer effektiven Strafverfolgung verschöbe, da immer wirkungsvollere Techniken der Kryptographie und Anonymisierung forensische Analysen sowie die Beschlagnahme von Beweisen zunehmend erschwerten. Tatsächlich steht eine umfassende Regulierung von Kryptographietechnologien daher immer wieder zur Diskussion, wobei die Vorschläge von einem totalen Verbot bestimmter Verfahren über eine gesetzlich geforderte technische Implementation von Hintertüren bis zur verpflichtenden Hinterlegung der Schlüssel bei öffentlichen Stellen oder einer Trusted Third Party reichen (vgl. Koop 2008).

In diesem Zusammenhang ist auch ein striktes Exportverbot für besonders sichere Kryptographieverfahren zu verstehen, das in den USA bis in das Jahr 2000 galt. Allerdings konnte auch dieses Verbot eine grenzüberschreitende Diffusion neuer Technologien nicht nachhaltig verhindern, stellte aber de facto einen bedeutenden Wettbewerbsnachteil für die amerikanische Wirtschaft dar. Dieser Umstand führte letztlich zu einer Lockerung der Bestimmungen. Auf internationaler Ebene beschloß die OECD 1997 *Guidelines for Cryptography Policy*. Diese nicht verpflichtenden Empfehlungen sol-

135 Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007, BGBl. I 3198.

136 Vgl. Pressemitteilung des BVerfG Nr. 11/2010 vom 2. März 2010.

137 Vgl. Pressemitteilung des EuGH Nr. 11/2009 vom 10. Februar 2009 zur Rs. C-301/06.

len sicherstellen, daß mögliche nationale Regulierungen der Kryptographie den freien internationalen Austausch von Informationen nicht behindern.

Hinsichtlich einer Harmonisierung des Informationsstrafrechts innerhalb der EU sind ferner eine Reihe einschlägiger Rahmenbeschlüsse relevant, die auf Grundlage des *Amsterdamer Vertrages*[138], der u. a. Einzelheiten der polizeilichen und justiziellen Zusammenarbeit[139] der EU-Länder regelt, gefaßt wurden. Diese Rahmenbeschlüsse entfalten nach einem Urteil[140] des Europäischen Gerichtshofes – ähnlich der Richtlinien des Rates und des Parlaments – unmittelbare Wirkung für Rechtsprechung und Verwaltung der einzelnen Mitgliedstaaten.[141] Hierzu zählt der *Rahmenbeschluß zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln*[142] von 2001, der *Rahmenbeschluß zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornographie*[143] von 2003 sowie der *Rahmenbeschluß über Angriffe auf Informationssysteme*[144] von 2005. Letzterer befaßt sich insbesondere mit den Straftatbeständen des „rechtswidrigen Zugangs zu Informationssystemen", des „rechtswidrigen Systemeingriffs" sowie des „rechtswidrigen Eingriffs in Daten". Auf eine europaweite Angleichung der sich auf Angriffe auf Informationssysteme beziehenden Straftatbestände sowie eine Verbesserung der internationalen Zusammenarbeit der Strafverfolgungsbehörden in diesem Bereich zielt schließlich auch die *Richtlinie über Angriffe auf Informationssysteme*[145] von 2013, die zugleich den Rahmenbeschluß 2005/222/JI ablöst. Seit Anfang 2013 existiert beim Europäischen Polizeiamt Europol ferner ein Europäisches Zentrum zur Bekämpfung der Cyberkriminalität, welches der Koordination einer grenzübergreifenden Strafverfolgung dient.

Eine Harmonisierung des Informationsstrafrechtes auf globaler Ebene ist Ziel der

138 Unterzeichnet am 2. Oktober 1997, in Kraft getreten am 1. Mai 1999.

139 Hierbei handelt es sich um die sog. dritte Säule der Europäischen Union, die gemäß dem Vertrag von Maastricht ergänzend neben die Europäischen Gemeinschaften (Wirtschafts- und Sozialpolitik) sowie die Gemeinsame Außen- und Sicherheitspolitik (GASP) tritt.

140 EuGH Rs. C-105/03 vom 16. Juni 2005.

141 Vgl. Frankfurter Allgemeine Zeitung Nr. 138 vom 17.06.2005, S. 2.

142 Rahmenbeschluß 2001/413/JI des Rates vom 28. Mai 2001.

143 Rahmenbeschluß 2004/68/JI des Rates vom 22. Dezember 2003.

144 Rahmenbeschluß 2005/222/JI des Rates vom 24. Februar 2005.

145 Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013.

UN-Resolutionen 55/63[146] aus dem Jahre 2001 sowie *56/261*[147] aus dem Jahre 2002. Resolution 55/63 hält die Mitgliedsstaaten an, sicherzustellen, daß die jeweilige nationale Rechtspraxis keine rechtsfreien Räume für den kriminellen Mißbrauch von Informationstechnologien eröffnet sowie den Schutz, die Vertraulichkeit und die Verfügbarkeit von Daten und Computer-Systemen gewährleistet. Resolution 56/261 fordert nochmals dazu auf, den Mißbrauch von Informationstechnologien unter Strafe zu stellen sowie die juristische Aufarbeitung grenzüberschreitender Verstöße zu regeln.

5.1.1.3 Urheberrecht

Die zunehmende Verbreitung von Personal- und Heimcomputern in den 1980er Jahren eröffnete einer großen Zahl privater Anwender die technischen Möglichkeiten einer digitalen und somit verlustfreien Vervielfältigung großer Datenmengen. Diese Entwicklung brachte vor allem Probleme hinsichtlich einer Verletzung geistiger Eigentumsrechte mit sich. Die bestehenden Gesetze berücksichtigten zumeist die spezifischen Eigenschaften immaterieller digitaler Güter nur unzureichend und machten daher Anpassungen erforderlich. Da Software nicht weltweit patentrechtlich geschützt werden kann, wurde der Ruf nach zivil- und strafrechtlichen Alternativen des Urheberrechtsschutzes laut (Sieber 1996: 631). In Deutschland führte dies u. a. 1985 zu einer Anpassung des *Urheberrechtsgesetzes*[148] (UrhG) von 1965 sowie 1990 zur Verabschiedung des *Produktpirateriegesetzes*[149] (PPG).

Im Rahmen der Verhandlungen zum Allgemeinen Zoll- und Handelsabkommen (GATT) in Uruguay wurde 1994 insbesondere auf Betreiben der USA mit dem *Agreement on Trade-Related Aspects of Intellectual Property Rights* (TRIPS) ein multilateraler Zusatzvertrag geschlossen, der Minimalstandards zum Schutz der Eigentumsrechte an immateriellen Gütern international verbindlich festschreibt. Seine Unterzeichnung ist zwingende Voraussetzung eines Beitritts zur Welthandelsorganisation. Darüber hinaus verabschiedete 1996 die World Intellectual Property Organization (WIPO), eine Teilorganisation der UNO, einen internationalen Urheberrechtsvertrag, laut dessen sich

146 Resolution 55/63 der UN-Vollversammlung vom 22. Januar 2001.

147 Resolution 56/261 der UN-Vollversammlung vom 15. April 2002.

148 Gesetz über Urheberrecht und verwandte Schutzrechte vom 9. September 1965, BGBl. I 1273.

149 Gesetz zur Stärkung des geistigen Eigentums und zur Bekämpfung der Produktpiraterie vom 7. März 1990, BGBl. I 422.

die Signatarstaaten verpflichten, Software gesetzlich analog zu literarischen Werken zu schützen. Implementiert wird dieser in den USA durch den *Digital Millennium Copyright Act*[150] von 1998 sowie in der EU durch die *Richtlinie über das Urheberrecht und verwandte Schutzrechte in der Informationsgesellschaft*[151] von 2001. Beide gewähren exklusive Eigentumsrechte an immateriellen Gütern und stellen das Umgehen technischer Schutzmaßnahmen unter Strafe. De jure wird damit die Verschlüsselung digitaler Daten dem Verwahren materieller Güter in besonders gesicherten Räumen gleichgestellt (Burstein 2003: 317).

Auf europäischer Ebene sind hinsichtlich des Schutzes von Eigentumsrechten an immateriellen Gütern ferner insbesondere die *Richtlinien über den Rechtsschutz von Computerprogrammen*[152] aus dem Jahr 1991, *über den rechtlichen Schutz von Datenbanken*[153] aus dem Jahr 1996 sowie *zur Durchsetzung der Rechte des geistigen Eigentums*[154] aus dem Jahr 2004 von Bedeutung. Die Umsetzung dieser Richtlinien in nationales Recht erfolgte in Deutschland im wesentlichen 1993, 1997 und 2003 jeweils durch eine Novellierung des UrhG sowie ein Artikelgesetz[155] aus dem Jahre 2008, welches u. a. Anpassungen am UrhG vornimmt, die im Falle einer illegalen Weitergabe bzw. Vervielfältigung digitaler Güter den jeweiligen Rechteinhabern einen Anspruch auf Herausgabe von Verbindungsdaten durch die Anbieter von Telediensten (Provider) einräumen.

Die Strafbarkeit der Umgehung technischer Schutzmaßnahmen der Zugangskontrolle zu immateriellen Gütern regelt die europäische *Richtlinie über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten*[156]. Analog hierzu dehnt ein *Europäisches Übereinkommen über Rechtsschutz für Dienstleistungen mit bedingtem Zugang und der Dienstleistungen zu bedingtem Zugang*[157] des Europarates diese Harmonisierungsbestrebungen noch über den Rahmen der EU hinaus aus. In

150 Digital Millennium Copyright Act of 1998 (DMCA).

151 Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001.

152 Richtlinie 91/250/EWG des Rates vom 14. Mai 1991.

153 Richtlinie 96/9/EG des Europäischen Parlaments und des Rates vom 11. März 1996.

154 Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004.

155 Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums vom 7. Juli 2008, BGBl. I 1191.

156 Richtlinie 98/84/EG des Europäischen Parlaments und des Rates vom 20. November 1998.

157 Konvention Nr. 178 des Europarates vom 24. Januar 2001, in Kraft getreten am 1. Juli 2003.

Deutschland wurden die einschlägigen rechtlichen Grundlagen hierfür 2002 durch das *Zugangskontrolldiensteschutz-Gesetz*[158] (ZKDSG) geschaffen.

5.1.1.4 Vertragsrecht

Nachdem eine weitgehende Vernetzung von Personal- und Heimcomputern im Rahmen des Internet in den 1990er Jahren neue Formen des elektronischen Rechtsverkehrs ermöglichte, wurden auch auf dem Gebiet des Vertragsrechts umfangreiche Gesetzesanpassungen notwendig. Zugleich rückte die Kritizität von Iuk-Systemen für moderne Volkswirtschaften in den Fokus öffentlicher Aufmerksamkeit. Im Jahr 1996 setzte der Deutsche Bundestag eine Enquete-Kommission „Zukunft der Medien in Wirtschaft und Gesellschaft; Deutschlands Weg in die Informationsgesellschaft“ ein, die sich auch mit der Sicherheit in elektronischen Netzen befaßte (vgl. Deutscher Bundestag 1998).

Im Jahr 1997 wurde das *Informations- und Kommunikationsdienstegesetz*[159] (IuKDG) – auch bekannt als „Multimediagesetz“ – verabschiedet. Dieses Artikelgesetz umfaßte Einzelgesetze zur „Nutzung von Telediensten“ (TDG), zum „Datenschutz in Telediensten“ (TDDSG) und zur „digitalen Signatur“ (SigG), näher ausgeführt durch die *Signaturverordnung* (SigVO), sowie eine Reihe von Anpassungsänderungen, u. a. im Strafgesetzbuch (StGB) sowie im Urheberrecht (UrhG). Das TDG regelte in Verbindung mit dem *Mediendienste-Staatsvertrag* (MDStV) der Länder Fragen der Verantwortlichkeit hinsichtlich illegaler Inhalte in elektronischen Netzen (Sieber 1999),[160] während das TDDSG Anbieter von Telediensten verpflichtete, deren Nutzung nach Möglichkeit anonym oder unter Angabe eines Pseudonyms zu ermöglichen und zugleich die Verwertung personenbezogener Nutzungsdaten durch die Betreiber selbst einschränkte. Darüber hinaus räumte es dem Nutzer Auskunftsrechte bezüglich dieser Daten ein. Das SigG regelt Inhalt und Vergabe von Zertifikaten im Rahmen einer Public

158 Gesetz über den Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten vom 19. März 2002, BGBl. I 1090.

159 Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste vom 22. Juli 1997, BGBl. I 1870.

160 Im föderalen System Deutschlands wird Telekommunikation (Fernmeldewesen) traditionell als gesamtstaatliche Infrastrukturaufgabe erachtet, die in die Kompetenz des Bundes fällt; während die Regulierung der Medien und ihrer Inhalte aufgrund der Nähe zur Kulturpolitik in der Kompetenz der Länder verbleibt. Diese Eigenheit erzwang vor dem Hintergrund der Konvergenz der Medien- und Kommunikationstechnik eine enge Kooperation von Bund und Ländern. Bezüglich des Internet wurde die Abgrenzung von Tele- und Mediendiensten jedoch 2007 durch das Telemediengesetz aufgehoben.

Key Infrastructure. Das deutsche IuKDG galt als europaweit einmaliges Pilotprojekt. Die gewonnen Erfahrungen flossen in die einschlägigen europäischen *Richtlinien über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen*[161] von 1999 sowie *über rechtliche Aspekte des elektronischen Geschäftsverkehrs*[162] von 2000 ein.

Deren Umsetzung erfolgte in Deutschland 2001 durch eine Neufassung von SigG und SigVO in Verbindung mit dem *Formanpassungsgesetz*[163] einerseits, sowie durch das *Gesetz zum elektronischen Geschäftsverkehr*[164] (EGG) andererseits. Das EGG, ebenfalls ein Artikelgesetz, novelliert vor allem einschlägige Vorschriften des TDG, des TDDSG sowie der Zivilprozeßordnung (ZPO) hinsichtlich europäischer Vorgaben. So wird etwa der elektronischen Signatur in der ZPO nunmehr Beweiskraft zugebilligt. Anfang 2007 schließlich wurde das TDG und das TDDSG sowie große Teile des MDStV durch das *Telemediengesetz*[165] (TMG) ersetzt, das die bestehenden Vorschriften zusammenfassend vereinheitlicht und um weitere Bestimmungen zum Schutz vor unerwünschter Werbung sowie zur Haftung der Provider für die von ihnen vermittelten Inhalte Dritter ergänzt und damit der Konvergenz vom Medien- und Kommunikationstechnik in besonderer Weise Rechnung trägt.

Das SigG von 2001 unterscheidet in § 2 Abs. 1 bis 3 gemäß den Erfordernissen der Richtlinie 2000/31/EG neben einfachen „elektronischen Signaturen“, die lediglich der Authentifikation bestimmter Daten dienen, ferner zwischen „fortgeschrittenen“ und „qualifizierten“ Signaturen. Erstere erlauben zusätzlich eine eindeutige Identifikation ihres Urhebers, während letztere darüber hinaus auf einem durch eine qualifizierte Zertifizierungsstelle ausgestellten Zertifikat beruhen. Aus diesem muß, neben dem Namen der Zertifizierungsstelle, u. a. der Name – oder aber ein eindeutiges Pseudonym – des Signaturschlüsselinhabers und der Signaturprüfschlüssel (Public Key) sowie dessen Gültigkeitsdauer hervorgehen (§ 7 SigG). Qualifizierte Zertifizierungsstellen sind gegenüber der Bundesnetzagentur[166] als zuständiger Regulierungsbehörde meldepflichtig und un-

161 Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999.

162 Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000.

163 Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr vom 13. Juli 2001, BGBl. I 1542.

164 Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr vom 14. Dezember 2001, BGBl. I 3721.

165 Verkündet im Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz vom 26. Februar 2007, BGBl. I 179.

166 Vormals Regulierungsbehörde für Telekommunikation und Post.

terliegen einer Reihe von technischen und organisatorischen Auflagen hinsichtlich der Erzeugung und Verwaltung von Schlüsseln sowie der Vergabe und Dokumentation von Zertifikaten. Auf Antrag werden sie von der Bundesnetzagentur explizit akkreditiert (zertifiziert), womit diese dann zugleich als Wurzelstelle (Root Authority) einer Public Key Infrastructure fungiert.

Das Formanpassungsgesetz 2001 fügt die §§ 126a und 126b in das Bürgerliche Gesetzbuch (BGB) ein. Ersterer stellt qualifizierte elektronische Signaturen der handschriftlichen Unterschrift in der bisherigen gesetzlichen Schriftform weitgehend gleich, während letzterer eine sog. „Textform" als alternatives Formerfordernis und Voraussetzung der juristischen Gültigkeit bestimmter Rechtsgeschäfte ohne erhebliche Rechtsfolgen einführt. Die Textform ist zwar an eine dauerhafte schriftliche Wiedergabe gebunden, sieht von einer handschriftlichen Unterschrift aber ab und eignet sich daher für eine vereinfachte elektronische Verarbeitung von Rechtsgeschäften in besonderem Maße. Durch eine Novelle[167] des Verwaltungsverfahrensgesetzes (VwVfG) findet 2002 die qualifizierte elektronische Signatur dann auch Eingang in das öffentliche Recht (§ 3a), so etwa im Rahmen des elektronischen Verwaltungsaktes (§ 37). Das *Justizkommunikationsgesetz*[168] (JKomG) von 2005 schließlich regelt Formen elektronischer Aktenbearbeitung für das Rechtswesen selbst.

Ähnlich wie bei der Regulierung des Datenschutzes gibt es auch bei der gesetzlichen Ausgestaltung elektronischer Signaturen gravierende Unterschiede zwischen der EU und den USA (vgl. Gollan u. Meinel 2001). Während in Europa insbesondere technische und organisatorische Verfahren der Schlüsselerzeugung und -verwaltung sowie der Vergabe und Dokumentation von Zertifikaten im Rahmen einer hierarchischen PKI detailliert geregelt sind, läßt der amerikanische *E-Sign Act*[169] von 2000 hier weitgehende Freiheiten. Dem europäischen Paradigma des umfassend regelnden paternalistischen Staates steht dabei das liberale Staatsverständnis der USA entgegen, demzufolge der Staat künftige technische und wirtschaftliche Entwicklungspotentiale so wenig wie möglich einschränken sollte.[170]

---

167 Drittes Gesetz zur Änderung verwaltungsverfahrensrechtlicher Vorschriften vom 21. August 2002, BGBl. I 3322.

168 Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz vom 22. März 2005, BGBl. I 837.

169 Electronic Signatures in Global and National Commerce Act of 2000 (E-Sign Act, Millennium Digital Commerce Act), 15 U.S.C. §§ 7001 ff.

170 Das Paradigma des „limited Government" ist eng mit der Chicagoer Schule und Wirtschaftswissen-

Zudem werden die Anforderungen an eine juristisch gültige Unterschrift im amerikanischen Vertragsrecht[171] (U.C.C.) traditionell anders definiert, als dies im Zivilrecht der meisten europäischen Staaten der Fall ist. Nach § 1-201 (37) U.C.C. gilt als Signatur jedes Zeichen, das mit dem Willen zur Akzeptanz eines bestimmten Schriftstücks angewandt wird, unabhängig von seiner Zuordenbarkeit. Im Gegensatz zu § 126 Abs. 1 BGB, der explizit eine *namentliche* Unterschrift – bzw. im Falle eines beliebigen Handzeichens dessen notarielle Beglaubigung – vorsieht, ist im amerikanischen Vertragsrecht damit bereits die Absicht zur Unterzeichnung hinreichende Bedingung für eine juristisch gültige Unterschrift, während im deutschen Recht zusätzlich eine Zuordenbarkeit der Signatur zur Voraussetzung gemacht wird. Analog definiert auch der „E-Sign Act" in sec. 106 § 5 die elektronische Signatur lediglich als

> electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.

Da das amerikanische Recht also auch hier eine Zuordenbarkeit nicht fordert, bedarf es im Unterschied zur europäischen Gesetzgebung folglich auch keiner spezifischen Regelung der technischen Einzelheiten einer PKI zur Gewährleistung eben dieser Zuordenbarkeit.

5.1.2 Informelle Ko- und Selbstregulierung

In der dynamischen und komplexen Sicherheitslage elektronischer IuK-Systeme sind Maßnahmen rechtlich sanktionierter (imperativer) Regulierung oftmals nur von bedingter Wirksamkeit. Zum einen können sich Regulierungsadressaten Sanktionen häufig leicht entziehen, zum anderen wirft eine regulative Politik ganz allgemein Probleme hinsichtlich informationeller Asymmetrien auf.[172] Im Fahrwasser technologischer Innovationen entstehen fortlaufend neue Handlungspotentiale, deren Problematik von Legislative und Exekutive teilweise nur unzureichend erkannt wird und deren abschließende

schaftlern wie Milton Friedman und George Stigler verbunden (vgl. Kleinsteuber 1983; Peltzman 1993).

171 Die USA kennen ursprünglich kein einheitliches Vertragsrecht auf Bundesebene. Allerdings existiert mit dem Uniform Commercial Code (U.C.C.) ein Modellgesetz, das auf eine Harmonisierung des Vertragsrechts abzielt und bis dato von allen Bundesstaaten mit Ausnahme von Louisiana in weiten Teilen übernommen wurde.

172 Zu den Problemen regulativer Politik siehe bspw. Mayntz (1987: 95 ff.).

rechtliche Regulierung nicht selten mit deutlicher zeitlicher Verzögerung erfolgt. Neben rechtlichen Sanktionen kommt daher Mechanismen einer zeitnahen Selbstregulierung eine herausgehobene Bedeutung bei der Produktion von Sicherheit in elektronischen Netzwerken zu. Kleinsteuber (2006) etwa konstatiert gerade im Umfeld des Internet eine generelle Tendenz zur Selbstregulierung. Auch Latzer et al. (2002: 100) identifizieren im Rahmen einer „transformierten Staatlichkeit im Mediamatiksektor" einen generellen „Trend *von der staatlichen Regulierung zur Selbst- und Ko-Regulierung*".

In großen sozio-technischen IuK-Systemen ergibt sich eine spezifische Steuerungsproblematik insbesondere aus der hohen Komplexität, die diesen Systemen inhärent ist. Multiple Interdependenzen technischer und sozialer Artefakte erlauben es einzelnen Akteuren nur unzureichend, die systemweiten Folgen – und damit etwaige negative Externalitäten – individuellen Handelns zu überblicken (siehe hierzu Espey u. Rudinger 1999). Die Ursache dysfunktionaler Handlungen auf der Mikroebene ist daher häufig in einer begrenzten Rationalität der Akteure zu suchen, die wiederum aus einem Informationsdefizit bezüglich der ethischen, rechtlichen, wirtschaftlichen und technischen Rahmenbedingungen des Handelns in elektronischen Räumen resultiert. Vor diesem Hintergrund lassen sich mindestens drei unabdingbare Voraussetzungen einer effektiven, dezentralen Selbststeuerung identifizieren: (1) eine umfassende Sensibilisierung bzw. Aufklärung aller Beteiligten, (2) eine Vermittlung von Kenntnissen über aktuelle Sicherheitspraktiken und -techniken, (3) eine hohe Informationstransparenz bezüglich sicherheitsrelevanter Vorfälle. Aufgrund der Charakteristik negativer Netzwerkeffekte tragen im aufgeklärten Eigeninteresse durchgeführte und daher intrinsisch motivierte Maßnahmen auf der Mikroebene dann zugleich zu einem erhöhten Sicherheitsniveau auf der Makroebene bei.

Insbesondere im Bereich der Sensibilisierung spielen kulturelle und normative Mechanismen institutioneller Verhaltenssteuerung eine bedeutende Rolle. So geht etwa Kuhlen (2005) von einer sich im Umfeld des Internet gegenwärtig gänzlich neu formierenden Informationsethik aus. Auch Spinello (2002) und Capurro (2003) befassen sich mit dieser Thematik und die in Abschnitt 5.1.1 bereits erwähnten OECD-Richtlinien für die Sicherheit von Informationssystemen und -netzwerken aus dem Jahr 2002 streben bereits in ihrem Untertitel ausdrücklich eine „Kultur der Sicherheit" an. Im Rahmen der Debatte über Medienkompetenz gibt es ferner didaktische Bestrebungen, IT-sicherheitsrelevante Themen im Bewußtsein aller Netzwerkteilnehmer zu verankern (siehe hierzu Friedrich 2002; Ulrich 2002). Eine Sensibilisierung hinsichtlich potentieller

Risiken und Gefahren sowie möglicher Maßnahmen zu deren Bekämpfung im Rahmen einer umfassenden Sicherheitskultur soll dabei zu einer vermehrten Berücksichtigung sicherheitsrelevanter Aspekte in Design, Implementation, Konfiguration und Anwendung elektronischer Informationssysteme führen.

Initiativen zur Sensibilisierung sowie zur Aus- und Weiterbildung der Akteure in elektronischen Räumen sind oftmals das Ergebnis einer sektorübergreifenden Kooperation öffentlicher und privater Organisationen. Begünstigt wird eine solche Zusammenarbeit durch vier Faktoren: (1) die spezifische Logik negativer Netzwerkeffekte, die eine hohe Inklusivität zur Voraussetzung einer effektiven Problemlösung werden läßt; (2) ein allgemeines Interesse aller an diesen Netzwerken partizipierenden Akteure an einem stabilen Inter- bzw. Transaktionsrahmen und damit einem erhöhten Sicherheitsniveau (Kollektivgut-Charakter); (3) die Eignung gemeinnütziger Initiativen zur erweiterten Legitimation unternehmerischer Tätigkeit im Rahmen einer *Corporate Social Responsibility*[173]; (4) ein allgemeines Interesse privater Akteure staatliche Intervention nach Möglichkeit zu vermeiden. Flankierend erhöhen einschlägige Informationsnetzwerke die horizontale Informationstransparenz zwischen den Akteuren und ermöglichen so eine zeitnahe Identifikation, Eindämmung und Lösung sicherheitsrelevanter Probleme im Wege der Selbstregulierung. Beispielhaft werden im folgenden einige dieser Initiativen herausgegriffen.

In den USA existiert mit der *National Cyber Security Alliance* (NCSA) seit 2002 ein Verbund, an dem neben dem amerikanischen Heimatschutzministerium (US-DHS) und der Federal Trade Commission (FTC) auch eine Reihe privater Akteure wie MS, eBay, AOL, Cisco Systems, Symantec, McAfee und RSA Security sowie die Unternehmensverband Business Software Alliance (BSA) beteiligt sind. Die NCSA verfolgt das Ziel, Privatnutzer, Ausbildungseinrichtungen und Kleinunternehmen für sicherheitsrelevante Themen im Umfeld des Internet zu sensibilisieren. Auf ihrer Web-Seite[174] finden sich einschlägige Hinweise zu potentiellen Gefahren und vorbeugenden Maßnahmen sowohl in technischer wie sozialer Hinsicht. Zentrale Themen sind u. a. der Schutz privater Daten, die Authentifizierung potentieller Transaktionspartner, die Installation und Wartung von Viren-Scannern und Firewalls sowie die Konfiguration und Wartung des

173 Salzmann et al. (2008: 6) verweisen bezüglich der *Corporate Social Responsibility* auf das Konzept einer „informal license to operate“ und definieren diese als „level of legitimacy granted to the company by non-regulatory stakeholders such as capital markets, NGOs and customers“.

174 Vgl. <`http://www.staysafeonline.org`>.

TABELLE 5.3: *Programme der Europäischen Union*

Programm	*Laufzeit*	*Entscheidung*	*Mio. Euro*
Safer Internet Action Plan	1999 – 2002	276/1999/EG	25,0
Safer Internet Action Plan extension	2003 – 2004	1151/2003/EG	13,3
Safer Internet plus Programme	2005 – 2008	854/2005/EG	45,0
Safer Internet Programme	2009 – 2013	1351/2008/EG	55,0

Betriebssystems. In Kooperation mit der National Cyber Security Division (NCSD) des US-DHS organisiert die NCSA jährlich im Oktober den sog. „National Cyber Security Awareness Month", anläßlich dessen im Rahmen von Aufklärungskampagnen Anzeigen in Medien geschaltet sowie Seminare, Workshops und Informationsveranstaltungen in Kleinunternehmen und Bildungseinrichtungen gefördert werden.

Einen verbesserten Informationsaustausch zwischen zentralen Akteuren des amerikanischen IT-Sektors soll das *Information Technology Information Sharing and Analysis Center* (IT-ISAC) gewährleisten (vgl. hierzu Schulze 2006: 234 ff.). Es umfaßt private Unternehmen der Soft- und Hardware-Industrie wie Cisco, CSC, HP, IBM, McAfee, MS, Oracle, RSA, Symantec und VeriSign. Die Institution des Information Sharing and Analysis Centers (ISAC) geht auf einen präsidialen Entscheidungserlaß[175] zum Schutz kritischer Infrastrukturen aus dem Jahr 1998 zurück. Dieser sieht die Einrichtung eines ISAC in allen kritischen Infrastruktursektoren der USA – so auch dem IT-Sektor – vor. Aufgabe des IT-ISAC ist es, Informationen zu Sicherheitslücken, -vorkommnissen und -maßnahmen sowie zu Bedrohungen und Angriffen in elektronischen Netzen zu sammeln, auszuwerten und an die zuständigen staatlichen sowie betroffene private Akteure weiterzuleiten. Hierzu betreibt das IT-ISAC eine rund um die Uhr besetzte Operationszentrale. Daneben werden in regelmäßigen Abständen Expertenkonferenzen zu aktuellen Sicherheitsthemen organisiert. Das IT-ISAC dient als zentrale Schnittstelle zwischen dem US-DHS und dem privaten IT-Sektor.

Die *Internet Security Alliance* (ISA) nimmt hinsichtlich des Informationsaustausches im privatwirtschaftlichen Sektor eine dem IT-ISAC vergleichbare Funktion wahr, beschränkt sich im Gegensatz zu diesem jedoch nicht allein auf Mitglieder aus dem IT-Bereich. Der beitragsfinanzierte Unternehmensverband wurde 2001 auf Initiative

175 Presidential Decision Directive 63 vom 22. Mai 1998.

des CERT/CC sowie der Electronic Industries Alliance (EIA) gegründet. Zu den Mitgliedern gehören u. a. IBM, RedSiren, Symantec und VeriSign. Der Verband vertritt die Interessen seiner Mitglieder hinsichtlich Maßnahmen zur Erhöhung der Sicherheit in elektronischen Netzen in Gesetzgebungs- und Regulierungsverfahren. Zu den erklärten Zielen gehört explizit eine umfassende Selbst-Regulierung der Industrie. Ferner unterhält die ISA Forschungsprojekte und Ausbildungsprogramme zu Sicherheitsthemen. Ihre Mitglieder werden durch das CERT/CC regelmäßig und unmittelbar zur aktuellen Sicherheitslage informiert.

Um die Aufklärung und Verfolgung von Straftaten in elektronischen Netzen zu erleichtern, gründete das FBI 1996 in Cleveland, Ohio, als Pilotprojekt die vertrauliche Informationsplattform *InfraGard*. Inzwischen ist InfraGard in zahlreichen amerikanischen Städten mit Verbindungsbüros vertreten (vgl. hierzu Schulze 2006: 238 f.). Insgesamt partizipieren neben dem FBI etwa 9.000 Akteure aus Wirtschaft und Wissenschaft sowie öffentlichen Strafverfolgungsbehörden. Durch die Präsenz von Verbindungsbüros vor Ort und die sich hieraus ergebenden lokalen Netzwerke persönlicher Kontakte verfügt InfraGard über ein sehr hohes Vertrauenskapital. Dieses ermöglicht einen zeitnahen Austausch sensibler Informationen. Seit 2005 existiert in Philadelphia ein vom US-DHS finanziertes Projekt, dessen Ziel der Aufbau eines *Cyber Incident Detection and Data Analysis Center* (CIDDAC) ist. Dieser technische Informationsverbund soll künftig ein automatisiertes Sammeln und Abgleichen von Daten über Angriffe in elektronischen Netzen erlauben. In Zusammenarbeit mit der Small Business Administration (SBA), dem National Center for Manufacturing Sciences (NCMS) sowie dem National Institute of Standards and Technology (NIST) unterhält InfraGard ferner ein Ausbildungsprogramm, in dessen Rahmen Workshops zu Sicherheitsthemen in Klein- und Mittelunternehmen abgehalten werden.

In Europa sind Sensibilisierungsmaßnahmen vor allem durch die Europäische Kommission (EC) auf supranationaler Ebene initiiert worden. Auf deren Vorschlag hin haben das Europäische Parlament (EUROPARL) und der Rat seit 1999 eine Reihe mehrjähriger Aktionspläne zur Förderung der Sicherheit in elektronischen Netzen angenommen (vgl. Tabelle 5.3).[176] Der Schwerpunkt dieser Programme liegt auf dem Schutz Minderjähriger sowie der Bekämpfung illegaler und schädlicher Web-Inhalte. Als Maßnahmen

176 Vgl. <`http://ec.europa.eu/information_society/activities/sip/index_en.htm`>.

TABELLE 5.4: *Nationale INSAFE-Projekte*

Land	*Träger-Konsortium*	*Status*
Belgien	European Centre for Missing and Sexually Exploited Children (ChildFocus)	mixed
	Centre de Recherche et d'Information des Organisations de Consommateurs (CRIOC)	private non-profit
Dänemark	Media Council for Children and Young People (MCCYP)	public
Deutschland	Landeszentrale für Medien und Kommunikation Rheinland-Pfalz (LMK)	public
	Landesanstalt für Medien Nordrhein-Westfalen (LfM)	public
	Europäisches Zentrum für Medienkompetenz (ecmc)	private for-profit
Finnland	Save the Children Finland (StCF)	private non-profit
	Mannerheim League for Child Welfare (MLL)	private non-profit
	Communications Regulatory Authority (Ficora)	public
Griechenland	Extreme Media Solutions (EMS)	private for-profit
	Hellenic Broadcasting Corporation (ERT)	public
Irland	National Centre for Technology and Education (NCTE)	public
	Irish Society for the Prevention of Cruelty to Children (ISPCC)	private non-profit
	National Parents Council (NPC)	private non-profit
Island	Heimili og skoli (HS)	private non-profit
	Barnaheill	private non-profit
	Capacent	private for-profit
Italien	Save the Children Italia	private non-profit
	Associazione Difesa Consumatori e Ambiente (Adiconsum)	private non-profit
Lettland	Ministry of Electronic Government Affairs	public
	Centre of Public Politics (Providus)	private non-profit
	Latvian Internet Association (LIA)	private non-profit
Litauen	Communications Regulatory Authority (CRA)	public
	Ministry of Education and Sciences	public
Luxemburg	Telindus	private for-profit
	Caritas Jeunes et Familles a.s.b.l.	private non-profit
	Centre de Recherche Public Henri Tudor	private for-profit
Niederlande	Pro-Sec/ECP.NL	mixed
	Integral Knowledge Utilization	private for-profit
Norwegen	Media Authority (Medietilsynet)	public
Österreich	Österreichisches Institut für angewandte Telekommunikation (OIAT)	private non-profit
	Internet Service Provider Austria (ISPA)	private non-profit
Polen	Naukowa i Akademicka Sieć Komputerowa (NASK)	mixed
	Fundacji Dzieci Niczyje (FDN)	private non-profit
Portugal	Knowledge Society Agency (UMIC)	public
	Directorate-General for Innovation and Curricular Development (DGIDC)	public
	Foundation for National Scientific Computing (FCCN)	private non-profit
	Microsoft	private for-profit
Schweden	Media Council (RADET)	public
	Children's Rights in Society (BRIS)	private non-profit
Slowakei	Občianskeho združenia eSlovensko (eSK)	private non-profit
	Ministry of Interior	public
	United Nations International Children's Emergency Fund (UNICEF)	public
Slowenien	University of Ljubljana, Faculty of Social Sciences	public
	Academic and Research Network of Slovenia (ARNES)	public
Tschechien	CZI Company	private for-profit
	Our Child Foundation	private non-profit
	Safety Line Association	private non-profit
	Software602	private for-profit
UK	Child Exploitation and Online Protection Centre (CEOP)	public
Zypern	Cyprus Neuroscience & Technology Institute (CNTI)	private non-profit

Datenquelle: <`http://ec.europa.eu/information_society/activities/sip/projects/awareness/index_en.htm`>.

werden u. a. ausdrücklich erwähnt:[177] (1) die „Förderung der Branchen-Selbstkontrolle und von Überwachungseinrichtungen für Inhalte“, (2) die „Ermutigung der Branche, Filter und Bewertungssysteme anzubieten“, (3) die „verstärkte Sensibilisierung der Benutzer“. Im Rahmen dieser Programme wurde unter dem Akronym *INSAFE* ein Netzwerk sog. „awareness nodes“ etabliert, welches Sensibilisierungs- und Aufklärungsprojekte in verschiedenen europäischen Staaten koordiniert und finanziert.[178] An diesen Projekten sind sowohl öffentliche als auch private Akteure beteiligt (vgl. Tabelle 5.4). Die INSAFE-Projekte informieren private Nutzer über potentielle Gefahren sowie vorbeugende Maßnahmen in elektronischen Räumen. Zudem wurde ein Newsletter sowie eine Web-Seite[179] zu sicherheitsrelevanten Themen eingerichtet. Auch wird seit 2005 im Februar jeden Jahres ein „Safer Internet Day“ organisiert, anläßlich dessen bspw. Schulwettbewerbe zu Internet-Themen stattfinden.

Die Internationale Handelskammer (ICC) unterhält seit 1998 in London eine Cybercrime Unit (CCU), welche Informationen über elektronische Sicherheitsvorfälle bei ICC-Mitgliedern sammelt, auswertet und weiterleitet. Auch die Aus- und Weiterbildung von Fachpersonal gehört zu den Aufgaben der CCU. Einschlägige Aus- und Weiterbildungsprogramme werden ferner von einer Reihe berufsspezifischer Verbände, so etwa AIT Global, ASIS International, dem Computer Security Institute (CSI), der Gesellschaft für Informatik (GI), der High Technology Crime Investigation Association (HTCIA), der Information Systems Audit and Control Association (ISACA), der Information Systems Security Association (ISSA), dem Institute of Electrical and Electronics Engineers (IEEE), der Internet Society (ISOC) sowie SANS angeboten. Im Bereich der Aufklärung von Privatnutzern engagieren sich daneben vor allem Bürgerrechtsgruppen wie bspw. die American Civil Liberties Union (ACLU), das Center for Democracy and Technology (CDT) oder das Electronic Privacy Information Center (EPIC).

177 Entscheidung Nr. 276/1999/EG des Europäischen Parlamentes und des Rates, S. 3.

178 Auf nationaler Ebene gibt es parallel zu den durch die EU initiierten Projekten teilweise weitere Bemühungen. So existiert etwa in Deutschland seit 2005 die Initiative „Deutschland sicher im Netz“ (<`http://www.sicher-im-netz.de`>), die 2006 in einen eingetragenen Verein umgewandelt wurde. Unter der Schirmherrschaft des Bundesministeriums des Innern sind an dieser Initiative u. a. die Deutsche Telekom, Hewlett-Packard (HP), Microsoft (MS) und SAP beteilgt.

179 Vgl. <`http://www.saferinternet.org`>.

5.2 Akteure und Ressourcen

5.2.1 Themenfelder und Tätigkeitsarten

Abbildung 5.3 zeigt für die Menge der einhundert untersuchten Organisationen die relativen *Status*- und *Scope*-Häufigkeiten. Hier ist zunächst zu erkennen, daß nichtgewinnorientierte private Akteure ein knappes Drittel aller untersuchten Organisationen stellen. Mit einem Anteil von 0.30 folgen unmittelbar danach öffentliche Akteure. Nicht ganz ein Viertel der Akteure ist privat und gewinnorientiert zugleich, während ein Anteil von nur 0.14 eine gemischte Organisationsform hat. Obwohl also eine Mehrheit der Akteure privat ist, wird demnach nur ein knappes Viertel über einen Marktmechanismus gesteuert. Eine zentrale Rolle spielen vor allem Non-Profit-Organisationen. Deutlich mehr als die Hälfte aller Akteure operiert auf globaler, etwa 40 Prozent auf nationaler Ebene. Weniger als 10 Prozent hingegen sind auf einer regionalen Zwischenebene tätig. Diese Verteilung entspricht dem transnationalen Problemcharakter (vgl. Abschnitt 4.2.3), deutet aber zugleich darauf hin, daß auch der nationalstaatlichen Aktionsebene beim Schutz der Informationsinfrastruktur weiterhin eine gewichtige Bedeutung zukommt.

Um die arbeitsteilige Struktur der Politikdomäne analysieren zu können, wurden sämtliche Organisationen unter Berücksichtigung der in Abschnitt 4.3 ausgeführten Überlegungen auf Grundlage einer Online-Recherche nach inhaltlicher Fokussierung (Themenfeldern bzw. *Issues*) und funktionalem Beitrag (Tätigkeitsarten bzw. *Activities*) im Prozeß der Produktion von Sicherheit in elektronischen Netzen klassifiziert (vgl. hierzu die Tabelle in Appendix B).

Für das häufbare Merkmal der *Issues* einer Organisation wurde folgende Ausprägungsmenge gewählt:

- *Computer Related Crimes*: Die Bekämpfung von Straftaten, die zwar nicht unmittelbar auf Informations- und Kommunikationssysteme selbst abzielen, bei deren Begehung diesen Systemen jedoch eine zentrale Bedeutung als Tatwerkzeug zukommt.
- *Identity/Access*: Die Authentifizierung zugangsberechtigter Nutzer sowie die Kontrolle von Zugangsrechten ist ein weitgehend in sich geschlossener Themenkomplex. In gewisser Weise stellt er einen Teilbereich des Systemschutzes dar. Im Verhältnis zu diesem ist er in etwa mit der Aufgabe des Checkpoints im klassischen Objektschutz zu vergleichen.

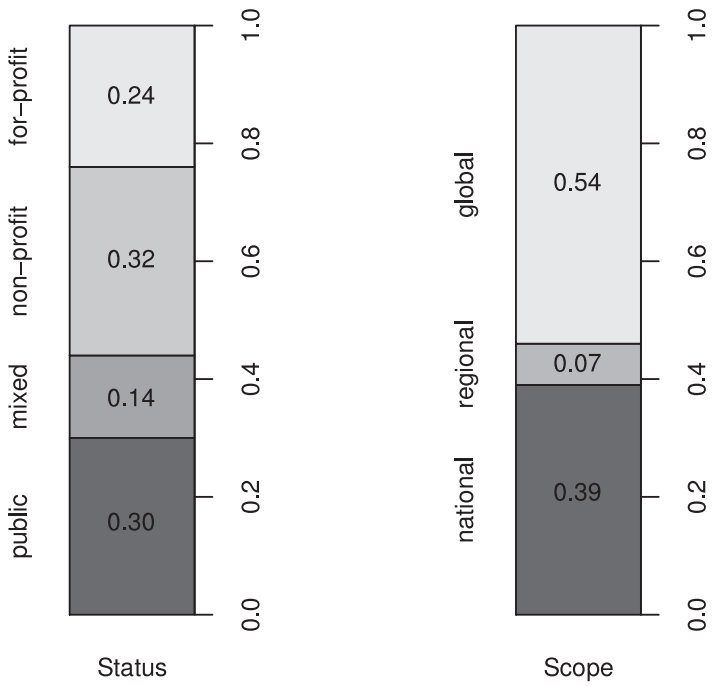


Abbildung 5.3: *Relative Status- und Scope-Häufigkeiten der Akteure*

- *Information Freedom*: Die Sicherstellung eines freien Zugangs zu Informationen ist eine zentrale Konfliktlinie moderner Informationsgesellschaften. Sie wird zumeist nicht durch kriminelle Angriffe sondern durch strukturelle Machtverhältnisse bedroht (vgl. Roberts 2001).
- *Intellectual Property*: Der Schutz geistigen Eigentums. Ziel ist hierbei, die Nutzung bestimmter Daten exklusiv zu gestalten, um deren Marktwert als privates Gut zu erhalten. Oft stehen der Schutz geistigen Eigentums und die Informationsfreiheit in einem Spannungsverhältnis, welches einen zentralen Zielkonflikt begründet.
- *Legal Framework*: Der rechtliche Regulierungsrahmen, vor dessen Hintergrund sicherheitsrelevante Handlungen im Cyberspace durch öffentliche Akteure sanktioniert bzw. gratifiziert werden.
- *Privacy/Data Protection*: Der Schutz der Privatsphäre sowie persönlicher Daten. Dieses Themenfeld ist historisch gesehen das älteste. Partiell steht es sowohl zur Informationsfreiheit als auch zum Schutz geistigen Eigentums in einem Zielkonflikt (vgl. Fischer-Hübner 2000; Raab 2006).
- *Secure Transactions*: In offenen Kommunikationssystemen kommt dem Schutz von Daten in der Phase ihrer Übertragung zwischen besonders gesicherten Teilsystemen eine herausgehobene Bedeutung zu. Hier bestehen

vielfältige Möglichkeiten der Manipulation, der Spionage sowie des Abfangens von Daten.

- *System Protection*: Der (zumeist präventive) Schutz weitgehend abgeschlossener Teilsysteme vor externen Angriffen. Dieses Themenfeld läßt sich am ehesten mit Aufgabenstellung und Zielsetzung des klassischen Objektschutzes vergleichen.
- *Technical Standards*: Im Bereich vernetzter Informations- und Kommunikationstechnologien spielen technische Standards als Modus der Koordination eine zentrale Rolle (vgl. Genschel 1995; Schmidt u. Werle 1998). Sofern sie relationale Objekteigenschaften normieren, dienen sie in erster Linie einer Sicherstellung der Kompatibilität von Netzwerkkomponenten verschiedener Hersteller, wovon dann auch sicherheitsrelevante Komponenten betroffen sind. Als Mindeststandards können sie aber auch spezifische sicherheitsrelevante Qualitätseigenschaften einzelner technischer Artefakte – so etwa deren Anfälligkeit gegenüber externen Störungen – normieren.

Ein erster Blick auf die relativen Anteile der *Issues* (vgl. Abbildung 5.4) zeigt, daß Schwerpunkte der Akteure vor allem im Bereich des Systemschutzes und – mit einigem Abstand – der Sicherung von Transaktionen sowie im Bereich Identifikation und Zugriff liegen. Mit diesen Themen des konkreten Schutzes technischer Informationssysteme beschäftigt sich jeweils deutlich mehr als die Hälfte der untersuchten Organisationen. Themen die den Schutz abstrakter Rechte betreffen werden hingegen von nur wenigen Organisationen aufgegriffen.

Zur statistischen Analyse wurden die *Issue*-Profile der Akteure binär kodiert. Methodisch muß in diesem Zusammenhang zwischen symmetrischen und asymmetrischen Binärvariablen unterschieden werden (Gower 1971: 858). Symmetrische Binärvariablen bilden dichotome Merkmale ab, d. h. die alternativen Werte 0 und 1 repräsentieren die Elemente einer dichotomen Ausprägungsmenge. Beide Werte sind daher prinzipiell gleichgewichtig. Asymmetrische Binärvariablen hingegen dienen zumeist – so auch im vorliegenden Falle – als Hilfsvariablen einer transformierten Kodierung polytomer (mehrkategorialer) Merkmale (vgl. Backhaus et al. 2006: 494 ff.). Da die Ausprägungsmenge hier mehr als zwei Elemente umfaßt, wird zur Kodierung ein Tupel binärer Hilfsvariablen benötigt. Der Wert 1 zeigt dann jeweils die Präsenz, der Wert 0 jedoch die Absenz einer konkreten Ausprägung an. Folglich kommt dem Wert 1 ein erhöhtes Gewicht zu, da er per definitionem den i. d. R. unwahrscheinlicheren Fall repräsentiert und damit im Vergleich zum Wert 0 einen höheren Informationsgehalt aufweist.

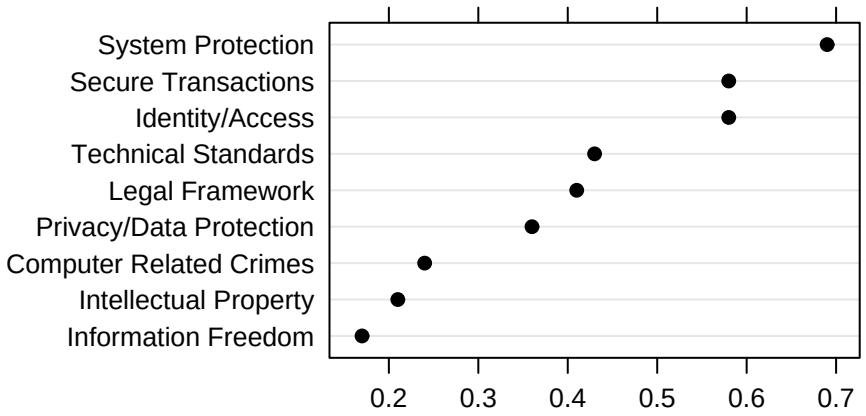


ABBILDUNG 5.4: *Relative Anteile der Issues*

Bei den *Issues* handelt es sich originär um ein polytomes Merkmal der Akteure, welches zudem häufbar ist, also mehr als eine Ausprägung parallel aufweisen kann. Das Merkmal wurde daher in einen Tupel asymmetrischer Binärvariablen transformiert. Aus dem resultierenden Datensatz läßt sich eine Matrix themenspezifischer Dissimilaritäten zwischen den Organisationen errechnen (vgl. Kaufman u. Rousseeuw 1990: 22 ff.). Hierzu werden jeweils sämtliche binären Hilfsvariablen eines Tupels über alle Akteure paarweise miteinander verglichen.

Es sei $\vec{x}_i$ ein binärer Tupel bzw. Vektor, welcher das *Issue*-Merkmal des Akteurs i kodiert. Die Anzahl möglicher Merkmalsausprägungen sei p. Mit x_{if} sei demnach die f-te von p binären Hilfsvariablen des Vektors bezeichnet. Hinsichtlich des Vergleichs zweier Akteure i und j sei ferner: a die Anzahl der Positiv-Übereinstimmungen[180], b die Anzahl der Fehler 1[181], c die Anzahl der Fehler 2[182] und d die Anzahl der Negativ-Übereinstimmungen[183]. Es gilt also: $p = a + b + c + d$. Der Dissimilaritäts-Koeffizient der beiden Akteure i und j schließlich sei mit δ_{ij} bezeichnet.

Da die Kodierung im vorliegenden Falle auf asymmetrischen Binärvariablen beruht, sind die die Werte 0 und 1 – und somit auch Negativ- und Positiv-Übereinstimmungen – bei der Berechnung von δ_{ij} unterschiedlich zu gewichten. Die Berechnung der

180 $x_{if} = 1 \wedge x_{jf} = 1$
181 $x_{if} = 1 \wedge x_{jf} = 0$
182 $x_{if} = 0 \wedge x_{jf} = 1$
183 $x_{if} = 0 \wedge x_{jf} = 0$

Dissimilaritäts-Matrix erfolgte deshalb im Statistik-System *GNU R*[184] auf Basis des *DAISY*-Algorithmus (vgl. Kaufman u. Rousseeuw 1990: 52 ff.). Dieser implementiert für asymmetrische Binärvariablen den Jaccard-Koeffizienten (vgl. Jaccard 1908):

$$\delta_{ij} = \frac{b + c}{a + b + c} \tag{5.1}$$

Wie aus Gleichung 5.1 ersichtlich wird, gehen die Negativ-Übereinstimmungen hier nicht in das Maß ein. Stattdessen setzt der Jaccard-Koeffizient lediglich die Fehlersumme zur Gesamtheit aller Positiv-Übereinstimmungen und Fehler in Bezug. Der Vollständigkeit halber sei erwähnt, daß es sich beim Jaccard-Koeffizienten damit um ein nicht-metrisches und daher zwar um ein Dissimilaritäts-, nicht aber zugleich um ein Distanz-Maß handelt. Dieses muß zwingend so sein, weil das Merkmal der *Issues* lediglich eine kategoriale, nominal skalierte Variable ist. Ein auf dieser Variable beruhendes Vergleichsmaß kann daher bestenfalls auf ordinalem Skalenniveau angesiedelt sein, da keinerlei sinnvolle Aussagen über einen etwaigen Differenzbetrag oder gar ein proportionales Verhältnis möglich sind.

Zur Visualisierung der themenspezifischen Konfiguration des Akteursfeldes bietet sich eine multidimensionale Skalierung (MDS) auf Basis der errechneten Unähnlichkeits-Matrix an. Die Menge der Organisationen wird hier als Punktwolke im hochdimensionalen Raum interpretiert, in welcher die Abstände zwischen den einzelnen Punkten mit den Dissimilaritäten der durch sie repräsentierten Akteure korrespondieren. Im Rahmen einer (metrischen) MDS wird diese Wolke sodann derart auf eine Euklidische Ebene projiziert bzw. in dieser konfiguriert, daß das Verhältnis der ursprünglichen Abstände δ_{ij} auch bei den Abständen $\tilde{\delta}_{ij}$ der MDS-Konfiguration in der Euklidischen Ebene weitestgehend gewahrt bleibt. Weil die Punktwolke hierzu jedoch zusammengequetscht werden muß, ist dies nur bedingt möglich. Das Ausmaß der unvermeidlich auftretenden Deformation beziffert ein *Stress*-Wert.

Bei einer nicht-metrischen MDS werden die Eingangs-Dissimilaritäten δ_{ij} zusätzlich monoton transformiert[185], wobei lediglich ihre Ordnung – nicht aber das metrische Verhältnis zueinander – erhalten bleibt. Dieses Vorgehen hat den Vorteil, eine gleichmä-

184 *GNU R* ist eine Programmierumgebung für statistische Auswertungen, die sich stark an die ursprünglich von den Bell Laboratories entwickelte Sprache *S* anlehnt. Es unterliegt einer GNU-Lizenz und ist daher frei erhältlich (vgl. <`http://www.r-project.org`>).

185 Dies geschieht i. d. R. mittels der Rang-Funktion.

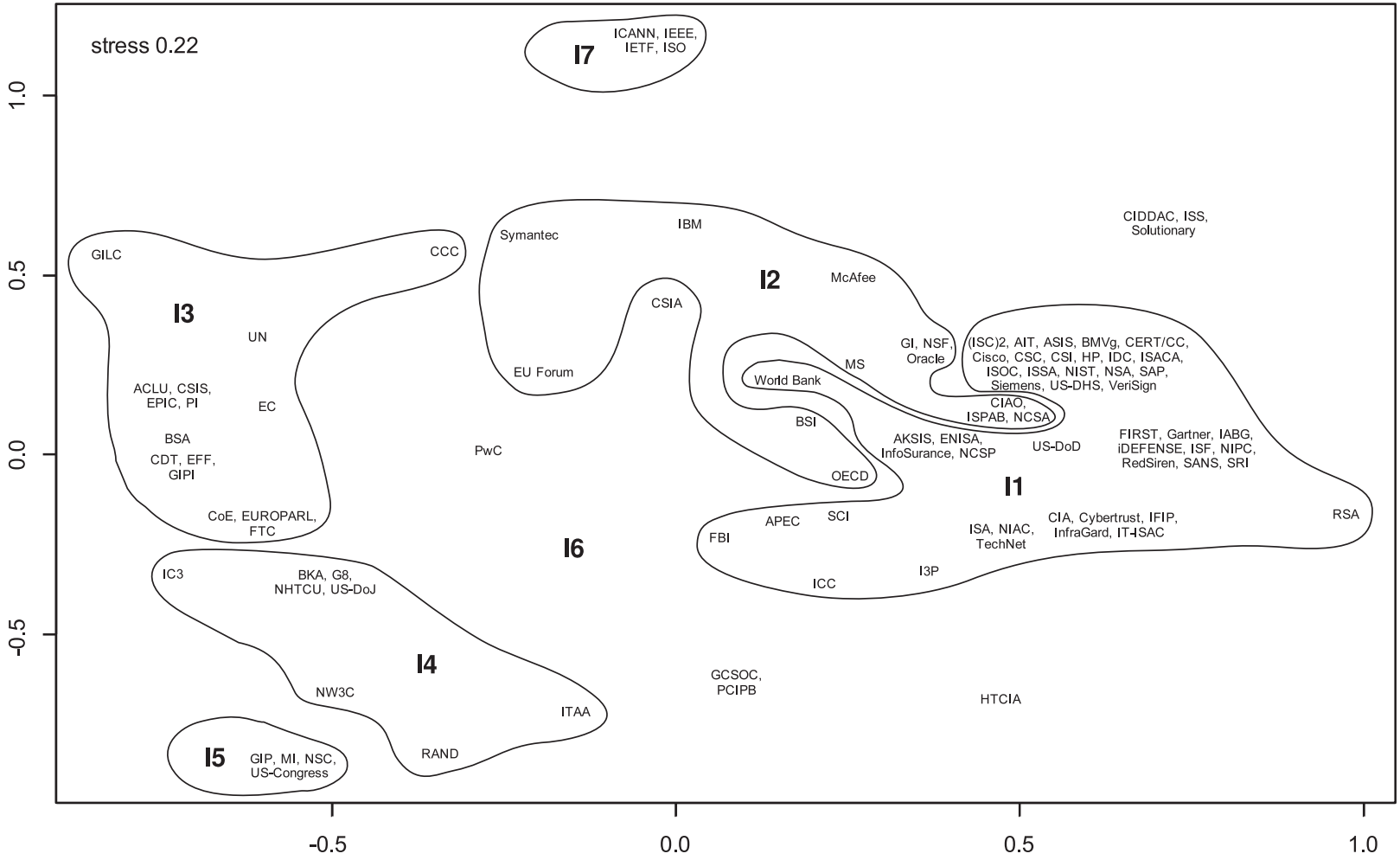


Abbildung 5.5: *Nicht-Metrische Multidimensionale Skalierung nach Issues*

ßigere Verteilung der Punkte in der MDS-Konfiguration zu erzielen, da lange Distanzen zu Gunsten kürzerer gestaucht werden. Wenn es sich – wie im vorliegenden Falle – bei den Eingangs-Dissimilaritäten δ_{ij} ohnehin nicht um ein Distanzmaß handelt, geht durch eine monotone Transformation letztlich keine Information verloren. Daher liegt hier die Wahl einer nicht-metrischen MDS nahe.

Die in Abbildung 5.5 dargestellte multidimensionale Skalierung wurde mittels des *isoMDS*-Algorithmus in *GNU R* (vgl. Venables u. Ripley 2002: 308) erstellt, der ein Verfahren nach Kruskal implementiert. Der *Stress*-Wert errechnet sich bei diesem Verfahren wie folgt:

$$stress = \sqrt{\frac{\sum\limits_{i \neq j} \left[\Theta(\delta_{ij}) - \tilde{\delta}_{ij}\right]^2}{\sum\limits_{i \neq j} \tilde{\delta}_{ij}^2}} \tag{5.2}$$

Aufgrund der als streng monoton definierten Funktion Θ hat das Verfahren nicht-metrischen Charakter. Wie aus Formel 5.2 hervorgeht, gibt das *Stress*-Maß den relativen Anteil der in der Projektion nicht korrekt dargestellten Dissimilaritäten an.[186] Mit einem Wert von ≈ 0.22 ist daher in der Interpretation der MDS-Konfiguration besonders in Feinheiten Vorsicht geboten, da immerhin fast ein Viertel aller Dissimilaritäten verzerrt wiedergegeben wurde. Allerdings ist das bei einem Datensatz dieser Größe nicht anders zu erwarten, denn offensichtlich fällt mit steigender Anzahl der zu skalierenden Objekte die Wahrscheinlichkeit der Möglichkeit einer verzerrungsfreien MDS-Konfiguration stark ab.

Eine analytisch schärfere Typologisierung ermöglichen Verfahren der Cluster-Bildung, deren Ziel die Exploration strukturell ähnlicher Klassen von Objekten (hier Akteuren) und damit einer abstrahierenden Taxonomie ist.[187] Cluster-Algorithmen unterteilen sich in partitionierende und hierarchische Verfahren. Während erstere den gesamten Datensatz in einem einzigen Schritt in eine a priori festzulegende Anzahl von Clustern unterteilen, gehen letztere iterativ vor. Dies hat den Vorteil, daß die Anzahl der Cluster vorerst offen bleiben kann und erscheint daher im Rahmen einer explora-

186 In der Praxis gleicht das Verfahren iterativ die paarweisen Distanzen $\tilde{\delta}_{ij}$ in der Euklidischen Ebene inkrementell an die (transformierten) Dissimilaritäten δ_{ij} an und bricht ab, sobald sich das *Stress*-Maß in jedem weiteren Schritt nurmehr unwesentlich senken läßt.

187 Einen guten – allerdings veralteten – Überblick vieler, auf Verfahren der Cluster-Analyse beruhender Studien gibt Hartigan (1975).

tiven Analyse des vorliegenden Datensatzes als die geeignete Methode. Hierarchische Cluster-Verfahren wiederum können agglomerativ (*bottom-up*) oder divisiv (*top-down*) aufgebaut sein, je nachdem, ob sie die Menge aller einelementigen Cluster oder aber das alle Untersuchungsobjekte umfassende triviale Cluster zum Ausgangspunkt nehmen. In beiden Fällen entsteht eine Baumstruktur ineinander verschachtelter Cluster, die sich als Dendrogramm visualisieren läßt.

In der Praxis sind agglomerative Cluster-Verfahren die am häufigsten genutzte Variante und daher methodisch am weitesten fortgeschritten. Sie beginnen bei der Menge aller einelementigen Cluster und fusionieren diese schrittweise aufgrund eines Proximitätskriteriums. Im ersten Schritt kann für dieses Kriterium zunächst die Matrix der Dissimilaritäten zwischen den einzelnen Objekten – im vorliegenden Falle also die Matrix der Jaccard-Koeffizienten – herangezogen werden. Sobald jedoch durch Fusion ein neues Cluster mit mehr als einem Element entsteht, wird ein weiteres Verfahren zur Bestimmung der Dissimilarität dieses Clusters im Verhältnis zu allen anderen Clustern benötigt. Lance u. Williams (1966) zeigen, daß sich die meisten der hierfür geeigneten Verfahren unter eine allgemeine Formel subsumieren lassen:

$$\delta(A \cup B, C) = \alpha_A \delta(A, C) + \alpha_B \delta(B, C) + \beta \delta(A, B) + \gamma \left| \delta(A, C) - \delta(B, C) \right| \qquad (5.3)$$

Hierbei stehen A und B für die beiden jeweils zu vereinigenden Cluster. Die Dissimilarität $\delta(A \cup B, C)$ des neuen Clusters $A \cup B$ zu einem beliebigen dritten Cluster C kann dann mittels der – aus den vorangegangenen Fusionsschritten bereits bekannten – Dissimilaritäten nach Formel 5.3 errechnet werden.

Je nach Wahl der Parameter α_A, α_B, β und γ lassen sich aus dieser allgemeinen Formel die gängigsten Agglomerationsverfahren herleiten, so auch *Single-*, *Complete-* und *Weighted-Average-Linkage* sowie die Methode nach Ward (1963)[188]. *Single-Linkage* ist die älteste und einfachste Methode, neigt allerdings zu unerwünschten Verkettungseffekten, die sich gerade bei größeren Datensätzen negativ auswirken. Durch Kontraktion entstehen relativ große Cluster mit einer hohen internen Heterogenität. Die *Complete-Linkage*-Methode hingegen zeigt exakt gegenteilige Effekte. Als dilatierende Methode führt sie zu relativ kleinen Clustern von hoher interner Homogenität (vgl. Backhaus et al. 2006: 527 ff.).

188 Zum Nachweis, daß auch die Methode von Ward lediglich einen Sonderfall der Lance-Williams-Formel darstellt, vgl. Wishart (1969).

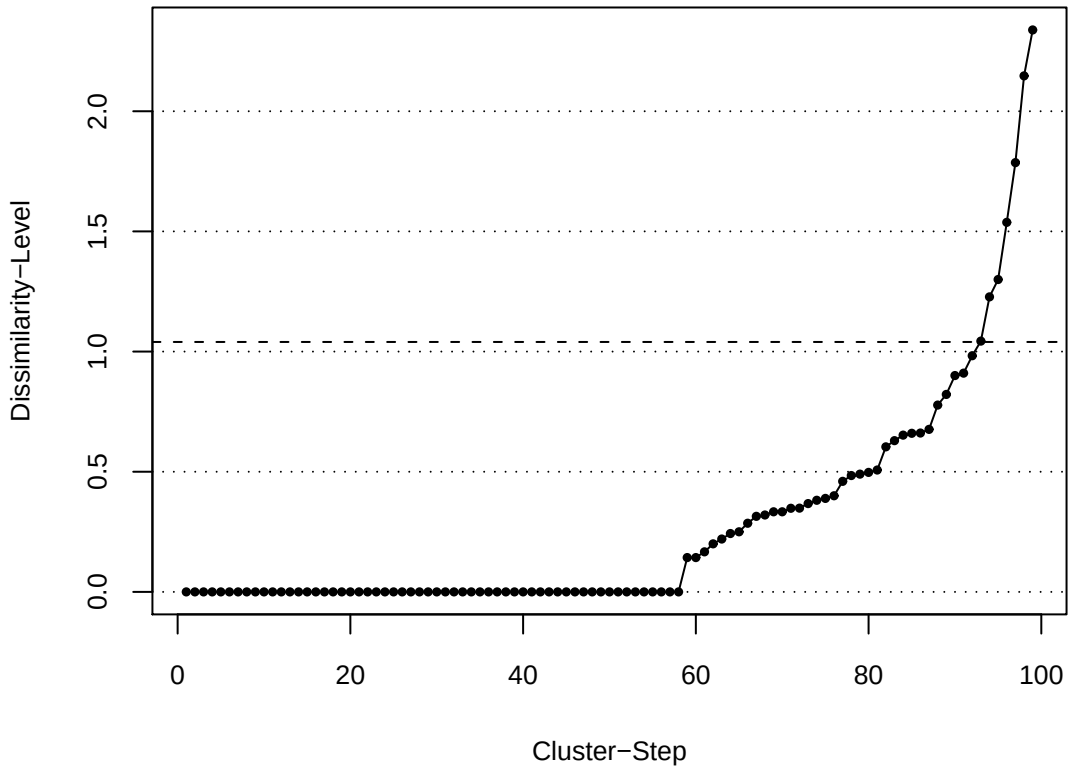


Abbildung 5.6: *Anstieg des Dissimilaritäts-Niveaus bei der Cluster-Bildung nach Issues*

Aus analytischer Perspektive jedoch gilt es sowohl die Anzahl der Cluster zu minimieren, um einen möglichst hohen Abstraktionsgrad zu erreichen, als auch die interne Homogenität der Cluster zu maximieren, um den durch Abstraktion entstehenden Informationsverlust so weit wie möglich zu reduzieren. Erstrebenswert ist also eine Methode, die weder zu kontrahierendem noch zu dilatierendem Verhalten neigt. Ein solches konservatives Verfahren ist die Methode nach Ward. Sie zieht die Zunahme an Varianz, die eine Vereinigung der beiden Cluster A und B zu einem neuen Cluster $A \cup B$ zur Folge hat, als Maß für die Dissimilarität $\delta(A, B)$ zwischen beiden heran und führt damit i. d. R. zu einer weitgehend gleichmäßigen und homogenen Cluster-Einteilung. Allerdings muß zur Berechnung der Varianz auf den Mittelwert bzw. den geometrischen Schwerpunkt der Variablenvektoren zurückgegriffen werden. Dieser aber ist nur für solche Dissimilaritäten definiert, die zugleich auch Euklidische Distanzen darstellen, weshalb diese Methode auf den vorliegenden Datensatz nicht anwendbar ist.

Es verbleibt als Mittelweg die ebenfalls konservative *Weighted-Average-Linkage-*

Methode nach Sokal u. Sneath (1963). Diese ergibt sich für $\alpha = \alpha_A = \alpha_B = 0.5$, $\beta = 0$ und $\gamma = 0$ aus Formel 5.3. Lance u. Williams (1966) schlagen eine weitere Flexibilisierung vor, indem α im Intervall $[0;1]$ variabel gehalten und $\beta = 1 - 2\alpha$ gesetzt wird. Für $\alpha = 0.5$ ergibt sich dann weiterhin die *Weighted-Average-Linkage*-Methode. Für $\alpha < 0.5$ tendiert das Verfahren jedoch zur Kontraktion, für $\alpha > 0.5$ zur Dilatation. Durch diese Eigenschaft läßt es sich flexibel an die spezifischen Eigenheiten eines Datensatzes anpassen. Lance und Williams selbst empfehlen im Allgemeinen einen α-Wert knapp über 0.5 (vgl. Kaufman u. Rousseeuw 1990: 237).

Im vorliegenden Falle wurde das agglomerative Cluster-Verfahren *AGNES* in *GNU R* herangezogen, das optional die Anwendung einer „flexible strategy“ nach Lance u. Williams (1966) erlaubt (vgl. Kaufman u. Rousseeuw 1990: 199 ff.). Als α-Wert wurde 0.6 gewählt, weshalb eine leichte Dilatation zu erwarten ist. Aufgrund der iterativen Vorgehensweise hierarchischer Verfahren stellt sich zusätzlich die Frage nach einem geeigneten Abbruchkriterium. Hier ergibt sich natürlicher Weise – wie bereits erläutert – ein Zielkonflikt zwischen Cluster-Größe und damit -Anzahl einerseits, sowie interner Homogenität der Cluster andererseits.

In Abbildung 5.6 wurde die Entwicklung des Dissimilaritäts-Niveaus im Verlauf der Cluster-Bildung gegen die einzelnen Schritte im Fusionsprozeß abgetragen. Auf diese Weise läßt sich visuell ein geeigneter Schnittpunkt bei Schritt 93 und einem Dissimilaritäts-Niveau von ≈ 1.04 ermitteln. Unmittelbar nach diesem Schritt folgt ein starker Anstieg des Dissimilaritäts-Niveaus, ohne daß sich die Cluster-Anzahl im weiteren Verlauf noch nennenswert reduziert. Die Grenzkosten durch Informationsverlust übersteigen an diesem Punkt also deutlich den Grenznutzen einer weiteren Abstraktion, weshalb es sich offensichtlich empfiehlt, den Schnitt an dieser Stelle anzulegen.

Überträgt man den Schnitt (gestrichelte Linie) in das zugehörige Dendrogramm der Cluster-Bildung (Abbildung 5.7), so lassen sich dort die entsprechenden Cluster-Grenzen ablesen. Es ergeben sich sieben Cluster (I1 – I7) von teilweise sehr unterschiedlichem Umfang. Die ermittelten Cluster-Grenzen wurden nachträglich ebenfalls in das MDS-Diagramm (Abbildung 5.5) eingezeichnet. Deutlich erkennbar ist hier zunächst, daß das Cluster I6 offensichtlich eine Residualkategorie darstellt.

Aus Tabelle 5.5 läßt sich die zahlenmäßige Bedeutung der einzelnen *Issue*-Cluster für die neun Themenfelder ablesen. Sie schlüsselt für jedes Themenfeld die relative Verteilung aller mit dem jeweiligen Thema befaßten Akteure auf die einzelnen *Issue*-Cluster auf. Fett gedruckt sind jene Anteile, die in der Summe mindestens die Hälfte der Ak-

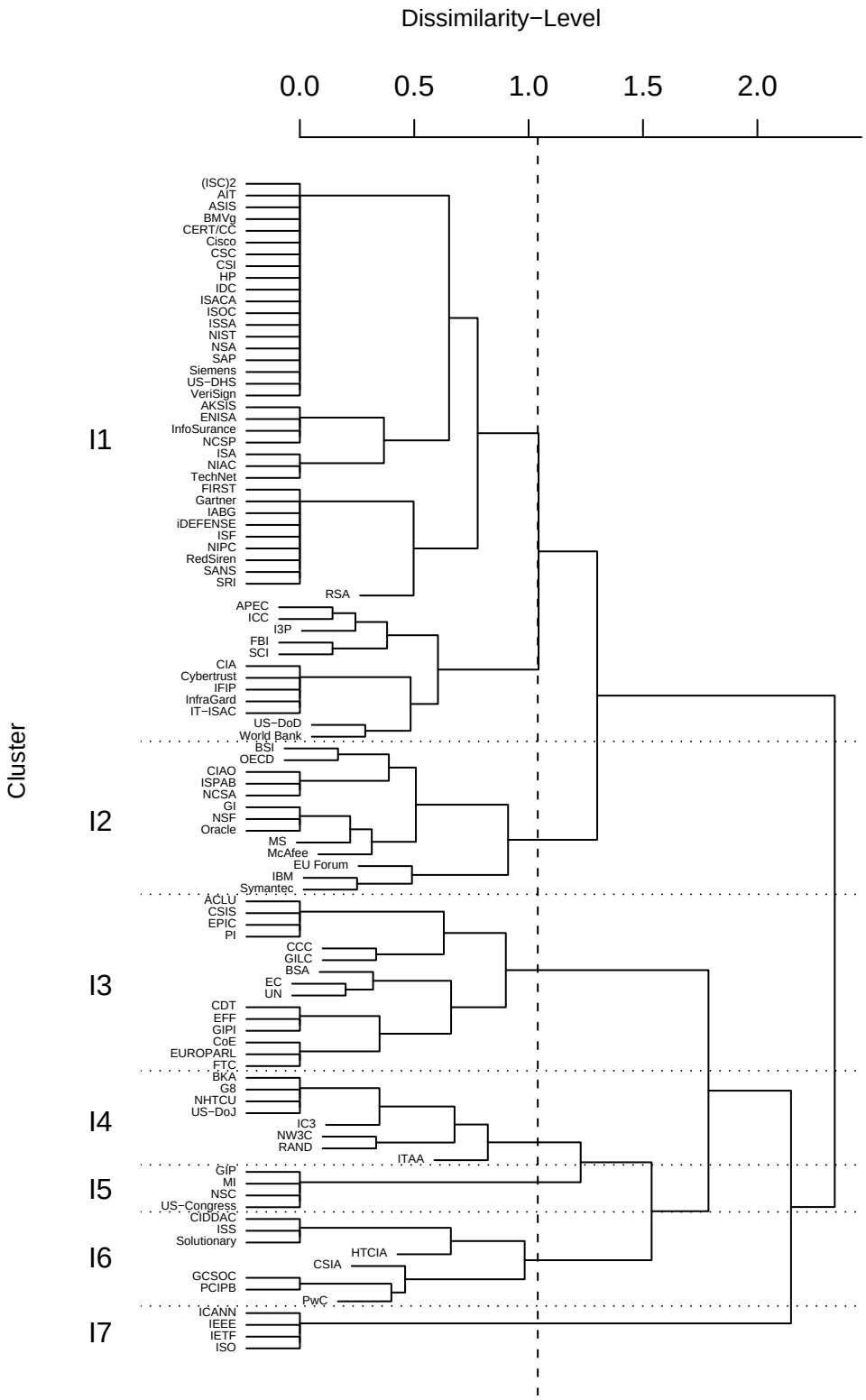


ABBILDUNG 5.7: *Agglomerative Cluster-Bildung nach Issues*

TABELLE 5.5: *Relative Anteile der Cluster an den Issues*

Issue/Cluster	I1	I2	I3	I4	I5	I6	I7
Computer Related Crimes	**0.50**	0.04	0.12	0.29		0.04	
Identity/Access	**0.83**	0.16		0.02			
Information Freedom	0.06	0.06	**0.88**				
Intellectual Property	0.19	0.10	**0.38**	**0.33**			
Legal Framework	**0.27**	0.05	**0.32**	0.17	0.10	0.10	
Privacy/Data Protection	0.08	**0.36**	**0.39**	0.14		0.03	
Secure Transactions	**0.83**	0.17					
System Protection	**0.68**	0.19	0.01			0.12	
Technical Standards	**0.60**	0.21	0.07			0.02	0.09

Anmerkung: Abweichungen der Zeilensummen von 1.00 sind rundungsbedingt.

teure eines Themenfeldes abdecken. Erkennbar wird, daß das Cluster I1 in den fünf Themenfeldern *Computer Related Crimes*, *Identity/Access*, *Secure Transactions*, *System Protection* und *Technical Standards* jeweils eine deutliche Mehrheit aller mit dem jeweiligen *Issue* befaßten Organisationen repräsentiert. Auch aus dem Themenfeld *Legal Framework* sind noch fast ein Drittel aller Organisationen in diesem Cluster vertreten. Dem Cluster I1 kommt damit – gemessen am zahlenmäßigen Anteil der Akteure in den einzelnen Themenfeldern – für den größten Teil der *Issues* eine zentrale Bedeutung zu. Mit deutlichem Abstand folgt das Cluster I3, welches das Themenfeld *Information Freedom* dominiert und in den Feldern *Intellectual Property*, *Legal Framework* und *Privacy/Data Protection* immerhin noch über ein Drittel der Akteure umfaßt.

Tabelle 5.6 verdeutlicht die spezifischen Charakteristika der Cluster. Sie zeigt für jedes *Issue*-Cluster die relative Verteilung aller im jeweiligen Cluster vertretenen Akteure auf die einzelnen Themenfelder. Fett gedruckt sind jene Anteile, die mehr als die Hälfte aller Akteure eines Clusters repräsentieren. Erkennbar wird, daß alle Akteure des Clusters I1 in den Feldern *Identity/Access* sowie *Secure Transactions* und nahezu alle im Feld *System Protection* tätig sind. Etwas über die Hälfte der Organisationen des Clusters befaßt sich ferner mit dem Themenfeld *Technical Standards*. Das Cluster I1 ist offensichtlich vor allem durch solche Akteure charakterisiert, die sich mit der Infrastruktur elektronischer Informationssysteme sowie technischen Maßnahmen zu deren Schutz beschäftigen. Diese Akteure lassen sich weitgehend unter dem in Abschnitt 3.3.3

TABELLE 5.6: *Relative Anteile der Issues an den Clustern*

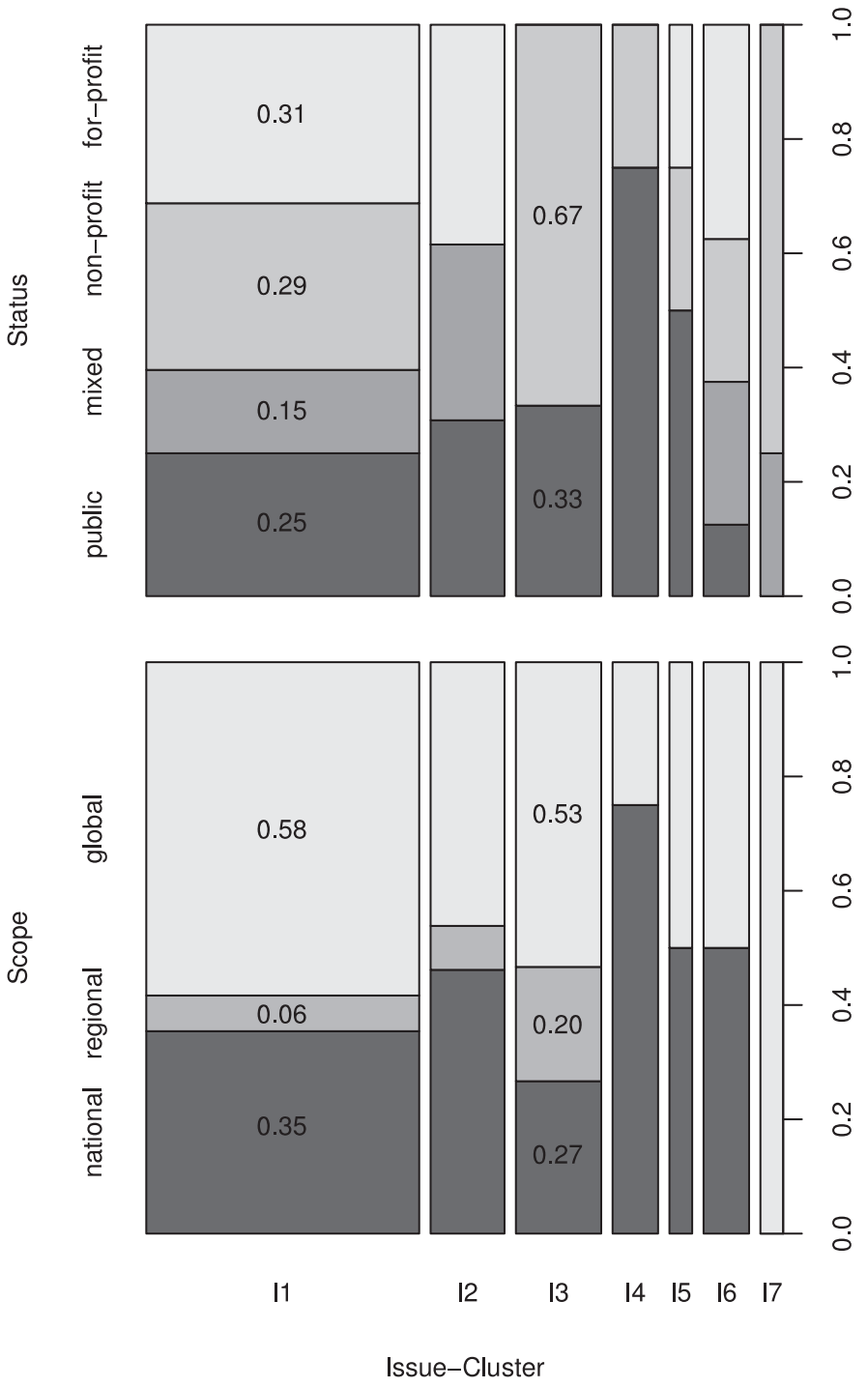
Issue/Cluster	I1	I2	I3	I4	I5	I6	I7
Computer Related Crimes	0.25	0.08	0.20	**0.88**		0.12	
Identity/Access	**1.00**	**0.69**		0.12			
Information Freedom	0.02	0.08	**1.00**				
Intellectual Property	0.08	0.15	**0.53**	**0.88**			
Legal Framework	0.23	0.15	**0.87**	**0.88**	**1.00**	0.50	
Privacy/Data Protection	0.06	**1.00**	**0.93**	**0.62**		0.12	
Secure Transactions	**1.00**	**0.77**					
System Protection	**0.98**	**1.00**	0.07			**1.00**	
Technical Standards	**0.54**	**0.69**	0.20			0.12	**1.00**

Anmerkung: Spaltensummen größer 1.00 sind durch die Häufbarkeit des Merkmals bedingt.

eingeführten Begriff der *Techno-Elite* subsumieren. Aus den Fallstudien sind hier das CERT/CC, das US-DHS sowie die ENISA vertreten.

Im Cluster I3 hingegen dominieren vor allem die Themenfelder *Information Freedom*, *Legal Framework* und *Privacy/Data Protection*. Auch das Feld *Intellectual Property* beschäftigt in diesem Cluster noch über die Hälfte der Organisationen. Die Akteure des Clusters I3 haben vorwiegend die Interessen konkreter Nutzer im Blick und konzentrieren sich primär auf den Schutz abstrakter Rechtsgüter. Diese Rechtsgüter sind zwar auch außerhalb elektronischer Handlungsräume von Bedeutung, unterliegen jedoch in der virtuellen Welt besonderen Bedrohungen. Aus den Fallstudien finden sich hier das CSIS, EPIC, die BSA sowie die EFF. Auffallend ist, daß sich die Cluster I1 und I3 im zugehörigen MDS-Diagramm (Abbildung 5.5) vor allem entlang der Abszisse differenzieren. Man kann hier bedingt das in Abschnitt 3.3.3 aufgezeigte Spannungsfeld der Interessen der Techno-Elite einerseits und der Anwender andererseits erkennen, wobei allerdings die BSA in gewisser Weise eine Ausnahme darstellt. Da sie für einen umfangreichen Schutz geistiger Eigentumsrechte eintritt, wäre ihre Positionierung eher ir im Bereich der Techno-Elite zu erwarten.

In einem weiteren Schritt kann nun versucht werden, die identifizierten *Issue*-Cluster als nominale Ausprägungen einer unabhängigen Variablen zu interpretieren und diese zur Prädiktion der beiden abhängigen ordinalen Merkmale *Status* und *Scope* heranzuziehen. Dem liegt die Annahme zugrunde, daß unterschiedliche Themen unterschiedliche



Anmerkung: Anteile wurden gerundet.

ABBILDUNG 5.8: *Relative Status- und Scope-Häufigkeiten je Issue-Cluster*

Steuerungsstrukturen und Aktionsradien bzw. -ebenen erfordern.

Nullhypothese H_0 ist jeweils, daß die empirischen Verteilungen der Merkmalsausprägungen der beiden Variablenkombinationen *Issue*-Cluster und *Status* bzw. *Issue*-Cluster und *Scope* unabhängig voneinander sind. Zunächst ist daher in beiden Kontingenztafeln zu testen, ob eine Ablehnung der jeweiligen Nullhypothese statistisch signifikant, also mit hinreichend geringer Irrtumswahrscheinlichkeit möglich ist. Da in einigen Feldern der Kontingenztafeln weniger als fünf Beobachtungen zu erwarten sind, ist ein exakter zweiseitiger Test nach Fisher hierbei dem sonst üblichen χ^2-Test vorzuziehen. Aufgrund der Rechenaufwändigkeit des Fisher-Tests muß bei größeren Kontingenztafeln auf eine Monte-Carlo-Simulation zurückgegriffen werden. Dies ist bei Überprüfung der Unabhängigkeit der Variablen *Issue*-Cluster und *Status* der Fall. Ein exakter zweiseitiger Test nach Fisher auf Basis einer Monte-Carlo-Simulation mit 2000 Wiederholungen ergibt hier eine Irrtumswahrscheinlichkeit von $p \approx 0.0005$. Eine Korrelation beider Variablen ist somit statistisch hochsignifikant. Hinsichtlich der Unabhängigkeit der Variablen *Issue*-Cluster und *Scope* ist eine Berechnung ohne Monte-Carlo-Simulation möglich, wobei sich die Irrtumswahrscheinlichkeit auf $p \approx 0.3794$ beläuft. Hier wird das üblicherweise geforderte Signifikanzniveau von $\alpha = 0.05$ deutlich verfehlt. Eine Interpretation ist demnach nur unter Vorbehalten möglich.

Zur Interpretation der Abhängigkeiten verdeutlicht Abbildung 5.8 die relativen *Status*- und *Scope*-Häufigkeiten der Akteure, differenziert nach *Issue*-Clustern. Zur Visualisierung derart kreuzklassifizierter Daten eignet sich in besonderer Weise der Typus des Mosaik-Diagramms (vgl. Hartigan u. Kleiner 1981, 1984; Friendly 1994). Hier wurde die spezielle Variante eines *Spine Plot* gewählt, die den Sonderfall eines segmentierten und normierten Säulendiagrammes mit variabler Säulenbreite darstellt (vgl. Hummel 1996). Die Breite der Säulen entspricht der relativen Verteilung der Akteure auf die jeweiligen Cluster, während die Höhe der einzelnen Säulensegmente die relativen Anteile der Merkmalsausprägungen innerhalb eines Clusters wiedergibt. Die Fläche der Säulensegmente ist folglich proportional zur Häufigkeit der durch sie repräsentierten Cluster-Merkmals-Kombination. Aus Gründen einer besseren Vergleichbarkeit wurden für die zentralen Cluster die relativen Anteile der Merkmalsausprägungen in das Diagramm übertragen.

Aus Abbildung 5.8 ist ersichtlich, daß bei den Themenfeldern das Cluster I1 mit einem Anteil von 0.48 bei weitem die meisten Akteure umfaßt. Ziemlich genau 60 Prozent dieser Akteure sind private Organisationen, von denen wiederum etwas mehr als

die Hälfte gewinnorientiert ist. Bei einem weiteren Viertel der Akteure im Cluster I1 handelt es sich um öffentliche, beim verbleibenden Rest um gemischte Organisationen. Ein Vergleich zur Verteilung in der Menge aller untersuchten Organisationen (Abbildung 5.3) zeigt, daß im Cluster I1 gewinnorientierte private Akteure überproportional vertreten sind. Der Anteil öffentlicher Akteure hingegen ist unterproportional. Deutlich über die Hälfte aller Organisationen im Cluster I1 operiert im globalen Rahmen, während ein starkes Drittel hauptsächlich national orientiert ist. Nur sehr wenige Organisationen bewegen sich auf einer regionalen Zwischenebene. Im Vergleich zur Gesamtmenge aller untersuchten Organisationen kann hier eine Verschiebung von der nationalen zur globalen Ebene konstatiert werden. Allerdings sei in diesem Zusammenhang noch einmal einschränkend auf die hohe Irrtumswahrscheinlichkeit bezüglich einer Korrelation von *Issue*-Cluster und *Scope* verwiesen. Der Schutz der technischen Infrastruktur erfolgt demnach tendenziell eher durch private Akteure auf globaler Ebene. Öffentliche Akteure machen zahlenmäßig nur ein Viertel der Organisationen aus.

Das Cluster I3 umfaßt mit einem Anteil von 0.15 deutlich weniger Akteure. Neben einem Drittel öffentlicher Organisationen sind in diesem Cluster ausschließlich nicht-gewinnorientierte private Akteure vertreten. Im Vergleich zur Gesamtmenge aller untersuchten Organisationen ist hier die starke Repräsentanz nicht-gewinnorientierter privater Akteure auffällig. Über die Hälfte der Organisationen des Clusters I3 sind auf globaler und etwa ein Fünftel auf regionaler Ebene aktiv. Verglichen mit der Gesamtmenge zeigt sich hier eine auffällige Verschiebung von der nationalen zur regionalen Aktionsebene. Der Schutz abstrakter Güter im Interesse der Anwender organisiert sich demnach offenbar ganz überwiegend durch nicht-gewinnorientierte private Akteure auf vermutlich regionaler und globaler Ebene.

Analog zur Vorgehensweise bei den *Issues* wurden auch die *Activities* der Organisationen untersucht. Diesem ebenfalls häufbaren Merkmal liegt folgende Ausprägungsmenge zugrunde:

- *Alerting*: Die Bekanntmachung und Verbreitung von Warnungen und Hinweisen zu akuten Gefährdungen.
- *Consulting/Advice*: Die konzeptionelle Beratung bezüglich sicherheitsrelevanter Maßnahmen und Strategien auf der Mikroebene.
- *Developing Strategies/Policies*: Die Entwicklung lang- und mittelfristiger Strategien und Programme zur Erhöhung des Sicherheitsniveaus auf der Makroebene.

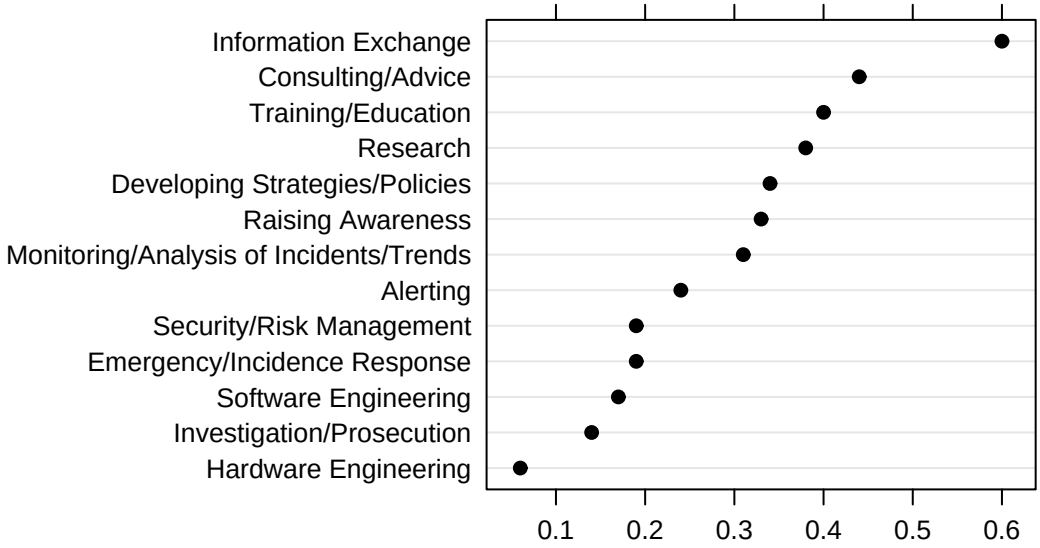


Abbildung 5.9: *Relative Anteile der Activities*

- *Emergency/Incidence Response*: Die Hilfeleistung und Beratung hinsichtlich konkreter sicherheitsrelevanter Vorfälle.
- *Hardware Engineering*: Die Entwicklung und Herstellung technischer Systemkomponenten.
- *Information Exchange*: Der Informationsaustausch zu sicherheitsrelevanten Themen.
- *Investigation/Prosecution*: Die kriminalistische und/oder forensische Untersuchung und Verfolgung konkreter Vorfälle.
- *Monitoring/Analysis of Incidents/Trends*: Die Überwachung und Auswertung sicherheitsrelevanter Vorfälle auf der Makroebene.
- *Raising Awareness*: Die Sensibilisierung von Entwicklern und Anwendern hinsichtlich sicherheitsrelevanter Aspekte.
- *Research*: Die Erforschung sicherheitsrelevanter Themen.
- *Security/Risk Management*: Die Übernahme eines umfassenden Sicherheits- und Risikomanagements für Dritte.
- *Software Engineering*: Die Entwicklung und Bereitstellung maschinell ausführbarer Algorithmen.
- *Training/Education*: Die Aus- und Weiterbildung von Anwendern, Administratoren und Entwicklern hinsichtlich sicherheitsrelevanter Maßnahmen.

Ein Vergleich der relativen Anteile der *Activities* (Abbildung 5.9) verdeutlicht, daß

der Austausch von Information mit Abstand die häufigste Tätigkeitsart ist. Dies entspricht erwartungsgemäß dem herausgehobenen Stellenwert der Ressource Information in modernen Wissensgesellschaften. Auch die nachfolgenden Tätigkeiten Beratung, Aus- und Weiterbildung sowie Forschung sind stark wissensbasiert. Sie beschäftigen jeweils deutlich mehr als ein Drittel der Akteure. Eher technisch orientierte Tätigkeiten hingegen konzentrieren sich auf einen kleinen Kern von Akteuren.

Da es sich auch bei den *Activities* der Akteure um ein polytomes sowie häufbares Merkmal handelt, wurden die *Activity*-Profile der Akteure ebenfalls binär kodiert (vgl. hierzu Appendix B) und eine Dissimilaritäts-Matrix auf Basis des Jaccard-Koeffizienten errechnet. Das zugehörige MDS-Diagramm ist in Abbildung 5.10 dargestellt. Der Stress-Wert von ≈ 0.25 läßt erkennen, daß ein Viertel aller Dissimilaritäten verzerrt wiedergegeben wurde. Auch hier ist in der Interpretation daher Vorsicht geboten.

Zur Cluster-Bildung wurde wieder das agglomerative Verfahren *AGNES* mit einem α-Wert von 0.6 herangezogen. Es ist demnach auch hier eine leichte Dilatation zu erwarten. Aus Abbildung 5.11 läßt sich ein geeigneter Schnittpunkt für die Cluster-Bildung bei Schritt 95 und einem Dissimilaritäts-Niveau von ≈ 1.26 identifizieren. Danach steigt das Dissimilaritäts-Niveau deutlich an, während sich die Cluster-Zahl nur noch geringfügig reduziert. Durch Übertragung des Schnitts auf das Dendrogramm der Cluster-Bildung (Abbildung 5.12) lassen sich wiederum die Cluster-Grenzen ablesen, wobei sich fünf Cluster (A1 – A5) herauskristallisieren. Nachdem diese in das MDS-Diagramm (Abbildung 5.10) eingezeichnet wurden, zeigt sich, daß offenbar das Cluster A3 eine Residualkategorie bildet. Ferner läßt sich durch Vergleich mit dem Dendrogramm der Cluster-Bildung erkennen, daß insbesondere das Cluster A1 im MDS-Diagramm stark verzerrt wurde. So fusionieren bspw. CSIA und NCSA im Dendrogramm auf einem relativ niedrigen Dissimilaritäts--Niveau, während sie sich im MDS-Diagramm an den entgegengesetzten Rändern des Clusters A1 befinden.

Aus Tabelle 5.7 wird die zahlenmäßige Bedeutung der einzelnen *Activity*-Cluster für die dreizehn Tätigkeitsarten ersichtlich. Aufgeschlüsselt ist für jede Tätigkeitsart die relative Verteilung aller mit der jeweiligen Tätigkeit befaßten Akteure auf die einzelnen *Activity*-Cluster. Fett gedruckt sind wiederum jene Anteile, die in der Summe mindestens die Hälfte der Akteure einer Tätigkeitsart abdecken. Deutlich wird die herausgehobene Bedeutung des Clusters A2, das nicht nur alle Akteure im Bereich *Alerting* umfaßt, sondern ebenfalls bezüglich der Tätigkeitsarten *Emergency/Incidence Response*, *Investigation/Prosecution* und *Monitoring/Analysis of Incidents/Trends* jeweils über zwei

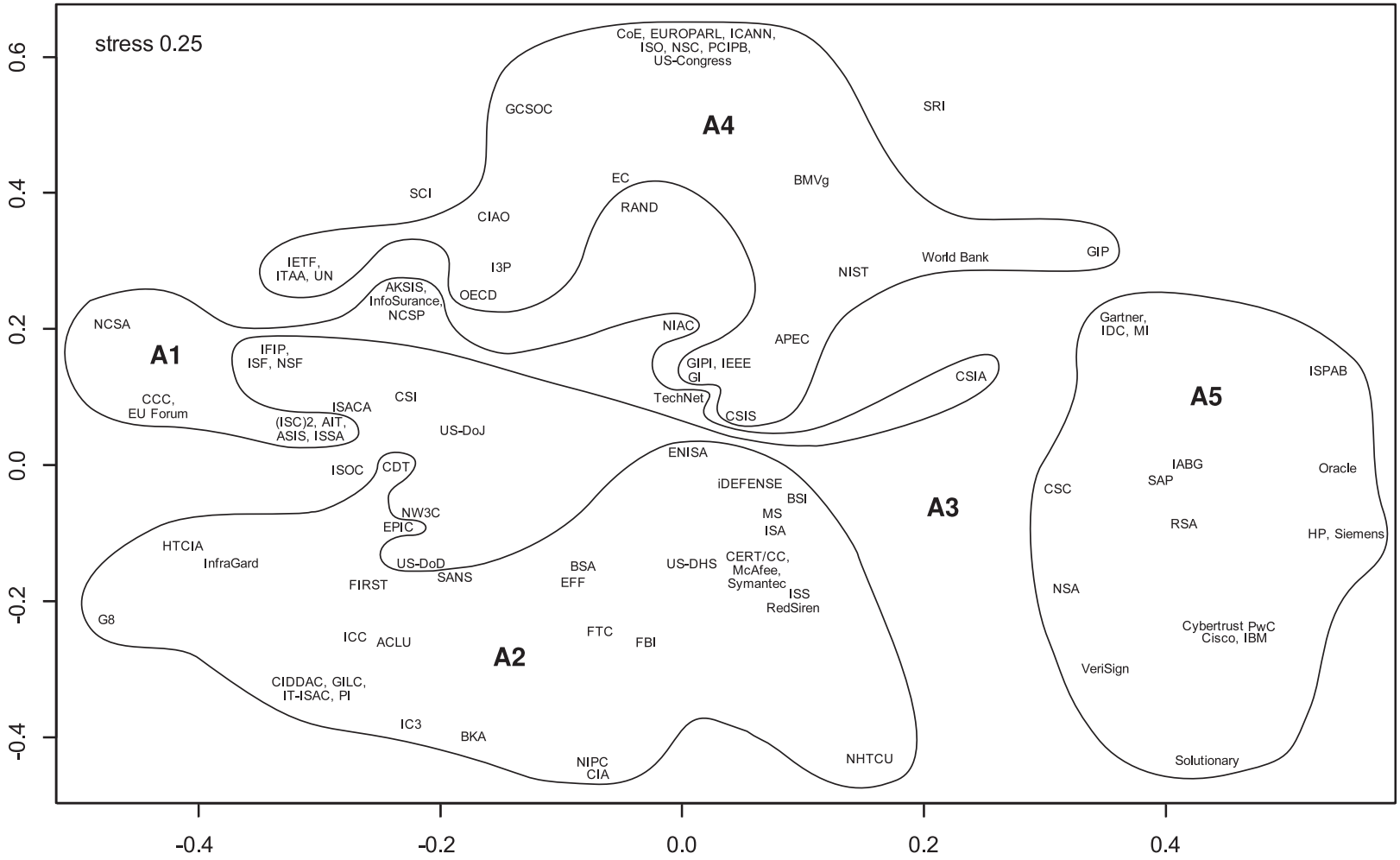


Abbildung 5.10: *Nicht-Metrische Multidimensionale Skalierung nach Activities*

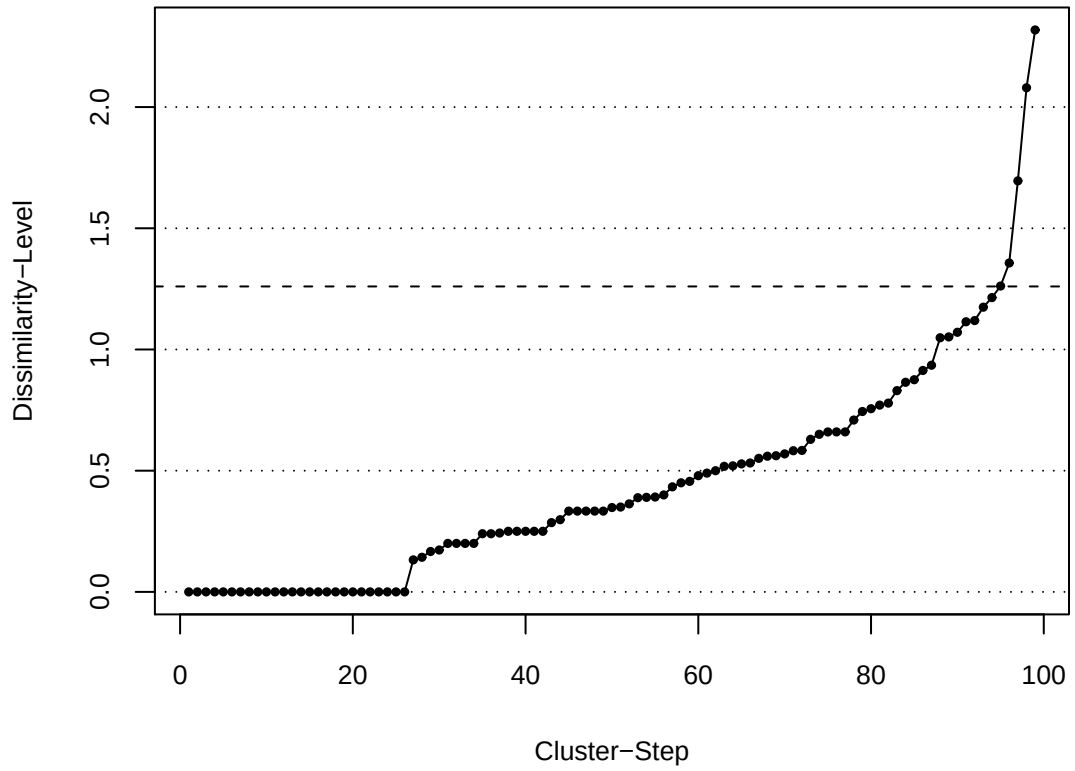


ABBILDUNG 5.11: *Anstieg des Dissimilaritäts-Niveaus bei der Cluster-Bildung nach Activities*

Drittel der Akteure repräsentiert. Auch im Bereich *Information Exchange* sind noch die Hälfte aller Akteure in diesem Cluster vertreten und bei den Tätigkeiten *Research* sowie *Training/Education* umfaßt das Cluster A2 eine relative Mehrheit.

Mit einigem Abstand folgt das Cluster A5, welchem vor allem bezüglich des *Hardware Engineering* überragende Bedeutung zukommt. Auch in den Tätigkeitsarten *Security/Risk Management* und *Software Engineering* findet sich hier eine relative Mehrheit der Akteure, während im Bereich *Consulting/Advice* die Cluster A2 und A5 von zahlenmäßig annähernd gleicher Bedeutung sind. Schließlich dominiert das Cluster A4 die Tätigkeitsart *Developing Strategies/Policies*.

Tabelle 5.8 zeigt die spezifische Charakteristik der einzelnen Cluster. Sie schlüsselt für jedes *Activity*-Cluster die relative Verteilung aller im jeweiligen Cluster vertretenen Akteure auf die einzelnen Tätigkeiten auf. Fett gedruckt sind jene Anteile, die mehr als die Hälfte aller Akteure eines Clusters repräsentieren. Klar zu erkennen ist, daß sich fast alle Akteure des Clusters A2 mit *Information Exchange* beschäftigen. Über zwei Drittel

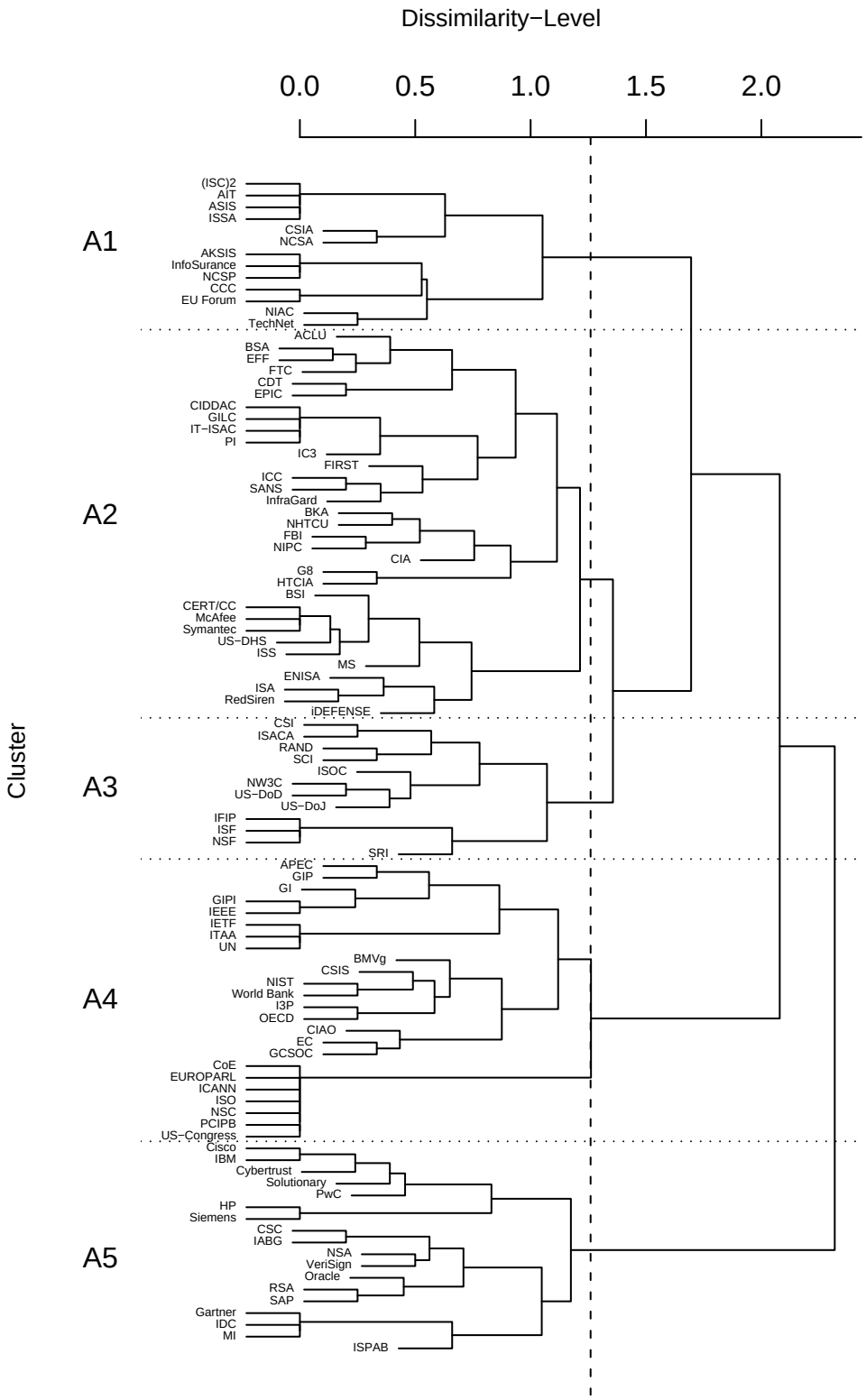


Abbildung 5.12: *Agglomerative Cluster-Bildung nach Activities*

TABELLE 5.7: *Relative Anteile der Cluster an den Activities*

Activity/Cluster	A1	A2	A3	A4	A5
Alerting		**1.00**			
Consulting/Advice	0.07	**0.36**		0.18	**0.39**
Developing Strategies/Policies	0.12	0.09	0.09	**0.71**	
Emergency/Incidence Response		**0.68**		0.05	0.26
Hardware Engineering					**1.00**
Information Exchange	0.18	**0.50**	0.15	0.17	
Investigation/Prosecution		**0.86**	0.14		
Monitoring/Analysis of Incidents/Trends		**0.77**	0.13	0.03	0.06
Raising Awareness	**0.39**	**0.39**	0.06	0.15	
Research		**0.34**	**0.29**	0.21	0.16
Security/Risk Management		0.47			**0.53**
Software Engineering		0.35			**0.65**
Training/Education	0.15	**0.48**	**0.20**	0.10	0.08

Anmerkung: Abweichungen der Zeilensummen von 1.00 sind rundungsbedingt.

der Akteure des Clusters sind ferner in den Bereichen *Alerting* und *Monitoring/Analysis of Incidents/Trends* tätig. Auch im Bereich *Training/Education* engagiert sich noch über die Hälfte der Akteure. Die im Cluster A2 vertretenen Akteure sind offenbar hauptsächlich mit der Rezeption akuter Bedrohungen sowie mit reaktiven Tätigkeiten zu deren operativer Bewältigung befaßt. Bis auf das CSIS deckt dieses Cluster alle Fallstudien ab.

Nahezu alle Akteure des Clusters A5 bieten Dienstleistungen im Bereich *Consulting/Advice* an. Auch in den Bereichen *Security/Risk Management* und *Software Engineering* ist noch über die Hälfte aller Akteure des Clusters tätig. Diese Tätigkeiten haben zwar überwiegend reaktiven, teils aber auch präventiven Charakter und bewegen sich daher auf einer taktisch-operativen Zwischenebene. Das Cluster A4 schließlich wird eindeutig durch die präventiv-strategische Tätigkeit *Development of Strategies/Policies* dominiert. Aus den Fallstudien ist hier das CSIS vertreten. Die Konfiguration der Cluster A2, A5 und A4 im zugehörigen MDS-Diagramm (Abbildung 5.10) läßt vermuten, daß hier die Ordinate eine Dimension des strategischen Abstraktionsniveaus im Tätigkeitsprofil der Akteure – respektive deren Zeithorizont – widerspiegelt.

Um die Unabhängigkeit der Variablen *Activity*-Cluster und *Status* zu prüfen, wurde

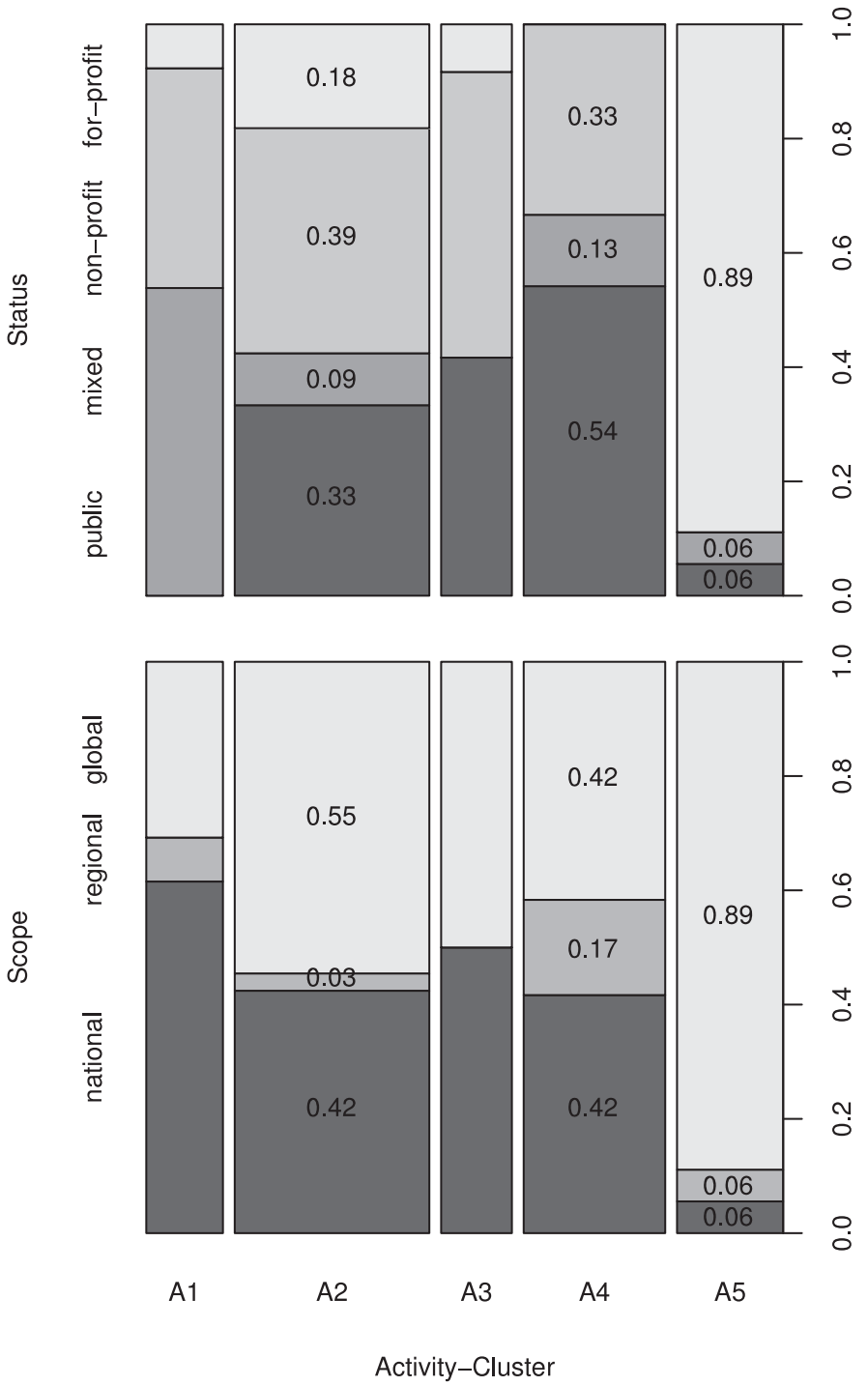
TABELLE 5.8: *Relative Anteile der Activities an den Clustern*

Activity/Cluster	A1	A2	A3	A4	A5
Alerting		**0.73**			
Consulting/Advice	0.23	0.48		0.33	**0.94**
Developing Strategies/Policies	0.31	0.09	0.25	**1.00**	
Emergency/Incidence Response		0.39		0.04	0.28
Hardware Engineering					0.33
Information Exchange	**0.85**	**0.91**	**0.75**	0.42	
Investigation/Prosecution		0.36	0.17		
Monitoring/Analysis of Incidents/Trends		**0.73**	0.33	0.04	0.11
Raising Awareness	**1.00**	0.39	0.17	0.21	
Research		0.39	**0.92**	0.33	0.33
Security/Risk Management		0.27			**0.56**
Software Engineering		0.18			**0.61**
Training/Education	0.46	**0.58**	**0.67**	0.17	0.17

Anmerkung: Spaltensummen größer 1.00 sind durch die Häufbarkeit des Merkmals bedingt.

analog zur Untersuchung der *Issues* ein exakter zweiseitiger Test nach Fisher auf Basis einer Monte-Carlo-Simulation mit 2000 Wiederholungen herangezogen. Dieser ergibt eine Irrtumswahrscheinlichkeit von $p \approx 0.0005$. Hinsichtlich der Unabhängigkeit der Variablen *Activity*-Cluster und *Scope* ist wiederum eine Berechnung ohne Monte-Carlo-Simulation möglich, wobei sich die Irrtumswahrscheinlichkeit auf $p \approx 0.0076$ beläuft. In beiden Fällen ist demnach mit hoher Signifikanz von einer Korrelation auszugehen.

Abbildung 5.13 schließlich zeigt die relativen *Status*- und *Scope*-Häufigkeiten der Akteure nach Tätigkeits-Clustern in Form eines *Spine Plots*. Ersichtlich wird, daß das Cluster A2 mit einem Anteil von 0.33 eine relative Mehrheit aller Akteure umfaßt. Der größte Teil davon entfällt mit 39 Prozent auf nicht-gewinnorientierte private Organisationen einerseits, sowie mit 33 Prozent auf öffentliche Akteure andererseits. Beide Merkmalsausprägungen sind im Vergleich zur Verteilung in der Gesamtmenge aller untersuchten Organisationen (Abbildung 5.3) überproportional vertreten. Über die Hälfte der Akteure operiert auf globaler und 42 Prozent auf nationaler Ebene. Verglichen mit der Gesamtmenge aller untersuchten Organisationen sind geringfügige Verschiebungen von der regionalen zur nationalen Ebene zu verzeichnen. In der operativen Bewältigung akuter Bedrohungen dominieren offensichtlich öffentliche Akteure im Verbund



Anmerkung: Anteile wurden gerundet.

ABBILDUNG 5.13: *Relative Status- und Scope-Häufigkeiten je Activity-Cluster*

mit nicht-gewinnorientierten privaten Organisationen schwerpunktmäßig auf globaler Aktionsebene. Zugleich wird deutlich, daß im nationalstaatlichen Rahmen tätige Akteure gerade im Kernbereich operativer Sicherheitsmaßnahmen zahlenmäßig nach wie vor von Bedeutung sind.

Das Cluster A5 repräsentiert 18 Prozent aller untersuchten Akteure. Mit einem Anteil von 0.89 sind gewinnorientierte private Organisationen hier deutlich stärker als in der Gesamtmenge aller Organisationen vertreten. Ihre dominierende Stellung erklärt sich aus der Tatsache, daß die Akteure des Clusters A5 vor allem präventiv über Technologie-Architekturen bzw. eine konzeptionelle Beratung der Anwender Einfluß auf die Sicherheit elektronischer Netze nehmen. Beide Leistungen stellen exklusive Güter dar, so daß Steuerung hier problemlos über Marktarrangements erfolgen kann. Dies geschieht zugleich größtenteils in einem globalen Rahmen.

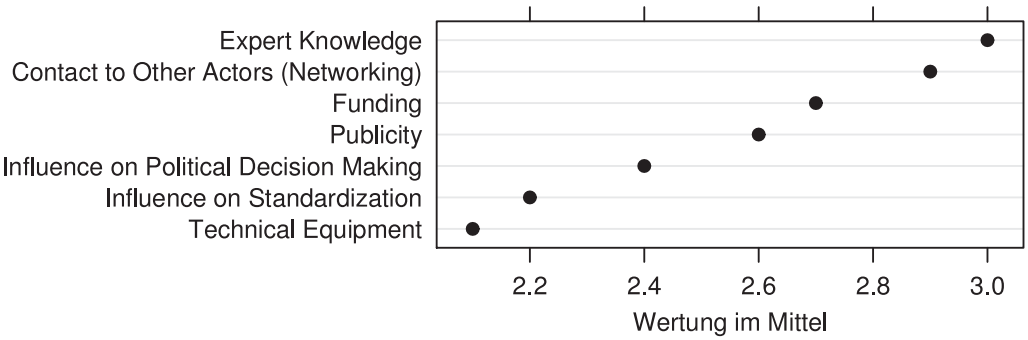
Das Cluster A4 umfaßt 24 Prozent der Akteure. Hier finden sich neben öffentlichen und gemischten ausschließlich nicht-gewinnorientierte private Akteure. Verglichen mit der Gesamtmenge aller Organisationen läßt sich eine signifikante Verschiebung von gewinnorientierten privaten Akteuren hin zu öffentlichen Akteuren identifizieren. Diese machen deutlich über die Hälfte aller Organisationen des Clusters A4 aus. Auch ist die regionale Ebene sehr viel stärker repräsentiert, als dies in der Gesamtmenge der Fall ist. Die ebenfalls präventive Ausarbeitung langfristiger Strategien respektive Politiken ist demnach eindeutig Aufgabe öffentlicher Akteure auf nationaler und zunehmend auch regionaler Ebene.

5.2.2 Gewicht und Verteilung relevanter Ressourcen

In jedem Handlungssystem spielen verschiedene Ressourcen im Prozeß der Produktion von Gütern eine zentrale Rolle (vgl. Abschnitt 2.2.1). Zur Ermittlung der für die Produktion von Sicherheit in elektronischen Netzen relevanten Ressourcen wurde im Verlauf der zehn Interviews (vgl. Abschnitt 1.3) folgende geschlossene Frage gestellt:

> To conduct its cyber-security related business successfully an organization needs several resources. Here I have compiled a list of possible resources. Can you tell me if in your opinion they are very important, important, or less important for the cyber-safety related business of your organization?

Zur Auswahl standen „expert knowledge“, „funding“, „technical equipment“, „influence on political decision making and legislation“, „influence on standardization“, „publicity“



Datenquelle: Interviews. *Codierung*: 1 "less important", 2 "important", 3 "very important".

Abbildung 5.14: *Gewichtung zentraler Ressourcen*

und „contact to other actors (networking)“. Weitere Ressourcen konnten ggf. ergänzt werden. Abbildung 5.14 zeigt das Gewicht, das den jeweiligen Ressourcen durch die Interviewpartner im Mittel zugemessen wurde.

Wichtigste Ressource ist Expertenwissen. Hier zeigt sich erwartungsgemäß – wie bereits bei der Untersuchung nach Tätigkeitsarten (vgl. Abschnitt 5.2.1) – die zentrale Rolle der Ressource Wissen in modernen Informationsgesellschaften. Information als problemrelevantes Wissen wird im Umfeld komplexer sozio-technischer Systeme verstärkt zur wesentlichen Voraussetzung einer rationalen Disposition verfügbarer Ressourcen und damit eines effektiven wie effizienten Handelns. Mit nur wenig Abstand folgen Kontakte zu anderen Akteuren. Dieses Sozialkapital ist Grundlage informeller Netzwerke und ermöglicht eine flexible, problemspezifische Mobilisation und Aggregation relevanter Ressourcen (vgl. hierzu Abschnitt 2.2.3). Das hohe Gewicht, welches dieser Ressource zugemessen wurde, unterstreicht somit die besondere Bedeutung des Netzwerkparadigmas als Steuerungsmechanismus im Prozeß der Produktion von Sicherheit in elektronischen Netzen.

Drittwichtigste Ressource sind Finanzmittel, gefolgt vom Zugang zu öffentlicher Aufmerksamkeit (Publizität) sowie dem Einfluß auf politische Rahmenentscheidungen. Einfluß auf Standardisierung und technische Ausstattung spielen überraschender Weise eine vergleichsweise geringe Rolle. Verantwortlich hierfür sind möglicherweise beschleunigte Innovationszyklen, die technische Systemkomponenten und Standards schnell veralten lassen.[189]

189 Vgl. hierzu das Konzept der „reverse salients“ bei Hughes (1987) sowie Abschnitt 3.3.1.

Im allgemeinen verteilen sich die zur Produktion eines Gutes benötigten Ressourcen auf mehr als einen Akteur (vgl. Abschnitt 2.2.1). Um diese Verteilung annähernd empirisch erfassen zu können, wurde in den Interviews nach den fünf wichtigsten Akteuren im globalen Politikfeld elektronischer Sicherheit im allgemeinen sowie den fünf wichtigsten Kooperationspartnern der jeweiligen Organisation im besonderen gefragt. Diesen insgesamt zehn Akteuren waren sodann jeweils zwei der oben genannten Ressourcen zuzuordnen. Eine Kreuztabelle in Appendix C faßt die ermittelten Ergebnisse zusammen. Hier finden sich alle Organisationen, die in mindestens einem Interview als wichtiger Akteur oder Kooperationspartner genannt wurden in Verbindung mit den Häufigkeiten der jeweiligen Ressourcenzuordnungen. Abbildung 5.14 veranschaulicht diese Zuordnungen als bipartiten Graphen. Die Dicke der Kanten korrespondiert mit der Häufigkeit der Nennungen.

Ersichtlich wird, daß die Ressourcen Expertenwissen, Kontakte (Sozialkapital) sowie Einfluß auf politische Rahmenentscheidungen vergleichsweise stark unter den Akteuren streuen. Die Ressourcen Finanzmittel, Publizität, technische Ausstattung und Einfluß auf Standards und Normen hingegen sind in der Kontrolle nur weniger Akteure. Insbesondere das US-DHS verfügt über ein breites Spektrum an Ressourcen, so u. a. ein hohes Sozialkapital, einen starken Einfluß auf politische Entscheidungen sowie ein hohes Maß an Publizität. Auch kontrolliert das US-DHS zusammen mit MS und der EC einen Großteil der zur Verfügung stehenden Finanzmittel. Ein weiterer zentraler Akteur ist MS, das über umfangreiches Expertenwissen und starken Einfluß in Standardisierungsverfahren verfügt. Dem CERT/CC wird primär Expertenwissen und soziales Kapital attestiert. Auffällig ist ferner, daß unter den großen Verbänden des IT-Sektors der ITAA hauptsächlich soziales Kapital, der BSA hingegen Einfluß auf politische Entscheidungsprozesse zugeschrieben wird.

Interessant ist die Frage, ob ein Zusammenhang zwischen *Status* bzw. *Scope* eines Akteurs sowie der Art der von ihm kontrollierten Ressourcen besteht. Abbildung 5.16 schlüsselt für jede Ressource die relative Verteilung nach *Status* und *Scope* der zugeordneten Akteure in Form eines segmentierten Balkendiagrammes auf. Mittels eines exakten zweiseitiger Tests nach Fisher wurde auch hier zunächst die Unabhängigkeit der beiden Variablenkombinationen *Status* und *Ressource* bzw. *Scope* und *Ressource* überprüft. Für die Kombination *Status* und *Ressource* ergab sich $p \approx 0.1579$[190], für

190 Mit Monte-Carlo-Simulation bei 2000 Wiederholungen.

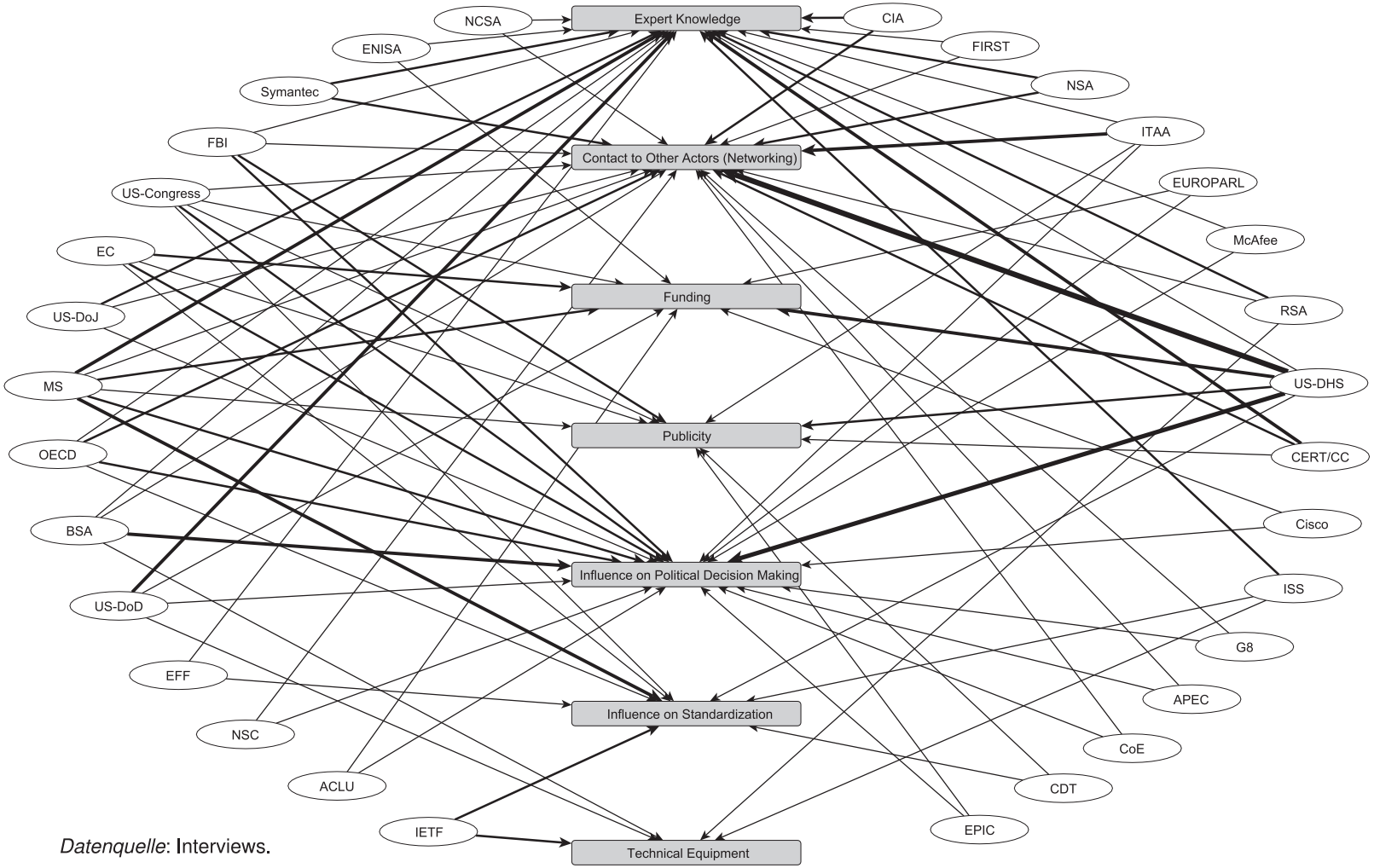


ABBILDUNG 5.15: *Kontrolle der Akteure über zentrale Ressourcen*

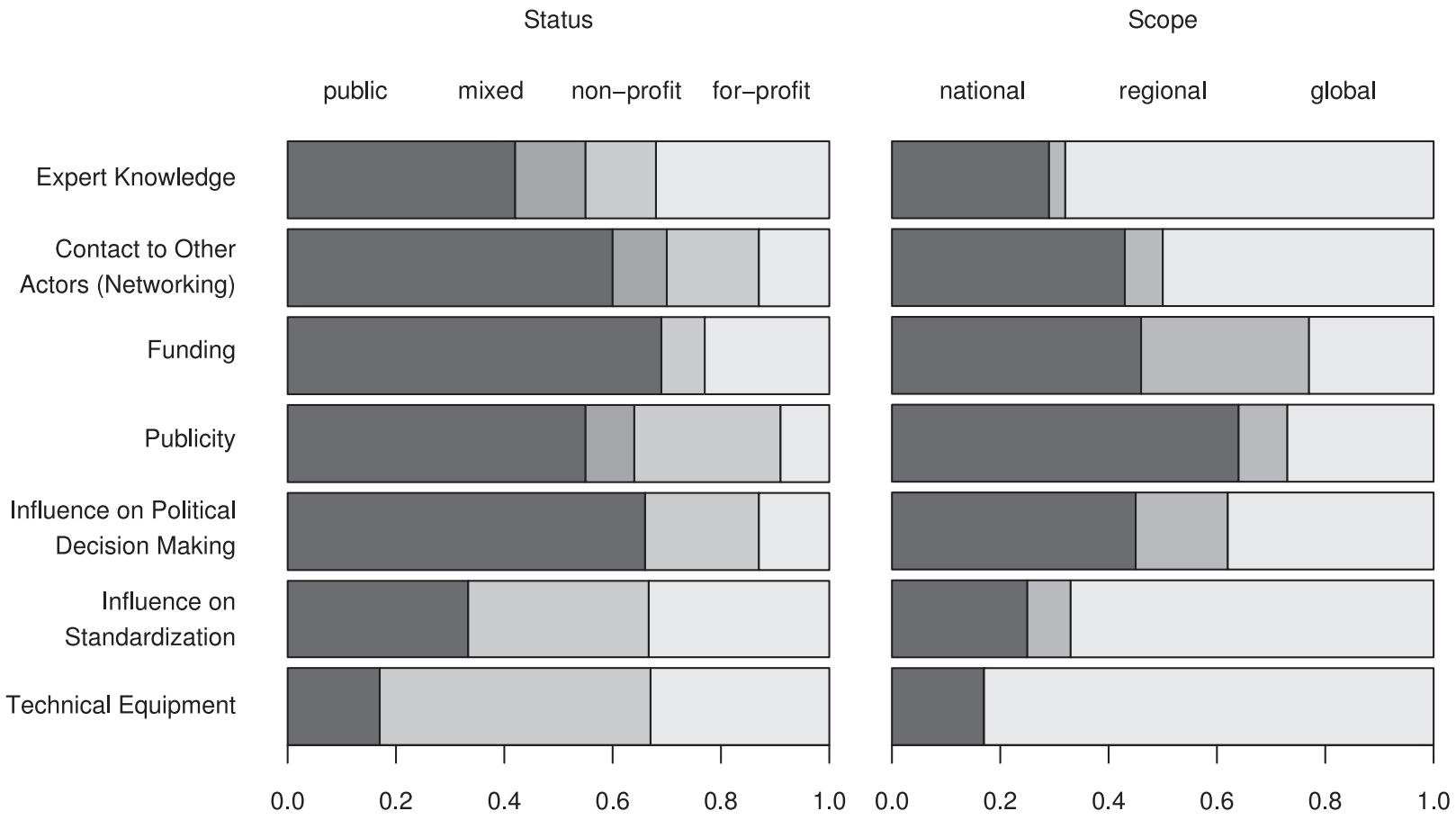


Abbildung 5.16: *Relative Verteilung der einzelnen Ressourcen nach Status und Scope der jeweils zugeordneten Akteure*

die Kombination *Scope* und *Ressource* $p \approx 0.0568$[191]. Im ersten Falle wird das üblicherweise geforderte Signifikanzniveau von $\alpha = 0.05$ demnach deutlich, im zweiten nur knapp verfehlt. Insbesondere eine Interpretation des Zusammenhangs von *Status* und *Ressource* kann daher nur unter Vorbehalten erfolgen.

Wie deutlich zu erkennen ist, befindet sich ein Großteil der Ressourcen in der Kontrolle öffentlicher Akteure. Dies gilt insbesondere für Finanzmittel und Einfluß auf politische Rahmenentscheidungen. Aber auch über soziales Kapital verfügen ganz überwiegend öffentliche Akteure. Der Kollektivgutcharakter elektronischer Sicherheit (vgl. hierzu Abschnitt 4.3.1) erklärt aufgrund der Trittbrettfahrerproblematik, warum eine ausreichende Versorgung mit diesem Gut öffentlich zu gewährleisten ist. Offenbar spielt in diesem Kontext die Bereitstellung finanzieller Mittel durch öffentliche Akteure eine zentrale Rolle. Daß öffentliche Akteure per se vielfältige Möglichkeiten der Einflußnahme auf politische Rahmenentscheidungen haben, bedarf keiner weiteren Erörterung. Interessant ist die Dominanz öffentlicher Akteure im Bereich des sozialen Kapitals, die eine zentrale Rolle der öffentlichen Hand bei der Steuerung der Produktion und Distribution des Gutes Sicherheit in elektronischen Netzen vermuten läßt.

Die Stärke privater Akteure liegt offensichtlich im Bereich der technischen Ausstattung sowie in ihrem Einfluß auf Standards und Normen. Da technische Komponenten den Charakter privater Güter haben, kann ihre Bereitstellung problemlos privaten Akteuren überlassen bleiben. Auffallend ist jedoch, daß über die Hälfte dieser Akteure nicht-gewinnorientiert ist. Ihr Beitrag zur Produktion des Gutes Sicherheit in elektronischen Netzen kann daher auch nicht unmittelbar über Anreizstrukturen des Marktes koordiniert werden. Dies und die – vermutlich durch Skaleneffekte bedingte – vergleichsweise geringe Anzahl von Akteuren, die über technische Ressourcen verfügen, legen Netzwerke als geeigneten Koordinationsmechanismus nahe. Ein ähnliches Bild ergibt sich bezüglich des Einflusses auf Standards und Normen. Auch hier dominieren mit zwei Dritteln eindeutig private Akteure. Diese sind zur Hälfte gewinnorientiert. Das verbleibende Drittel nehmen öffentliche Akteure ein. Die gleichmäßige Verteilung der Akteure auf diese drei *Status* läßt erkennen, daß Standardisierung vermutlich das Ergebnis eines Aushandlungsprozesses zentraler Akteure sowohl des öffentlichen als auch des privaten Sektors ist. Auch hier spricht die vergleichsweise geringe Zahl beteiligter Akteure für den Koordinationsmechanismus des Netzwerkes.

191 Ohne Monte-Carlo-Simulation.

Die zentrale Ressource Expertenwissen streut – wie bereits erwähnt – stark. Sie befindet sich zu etwa gleichen Teilen in der Kontrolle privater sowie öffentlicher Akteure. Im privaten Sektor dominieren allerdings mit deutlichem Abstand gewinnorientierte Akteure. Offenbar hat Expertenwissen bzw. Information hier primär den Charakter eines über Marktmechanismen allozierbaren Privatgutes (vgl. Abschnitt 3.1.4). Andererseits verfügen aber auch und gerade öffentliche Akteure über profundes sicherheitsrelevantes Wissen, nicht zuletzt wohl deshalb, weil die Aufgabe der Produktion gesellschaftlicher Sicherheit traditionell staatlichen Institutionen zukommt. Zugleich reflektiert die breite Dispersion über Akteure aller *Status* die zentrale Bedeutung dieser Ressource in modernen Gesellschaften.

Über die Ressource Publizität – also die Fähigkeit Informationen an eine große Anzahl anderer Akteure richten zu können – verfügen nur wenige Akteure. Da die kognitive Kapazität einzelner Akteure beschränkt ist, fokussieren diese ihre Aufmerksamkeit notwendigerweise auf einige wenige Informationsquellen. Akteure, denen es gelingt, solchermaßen knappe Aufmerksamkeit zu attrahieren, besetzen innerhalb kommunikativer Netzwerke folglich eine exponierte – durch eine große Anzahl ausgehender Informationsbeziehungen gekennzeichnete – multiplikative Position, die ihnen Publizität verschafft. Ihr Verhältnis zu anderen Akteuren entspricht einer Punkt-zu-Multipunkt-Beziehung. Wesentlicher Unterschied zu sozialem Kapital ist die einseitige Gerichtetheit der Kommunikationsbeziehung vom Multiplikator zu einem weitgehend anonymen Publikum. Erreicht ein Akteur auf diese Weise eine sehr hohe Zahl anderer Akteure, so kann er Information als öffentliche, entscheidungsrelevante Ressource bereitstellen und damit zugleich steuernden Einfluß auf das Handeln dieser Akteure gewinnen. Über Publizität verfügen vor allem öffentliche und nicht-gewinnorientierte private Akteure. Vermutlich ist eine Mehrheit aller Akteure geneigt, diese aufgrund ihrer fehlenden Gewinnabsicht bevorzugt als vertrauenswürdige Informationsquelle heranzuziehen.

Eine Betrachtung der Verteilung der Ressourcen nach der Aktionsebene der zugeordneten Akteure zeigt, daß Expertenwissen, technische Komponenten sowie Einfluß auf Standards und Normen in starkem Maße durch global operierende Akteure kontrolliert werden. Hinsichtlich der technischen Ausstattung ist dies aufgrund von Skaleneffekten sowie der notwendigen Kompatibilität global vernetzter technischer Komponenten nicht verwunderlich. Auch Standards und Normen entfalten ihr Nutzenmaximum selbstverständlich erst im Rahmen einer globalen Harmonisierung. Der globale bzw. transnationale Problemcharakter (vgl. Abschnitt 4.2.3) bedingt offenbar ferner, daß insbesondere

global operierende Akteure handlungsrelevantes Expertenwissen akkumulieren.

Bei der Ressource Publizität ist eine starke Bindung an die nationalstaatliche Ebene zu beobachten. Ursächlich mögen sprachliche Differenzen sowie eine weitgehende Kongruenz von kulturellem Bezugs- und nationalem Handlungsrahmen sein. Beides verschafft möglicherweise auf nationaler Ebene handelnden Akteuren ein höheres Maß an Aufmerksamkeit und Vertrauen. Finanzielle Ressourcen werden ebenfalls hauptsächlich durch nationale Akteure bereitgestellt. Darüber hinaus spielen in diesem Kontext regionale Akteure eine bedeutende Rolle. Ein ähnliches Bild ergibt sich bezüglich des Einflusses auf politische Rahmenentscheidungen. Hier zeigt sich ansatzweise, daß der transnationale Problemcharakter zunächst im regionalen Kontext eine grenzüberschreitende Lastenteilung und Entscheidungsfindung erzwingt. Über Kontakte zu anderen Akteuren (Sozialkapital) schließlich verfügen globale und nationale Akteure in etwa gleichermaßen.

5.2.3 Problemlösungskapazität und Koordinationsbedarf

Nachdem in Abschnitt 5.2.2 Gewicht und Verteilung zentraler Ressourcen untersucht wurde, kann nun in einem weiteren Schritt die Problemlösungskapazität der Akteure ermittelt werden. Unter der Problemlösungskapazität eines Akteurs soll dessen Fähigkeit verstanden werden, substantiell zur Produktion von Sicherheit in elektronischen Netzen beizutragen. Ein solcher potentieller Beitrag beruht – gemäß den in Abschnitt 2.2 erläuterten theoretischen Annahmen – wesentlich auf Art und Umfang der von dem jeweiligen Akteur kontrollierten Ressourcen. Zur Operationalisierung der Problemlösungskapazität eines Akteurs i wird daher die auf diesen Akteur entfallende gewichtete Ressourcenkonzentration, also dessen relativer Anteil s_i am gesamten gewichteten Ressourcenpool, vorgeschlagen:

$$s_i = \frac{\sum_k x_{ik} \cdot w_k}{\sum_{jk} x_{jk} \cdot w_k} \tag{5.4}$$

Es seien x_{ik} sowie x_{jk} die Häufigkeiten der Zuordnungen der Ressource k zu den Akteuren i bzw. j (vgl. Appendix C) und w_k das gemittelte Gewicht der Ressource k (vgl. Abbildung 5.14).

Anhand der sich aus Formel 5.4 ergebenden Werte verdeutlicht Abbildung 5.17 links die Konzentration der gewichteten Ressourcen. Rechts sind die kumulierten Anteile wiedergegeben, aus denen sich die zugehörige Lorenz-Kurve ableitet. Erkennbar ist

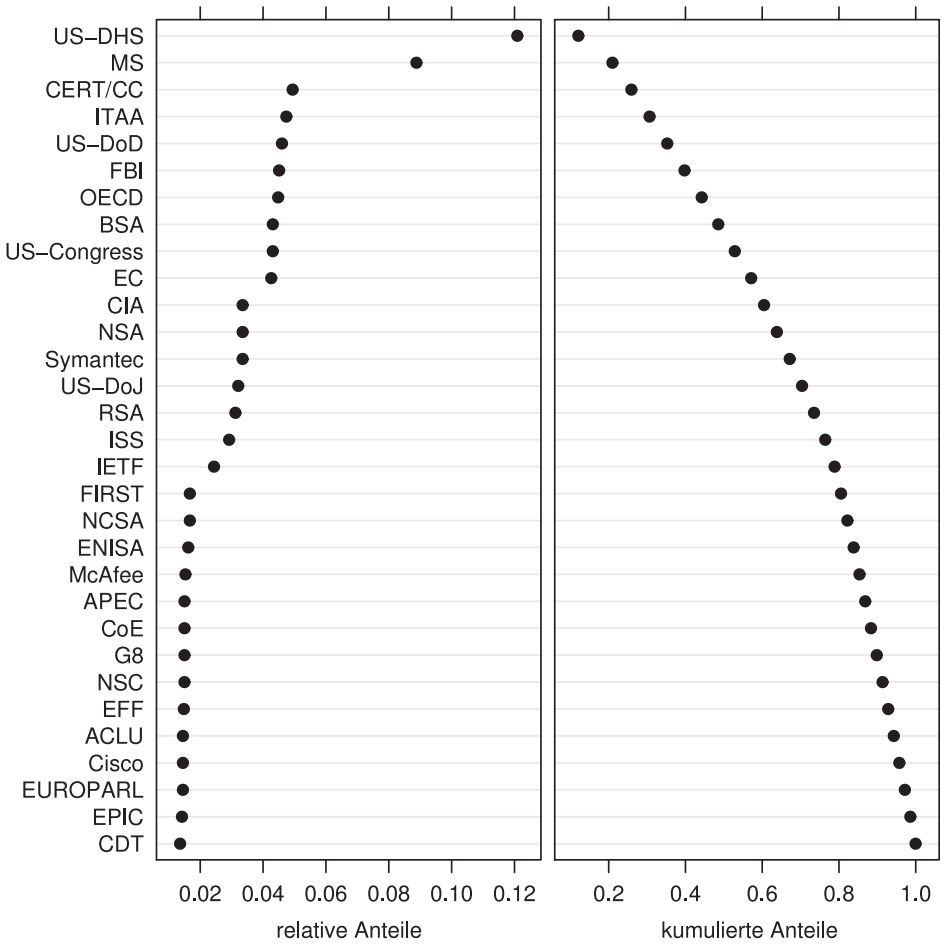


Abbildung 5.17: *Die gewichtete Ressourcenkonzentration*

das US-DHS der Akteur mit der höchsten gewichteten Ressourcenkonzentration und damit größten Problemlösungskapazität. Mit einigem Abstand folgt MS. Alle anderen Organisationen sind weit abgeschlagen und verfügen jeweils für sich genommen über weniger als fünf Prozent des Ressourcenpools. Bei Betrachtung der kumulierten Anteile wird deutlich, daß auch die beiden stärksten Akteure US-DHS und MS zusammen nur etwas mehr als ein Fünftel des Ressourcenpools kontrollieren und demnach auf eine enge Zusammenarbeit mit anderen Akteuren angewiesen sind.

Die gewichtete Ressourcenkonzentration gibt über den zu erwartenden Koordinationsbedarf Auskunft, denn je gleichmäßiger sich die zur Produktion von Sicherheit in elektronischen Netzen benötigten Ressourcen auf die einzelnen Akteure verteilen, desto mehr dieser Akteure müssen offensichtlich in den Prozeß der Problemlösung einge-

bunden werden. Verfügte hingegen ein einzelner Akteur über sämtliche Ressourcen, so wäre Koordination gänzlich überflüssig. Entscheidend für den Koordinationsaufwand ist daher offenbar die Wahrscheinlichkeit, mit welcher ein Akteur bestimmte sicherheitsrelevante Ressourcen kontrolliert. Die Konzentration der gewichteten Ressourcen kann als genau diese Wahrscheinlichkeit interpretiert werden.

Üblicherweise wird als Maßzahl einer Ungleichverteilung der Gini-Koeffizient herangezogen. Hier jedoch soll dem Theil-Index (vgl. Cowell 1995: 47 ff.) der Vorzug gegeben werden, da sich dieser vom informationstheoretischen Entropie-Maß Shannons ableitet (vgl. hierzu Formel 3.1):

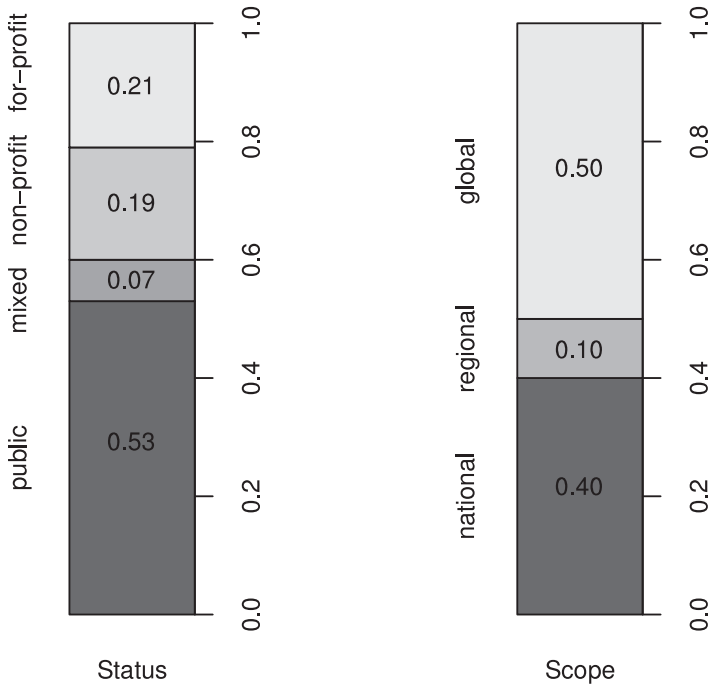
$$T = \frac{1}{n} \sum_i \frac{s_i}{\bar{s}} \cdot ln\left(\frac{s_i}{\bar{s}}\right) \tag{5.5}$$

Es bezeichnet n die Anzahl der Akteure und $\bar{s} = \frac{1}{n} \sum_i s_i$ den durchschnittlichen Anteil gewichteter Ressourcen.

Warum eine informationstheoretische Betrachtungsweise für die vorliegende Untersuchung von Vorteil ist, wird deutlich, wenn man unterstellt, daß die im Rahmen der Koordination anfallenden Transaktionskosten auch und vor allem Informationskosten sind (vgl. hierzu Abschnitt 2.2.1). Der Theil-Index interpretiert im Sinne der Informationstheorie (vgl. hierzu Abschnitt 3.1.3) die einzelnen Akteure als Elementarereignisse und die auf sie entfallenden relativen Anteile als deren Eintrittswahrscheinlichkeit. Als Differenz der tatsächlichen Entropie einer Verteilung zu deren maximal möglicher Entropie, wie sie sich im Falle einer vollkommenen Gleichverteilung ergäbe, stellt er ein Redundanz-Maß dar. Im vorliegenden Falle ist $T \approx 0.19$ und die maximal mögliche Entropie $H_{max} = ln(n) = ln(31) \approx 3.43$, woraus sich eine tatsächliche Entropie von $H = H_{max} - T \approx 3.24$ errechnet.

Diese Entropie ist nun ein quantitatives Maß für jene Menge an Information, die benötigt wird, um den eine bestimmte Ressource kontrollierenden Akteur zu identifizieren. Wenn aber Koordination vor allem der Mobilisation verstreuter Ressourcen zum Zwecke der Produktion eines Gutes dient (vgl. Abschnitt 2.2), so ist genau diese Information entscheidend. Weil $H \approx 3.24$ verhältnismäßig nahe an $H_{max} \approx 3.43$ liegt, wird deutlich, daß insgesamt mit einem relativ hohen Koordinationsaufwand zu rechnen ist. Da sich die Ressourcen, abgesehen von den beiden Ausreißern US-DHS und MS, relativ gleichmäßig auf die Akteure verteilen, entspricht dies den theoretischen Erwartungen.

Aus der Lorenz-Kurve läßt sich ablesen, daß die ersten zehn Akteure (einschließlich



Anmerkung: Anteile wurden gerundet.

ABBILDUNG 5.18: *Relative Anteile am gesamten gewichteten Ressourcenpool nach Status und Scope der zugeordneten Akteure*

.

EC) und damit das obere Drittel zusammen genommen über annähernd zwei Drittel der gewichteten Ressourcen verfügen. Eine effektive Ressourcenmobilisation im Prozeß der Produktion elektronischer Sicherheit setzt also offenbar eine enge Koordination und damit Vernetzung insbesondere dieser zentralen Akteure voraus.

Abbildung 5.18 zeigt die relativen Anteile am gesamten gewichteten Ressourcenpool, differenziert nach *Status* und *Scope* der zugeordneten Akteure. Hier wird noch einmal erkennbar, daß sich über die Hälfte des gewichteten Ressourcenpools in der Kontrolle öffentlicher Akteure befindet. Private gewinnorientierte Akteure verfügen hingegen nur über etwa ein Fünftel. Ein Großteil der zentralen Ressourcen im Prozeß der Produktion elektronischer Sicherheit wird demnach von öffentlichen Akteuren bereitgestellt. Ferner läßt sich erkennen, daß global agierende Organisationen über rund die Hälfte des Ressourcenpools verfügen. Weitere 40 Prozent entfallen auf nationale Akteure.

Interessant ist ferner ein Vergleich zwischen der faktischen, ressourcenbezogenen Problemlösungskapazität der Akteure einerseits, sowie der attribuierten Reputation

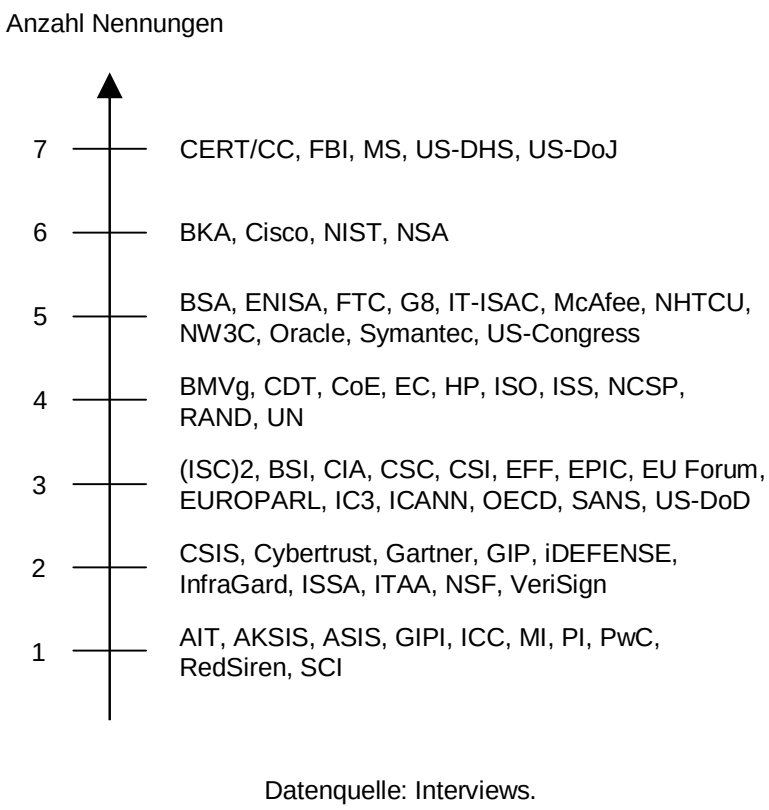


ABBILDUNG 5.19: *Reputation der Akteure in den Interviews*

dieser Akteure, also deren vermeintlicher Problemlösungskapazität, andererseits. Hierzu sollten die Interviewpartner auf einer Liste jene Organisationen markieren, die ihrer Meinung nach hinsichtlich der Produktion von Sicherheit in elektronischen Netzen wichtig seien. Abbildung 5.19 zeigt die Anzahl der Nennungen, die auf die jeweiligen Akteure entfielen, als Maß für deren Reputation. Um zumindest eine eingeschränkte Vergleichbarkeit des diskreten Reputationsindexes mit dem kontinuierlichen Index der gewichteten Ressourcenkonzentration (Abbildung 5.17) zu ermöglichen, wurde der Wertebereich des letzteren in sieben gleichgroße Intervalle unterteilt und die Akteure entsprechend klassifiziert.

Tabelle 5.9 schlüsselt für die Schnittmenge der Akteure aus Abbildung 5.17 und 5.19 die Abweichungen zwischen Reputation und Ressourcen-Intervall auf. Die Reputation der Akteure ITAA, OECD, US-DoD, US-DHS, CIA und EC korrespondiert demnach weitgehend mit ihrer tatsächlichen Problemlösungskapazität. MS, EPIC, EUROPARL, EFF, ISS, US-Congress, BSA, CDT, CoE und Symantec werden leicht überschätzt.

Tabelle 5.9: *Abweichung von Reputation und Problemlösungskapazität*

Akteur	*Ressourcen-Intervall*	*Reputation*	*Abweichung*
ITAA	3	2	-1
OECD	3	3	0
US-DoD	3	3	0
US-DHS	7	7	0
CIA	2	3	1
EC	3	4	1
MS	5	7	2
EPIC	1	3	2
EUROPARL	1	3	2
EFF	1	3	2
ISS	2	4	2
US-Congress	3	5	2
BSA	3	5	2
CDT	1	4	3
CoE	1	4	3
Symantec	2	5	3
G8	1	5	4
McAfee	1	5	4
ENISA	1	5	4
NSA	2	6	4
FBI	3	7	4
CERT/CC	3	7	4
Cisco	1	6	5
US-DoJ	2	7	5

Deutlich überbewertet werden hingegen G8, McAfee, ENISA, NSA, FBI, CERT/CC, CISCO und US-DoJ.

5.3 Koordinationskonfigurationen

5.3.1 Das Gesamtnetzwerk der Fallstudien

Im Rahmen der zehn Fallstudien wurden die Interviewpartner u. a. nach den direkten Kooperationsbeziehungen ihrer jeweiligen Organisation befragt. Aus den erhobenen Daten lassen sich egozentrierte Netzwerke, d. h. solche, die jeweils perspektivisch in einem bestimmten Akteur verankert sind, ermitteln (vgl. Pappi 1987: 20 ff.). Als „name

TABELLE 5.10: *Vergleich der Fallstudien*

Akteur	*Anzahl der Kontakte**			*relative Anteile der Status***			
	gesamt	regel-mäßig	gelegent-lich	public	mixed	non-profit	for-profit
BSA	40 (1.00)	33 (0.83)	7 (0.18)	0.38	0.04	0.26	0.32
BSI	19 (1.00)	9 (0.47)	10 (0.53)	0.57	0.25	0.04	0.14
CERT/CC	keine Angaben						
CSIS	27 (1.00)	7 (0.26)	20 (0.74)	0.44	0.06	0.18	0.32
EFF	4 (1.00)	4 (1.00)	0 (0.00)	0.25		0.75	
EPIC	6 (1.00)	1 (0.17)	5 (0.83)	0.43		0.43	0.14
ENISA	8 (1.00)	1 (0.14)	7 (0.86)	0.44	0.11	0.22	0.22
MS	13 (1.00)	12 (0.92)	1 (0.08)	0.36	0.16	0.24	0.24
Symantec	60 (1.00)	48 (0.80)	12 (0.20)	0.41	0.09	0.27	0.23
US-DHS	44 (1.00)	16 (0.36)	28 (0.64)	0.42	0.12	0.22	0.25

* relative Anteile in Klammern gerundet

** regelmäßige Kontakte doppelt gewichtet, Werte gerundet

generator“ (Burt 1984: 296) diente folgende, in Verbindung mit einer Akteurs-Liste, gestellte Frage:

> Could you identify those organizations that your organization is regularly or occasionally cooperating with in order to enhance security and trustworthiness of electronic transactions? Please feel free to add any missing organizations.

Für die jeweiligen egozentrierten Kooperationsnetzwerke (vgl. Abbildungen 5.21 bis 5.29) wurden sodann die relativen Anteile der Kooperationspartner nach *Status* berechnet. Kooperationspartner, zu denen die untersuchten Organisationen regelmäßige Beziehungen unterhalten, wurden hierfür doppelt gewichtet. Tabelle 5.10 faßt die entsprechenden Daten in einer Übersicht zusammen.

Möglich ist ferner eine Rekonstruktion des Kooperationsnetzwerkes der zehn Fallbeispiele untereinander. Dieses Netzwerk entspricht einem voll erhobenen Ausschnitt aus dem gesamten Kooperationsnetzwerk aller Akteure. Einschränkend ist hier zu erwähnen, daß das CERT/CC aus Gründen der Geheimhaltung keine Auskunft zu Kooperationsbeziehungen gab. Abbildung 5.20 zeigt den entsprechenden induzierten Teilgraphen, visualisiert mit Hilfe der freien Software *VISONE*[192] und basierend auf der Eigenvektor- bzw. Standard-Zentralität (Brandes u. Wagner 2004b: 324).

192 Vgl. hierzu Brandes u. Wagner (2004a,b) sowie <`http://visone.info`>.

Die Eigenvektor-Zentralität ist ein rekursiv definiertes Feedback-Maß. Die Zentralität eines Knotens errechnet sich dabei aus der Zentralität aller jeweils angrenzenden Knoten. Wie in Abschnitt 2.2 ausgeführt, wird Kooperation im Kontext der vorliegenden Arbeit vor allem als Koordinationsmechanismus zur Mobilisation verstreuter Ressourcen verstanden. Aus einer solchen theoretischen Perspektive kann ein Akteur dann effizient Ressourcen mobilisieren, wenn er möglichst viele Kooperationskontakte zu solchen Akteuren unterhält, die ihrerseits über eine Vielzahl von Kontakten verfügen. Als Indikator für die Mobilisationsfähigkeit der Akteure im Kooperationsnetzwerk eignet sich daher ein Feedback-Maß in besonderer Weise.

Deutlich zu erkennen ist, daß die drei Akteure US-DHS, MS und CERT/CC bezüglich der Ressourcenmobilisation eine zentrale Stellung innerhalb des Teilnetzwerkes der Fallbeispiele einnehmen. Ihre Zentralität im Kooperationsnetzwerk korrespondiert auffällig mit der jeweiligen Problemlösungskapazität (vgl. Abschnitt 5.2.3). Die drei Organisationen lassen sich daher jeweils als Exponenten des öffentlichen, des gewinnorientierten privaten sowie des gemischten Sektors betrachten. Als Exponent des nichtgewinnorientierten privaten Sektors kann ferner die BSA herangezogen werden, die allerdings im Kooperationsnetzwerk etwas weniger zentral verortet ist. Damit sind im Kern des Netzwerkes Organisationen aller vier *Status* vertreten. Die beiden Bürgerrechtsorganisationen EFF und EPIC hingegen bilden eine Clique, welche zwar intern eng kooperiert, extern jedoch nur zu wenigen anderen Akteuren Kontakte unterhält und sich in Folge dessen eher an der Peripherie des Netzwerkes bewegt. Auch diese Beobachtung entspricht in hohem Maße der in Abschnitt 5.2.3 gemessenen Problemlösungskapazität beider Akteure.

Eine mögliche Hypothese wäre hier, daß vor allem solche Akteure, die bereits genuin über einen hohen gewichteten Ressourcenanteil und damit eine hohe Problemlösungskapazität verfügen, innerhalb des Kooperationsnetzwerkes am ehesten in der Lage sind, zusätzliche Ressourcen zu mobilisieren. Aufgrund ihrer hohen Problemlösungskapazität stellen sie offenbar für andere Akteure besonders attraktive Kooperationspartner dar. Im Umfeld dieser zentralen Akteure bilden sich im Netzwerk Governance-Strukturen zur Aggregation und Mobilisation relevanter Ressourcen, die eine flexible Lösung auftretender Sicherheitsprobleme ermöglichen.

Weiter läßt sich beobachten, daß annähernd zwei Drittel (≈ 0.62) der Kooperationsbeziehungen des Teilnetzwerkes auf regelmäßigen Kontakten beruhen. Das Netzwerk befindet sich somit in diesem Punkt näher an den formalen Strukturen einer Hierarchie

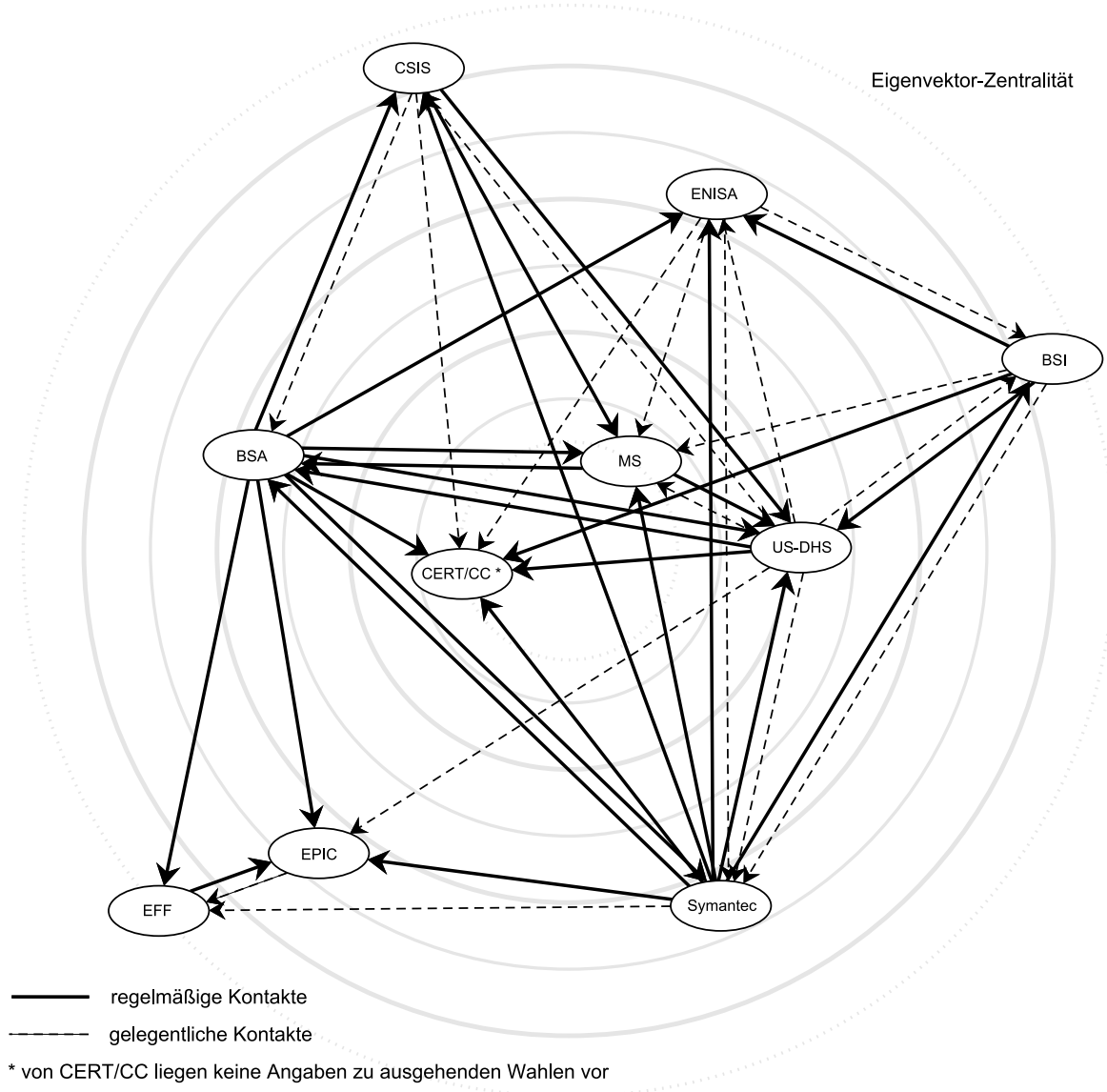


Abbildung 5.20: *Das Kooperationsnetzwerk der zehn Fallstudien untereinander*

als an der anonymen und atomistischen Struktur des Marktes (vgl. hierzu Tabelle 2.1). Eine weitere Hypothese ist daher, daß gerade das in sicherheitsrelevanten Bereichen unabdingbare Vertrauen vor allem auf dauerhaften Kooperationsbeziehungen beruht, ohne dabei den vertikalen Integrationsgrad einer Hierarchie zu erreichen. Durch die Polyzentralität der Koordination bleibt so zugleich eine gewisses Maß an Flexibilität erhalten.

5.3.2 Die Konfigurationen der Fallbeispiele

5.3.2.1 BSA

Die *Business Software Alliance* (BSA) ist ein international tätiger Interessenverband der Software-Industrie mit etwa 100 Mitarbeitern. Er wurde im Jahre 1988 in den USA gegründet und ist derzeit weltweit in über 80 Ländern auf allen fünf Kontinenten aktiv. Hauptsitz des Verbandes ist Washington, DC. Daneben werden Büros in Brüssel, London, München, Peking, Delhi, Jakarta, Kuala Lumpur, Taipeh, Tokio, Singapur und São Paulo unterhalten. In den USA ist die BSA – neben der ITAA – einer der führenden Interessenverbände des IT-Sektors. Der Verband finanziert sich ausschließlich aus den Beiträgen seiner Mitglieder, zu denen bedeutende Wirtschaftsunternehmen wie Cisco, HP, IBM, ISS, McAfee, MS, Oracle, RSA, SAP, Siemens und Symantec gehören. Partnerschaften werden u. a. zu IC3 und ISSA unterhalten.

Als wichtigste Ressource wird der BSA Einfluß auf politische Rahmenentscheidungen attestiert (vgl. Abbildung 5.15). Dieser Einfluß manifestiert sich u. a. in personellen Verquickungen. So wechselte bspw. Anfang 2009 der bisherige stellvertretende Geschäftsführer der BSA, Neil MacBride, im Zuge der neuen Administration Obama in das US-DoJ.[193] Weitere wichtige Ressourcen der BSA sind Sozialkapital, Expertenwissen und technische Ausstattung. Aufgrund dieser Ressourcen verfügt der Verband über eine vergleichsweise hohe Problemlösungskapazität (vgl. Abbildung 5.17).

Im Gegensatz zu CERT/CC und US-DHS lehnt die BSA als Interessenvertretung der Software-Industrie umfangreiche Sicherheitsauflagen für Wirtschaftsunternehmen als Kostenfaktor und Innovationshindernis ab. Daher opponierte der Verband bspw. zusammen mit der ITAA und anderen im Jahre 2003 in den USA erfolgreich gegen einen Gesetzentwurf[194], der börsengehandelte Unternehmen zu einer regelmäßigen und unabhängigen Sicherheitsüberprüfung ihrer Informationsinfrastruktur sowie einer Offenlegung der Ergebnisse im jeweiligen Jahresbericht verpflichtet hätte. Da das Hauptinteresse des Verbandes dem Schutz geistiger Eigentumsrechte im Kontext digitaler Informations- und Kommunikationssysteme gilt, favorisiert die BSA stattdessen nationale Gesetze und internationale Verträge, die eine effektive Aufklärung und Strafverfolgung von Urheberrechtsverletzungen auch im transnationalen Rahmen ermöglichen

193 Vgl. hierzu die Mitteilung der BSA unter <`http://www.bsa.org/country/News\%20and\%20Events/News\%20Archives/en/2009/en-01222009-macbride.aspx`>.

194 Corporate Information Security Accountability Act of 2003, auch bekannt als Putnam Bill.

sollen. So unterstützte der Verband nachdrücklich die Cybercrime-Konvention[195] des Europarates.

Dieser Konvention wird von Seiten der BSA Modellcharakter hinsichtlich einer künftigen Sicherheitspolitik in elektronischen Netzen beigemessen. Sie verpflichtet die Unterzeichnerstaaten in ihrem jeweiligen nationalen Recht Regelungen zur Aufklärung und Verfolgung elektronischer Straftaten, zur grenzüberschreitenden Zusammenarbeit ihrer Strafverfolgungsbehörden sowie zur Auslieferung Angeklagter zu etablieren. Um den Strafverfolgungsbehörden eine Rückverfolgung von Straftaten sowie eine entsprechende Beweiserhebung in elektronischen Netzen zu ermöglichen, erklären sich die Unterzeichnerstaaten ferner bereit, eine Speicherung und ggf. Offenlegung der Verbindungsdaten rechtlich zu gewährleisten. Insbesondere diese Regelungen konfligieren eo ipso mit Zielen des Persönlichkeits- bzw. Datenschutzes und werden daher teilweise von Bürgerrechtsorganisationen – wie etwa ACLU, CCC, CDT, EFF, EPIC, ISOC, PI sowie deren internationalem Dachverband GILC – kritisiert.

Innerhalb bestehender nationaler Rechtssysteme bemüht sich die BSA proaktiv um die Durchsetzung geistiger Eigentumsrechte und übernimmt dabei als privater Akteur teilweise auch Ermittlungsaufgaben. So führt der Verband selbst Untersuchungen zu möglichen Urheberrechtsverletzungen durch und verfolgt diese ggf. vor Gericht. Die Maßnahmen hierfür reichen von Mahnschreiben bis zur Auslobung von Belohnungen für die Aufdeckung von Verstößen gegen das Urheberrecht. Eine Überprüfung der Software-Lizenzen wird dann gerichtlich erzwungen. Darüber hinaus unterstützt die BSA Aufklärungs- und Werbekampagnen gegen Software-Piraterie.

Zur Durchsetzung seiner Ziele kooperiert der Verband im Rahmen verschiedener Partnerschaften sowohl mit öffentlichen als auch privaten Akteuren. Ein Beispiel hierfür ist die *National Cyber-Forensics and Training Alliance* (NCFTA)[196], die Akteuren aus Wirtschaft, Wissenschaft und öffentlicher Verwaltung als Forum des vertraulichen Informationsaustausches und der Weiterbildung zu sicherheitsrelevanten Vorfällen in elektronischen Netzen dient. Ebenfalls beteiligt sich die BSA – neben der ITAA, TechNet sowie der amerikanischen Handelskammer – an der *National Cyber Security Partnership* (NCSP). Diese geht auf eine Initiative des US-DHS zurück und koordiniert privatwirt-

195 Zur Budapester Konvention, auch bekannt als Cybercrime-Konvention, vgl. Abschnitt 5.1.1.2.
196 Vgl. <`http://www.ncfta.net`>.

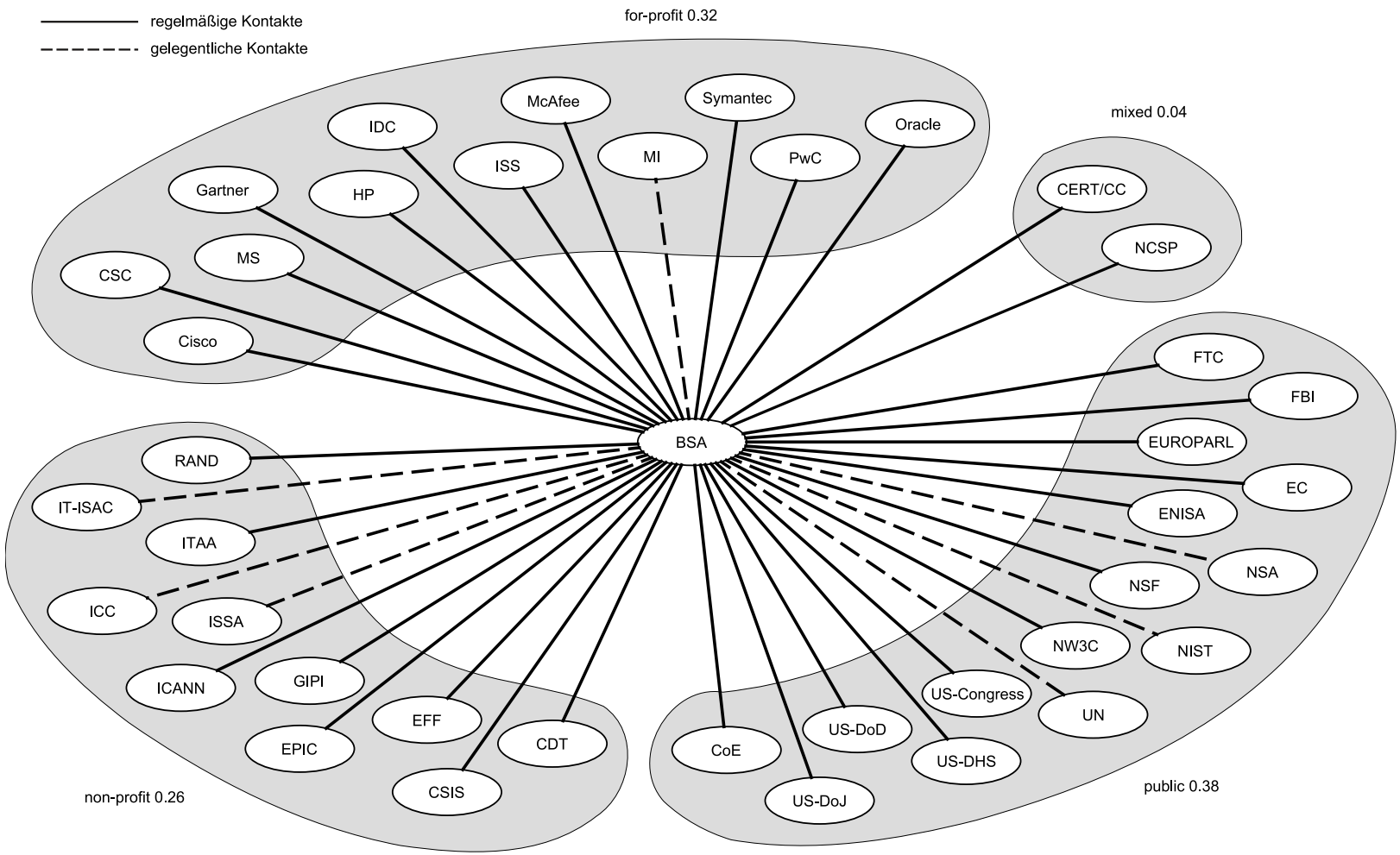


Abbildung 5.21: *Das egozentrierte Kooperationsnetzwerk der BSA*

schaftliche Bemühungen im Rahmen der *National Strategy to Secure Cyberspace*[197]. Die NCSP unterhält fünf Arbeitsgruppen zu den Themen: (1) Sensibilisierung privater Anwender und kleiner Unternehmen, (2) Frühwarnung bei Gefährdungen in elektronischen Netzen, (3) Corporate Security Governance, (4) Sicherheit bei der Entwicklung und während des Lebenszyklus von Software, (5) Technische Standards.

Abbildung 5.21 zeigt, daß die BSA nach den Angaben im Interview neben den bereits erwähnten Partnerschaften auch eine Vielzahl von Kooperationsbeziehungen zu anderen Akteuren unterhält, von denen der bei weitem überwiegende Anteil (≈ 0.83) auf regelmäßigen Kontakten beruht. Hier zeigt sich nochmals das hohe Sozialkapital, über welches der Verband verfügt. Im Kooperationsnetzwerk der untersuchten Fallstudien (vgl. Abbildung 5.20) erreicht die BSA eine mittlere Zentralität, die mit einer überdurchschnittlichen Reputation korrespondiert (vgl. Abbildung 5.19). Der Verband verfügt u. a. über bestätigte regelmäßige Kooperationsbeziehungen zu den beiden zentralen Akteuren MS und US-DHS sowie über unbestätigte regelmäßige Kontakte zum ebenfalls zentralen CERT/CC.

Im Vergleich zur relativen Verteilung der *Status* in der Gesamtmenge aller untersuchten Organisationen (vgl. Abbildung 5.3) sind unter den Kontakten der BSA gewinnorientierte private Akteure mit einem relativen Anteil von ≈ 0.32 (gesamt ≈ 0.24) sowie öffentliche Organisationen mit einem relativen Anteil von ≈ 0.38 (gesamt ≈ 0.30) deutlich überrepräsentiert. Hier wird deutlich, daß die BSA eine prominente Scharnierfunktion an der Schnittstelle zwischen privater Wirtschaft und öffentlichem Sektor wahrnimmt. Als Verband der Software-Industrie vertritt die Organisation gegenüber öffentlichen Akteuren vor allem die ökonomischen Interessen ihrer Mitglieder im Prozeß der Politikformulierung. Als Gegenleistung stellt sie zur Produktion von Sicherheit in elektronischen Netzen die Ressourcen Sozialkapital, Expertenwissen und technische Ausstattung zur Verfügung.

197 Die „National Strategy to Secure Cyberspace“ (vgl. US Department of Homeland Security 2003) wurde – veranlaßt durch die Terroranschläge des 11. September 2001 – vom US-DHS im Februar 2003 als Teil einer umfassenderen Strategie des Heimatschutzes entworfen. Sie enthält eine Reihe nicht verpflichtender Empfehlungen zum Schutz elektronischer Netze und richtet sich an Akteure aus Wirtschaft und Wissenschaft sowie private Anwender.

5.3.2.2 BSI

Das *Bundesamt für Sicherheit in der Informationstechnik* (BSI) ist eine obere Bundesbehörde im Geschäftsbereich des Innenministeriums der Bundesrepublik Deutschland mit Hauptsitz in Bonn. Vorläuferorganisationen waren die Zentralstelle für Sicherheit in der Informationstechnik (ZSI) sowie die Zentralstelle für das Chiffrierwesen (ZfCh). Letztere war seit 1962 für die Verschlüsselung des Fernmeldeverkehrs der Bundesregierung zuständig. Im Jahre 1986 wurde ihr auch der Aufgabenbereich Computersicherheit übertragen. Bedingt durch die telematische Konvergenz der Informations- und Kommunikationstechnologie gewann dieser Bereich zunehmend an Bedeutung, so daß 1989 eine Umwandlung in die Zentralstelle für Sicherheit in der Informationstechnik erfolgte. Aus dieser ging 1991 schließlich das BSI hervor.

Das BSI beschäftigt etwa 500 Mitarbeiter der Disziplinen Mathematik, Informatik und Physik. Die Behörde analysiert technische und soziale Sicherheitslücken und Risiken in Informations- und Kommunikationssystemen und berät hauptsächlich die Behörden des Bundes – aber auch der Länder sowie private Unternehmen und Anwender – hinsichtlich möglicher Schutzmaßnahmen. Schwerpunkte bilden die sechs Fachbereiche: (1) Sicherheit in Anwendungen, (2) Sicherheit in Kritischen Infrastrukturen und im Internet, (3) Kryptotechnik, (4) Abhörsicherheit, (5) Neue Technologien und Konformitätsprojekte, (6) Konformitätsprüfungen. Insgesamt sieht sich das BSI dabei in einer umfassenden Verantwortung für die IT-Sicherheit in Deutschland (vgl. Helmbrecht 2004: 98).

Für die öffentliche Verwaltung des Bundes betreibt das BSI die Public Key Infrastructure (PKI) sowie ein Computer Emergency Response Team (CERT-Bund). Im Rahmen des *Informationsverbundes Berlin-Bonn* stellt es mittels Kryptographieverfahren eine vertrauliche Kommunikationsverbindung zwischen Regierungsstellen in beiden Städten sicher. Die Behörde unterstützte das Bundesministerium des Innern bei der Ausarbeitung eines *Nationalen Plans zum Schutz der Informationsinfrastrukturen*[198]. Ferner publiziert das BSI regelmäßig *IT-Grundschutz-Kataloge*, die Behörden und Unternehmen ein standardisiertes Sicherheitskonzept für Informations- und Kommunikationssysteme zur Verfügung stellen. Auf Grundlage dieser Kataloge kann eine Bewertung

198 Der „Nationale Plan zum Schutz der Informationsinfrastrukturen“ (vgl. Bundesministerium des Innern 2005) von 2005 ist die nationale IT-Sicherheitsstrategie der Bundesrepublik Deutschland. Sie befaßt sich u. a. mit Maßnahmen zur Prävention, Reaktion und Nachhaltigkeit.

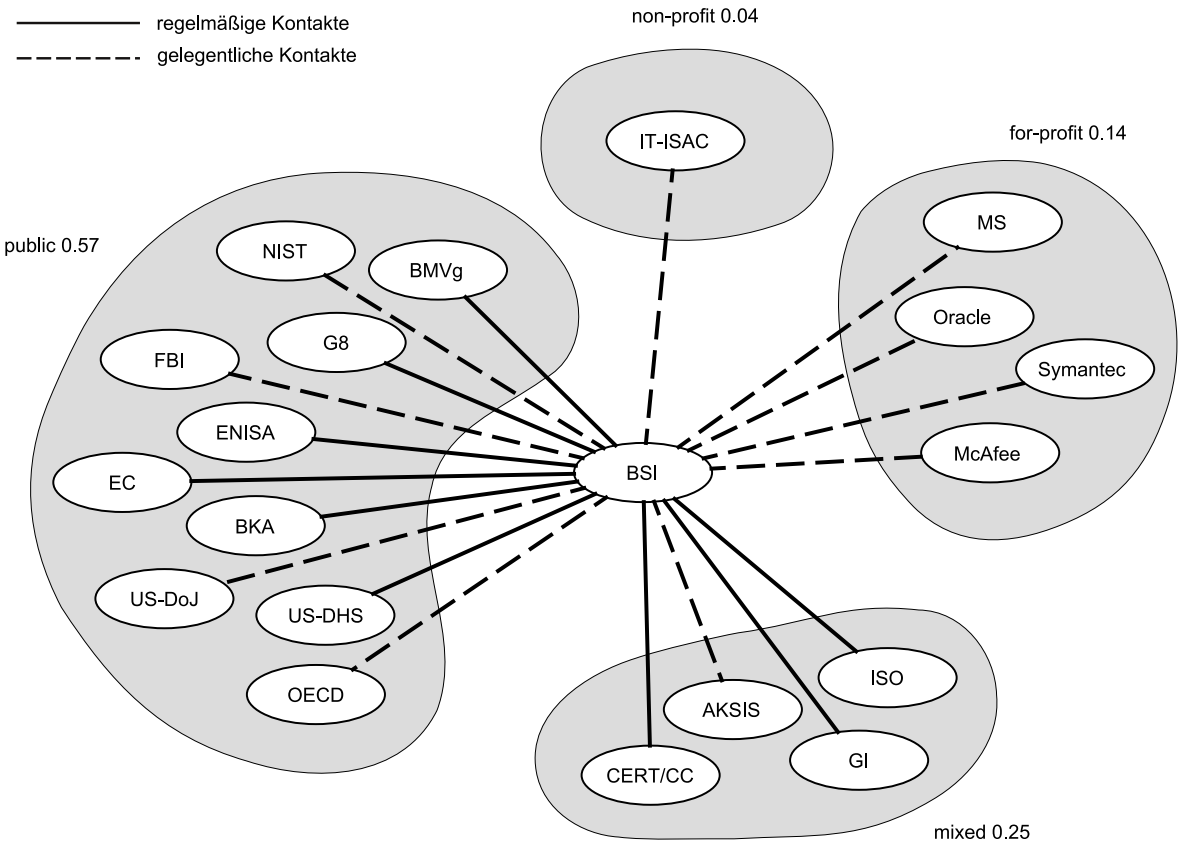


Abbildung 5.22: *Das egozentrierte Kooperationsnetzwerk des BSI*

und Zertifizierung der Sicherheitsarchitektur eines Informations- und Kommunikationssystems vorgenommen werden. Auch schult das BSI Multiplikatoren und Fachpersonal aus Wirtschaft und öffentlicher Verwaltung.

Da das BSI von den neun anderen Interviewpartnern weder als einer der fünf wichtigsten Kooperationspartner, noch als eine der fünf wichtigsten Organisation überhaupt eingestuft wurde, liegen keine expliziten Ressourcenzuordnungen vor. Aufgrund des oben beschriebenen Profils der Organisation verfügt das BSI jedoch vermutlich vor allem über Expertenwissen und technische Ausstattung sowie Einfluß auf politische Rahmenentscheidungen.

Das BSI beteiligt sich u. a. an dem *Arbeitskreis Schutz von Infrastrukturen* (AKSIS), federführend organisiert von der IABG. Zu diesem Arbeitskreis gehören Akteure aus der öffentlichen Verwaltung, der privaten Wirtschaft sowie Wissenschaft und Forschung. Vorrangiges Ziel ist der Austausch von Informationen über sicherheitsrelevante Bedro-

hungen und Maßnahmen zum Schutz kritischer Infrastrukturen in Deutschland. Ferner sollen Führungsebenen privater und öffentlicher Organisationen hinsichtlich dieser Sicherheit sensibilisiert werden. Aus dem Arbeitskreis heraus entstand u. a. die Planübung „CYTEX“[199]. Szenario dieser Übung waren Angriffe auf die Informations- und Kommunikationssysteme kritischer Infrastrukturen. Identifiziert werden sollten mögliche Schwächen öffentlicher sowie privater Akteure in der Abwehr.

Die Behörde unterhält nach eigenen Angaben darüber hinaus Kooperationsbeziehungen zu einer Reihe anderer Organisationen (vgl. Abbildung 5.22). Annähernd die Hälfte (≈ 0.47) dieser Kontakte sind regelmäßig. Unter diesen regelmäßigen Kooperationsbeziehungen sind vor allem öffentliche Akteure wie BMVg, US-DHS, EC und ENISA. Dies unterstreicht den Charakter des BSI als zentralem Dienstleister innerhalb des öffentlichen Sektors. So entfällt denn auch ein überproportionaler Anteil (≈ 0.57 bei gesamt ≈ 0.30) der Kooperationskontakte auf öffentliche Organisationen. Unter den Kontakten überproportional vertreten sind ferner gemischte Organisationen mit einem relativen Anteil von ≈ 0.25 (gesamt ≈ 0.14).

Im Kooperationsnetzwerk der untersuchten Fallstudien (vgl. Abbildung 5.20) befindet sich das BSI an der Peripherie. Dem entspricht eine leicht unterdurchschnittliche Reputation der Organisation (vgl. Abbildung 5.19). Zwar unterhält sie unbestätigte regelmäßige Kontakte zu den zentralen Akteuren CERT/CC und US-DHS sowie gelegentliche Beziehungen zu dem ebenfalls zentralen Akteur MS, agiert jedoch zugleich primär auf nationaler Ebene und rückt daher in einem internationalen Kontext hinsichtlich der Produktion von Sicherheit in elektronischen Netzen zwangsläufig an den Rand, obwohl genau diese Aufgabe im nationalen Rahmen unzweifelhaft zu den Kernkompetenzen des BSI gehört.

5.3.2.3 CSIS

Das *Center for Strategic and International Studies* (CSIS) ist eine unabhängige, akademisch ausgerichtete Denkfabrik mit Sitz in Washington, DC. Das CSIS finanziert sich aus öffentlichen Zuschüssen sowie privaten Spenden. Es wurde im Jahre 1962 im Kontext des sich verschärfenden kalten Krieges an der Georgetown University gegründet und ist seit 1987 von dieser unabhängig. Beschäftigt werden etwa 200 Mitarbeiter,

199 Zur Planübung „CYber Terror EXercise“ vgl. <`http://www.heise.de/tp/r4/artikel/11/11746/1.html`>.

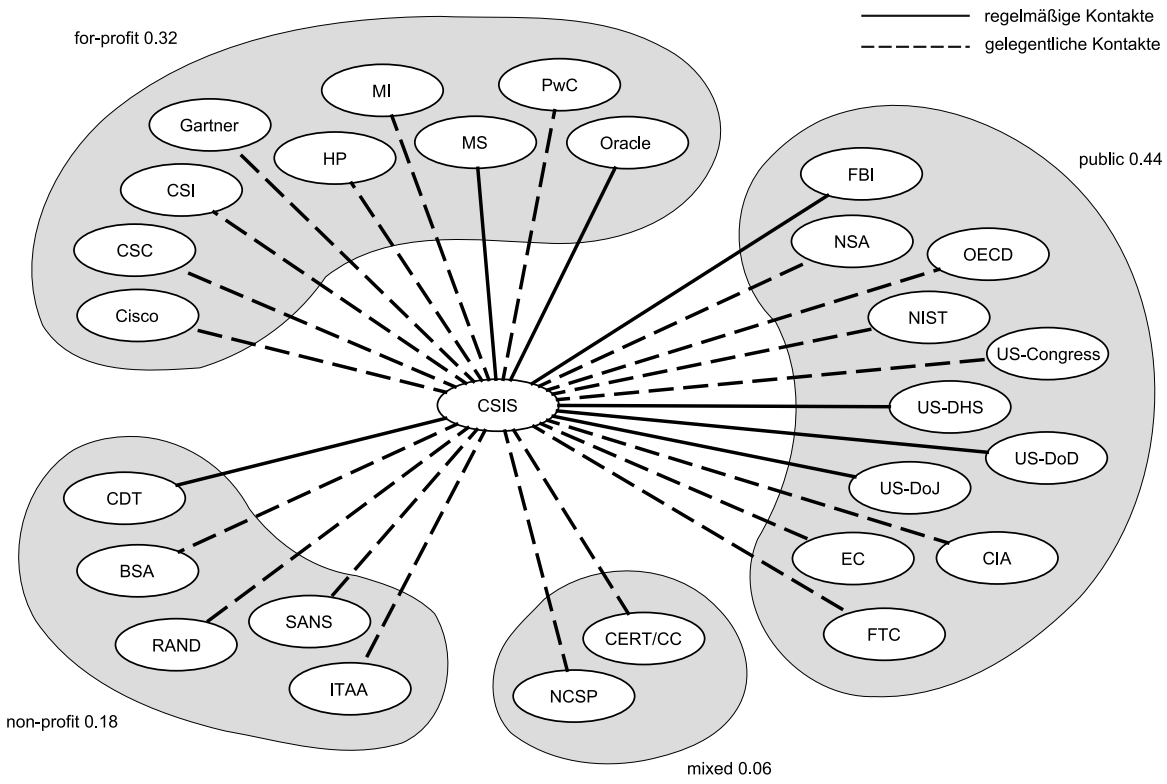


ABBILDUNG 5.23: *Das egozentrierte Kooperationsnetzwerk des CSIS*

von denen ein Großteil aus dem öffentlichen Sektor stammt. Im Mittelpunkt des Forschungsinteresses stehen traditionell Themen der Außen- und Sicherheitspolitik. Seit dem Ende der Blockkonfrontation richtet sich der Fokus vermehrt auf asymmetrische Bedrohungen sowie den Heimatschutz. Vor diesem Hintergrund gewinnt auch die Sicherheit kritischer Informationsinfrastrukturen zunehmend an Bedeutung.

Im Rahmen des *Technology and Public Policy Program* beschäftigt sich das CSIS u. a. mit sicherheitsrelevanten Vorfällen in elektronischen Netzen und entwickelt politische Strategien zu deren Vermeidung (vgl. hierzu Lewis 2003a). Wie bei einer Denkfabrik nicht anders zu erwarten, umfaßt dies auch die Beratung öffentlicher Entscheidungsträger, insbesondere der amerikanischen Bundesregierung. Im Mittelpunkt steht hierbei die Identifikation aktueller Probleme sowie die Ausarbeitung politischer Lösungsansätze. Ferner versteht sich das CSIS als Plattform einer öffentlichen Diskussion sicherheitsrelevanter Themen und trägt so wesentlich zum Agenda Setting bei.

Da das CSIS von den neun anderen Interviewpartnern weder als einer der fünf

wichtigsten Kooperationspartner, noch als eine der fünf wichtigsten Organisation überhaupt eingestuft wurde, liegen keine expliziten Ressourcenzuordnungen vor. Weil sich die Organisation jedoch schwerpunktmäßig auf die Beratung der amerikanischen Bundesregierung konzentriert, kann angenommen werden, daß das CSIS vor allem Einfluß auf politische Rahmenentscheidungen ausübt. Aus Abbildung 5.23 läßt sich ferner entnehmen, daß das CSIS nach eigenen Angaben über eine verhältnismäßig breite Palette von Kontakten zu anderen Akteuren verfügt. Dies könnte als Hinweis auf Sozialkapital interpretiert werden.

Etwa ein Viertel (≈ 0.26) dieser Kontakte finden regelmäßig statt. Diese dauerhaften Kontakte konzentrieren sich zugleich schwerpunktmäßig auf den öffentlichen Sektor, hier in Sonderheit auf die Ministerien der Justiz, des Heimatschutzes sowie der Verteidigung. Unter den gewinnorientierten privaten Akteuren bestehen regelmäßige Kooperationskontakte vor allem zu großen Unternehmen der IT-Branche wie bspw. MS und Oracle. Auch im Vergleich zur relativen Verteilung der *Status* in der Gesamtmenge aller untersuchten Organisationen (vgl. Abbildung 5.3) sind unter den Kontakten des CSIS die öffentlichen Organisationen mit einem relativen Anteil von ≈ 0.44 (gesamt ≈ 0.30) sowie die gewinnorientierten privaten Akteure mit einem relativen Anteil von ≈ 0.32 (gesamt ≈ 0.24) leicht überrepräsentiert.

Im Kooperationsnetzwerk der untersuchten Fallstudien (vgl. Abbildung 5.20) ist das CSIS am äußeren Rand verortet. Diese Positionierung reflektiert den ebenfalls geringen Reputationswert der Organisation (vgl. Abbildung 5.19), die nur über unbestätigte regelmäßige Kontakte zu den beiden zentralen Akteuren US-DHS und MS sowie über gelegentliche Kontakte zu dem ebenfalls zentralen CERT/CC verfügt. Insgesamt handelt es sich beim CSIS somit um einen im Prozeß der Produktion von Sicherheit in elektronischen Netzen eher unbedeutenden Akteur.

5.3.2.4 CERT/CC

Sitz des *Computer Emergency Response Team/Coordination Center* (CERT/CC) ist Pittsburgh, PA. Hier wurde 1988 als Reaktion auf den sog. Morris-Wurm[200] am Software Engineering Institute (SEI) der Carnegie Mellon University das weltweit erste CERT gegründet, dessen Aufgabe darin bestand, als zentrale Task Force zukünftig ähnliche Sicherheitsvorfälle frühzeitig zu erkennen und rechtzeitig entsprechende Ge-

200 Vgl. hierzu weiter oben Fußnote 86.

genmaßnahmen einzuleiten. Finanziert wurde das Projekt durch die Defense Advanced Research Projects Agency (DARPA), eben jene Organisation, die bereits Jahre zuvor eine tragende Rolle bei der Finanzierung zentraler Internet-Technologien gespielt hatte. Heute betreibt das SEI im Rahmen seines *Networked Systems Survivability Program* ein Coordination Center (CC) mit etwa 40 Mitarbeitern, das als zentrale Anlaufstelle und Koordinationsinstanz einer Vielzahl weltweit verteilter Teams dient. Statt CERT nennen sich diese teilweise auch „Computer Security Incident Response Team“ (CSIRT), da diese Bezeichnung auf ein breiter angelegtes Konzept verweist, das neben reaktiven auch und vor allem präventive Maßnahmen umfaßt.

Obwohl die Carnegie Mellon University selbst eine private Universität ist, wird das SEI und damit auch das CERT/CC, größtenteils durch öffentliche Akteure, vor allem das US-DoD sowie das US-DHS, finanziert und als nicht-akademisches Institut unter besonderen Sicherheitsauflagen betrieben. Zu den Hauptaufgaben des CERT/CC gehören: (1) die Koordination von Reaktionen auf Sicherheitsvorfälle in elektronischen Netzen, (2) die Bereitstellung technischer Hinweise, (3) die Identifikation neuer Angriffsvektoren, (4) die Bewertung potentieller Schwachstellen, (5) die Entwicklung neuer Sicherheitslösungen.

Neben dem CERT/CC gibt es gegenwärtig eine Vielzahl weiterer Computer-Sicherheits-Teams in fast allen Industriestaaten der Welt. Diese werden sowohl von öffentlichen als auch privaten Akteuren unterhalten. Oft sind sie nach dem Vorbild des CERT/CC aufgebaut und koordinieren sich aus historischen Gründen über dieses, sind aber ansonsten gleichwohl von diesem unabhängig. Als öffentliche Akteure betreiben in Deutschland bspw. das BSI das CERT Bund, welches die Bundesbehörden betreut, sowie die Universität Hamburg das DFN CERT, welches für das Netzwerk nationaler Forschungseinrichtungen zuständig ist. Als private Akteure verfügen etwa die Telekom und Siemens jeweils über ein eigenes CERT. Eine internationale Dachorganisation für Computer-Sicherheits-Teams ist das 1990 gegründete *Forum of Incident Response and Security Teams* (FIRST). Viele aber nicht alle Sicherheits-Teams sind Mitglied dieses Forums. Das CERT/CC selbst zählt zu den Gründungsmitgliedern. Aus Gründen der Geheimhaltung wurden im Interview von Seiten des CERT/CC darüber hinaus keine Angaben zu Kooperationspartnern gemacht, so daß hier keine Aussagen zum egozentrierten Netzwerk der Organisation getroffen werden können.

Aus Abbildung 5.15 geht hervor, daß dem CERT/CC vor allem die Ressourcen Expertenwissen und Sozialkapital sowie ferner Publizität attribuiert werden. Diese Res-

sourcen verleihen dem CERT/CC eine vergleichsweise hohe Problemlösungskapazität (vgl. Abbildung 5.17). Diese wird noch deutlich übertroffen durch die hohe Reputation der Organisation (vgl. Abbildung 5.19). Hiermit korrespondiert auch eine zentrale Stellung des CERT/CC im Kooperationsnetzwerk der untersuchten Fallstudien (vgl. Abbildung 5.20). An ähnlich zentraler Position befindet sich sonst nur noch MS. Hier wird deutlich, daß das CERT/CC einer der führenden Akteure im Prozeß der Produktion von Sicherheit in elektronischen Netzen ist. Diese historisch gewachsene Führungsrolle im öffentlichen Auftrag stützt sich auf die einzigartige Kombination aus umfangreichem Expertenwissen und hohem Sozialkapital, die das CERT/CC weltweit in den Fokus von Sicherheitsexperten rücken läßt und ihm somit zugleich ein hohes Maß an Publizität verschafft.

5.3.2.5 EFF

Bei der *Electronic Frontier Foundation* (EFF) handelt es sich um eine spendenfinanzierte Bürgerrechtsinitiative mit Sitz in San Francisco, CA, die ihre Hauptaufgabe im Schutz der Informations- und Meinungsfreiheit sowie der Privatsphäre im digitalen Zeitalter sieht. Mittel zur Erreichung dieses Zieles sind hauptsächlich einschlägige Klagen sowie die Anstrengung gerichtlicher Musterprozesse. Die Organisation beschäftigt ca. 25 Mitarbeiter, unter ihnen Rechtsanwälte, Politik-Analysten und technische Experten. Die EFF konzentriert ihre Tätigkeit insbesondere auf die USA, eröffnete jedoch 2007 auch ein europäisches Büro in Brüssel.

Ursächlich für die Gründung der EFF im Jahre 1990 war der sog. Steve-Jackson-Games-Fall. Der in Texas ansässige Spieleverlag Steve Jackson Games war zuvor vom United States Secret Service im Rahmen einer bundesweiten Razzia gegen Computerstraftaten durchsucht worden, die unter dem Namen „Operation Sundevil“ Bekanntheit erlangte. Gesucht wurde nach einer Textdatei, die von einem Rechner des Telekommunikationsunternehmens BellSouth illegal kopiert worden war und die vertrauliche Informationen über das telefonische Notrufsystem der USA enthielt. Vor diesem Hintergrund entschlossen sich Mitchell Kapor, der Gründer von Lotus Development, John Gilmore, ein ehemaliger Mitarbeiter von Sun Microsystems sowie John P. Barlow zur Gründung der EFF. Zusammen mit Steve Jackson Games verklagten sie erfolgreich den United States Secret Service wegen Verstoßes gegen den Electronic Communications Privacy Act. Seitdem hat sich die EFF in einer Reihe ähnlich gelagerter Fälle engagiert.

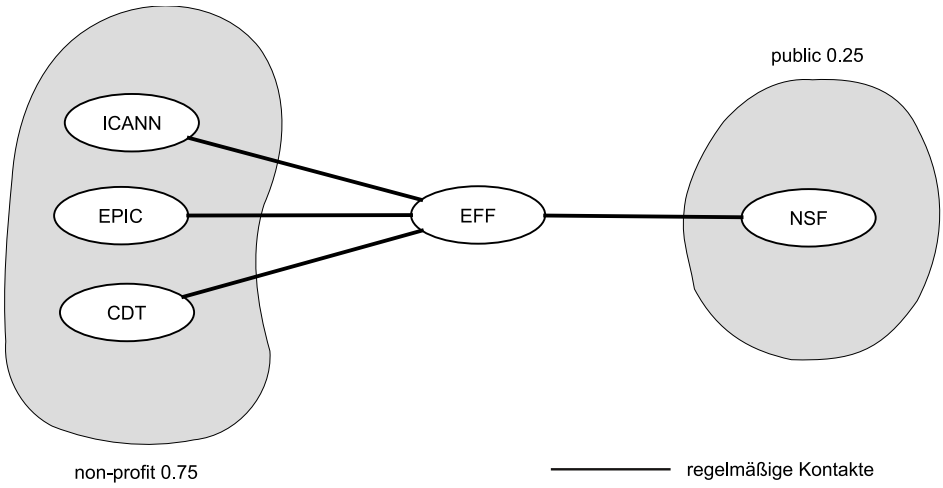


ABBILDUNG 5.24: *Das egozentrierte Kooperationsnetzwerk der EFF*

In seiner 1996 im Internet publizierten „Declaration of the Independence of Cyberspace“[201] postuliert Barlow, daß nationalstaatliche Regierungen in neuen elektronischen Handlungsräumen keine Souveränität besäßen. Traditionelle Rechtskonzepte des Eigentums, der Meinungsäußerung oder der Identität seien daher nicht in diese virtuelle Welt, die eine reine „Zivilisation des Geistes“ sei, übertragbar. Entsprechend interpretiert die EFF diese Handlungsräume als neue kulturelle Qualität, die neue Formen der Regulation erfordere, welche aus dem Kreis der Nutzer dieser Räume selbst konstituiert werden müßten.

Die EFF gehört zu den Gründungsmitgliedern der *Global Internet Liberty Campaign* (GILC), einem internationalen Dachverband von Bürger- und Menschenrechtsorganisationen. Abbildung 5.24 zeigt, daß die EFF darüber hinaus nach eigenen Angaben nur über sehr wenige, dafür aber ausschließlich regelmäßige Kooperationskontakte zu anderen Akteuren verfügt. Auffällig viele Kontakte bestehen zu nicht-gewinnorientierten privaten Organisationen mit einer ähnlichen Zielsetzung. Enge Beziehungen werden u. a. zu EPIC unterhalten. Im Kooperationsnetzwerk der untersuchten Fallstudien (vgl. Abbildung 5.20) findet sich die EFF dementsprechend am äußersten Rand wieder. Als einzige Organisation unterhält sie zu keiner der drei zentralen Akteure CERT/CC, MS und US-DHS Verbindungen.

201 Vgl. <`http://homes.eff.org/~barlow/Declaration-Final.html`> zum vollständigen Wortlaut.

An zentralen Ressourcen werden der Organisation Expertenwissen und Einfluß auf Standardisierungsprozesse zugeschrieben (vgl. Abbildung 5.15). Allerdings ist die Problemlösungskapazität der EFF insgesamt nicht sehr hoch (vgl. Abbildung 5.17). Abbildung 5.19 zeigt ferner, daß sich auch die Reputation der Organisation auf einem unterdurchschnittlichen Niveau bewegt. Gleichwohl nimmt sie eine wichtige Funktion im Prozeß der Produktion von Sicherheit in elektronischen Netzen wahr. Auf juristischem Wege wahrt sie als Korrektiv grundlegende Interessen individueller Nutzer vor weitgehenden staatlichen Eingriffen und stärkt damit deren Vertrauen in die Informationsinfrastruktur.

5.3.2.6 EPIC

Eine weitere spendenfinanzierte Bürgerrechtsinitiative ist das 1994 gegründete *Electronic Privacy Information Center* (EPIC), das sich selbst als „public interest research center“[202] bezeichnet. EPIC unterhält ein Büro mit etwa 10 Mitarbeitern in Washington, DC und ist hauptsächlich in Nordamerika, teilweise aber auch in Europa, tätig. Erklärtes Ziel der Organisation ist es, die öffentliche Aufmerksamkeit insbesondere auf solche Gefährdungen der Privatsphäre sowie der Informationsfreiheit einzelner Bürger zu lenken, welche sich aus der Entwicklung, Verbreitung und Anwendung neuer elektronischer Technologien ergeben oder mit diesen in unmittelbarem Zusammenhang stehen. Das EPIC überwacht und analysiert daher laufend einschlägige Aktivitäten öffentlicher und privater Akteure und bewertet diese hinsichtlich potentieller Einschränkungen für die oben genannten Bürgerrechte. Die Ergebnisse werden regelmäßig in verschiedenen Publikationen und Reporten sowie im Rahmen eines elektronischen Rundbriefes, „EPIC Alert“ genannt, thematisiert. Nicht selten werden Vertreter der Organisation darüber hinaus in Massenmedien als Experten zitiert, so daß das EPIC einen gewissen Einfluß im Rahmen eines öffentlichen Agenda-Settings entfalten kann.

Zum Schutz der Privatsphäre vor staatlicher Überwachung wirbt die Organisation für den Einsatz starker Kryptographie-Technologien. In diesem Zusammenhang kritisiert das EPIC vor allem das US-DoD sowie die NSA bezüglich deren Bestrebungen die Möglichkeiten und damit zugleich die Wirksamkeit privat genutzter Kryptographie-Verfahren gesetzlich einzuschränken. Aus Sicht der Organisation wird der Diskurs über den Schutz der kritischen Informationsinfrastruktur hierbei einseitig zu Lasten der In-

202 Vgl. <`http://epic.org`>.

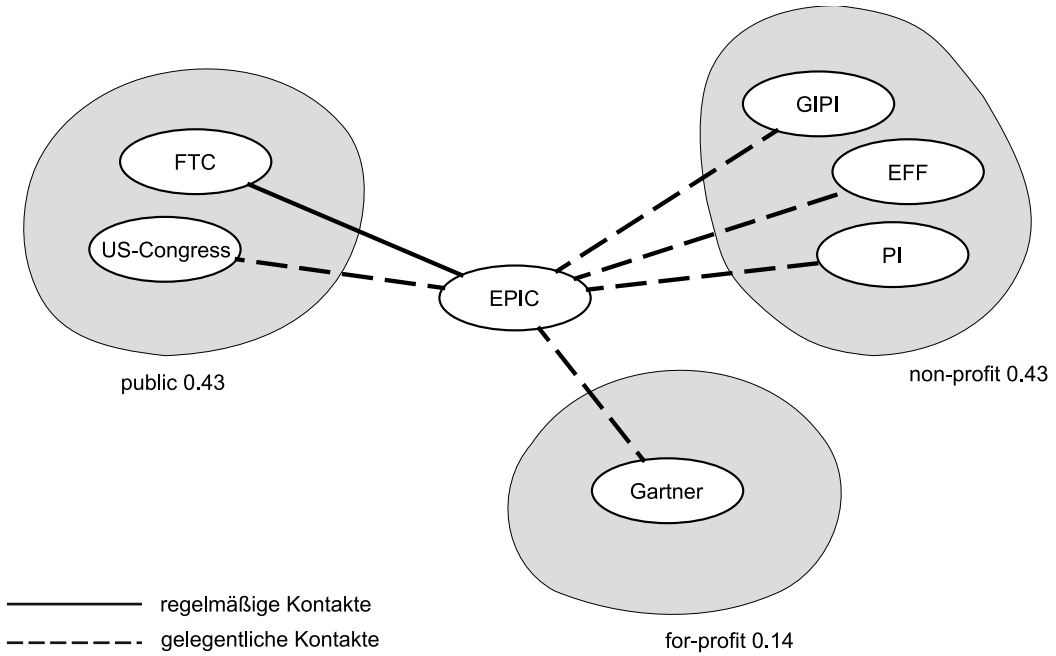


Abbildung 5.25: *Das egozentrierte Kooperationsnetzwerk des EPIC*

formationsfreiheit und Privatsphäre einzelner Nutzer geführt.

Wie aus Abbildung 5.25 hervorgeht kooperiert das EPIC nach eigenen Angaben nur mit sehr wenigen Akteuren. Regelmäßige Kontakte bestehen danach sogar nur zur FTC. Die meisten Kooperationspartner sind ebenfalls nicht-gewinnorientierte private Organisationen sowie ausgewählte öffentliche Akteure. Im Kooperationsnetzwerk der untersuchten Fallstudien (vgl. Abbildung 5.20) bildet die Organisation zusammen mit der EFF eine eher periphere Clique. Beide Akteure verstehen sich in erster Linie als Korrektiv weitgehender Eingriffe mächtiger kollektiver Akteure in die Rechte Einzelner und übernehmen daher schon per definitionem die Außenseiterrolle eines „David gegen Goliath“. Im Vergleich zur EFF erreicht das EPIC allerdings eine höhere Eigenvektor-Zentralität und liegt damit immerhin in etwa auf einer Höhe mit der ENISA sowie Symantec.

Als zentrale Ressourcen werden der Organisation Publizität und Einfluß auf politische Rahmenentscheidungen attestiert (vgl. Abbildung 5.15). Jedoch fällt die Problemlösungskapazität des EPIC sogar noch etwas geringer als jene der EFF aus (vgl. Abbildung 5.17), was vermutlich auch der geringen Größe der Organisation geschuldet ist. Hiermit korrespondiert eine ebenfalls unterdurchschnittliche Reputation (vgl.

Abbildung 5.19). Dennoch nimmt auch das EPIC eine zentrale Funktion im Prozeß der Produktion von Sicherheit in elektronischen Netzen wahr. Als unabhängiger und nicht-gewinnorientierte Akteur überwacht sie laufend technische und rechtliche Entwicklungen und informiert über Probleme des Datenschutzes, der Privatsphäre und der Informationsfreiheit in elektronischen Netzen. Sie trägt damit zur Transparenz informationstechnischer Systeme bei und erhöht somit ebenfalls das Vertrauen individueller Nutzer in diese Systeme.

5.3.2.7 ENISA

Die *European Network and Information Security Agency* (ENISA) ist eine 2004 gegründete Behörde der Europäischen Union mit Sitz in Heraklion auf der griechischen Insel Kreta. Sie ist für die Netz- und Informationssicherheit innerhalb der Europäischen Union zuständig.[203] Zu ihren Aufgaben gehört u. a. die Beratung der EC und anderer EU-Institutionen sowie der Mitgliedsstaaten, die Analyse potentieller Risiken und Bedrohungen sowie die Sensibilisierung privater und öffentlicher Akteure für Fragen der elektronischen Sicherheit. Im Verwaltungsrat der Organisation sitzen sowohl Delegierte der Mitgliedsstaaten und der EC als auch Interessenvertreter aus den Bereichen Wirtschaft, Wissenschaft und Gesellschaft (Permanent Stakeholder Group). Die Behörde umfaßt zur Zeit ca. 50 Mitarbeiter.

Aus Abbildung 5.15 geht hervor, daß der Organisation die Ressourcen Expertenwissen und finanzielle Mittel zugeschrieben werden. Zugleich wird der Behörde jedoch eine relativ geringe Problemlösungskapazität beigemessen (vgl. Abbildung 5.17). Ursächlich hierfür ist möglicherweise, daß die ENISA lediglich beratende Funktionen wahrnimmt. Allerdings befand sich die Behörde zum Zeitpunkt der Interviews noch im Aufbau, so daß Potential und Ressourcen der Organisation durch die Interviewpartner möglicherweise unterschätzt wurden. So könnte die Behörde künftig vermutlich auch verstärkten Einfluß auf die politische Entscheidungsfindung sowie Standardisierungsprozesse der EU-Mitgliedsstaaten gewinnen. Ein Blick in Tabelle 5.9 zeigt denn auch eine deutliche Abweichung von Problemlösungskapazität und Reputation.

Im Kooperationsnetzwerk der untersuchten Fallstudien (vgl. Abbildung 5.20) erreicht die Organisation eine eher geringe Zentralität und liegt damit in etwa auf einer Höhe mit dem EPIC sowie Symantec. Es existieren jeweils unbestätigte gelegentliche

203 Verordnung 460/2004 des Europäischen Parlamentes und des Rates vom 10. März 2004.

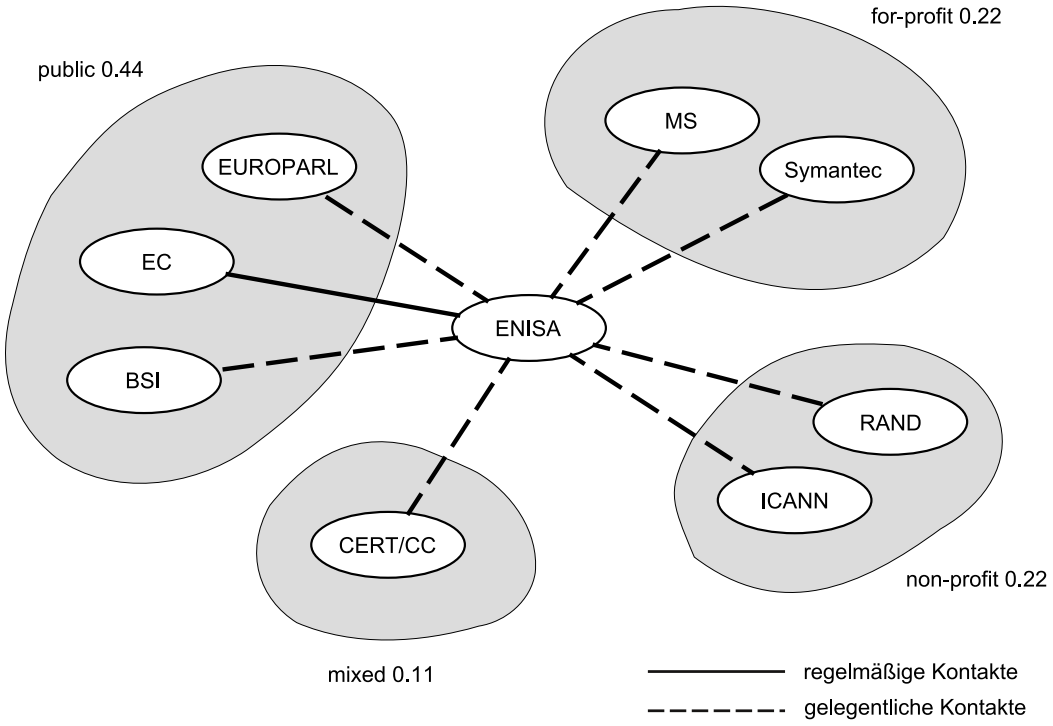


Abbildung 5.26: *Das egozentrierte Kooperationsnetzwerk der ENISA*

Kontakte zu den drei zentralen Akteuren MS, CERT/CC und US-DHS. Auch hier gilt es zu berücksichtigen, daß sich die Behörde zum Zeitpunkt der Interviews noch in der Aufbauphase befand und regelmäßige Beziehungen daher nicht zu erwarten waren.

Die Organisation kooperiert nicht nur mit der EC sowie dem EUROPARL, sondern auch mit den einschlägigen Fachministerien der EU-Mitgliedsstaaten sowie ggf. mit nachgeordneten nationalen Regulierungs-, Fach- und Polizeibehörden sowie öffentlichen CERTs. Im Mittelpunkt steht hierbei eine supranationale Koordination und Harmonisierung nationaler Bemühungen zum Schutz der Informationsinfrastruktur. Eine enge Kooperation besteht auch mit dem deutschen BSI, dessen vormaliger Präsident Udo Helmbrecht seit Oktober 2009 Direktor der ENISA ist.[204]

Abbildung 5.26 verdeutlicht, daß darüber hinaus ferner Kontakte zu außereuropäischen Akteuren bestehen. Die Kontakte insgesamt verteilen sich weitgehend gleichmäßig auf Akteure aller *Status*, was eine neutrale Mittlerfunktion der Organisation reflek-

204 Vgl. hierzu die Pressemitteilung vom 16. Oktober 2009 unter <`http://www.enisa.europa.eu`>.

tiert. Im Prozeß der Produktion von Sicherheit in elektronischen Netzen übernimmt die ENISA vor allem koordinative Aufgaben auf internationaler Ebene. Ferner stellt sie als supranationaler öffentlicher Akteur eine – von ökonomischen Eigeninteressen weitgehend freie – Fachexpertise bereit.

5.3.2.8 MS

Die Firma *Microsoft* (MS) ist ein multinational agierender Hersteller von Software für Personal- und Heimcomputer mit Hauptsitz in Redmond, WA. Das Unternehmen wurde 1975 gegründet und beschäftigt weltweit ca. 93.000 Mitarbeiter. In den 1990er Jahren konnte sich MS mit seinem Betriebssystem *Windows* sowie im Bereich der Büro-Anwendungen mit dem Programmpaket *Microsoft Office* als globaler Marktführer etablieren. Schätzungsweise laufen über 90 Prozent aller Personal- und Heimcomputer unter einem Betriebssystem von MS. Eine solche Software-Monokultur birgt eine nicht unerhebliche Gefährdung elektronischer Netzwerke, da sie die Diffusion schädlicher Programme, welche sich gezielt Schwachstellen dieser Software zu Nutze machen, in besonderer Weise begünstigt. Das zeitnahe Schließen erkannter Schwachstellen ist daher von kritischer Bedeutung. Hierzu stellt MS in regelmäßigen Abständen im Internet Aktualisierungen und Korrekturen für seine Programme bereit, die automatisch oder manuell heruntergeladen und installiert werden können. Ferner veröffentlicht MS zweimal jährlich einen *Security Intelligence Report*, der einen Überblick über die aktuelle Sicherheitslage enthält (vgl. Microsoft Corporation 2009).

MS wurden in den Interviews vor allem die Ressourcen Expertenwissen und Einfluß auf Standardisierungsprozesse zugeschrieben (vgl. Abbildung 5.15). Letzteres ist faktisch eine Folge der hohen Marktdurchdringung des hauseigenen Betriebssystems. Ferner verfügt das Unternehmen offenbar schon allein aufgrund seiner Größe und Marktposition über bedeutende finanzielle Ressourcen sowie nachhaltigen Einfluß auf politische Rahmenentscheidungen. Abbildung 5.17 zufolge hat MS damit nach dem US-DHS die mit Abstand größte Problemlösungskapazität. Dem entspricht eine ebenfalls sehr hohe Reputation, wie aus Abbildung 5.19 hervorgeht.

Auch im Kooperationsnetzwerk der untersuchten Fallstudien (vgl. Abbildung 5.20) findet sich MS zusammen mit dem CERT/CC sowie dem US-DHS an exponierter Stelle. Diese zentrale Positionierung korrespondiert in hohem Maße mit der herausgehobenen Problemlösungskapazität dieser drei Akteure. MS verfügt u. a. über bestätigte Koope-

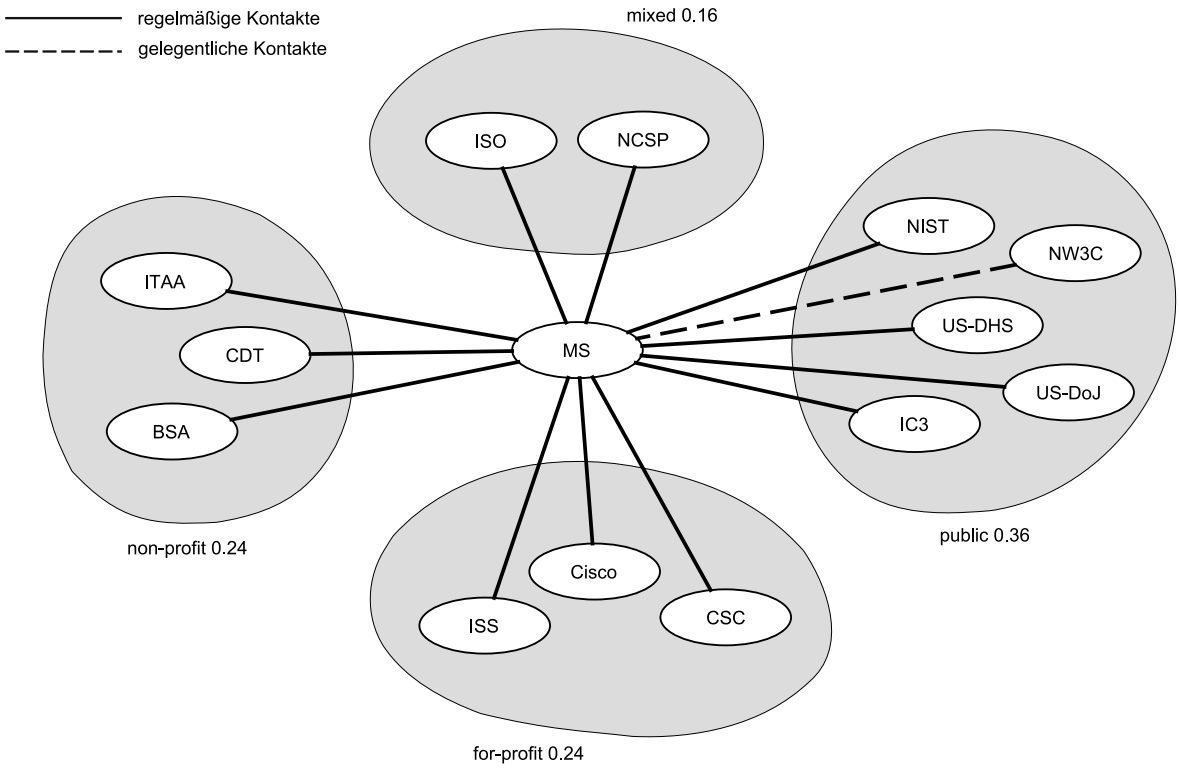


Abbildung 5.27: *Das egozentrierte Kooperationsnetzwerk von MS*

rationsbeziehungen zu den Akteuren US-DHS und BSA und ist zugleich Empfänger einer Vielzahl eingehender Wahlen.

Abbildung 5.27 verdeutlicht, daß sich das Unternehmen nach eigenen Angaben auf relativ wenige, dafür aber nahezu ausschließlich (≈ 0.92) regelmäßige Kooperationskontakte konzentriert. Im Vergleich zur relativen Häufigkeit der *Status* in der Gesamtmenge aller untersuchten Organisationen (vgl. Abbildung 5.3) zeigt sich unter diesen Kontakten ferner ein leichtes Übergewicht öffentlicher Akteure (≈ 0.36 bei gesamt ≈ 0.30). Unterrepräsentiert sind hingegen nicht-gewinnorientierte private Akteure mit einem Anteil von ≈ 0.24 (gesamt ≈ 0.32). Gemischte (≈ 0.16 bei gesamt ≈ 0.14) sowie gewinnorientierte private Akteure (≈ 0.24 bei gesamt ≈ 0.24) entsprechen jedoch den Erwartungen. Diese weitgehend ausgewogene Verteilung der Kooperationspartner unterstreicht noch einmal die zentrale Rolle des Unternehmens im Prozeß der Produktion von Sicherheit in elektronischen Netzen. MS fungiert offenbar als dauerhaft bevorzugter Ansprechpartner für Akteure aller *Status* und kann so sektorübergreifend eine stabili-

TABELLE 5.11: *Der Aufbau der MSRA*

Organization	*Focus*	*Purpose*
The Global Infrastructure Alliance for Internet Safety (GIAIS)	Internet service providers (ISPs)	Fosters cooperation between Microsoft and the world's leading ISPs to keep their customers safe on the Internet
The Microsoft Virus Initiative (MVI)	Security researchers, antivirus software vendors	Enables Microsoft to share key technical details of Microsoft technologies with partners, to facilitate development of well-integrated security solutions
Virus Information Alliance (VIA)	Antivirus software vendors	Provides AV partners with detailed technical information about significant viruses affecting Microsoft products and customers
Microdsoft Security Cooperation Program (SCP)	Public sector infrastructure, law enforcement, public safety, and education	Provides a framework for information exchange and collaboration between Microsoft and the public sector, primarily in the areas of response and outreach
Microsoft Security Support Alliance (MSSA)	Microsoft original equipment manufacturer (OEM) partners	Provides authoritative and timely information on newly discovered security threats to Microsoft's OEM partners, enabling them to better communicate security information to their customers
Security Alliance for Financial Institutions (SAFI)	Financial Institutions	Facilitate collaboration between Microsoft and financial institutions worldwide regarding the threats that such institutions face

Quelle: Microsoft Corporation (2009: 28)

sierende Koordinationsfunktion wahrnehmen.

Dies geschieht etwa im Rahmen der 2006 gegründeten *Microsoft Security Response Alliance* (MSRA).[205] Unter dem Dach dieser Initiative kooperiert MS mit unterschiedlichen Akteuren aus Wirtschaft und öffentlicher Verwaltung, um ein sicheres Umfeld in elektronischen Netzen zu schaffen. Die MSRA gliedert sich hierzu in verschiedene Unterorganisationen und Arbeitsgruppen und dient primär einem koordinativen Informationsaustausch (vgl. Tabelle 5.11).

205 Vgl. <`http://www.microsoft.com/security/msra/default.mspx`>.

5.3.2.9 Symantec

Symantec ist ein multinational agierender Software-Hersteller mit über 17.000 Mitarbeitern und Sitz in Cupertino, CA. Seit seiner Gründung im Jahr 1982 akquirierte Symantec eine umfangreiche Reihe weiterer Unternehmen, zu denen Norton Computing, Riptech, @stake und Veritas Software zählen. Die Kernkompetenz des Unternehmens verschob sich hierbei zunehmend in den Bereich des softwaretechnischen Schutzes elektronischer Informations- und Kommunikationssysteme sowohl im privaten als auch im professionellen Umfeld. Zur Produktpalette gehören verschiedene Antiviren-, Firewall-, Intrusion-Detection- sowie Verschlüsselungs-Lösungen. Für 2010 ist die Übernahme der Sparte Sicherheitsdienstleistungen des Unternehmens VeriSign avisiert. Hierdurch erwirbt Symantec u. a. Kompetenzen im Bereich des Betriebes einer Public Key Infrastructure (PKI) sowie bei Verfahren zur Authentifizierung. Nach eigenen Angaben verfügt das Unternehmen ferner über eines der weltweit größten Sensor-Netzwerke zur Früherkennung neuer Bedrohungen im Internet sowie eine der umfangreichsten Datenbanken zu elektronischen Schadprogrammen.

Aus Abbildung 5.15 läßt sich erkennen, daß Symantec vor allem die Ressourcen Expertenwissen und Sozialkapital attestiert werden. Die am relativen Ressourcenanteil gemessene Problemlösungskapazität des Unternehmens bewegt sich dabei insgesamt im Mittelfeld der untersuchten Akteure (vgl. Abbildung 5.17) und liegt in etwa gleich auf mit der NSA und dem US-DoJ. Mit der NSA teilt sich Symantec ebenfalls eine leicht überdurchschnittliche Reputation, während das US-DoJ hier auf einen Spitzenwert kommt (vgl. Abbildung 5.19).

Das hohe Expertenwissen des Unternehmens ist vermutlich das Ergebnis einer fortgesetzten Strategie der horizontalen Integration, die mit einer deutlichen Profilierung des Unternehmens im Bereich der Sicherung elektronischer Informations- und Kommunikationssysteme einhergeht. Vergleicht man Abbildung 5.28, so wird darüber hinaus deutlich, daß Symantec nach eigenen Angaben über eine außerordentliche Vielzahl an Kontakten verfügt, welche offenbar das dem Unternehmen auch von Dritten zugeschriebene Sozialkapital widerspiegeln. Diese Kontakte beruhen zu vier Fünfteln auf regelmäßiger Kooperation.

Im Vergleich zur relativen Häufigkeit der *Status* in der Gesamtmenge aller untersuchten Organisationen (vgl. Abbildung 5.3) zeigt sich, daß unter den Kontakten des Unternehmens vor allem öffentliche Akteure mit einem relativen Anteil von ≈ 0.41

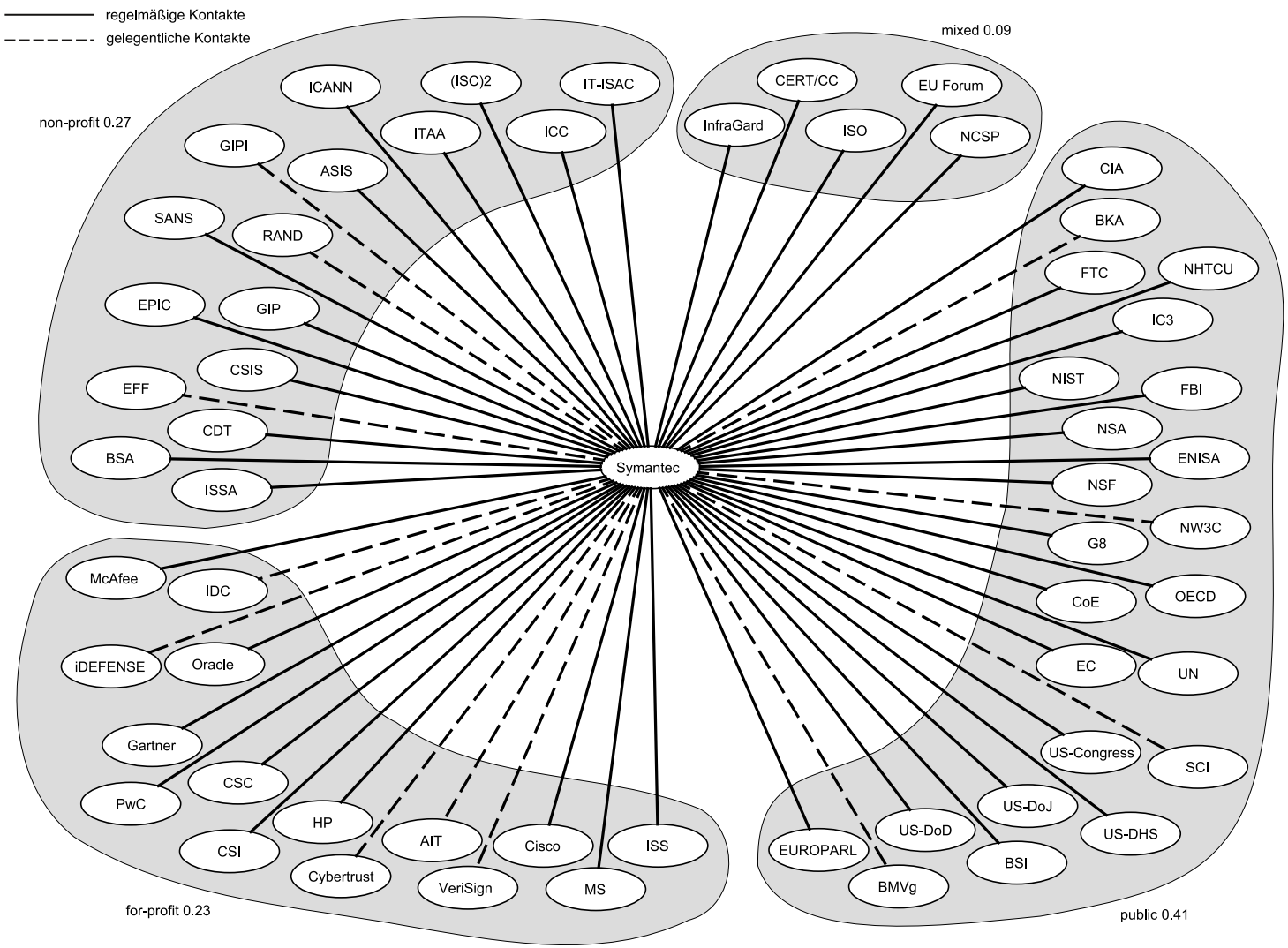


Abbildung 5.28: *Das egozentrierte Kooperationsnetzwerk von Symantec*

(gesamt ≈ 0.30) deutlich überproportional vertreten sind. Gemischte Akteure sind mit einem Anteil von ≈ 0.09 (gesamt ≈ 0.14) hingegen leicht unterrepräsentiert. Gleiches gilt für nicht-gewinnorientierte private Akteure mit einem Anteil von ≈ 0.27 (gesamt ≈ 0.32). Der Anteil der gewinnorientierten privaten Akteure (≈ 0.23 bei gesamt ≈ 0.24) entspricht den Erwartungen.

Trotz des hohen Sozialkapitals ist die Eigenvektor-Zentralität des Unternehmens im Kooperationsnetzwerk der untersuchten Fallstudien jedoch verhältnismäßig gering (vgl. Abbildung 5.20). Symantec bewegt sich hier in etwa auf einer Höhe mit der ENISA und dem EPIC. Trotz seines hohen Sozialkapitals verfügt das Unternehmen damit über eine geringere Fähigkeit zur kooperativen Ressourcenmobilisation, als dies etwa bei den zentralen Akteuren MS, CERT/CC oder US-DHS der Fall ist. Die Gründe hierfür lassen sich nur vermuten. So könnte gerade das umfangreiche Expertenwissen Informationsasymmetrien hervorrufen, die in Verbindung mit dem – im wesentlichen auf dem Verkauf von Sicherheitstechnologien beruhenden – Kerngeschäft des Unternehmens Probleme des *Moral Hazard* aufwerfen und so zu einem Vertrauensverlust seitens dritter Akteure führen (vgl. hierzu Ding et al. 2005).

5.3.2.10 US-DHS

Das *US Department of Homeland Security* (US-DHS) wurde auf Grundlage des *Homeland Security Act*[206] als Ministerium für Heimatschutz der USA errichtet. Es nahm offiziell am 24. Januar 2003 die Arbeit auf. Seine Gründung war unmittelbare Folge der Terroranschläge vom 11. September 2001. Unter dem Dach des Ministeriums wurden über zwanzig bereits bestehende amerikanische Bundesbehörden zusammengefaßt, so etwa das *Critical Infrastructure Assurance Office* (CIAO) des Department of Commerce, das *National Infrastructure Protection Center* (NIPC; mit Ausnahme der Abteilung Computer Investigations and Operations) des FBI sowie das *Energy Assurance Office* (EAO) des Department of Energy.

Das US-DHS beschäftigt über 200.000 Mitarbeiter und untergliedert sich u. a. in eine Abteilung für *Information Analysis and Infrastructure Protection* (IAIP), geführt von einem Unterstaatssekretär. Innerhalb dieser ist wiederum eine Unterabteilung für Infrastrukturschutz aufgehängt, in welcher 2003 die *National Cyber Security Division* (NCSD) mit etwa 120 Mitarbeitern eingerichtet wurde. Hauptaufgaben der NCSD sind

206 Homeland Security Act of 2002, 6 U.S.C. §§ 101 ff.

gemäß der *National Strategy to Secure Cyberspace* (US Department of Homeland Security 2003): (1) die Errichtung eines einheitlichen nationalen Warn- und Reaktionssystems für Angriffe im Cyberspace, basierend auf einer umfassenden Vernetzung privater und öffentlicher Akteure; (2) das Zurückdrängen von Bedrohungen und Sicherheitslücken durch die Förderung von Sicherheitssoftware, die Identifikation neuer Sicherheitslücken und die Unterstützung der Strafverfolgungsbehörden mit neuen Instrumenten zur kriminaltechnischen Untersuchung und Verfolgung von Straftaten im Cyberspace; (3) eine Steigerung des allgemeinen Sicherheitsbewußtseins durch Ausbildungs- und Schulungsprogramme; (4) eine Stärkung des Reaktionsvermögens der Regierung hinsichtlich möglicher Bedrohungen, Sicherheitslücken und Angriffe in elektronischen Netzen; (5) die Schaffung eines Rahmens zum internationalen Informationsaustausch sowie zur internationalen Kooperation bei Sicherheitsvorfällen.

Zum Schutz der amerikanischen Informationsinfrastruktur auf nationaler Ebene unterhält die NCSD – im Rückgriff auf personelle und technische Ressourcen des CERT/CC – das US-CERT. Dieses ist als landesweite Partnerschaft zwischen dem US-DHS sowie Experten sowohl des öffentlichen als auch privaten Sektors konzipiert. Auf globaler Ebene engagiert sich die NCSD darüber hinaus – im Verbund und in Abstimmung mit dem US Department of State – in einer Reihe internationaler Organisationen, so etwa der OECD, den G8-Gipfeln, der APEC oder der OAS. Direkte bilaterale Kontakte bestehen u. a. zu Großbritannien, Kanada, Mexiko, Australien, Deutschland und Indien.

Als zentrale Ressourcen wurden dem US-DHS in den Interviews vor allem Sozialkapital und Einfluß auf politische Rahmenentscheidungen zugeschrieben (vgl. Abbildung 5.15). Ferner verfügt es über einen hohen Grad an Publizität sowie beachtliche finanzielle Mittel. Aufgrund dieser Ressourcen stellt sich das US-DHS hinsichtlich seiner Problemlösungskapazität unter den untersuchten Organisationen als mit Abstand stärkster Akteur dar (vgl. Abbildung 5.17).

Bei Betrachtung der Abbildung 5.29 zeigt sich, daß das US-DHS auch nach eigenen Angaben über eine Vielzahl an Kooperationskontakten und damit ein hohes Sozialkapital verfügt. Diese Kontakte haben zu einem überwiegenden Teil (≈ 0.64) gelegentlichen Charakter. Hier wird deutlich, daß das US-DHS bezüglich der Produktion von Sicherheit in elektronischen Netzen offenbar eine übergeordnete Koordinations- bzw. Steuerungsfunktion wahrnimmt. Es ist dabei in der Lage mit nahezu allen anderen Akteuren punktuell zu kooperieren und so von Fall zu Fall neue Ordnungsmuster zu etablieren.

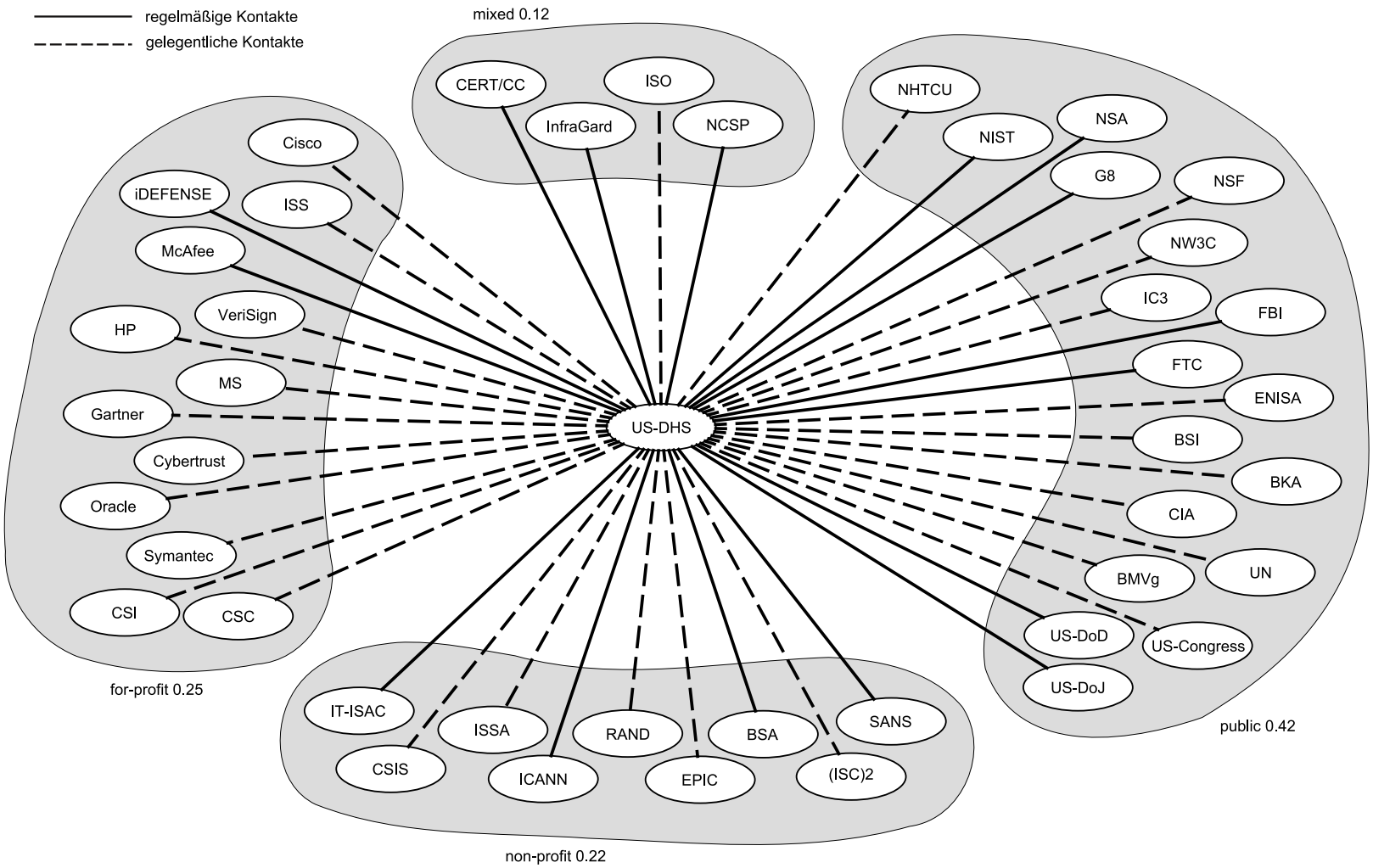


Abbildung 5.29: *Das egozentrierte Kooperationsnetzwerk des US-DHS*

Im Vergleich zur relativen Häufigkeit der *Status* in der Gesamtmenge aller untersuchten Organisationen (vgl. Abbildung 5.3) zeigt sich unter diesen Kontakten ein deutliches Übergewicht öffentlicher Akteure (≈ 0.42 bei gesamt ≈ 0.30). Nicht-gewinnorientierte private Akteure sind mit einem relativen Anteil von ≈ 0.22 (gesamt ≈ 0.32) im Gegensatz hierzu deutlich unterrepräsentiert. Die Kontakte zu gemischten (≈ 0.12 bei gesamt ≈ 0.14) und gewinnorientierten privaten Akteuren (≈ 0.25 bei gesamt ≈ 0.24) fallen erwartungsgemäß aus.

Die dominierende Rolle des US-DHS wird auch im Kooperationsnetzwerk der untersuchten Fallstudien (Abbildung 5.20) ersichtlich. Es verfügt über bestätigte Kooperationsbeziehungen zu dem ebenfalls zentralen Akteur MS sowie zur BSA, dem CSIS, dem BSI und Symantec. Zusammen mit dem CERT/CC sowie MS bildet das US-DHS den Nucleus des Netzwerkes. Aufgrund des hohen Anteils gelegentlicher Beziehungen erreicht es hierbei allerdings eine nicht ganz so hohe Eigenvektor-Zentralität wie die beiden anderen Akteure.

6 Konklusion

Abbildung 6.1 faßt den Prozeß der kybernetischen Regelung der Produktion und Distribution elektronischer Sicherheit innerhalb des komplexen sozio-technischen Systems einer globalen Informationsgesellschaft schematisch zusammen. In dieser Gesellschaft spielt die Ressource Wissen im Allgemeinen, sowie Information als handlungsrelevantes Wissen in Sonderheit, im Rahmen der Wertschöpfung eine fundamentale Rolle. Vernetzte elektronische Informations- und Kommunikationssysteme, die der Verarbeitung, Speicherung, Übertragung und Verteilung von Informationen dienen, bilden folglich ein kritisches, infrastrukturelles Subsystem dieser Gesellschaften. Sie spannen einen neuen virtuellen Handlungsraum auf, in welchen sich mehr und mehr (Trans-)Aktionen verlagern. Diese Systeme haben oftmals großtechnischen Charakter, d. h. sie verbinden eine Vielzahl technischer und sozialer Komponenten in einer komplexen Architektur wechselseitiger Interdependenzen. Dieser Umstand bedingt eine hohe Störanfälligkeit und damit zugleich Verwundbarkeit solcher Systeme. Ihre funktionelle Beinträchtigung aber kann direkt oder indirekt zu kaskadierenden oder eskalierenden Effekten führen und so die Wohlfahrt des gesamtgesellschaftlichen Suprasystems gefährden.

Eine gefährliche Störquelle für kritische Informationsinfrastrukturen ist Cybercrime, i. e. elektronische Kriminalität, die von Hackern, Datendieben und -saboteuren, Terroristen, Extremisten sowie Sozialstraftätern ausgehen kann. Mittels einer Reihe von Angriffstechniken versuchen diese, Informations- und Kommunikationssysteme zu infiltrieren bzw. manipulieren. Einige dieser Techniken können die Funktionsweise elektronischer Netze und damit die Verfügbarkeit, Verläßlichkeit und Vertraulichkeit von Informationen nachhaltig beeinträchtigen. Um die Sicherheit kritischer Informationsinfrastrukturen zuverlässig zu gewährleisten sind Schutzmaßnahmen zur Bekämpfung solcher Bedrohungen notwendig. Ein umfangreiches Risikomanagement erfordert eine facettenreiche Palette präventiver, reaktiver und kompensatorischer Maßnahmen.

Sicherheit in elektronischen Netzen weist jedoch die Charakteristik eines globalen Kollektivgutes auf, weshalb es für private Akteure im Rahmen des dezentralen Steuerungsarrangements eines Marktes zumeist nicht genügend Anreize gibt, die hier-

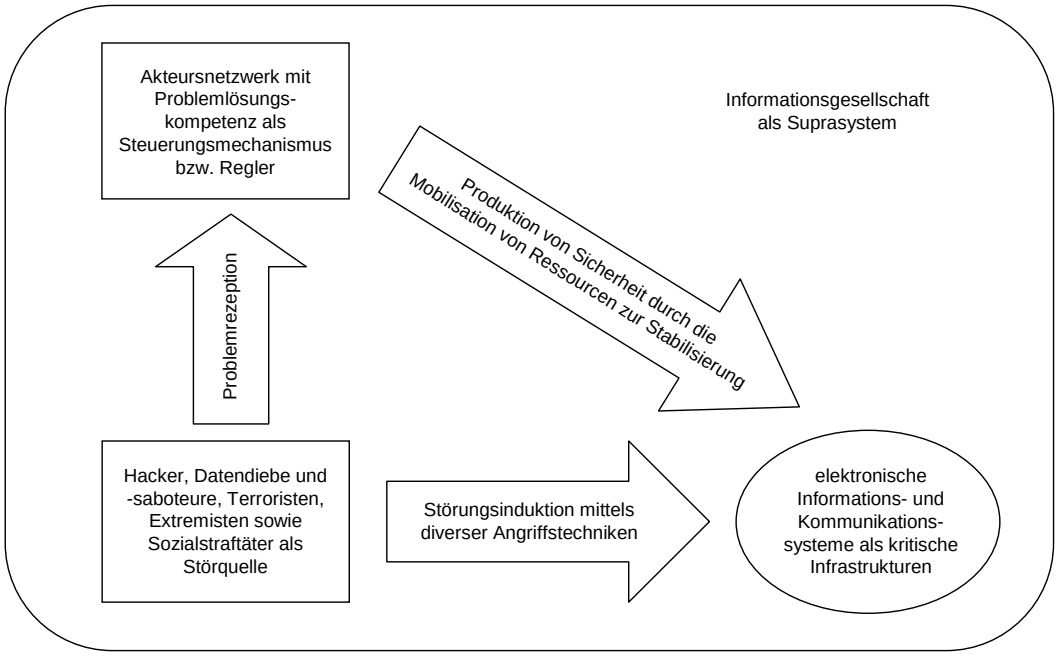


ABBILDUNG 6.1: *Der kybernetische Regelungsprozeß zur Sicherung kritischer Informationsinfrastrukturen*

für notwendigen Ressourcen in ausreichendem Maße zu mobilisieren. Andererseits fehlt es auf globaler Ebene aber zugleich an einer Hierarchie öffentlicher Akteure, welche die Mobilisation entsprechender Ressourcen in ausreichendem Maße zentral regulieren könnte. Die Steuerung der Produktion von Sicherheit in elektronischen Informations- und Kommunikationssystemen bleibt daher überwiegend einem polyzentralen Netzwerk privater und öffentlicher Akteure überlassen. Dieses Netzwerk fungiert aus kybernetischer Sicht als Regler, indem es kontinuierlich die aktuelle Bedrohungslage überwacht, um ggf. entsprechende Ressourcen zur Sicherung und damit zur Stabilisierung kritischer Informationssysteme zu mobilisieren.

Ein wirkungsvoller Regelungsmechanismus muß über Sensoren verfügen, die ihn in die Lage versetzen, problematische Störungen rechtzeitig zu rezipieren. Darüber hinaus benötigt er Effektoren, um in geeignetem Maße auf das zu regulierende System einwirken zu können. Die Aufgabe des Sensors entspricht hauptsächlich der Tätigkeitsart *Monitoring/Analysis of Incidents/Trends*, die des Effektors hauptsächlich der Tätigkeitsart *Emergency/Incident Response*. Diese Tätigkeiten werden vorwiegend von Akteuren des Clusters A2 wahrgenommen (vgl. Tabelle 5.7). In diesem Cluster spie-

len aber auch die Tätigkeitsarten *Information Exchange* und *Alerting* sowie *Investigation/Prosecution* eine zentrale Rolle. Die Akteure des Clusters A2 rezipieren akute Bedrohungen und kommunizieren diese sowohl gerichtet (1:1) als auch in der Breite (1:n). Sie steuern die Mobilisation von Ressourcen für reaktive und/oder kompensatorische Maßnahmen zur Sicherung bzw. Stabilisierung kritischer Informationsinfrastrukturen in erster Linie auf operativer Ebene und mit kurzfristigem Zeithorizont.

Strukturell setzt sich das Cluster A2 zu deutlich über zwei Dritteln aus öffentlichen sowie nicht-gewinnorientierten privaten Organisationen zusammen, die mehrheitlich auf globaler Ebene agieren (vgl. Abbildung 5.13). Die fehlende Gewinnorientierung läßt erkennen, daß sich die beteiligten Akteure nicht primär über einen Marktmechanismus, sondern vielmehr über global vernetzte, sich selbst organisierende Steuerungsstrukturen koordinieren. Das Cluster A2 umfaßt u. a. das US-DHS, MS sowie das CERT/CC. Es bündelt einen Großteil relevanter Ressourcen und verfügt daher über eine ausreichende Problemlösungskapazität, um flexibel und dynamisch auf aktuelle Bedrohungen reagieren zu können (vgl. Abbildung 5.17). Die drei genannten Akteure konfigurieren zugleich das Polyzentrum eines stabilen Kooperationsnetzwerkes (vgl. Abbildung 5.20).

Während die Akteure des Clusters A2 durch eine schnelle und flexible Mobilisation von Ressourcen eine kurzfristige, operative Reaktion und ggf. Kompensation ermöglichen, beschäftigen sich jene des Clusters A4 überwiegend mit der Entwicklung langfristiger Strategien zur Prävention. Im Mittelpunkt steht die Transformation institutioneller Rahmenbedingungen, um potentiellen Bedrohungen strukturell vorzubeugen. Über die Hälfte der Organisationen in diesem Cluster sind öffentlich, keine einzige ist gewinnorientiert. Ressourcen für strategische Maßnahmen, deren Nutzen weder kurzfristig noch direkt zurechenbar ist, werden demnach über hierarchische Organisationsformen mobilisiert. Wichtige Akteure sind bspw. OECD, EC und US-Congress, da sie jeweils über nennenswerte Ressourcen verfügen. Verhältnismäßig viele Akteure des Clusters A4 agieren auf regionaler Ebene. Insbesondere im supranationalen Rahmen der Europäischen Union konnte bereits eine weitgehende Harmonisierung erreicht werden. Das Beispiel der Cybercrime-Konvention des Europarates zeigt ferner, daß ein regional harmonisierter Rechtsraum bei Überschreiten einer kritischen Masse zum Nucleus globaler Ordnungsinduktion werden kann.

Zwischen der operativen Ebene des Clusters A2 und der strategischen Ebene des Clusters A4 läßt sich das Cluster A5 verorten. Dessen Akteure sind hauptsächlich mit der Entwicklung von Hard- und Software befaßt. Auf taktischer Ebene setzen sie im

TABELLE 6.1: *Tätigkeitsebenen der Produktion von Sicherheit*

Ebene	*Cluster*	*Zeithorizont*	*Koordination*	*Scope*	*Fokus*
strategisch	A4	langfristig	Hierarchie	regional	Institutionen
taktisch	A5	mittelfristig	Markt	global	Technik
operativ	A2	kurzfristig	Netzwerk	global	Reaktion/Kompensation

Rahmen institutioneller Vorgaben das technisch Mögliche mittelfristig um. Gestalten die Akteure des Clusters A4 vor allem die sozialen Komponenten des sozio-technischen Gesamtsystems der Informationsgesellschaft, so prägen die Akteure des Clusters A5 vorwiegend präventiv dessen technische Artefakte. Auffällig ist die große Zahl gewinnorientierter privater Organisationen in diesem Cluster. Technische Innovationen werden offensichtlich am wirkungsvollsten durch die Kräfte des Marktes vorangetrieben. Steuerung kann problemlos über monetäre Anreize erfolgen. Hinsichtlich der Problemlösungskapazität reicht das Cluster A5 jedoch bei weitem nicht an die beiden anderen Cluster heran. Es dient lediglich als Transmissionsriemen zwischen strategischer und operativer Ebene. Tabelle 6.1 verdeutlicht noch einmal die drei beschriebenen Tätigkeitsebenen im Prozeß der Produktion von Sicherheit in elektronischen Netzen.

Sicherheit bewegt sich auch in elektronischen Netzen in einem Spannungsfeld zwischen Kontrolle und Regulierung einerseits, sowie freien Entfaltungsmöglichkeiten andererseits (vgl. Tabelle 3.4). Während sich die Akteure des Clusters I1 vor allem auf die Themenfelder *Identity/Access*, *Secure Transactions*, *System Protection* und *Technical Standards* und damit auf den Schutz der Informationsinfrastruktur fokussieren, konzentrieren sich jene des Clusters I3 primär auf die Themenfelder *Information Freedom*, *Intellectual Property*, *Privacy/Data Protection* und *Legal Framework*, also den Schutz abstrakter Rechtsgüter (vgl. Tabelle 5.5). Der Schutz der Informationsinfrastruktur beschäftigt jedoch zahlenmäßig weit mehr Akteure, als dies beim Schutz abstrakter Rechtsgüter der Fall ist (vgl. Abbildung 5.4).

Strukturell umfaßt das Cluster I1 Akteure aller *Status*. Private – und hier vor allem gewinnorientierte – Organisationen sind allerdings überproportional vertreten. Im Cluster I3 hingegen dominieren nicht-gewinnorientierte private Organisationen. Auch wird in diesem Kontext überproportional auf regionaler Ebene agiert (vgl Abbildung 5.8). Im Cluster I1 finden sich u. a. das CERT/CC, das US-DoD, das US-DHS, das FBI

sowie ENISA. Im Cluster I3 die BSA, die EC sowie EPIC und EFF. Das Cluster I1 verfügt damit im Vergleich zum Cluster I3 über eine deutlich höhere Problemlösungskapazität (vgl. Abbildung 5.17). Auch im Kooperationsnetzwerk der Fallstudien sind die Akteure des Clusters I1 erkennbar zentraler verortet als jene des Clusters I3 (vgl. Abbildung 5.20). Sofern es im Prozeß der Produktion von Sicherheit in elektronischen Netzen zu einem Interessenkonflikt zwischen Techno-Elite und Anwendern kommt, setzen sich daher vermutlich langfristig die Interessen ersterer durch.

Eine herausgehobene Bedeutung bei der Produktion von Sicherheit in elektronischen Netzen kommt den Ressourcen *Expertenwissen* und *Sozialkapital* – i. e. Beziehungen zu anderen Akteuren – zu (vgl. Abbildung 5.14). Dies ist offensichtlich paradigmatisch für komplexe Koordinationsprozesse in modernen Informationsgesellschaften. Zugleich kann eine starke Konzentration relevanter Ressourcen und damit einhergehend der Problemlösungskapazität auf wenige Akteure beobachtet werden (vgl. Abbildung 5.17). Dennoch verfügt keiner dieser Akteure für sich genommen über ausreichende Ressourcen, um Sicherheit in elektronischen Netzen allein gewährleisten zu können.

Appendices

A Glossar der Organisationen

(ISC)2

International Information Systems Security Certification Consortium

33920 US Highway 19 North
Palm Harbor, FL 34684
USA

Status: private non-profit
Ebene: global
Sektor: Organisierte Interessen
Jahr der Gründung: 1989

Partner:
ASIS

Web: <`http://www.isc2.org`>

Durch Zusammenschluß mehrerer Berufsverbände entstandene Vereinigung von IT-Experten, deren Ziel eine Standardisierung von Ausbildungsnormen ist. (ISC)2 bietet verschiedene Ausbildungsprogramme für IT-Sicherheitsfachleute an und vergibt entsprechende Zertifikate. Die Mitglieder verpflichten sich freiwillig zu kontinuierlicher Weiterbildung sowie zur Wahrung eines berufsethischen Kodex. (ISC)2 unterhält Büros in den USA, London und Hong Kong sowie Beziehungen zu Partnern in Nord- und Süd-Amerika, Europa, Asien, Südafrika und dem Mittleren Osten. Die Organisation finanziert sich aus Beiträgen sowie Prüfungs- und Teilnahmegebühren. (ISC)2 und ASIS International erkennen ihre jeweiligen Abschlußzertifikate gegenseitig an.

ACLU

American Civil Liberties Union

125 Broad Street
New York, NY 10004
USA

Status: private non-profit
Ebene: national
Sektor: Organisierte Interessen
(Einzel-)Mitglieder: ca. 400.000
Jahr der Gründung: 1920

Web: <`http://www.aclu.org`>

US-amerikanische Bürgerrechtsorganisation, deren Ziel der Schutz verfassungsmäßiger Rechte, insbesondere der freien Meinungsäußerung, Gleichheit, Freiheit und Privatsphäre ist. Die ACLU verfolgt politische Entwicklungen im Bereich der Informationstechnologie und des Datenschutzes und informiert über staatliche Maßnahmen. Die Organisation beteiligt sich jährlich an über 60.000 Gerichtsverfahren und finanziert sich hauptsächlich aus Spenden und Beiträgen ihrer Mitglieder.

AIT

AIT Global

9 Byrd Court
Kings Park, NY 11754
USA

Status: private for-profit
Ebene: global
Sektor: Organisierte Interessen
Jahr der Gründung: 1986

Partner:
UN

Web: <`http://www.aitglobal.com`>

Berufsverband für Management- und IT-Fachleute, der in Zusammenarbeit mit der State University of New York in Farmingdale Weiterbildungsprogramme im Bereich der IKT anbietet. Zunächst unter der Bezeichnung „Association for the Advancement of Communications Technologies“, ab 1992 dann in „Association for Information Technologies“ und ab 1997 in „AIT Global“ umbenannt. Für seine korporativen Mitglieder, unter ihnen nach eigenen Angaben mehrere nationale und internationale Großunternehmen sowie verschiedene staatliche und akademische Organisationen, richtet AIT Global Ausbildungsprogramme und Konferenzen aus.

AKSIS

Arbeitskreis Schutz von Infrastrukturen

Einsteinstraße 20
85521 Ottobrunn
Deutschland

Status: mixed
Ebene: national
Sektor: sektorübergreifende Foren
Jahr der Gründung: 1999

Korporative Mitglieder:
BKA, BMVg, BSI, IABG, Siemens

Von der IABG federführend organisierter Gesprächskreis zur Analyse der IT-Abhängigkeit kritischer Infrastrukturen. Im Rahmen des Arbeitskreises treffen sich zweimal jährlich Vertreter aus öffentlicher Verwaltung und privater Wirtschaft (u. a. BMVg, BMI, BSI, BND, BKA, Siemens, Deutsche Telekom, Deutsche Bank und Deutsche Bahn) zum Austausch von Informationen über Sicherheitsrisiken und -vorfälle sowie geeignete Maßnahmen im Rahmen eines übergreifenden Sicherheitsmanagements.

APEC

Asia-Pacific Economic Cooperation

35 Heng Mui Keng Terrace
Singapore 119616
Singapur

Status: public
Ebene: regional
Sektor: Internationale Organisationen
Jahr der Gründung: 1989

Partner:
OECD

Web: <`http://www.apec.org`>

Internationale Organisation zur Förderung von Wirtschaft und Handel im asiatisch-pazifischen Raum mit derzeit 21 Mitgliedsstaaten, unter ihnen Japan, China, Australien und die USA. Der APEC-Ausschuß für Handel und Investitionen beschäftigt sich in Unterausschüssen auch mit dem Schutz geistigen Eigentums sowie technischen Standards im Bereich der IT-Sicherheit. Für eine einheitliche APEC Cybersecurity Strategy ist vor allem die Arbeitsgruppe für Telekommunikation und Information zuständig. Diese befaßt sich, unter enger Einbindung des privaten Sektors, neben anderen Themen auch mit dem Schutz und der Sicherheit von Informationsinfrastrukturen und entwickelte verschiedene Richtlinien, um den rechtsraumübergreifenden elektronischen Handel zu erleichtern.

ASIS

ASIS International

1625 Prince Street
Alexandria, VA 22314–2818
USA

Status: private non-profit
Ebene: global
Sektor: Organisierte Interessen
(Einzel-)Mitglieder: ca. 34.000
Jahr der Gründung: 1955

Partner:
(ISC)2, ISACA, ISSA

Web: <`http://www.asisonline.org`>

Unter der Bezeichnung „American Society for Industrial Security“ gegründeter, weltweit vertretener Berufsverband für Sicherheitsfachleute aus Wirtschaft und Verwaltung. ASIS hält jährliche Konferenzen ab, gibt monatlich die Publikation „Security Management“ heraus und bietet zertifizierte Aus- und Weiterbildungsprogramme an. Die Mitglieder verpflichten sich freiwillig zu kontinuierlicher Weiterbildung sowie zur Wahrung eines berufsethischen Kodex. ASIS, ISACA und ISSA gründeten 2005 eine Allianz, deren Ziel die strategische Entwicklung eines ganzheitlichen Sicherheitsmanagements in Unternehmen ist.

BKA

Bundeskriminalamt

Thaerstraße 11
65193 Wiesbaden
Deutschland

Status: public
Ebene: national
Sektor: Staat/Öffentliche Verwaltung
Mitarbeiter: ca. 5.300
Jahr der Gründung: 1951

Partner:
BMVg, BSI

Web: <`http://www.bka.de`>

Bundesoberbehörde im Geschäftsbereich des Innenministeriums der Bundesrepublik Deutschland. Das BKA koordiniert die Arbeit der Polizeibehörden der Länder untereinander und bündelt den gesamten polizeilichen Dienstverkehr mit dem Ausland. Aufgrund der Hoheit der Bundesländer in Fragen der inneren Sicherheit führt das BKA als Institution des Bundes eigene Ermittlungen nur in besonderen Fällen durch. Zur verstärkten Bekämpfung der Computerkriminalität wurde 1998 auf Beschluß der Konferenz der Innenminister der Länder innerhalb des BKA die „Zentrale anlaßunabhängige Recherche in Datennetzen“ (ZaRD) mit derzeit etwa 60 Mitarbeitern eingerichtet. Diese „Netzstreife“ weist seit 1999 in jährlichen Statistiken strafbare Inhalte im Internet aus und gibt die Ermittlungen an die entsprechenden nationalen und internationalen Polizeibehörden weiter.

BMVg

Bundesministerium der Verteidigung

Hardthöhe
53125 Bonn
Deutschland

Status: public
Ebene: national
Sektor: Staat/Öffentliche Verwaltung
Mitarbeiter: ca. 390.000
Jahr der Gründung: 1955

Partner:
BKA, BSI, IABG

Web: <`http://www.bmvg.de`>

Oberste Bundesbehörde der Bundesrepublik Deutschland. Zugleich höchste Kommandobehörde der Bundeswehr. Für das BMVg ist vor allem Sicherung und Schutz des eigenen Führungs- und Informationssystemverbundes von Interesse. Hinsichtlich dessen arbeitet das BMVg mit der IABG und dem BSI zusammen. Die Bundeswehr betreibt ein eigenes CERT (CERTBw) nach dem Vorbild des CERT/CC. Einem Bericht von *Spiegel Online* (vgl. <`http://www.spiegel.de/netzwelt/tech/0,1518,606096,00.html`>) vom 07.02.2009 zufolge baut die Bundeswehr darüber hinaus ferner eigene Fähigkeiten zur Infiltration fremder Netze aus.

BSA

Business Software Alliance

1150 18th Street NW
Washington, DC 20036
USA

Status: private non-profit
Ebene: global
Sektor: Organisierte Interessen
Mitarbeiter: ca. 100
Jahr der Gründung: 1988

Korporative Mitglieder:
Cisco, HP, IBM, ISS, McAfee, MS, Oracle, RSA, SAP, Siemens, Symantec

Partner:
IC3, ISSA

Web: <`http://www.bsa.org`>

Beitragsfinanzierter, in über 80 Ländern aktiver Interessenverband der Software-Industrie. Hauptanliegen der BSA ist die Förderung der wirtschaftlichen Interessen ihrer Mitglieder, insbesondere im Kampf gegen Softwarepiraterie. Als organisierter Interessenverband betreibt die BSA vor allem Lobbying im nationalen und internationalen Kontext. Sie zählt zu den stärksten Befürwortern der Cybercrime-Konvention des Europarates. Darüber hinaus engagiert sich die BSA schwerpunktmäßig in der Durchsetzung des Schutzes von geistigem Eigentum. Hierzu dienen Maßnahmen wie die Ausschreibung von Belohnungen für die Aufdeckung von Urherberrechtsverletzungen, eigenständige Ermittlungen und ggf. gerichtlich erzwungene Lizenzüberprüfungen.

BSI

Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185–189
53175 Bonn
Deutschland

Status: public
Ebene: national
Sektor: Staat/Öffentliche Verwaltung
Mitarbeiter: ca. 500
Jahr der Gründung: 1991

Partner:
BKA, BMVg, ENISA, IABG

Web: <`http://www.bsi.bund.de`>

Bundesoberbehörde im Geschäftsbereich des Innenministeriums der Bundesrepublik Deutschland. Nachfolgerin der „Zentralstelle für Sicherheit in der Informationstechnik“ (ZSI), deren Vorläuferin die dem Bundesnachrichtendienst (BND) zugeordnete „Zentralstelle für Chiffrierwesen“ (ZfCh) war. Sie berät Bundes- und Landesbehörden hinsichtlich der Informationssicherheit. Das BSI betreibt das CERT-Bund, testet verfügbare Software auf potentielle Sicherheitslücken und gibt IT-Grundschutzhandbücher heraus, welche grundlegende Standards des IT-Sicherheitsmanagements umreißen. Das BSI betreibt den Informationsverbund Berlin–Bonn, der eine sichere und vertrauliche Datenkommunikation zwischen beiden Regierungssitzen ermöglicht. Seit 2011 ist beim BSI das Nationale „Cyber-Abwehrzentrum“ (NCAZ) angesiedelt, in dessen Rahmen die Bundesämter für Verfassungsschutz sowie Bevölkerungsschutz und Kathastrophenhilfe, das Bundeskriminalamt, die Bundespolizei, der Bundesnachrichtendienst und das Zollkriminalamt kooperieren.

CCC

Chaos Computer Club

Lokstedter Weg 72
20251 Hamburg
Deutschland

Status: private non-profit
Ebene: national
Sektor: Stiftungen/Vereine
Jahr der Gründung: 1986

Web: <`http://www.ccc.de`>

Privater Verein von IT-Experten zur Förderung von Informationsfreiheit und Datenschutz. Auf seinen Webseiten stellt der CCC Informationen zur Computersicherheit zur Verfügung. Informell bereits 1981 gegründet, existiert der CCC seit 1986 als eingetragener Verein in Hamburg. Vor allem in den 1980er Jahren sorgten verschiedene Hacker aus dem Umfeld des CCC durch erfolgreiche Angriffe, u. a. auf Rechner des BTX-Systems und der NASA, für Aufsehen.

CDT

Center for Democracy and Technology

1634 I Street NW
Washington, DC 20006
USA

Status: private non-profit
Ebene: national
Sektor: Organisierte Interessen
Mitarbeiter: ca. 20
Jahr der Gründung: 1994

Web: <`http://www.cdt.org`>

Das CDT entstand als Abspaltung der poltitischen Interessenvertretung der EFF in Washington. Die Bürgerrechtsgruppierung tritt insbesondere für Datenschutz sowie Informations- und Meinungsfreiheit in digitalen Kommunikationsmedien ein. Einschlägige US-Gesetze und allgemeine technische Entwicklungen werden hinsichtlich möglicher Einschränkungen dieser Grundrechte analysiert. Daneben beschäftigt sich CDT mit einem Interessenausgleich im Spannungsfeld der Wahrung von Urheberrechten einerseits und dem freiem Informationsaustausch und Wissenszugang andererseits. Hinsichtlich der DNS-Regulierung des Internet setzt sich die Organisation für eine internationale Beteiligung entsprechend demokratischer Prinzipien ein.

CERT/CC

Computer Emergency Response Team Coordination Center

Carnegie Mellon University
Pittsburgh, PA 15213–3890
USA

Status: mixed
Ebene: global
Sektor: Wissenschaft und Forschung
Mitarbeiter: ca. 40
Jahr der Gründung: 1988

Partner:
ISA, US-DHS, US-DoD

Web: <`http://www.cert.org`>

Zentrale Koordinationsstelle zur Auswertung und Bewältigung sicherheitsrelevanter Vorfälle im Internet. Das CERT/CC entstand als unmittelbare Reaktion auf den Morris-Worm im Rahmen des „Network Systems Survivability Program“ am Sofware Engineering Institute (SEI) der privaten Carnegie Mellon University. Das SEI wurde 1984 mit finanzieller Unterstützung des US-DoD zur Verbesserung von Qualitätsstandards bei der Software-Entwicklung gegründet und wird seitdem überwiegend aus öffentlichen Mitteln finanziert. Es unterliegt speziellen Sicherheitsvorschriften. Seit 2003 existiert in Frankfurt a. M. auch ein europäischer Ableger des SEI (SEI Europe), der sich aus Spenden großer europäischer Unternehmen finanziert. Gegenwärtig umfassen die Aufgaben des CERT/CC, neben der unmittelbaren Bearbeitung akuter Sicherheitsvorfälle, vor allem die Schulung von Software-Entwicklern, die Bereitstellung von Werkzeugen zur Bedrohungsanalyse in Netzwerken, sowie die Aufklärung privater Nutzer über Sicherheitsrisiken und vorbeugende Maßnahmen.

CIA

Central Intelligence Agency

Langley, VA
USA

Status: public
Ebene: global
Sektor: Staat/Öffentliche Verwaltung
Jahr der Gründung: 1947

Partner:
FBI, SRI, US-DHS, US-DoD, US-DoJ

Web: <`http://www.cia.gov`>

Von Präsident Harry S. Truman errichteter Auslandsnachrichtendienst der USA. Die CIA beteiligt sich u. a. in Zusammenarbeit mit dem FBI, dem US-DoD und dem US-DHS an Untersuchungen über vom Ausland ausgehende Gefahren für die Informations-Infrastruktur der USA, so etwa asymmetrische Formen der Kriegsführung oder des Terrorismus im Cyberspace.

CIAO

Critical Infrastructure Assurance Office

1401 Constitution Avenue NW
Washington, DC 20230
USA

Status: public
Ebene: national
Sektor: Staat/Öffentliche Verwaltung
Jahr der Gründung: 1998

Partner:
US-DHS

Von US-Präsident Clinton aufgrund des Abschlußberichts (Marsh-Report) der President's Commission on Critical Infrastructure Protection (PCCIP) im Verantwortungsbereich des Handelsministeriums eingerichtete Behörde zur Koordination von Regierungsmaßnahmen, die dem Schutz kritischer Infrastrukturen in der Informationsgesellschaft dienen. Anfang 2000 gab das CIAO einen „Nationalen Plan zum Schutz von Informationssystemen" heraus, der sich vor allem mit Maßnahmen innerhalb der Verwaltung selbst befaßte. Ein 2002 erschienener zweiter Teil bezog sich schwerpunktmäßig auf die Kooperation von Verwaltung und privatem Sektor. Seit dem Jahr 2003 fällt das CIAO in den Verantwortungsbereich des neugegründeten US-DHS.

CIDDAC

Cyber Incident Detection and Data Analysis Center

Philadelphia, PA
USA

Status: mixed
Ebene: national
Sektor: sektorübergreifende Foren
Jahr der Gründung: 2005

Korporative Mitglieder:
InfraGard

Partner:
US-DHS

Web: <`http://www.ciddac.org`>

Aus dem lokalen InfraGard-Büro in Philadelphia hervorgegangene Initiative des privaten Sektors zur Einreichtung eines Informationsverbundes, der ein automatisiertes Sammeln und Abgleichen von Daten über Angriffe im Cyberspace erlaubt. Ein entsprechendes Pilotprojekt wurde 2005 am Institute of Strategic Threat Analysis and Response (ISTAR) der University of Pennsylvania in Philadelphia entwickelt und vom US-DHS finanziert. Das System ermöglicht es Teilnehmern, sich in Echtzeit nicht nur über die jeweils eigene Bedrohungssituation, sondern auch über die Lage der angrenzenden Netzsektoren zu informieren. Darüber hinaus verschafft es öffentlichen Akteuren einen permanent aktualisierten Lageüberblick. Bei den teilnehmenden Organisationen werden sog. Real-Time Cyber Attack Detection Sensors (RCADS) installiert, die im Falle eines erkannten Angriffs unmittelbar Daten an eine zentrale Auswertungsstelle weiterleiten. Das System ermöglicht so eine Strafverfolgung ohne die Offenlegung sensibler Unternehmensdaten.

Cisco

Cisco Systems

170 West Tasman Drive
San Jose, CA 95134
USA

Status: private for-profit
Ebene: global
Sektor: Wirtschaft
Mitarbeiter: ca. 50.000
Jahr der Gründung: 1984

Partner:
Cybertrust, HP, IBM, McAfee, MS, Oracle, RedSiren, RSA, Siemens, Solutionary, UN, VeriSign

Web: <`http://www.cisco.com`>

Von Wissenschaftlern der Stanford University gegründetes, börsennotiertes Unternehmen für Netzwerktechnik. Der Umsatz von Cisco belief sich im Geschäftsjahr 2007 auf 34,9 Mrd. US-Dollar (<`http://hoovers.com`>). Auf der Forbes-Liste der weltweit größten Unternehmen belegte Cisco 2007 den 103. Platz. Zum Kerngeschäft des Unternehmens zählen größtenteils Hardware-, teilweise aber auch Software-Produkte zum Aufbau IP-basierter Computernetzwerke. Traditionell liegen die Schwerpunkte dabei im Bereich Routing und Switching, in jüngster Zeit aber auch vermehrt bei Themen der Netzwerksicherheit. Weitere Geschäftsfelder sind Wireless-LAN und IP-Telefonie.

CoE

Europarat

Avenue de l'Europe
67075 Strasbourg Cedex
Frankreich

Status: public
Ebene: regional
Sektor: Internationale Organisationen
Jahr der Gründung: 1949

Web: <`http://www.coe.int`>

Internationale Organisation mit z. Z. 47 europäischen Mitgliedsstaaten sowie fünf überwiegend außereuropäischen Staaten mit Beobachterstatus. Zu den zentralen Einrichtungen des CoE gehören das Ministerkomitee, die parlamentarische Versammlung sowie der Europäische Gerichtshof für Menschenrechte. Ziel des CoE ist, neben der Wahrung der Menschenrechte sowie der Prinzipien der Rechtsstaatlichkeit, eine Harmonisierung der Rechtssysteme seiner Mitglieder. Mit der Ende 2001 vom Europarat verabschiedeten Cybercrime-Konvention wurde zum ersten Mal ein internationaler, vertraglich bindender Rahmen zur umfassenden Bekämpfung von Computerkriminalität geschaffen. Bereits 1981 beschloß der Europarat eine Konvention zum Schutz personenbezogener Daten in elektronischen Systemen.

CSC

Computer Sciences Corporation

2100 East Grand Avenue
El Segundo, CA 90245
USA

Status: private for-profit
Ebene: global
Sektor: Wirtschaft
Mitarbeiter: ca. 79.000
Jahr der Gründung: 1959

Partner:
HP, IBM, MS, Oracle, RSA, SAP, Symantec, US-DoD

Web: <`http://www.csc.com`>

Börsennotiertes IT-Dienstleistungs- und Beratungsunternehmen. Im Geschäftsjahr 2007 erwirtschaftete CSC einen Umsatz von 14,9 Mrd. US-Dollar (<`http://hoovers.com`>). Auf der Forbes-Liste der weltweit größten Unternehmen erreichte CSC 2007 den 743. Platz. Das Unternehmen produzierte zunächst Assembler- und Compilerprogramme sowie Betriebssysteme, weitete dann jedoch durch eine Reihe von Übernahmen (bspw. Computer Sciences Australia (1993), Ploenzke AG (1994), Gruppe für Angewandte Informatik (1997)) seine Kompetenzen systematisch aus und ist heute in über 80 Ländern tätig. CSC beteiligte sich u. a. an IT-Projekten in den Bereichen Luft- und Raumfahrt, Verteidigungstechnik, Energieversorgung, Finanzdienstleistungen sowie der öffentlichen Verwaltung. Das Unternehmen ist einer der größten IT-Dienstleister im Auftrag der US-Regierung. Etwa ein Viertel seiner Einnahmen stammt aus Verträgen mit dem US-DoD.

CSI

Computer Security Institute

600 Harrison Street
San Francisco, CA 94107
USA

Status: private for-profit
Ebene: global
Sektor: Wirtschaft
Jahr der Gründung: 1974

Partner:
FBI, ISSA

Web: <`http://www.gocsi.com`>

Berufsvereinigung zur Aus- und Weiterbildung von IT-Sicherheitsfachleuten. Das CSI organisiert jährliche Konferenzen zu unterschiedlichen Sicherheitsthemen und bietet umfangreiche Weiterbildungsprogramme an. Seit 1996 führt es in Kooperation mit dem FBI jährlich eine Umfrage unter großen amerikanischen Unternehmen zu den Themen Computerkriminalität und -sicherheit (Computer Crime and Security Survey) durch.

CSIA

Cyber Security Industry Alliance

2020 North 14th Street
Arlington, VA 22201
USA

Status: mixed
Ebene: national
Sektor: Organisierte Interessen
Jahr der Gründung: 2004

Korporative Mitglieder:
IBM, RSA, Symantec

Web: <`https://www.csialliance.org`>

Auf der RSA-Konferenz Anfang 2004 in San Francisco gegründeter Interessenverband für IT-Sicherheitsunternehmen. Als Pressure Group setzte sich die CSIA für die Unterzeichnung der Cybercrime-Konvention des CoE durch die US-Regierung ein. Ferner werden in Zusammenarbeit mit wissenschaftlichen Einrichtungen Ausbildungsprogramme entwickelt sowie Awareness-Kampagnen unterstützt werden. Auch beabsichtigt die CSIA sich an der Definition technischer Sicherheitsstandards zu beteiligen. Sie ist gegen eine staatliche Regulierung dieser Standards und tritt stattdessen für eine freiwillige Partnerschaft zwischen öffentlichem und privatem Sektor ein.

CSIS

Center for Strategic and International Studies

1800 K Street NW
Washington, DC 20006
USA

Status: private non-profit
Ebene: global
Sektor: Wissenschaft und Forschung
Mitarbeiter: ca. 200
Jahr der Gründung: 1962

Partner:
US-Congress

Web: <`http://www.csis.org`>

Unabhängige, gemeinnützige Denkfabrik, die sich durch Zuwendungen aus der Wirtschaft, durch öffentliche Mittel und private Spenden finanziert. Ein Großteil der Mitarbeiter kommt aus dem öffentlichen Sektor. Schwerpunktmäßig konzentriert sich das CSIS auf Themen der nationalen und internationalen Sicherheitspolitik sowie den Bereich Global Governance. Ziel ist die Identifikation neuer Probemfelder sowie die Formulierung von Lösungsstrategien, die sich primär an die US-Bundesregierung richten. Mit dem Ende der Blockkonfrontation und dem Entstehen neuer, asymmetrischer Bedrohungsszenarien rückte auch das Thema Heimatschutz und in diesem Kontext die Sicherheit elektronischer Netzwerke in den Mittelpunkt des Interesses.

Cybertrust

Cybertrust

13650 Dulles Technology Drive
Herndon, VA 20171–4602
USA

Status: private for-profit
Ebene: global
Sektor: Wirtschaft
Mitarbeiter: ca. 210
Jahr der Gründung: 2004

Partner:
Cisco, MS, RSA, Symantec

Web: <`http://www.cybertrust.com`>

Privates Unternehmen, das durch Fusion von TrueSecure (Risk Management) und BeTrusted (Identity Management) sowie großer Teile von Ubizen (Security Management) im Jahr 2004 entstand. Cybertrust bietet hauptsächlich Management- und Beratungsdienstleistungen zur Sicherung von IT-Infrastrukturen sowie Software zum Aufbau sicherer Transaktionsverbindungen (PKI) an. Im Jahr 2007 wurde Cybertrust von Verizon Business übernommen.

EC

Europäische Kommission

Rue de la Loi 200
1049 Brussels
Belgien

Status: public
Ebene: regional
Sektor: Staat/Öffentliche Verwaltung
Mitarbeiter: ca. 20.000
Jahr der Gründung: 1957

Partner:
ENISA, EU Forum, EUROPARL, RAND

Web: <`http://europa.eu.int/comm/`>

Exekutivorgan der Europäischen Union, das über ein Initiativrecht für Richtlinien, Verordnungen und Entscheidungen verfügt. Seit 1999 initiiert die Kommission Programme (Beschlüsse des Europäischen Parlamentes und Rates Nr. 276/1999/EG, Nr. 1151/2003/EG, Nr. 854/2005/EG), die auf eine Bekämpfung illegaler und schädlicher Inhalte in elektronischen Netzen abzielen. Von 2001 bis 2003 förderte die Kommission das Projekt CTOSE (Cyber Tools On-Line Search for Evidence) zur Entwicklung neuer Technologien der Beweiserhebung in elektronischen Netzen. Die Kommission ist Urheberin der Initiativen „eEurope 2002“, „eEurope 2005“ und „eEurope 2010“, in denen dem Schutz kritischer Informationsinfrastrukturen ein besonderer Stellenwert eingeräumt wird. Ferner initiierte sie 2006 das Europäische Programm für den Schutz kritischer Infrastrukturen (EPSKI) sowie eine Strategie für eine sichere Informationsgesellschaft (KOM (2006) 251). Gemeinsam mit der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik veröffentlichte die Komission Anfang 2013 eine Cybersicherheitsstrategie (JOIN (2013) 1).

EFF

Electronic Frontier Foundation

454 Shotwell Street
San Francisco, CA 94110
USA

Status: private non-profit
Ebene: global
Sektor: Organisierte Interessen
Mitarbeiter: ca. 25
Jahr der Gründung: 1990

Web: <`http://www.eff.org`>

Spendenfinanzierte, gemeinnützige Gruppierung, deren Ziel der Schutz von Bürgerrechten im Umfeld elektronischer Medien ist. Die EFF wurde anläßlich des sog. E911-Falles gegründet, in dessen Rahmen der US Secret Service aufgrund des Diebstahls elektronischer Dokumente mit technischen Einzelheiten des Telefon-Notrufsystems private Computer beschlagnahmte. Die EFF beteiligte sich seitdem sowohl in diesem als auch in einer Reihe weiterer Fälle an gerichtlichen Verfahren gegen US-Behörden. Aus Sicht der EFF bilden digitale Medien einen speziellen techno-kulturellen Kontext, in welchem staatliche Regulierung weitgehend zu vermeiden sei. Anfang der 1990er Jahre beriet die Gruppierung die US-Regierung zu Fragen der IuK-Politik. Dies führte aus ideologischen Gründen 1994 zu einer Abspaltung der CDT als politischer Interessenvertretung, während sich die EFF selbst aus dem politischen Prozeß zurückzog. Die Gruppierung informiert in Pressemitteilungen und im Internet regelmäßig über politische, technische und juristische Einzelheiten zu Themen wie Anonymität, Privatsphäre, biometrische Daten oder geistigem Eigentum.

ENISA

European Network and Information Security Agency

Vassilika Vouton
700 13 Heraklion
Griechenland (Kreta)

Status: public
Ebene: regional
Sektor: Staat/Öffentliche Verwaltung
Mitarbeiter: ca. 50
Jahr der Gründung: 2004

Partner:
BSI, EC, EU Forum, EUROPARL

Web: <`http://www.enisa.europa.eu`>

EU-Behörde für Netz- und Informationssicherheit, deren Verwaltungsrat sich aus Vertretern der EU-Mitgliedsstaaten und der Kommission einerseits – sowie aus Interessenvertretern der Bereiche Wirtschaft, Wissenschaft und Gesellschaft (Permanent Stakeholder Group) andererseits – zusammensetzt. Die ENISA berät die Kommission sowie die Mitgliedsstaaten zu Fragen der Informationssicherheit, sammelt und wertet Daten zu sicherheitsrelevanten Vorfällen im europäischen Raum aus und klärt über mögliche Risiken auf. Hierzu kooperiert die ENISA auch mit privaten Organisationen. Die Behörde organisierte eine Reihe von Arbeitskreisen, u. a. zu dem Thema Risikobewertung und -management.

EPIC

Electronic Privacy Information Center

1718 Conneticut Avenue NW
Washington, DC 20009
USA

Status: private non-profit
Ebene: global
Sektor: Organisierte Interessen
Mitarbeiter: ca. 10
Jahr der Gründung: 1994

Web: <`http://www.epic.org`>

Unabhängige, gemeinnützige Interessengruppierung zum Schutz verfassungsmäßig garantierter Bürgerrechte, insbesondere vor solchen Bedrohungen, die sich aus der Entwicklung neuer Technologien ergeben. Vorläufer war die 1983 gegründete Vereinigung „Computer Professionals for Social Responsibility“ (CPSR). Die Finanzierung erfolgt über Spendenmitteln und Stiftungen. Das EPIC beschäftigt sich allgemein mit der Analyse und Bewertung neuer Entwicklungen in Politik und Technik, die Einschränkungen der Privatspähre und freien Meinungsäußerung zur Folge haben. Ergebnisse und Hinweise werden in Form eines regelmäßig erscheinenden elektronischen Newsletters publiziert. Daneben engagiert sich die Organisation in einzelnen Präzedenzfällen auch vor Gericht.

EU Forum

EU Forum on Cybercrime

Rue de la Loi 200
1049 Brussels
Belgien

Status: mixed
Ebene: regional
Sektor: sektorübergreifende Foren
Jahr der Gründung: 2001

Partner:
EC, ENISA

Web:
<`http://cybercrime-forum.jrc.it`>

In Folge der Mitteilung der Europäischen Kommission KOM(2000) 890 (Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität) eingerichtetes Gesprächsforum, in dessen Rahmen sich Strafverfolgungsbehörden, Internet-Anbieter, Telekommunikationsbetreiber, Bürgerrechtsorganisationen, Datenschutzbehörden und Verbrauchervertreter zu Themen der Computerkriminalität austauschen. Das Forum soll das allgemeine Bewußtsein für Bedrohungen in elektronischen Netzen erhöhen und die Zusammenarbeit innerhalb der EU fördern.

EUROPARL

Europäisches Parlament

Allée du Printemps
67070 Strasbourg Cedex
Frankreich

Status: public
Ebene: regional
Sektor: Staat/Öffentliche Verwaltung
Mitarbeiter: ca. 3.860
Jahr der Gründung: 1979

Partner:
EC, ENISA

Web: <`http://www.europarl.eu.int`>

In fünfjähriger Legislaturperiode gewählte Volksvertretung der Europäischen Union. Das Europäische Parlament hat Mitwirkungsrechte bei Richtlinien, Verordnungen und Entscheidungen der EU. Hinsichtlich der Sicherheit in Computernetzwerken standen bisher hauptsächlich Fragen des Datenschutzes im Mittelpunkt. Wichtige Richtlinien sind: Datenschutz Richtlinie (1995/46/EC), Telekommunikations-Datenschutz Richtlinie (1997/66/EC), Richtlinie für Elektronische Signaturen (1999/93/EC).

FBI

US Federal Bureau of Investigation

935 Pennsylvania Avenue NW
Washington, DC 20535
USA

Status: public
Ebene: national
Sektor: Staat/Öffentliche Verwaltung
Mitarbeiter: ca. 30.000
Jahr der Gründung: 1908

Partner:
CIA, CSI, IC3, InfraGard, NIPC, NSA, NW3C, RAND, SCI, US-DHS, US-DoJ

Web: <`http://www.fbi.gov/cyberinvest/cyberhome.htm`>

Zentrale Ermittlungsbehörde des US-DoJ. Zunächst als „Bureau of Investigation“ (BOI), seit 1935 dann als FBI bezeichnet. Im Zuge einer – durch die Terroranschläge des 11. September 2001 ausgelösten – Reorganisation des FBI erfolgte 2002 die Einrichtung einer eigenständigen Abteilung für Computerkriminalität (Cyber Division). Diese ist federführend in der Aufklärung und Abwehr von Angriffen und Straftaten gegen oder unter Zuhilfenahme von IKT-Systemen. Im Rahmen der Prävention und Abwehr von Straftaten in elektronischen Netzen unterhält das FBI Partnerschaften mit privaten und öffentlichen Akteuren (z. B. InfraGard), deren Ziel ein Austausch von Informationen und die Aus- und Weiterbildung von IT-Experten ist. Als Online-Annahmestelle für Anzeigen dient das IC3. Das FBI überwacht in gezielten Fällen auch den Datenverkehr in elektronischen Netzen. Bis Anfang 2005 wurde hierzu bspw. ein Paket-Sniffer mit dem Decknamen „Carnivore“ eingesetzt.

FIRST

Forum of Incident Response and Security Teams

650 Castro Street
Mountain View, CA 94041–2055
USA

Status: private non-profit
Ebene: global
Sektor: sektorübergreifende Foren
Jahr der Gründung: 1990

Korporative Mitglieder:
BMVg, BSI, CERT/CC, Cisco, HP, IBM, ISS, MS, NIST, Oracle, Siemens, Symantec, US-DHS, US-DoD, VeriSign

Web: <`http://www.first.org`>

Internationaler, beitragsfinanzierter Dachverband von Computernotfall- und Sicherheitsteams aus öffentlicher Verwaltung, privater Wirtschaft und Wissenschaft. Zu den Mitgliedsteams gehören u. a. : CERT-Bund (BSI), CERTBw (BMVg), CERT/CC, Cisco, DoD-CERT (US-DoD), HP SSRT (HP), IBM MSS (IBM), ISS, MSCERT (MS), NIST, ORACERT (Oracle), Siemens-CERT, SymCERT (Symantec), US-CERT (US-DHS) und VeriSign. FIRST veranstaltet jährlich einen Workshop zum Thema Incident Response.

FTC

US Federal Trade Commission

600 Pennsylvania Avenue NW
Washington, DC 20580
USA

Status: public
Ebene: national
Sektor: Staat/Öffentliche Verwaltung
Jahr der Gründung: 1914

Partner:
IC3

Web: <`http://www.ftc.gov`>

Unabhängige US-Aufsichtsbehörde zur Regulierung von Wettbewerb und Verbraucherschutz. Die Abteilung für Verbraucherschutz (Bureau of Consumer Protection) der FTC ist für die Umsetzung von Bundesgesetzen gegen die Straftaten Betrug und Täuschung zuständig, die u. a. auch elektronische Transaktionen betreffen. Seit 2003 fällt ferner die Umsetzung von Bestimmungen gegen Spamming (CAN-SPAM Act) in den Aufgabenbereich der FTC. In dieser Eigenschaft erhob die FTC erstmals im Januar 2005 Anklage gegen eine Reihe von Unternehmen und Privatpersonen. Als Verbraucherschutzbehörde obliegt der FTC die Herausgabe von Richtlinien zum Schutz elektronisch gespeicherter Kundendaten gemäß GLB-Act von 1999.

G8

Gruppe der Acht

Status: public
Ebene: global
Sektor: Internationale Organisationen
Jahr der Gründung: 1975

Korporative Mitglieder:
US-DoJ

Partner:
UN, US-DoJ

Web: <`http://www.g8.utoronto.ca/summit/1997denver/`>

Im Jahr 1997 richteten die Staats- und Regierungschefs der sieben führenden Industriestaaten und Rußlands (G8) auf Anregung der USA unter dem Vorsitz des US-DoJ eine Arbeitsgruppe zur High-Tech-Kriminalität ein. Diese Arbeitsgruppe diskutiert in regelmäßigen Abständen verschiedene Sicherheitsthemen und initiierte eine 24-Stunden-Kontaktgruppe, deren Ziel eine Verbesserung des internationalen Informationsaustauschs im Rahmen der Strafermittlung und -verfolgung ist. An dieser Kontaktgruppe beteiligen sich neben den G8-Staaten Deutschland, Frankreich, Italien, Japan, Kanada, Rußland, UK und USA auch Australien, Brasilien, Dänemark, Finnland, die Niederlande, Schweden und Spanien. Die Innen- und Justizminister der G8-Staaten einigten sich ferner 2003 auf einen gemeinsamen Maßnahmenkatalog zum Schutz kritischer Informationsinfrastrukturen.

Gartner

Gartner

56 Top Gallant Road
Stamford, CT 06904
USA

Status: private for-profit
Ebene: global
Sektor: Wirtschaft
Mitarbeiter: ca. 3.800
Jahr der Gründung: 1979

Web: <`http://www.gartner.com`>

Börsennotiertes Unternehmen für Marktforschung mit weltweit 75 Niederlassungen. Der Umsatz von Gartner belief sich im Geschäftsjahr 2006 auf 1,1 Mrd. US-Dollar (<`http://hoovers.com`>). Kerngeschäft des Unternehmens sind globale Marktanalysen im Bereich der IT-Industrie sowie die Beratung von Unternehmen zu verschiedenen Fragen der IKT, so auch der IT-Sicherheit.

GCSOC

Global CSO Council

4616 Henry Street
Pittsburgh, PA 15213
USA

Status: private non-profit
Ebene: national
Sektor: Organisierte Interessen
(Einzel-)Mitglieder: 10
Jahr der Gründung: 2003

Korporative Mitglieder:
MS, Oracle

Think Tank, entstanden als Zusammenschluß von Chief Security Officers (CSOs) führender US-Organisationen aus Wirtschaft, Wissenschaft und öffentlicher Verwaltung. GCSOC beschäftigte sich mit Fragen der IT-Sicherheit aus betriebswirtschaftlicher Perspektive. Ziel war die Ausarbeitung einer einheitlichen Aufgaben- und Tätigkeitsdefinition für CSOs hinsichtlich der IT-Sicherheit in Organisationen sowie bei der Umsetzung der National Strategy to Secure Cyberspace. Das Sekretariat von GCSOC wurde vom CyLab der Carnegie Mellon University in Pittsburgh geführt. Seit Ende 2007 existiert die Web-Präsenz des GCSOC nicht mehr.

GI

Gesellschaft für Informatik

Ahrstraße 45
53175 Bonn
Deutschland

Status: mixed
Ebene: national
Sektor: Stiftungen/Vereine
Jahr der Gründung: 1969

Korporative Mitglieder:
BMVg, BSI, IBM, SAP, Siemens

Partner:
ICANN, IEEE, IFIP

Web:
<`http://www.gi-fb-sicherheit.de`>

Eingetragener deutscher Verein für Informatik, der einschlägige Fachpublikationen herausgibt, Konferenzen organisiert, Nachwuchswissenschaftler fördert und Stellungnahmen sowie Empfehlungen zur Technologiepolitik erarbeitet. Zu den korporativen Mitgliedern gehören Organisationen aus Wirtschaft und Wissenschaft sowie der öffentlichen Verwaltung. Im Jahr 2002 richtete die GI den Fachbereich „Sicherheit – Schutz und Zuverlässigkeit“ ein, innerhalb dessen sich eine Reihe von Fachgruppen mit verschiedenen Themen der IT-Sicherheit befaßt. Hierzu zählen u. a. Kryptographie, Biometrik, Datenschutz, eCommerce und elektronische Signaturen.

GILC

Global Internet Liberty Campaign

125 Broad Street
New York, NY 10004
USA

Status: private non-profit
Ebene: global
Sektor: Organisierte Interessen
Jahr der Gründung: 1996

Korporative Mitglieder:
ACLU, CCC, CDT, EFF, EPIC, ISOC, PI

Web: <`http://www.gilc.org`>

Auf dem ISOC-Jahrestreffen 1996 in Montreal gegründeter, internationaler Dachverband von Bürger- und Menschenrechtsorganisationen. GILC setzt sich auf globaler Ebene für Belange der Informationsfreiheit und des Datenschutzes ein und informiert im Internet über aktuelle Entwicklungen und Kampagnen.

GIP

Global Internet Project

1401 Wilson Boulevard
Arlington, VA 22209
USA

Status: private non-profit
Ebene: global
Sektor: Organisierte Interessen
Jahr der Gründung: 1996

Korporative Mitglieder:
IBM, ITAA, MS

Web: <`http://www.witsa.org/gip/`>

Initiative der World Information Technology and Services Alliance (WITSA), einer Interessenvereinigung von Verbänden der IT-Industrie aus 65 Ländern unter Führung der ITAA. Das beratende GIP Advisory Committee setzt sich aus Führungskräften großer asiatischer, europäischer und nordamerikanischer Unternehemen (u. a. Deutsche Bank, Deutsche Telekom, IBM, Fujitsu, Sony, Nokia und MS) zusammen. Ziel des GIP ist die Förderung eines wirtschaftsfreundlichen, selbstregulierten Internets. Vor diesem Hintergrund veranstaltet das GIP Workshops und veröffentlicht Publikationen und Präsentationen zu den Themenbereichen eCommerce, Web-Inhalte, Datenschutz, Sicherheit, Governance und Infrastrukturen.

GIPI

Global Internet Policy Initiative

1634 I Street NW
Washington, DC 20006
USA

Status: private non-profit
Ebene: global
Sektor: Organisierte Interessen
Jahr der Gründung: 2001

Korporative Mitglieder:
CDT

Web:
<`http://www.internetpolicy.net`>

Gemeinsame Initiative des CDT und des Medien-Netzwerkes Internews. Ziel ist eine Liberalisierung und Deregulierung der Rahmenbedingungen in Entwicklungs- und Schwellenländern, um eine globale Ausdehnung und weitgehend offene Nutznung des Internet zu fördern. GIPI unterhält Koordinationsbüros in 15 Ländern, die jeweils auf nationaler Ebene Vertreter aus Interessengruppen, Wirtschaft und Staat in Diskussionsforen und Ausbildungsprogrammen zusammenbringen. Finanziert wird GIPI durch Spenden verschiedener Stiftungen wie etwa der AOL Time-Warner Foundation und privater Unternehmen (bspw. MS), aber auch durch Zuwendungen der Weltbank, des US-Außenministeriums sowie der Europäischen Union.

HP

Hewlett-Packard

3000 Hanover Street
Palo Alto, CA 94304
USA

Status: private for-profit
Ebene: global
Sektor: Wirtschaft
Mitarbeiter: ca. 156.000
Jahr der Gründung: 1939

Partner:
Cisco, CSC, Oracle, SAP, Siemens, Symantec, UN

Web: <`http://www.hp.com`>

Von Absolventen der Stanford University gegründetes, börsennotiertes Unternehmen für Hardware. HP erzielte im Geschäftsjahr 2007 einen Umsatz von 104,3 Mrd. US-Dollar (<`http://hoovers.com`>) und belegte in der Forbes-Liste der weltweit größten Unternehmen den 55. Platz. Kerngeschäft des Unternehmens ist die Produktion von Hardware. HP bietet aber auch Beratungs- und Managementdienstleistungen für IT-Infrastrukturen sowie Lösungen für Identity/Access Management und Virtual Private Networks (VPN) an.

HTCIA

High Technology Crime Investigation Association

1474 Freeman Drive
Amissville, VA 20106
USA

Status: private non-profit
Ebene: global
Sektor: sektorübergreifende Foren
Jahr der Gründung: 1986

Web: <`http://www.htcia.org/`>

Gemeinnütziger Verein von Sicherheitsexperten aus Wirtschaft und Verwaltung zum Austausch von Informationen zur Aufklärung und Verhinderung von High-Tech-Straftaten. Die HTCPA ist in lokale Teilverbände gegliedert und beschränkt sich bis auf wenige Ausnahmen (UK, Europa) fast ausschließlich auf die USA.

I3P

Institute for Information Infrastructure Protection

45 Lyme Road
Hanover, NH 03755
USA

Status: mixed
Ebene: national
Sektor: Wissenschaft und Forschung
Jahr der Gründung: 2001

Korporative Mitglieder:
CERT/CC, RAND, SRI

Partner:
NIST, US-DHS

Web: <`http://www.thei3p.org`>

Arbeitsgemeinschaft von 24 privaten und öffentlichen Forschungseinrichtungen in den USA, deren Ziel eine landesweite Koordination von Forschungs- und Entwicklungsprojekten im Bereich des Schutzes der Informationsinfrastruktur ist. Zu den Mitgliedern gehören das SEI der Carnegie Mellon University (CERT/CC), RAND, SRI sowie mehrere Laboratorien des Massachusetts Institute of Technology (MIT). Finanziell unterstützt wird I3P durch das US-DHS und NIST.

IABG

Industrieanlagen-Betriebsgesellschaft

Einsteinstraße 20
85521 Ottobrunn
Deutschland

Status: private for-profit
Ebene: regional
Sektor: Wirtschaft
Mitarbeiter: ca. 1.000
Jahr der Gründung: 1961

Partner:
BMVg, BSI

Web: <`http://www.iabg.de`>

Von der Bundesrepublik Deutschland ursprünglich als Test- und Analyseeinrichtung für Luft- und Raumfahrt sowie Verteidigungstechnik gegründetes Unternehmen, das 1992 privatisiert wurde. Die IABG stellt ihren Kunden verschiedene Dienstleistungen im Bereich der IKT zur Verfügung, zu denen auch Planung und Betrieb von Informationsinfrastrukturen gehören. Das Unternehmen arbeitet mit verschiedenen Polizeibehörden, BMVg und BSI zusammen und ist europaweit tätig. Die IABG ist einer der Hauptinitiatoren von AKSIS.

IBM

International Business Machines

New Orchard Road
Armonk, NY 10504
USA

Status: private for-profit
Ebene: global
Sektor: Wirtschaft
Mitarbeiter: ca. 427.000
Jahr der Gründung: 1896

Partner:
Cisco, CSC, ISOC, McAfee, Oracle, Siemens, Symantec, VeriSign

Web: <`http://www.ibm.com`>

Börsennotiertes Hardware-Unternehmen, das 2007 einen Umsatz von 98,8 Mrd. US-Dollar erwirtschaftete (<`http://hoovers.com`>). Auf der Forbes-Liste der weltweit größten Unternehmen 2007 belegte IBM den 42. Platz. Unter der Bezeichnung „Tabulating Machine Company“ gegründet, wurde das Unternehmen 1924 in „International Business Machines“ umbenannt. Mit der Übernahme der Unternehmensberatungssparte von PwC im Jahr 2002 richtete IBM sich verstärkt auf Beratungsdienstleistungen aus. Das Unternehmen bietet auch Dienstleistungen im Bereich des IT-Sicherheitsmanagements an.

IC3

Internet Crime Complaint Center

1 Huntington Way
Fairmont, WV 26554
USA

Status: public
Ebene: national
Sektor: Staat/Öffentliche Verwaltung
Mitarbeiter: ca. 70
Jahr der Gründung: 2000

Korporative Mitglieder:
FBI, NW3C, US-DoJ

Partner:
BSA, FBI, FTC, MS

Web: <`http://www.ic3.gov`>

Unter der Bezeichnung „Internet Fraud Complaint Center“ (IFCC) eingerichtete Kooperation zwischen dem FBI und dem NW3C. Die Organisation sammelt Daten über Internetbetrugsfälle und andere elektronische Straftaten und wertet diese statistisch aus. Die gewonnenen Erkenntnisse werden den Strafverfolgungsbehörden zur Verfügung gestellt. IC3 dient als zentrale Anlauf- und Sammelstelle für Online-Anzeigen und leitet diese an die jeweils zuständigen Behörden weiter. Die gemeldeten Vorfälle gehen häufig über den reinen Straftatbestand des Betruges hinaus und umfassen u. a. auch unerlaubten Datenzugriff, Verletzungen des Urheberrechts, Erpressung, Spionage und andere Formen elektronischer Kriminalität. Um diesem Umstand Rechnung zu tragen, wurde das IFCC Ende 2003 in „Internet Crime Complaint Center“ (IC3) umbenannt.

ICANN

Internet Corporation for Assigned Names and Numbers

4676 Admiralty Way
Marina del Rey, CA 92092
USA

Status: private non-profit
Ebene: global
Sektor: Internationale Organisationen
Mitarbeiter: ca. 40
Jahr der Gründung: 1998

Partner:
GI, IETF, ISOC

Web: <`http://www.icann.org`>

Auf Initiative der US-Regierung als Nachfolgerin der Internet Assigned Numbers Authority (IANA) gegründete Organisation zur globalen Koordination der Adreßvergabe im Internet. ICANN ist für die technische Koordination des IP-Adreßraumes, des Top-Level DNS sowie der Root-Server-Systeme zuständig und trägt damit Verantwortung für große Teile der Infrastruktur des Internet. Im Direktorium der Organisation sitzen Vertreter aus verschiedenen Ländern. Dennoch wird ICANN international häufig hinsichtlich seiner Abhängigkeit vom US-Handelsministerium kritisiert.

ICC

International Chamber of Commerce

38 Cours Albert 1er
75008 Paris
Frankreich

Status: private non-profit
Ebene: global
Sektor: Organisierte Interessen
Jahr der Gründung: 1919

Korporative Mitglieder:
HP, IBM, MS, Oracle, PwC

Partner:
UN

Web: <`http://www.icc-ccs.org`>

Die internationale Handelskammer ICC wurde 1919 gegründet. Seit 1998 unterhält die in London ansässige Abteilung für Wirtschaftsstraftaten – Commercial Crimes Service (CCS) – eine Cybercrime Unit (CCU), welche Informationen über elektronische Sicherheitsvorfälle bei ICC-Mitgliedern sammelt, auswertet und weitergibt. Auch Warnungen vor möglichen Sicherheitslücken und die Aus- und Weiterbildung von Fachpersonal gehören zu den Aufgaben der CCU.

IDC

International Data Corporation

5 Speen Street
Framingham, MA 01701
USA

Status: private for-profit
Ebene: global
Sektor: Wirtschaft
Mitarbeiter: ca. 1.200
Jahr der Gründung: 1964

Web: <`http://www.idc.com`>

Auf Marktanalysen im IKT-Sektor spezialisiertes Unternehmen mit einem Jahresumsatz 2007 von 39,2 Mio. US-Dollar (<`http://hoovers.com`>). IDC ist ein in 50 Ländern tätiges Zweigunternehmen der International Data Group (IDG). Das Hauptgeschäftsfeld von IDC ist die Analyse von Entwicklungstrends in der IKT sowie ein darauf beruhendes Angebot von Beratungsdienstleistungen für Unternehmen.

iDEFENSE

Infrastructure Defense

1875 Campus Commons Drive
Reston, VA 20191
USA

Status: private for-profit
Ebene: global
Sektor: Wirtschaft
Mitarbeiter: ca. 50
Jahr der Gründung: 1998

Partner:
VeriSign

Web: <`http://labs.idefense.com`>

Privates Analyseunternehmen, das unter dem Namen „Infrastructure Forum“ gegründet wurde. Das Unternehmen analysiert und erforscht Gefahren, Bedrohungen und Sicherheitslücken im Bereich der IT-Infrastruktur und bietet entsprechende Informations- und Beratungsdienstleistungen an. Zu den Kunden gehören neben der öffentlichen Verwaltung auch mehrere Großunternehmen.

IEEE

Institute of Electrical and Electronics Engineers

1730 Massachusetts Avenue, NW
Washington, DC 20036–1992
USA

Status: private non-profit
Ebene: global
Sektor: Organisierte Interessen
(Einzel-)Mitglieder: ca. 370.000
Jahr der Gründung: 1963

Partner:
GI

Web: <`http://www.ieee.org`>

Internationaler Berufsverband für Fachleute aus dem Bereich der Elektrotechnik und Informatik. Das IEEE entstand 1963 durch Zusammenschluß des American Institute of Electrical Engineers (AIEE) und des Institute of Radio Engineers (IRE). Die Mitglieder des IEEE stammen aus über 175 Ländern. Das IEEE spielt vor allem bei der Definition von Standards der Informationsübertragung eine wichtige Rolle. Seit 2003 ist das IEEE Herausgeber der Zeitschrift IEEE Security & Privacy, in der regelmäßig Artikel zu Themen der Computersicherheit veröffentlicht werden.

IETF

Internet Engineering Task Force

1895 Preston White Drive
Reston, VA 20191–5434
USA

Status: private non-profit
Ebene: global
Sektor: sektorübergreifende Foren
Jahr der Gründung: 1986

Partner:
ICANN, ISOC

Web: <`http://www.ietf.org`>

Internationaler Zusammenschluß von IT-Experten, die beruflich oder privat an der Entwicklung technischer Standards für das Internet beteiligt sind. Zu den Zielen der IETF gehört die Identifikation technischer Probleme sowie die Ausarbeitung entsprechender Lösungsvorschläge. Die IETF beschäftigt sich vor allem mit der Spezifikation neuer Übertragungsprotokolle. Unter dem Dach der IETF arbeiten z. Z. insgesamt 17 Arbeitsgruppen zu sicherheitsrelevanten Themen.

IFIP

International Federation for Information Processing

Hofstraße 3
2361 Laxenburg
Österreich

Status: private non-profit
Ebene: global
Sektor: Stiftungen/Vereine
Jahr der Gründung: 1960

Partner:
GI, UN

Web: <`http://www.ifip.or.at`>

Internationaler Dachverband privater Vereine, die sich im Bereich Informationsverarbeitung engagieren. IFIP steht unter der Schirmherrschaft der UNESCO und in engem Kontakt mit fachlich einschlägigen UN-Organisationen. Alle zwei Jahre veranstaltet IFIP den Welt-Computer-Kongreß. Zur Zeit unterhält IFIP 13 technische Ausschüsse zu verschiedenen IT-Themen. Unter ihnen beschäftigt sich der Ausschuß 11 explizit mit der Sicherheit und dem Schutz von informationsverarbeitenden Systemen. Er gliedert sich gegenwärtig in acht Arbeitsgruppen: (1) Information Security Management, (2) Small System Security, (3) Data and Application Security, (4) Network Security, (5) Systems Integrity and Control, (6) Information Technology – Misuse and The Law, (7) Information Security Education sowie (8) Digital Forensics.

InfoSurance

InfoSurance

Badener Strasse 551
8048 Zürich
Schweiz

Status: mixed
Ebene: national
Sektor: Stiftungen/Vereine
Jahr der Gründung: 1999

Korporative Mitglieder:
MS, Siemens

Web: <`http://www.infosurance.ch`>

Schweizer Stiftung, deren Ziel die Förderung einer sicheren Informationsinfrastruktur ist. Dies soll vor allem durch eine Vernetzung von Entscheidungsträgern aus Wirtschaft, Wissenschaft und öffentlicher Verwaltung sowie ein erhöhtes allgemeines Risikobewußtsein erreicht werden. Zu den Trägern gehören u. a. die Schweizer Post sowie die Schweizer Bundesbahnen, Migros, MS, Symantec, UBS und der Genfer Flughafen.

InfraGard

InfraGard

935 Pennsylvania Avenue NW
Washington, DC 20535
USA

Status: mixed
Ebene: national
Sektor: sektorübergreifende Foren
(Einzel-)Mitglieder: ca. 9.000
Jahr der Gründung: 1996

Korporative Mitglieder:
FBI

Partner:
FBI, NIST

Web: <`http://www.infragard.net`>

Als Public-Private-Partnership konzipiertes Forum des FBI zum Schutz kritischer Infrastrukturen. InfraGard dient als Plattform des vertraulichen Informationsaustauschs zwischen dem FBI, der Wirtschaft, der Wissenschaft sowie anderen Strafverfolgungsbehörden auf nationaler und lokaler Ebene. Hierzu unterhält InfraGard mehrere lokale Verbindungsbüros. Unter der Ägide des NIPC, in dessen Zuständigkeit Infragard von 1998 bis 2003 fiel, lag der Schwerpunkt zunächst im Bereich kritischer Informationsinfrastrukturen. In Folge der Terroranschläge des 11. September 2001 verlagerte sich der Fokus von InfraGard vermehrt auf den Schutz physischer Infrastrukturen. Seit dem Ausscheiden des NIPC aus dem FBI im Zuge der Neugründung des US-DHS 2003 ist InfraGard Teil der Cyber Division. InfraGard unterhält in Zusammenarbeit mit der US Small Business Administration (SBA), dem National Center for Manufacturing Sciences (NCMS) sowie NIST ein Security Workshop Program für KMU.

ISA

Internet Security Alliance

2500 Wilson Boulevard
Arlington, VA 22201
USA

Status: private non-profit
Ebene: national
Sektor: Organisierte Interessen
Jahr der Gründung: 2001

Korporative Mitglieder:
IBM, RedSiren, Symantec, VeriSign

Partner:
CERT/CC

Web: <`http://www.isalliance.org`>

Vom CERT/CC in Kooperation mit der Electronic Industries Alliance (EIA) initiierter, beitragsfinanzierter Unternehmensverband. Die ISA vertritt die Interessen ihrer Mitglieder in Gesetzgebungs- und Regulierungsverfahren und dient als Forum des Informationsaustauschs in Fragen der IT-Sicherheit. Die Mitglieder erhalten aktuelle Warnungen des CERT/CC gegen eine Gebühr unmittelbar und ohne die sonst übliche Verzögerungsfrist. Ferner unterhält ISA eigene Forschungsprojekte zu grundlegenden Problemen in der IT-Sicherheit und führt Weiterbildungsseminare zu Themen wie Risk Assessment und Information Assurcance durch. Im Jahr 2002 gab ISA als Empfehlung ein Kompendium von 10 Sicherheitsrichtlinien für Führungskräfte heraus.

ISACA

Information Systems Audit and Control Association

3701 Algonquin Road
Rolling Meadows, IL 60008
USA

Status: private non-profit
Ebene: global
Sektor: Organisierte Interessen
(Einzel-)Mitglieder: ca. 35.000
Jahr der Gründung: 1969

Partner:
ASIS, ISSA

Web: <`http://www.isaca.org`>

Ursprünglich unter dem Namen „EDP Auditors Association“ gegründeter, internationaler Berufsverband von IT-Fachleuten mit Zweigstellen in über 60 Ländern. ISACA führt Aus- und Weiterbildungsprogramme für EDV-Revisoren durch und vergibt das Abschlußzertifikat eines „Certified Information Systems Auditor“ (CISA). Seit 2002 tritt daneben ein „Certified Information Security Manager“ (CISM) genanntes Zertifikat, das speziell auf Probleme der IT-Sicherheit ausgerichtet ist. Der Verband unterhält eine Stiftung zur Forschungsförderung. Anfang 2005 gaben ASIS, ISACA und ISSA die Gründung einer gemeinsamen Allianz zur Entwicklung von Strategien für ein ganzheitliches Sicherheitsmanagement in Unternehmen bekannt.

ISF

Information Security Forum

Southwark Towers
32 London Bridge Street
London SE1 9SY
UK

Status: private non-profit
Ebene: global
Sektor: sektorübergreifende Foren
Jahr der Gründung: 1989

Korporative Mitglieder:
(ISC)2, BSI, IBM, MS, NHTCU, PwC, SAP, Siemens, Symantec, VeriSign

Web: <`http://www.securityforum.org`>

Internationaler Verband von gegenwärtig 306 Organisationen aus dem privaten und öffentlichen Sektor zur Forschungsförderung und -kooperation im Bereich der IT-Sicherheit. Seinen Mitgliedern stellt das ISF in verschiedenen Projekten gewonnenen Erkenntnisse in Publikationen zur Verfügung. Themen sind hier u. a. Identity/Access Management, Incident Management, Information Risk Analysis, Information Security Governance, Malware Protection und Network Security. Ferner organisiert das ISF Arbeitsgruppen und Konferenzen zu verschiedenen Sicherheitsthemen.

ISO

International Organization for Standardization

1, rue de Varembé
Case postale 56
1211 Geneva 20
Schweiz

Status: mixed
Ebene: global
Sektor: Internationale Organisationen
Jahr der Gründung: 1946

Web: <`http://www.iso.org`>

Von der UNO gegründete Organisation zur Angleichung internationaler Standards. Neben der International Telecommunication Union (ITU) eine der wichtigsten internationalen Standardisierungsorganisationen im Bereich elektronischer Sicherheit. Zusammen mit der International Electrotechnical Commission (IEC) ist die ISO für die Normen ISO/IEC 27001:2005 und ISO/IEC 27002:2005 verantwortlich, die Maßnahmen im Bereich des Informationssicherheits-Managements spezifizieren.

ISOC

Internet Society

1775 Wiehle Avenue
Reston, VA 20190
USA

Status: private non-profit
Ebene: global
Sektor: sektorübergreifende Foren
(Einzel-)Mitglieder: ca. 20.000
Jahr der Gründung: 1992

Korporative Mitglieder:
IETF

Partner:
IBM, ICANN, IETF, MS, NSA

Web: <`http://www.isoc.org`>

Internationale Vereinigung von Organisationen und Fachleuten der IT-Branche aus über 180 Ländern. ISOC ist für grundlegende Fragen der technischen Weiterentwicklung des Internet zuständig und dient als Dachverband für Standardisierungsorganisationen wie das IETF. ISOC unterstützt das jährlich stattfindende Network and Distributed System Security Symposium (NDSS), eine Konferenz, auf der sich Sicherheitsexperten aus privatem und öffentlichem Sektor zu technischen Fragen der Netzwerksicherheit austauschen. Bisherige NDSS-Konferenzen wurden u. a. von der NSA, IBM und MS gefördert.

ISPAB

Information Security and Privacy Advisory Board

Status: mixed
Ebene: national
Sektor: sektorübergreifende Foren
(Einzel-)Mitglieder: 13
Jahr der Gründung: 1987

Partner:
MS, NIST, NSA

Web: <`http://csrc.nist.gov/ispab`>

Auf Grundlage des Computer Security Act von 1987, ursprünglich unter der Bezeichnung „Computer System Security and Privacy Advisory Board“ (CSSPAB) eingerichtetes, im Jahr 2002 in ISPAB umbenanntes US-amerikanisches Gremium aus Vertretern des öffentlichen und privaten Sektors. Aufgabe des ISPAB ist die Analyse von Sicherheits- und Datenschutzmängeln in den Informationssystemen der öffentlichen Verwaltung. Das Gremium berät NIST, das Handelsministerium, das Office of Management and Budget, die NSA sowie verschiedene Kongreßausschüsse zu Fragen der Sicherheit und des Datenschutzes in Informationssystemen. Das ISPAB ist NIST und dem US-Handelsministerium zugeordnet.

ISS

Internet Security Systems

6303 Barfield Road
Atlanta, GA 30328
USA

Status: private for-profit
Ebene: global
Sektor: Wirtschaft
Mitarbeiter: ca. 1.250
Jahr der Gründung: 1994

Partner:
RedSiren

Web: <`http://www.iss.net`>

Börsennotiertes Unternehmen, das Software zum Schutz elektronischer Netze anbietet. ISS erwirtschaftete 2007 einen Jahresumsatz von 127,2 Mio. US-Dollar (<`http://hoovers.com`>) und unterhält über 35 Niederlassungen in 20 Ländern. Die Produktpalette umfaßt Software für Intrusion Prevention und Detection, Vulnerability Assessment sowie Web- und Mail-Filter. Daneben engagiert sich ISS auch im Bereich des Informationssicherheitsmanagements. Im Jahr 2006 wurde ISS von IBM übernommen.

ISSA

Information Systems Security Association

7044 South 13th Street
Oak Creek, WI 53154
USA

Status: private non-profit
Ebene: global
Sektor: Organisierte Interessen
(Einzel-)Mitglieder: ca. 13.000
Jahr der Gründung: 1984

Partner:
ASIS, BSA, CSI, ISACA, MS

Web: <`http://www.issa.org`>

Internationaler Berufsverband für Fachleute aus dem Bereich IT-Sicherheit mit mehr als 10.000 Mitgliedern in über 100 Ländern. Die ISSA organisiert regelmäßige Konferenzen, gibt ein monatliches Journal sowie weitere Fachpublikationen heraus und bietet zertifizierte Fortbildungsseminare für IT-Sicherheitsexperten an. Zu den Sponsoren der ISSA zählt u. a. das CSI. Anfang 2005 gaben ASIS, ISACA und ISSA die Gründung einer gemeinsamen Allianz bekannt. Eine weitere Allianz ging der Verband 2006 mit MS ein.

ITAA

Information Technology Association of America

1401 Wilson Boulevard
Arlington, VA 22209
USA

Status: private non-profit
Ebene: national
Sektor: Organisierte Interessen
Jahr der Gründung: 1961

Korporative Mitglieder:
Cisco, CSC, HP, IBM, McAfee, MI, MS, SAP, Symantec, VeriSign

Web: <`http://www.itaa.org`>

US-Interessenverband der IT-Industrie. ITAA wurde ursprünglich unter dem Namen „Association of Data Processing Service Organizations“ (ADAPSO) gegründet. Die ITAA unterhält u. a. ein Homeland Security Committee, ein InfoSec Committee sowie einen Intellectual Property Counsels Roundtable. Im Rahmen dieser Gremien tauschen sich Unternehmen in regelmäßigen Abständen zu verschiedenen Fragen der IT-Sicherheit aus und stimmen gemeinsame Politiken und Strategien ab.

IT-ISAC

Information Technology Information Sharing and Analysis Center

227 Sandy Springs Place
Sandy Springs, GA 30328
USA

Status: private non-profit
Ebene: national
Sektor: sektorübergreifende Foren
Jahr der Gründung: 2001

Korporative Mitglieder:
Cisco, CSC, HP, IBM, McAfee, MS, Oracle, RSA, Symantec, VeriSign

Partner:
NIAC, US-DHS

Web: <`https://www.it-isac.org`>

Im Jahr 1998 forderte US-Präsident Clinton in einer Richtlinie (PDD 63) die Einrichtung von Information Sharing and Analysis Centers (ISAC) in den privaten, kritischen Infrastruktursektoren, so auch dem IT-Sektor. Diese ISACs sollten als Schnittstelle zwischen dem neu eingerichteten NIPC und dem privaten Sektor fungieren. Anfang 2001 schlossen sich 19 private Unternehmen der Soft- und Hardwarebranche zum IT-ISAC Verbund zusammen. IT-ISAC finanziert sich aus Beiträgen seiner Mitglieder.

McAfee

McAfee

3965 Freedom Circle
Santa Clara, CA 95054
USA

Status: private for-profit
Ebene: global
Sektor: Wirtschaft
Mitarbeiter: ca. 3.300
Jahr der Gründung: 1989

Partner:
Cisco, IBM, MS, RedSiren

Web: <`http://www.mcafee.com`>

Börsennotiertes Unternehmen für Sicherheitssoftware mit einem Jahresumsatz 2006 von 1,2 Mrd. US-Dollar (<`http://hoovers.com`>). McAffee begann 1989 als Anbieter von Anti-Viren-Programmen. Bereits seit 1986 existierte ein gleichnamiges Shareware-Programm. Nach und nach erweiterte McAfee seine Produktpalette um zusätzliche Sicherheitssoftware. Im Jahr 1997 erfolgte unter dem Namen „Network Associates Incorporated“ (NAI) eine Fusion mit Network General, einem Hersteller von Software für Netzwerkmanagement. Kurz darauf ergänzte NAI mit der Übernahme von Pretty Good Privacy (PGP) sein Angebot auch um Kryptographie-Software. Seit 2002 ist PGP jedoch wieder eigenständig. Weitere Übernahmen waren der Firewall-Hersteller Trusted Information Systems (TIS) sowie der Anti-Viren-Hersteller Dr. Solomon. Nach Verlusten und einer daraus resultierenden Umstrukturierung des Unternehmens nennt sich NAI seit 2004 erneut McAfee und konzentriert sich wieder vermehrt auf sein ursprüngliches Kerngeschäft im Bereich der IT-Sicherheit.

MI

McConnell International

1301 K Street NW
Washington, DC 20005
USA

Status: private for-profit
Ebene: global
Sektor: Wirtschaft
Jahr der Gründung: 2000

Web: <`http://www.mcconnellinternational.com`>

Vom vormaligen Direktor des International Year 2000 Cooperation Centers (IY2KCC), Bruce W. McConnell, gegründetes, privates Beratungsunternehmen. Das IY2KCC wurde 1999 unter der Schirmherrschaft der UNO errichtet und durch die Weltbank finanziert. Es sollte im internationalen Rahmen eine verstärkte Kooperation des öffentlichen und privaten Sektors zur Bewältigung des Y2K-Problems fördern. Aus dieser Zeit stammende nationale und internationale Kontakte zu Regierungsstellen nutzt McConnell für seine Klienten. MI veröffentlichte eine Reihe von Studien im Bereich der Technologiepolitik, darunter einen vergleichenden Bericht über die Cybercrime-Gesetzgebung in 52 Ländern.

MS

Microsoft

1 Microsoft Way
Redmond, WA 98052–6399
USA

Status: private for-profit
Ebene: global
Sektor: Wirtschaft
Mitarbeiter: ca. 93.000
Jahr der Gründung: 1975

Partner:
Cisco, CSC, Cybertrust, IC3, ISOC, ISPAB, ISSA, McAfee, Oracle, RedSiren, RSA, Siemens, Solutionary, Symantec, VeriSign

Web: <`http://www.microsoft.com`>

Börsennotiertes Software-Unternehmen. MS erzielte im Geschäftsjahr 2007 einen Jahresumsatz von 51,1 Mrd. US-Dollar (<`http://hoovers.com`>). Auf der Forbes-Liste der weltweit größten Unternehmen belegte MS 2007 den 66. Platz. Hauptgeschäftsfeld ist der Vertrieb des Betriebssystems „Windows“ sowie verschiedener Anwendungsprogramme. Durch den hohen Verbreitungsgrad von „Windows“ ziehen dessen Sicherheitslücken verstärkt Angriffe auf sich und stellen damit ein erhöhtes Sicherheitsrisiko in elektronischen Netzen dar. Zusammen mit dem US-DoJ schrieb MS daher Preisgelder für Informationen zur Ergreifung von Hackern aus.

NCSA

National Cyber Security Alliance

1150 18th Street NW
Washington, DC 20036
USA

Status: mixed
Ebene: national
Sektor: sektorübergreifende Foren
Jahr der Gründung: 2002

Korporative Mitglieder:
(ISC)2, ASIS, BSA, Cisco, CSIA, FTC, HP, InfraGard, ISS, ITAA, IT-ISAC, McAfee, MS, RSA, Symantec, US-DHS

Web:
<`http://www.staysafeonline.org`>

Kooperation des US-DHS und der FTC mit Organisationen des privaten Sektors, deren Ziel eine Sensibilisierung von Privatnutzern, Ausbildungseinrichtungen und Kleinunternehmen für Themen der Computersicherheit ist. Die NCSA führt Informations- und Ausbildungskampagnen durch. Förderer der NCSA sind u. a. ASIS, BSA, CSIA, HP, InfraGard, ISA, ISS, ITAA, IT-ISAC, McAfee, Microsoft, RSA und Symantec.

NCSP

National Cyber Security Partnership

Status: mixed
Ebene: national
Sektor: sektorübergreifende Foren
Jahr der Gründung: 2003

Korporative Mitglieder:
BSA, ITAA, TechNet

Web:
<`http://www.cyberpartnership.org`>

In Folge der US National Strategy to Secure Cyberspace gegründete Arbeitsgemeinschaft unter der Führung von ITAA, BSA, TechNet und US-Handelskammer, an der sich Vertreter aus Wissenschaft, Wirtschaft und US-Bundesverwaltung beteiligten. NCSP setzte sich aus fünf Arbeitsgruppen zu den Themen allgemeines Risikobewußtsein, Frühwarnsysteme, Corporate Governance, Sofware-Entwicklung und technische Standards zusammen, die jeweils in ihrem Bereich Vorschläge und Strategien zur Verbesserung der IT-Sicherheit erarbeiteten und diese im Internet publizierten. Seit Vorstellung der Ergebnisse wurde die Arbeitsgruppe nicht mehr aktiv. Auch die Web-Seite existierte nur bis Anfang 2008.

NHTCU

National High-Tech Crime Unit

PO Box 10101
London E14 9NF
UK

Status: public
Ebene: national
Sektor: Staat/Öffentliche Verwaltung
Jahr der Gründung: 2001

Web: <`http://www.nhtcu.org`>

Zentrale britische Strafermittlungs- und -verfolgungsbehörde für Computerkriminalität. Die Gründung der NHTCU erfolgte aufgrund der 2000 vom britischen Innenmenister vorgestellten National High-Tech Crime Strategy im April 2001 als Teil des seit 1998 bestehenden National Crime Squad (NCS).

NIAC

National Infrastructure Advisory Council

Status: mixed
Ebene: national
Sektor: Staat/Öffentliche Verwaltung
(Einzel-)Mitglieder: ca. 30
Jahr der Gründung: 2001

Partner:
IT-ISAC, US-DHS

Web: <`http://www.dhs.gov/niac`>

Beratungsgremium, dessen Mitglieder sowohl aus dem privaten als auch öffentlichen Sektor kommen und direkt vom US-Präsidenten ernannt werden. NIAC berät die US-Administration bezüglich kritischer Infrastrukturen und deren Informationssystemen. Das Gremium koordiniert u. a. die Tätigkeit der Information Sharing and Analysis Center (ISACs) in den verschiedenen kritischen Infrastruktursektoren, so auch des IT-ISAC. Seit 2003 ist das NIPC nicht mehr direkt dem Präsidenten sondern dem US-DHS zugeordnet.

NIPC

National Infrastructure Protection Center

935 Pennsylvania Avenue NW
Washington, DC 20535–0001
USA

Status: public
Ebene: national
Sektor: Staat/Öffentliche Verwaltung
Jahr der Gründung: 1998

Partner:
FBI, US-DHS

Von US-Präsident Clinton aufgrund des Abschlußberichts (Marsh-Report) der President's Commission on Critical Infrastructure Protection (PCCIP) unter dem Dach des FBI eingerichtete Zentralstelle zur Analyse, Verfolgung und Aufklärung von – sowie zur Warnung vor – Angriffen in Computernetzwerken. Im Jahr 2003 ging das NIPC, bis auf die Abteilung für Computerermittlungen, im neugegründeten US-DHS auf. Das NIPC legte 2000 und 2001 Gutachten zu Gefahrenpotentialen im Bereich des eCommerce vor.

NIST

National Institute of Technology

100 Bureau Drive
Gaithersburg, MD 20899–1070
USA

Status: public
Ebene: national
Sektor: Staat/Öffentliche Verwaltung
Mitarbeiter: ca. 3.000
Jahr der Gründung: 1901

Partner:
I3P, InfraGard, ISPAB, NSA

Web: <`http://csrc.nist.gov`>

Aus dem National Bureau of Standards (NBS) hervorgegangene Organisation, die dem US-Handelsministerium untersteht und mit der Entwicklung technischer Normen und Standards betraut ist, jedoch nicht die weitgehenden Aufsichtskompetenzen einer Regulierungsbehörde besitzt. Gemäß dem Computer Security Act von 1987 fallen in den Zuständigkeitsbereich des NIST alle nicht-militärischen Standards der IT-Sicherheit. Hierzu gehören u. a. die Federal Information Processing Standards (FIPS) der öffentlichen Verwaltung. Seit dem Federal Information Security Management Act (FISMA) von 2002 kommt dem NIST hier besondere Bedeutung zu. Die Organisation entwarf u. a. die krytographischen Verfahren DES und AES, die auch im privaten Sektor weit verbreitet sind. Im Rahmen der National Information Assurance Partnership (NIAP) kooperiert das NIST mit der NSA. Die Organisation unterhält eine spezielle Computer Security Devision (CSD).

NSA

National Security Agency

Fort Meade, MD
USA

Status: public
Ebene: global
Sektor: Staat/Öffentliche Verwaltung
Jahr der Gründung: 1952

Partner:
FBI, ISOC, ISPAB, NIST, US-DHS, US-DoD, US-DoJ

Web: <`http://www.nsa.gov/ia/`>

Von US-Präsident Harry S. Truman im Verantwortungsbereich des US-DoD gegründete Behörde für elektronische Auslandsaufklärung. Die NSA ist gegenwärtig der größte US-Geheimdienst. Zu ihren Kernaufgaben gehörte von Anfang an die Sicherstellung einer vertraulichen Kommunikation der US-Regierung. Besonders in den letzten Jahren wurde dieser Aufgabenbereich immer mehr auf den Schutz der Nationalen Informationsinfrastruktur (NII) insgesamt ausgedehnt, so daß die NSA heute in der Überwachung des Internet eng mit dem FBI kooperiert. Gerechtfertigt wird die zunehmende Tätigkeit der NSA auch innerhalb der USA selbst gegenüber der Öffentlichkeit mit der besonderen Charakteristik elektronischer Netze, welche eine Trennung zwischen In- und Ausland erschwere. Innerhalb der NSA ist das Information Assurance Directorate (IAD) für den Schutz der NII zuständig. Im Rahmen der National Information Assurance Partnership (NIAP) arbeitet die NSA mit NIST zusammen.

NSC

National Security Council

The White House
Washington, DC
USA

Status: public
Ebene: national
Sektor: Staat/Öffentliche Verwaltung
(Einzel-)Mitglieder: 6
Jahr der Gründung: 1947

Korporative Mitglieder:
CIA, US-DoD

Web:
<`http://www.whitehouse.gov/nsc/`>

Gremium, das den US-Präsidenten in nationalen Sicherheitsfragen berät. Reguläre Mitglieder sind neben dem Präsidenten der Vizepräsident, die Minister des Äußeren, der Finanzen, der Verteidigung sowie der nationale Sicherheitsberater des Präsidenten. Das Gremium wird ferner beraten durch den Chef der vereinigten Generalstäbe und den Direktor der CIA. Bei Bedarf werden weitere Fachleute hinzugezogen.

NSF

National Science Foundation

4201 Wilson Boulevard
Arlington, VA 22230
USA

Status: public
Ebene: national
Sektor: Stiftungen/Vereine
Mitarbeiter: ca. 1.300
Jahr der Gründung: 1950

Web: <`http://www.nsf.gov`>

Unabhängige US-Bundesstiftung. Aufgabe der NSF ist die Förderung von Wissenschaft und Forschung in den USA. Die NSF entscheidet über die Vergabe von Fördergeldern sowohl für Grundlagen- als auch für angewandte Forschung. Im Bereich Computer and Information Science and Engineering (CISE) förderte die NSF bisher u. a. Projekte zu den Themen Trusted Computing (Datenschutz und Datensicherheit) und Cyber Trust (Netzwerksicherheit).

NW3C

National White Collar Crime Center

7401 Beaufont Springs Drive
Richmond, VA 23225–5504
USA

Status: public
Ebene: national
Sektor: Stiftungen/Vereine
Mitarbeiter: ca. 150
Jahr der Gründung: 1992

Partner:
FBI, SCI, US-DoJ

Web: <`http://www.nw3c.org`>

Aus dem Projekt „Leviticus“ hervorgegangene, vom US-Justizministerium finanzierte Organisation. NW3C unterstützt landesweit mit Ausbildungsprogrammen US-Behörden, die sich mit der Vorbeugung, Aufkärung oder Verfolgung von Wirtschafts- und High-Tech-Straftaten befassen. Seit 1995 betreibt die Organisation ein eigenes Forschungszentrum. Im Rahmen der National Cybercrime Training Partnership (NCTP) bemühte sich das NW3C vermehrt um eine stärkere Vernetzung von privaten und öffentlichen Akteuren. Das NW3C unterhält in Zusammenarbeit mit dem FBI das IC3.

OECD

Organisation for Economic Co-operation and Development

2, rue André Pascal
75775 Paris Cedex 16
Frankreich

Status: public
Ebene: global
Sektor: Internationale Organisationen
Jahr der Gründung: 1961

Partner:
APEC

Web: <`http://www.oecd.org`>

Aus der Organisation for European Economic Co-operation (OEEC) hervorgegangene internationale Organisation mit derzeit 30 Mitgliedsstaaten. Ziel der OECD ist die Förderung einer umfangreichen wirtschaftlichen Zusammenarbeit ihrer Mitglieder auf freiwilliger Basis (Einstimmigkeitsprinzip). Die OECD untergliedert sich in Direktorate zu verschiedenen Sachthemen. Dem Directorate for Science, Technology and Industry (STI) ist ein Ausschuß für Information-, Computer and Communications Policy (ICCP) unterstellt, innerhalb dessen sich eine Working Party on Information Security and Privacy (WPISP) explizit mit Themen des Datenschutzes und der Informationssicherheit befaßt. Die OECD verabschiedete eine Reihe einschlägiger Richtlinien, so etwa zum Datenschutz (1980) sowie zur Sicherheit von Informationssystemen (1992), zum Umgang mit Kryptographie (1997) und für eine „Kultur der Sicherheit“ in IT-Netzwerken (2002). Ferner organisiert die OECD weitere Foren, u. a. in enger Zusammenarbeit mit der APEC.

Oracle

Oracle

500 Oracle Parkway
Redwood City, CA 94065
USA

Status: private for-profit
Ebene: global
Sektor: Wirtschaft
Mitarbeiter: ca. 74.700
Jahr der Gründung: 1979

Partner:
Cisco, CSC, HP, IBM, MS, Siemens, VeriSign

Web: <`http://www.oracle.com`>

Börsennotiertes Unternehmen für Software im Bereich Datenbanken und Informationsmanagement. Oracle erzielte 2007 einen Jahresumsatz von 18,0 Mrd. US-Dollar (<`http://hoovers.com`>) und belegte auf Forbes-Liste der weltweit größten Unternehmen den 205. Platz. Im Jahr 2005 übernahm Oracle neben PeopleSoft, einem seiner größten Konkurrenten, auch Oblix, ein Unternehmen für Sicherheitssoftware im Bereich Identitätsmanagement.

PCIPB

President's Critical Infrastructure Protection Board

Status: public
Ebene: national
Sektor: Staat/Öffentliche Verwaltung
(Einzel-)Mitglieder: ca. 25
Jahr der Gründung: 2001

Von US-Präsident George W. Bush 2001 etabliertes und 2003 im Zuge der Neugründung des US-DHS wieder aufgelöstes Gremium aus hohen Regierungsbeamten, deren Aufgabe die Koordination von Maßnahmen zum Schutz kritischer Infrastrukturen war. Der Vorsitzende des PCIPB, Richard Clarke, war zugleich Sonderberater des Präsidenten für Cyber Space Security. Von den Medien wurde er daher als „Cyber-Zar“ tituliert. Im Jahr 2002 veröffentlichte das PCIPB die National Strategy to Secure Cyberspace, welche die besondere Bedeutung von Public-Private-Partnerships hervorhebt.

PI

Privacy International

6–8, Amwell Street
London EC1R 1UQ
UK

Status: private non-profit
Ebene: global
Sektor: Organisierte Interessen
Jahr der Gründung: 1990

Korporative Mitglieder:
EPIC

Web: <`http://www.privacyinternational.org`>

Unabhängige, internationale Bürgerrechtsorganisation, die sich mit Themen des Datenschutzes und der Informationsfreiheit befaßt. PI wurde von privaten Interessengruppen aus über 40 Ländern gegründet. Die Organisation verfolgt internationale Politikentwicklungen, bspw. in der EU, dem Europarat oder der UN, und informiert über mögliche Folgen für Datenschutz und Informationsfreiheit. Auch Lobbying und politische Kampagnen gehören zu ihrem Tätigkeitsfeld.

PwC

PricewaterhouseCoopers International

1177 Avenue of the Americas
New York, NY 10036
USA

Status: private for-profit
Ebene: global
Sektor: Wirtschaft
Mitarbeiter: ca. 146.800
Jahr der Gründung: 1998

Web: <`http://www.pwcglobal.com`>

Aus dem Zusammenschluß von Price Waterhouse und Coopers & Lybrand hervorgegangenes, privates Beratungs- und Wirtschaftsprüfungsunternehmen mit einem Jahresumsatz 2007 von 25,2 Mrd. US-Dollar (<`http://hoovers.com`>). PwC bietet Beratungsleistungen im Bereich Informationssicherheit an, welche die Bewertung von Risiken und Sicherheitslücken, Konzepte für ein Sicherheitsmanagement sowie die schnelle Hilfe in Notfällen umfassen. PwC erarbeitete im Rahmen des Global Security Consortium (GSC) zusammen mit Ernst & Young, Deloitte & Touche, KPMG International und AIG International einen Index zur einheitlichen Bewertung von IT-Risiken in Großunternehmen.

RAND

RAND

1776 Main Street
Santa Monica, CA 90401-3208
USA

Status: private non-profit
Ebene: global
Sektor: Wissenschaft und Forschung
Mitarbeiter: ca. 1.600
Jahr der Gründung: 1945

Partner:
EC, FBI, US-DHS, US-DoD, US-DoJ

Web: <`http://www.rand.org`>

Unter Aufsicht der Douglas Aircraft Company eingerichtete Kooperation von Wissenschaft, Wirtschaft und US-Militär in Forschung und Entwicklung, dessen Bezeichnung als Akronym aus „Research ANd Development“ entstand. Seit 1948 ist RAND ein organisationell eigenständiger, unabhängiger Think Tank, der mittlerweile auch Niederlassungen in Europa (Leiden und Berlin) unterhält. RAND finanziert sich zu einem Großteil aus Spenden und Stiftungen. Ursprünglich beschäftigte sich die Organisation hauptsächlich mit Fragen, die für die nationale Sicherheit der USA von besonderer strategischer Bedeutung waren. Schrittweise wurde der Fokus allerdings auch auf weitere, gesamtgesellschaftlich relevante Themenbereiche ausgeweitet. RAND führte u. a. umfangreiche Forschungsarbeiten zur strategischen Informationskriegsführung (Strategic Information Warfare) durch.

RedSiren

RedSiren

650 Smithfield Street
Pittsburgh, PA 15222
USA

Status: private for-profit
Ebene: global
Sektor: Wirtschaft
Jahr der Gründung: 1999

Partner:
Cisco, ISS, McAfee, MS, RSA

Web: <`http://www.redsiren.com`>

Privates Unternehmen, das Dienstleistungen im Bereich des Sicherheitsmanagements von IT-Infrastrukturen anbietet (MSSP). Hierzu zählt vor allem der Aufbau und die Überwachung von Firewalls sowie IDS-Lösungen. RedSiren übernahm seit seiner Gründung eine Reihe weiterer Firmen, so etwa die Ableger des Carnegie Mellon Institute – Secure360 – und des Stanford Research Institute (SRI) – AtomicTangerine. Das Unternehmen betreibt das International Information Integrity Institute (I-4), ein von SRI gegründetes, vertrauliches Forum zum Austausch sicherheitsrelevanter Informationen. Anfang 2005 wurde RedSiren von dem niederländischen IT-Unternehmen Getronics übernommen.

RSA

RSA Security

174 Middlesex Turnpike
Bedford, MA 01730
USA

Status: private for-profit
Ebene: global
Sektor: Wirtschaft
Mitarbeiter: ca. 1.300
Jahr der Gründung: 1989

Partner:
Cisco, CSC, Cybertrust, MS, RedSiren

Web: <`http://www.rsasecurity.com`>

Börsennotiertes Unternehmen mit einem Jahresumsatz 2007 in Höhe von 141,9 Mio. US-Dollar (<`http://hoovers.com`>). RSA bietet Soft- und Hardware für Identitäts- und Zugriffsmanagement sowie sichere Transaktionsverbindungen an. Das Unternehmen ist jährlich Veranstalter der weltweit beachteten RSA-Konferenzen, auf denen sich Fachleute aus Wirtschaft, Politik und Wissenschaft zum Informationsaustausch über aktulle Sicherheitsthemen und Technologietrends treffen. RSA wurde 1989 unter dem Namen RSA Data Security gegründet und 1996 von Security Dynamics übernommen. Im Jahr 1999 verschmolzen dann beide zu RSA Security. Der Firmenname geht auf den gleichnamigen Krytopgraphiealgorithmus zurück, der von den RSA-Gründern (Rivest, Shamir und Adleman) im Jahre 1977 entwickelt wurde und heute de facto einen Standard für asymmetrische Verschlüsselungsverfahren darstellt.

SANS

SysAdmin/Audit/Network/Security Institute

4610 Tournay Road
Bethesda, MD 20816
USA

Status: private non-profit
Ebene: global
Sektor: Wissenschaft und Forschung
Jahr der Gründung: 1989

Web: <`http://www.sans.org`>

Forschungs- und Ausbildungsinstitut, das sich auf die Sicherheit von IKT-Systemen mit Schwerpunkt im Bereich Intrusion Detection konzentriert. SANS stützt sich dabei vor allem auf die Erfahrung von Spezialisten aus der Praxis. Das Institut vergibt nach bestandenem Ausbildungsprogramm ein „Global Information Assurance Certification“ (GIAC) genanntes Zertifikat und stellt im Internet umfangreiche Materialien zum Thema Informationssicherheit zur Verfügung. Daneben betreibt SANS mit dem Internet Storm Center ein Frühwarnsystem, welches weltweit und zeitnah die aktuelle Bedrohungslage im Internet analysiert und statistisch aufbereitet.

SAP

SAP

Neurottstraße 16
69190 Walldorf
Deutschland

Status: private for-profit
Ebene: global
Sektor: Wirtschaft
Mitarbeiter: ca. 32.800
Jahr der Gründung: 1972

Partner:
CSC, HP, Siemens

Web: <`http://www.sap.com`>

Von fünf ehemaligen IBM-Mitarbeitern gegründetes, börsennotiertes Unternehmen. Hauptgeschäft ist die Entwicklung und der Vertrieb von Software zur Abbildung unternehmensinterner Geschäftsprozesse. Der Name „SAP“ steht für „Systeme, Anwendungen und Produkte in der Datenverarbeitung“. Im Geschäftsjahr 2006 betrug der Umsatz von SAP 12,4 Mrd. US-Dollar (<`http://hoovers.com`>). Auf der Forbes-Liste der weltweit größten Unternehmen 2007 belegt SAP den 357. Platz.

SCI

Southeast Cybercrime Institute

1000 Chastain Road 3301
Kennesaw, GA 30144
USA

Status: public
Ebene: national
Sektor: Wissenschaft und Forschung
Jahr der Gründung: 2001

Partner:
FBI, NW3C

Web: <`http://www.kennesaw.edu/coned/sci/`>

Institut an der Kennesaw State University, das Kurse zur Computer-Forensik anbietet. Das SCI arbeitet zusammen mit dem FBI, dem Georgia Bureau of Investigation, dem Justizministerium des Staates Georgia sowie der Georgia Technology Authority, deren Mitarbeiter es regelmäßig weiterbildet. Für die Zukunft strebt das SCI eine verstärkte Einbindung privater Unternehmen an.

Siemens

Siemens

Wittelsbacherplatz 2
80333 München
Deutschland

Status: private for-profit
Ebene: global
Sektor: Wirtschaft
Mitarbeiter: ca. 398.000
Jahr der Gründung: 1847

Partner:
Cisco, HP, IBM, MS, Oracle, SAP, Solutionary, Symantec

Web: <`http://www.siemens.com`>

Börsennotiertes Unternehmen für Elektronik und Elektrotechnik. Siemens erzielte im Geschäftsjahr 2007 einen Umsatz von 112,6 Mrd. US-Dollar (<`http://hoovers.com`>) und belegte auf der Forbes-Liste der weltweit größten Unternehmen den 60. Platz. Sämtliche IT-Dienstleistungen, so auch das Management von IT-Infrastrukturen, wurden Anfang 2007 in der Unternehmenssparte Siemens IT Solutions und Services (SIS) – formals Siemens Business Services (SBS) – gebündelt. SIS bietet hinsichtlich einer sicheren IT-Infrastrukur verschiedene Dienstleistungen an, die von der Beratung und Risikoanalyse bis zum Sicherheitsmanagement reichen. Siemens stellt auch Lösungen für Identity- und Access-Management sowie Virtual Private Networks (VPN) zur Verfügung.

Solutionary

Solutionary

9420 Underwood Avenue
Omaha, NE 68114
USA

Status: private for-profit
Ebene: global
Sektor: Wirtschaft
Mitarbeiter: ca. 55
Jahr der Gründung: 2000

Partner:
Cisco, MS, Siemens

Web: <`http://www.solutionary.com`>

Privates Unternehmen, das Dienstleistungen im Bereich des Sicherheitsmanagements von IT-Infrastrukturen erbringt (MSSP). Hierzu zählt vor allem der Aufbau und die Überwachung von Firewalls sowie von IDS-Lösungen. Solutionary erwirtschaftete einen Jahresumsatz 2007 von 22,0 Mio. US-Dollar (<`http://hoovers.com`>). Seit Mitte 2004 arbeitet Solutionary eng mit Siemens Business Services (SBS) zusammen. Beide unterhalten ein gemeinsames Security Operations Center (SOC), das Kunden weltweit und rund um die Uhr betreut.

SRI

SRI International

333 Ravenswood Avenue
Menlo Park, CA 94025–3493
USA

Status: private non-profit
Ebene: national
Sektor: Wissenschaft und Forschung
Mitarbeiter: ca. 2.000
Jahr der Gründung: 1946

Partner:
CIA, US-DHS, US-DoD

Web: <`http://www.sri.com`>

Privates US-Forschungsinstitut, das sich u. a. mit Computertechnologie befaßt. Ursprünglich als „Stanford Research Institute“ gegründet, ist SRI seit 1970 von der Stanford University unabhängig und nennt sich seit 1977 SRI International. Zu den Hauptauftraggebern zählen das US-DoD, das US-DHS sowie die CIA. SRI war bereits Ende der 1960er Jahren an der Entwicklung des Internet-Vorläufers ARPANET beteiligt und betrieb das erste für die Domain-Name-Vergabe zuständige NIC. Das Institut führt seit den 1980er Jahren Forschungsprojekte zu Intrusion Detection Systemen durch. Im Auftrag des US-DHS betreibt SRI seit 2004 ein Cyber Security R&D Center zur Entwicklung neuer Technologien zum Schutz der Informationsinfrastruktur der USA.

Symantec

Symantec

20330 Stevens Creek Boulevard
Cupertino, CA 95014
USA

Status: private for-profit
Ebene: global
Sektor: Wirtschaft
Mitarbeiter: ca. 17.000
Jahr der Gründung: 1982

Partner:
CSC, Cybertrust, HP, IBM, MS, Siemens

Web: <`http://www.symantec.com`>

Börsennotiertes Unternehmen für Sicherheitstechnologien zum Schutz elektronischer Infrastrukturen. Symantec hat Niederlassungen in mehr als 40 Ländern. Im Geschäftsjahr 2007 betrug der Umsatz 5,2 Mrd. US-Dollar (<`http://hoovers.com`>). Auf der Forbes-Liste der weltweit größten Unternehmen erreichte Symantec 2007 den 728. Platz. Seit der Gründung werden die Kernkompetenzen stetig durch die Übernahme weiterer Unternehmen ausgeweitet. Zu den aquirierten Unternehmen zählen u. a. Norton Computing (1990), Riptech (2002), @stake (2004) und Veritas Software (2005). Für 2010 ist ferner die Übernahme von Teilen des Unternehmens VeriSign avisiert. Anfangs hauptsächlich im Bereich Anwender-Software für Personal-Computer tätig, spezialisierte sich das Unternehmen zunehmend auf Themen der Informationssicherheit sowohl im privaten als auch im professionellen Kontext. Symantec verfügt nach eigenen Angaben über eines der weltweit größten Sensor-Netzwerke zur Früherkennung neuer Bedrohungen im Internet sowie eine der umfangreichsten Datenbanken zu elektronischen Schadprogrammen.

TechNet

Technology Network

101 University Avenue
Palo Alto, CA 94303
USA

Status: private non-profit
Ebene: national
Sektor: Organisierte Interessen
(Einzel-)Mitglieder: ca. 200
Jahr der Gründung: 2000

Korporative Mitglieder:
Cisco, HP, ITAA, MS, Oracle, RSA, Symantec, VeriSign

Web: <`http://www.technet.org`>

US-amerikanischer Interessenverband von CEOs der High-Tech-Industrie. Zu den Mitgliedern gehören Führungskräfte von MS, Cisco, HP und Intel. Als Antwort auf die National Strategy to Secure Cyberspace formierte sich unter dem Dach von TechNet eine CEO Cyber Security Task Force, deren Ziel eine weitere Sensibilisierung von Unternehmen hinsichtlich der Sicherheit von IT-Infrastrukturen sowie ein Austausch über geeignete Maßnahmen auf der Führungsebene ist.

UN

United Nations

First Avenue at 46th Street
New York, NY 10017
USA

Status: public
Ebene: global
Sektor: Internationale Organisationen
Jahr der Gründung: 1945

Partner:
AIT, Cisco, G8, HP, ICC, IFIP, World Bank

Web: <`http://www.un.org`>

Internationaler Zusammenschluß von 192 Staaten, der sich in mehrere Teilorganisationen untergliedert. Der Wirtschafts- und Sozialrat (ECOSOC) mandatiert seit 1995 jährlich eine Arbeitsgruppe Informatik. Seit 2001 unterhält ECOSOC zudem eine ICT Task Force, die jährliche Global-InfoSec-Konferenzen ausrichtet, auf denen Regierungsvertreter und Führungskräfte der IT-Industrie Sicherheitsthemen diskutieren. Die ITU-T, eine Unterorganisation der International Telecommunication Union (ITU), schlägt internationale Telekommunikationsstandards vor und hielt 2002 einen Workshop zu Sicherheitsthemen ab. Die ITU organisierte ferner in den Jahren 2003 und 2005 zwei konsekutive UN-Weltgipfel zur Informationsgesellschaft (WSIS), auf welchen der private Sektor durch die ICC vertreten wurde. In Folge dieser Gipfel wurde 2006 das Internet Governance Forum (IGF) eingerichtet, welches Akteuren aus allen Sektoren zugänglich ist und u. a. Themen der Sicherheit des Internets diskutiert. Schließlich befaßt sich die World Intellectual Property Organization (WIPO) mit dem Schutz geistigen Eigentums.

US-Congress

US Congress

Washington, DC 20515
USA

Status: public
Ebene: national
Sektor: Staat/Öffentliche Verwaltung
Jahr der Gründung: 1789

Partner:
CSIS, US-DoJ

Web: <`http://www.house.gov`>

Bundesparlament der USA mit insgesamt 535 Abgeordneten, verteilt auf die beiden Kammern Senat und Repräsentantenhaus. Im Bereich der IT-Sicherheit erließ der Kongreß eine Reihe zentraler Gesetze: Computer Security Act of 1987, Communications Assistance for Law Enforcement Act of 1994 (CALEA), Health Insurance Portability and Accountability Act of 1996 (HIPAA), Gramm-Leach-Bliley Act of 1999 (GLBA), Government Information Security Reform Act of 2000 (GISRA), Federal Information Security Management Act of 2002 (FISMA), Cyber Security R&D Act of 2002 (CSRDA), Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM). Für den Bereich des Schutzes kritischer Informationsinfrastrukturen ist im Repäsentantenhaus das Subcommittee on Cybersecurity, Science, and R&D, im Senat das Subcommittee on Terrorism, Technology, and Homeland Security zuständig.

US-DHS

US Department of Homeland Security

245 Murray Drive
Washington, DC 20528
USA

Status: public
Ebene: national
Sektor: Staat/Öffentliche Verwaltung
Mitarbeiter: ca. 216.000
Jahr der Gründung: 2002

Partner:
CERT/CC, CIA, CIAO, CIDDAC, FBI, I3P, IT-ISAC, NIAC, NIPC, NSA, RAND, SRI, US-DoJ

Web: <`http://www.dhs.gov`>

US-Ministerium für Heimatschutz, zuständig auch für den Schutz der kritischen IT-Infrastruktur. Dem Staatssekretär für Information Analysis and Infrastructure Protection (IAIP) ist seit 2003 die National Cyber Security Division (NCSD) mit etwa 120 Mitarbeitern zugeordnet, deren Hauptaufgabe die Umsetzung der Anfang 2003 veröffentlichten National Strategy to Secure Cyberspace ist. Die NCSD betreibt in Zusammenarbeit mit dem CERT/CC das nationale US-CERT. Anfang 2004 wurde in der Abteilung für Wissenschaft und Technologie mit Unterstützung von SRI ein Cyber Security Research and Development Center eingerichtet, das Kontakte zu privaten und öffentlichen Forschungseinrichtungen unterhält. In den Jahren 2006, 2008 und 2010 organisierte das US-DHS unter der Bezeichnung „Cyber Storm“ eine Reihe von Sicherheitsübungen im Cyberspace, an der zuletzt auch Frankreich, Deutschland, Ungarn, Italien, die Niederlande, Schweden und das Vereinigte Königreich sowie beobachtend die Europäische Kommission und ENISA teilnahmen.

US-DoD

US Department of Defense

The Pentagon
Washington, DC 20301
USA

Status: public
Ebene: national
Sektor: Staat/Öffentliche Verwaltung
Mitarbeiter: ca. 3.254.000
Jahr der Gründung: 1947

Partner:
CERT/CC, CIA, CSC, NSA, RAND, SRI

Web: <`http://www.dcfl.gov`>

Das US-Verteidigungsministerium unterhält im Rahmen des 2001 eingerichteten Department of Defense Cyber Crime Center (DC3) Einrichtungen und Programme, die unmittelbar dem Schutz der eigenen IT-Infrastruktur vor kriminellen oder feindlichen Angriffen dienen. Zu diesen gehört das Defense Cyber Crime Institute (DCCI), das Defense Computer Forensics Lab (DCFL) sowie das Defense Computer Investigations Training Program (DCITP). DCITP und DCFL bestehen bereits seit 1998, während das DCCI erst 2001 gegründet wurde. Das DC3 bildet intern Personal des US-DoD aus und stellt Kapazitäten zur Aufklärung und Verfolgung von Angriffen im Netz zur Verfügung. Das US-DoD unterhält ein eigenes DoD-CERT.

US-DoJ

US Department of Justice

10th at Constitution Avenue NW
Washington, DC 20530
USA

Status: public
Ebene: national
Sektor: Staat/Öffentliche Verwaltung
Mitarbeiter: ca. 112.000
Jahr der Gründung: 1870

Partner:
CIA, FBI, G8, NSA, NW3C, RAND, US-Congress, US-DHS

Web: <`http://www.cybercrime.gov`>

Innerhalb des US-Justizministeriums fallen Internetstraftaten in den Verantwortungsbereich der Computer Crimes und Intellectual Property Section (CCIPS). Die CCIPS ist der Kriminalabteilung (Criminal Division) zugeordnet und wurde 1991 als Computer Crime Unit gegründet. Im Jahre 1996 wurde das Referat als CCIPS zu einer eigenen Unterabteilung erhoben und beschäftigt gegenwärtig etwa 40 Juristen, von denen über die Hälfte als Staatsanwälte tätig ist. Zu ihren Aufgaben gehört neben der Prozeßführung auch die Schulung und Weiterbildung von Strafverfolgungsbeamten auf allen Verwaltungsebenen sowie die Beratung des US-DoD, der NSA und der CIA in computerrechtlichen Fragen. Darüber hinaus führt die CCIPS den Vorsitz in der G8 Arbeitsgruppe High-Tech Crime.

VeriSign

VeriSign

487 East Middlefield Road
Mountain View, CA 94043
USA

Status: private for-profit
Ebene: global
Sektor: Wirtschaft
Mitarbeiter: ca. 5.300
Jahr der Gründung: 1995

Partner:
Cisco, IBM, iDEFENSE, MS, Oracle

Web: <`http://www.verisign.com`>

Seit 1998 börsennotiertes Unternehmen, dessen Kerngeschäft der Betrieb von Netzwerkinfrastrukturen ist. Der Unternehmensumsatz belief sich im Geschäftsjahr 2006 auf 1,6 Mrd. US-Dollar (<`http://hoovers.com`>). Zu den Produkten des Unternehmens gehört auch Software zur Einrichtung sicherer Netzwerkverbindungen. VeriSign bietet u. a. Dienstleistungen im Bereich der Verschlüsselung, der Authentifizierung sowie des Betriebes einer Public Key Infrastructure. Mit der Übernahme von Guardent Anfang 2004 erwarb VeriSign ferner Kompetenzen im Bereich des Sicherheitsmanagements sowie der Unternehmensberatung. Darüber hinaus verwaltet VeriSign im Auftrag der ICANN zwei von insgesamt dreizehn Root-Name-Servern des Internet (Top-Level-Domains „.com“ und „.net“). VeriSign wickelt nach eigenen Angaben etwa 30 Prozent aller eCommerce-Transaktionen in Nordamerika ab. Für 2010 ist die Übernahme der Sicherheitssparte durch Symantec vereinbart.

World Bank

World Bank Group

1818 H Street NW
Washington, DC 20433
USA

Status: public
Ebene: global
Sektor: Internationale Organisationen
Jahr der Gründung: 1945

Partner:
UN

Web: <`http://www.worldbank.org`>

Gruppe verschiedener internationaler Organisationen, deren Aufgabe die Förderung der wirtschaftlichen Entwicklung ärmerer Länder ist. Die World Bank Group finanziert zu diesem Zweck eine Reihe von Entwicklungsprojekten, so u. a. das Information for Development Program (infoDev), das der Förderung der IT-Infrastruktur in den Entwicklungsländern dient. Dieses Programm beschäftigt sich auch mit der Sicherheit von IT-Infrastrukturen und veröffentlichte hierzu ein Information Technology Security Handbook.

B Issues und Activities

Akteure	*Issues*										*Activities*												
	Computer Related Crimes	Identity/Access	Information Freedom	Intellectual Property	Legal Framework	Privacy/Data Protection	Secure Transactions	System Protection	Technical Standards		Alerting	Consulting/Advice	Developing Strategies/Policies	Emergency/Incidence Response	Hardware Engineering	Information Exchange	Investigation/Prosecution	Monitoring/Analysis of Incidents/Trends	Raising Awareness	Research	Security/Risk Management	Software Engineering	Training/Education
public																							
APEC	×	×		×	×		×	×	×			×	×			×							
BKA	×			×	×	×								×		×	×	×					
BMVg		×					×	×	×				×	×						×			
BSI		×			×	×	×	×	×			×	×	×		×		×	×	×	×	×	×
CIA	×	×					×	×									×	×		×			
CIAO		×				×	×	×					×						×				×
CoE	×		×	×	×	×							×										
EC			×	×	×	×			×				×						×	×			
ENISA		×			×		×	×	×		×	×	×			×			×		×		×
EUROPARL	×		×	×	×	×							×										
FBI	×	×		×	×	×	×	×			×	×		×		×	×	×					×
FTC	×		×	×	×	×						×				×	×	×	×				
G8	×			×	×	×										×	×						
IC3	×			×		×					×			×		×		×					
NHTCU	×			×	×	×								×			×	×					
NIPC		×					×	×			×			×			×	×					×
NIST		×					×	×	×			×	×						×	×			
NSA		×					×	×	×			×			×			×		×		×	
NSC					×								×										
NSF		×				×	×	×	×							×				×			
NW3C	×			×	×											×		×		×			×
OECD		×			×	×	×	×					×			×			×	×			
PCIPB					×			×					×										
SCI	×	×		×		×	×	×												×			×
UN			×		×	×			×				×			×							
US-Congress					×								×										
US-DHS		×					×	×	×		×	×		×		×		×	×	×	×		×
US-DoD	×	×					×	×	×							×	×	×		×			×
US-DoJ	×			×	×	×							×			×	×	×	×	×			×
World Bank	×	×	×			×	×	×	×			×	×							×			
mixed																							
AKSIS		×			×		×	×	×				×			×			×				
CERT/CC		×					×	×	×		×	×		×		×		×	×	×	×	×	×

(Fortsetzung nächste Seite)

Akteure	*Issues*									*Activities*												
	Computer Related Crimes	Identity/Access	Information Freedom	Intellectual Property	Legal Framework	Privacy/Data Protection	Secure Transactions	System Protection	Technical Standards	Alerting	Consulting/Advice	Developing Strategies/Policies	Emergency/Incidence Response	Hardware Engineering	Information Exchange	Investigation/Prosecution	Monitoring/Analysis of Incidents/Trends	Raising Awareness	Research	Security/Risk Management	Software Engineering	Training/Education
(Fortsetzung)																						
CIDDAC								×		×					×		×					
CSIA					×			×	×		×							×					×
EU Forum	×			×		×		×	×						×			×					
GI		×				×	×	×	×		×	×			×				×				×
I3P	×	×			×		×	×				×			×				×				
InfoSurance		×			×		×	×	×			×			×			×					
InfraGard	×	×					×	×		×					×								×
ISO									×			×											
ISPAB		×				×	×	×			×												
NCSA		×				×	×	×										×					×
NCSP		×			×		×	×	×			×			×			×					
NIAC		×			×		×	×			×	×			×			×					
private non-profit																						
(ISC)2		×					×	×	×						×			×					×
ACLU			×		×	×				×					×	×	×	×					
ASIS		×					×	×	×						×			×					×
BSA			×	×	×				×		×				×	×	×	×					×
CCC			×			×		×							×			×					
CDT			×	×	×	×									×		×	×	×				
CSIS			×		×	×					×	×			×		×		×				
EFF			×	×	×	×				×	×				×	×	×	×					×
EPIC			×		×	×				×					×		×	×	×				
FIRST		×					×	×		×			×		×			×					×
GCSOC					×			×				×						×					
GILC			×			×				×					×		×						
GIP					×						×	×											
GIPI			×	×	×	×					×	×			×								×
HTCIA	×							×							×	×							×
ICANN									×			×											
ICC	×	×		×	×		×	×		×					×		×						×
IEEE									×		×	×			×								×
IETF									×			×			×								
IFIP	×	×					×	×							×				×				
ISA		×			×		×	×		×	×				×				×	×			×
ISACA		×					×	×	×						×				×				×
ISF		×					×	×							×				×				
ISOC		×					×	×	×			×			×		×						×
ISSA		×					×	×	×						×			×					×
ITAA		×		×	×							×			×								

(Fortsetzung nächste Seite)

Akteure	*Issues*									*Activities*												
	Computer Related Crimes	Identity/Access	Information Freedom	Intellectual Property	Legal Framework	Privacy/Data Protection	Secure Transactions	System Protection	Technical Standards	Alerting	Consulting/Advice	Developing Strategies/Policies	Emergency/Incidence Response	Hardware Engineering	Information Exchange	Investigation/Prosecution	Monitoring/Analysis of Incidents/Trends	Raising Awareness	Research	Security/Risk Management	Software Engineering	Training/Education
(Fortsetzung)																						
IT-ISAC	×	×					×	×		×					×		×					
PI			×		×	×				×					×		×					
RAND	×				×							×							×			×
SANS		×					×	×		×					×		×		×			×
SRI		×					×	×											×			
TechNet		×			×		×	×			×				×			×				
private for-profit																						
AIT		×					×	×	×						×			×				×
Cisco		×					×	×	×			×		×						×	×	
CSC		×					×	×	×			×							×	×	×	×
CSI		×					×	×	×						×			×	×			×
Cybertrust	×	×					×	×				×								×	×	
Gartner		×					×	×				×							×			
HP		×					×	×	×			×		×						×		
IABG		×					×	×				×							×	×	×	
IBM						×		×	×			×		×						×	×	
IDC		×					×	×	×			×							×			
iDEFENSE		×					×	×		×		×			×				×			
ISS								×		×		×			×		×		×	×	×	×
McAfee						×	×	×	×	×		×			×		×	×	×	×	×	×
MI					×							×							×			
MS		×		×		×	×	×	×	×		×	×		×	×			×		×	×
Oracle		×				×	×	×	×			×									×	
PwC					×	×		×				×								×		
RedSiren		×					×	×		×		×			×					×		×
RSA		×					×					×		×							×	×
SAP		×					×	×	×			×									×	×
Siemens		×					×	×	×			×		×						×		
Solutionary								×					×							×	×	
Symantec			×			×		×	×	×		×			×		×	×	×	×	×	×
VeriSign		×					×	×	×			×					×			×	×	

C Ressourcen-Kontrolle

Akteur/Ressource	Contact to Other Actors (Networking)	Expert Knowledge	Funding	Influence on Political Decision Making	Influence on Standardization	Publicity	Technical Equipment	
ACLU			1	1				2
APEC	1			1				2
BSA	1	1		3			1	6
CDT					1	1		2
CERT/CC	2	3				1		6
CIA	2	2						4
Cisco			1	1				2
CoE	1			1				2
EC			2	2	1	1		6
EFF		1			1			2
ENISA		1	1					2
EPIC				1		1		2
EUROPARL			1	1				2
FBI	1	1		2		2		6
FIRST	1	1						2
G8	1			1				2
IETF					2		2	4
ISS		2			1		1	4
ITAA	3	1		1		1		6
McAfee		1		1				2
MS	1	3	2	2	3	1		12
NCSA	1	1						2
NSA	2	2						4
NSC	1			1				2
OECD	2	1		2	1			6
RSA	1	2					1	4
Symantec	2	2						4
US-Congress	1		1	2	1	1		6
US-DHS	5	1	3	4	1	2		16
US-DoD		3	1	1			1	6
US-DoJ	1	2		1				4
	30	31	13	29	12	11	6	132

Literaturverzeichnis

Abbate, Janet (1999a): From Control to Coordination: New governance models for information networks and other large technical systems. In: Coutard, Olivier (Hrsg.): *The Governance of Large Technical Systems*. London: Routledge, 114 – 129.

Abbate, Janet (1999b): *Inventing the Internet*. Cambridge, MA: MIT Press.

Abele-Wigert, Isabelle; Dunn, Myriam (2006): *International CIIP Handbook 2006. Vol. I. An inventory of 20 national and 6 international critical information infrastructure protection policies*. Zürich: Center for Security Studies, ETH.

Albert, Hans (1968): *Traktat über kritische Vernunft*. Tübingen: Mohr.

Albert, Hans (2000): *Kritischer Rationalismus*. Tübingen: Mohr.

Alt, Rainer; Schmid, Beat (2000): Logistik und Electronic Commerce: Perspektiven durch zwei sich wechselseitig ergänzende Konzepte. In: *Zeitschrift für Betriebswirtschaft* 70 (1), 75 – 99.

Arens, Yigal; Rosenbloom, Paul S. (2003): Responding to the Unexpected: How IT can help prepair for future attacks and disasters. In: *Communications of the Association for Computing Machinery* 46 (9), 33 – 35.

Argyris, Chris; Schön, Donald A. (1978): *Organizational Learning: A theory of action perspective*. Reading, MA: Addison-Wesley.

Arquilla, John J.; Ronfeldt, David F. (1996): *The Advent of Netwar*. <`http://www.rand.org/publications/MR/MR789/`>. Online-Ressource, Abruf: 08.04.2005. RAND Corporation.

Arquilla, John J.; Ronfeldt, David F. (2001): *Networks and Netwars: The Future of Terror, Crime, and Militancy*. <`http://www.rand.org/publications/MR/MR1382/`>. Online-Ressource, Abruf: 08.04.2005.

Arreguín-Toft, Ivan (2005): *How the Weak Win Wars. A Theory of Asymmetric Conflict*. Cambridge, UK: Cambridge University Press.

Arrow, Kenneth J. (1963): Uncertainty and the Welfare Economics of Medical Care. In: *American Economic Review* 53 (5), 941 – 973.

Arrow, Kenneth J. (1969): The Organization of Economic Activity: Issues Pertinent to the Choice of Market vs. Non-Market Allocation. In: Government Printing Office (Hrsg.): *The Analysis and Evaluation of Public Expenditure: The PBB System*. Washington, DC: US Government Printing Office, 47 – 64.

Arrow, Kenneth J. (1974): Limited Knowledge and Economic Analysis. In: *American Economic Review* 64, 1 – 10.

Arrow, Kenneth J. (1979): The Economics of Information. In: Dertouzos, Michael L.; Moses, Joel (Hrsg.): *The Computer Age: A Twenty-Year View.* Cambridge, MA: MIT Press, 306 – 317.

Arts, Bas (2006): Non-State Actors in Global Environmental Governance: New Arrangements Beyond the State. In: Koenig-Archibugi, Mathias; Zürn, Michael (Hrsg.): *New Modes of Governance in the Global System. Exploring Publicness, Delegation and Inclusiveness.* Basingstoke: Palgrave Macmillan, 177 – 200.

Ashby, W. R. (1974): *Einführung in die Kybernetik.* Frankfurt a. M.: Suhrkamp.

Ashby, William R. (1960): *Design for a Brain. The origin of adaptive behaviour.* New York, NY: John Wiley & Sons.

Axelrod, Robert (1984): *The Evolution of Cooperation.* New York, NY: Basic Books.

Backhaus, Klaus; Erichson, Bernd; Plinke, Wulff; Weiber, Rolf (2006): *Multivariate Analysemethoden. Eine anwendungsorientierte Einführung.* Berlin: Springer.

Bagnoli, Mark; Lipman (1989): Provision of Public Goods: Fully Implementing the Core through Private Contributions. In: *Review of Economic Studies* (56), 583 – 601.

Baird, Zoë (2002): Governing the Internet: Engaging Government, Business, and Nonprofits. In: *Foreign Affairs* 81 (6), 15 – 20.

Baran, Paul (1964): *On Distributed Communications: I. Introduction to Distributed Communications Networks.* <`http://www.rand.org/publications/RM/RM3420/`>. Online-Ressource, Abruf: 08.04.2005. RAND Corporation.

Bauer, Johannes M. (2009): Cybersecurity: Stakeholder incentives, externalities, and policy options. In: *Telecommunications Policy* 33 (10 – 11), 706 – 719.

Baum, Joel A. C. (1996): Organizational Ecology. In: Clegg, Steward R.; Hardy, Cynthia; Nord, Walter R. (Hrsg.): *Handbook of Organization Studies.* London: Sage, 71 – 108.

Beck, Ulrich (2003): *Risikogesellschaft. Auf dem Weg in eine andere Moderne.* Frankfurt a. M.: Suhrkamp.

Bedford, Tim; Cooke, Roger (2001): *Probabilistic Risk Analysis. Foundations and Methods.* Cambridge, UK: Cambridge University Press.

Beer, Thomas (2004): Kritische Infrastrukturen im internationalen Umfeld. In: von Knop, Jan; Frank, Hans (Hrsg.): *Netz- und Computersicherheit. Sind wir auf einen Angriff auf unsere Informationssysteme und Informations-Infrastrukturen vorbereitet?* Bielefeld: Bertelsmann, 93 – 111. Kongressband 2003 der Bundesakademie für Sicherheitspolitik und der Heinrich-Heine-Universität Düsseldorf.

Belanger, France; Hiller, Janine S.; Smith, Wanda J. (2002): Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes. In: *Journal of Strategic Information Systems* 11 (3 – 4), 245 – 270.

Bell, Daniel (1973): *The Coming of the Post-industrial Society. A Venture in Social Forecasting.* New York, NY: Basic Books.

Bell, Daniel (1979): The Social Framework of the Information Society. In: Dertouzos, Michael L.; Moses, Joel (Hrsg.): *The Computer Age: A Twenty-Year View.* Cambridge, MA: MIT Press, 163 – 211.

Bell, Daniel (1998): The Internet and the Trajectories of Technology. In: *The Tocqueville Review* 19 (2), 111 – 125.

Bendiek, Annegret (2012): *Europäische Cybersicherheitspolitik.* Berlin, Stiftung Wissenschaft und Politik, Studie 15.

Benedikt, Michael (1992): Cyberspace: Some Proposals. In: Benedikt, Michael (Hrsg.): *Cyberspace: First Steps.* Cambridge, MA: MIT Press, 119 – 224.

Beniger, James R. (1986): *The control revolution: technological and economic origins of the information society.* Cambridge, MA: Harvard University Press.

Benner, Thorsten; Reinicke, Wolfgang H. (1999): Politik im globalen Netz: Globale Politiknetzwerke und die Herausforderung offener Systeme. In: *Internationale Politik* (8), 25 – 32.

Benner, Thorsten; Reinicke, Wolfgang H.; Witte, Jan M. (2002): Shaping Globalization: The role of global public policy networks. In: Bertelsmannstiftung (Hrsg.): *Transparency: A Basis For Responsibility and Cooperation.* Gütersloh: Bertelsmann, 21 – 48.

Benner, Thorsten; Reinicke, Wolfgang H.; Witte, Jan M. (2003): Global Public Policy Networks: Lessons Learned and Challenges Ahead. In: *Brookings Review* 21 (2), 18 – 21.

Benner, Thorsten; Reinicke, Wolfgang H.; Witte, Jan M. (2004): Multisectoral Networks in Global Governance: Towards a Pluralistic System of Accountability. In: Held, David; Koenig-Archibugi, Mathias (Hrsg.): *Global Governance and Public Accountability.* Oxford: Blackwell, 191 – 210.

Bennett, Colin J. (1988): Different Processes, One Result: The Convergence of Data Protection Policy in Europe and the United States. In: *Governance: An International Journal of Policy and Administration* 1 (4), 415 – 441.

Benson, J. K. (1982): A framework for policy analysis. In: Rogers, David C.; Whetten, David A. (Hrsg.): *Interorganizational Coordination. Theory, Research, and Implementation.* Ames: Iowa State University Press, 137 – 176.

Berger, Peter L.; Luckmann, Thomas (2003): *Die gesellschaftliche Konstruktion der Wirklichkeit. Eine Theorie der Wissenssoziologie.* Frankfurt a. M.: Fischer.

Berkowitz, Bruce; Hahn, Robert W. (2003): Cybersecurity: Who's Watching the Store? In: *Issues in Science and Technology* 19 (3), 55 – 62.

Beukelmann, Stephan (2001): *Prävention von Computerkriminalität.* Frankfurt a. M.: Peter Lang. Universität Rostock, Dissertation.

Beyrer, Klaus (1998): Die optische Telegraphie als Beginn der modernen Telekommunikation. In: Teuteberg, Hans-Jürgen; Neutsch, Cornelius (Hrsg.): *Vom Flügeltelegraphen zum Internet. Geschichte der modernen Telekommunikation.* Stuttgart: Steiner, 14 – 26.

Bühl, Achim (1996): *CyberSociety. Mythos und Realität der Informationsgesellschaft.* Köln: PapyRossa.

Bühl, Achim (2000): *Die virtuelle Gesellschaft des 21. Jahrhunderts. Sozialer Wandel im digitalen Zeitalter.* Wiesbaden: Westdeutscher Verlag.

BKA (1999): *Electronic Commerce. Markt der Zukunft – auch für Kriminelle? Strategische Kriminalitätsanalyse.* Wiesbaden: Bundeskriminalamt.

Blatter, Joachim (2006): Governance als transdisziplinäres Brückenkonzept für die Analyse von Formen und Transformationen politischer Steuerung und Integration. In: Bogumil, Jörg; Werner, Jann; Nullmeier, Frank (Hrsg.): *Politik und Verwaltung. PVS – Politische Vierteljahresschrift Sonderheft 37.* Wiesbaden: VS Verlag, 50 – 76.

Bless, Roland; Mink, Stefan; Blass, Erik-Oliver; Conrad, Michael; Hof, Hans-Joachim; Kutzner, Kendy; Schöller, Marcus (2005): *Sichere Netzwerkkommunikation.* Heidelberg: Springer.

Bolter, Jay D. (1997): Das Internet in der Geschichte der Technologien des Schreibens. In: Münker, Stefan; Roesler, Alexander (Hrsg.): *Mythos Internet.* Frankfurt a. M.: Suhrkamp, 37 – 55.

Borg, Scott (2005): Economically Complex Cyberattacks. In: *IEEE Security & Privacy* 3 (6), 64 – 67.

Bourdieu, Pierre (1983): Ökonomisches Kapital, kulturelles Kapital, soziales Kapital. In: Kreckel, Reinhard (Hrsg.): *Soziale Ungereimtheiten. Soziale Welt, Sonderband 2.* Göttingen: Verlag Otto Schwartz, 183 – 198.

Bourdieu, Pierre (1985): The Forms of Capital. In: Richardson, Jeremy G. (Hrsg.): *Handbook of Theroy and Research for the Sociology of Education.* New York, NY: Greenwood, 241 – 258.

Boyd-Barrett, Oliver (2004): U.S. Global Cyberspace. In: Schuler, Douglas; Day, Peter (Hrsg.): *Shaping the Network Society. The New Role of Civil Society.* Cambridge, MA: MIT Press, 19 – 42.

Brandes, Ulrik; Wagner, Dorothea (2004a): Netzwerkvisualisierung. In: *Information Technology* 46 (3), 129 – 134.

Brandes, Ulrik; Wagner, Dorothea (2004b): Visone – Analysis and Visualization of Social Networks. In: Jünger, Michael; Mutzel, Petra (Hrsg.): *Graph Drawing Software*. Berlin: Springer, 321 – 340.

Brandes, Wilhelm; Recke, Guido; Berger, Thomas (1997): *Produktions- und Umweltökonomik. Band 1*. Stuttgart: Eugen Ulmer.

Brenner, Susan W.; Schwerha, Joseph J. (2002): Transnational Evidence Gathering And Local Prosecution Of International Cybercrime. In: *John Marshall Journal of Computer & Information Law* 20 (3), 347 – 395.

Breyer, Friedrich; Kolmar, Martin (2001): *Grundlagen der Wirtschaftspolitik*. Tübingen: Mohr.

Brin, Sergey; Page, Lawrence (2001): *The Anatomy of a Large-Scale Hypertextual Web Search Engine*. 2001. Paper of the Computer Science Department of the Stanford University, CA.Ausdruck.

Bross, Peter; Garbes, Axel (2006): Digitale Konvergenz und Handlungskonsequenzen. In: Klumpp, Dieter; Kubicek, Herbert; Rossnagel, Alexander; Schulz, Wolfgang (Hrsg.): *Medien, Ordnung und Innovation*. Berlin: Springer, 77 – 94.

Börzel, Tanja A. (1998): Organizing Babylon: On the different Conceptions of Policy Networks. In: *Public Administration* 76, 253 – 273.

Börzel, Tanja A. (2000): *Private Actors on the Rise? The Role of Non-State Actors in Compliance with International Institutions*. <`http://www.mpp-rdg.mpg.de/pdf_dat/00014.pdf`>. Online-Ressource, Abruf: 17.11.2003.

Börzel, Tanja A. (2002): Non-State Actors and the Provision of Common Goods: Compliance with International Institutions. In: Héritier, Adrienne (Hrsg.): *Common Goods. Reinventing European and International Governance*. Lanham: Rowman & Littlefield, 159 – 182.

Börzel, Tanja A.; Risse, Thomas (2005): Public-Private Partnerships. Effective and Legitimate Tools of Transnational Governance? In: Grande, Edgar; Pauly, Louis W. (Hrsg.): *Complex Sovereignty. Reconstituting Political Authority in the Twenty-First Century*. Toronto: University of Toronto Press, 195 – 216.

BSI (1999): *Security Considerations with Electronic Commerce*. <`http://www.bsi.de/literat/ecomerz/ecom_es.pdf`>. Online-Ressource, Abruf: 14.05.2003. Publikation des Bundesamtes für Sicherheit in der Informationstechnik.

Buchanan, James M. (1965): An Economic Theory of Clubs. In: *Economica* 32 (125), 1 – 14.

Buchner, Benedikt (2006): *Informationelle Selbstbestimmung im Privatrecht.* Tübingen: Mohr Siebeck.

Bundesministerium des Innern (2005): *Nationaler Plan zum Schutz der Informationsinfrastrukturen.* <http://www.bmi.bund.de/cae/servlet/contentblob/121734/publicationFile/13577/Nationaler_Plan_Schutz_Informationsinfrastrukturen.pdf>. Online-Ressource, Abruf: 17.06.2009.

Bunge, Mario (2001): The Status of Concepts. In: Mahner, Martin (Hrsg.): *Scientific Realism. Selected Essays of Mario Bunge.* Amherst, NY: Prometheus Books, 92 – 102.

Bunge, Mario; Mahner, Martin (2004): *Über die Natur der Dinge. Materialismus und Wissenschaft.* Stuttgart: Hirzel.

Burnett, Steve; Paine, Stephen (2001): *RSA Security's Official Guide to Cryptography.* New York, NY: McGraw-Hill.

Burstein, Aaron (2003): A Survey of Cybercrime in the United States. In: *Berkeley Technology Law Journal* 18 (18), 313 – 338.

Burt, Ronald S. (1984): Network items and the General Social Survey. In: *Social Networks* 6, 293 – 339.

Cairncross, Frances (1997): *The Death of Distance. How the Communications Revolution will Change Our Lives.* London: Orion Business.

Campbell, Philip L. (2005): The Denial-of-Service Dance. In: *IEEE Security & Privacy* 3 (6), 34 – 40.

Capurro, Rafael (1978): *Information. Ein Beitrag zur etymologischen und ideengeschichtlichen Begründung des Informationsbegriffs.* München: Saur.

Capurro, Rafael (2003): *Ethik im Netz.* Stuttgart: Franz Steiner Verlag.

Carbo, Toni; Wallace, David A. (1997): National and Global Information Infrastructures: Status, Issues, and Challenges. In: Williams, James G.; Carbo, Toni (Hrsg.): *Information Science: Still an Emerging Discipline.* Pittsburgh, PA: Cathedral Publishing, 153 – 174.

Castells, Manuel (2000a): *The Rise of the Network Society.* Oxford: Blackwell.

Castells, Manuel (2000b): Toward a Sociology of the Network Society. In: *Contemporary Sociology* 29 (5), 693 – 699.

Castells, Manuel (2001a): *Der Aufstieg der Netzwerkgesellschaft. Teil 1 der Triologie. Das Informationszeitalter.* Opladen: Leske + Budrich.

Castells, Manuel (2001b): *The Internet Galaxy. Reflections on the Internet, Business, and Society.* Oxford: Oxford University Press.

Cave, Martin; Mason, Robin (2001): The Economics of the Internet: Infrastructure and Regulation. In: *Oxford Review of Economic Policy* 17 (5), 188 – 201.

Cerny, Dietrich (2000): Schutz kritischer Infrastrukturen in Wirtschaft und Verwaltung. In: Geiger, Gebhard (Hrsg.): *Sicherheit der Informationsgesellschaft.* Baden-Baden: Nomos, 21 – 42.

Cerny, Philip G. (1995): Globalization and the Changing Logic of Collective Action. In: *International Organization* 49 (4), 595 – 625.

Ceruzzi, Paul E. (2000): *A History of Modern Computing.* Cambridge, MA: MIT Press.

Chandler, Alfred D. (1977): *The Visible Hand: The Managerial Revolution in American Business.* Cambridge, MA: Harvard University Press.

Chang, Weiping; Chung, Wingyan; Chen, Hsinchun; Chou, Shihchieh (2003): An International Perspective on Fighting Cybercrime. In: *Lecture Notes in Computer Science* (2665), 379 – 384.

Christiansen, Per (2000): Selbstregulierung, regulatorischer Wettbewerb und staatliche Eingriffe im Internet. In: *Multimedia und Recht* 3 (3), 123 – 129.

Clark, Colin (1940): *The Conditions of Economic Progress.* London: MacMillan.

Coase, Ronald H. (1960): The Problem of Social Cost. In: *Journal of Law and Economics* (3), 1 – 44.

Coase, Ronald H. (1988): *The Firm, the Market, and the Law.* Chicago, IL: University of Chicago Press.

Coleman, James S. (1974): *Power and the Structure of Society.* New York, NY: Norton.

Coleman, James S. (1988): Social Capital in the Creation of Human Capital. In: *American Journal of Sociology* 94, Supplement 95 – 120.

Coleman, James S. (1990): *Foundations of Social Theory.* Cambridge, MA: Belknap Press.

Coleman, William D. (1999): Associational Governance in a Globalizing Era: Weathering the Storm. In: Hollingsworth, J. R.; Boyer, Robert (Hrsg.): *Contemporary Capitalism. The Embeddedness of Institutions.* Cambridge, UK: Cambridge University Press, 127 – 153.

Computer Security Institute (2008): *Computer Crime and Security Survey.* <`http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf`>. Online-Ressource, Abruf: 03.11.2009.

Conlisk, John (1996): Why Bounded Rationality? In: *Journal of Economic Literature* 34, 669 – 700.

Cornes, Richard (1993): Dyke Maintenance and Other Stories: Some Neglected Types of Public Goods. In: *Quarterly Journal of Economics* 108 (1), 259 – 271.

Cornes, Richard; Sandler, Todd (1996): *The Theory of Externalities, Public Goods and Club Goods*. 2. Cambridge, UK: Cambridge University Press.

Coutard, Olivier (Hrsg.) (1999): *The Governance of Large Technical Systems*. London: Routledge.

Cowell, Frank A. (1995): *Measuring Inequality*. London: Prentice Hall / Harvester Wheatsheaf.

Coy, Wolfgang (1996): Bauelemente der Informationsgesellschaft. Folgt der Gutenberg-Galaxis eine Turing-Galaxis? In: Tauss, Jörg; Kollbeck, Johannes; Mönikes, Jan (Hrsg.): *Deutschlands Weg in die Informationsgesellschaft. Herausforderungen und Perspektiven für Wirtschaft, Wissenschaft, Recht und Politik*. Baden-Baden: Nomos, 285 – 310.

CSI/FBI (2006): *Computer Crime and Security Survey*. <`http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml`>. Online-Ressource, Abruf: 13.01.2007.

Czada, Roland; Lütz, Susanne; Mette, Stefan (2003): *Regulative Politik. Zähmungen von Markt und Technik*. Opladen: Leske + Budrich.

Czada, Roland; Schimank, Uwe (2000): Institutionendynamik und politische Institutionengestaltung. Die zwei Gesichter sozialer Ordnungsbildung. In: Werle, Raymund; Schimank, Uwe (Hrsg.): *Gesellschaftliche Komplexität und kollektive Handlungsfähigkeit*. Frankfurt a. M.: Campus, 23 – 43.

Dahlman, Carl J. (1979): The Problem of Externality. In: *Journal of Law and Economics* 22 (10), 141 – 162.

Dahrendorf, Ralf (1974): *Homo Sociologicus. Ein Versuch zur Geschichte, Bedeutung und Kritik der Kategorie der sozialen Rolle*. Opladen: Westdeutscher Verlag.

Deibert, Ronald J. (2002): Circuits of Power. Security in the Internet Environment. In: Rosenau, James N.; Singh, J. P. (Hrsg.): *Information Technologies and Global Politics. The Changing Scope Power of Power and Governance*. Albany, NY: State University of New York Press, 115 – 142.

Denning, Dorothy E. (2001): Cyberwarriors: Activists and Terrorists Turn to Cyberspace. In: *Harvard International Review* 23 (2), 70 – 75.

Denning, Dorothy E.; Baugh, William E. (2000): Hiding crimes in cyberspace. In: Thomas, Douglas; Loader, Brian D. (Hrsg.): *Cybercrime: Law enforcement, security and surveillance in the information age*. London: Routledge, 105 – 131.

Desai, Meghnad (2003): Public Goods: A Historical Perspective. In: Kaul, Inge; Conceição, Pedro; Le Goulven, Katell; Mendoza, Ronald U. (Hrsg.): *Providing Global Public Goods. Managing Globalization*. New York, NY: Oxford University Press, 63 – 78.

Deutscher Bundestag (Hrsg.) (1998): *Sicherheit und Schutz im Netz*. Bonn: ZV Zeitungs-Verlag Service. Schriftenreihe der Enquete-Kommission „Zukunft der Medien in Wirtschaft und Gesellschaft; Deutschlands Weg in die Informationsgesellschaft".

Diffie, Whitfield; Hellman, Martin E. (1976): New Directions in Cryptography. In: *IEEE Transactions on Information Theory* 22 (6), 644 – 654.

DiMaggio, Paul J.; Powell, Walter W. (1983): The iron cage revisited: institutional isomorphism and collective rationality in organizational fields. In: *American Sociological Review* 48, 147 – 160.

Ding, Wen; Yurcik, William; Yin, Xiaoxin (2005): Outsourcing Internet Security. Economic Analysis of Incentives for Managed Security Service Providers. In: *Internet and Network Economics. Lecture Notes in Computer Science*. Berlin: Springer, 947 – 958.

Dornseif, Maximilian (2005): *Phänomenologie der IT-Delinquenz*. Bonn, Friedrich-Wilhelms-Universität Bonn, Dissertation.

Dostal, Werner (1995): Die Informatisierung der Arbeitswelt. Multimedia, offene Arbeitsformen und Telearbeit. In: *Mitteilungen aus der Arbeitsmarkt- und Berufsforschung* 28 (4), 527 – 543.

Downs, Roger M.; Stea, David (1977): *Maps in minds: reflections on cognitive mapping*. New York, NY: Harper Row.

Drosdowski, Günther; Müller, Wolfgang; Scholze-Stubenrecht, Werner; Wermke, Matthias (1989): *Duden Etymologie. Das Herkunftswörterbuch der deutschen Sprache*. Mannheim: Dudenverlag.

Drozdova, Ekaterina A. (2001): Civil Liberties and Security in Cyberspace. In: Sofaer, Abraham D.; Goodman, Seymour E. (Hrsg.): *The Transnational Dimension of Cyber Crime and Terrorism*. Stanford, CA: Hoover Institution Press, 183 – 220.

Drucker, Peter F. (1968): *The Age of Discontinuity. Guidelines to our changing society*. New York, NY: Harper & Row.

Drucker, Peter F. (1989): *The New Realities. In government and politics ... in economy and business ... in society ... and in world view*. Oxford: Heinemann.

Drucker, Peter F. (1993): *Post-capitalist Society*. Oxford: Butterworth-Heinemann.

Dunn Cavelty, Myriam (2008): *Cyber-Security and Threat Politics. US efforts to secure the information age*. London: Routledge.

Dunsire, Andrew (1993): Modes of Governance. In: Kooiman, Jan (Hrsg.): *Modern Governance. New Government – Society Interactions*. London: Sage, 21 – 34.

Dutton, William H. (1999): *Society on the Line. Information Politics in the Digital Age*. Oxford: Oxford University Press.

Easton, David (1965): *A Systems Analysis of Political Life.* New York, NY: John Wiley & Sons.

Eberlein, Burkhard; Newman, Abraham L. (2008): Escaping the International Governance Dilemma? Incorporated Transgovernmental Networks in the European Union. In: *Governance* 21 (1), 25 – 52.

Eckstein, Harry (2000): Case Study and Theory in Political Science. In: Gomm, Roger; Hammersley, Martyn; Foster, Peter (Hrsg.): *Case Study Method.* London: Sage, 119 – 164.

Edwards, Michael; Zadek, Simon (2003): Governing the Provision of Global Public Goods: The Role and Legitimacy of Nonstate Actors. In: Kaul, Inge; Conceição, Pedro; Le Goulven, Katell; Mendoza, Ronald U. (Hrsg.): *Providing Global Public Goods. Managing Globalization.* New York, NY: Oxford University Press, 200 – 224.

Eilstrup-Sangiovanni, Mette (2005): Transnational Networks and New Security Threats. In: *Cambridge Review of International Affairs* 18 (1), 7 – 13.

Eisner Gillett, Sharon; Kapor, Mitchell (1997): The Self-Governing Internet: Coordination and Design. In: Kahin, Brian; Keller, James H. (Hrsg.): *Coordinating the Internet.* Cambridge, MA: MIT Press, 3 – 38.

Elias, Norbert (1939): *Über den Prozess der Zivilisation. Band II.* Basel: Verlag Haus zum Falken.

Espey, Jürgen; Rudinger, Georg (1999): Der überforderte Techniknutzer: IT-Sicherheit aus psychologischer Sicht. In: *Praxis der Informationsverarbeitung und Kommunikation* 22 (3), 178 – 184.

Esser, Hartmut (1999a): *Soziologie. Spezielle Grundlagen. Bd. 1: Situationslogik und Handeln.* Frankfurt a. M.: Campus.

Esser, Hartmut (1999b): *Soziologie. Spezielle Grundlagen. Bd. 3: Soziales Handeln.* Frankfurt a. M.: Campus.

Esser, Hartmut (1999c): *Soziologie. Spezielle Grundlagen. Bd. 4: Opportunitäten und Restriktionen.* Frankfurt a. M.: Campus.

Fallenböck, Markus (2003): Vertrauen in der vernetzten Wirtschaft: Die Rolle von Recht. In: Petrovic, Otto; Ksela, Michael; Fallenböck, Markus; Kittl, Christian (Hrsg.): *Trust in the Network Economy.* Wien: Springer, 153 – 176.

Farrell, Henry (2002): Negotiating Privacy across Arenas: The EU-U.S. "Safe Harbor" Discussions. In: Héritier, Adrienne (Hrsg.): *Common Goods. Reinventing European and International Governance.* Lanham: Rowman & Littlefield, 105 – 126.

Farrell, Henry (2003): Constructing the International Foundation of E-Commerce: The EU-US Safe Harbor Arrangement. In: *International Organization* 57 (2), 277 – 306.

Felzmann, Frank W. (2000): Programme mit Schadensfunktion. In: Geiger, Gebhard (Hrsg.): *Sicherheit der Informationsgesellschaft.* Baden-Baden: Nomos, 81 – 93.

Fink, Simon (2002): *Datenschutz zwischen Markt und Staat. Die „Safe Harbor"-Lösung als Ergabnis einer strategischen Interaktion zwischen der EU, den USA und der IT-Industrie.* Konstanz, Universität Konstanz, Magisterarbeit.

Fischer-Hübner, Simone (2000): Privacy and security at risk in the global information society. In: Thomas, Douglas; Loader, Brian D. (Hrsg.): *Cybercrime: Law enforcement, security and surveillance in the information age.* London: Routledge, 173 – 192.

Fisher, Allan G. B. (1939): Production, Primary, Secondary and Tertiary. In: *The Economic Record* 15, 24 – 38.

Fishman, Renee M.; Josephburg, Kara; Linn, Jane; Pollack, Jane; Victoriano, Jenna (2002): Threat of International Cyberterrorism on the Rise. In: *Intellectual Property and Technology Law Journal* 14 (10).

Floyd, Christiane (1999): Menschsein in der informatisierten Gesellschaft – zur Virtualisierung des Selbst. In: Bittner, Peter; Woinowski, Jens (Hrsg.): *Mensch – Informatisierung – Gesellschaft.* Münster: LIT, 21 – 41.

Fourastié, Jean (1954): *Die große Hoffnung des zwanzigsten Jahrhunderts.* Köln-Deutz: Bund.

Francis, John G. (1993): *The Politics of Regulation. A Comparative Perspective.* Cambridge, MA: Blackwell.

Frank, Thomas (2004a): 20 Jahre Computervirus und 132 Jahre StGB. Strafrechtliche Instrumentarien gegen Schadprogramme im Computer. In: Hilgendorf, Eric (Hrsg.): *Informationsstrafrecht und Rechtsinformatik. Das Strafrecht vor neuen Herausforderungen.* Berlin: Logos, 23 – 55.

Frank, Thomas (2004b): *Zur strafrechtlichen Bewältigung des Spamming.* Berlin: Logos.

Franklin, Benjamin; Franklin, William T. (1818): *Memoirs of the Life and Writings of Benjamin Frabklin. Vol. I.* London: Henry Colburn.

Frenken, Koen (2006): *Innovation, Evolution and Complexity Theory.* Cheltenham: Edward Elgar.

Frey, René L. (1972): *Infrastruktur. Grundlagen der Planung öffentlicher Investitionen.* Tübingen: Mohr.

Frey, René L. (1988): Infrastruktur. In: Albers, Willi (Hrsg.): *Handwörterbuch der Wirtschaftswissenschaft.* Stuttgart: Gustav Fischer, 201 – 215.

Friedrich, Käthe (2002): Schwachstelle Sicherheitsbewusstsein? In: Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *Mit IT-Sicherheit gegen Internet-Kriminalität?!* Ingelheim: SecuMedia, 54 – 70.

Friendly, Michael (1994): Mosaic Displays for Multi-Way Contingency Tables. In: *Journal of the American Statistical Association* 89 (425), 190 – 200.

Froomkin, A. M. (2000): Semi-private international rulemaking: lessons learned from the WIPO domain name process. In: Marsden, Christopher T. (Hrsg.): *Regulating the Global Information Society.* London: Routledge, 211 – 232.

Fuhrberg, Kai (2000): Sicherheit im Internet. In: Geiger, Gebhard (Hrsg.): *Sicherheit der Informationsgesellschaft.* Baden-Baden: Nomos, 94 – 107.

Fuhrberg, Kai; Häger, Dirk; Wolf, Stefan (2001): *Internet-Sicherheit. Browser, Firewalls und Verschlüsselung.* München: Hanser.

Fukuyama, Francis (1989): The End of History? In: *National Interest* (16), 3 – 18.

Furnell, Steven (2002): *Cybercrime. Vandalizing the Information Society.* London: Addison-Wesley.

Gans, Joshua S. (2001): Regulating Private Infrastructure Investment: Optimal Pricing for Access to Essential Facilities. In: *Journal of Regulatory Economics* 20 (2), 167 – 189.

Gehlen, Arnold (1966): *Die Seele im technischen Zeitalter.* Hamburg: Rowohlt.

Gehlen, Arnold (1975): *Urmensch und Spätkultur.* Wiesbaden: Athenaion.

Geiger, Gebhard (Hrsg.) (2000): *Sicherheit der Informationsgesellschaft: Gefährdung und Schutz informationsabhängiger Infrastrukturen.* Baden-Baden: Nomos.

Gell-Mann, Murray (1994): *Das Quark und der Jaguar. Vom Einfachen zum Komplexen – die Suche nach einer neuen Erklärung der Welt.* München: Piper.

Gell-Mann, Murray (1995a): Complex Adaptive Systems. In: Morowitz, H.; Singer, J. (Hrsg.): *The Mind, the Brain, and CAS.* Reading, MA: Addison-Wesley, 11 – 23.

Gell-Mann, Murray (1995b): What Is Complexity? In: *Complexity* 1 (1), 16 – 19.

Genschel, Philipp (1995): *Standards in der Informationstechnik. Institutioneller Wandel in der internationalen Standardisierung.* Frankfurt a. M.: Campus.

George, Alexander L.; Bennett, Andrew (2005): *Case Studies and Theory Development in the Social Sciences.* Cambridge, MA: MIT Press.

Geuss, Raymond (2003): *Public Goods, Private Goods.* Princeton: Princeton University Press.

Gibson, William (1984): *Neuromancer.* New York, NY: Fantasia Press.

Gilder, George F. (2000): *Telecosm: how infinite bandwidth will revolutionize our world.* New York, NY: Free Press.

Glotz, Peter (1999): *Die beschleunigte Gesellschaft. Kulturkämpfe im digitalen Kapitalismus.* München: Kindler.

Glotz, Peter (2001): *Von Analog nach Digital. Unsere Gesellschaft auf dem Weg zur digitalen Kultur.* Frauenfeld: Huber.

Gollan, Lutz; Meinel, Christoph (2001): Elektronische Signaturen. Eine amerikanische und europäische Perspektive. In: Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *2001 – Odyssee im Cyberspace? Sicherheit im Intenet!* Ingelheim: SecuMedia, 97 – 111.

Gould, Mark (2000): Locating Internet governance: Lessons from the standards process. In: Marsden, Christopher T. (Hrsg.): *Regulating the Global Information Society.* London: Routledge, 193 – 210.

Gower, John C. (1971): A general coefficient of similarity and some of its properties. In: *Biometrics* (27), 857 – 871.

Gramlich, Edward M. (1994): Infrastucture Investment: A Review Essay. In: *Journal of Economic Literature* 32 (3), 1176 – 1196.

Granovetter, Mark S. (1973): The Strength of Weak Ties. In: *American Journal of Sociology* 78 (6), 1360 – 1380.

Granovetter, Mark S. (1985): Economic Action and Social Structure: The Problem of Embeddedness. In: *American Journal of Sociology* 91 (3), 481 – 511.

Greenstein, Marilyn; Vasarhelyi, Miklos (2002): *Electronic Commerce. Security, Risk Management, and Control.* New York, NY: McGraw-Hill.

Groebel, Jo; Metze-Mangold, Verena; van der Peet, Jowon; Ward, David (2001): *Twilight Zones in Cyberspace: Crimes, Risk, Surveillance and User-Driven Dynamics.* Bonn, Friedrich-Ebert-Stiftung, Forschungsbericht.

Habermas, Jürgen (1999): *Die Einbeziehung des Anderen: Studien zur politischen Theorie.* Frankfurt a. M.: Suhrkamp.

Hamelink, Cees J. (1994): *Trends in World Communication. On Disempowerment and Self-empowerment.* Penang: Southbound.

Hammer, Volker (1995): Infrastruktur. In: *Datenschutz und Datensicherheit* (5), 293 – 294.

Harbort, Stephan (1996): Verbrechen im Cyberspace: Neue Erscheinungsformen zeitspezifischer Computerkriminalität. In: *Kriminalistik* (3), 194 – 198.

Hardin, Garrett (1968): The Tragedy of the Commons. In: *Science* 162, 1243 – 1248.

Hartigan, John A. (1975): *Cluster Algorithms*. London: John Wiley & Sons.

Hartigan, John A.; Kleiner, Beat (1981): Mosaics for Contingency Tables. In: Eddy, William F. (Hrsg.): *Computer Science and Statistics. Proceedings of the 13th Symposium on the Interface*. New York, NY: Springer, 268 – 273.

Hartigan, John A.; Kleiner, Beat (1984): A Mosaic of Television Ratings. In: *American Statistician* 38 (1), 32 – 35.

Hayek, Friedrich A. (2003): Arten der Ordnung (1963). In: Streit, Manfred E. (Hrsg.): *F.A. Hayek: Rechtsordnung und Handelsordnung. Aufsätze zur Ordnungsökonomik*. Tübingen: Mohr, 15 – 29.

Heclo, Hugh (1978): Issue Networks and the Executive Establishment. In: King, Anthony (Hrsg.): *The New American Political System*. Washington, DC: American Enterprise Institute, 87 – 124.

Hedtkamp, Günter (1996): *Die Bedeutung der Infrastruktur in makroökonomischer Sicht*, Osteuropa-Institut, Thesenpapier.

Held, David (Hrsg.) (2000): *A globalizing world? Culture, Economics, Politics*. London: Routledge.

Held, David; McGrew, Anthony (1999): Globalization. In: *Global Governance* 5 (4), 483 – 496.

Held, David; McGrew, Anthony (2003): Political Globalization: Trends and Choices. In: Kaul, Inge; Conceição, Pedro; Le Goulven, Katell; Mendoza, Ronald U. (Hrsg.): *Providing Global Public Goods. Managing Globalization*. New York, NY: Oxford University Press, 185 – 199.

Held, David; McGrew, Anthony; Goldblatt, David; Perraton, Jonathan (Hrsg.) (1999): *Global Transformations: Politics, Economics, and Culture*. Palo Alto, CA: Stanford University Press.

Held, David; McGrew, Anthony G. (Hrsg.) (2002): *Governing Globalization: Power, Authority, and Global Governance*. Cambridge, MA: Polity Press.

Helmbrecht, Udo (2004): Kritische Infrastrukturen: Präventionsmaßnahmen aus Sicht des BSI. In: Bundeskriminalamt (Hrsg.): *Informations- und Kommunikationskriminalität*. München: Luchterhand, 93 – 100.

Hempel, Carl G.; Oppenheim, Paul (1948): Studies in the Logic of Explanation. In: *Philosophy of Science* 15 (2), 135 – 175.

Hertel, Shareen (2003): The Private Side of Global Governance. In: *Journal of International Affairs* 57 (1), 41 – 50.

Hey, Andreas (2001): Unternehmen und Internet: Aktuelle Sicherheits- und Strafrechtsfragen zur Computerkriminalität. In: *Betrieb und Wirtschaft* (5), 200 – 207.

Hilgendorf, Eric (2004): *Informationsstrafrecht und Rechtsinformatik. Das Strafrecht vor neuen Herausforderungen.* Berlin: Logos.

Hilgendorf, Eric; Frank, Thomas; Valerius, Brian (2005): *Computer- und Internetstrafrecht.* Berlin: Springer.

Hinde, Stephen (2002): The Perils of Privacy. In: *Computers & Security* 21 (5), 424 – 433.

Hirschman, Albert O. (1958): *The Strategy of Economic Development.* New Haven, CT: Yale University Press.

Hirschman, Albert O. (1970): *Exit, Voice, and Loyalty. Responses to Decline in Firms, Organizations, and States.* Cambridge, MA: Harvard University Press.

Hirschman, Albert O. (1984): Against Parsimony: Three easy ways of complicating some categories of economic discourse. In: *American Economic Review* 74 (2), 89 – 96.

Hirschman, Albert O. (1986): The Concept of Interest: From Euphemism to Tautology. In: Hirschman, Albert O. (Hrsg.): *Rival Views of Market Society and Other Recent Essays.* New York, NY: Viking Penguin, 35 – 55.

Hirschman, Albert O. (2002): *Shifting Involvements. Private Interest and Public Action.* Princeton: Princeton University Press.

Hirshleifer, Jack (1983): From Weakest-Link to Best-Shot: The Voluntary Provision of Public Goods. In: *Public Choice* 41, 371 – 386.

Hirshleifer, Jack (1985): From Weakest-Link to Best-Shot: Correction. In: *Public Choice* 46, 221 – 223.

Holitscher, Mark (1999): Global Internet Governance and the Rise of the Private Sector. In: *Schweizerische Zeitschrift für Politikwissenschaft*, 134 – 143.

Holland, John H. (1995): Can There Be a Unified Theory of Complex Adaptive Systems? In: Morowitz, Harold J.; Singer, Jerome L. (Hrsg.): *The Mind, the Brain, and CAS* Bd. 22. Reading, MA: Addison-Wesley, 45 – 50.

Hollingsworth, J. R. (1996): Die Logik der Koordination des verarbeitenden Gewerbes in Amerika. In: Kenis, Patrick; Schneider, Volker (Hrsg.): *Organisation und Netzwerk. Institutionelle Steuerung in Wirtschaft und Politik.* Frankfurt a. M.: Campus, 273 – 311.

Holzinger, Katharina (2001): Aggregation Technology of Common Goods and its Strategic Consequences: Global Warming, Biodiversity and Siting Conflicts. In: *European Journal of Political Research* 40, 117 – 138.

Hughes, Thomas P. (1987): The Evolution of Large Technological Systems. In: Bijker, Wiebe E.; Hughes, Thomas P.; Pinch, Trevor J. (Hrsg.): *The Social Construction of Technological Systems. New Directions in the Sociology and History of Technology.* Cambridge, MA: MIT Press, 51 – 82.

Hummel, Jürgen (1996): Linked bar charts: Analysing categorial data graphically. In: *Computational Statistics* 11 (1), 23 – 33.

Humphreys, Peter J. (1990): The International Political Economy of the Communications Revolution: The Case for a Neo-pluralist Approach. In: *Government and Opposition* 25 (4), 497 – 518.

Hunker, Jeffrey (2002): Policy Challenges in Building Dependability in Global Infrastructures. In: *Computers & Security* 21 (8), 705 – 711.

Hutter, Reinhard (2002): 'Cyber-Terror': Risiken im Informationszeitalter. In: *Aus Politik und Zeitgeschichte* (10 – 11), 31 – 39.

Huysmans, Jef (1998): Security! What Do You Mean? From Concept to Thick Signifier. In: *European Journal of International Relations* 4 (2), 226 – 255.

Hyner, Dirk (2000): *Survival of the Most Flexible? – Eine Analyse der Entwicklung des soziotechnischen Systems Btx/T-Online in einer revolutionär veränderten Umwelt.* Konstanz, Universität Konstanz, Diplomarbeit.

Jaccard, Paul (1908): Nouvelles recherches sur la distribution florale. In: *Bulletin de la Societe Vaudoise de Sciences Naturelles* 44, 223 – 270.

Jackson, Margaret (2000): Keeping Secrets: International developments to protect undisclosed business information and trade secrets. In: Thomas, Douglas; Loader, Brian D. (Hrsg.): *Cybercrime: Law enforcement, security and surveillance in the information age.* London: Routledge, 153 – 172.

James, Jeffrey (2001): The Global Information Infrastructure Revisited. In: *Third World Quaterly* 22 (5), 813 – 822.

Jameson, Fredric (1993): Postmoderne – zur Logik der Kultur im Spätkapitalismus. In: Huyssen, Andreas; Scherpe, Klaus R. (Hrsg.): *Postmoderne. Zeichen eines kulturellen Wandels.* Reinbeck bei Hamburg: Rowohlt, 45 – 102.

Janning, Frank (1998): *Das politische Organisationsfeld: Politische Macht und soziale Homologie in komplexen Demokratien.* Opladen: Westdeutscher Verlag.

Jansen, Dorothea; Schubert, Klaus (Hrsg.) (1995): *Netzwerke und Politikproduktion.* Marburg: Schüren.

Jochimsen, Reimut (1966): *Theorie der Infrastruktur.* Tübingen: Mohr.

Jochimsen, Reimut; Gustafsson, Knut (1977): Infrastruktur. Grundlage der marktwirtschaftlichen Entwicklung. In: Simonis, Ernst (Hrsg.): *Infrastruktur. Theorie und Politik.* Köln: Kiepenheuer & Witsch, 38 – 53.

Joerges, Bernward (1988): Large technical systems: Concepts and issues. In: Mayntz, Renate; Hughes, Thomas P. (Hrsg.): *The Development of Large Technical Systems.* Frankfurt a. M.: Campus, 9 – 36.

Joerges, Bernward (1996): *Technik: Körper der Gesellschaft.* Frankfurt a. M.: Suhrkamp.

Joerges, Bernward; Braun, Ingo (Hrsg.) (1994): *Technik ohne Grenzen.* Frankfurt a. M.: Suhrkamp.

Johnson, David R.; Post, David G. (1997): And How Shall the Net Be Goverened? A Mediation on the Relative Virtues of Decentralized, Emergent Law. In: Kahin, Brian; Keller, James H. (Hrsg.): *Coordinating the Internet.* Cambridge, MA: MIT Press, 62 – 91.

Jones, Candace; Hesterley, William S.; P., Borgatti S. (1997): A General Theory of Network Governance: Exchange Conditions and Social Mechanisms. In: *The Academy of Management Review* 22 (4), 911 – 945.

Jordan, Tim (1999): *Cyberpower. The Culture and Politics of Cyberspace and the Internet.* London: Routledge.

Judge, Anthony J. N. (1995): NGOs and civil society: some realities and distortions; the challenge of "necessary-to-governance organizations" (NGOs). In: *Transnational Associations* 3 (47), 156 – 180.

Just, Natascha; Latzer, Michael; Saurwein, Florian (2006): *Communications Governance: Entschweidungshilfe für die Wahl des Regulierungsarrangements am Beispiel Spam.* <`http://epub.oeaw.ac.at/ita/ita-manuscript/ita_06_02.pdf`>. Online-Ressource, Abruf: 14.12.2006.

Kagan, Robert A. (2001): *Adversarial Legalism. The American Way of Law.* Cambridge, MA: Harvard University Press.

Kahin, Brian; Keller, James H. (Hrsg.) (1997): *Coordinating the Internet.* Cambridge, MA: MIT Press.

Kahler, Miles; Lake, David A. (2003): Globalization and Governance. In: Kahler, Miles; Lake, David A. (Hrsg.): *Governance in a Global Economy. Political Authority in Transition.* Princeton, NJ: Princeton University Press, 1 – 30.

Kahn, David (1996): *The Codebreakers. The Comprehensive History of Secret Communication from Ancient Times to the Internet.* New York, NY: Scribner.

KAISER, Karl (1969): Transnationale Politik. Zu einer Theorie der multinationalen Politik. In: CZEMPIEL, Ernst-Otto (Hrsg.): *Die anachronistische Souveränität. Zum Verhältnis von Innen- und Außenpolitik*. Opladen: Westdeutscher Verlag, 80 – 109.

KAPPELHOFF, Peter (2000a): Komplexitätstheorie und Steuerung von Netzwerken. In: SYDOW, Jörg; WINDELER, Arnold (Hrsg.): *Steuerung von Netzwerken*. Opladen: Westdeutscher Verlag, 347 – 389.

KAPPELHOFF, Peter (2000b): Der Netzwerkansatz als konzeptueller Rahmen für eine Theorie interorganisationaler Netzwerke. In: SYDOW, Jörg; WINDELER, Arnold (Hrsg.): *Steuerung von Netzwerken*. Opladen: Westdeutscher Verlag, 25 – 57.

KAPPELHOFF, Peter (2003a): *Chaos- und Komplexitätstheorie*. <`http://www.wiwi.uni-wuppertal.de/kappelhoff/papers/cckk.pdf`>. Online-Ressource, Abruf: 24.02.2004.

KAPPELHOFF, Peter (2003b): *Evolutionäre Erkenntnistheorie als Grundlage eines aufgeklärten Kritischen Rationalismus*. <`http://www.wiwi.uni-wuppertal.de/kappelhoff/papers/eekr.pdf`>. Online-Ressource, Abruf: 12.03.2004.

KASPERSEN, Henrik (2003): A Gate Must Either Be Open or Be Shut. The Council of Europe Cybercrime Convention Model. In: LEWIS, James A. (Hrsg.): *Cyber Security. Turning National Solutions into International Cooperation*. Washington, DC: CSIS Press, 13 – 29.

KATZ, Raul L. (1988): *The Information Society. An International Perspective*. New York, NY: Praeger.

KAUFFMAN, Stuart A. (1993): *The Origins of Order. Self-Organization and Selection in Evolution*. New York, NY: Oxford University Press.

KAUFFMAN, Stuart A. (1995): *At home in the Universe. The Search for Laws of Self-Organization and Complexity*. Oxford: Oxford University Press.

KAUFMAN, Charlie; PERLMAN, Radia; SPECINER, Mike (1995): *Network Security. Private Communication in a Public World*. Englewood Cliffs, NJ: Prentice Hall.

KAUFMAN, Leonard; ROUSSEEUW, Peter J. (1990): *Finding Groups in Data. An Introduction to Cluster Analysis*. New York, NY: John Wiley & Sons.

KAUFMANN, Franz-Xaver (1973): *Sicherheit als soziologisches und sozialpolitisches Problem. Untersuchungen zu einer Wertidee hochdifferenzierter Gesellschaften*. Stuttgart: Ferdinand Enke Verlag.

KAUL, Inge; CONCEIÇÃO, Pedro; LE GOULVEN, Katell; MENDOZA, Ronald U. (2003): Why Do Global Public Goods Matter Today? In: KAUL, Inge; CONCEIÇÃO, Pedro; LE GOULVEN, Katell; MENDOZA, Ronald U. (Hrsg.): *Providing Global Public Goods. Managing Globalization*. New York, NY: Oxford University Press, 2 – 20.

Kenis, Patrick; Schneider, Volker (1991): Policy Networks and Policy Analysis: Scrutinizing a New Analytical Toolbox. In: Marin, Bernd; Mayntz, Renate (Hrsg.): *Policy Networks. Empirical Evidence and Theoretical Considerations.* Frankfurt a. M.: Campus, 25 – 59.

Keohane, Robert O. (2002): *Power and Governance in a Partially Globalized World.* London: Routledge.

Keohane, Robert O. (2005): *After Hegemony. Cooperation and Discord in the World Political Economy.* Princeton, NJ: Princeton University Press.

Keohane, Robert O.; Nye, Joseph S. (1977): *Power and Interdependence. World Politics in Transition.* Boston, MA: Little, Brown & Co.

Keohane, Robert O.; Nye, Joseph S. (2000a): Globalization: What's New? What's Not? (And So What?). In: *Foreign Policy* 118, 104 – 119.

Keohane, Robert O.; Nye, Joseph S. (2000b): Introduction. In: Nye, Joseph S.; Donahue, John D. (Hrsg.): *Governance in a Globalizing World.* Washington, DC: Brookings Institution, 1 – 41.

Kesdogan, Dogan (2000): *Privacy im Internet. Vertrauenswürdige Kommunikation in offenen Umgebungen.* Braunschweig: Vieweg.

Köhntopp, Marit; Köhntopp, Kristian (2000): Datenspuren im Internet. In: *Computer und Recht* (4), 248 – 257.

Kleinsteuber, Hans J. (1983): Regulierung und politisch-ökonomische Kultur der USA. In: Thiemeyer, Theo (Hrsg.): *Öffentliche Bindung von Unternehmen. Beiträge zur Regulierungsdebatte.* Baden-Baden: Nomos, 175 – 192.

Kleinsteuber, Hans J. (2006): Was kommt nach der Verrechtlichung? Von der Regulierung zur Governance. In: Klumpp, Dieter; Kubicek, Herbert; Rossnagel, Alexander; Schulz, Wolfgang (Hrsg.): *Medien, Ordnung und Innovation.* Berlin: Springer, 185 – 199.

Knill, Christoph; Lehmkuhl, Dirk (2002a): Governance and Globalization: Conceptualizing the Role of Public and Private Actors. In: Héritier, Adrienne (Hrsg.): *Common Goods. Reinventing European and International Governance.* Lanham: Rowman & Littlefield, 85 – 104.

Knill, Christoph; Lehmkuhl, Dirk (2002b): Private Actors and the State: Internationalization and Changing Patterns of Governance. In: *Governance* 15 (1), 41 – 63.

Koch, Alexander (2008): *Strafrechtliche Probleme des Angriffs und der Verteidigung in Computernetzen.* Baden-Baden: Nomos. Universität Marburg, Dissertation.

Koch, Karl-Friedrich (2001): Electronic Commerce: Chancen auch für Kriminelle? In: *Kriminalistik* (3), 179 – 185.

Kolb, Anne (2000): *Transport und Nachrichtentransfer im Römischen Reich.* Berlin: Akademie Verlag.

Kooiman, Jan (Hrsg.) (1993): *Modern Governance. New Government – Society Interactions.* London: Sage.

Kooiman, Jan (2002): Governance: A Social-Political Perspective. In: Grote, Jürgen R.; Gbikpi, Bernard (Hrsg.): *Participatory Governance. Political and Social Implications.* Opladen: Leske + Budrich, 71 – 96.

Koop, Bert-Jaap (2008): *Crypto Law Survey.* <`http://rechten.uvt.nl/koops/cryptolaw/`>. Online-Ressource, Abruf: 25.03.2008.

Krahmann, Elke (2005): Security Governance and Networks: New Theoretical Perspectives in Transatlantic Security. In: *Cambridge Review of International Affairs* 18 (1), 15 – 30.

Krause, Keith; Williams, Michael (1996): *Critical Security Studies.* Minneapolis, MN: University of Minneapolis Press.

Krohn, Wolfgang; Küppers, Günter (Hrsg.) (1992): *Emergenz: Die Entstehung von Ordnung, Organisation und Bedeutung.* Frankfurt a. M.: Suhrkamp.

Kubicek, Herbert (1997): Das Internet auf dem Weg zum Massenmedium? Ein Versuch, Lehren aus der Geschichte alter und neuer Medien zu ziehen. In: Werle, Raymund; Lang, Christa (Hrsg.): *Modell Internet? Entwicklungsperspektiven neuer Kommunikationsnetze.* München: Campus, 213 – 239.

Kuhlen, Rainer (1995): *Informationsmarkt: Chancen und Risiken der Kommerzialisierung von Wissen.* Konstanz: Universitätsverlag.

Kuhlen, Rainer (1997): Hypertext. In: Buder, Marianne; Rehfeld, Werner; Seeger, Thomas; Dietmar, Strauch (Hrsg.): *Grundlagen der praktischen Information und Dokumentation.* München: Saur, 355 – 369.

Kuhlen, Rainer (1999): *Die Konsequenzen von Informationsassistenten. Was bedeutet informationelle Autonomie oder wie kann Vertrauen in elektronische Dienste in offenen Informationsmärkten gesichert werden?* Frankfurt a.M.: Suhrkamp.

Kuhlen, Rainer (2005): Informationsethik: Die Entwicklung von Normen für den Umgang mit Wissen und Information in elektronischen Räumen. In: Hauke, Petra (Hrsg.): *Bibliothekswissenschaft – quo vadis? Eine Disziplin zwischen Traditionen und Visionen. Programme – Modelle – Forschungsaufgaben.* München: K.G. Saur, 159 – 172.

Kuhn, Thomas S. (1962): *The Structure of Scientific Revolutions.* Chicago, IL: University of Chicago Press.

Kyas, Othmar; a Campo, Markus (2002): *IT-Crackdown. Sicherheit im Internet.* Bonn: mitp-Verlag.

Lance, G. N.; Williams, William T. (1966): A general theory of classificatory sorting strategies: 1. Hierarchical systems. In: *Computer Journal* (9), 373 – 380.

Latzer, Michael (1997): *Mediamatik. Die Konvergenz von Telekommunikation, Computer und Rundfunk.* Opladen: Westdeutscher Verlag.

Latzer, Michael; Just, Natascha; Saurwein, Florian; Slominski, Peter (2002): *Selbst- und Ko-Regulierung im Mediamatiksektor. Alternative Regulierungsformen zwischen Staat und Markt.* Wiesbaden: Westdeutscher Verlag.

Latzer, Michael; Schmitz, Stefan W. (2002): *Die Ökonomie des eCommerce. New Economy, Digitale Ökonomie und realwirtschaftliche Auswirkungen.* Marburg: Metropolis.

Laumann, Edward O.; Knoke, David (1987): *The Organizational State. Social Choice in National Policy Domain.* Madison: University of Wisconsin Press.

Lax, David A.; Sebenius, James K. (1986): *The Manager as Negotiator: Bargaining for Cooperation and Competitive Gain.* New York, NY: Free Press.

Lehmbruch, Gerhard (1967): *Proporzdemokratie. Politisches System und politische Kultur in der Schweiz und in Österreich.* Tübingen: Mohr.

Leib, Volker (2002): *ICANN und der Konflikt um die Internet-Ressourcen: Institutionenbildung im Problemfeld Internet Governance zwischen multinationaler Staatstätigkeit und globaler Selbstregulierung.* Konstanz, Universität Konstanz, Dissertation.

Lepschies, Gunter (2000): *E-Commerce und Hackerschutz. Leitfaden für die Sicherheit elektronischer Zahlungssysteme.* Braunschweig: Vieweg.

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

Lewis, James A. (Hrsg.) (2003a): *Cyber Security. Turning National Solutions into International Cooperation.* Washington, DC: CSIS Press.

Lewis, James A. (2003b): Introduction. In: Lewis, James A. (Hrsg.): *Cyber Security. Turning National Solutions into International Cooperation.* Washington, DC: CSIS Press, xi – xxiii.

Lewis, James A. (2003c): Overcoming Obstacles to Cooperation. The Council of Europe Convention on Cybercrime. In: Lewis, James A. (Hrsg.): *Cyber Security. Turning National Solutions into International Cooperation.* Washington, DC: CSIS Press, 90 – 97.

Li, Ming; Vitanyi, Paul (1993): *An Introduction to Kolmogorov Complexity and Its Applications.* New York, NY: Springer.

Libicki, Martin C. (2007): *Conquest in Cyberspace. National Security and Information Warfare.* Cambridge, MA: Cambridge University Press.

Liebowitz, S.J.; Margolis, Stephen E. (1995): Are Network Externalities a New Source of Market Failure? In: *Research in Law and Economics* 17, 1 – 22.

Lincke, David-Michael (1998): Evaluating Integrated Electronic Commerce Systems. In: *Electronic Markets* 8 (1), 7 – 11.

Lindblom, Charles E. (2001): *The Market System: What It Is, How It Works, and What To Make of It.* New Haven, CT: Yale University Press.

Lipp, Peter (2003): On Technical Trust: An Introduction. In: Petrovic, Otto; Ksela, Michael; Fallenböck, Markus; Kittl, Christian (Hrsg.): *Trust in the Network Economy.* Wien: Springer, 243 – 252.

Long, William J.; Quek, Marc P. (2002): Personal Data Privacy Protection in an Age of Globalization: The US-EU Safe Harbor Compromise. In: *Journal of European Public Policy* 9 (3), 325 – 344.

Lorenz, Konrad (1973): *Die Rückseite des Spiegels. Versuch einer Naturgeschichte des menschlichen Erkennens.* München: Piper.

Lütz, Susanne (2003): *Governance in der politischen Ökonomie.* Köln, Max-Planck-Institut für Gesellschaftsforschung, Discussion Paper.

Luhmann, Niklas (1975): *Soziologische Aufklärung 2.* Opladen: Westdeutscher Verlag.

Luhmann, Niklas (1990): *Risiko und Gefahr.* St. Gallen: Hochschule St. Gallen für Wirtschafts-, Rechts- und Sozialwissenschaften.

Luhmann, Niklas (1991): *Soziologie des Risikos.* Berlin: de Gruyter.

Luhmann, Niklas (1993a): Die Moral des Risikos und das Risiko der Moral. In: Bechmann, Gotthard (Hrsg.): *Risiko und Gesellschaft. Grundlagen und Ergebnisse interdisziplinärer Risikoforschung.* Opladen: Westdeutscher Verlag, 327 – 338.

Luhmann, Niklas (1993b): *Soziale Systeme. Grundriß einer allgemeinen Theorie.* Frankfurt a. M.: Suhrkamp.

Lyre, Holger (2002): *Informationstheorie. Eine philosophisch-naturwissenschaftliche Einführung.* München: Wilhelm Fink.

Machlup, Fritz (1962): *The Production and Distribution of Knowledge in the United States.* Princeton, NJ: Princeton University Press.

Mainzer, Klaus (2004): *Thinking in Complexity. The Complex Dynamics of Matter, Mind, and Mankind.* Berlin: Springer.

March, James G.; Simon, Herbert A. (1958): *Organizations.* New York, NY: John Wiley & Sons.

Marin, Bernd (Hrsg.) (1990a): *Generalized Political Exchange. Antagonistic Cooperation and Integrated Policy Circuits.* Frankfurt a. M.: Campus.

Marin, Bernd (Hrsg.) (1990b): *Governance and Generalized Exchange. Self-Organizing Policy Networks in Action.* Frankfurt a. M.: Campus.

Marsden, Christopher T. (2000a): Information and communications technologies, globalisation and regulation. In: Marsden, Christopher T. (Hrsg.): *Regulating the Global Information Society.* London: Routledge, 1 – 40.

Marsden, Christopher T. (Hrsg.) (2000b): *Regulating the Global Information Society.* London: Routledge.

Maturana, Humberto R. (1980): Biology of Cognition. In: Varela, Francisco J.; Maturana, Humberto R. (Hrsg.): *Autopoiesis and Cognition: The Realization of the Living.* Dordrecht: Reidel, 5 – 58.

Mayntz, Renate (1987): Politische Steuerung und gesellschaftliche Steuerungsprobleme – Anmerkungen zu einem theoretischen Paradigma. In: Ellwein, Thomas; Hesse, Joachim J.; Mayntz, Renate; Scharpf, Fritz W. (Hrsg.): *Jahrbuch zur Staats- und Verwaltungswissenschaft* Bd. 1. Baden-Baden: Nomos, 89 – 110.

Mayntz, Renate (1988a): Soziale Diskontinuitäten: Erscheinungsform und Ursachen. In: Hierholzer, Klaus; Wittmann, Heinz-Günter (Hrsg.): *Phasensprünge und Stetigkeit in der natürlichen und kulturellen Welt – Wissenschaftskonferenz in Berlin 8. – 10. Oktober 1987.* Stuttgart: Wissenschaftliche Verlagsgesellschaft, 15 – 37.

Mayntz, Renate (1988b): Zur Entwicklung technischer Infrastruktursysteme. In: Mayntz, Renate; Rosewitz, Bernd; Schimank, Uwe; Stichweh, Rudolf (Hrsg.): *Differenzierung und Verselbständigung. Zur Entwicklung gesellschaftlicher Teilsysteme.* Frankfurt a. M.: Campus, 233 – 259.

Mayntz, Renate (1993): Große Technische Systeme und ihre gesellschaftstheoretische Bedeutung. In: *Kölner Zeitschrift für Soziologie und Sozialpsychologie* 45 (1), 97 – 108.

Mayntz, Renate (1995): Zum Status der Theorie sozialer Differenzierung als Theorie sozialen Wandels. In: Müller, Hans-Peter; Schmid, Michael (Hrsg.): *Sozialer Wandel. Modellbildung und theoretische Ansätze.* Frankfurt a. M.: Suhrkamp, 139 – 150.

Mayntz, Renate (1996): Policy-Netzwerke und die Logik von Verhandlungssystemen. In: Kenis, Patrick; Schneider, Volker (Hrsg.): *Organisation und Netzwerk: Institutionelle Steuerung in Wirtschaft und Politik.* Frankfurt a. M.: Campus, 471 – 496.

Mayntz, Renate (1997a): *Soziale Dynamik und politische Steuerung. Theoretische und methodologische Überlegungen.* Frankfurt a. M.: Campus.

Mayntz, Renate (1997b): *Soziologie der öffentlichen Verwaltung.* Heidelberg: Müller.

Mayntz, Renate (2002a): Common Goods and Governance. In: Héritier, Adrienne (Hrsg.): *Common Goods. Reinventing European and International Governance.* Lanham: Rowman & Littlefield, 15 – 27.

MAYNTZ, Renate (2002b): Zur Theoriefähigkeit makro-sozialer Analysen. In: MAYNTZ, Renate (Hrsg.): *Akteure – Mechanismen – Modelle: Zur Theoriefähigkeit makro-sozialer Analysen.* Frankfurt a. M.: Campus, 7 – 43.

MAYNTZ, Renate (2004): *Governance Theory als fortentwickelte Steuerungstheorie?* Köln, Max-Planck-Institut für Gesellschaftsforschung, Working Paper.

MAYNTZ, Renate (2005): *Embedded Theorizing. Perspectives on Globalization and Global Governance.* Köln, Max-Planck-Institut für Gesellschaftsforschung, Discussion Paper.

MAYNTZ, Renate; HUGHES, Thomas P. (1988): *The Development of Large Technical Systems.* Frankfurt a. M.: Campus.

MAYNTZ, Renate; ROSEWITZ, Bernd; SCHIMANK, Uwe; STICHWEH, Rudolf (Hrsg.) (1988): *Differenzierung und Verselbständigung. Zur Entwicklung gesellschaftlicher Teilsysteme.* Frankfurt a. M.: Campus.

MAYNTZ, Renate; SCHARPF, Fritz W. (1995a): Der Ansatz des akteurzentrierten Institutionalismus. In: MAYNTZ, Renate; SCHARPF, Fritz W. (Hrsg.): *Gesellschaftliche Selbstregelung und Politische Steuerung.* Frankfurt a. M.: Campus, 39 – 72.

MAYNTZ, Renate; SCHARPF, Fritz W. (1995b): Steuerung und Selbstorganisation in staatsnahen Sektoren. In: MAYNTZ, Renate; SCHARPF, Fritz W. (Hrsg.): *Gesellschaftliche Selbstregulierung und politische Steuerung.* Frankfurt a. M.: Campus, 9 – 38.

MCLUHAN, Marshall (1962): *The Gutenberg Galaxy: The Making of Typographic Man.* London: Routledge & Kegan Paul.

MEAD, George H. (1998): *Geist, Identität und Gesellschaft.* Frankfurt a. M.: Suhrkamp.

MENDEZ, Fernando (2005): The European Union and cybercrime: Insights from Comperative Federalism. In: *Journal of European Public Policy* 12 (3), 509 – 527.

MICROSOFT CORPORATION (2009): *Microsoft Security Intelligence Report Volume 7 (January – June 2009).* <`http://www.microsoft.com/downloads/details.aspx?FamilyID=037f3771-330e-4457-a52c-5b085dc0a4cd&displaylang=en`>. Online-Ressource, Abruf: 03.11.2009.

MIHALACHE, Adrian (2002): The Cyber Space-Time Continuum: Meaning and Metaphor. In: *The Information Society* (4), 293 – 301.

MITTELSTRASS, Jürgen (2001): Konstruktion und Deutung. Über Wissenschaft in einer Leonardo- und Leibniz-Welt. Festvortrag anläßlich der Verleihung der Ehrendoktorwürde der Humboldt-Universität zu Berlin.

MITTERAUER, Michael (1998): Predigt – Holzschnitt – Buchdruck: Europäische Frühformen der Massenkommunikation. In: *Beiträge zur historischen Sozialkunde* (2), 69 – 78.

Münker, Stefan (1997): Was heißt eigentlich: „virtuelle Realität“? Ein philosophischer Kommentar zum neuesten Versuch der Verdopplung der Welt. In: Münker, Stefan; Roesler, Alexander (Hrsg.): *Mythos Internet*. Frankfurt a. M.: Suhrkamp, 108 – 127.

Münkler, Herfried (2006): *Der Wandel des Krieges. Von der Symmetrie zur Asymmetrie*. Weilerswist: Velbrück Wissenschaft.

Molander, Roger C.; Riddile, Andrew S.; Wilson, Peter A. (1996): *Strategic Information Warfare. A New Face of War*. Santa Monica, CA, RAND Corporation, Forschungsbericht.

Moore, Gordon E. (1965): Cramming more components onto integrated circuits. In: *Electronics* 38, 114 – 117.

Morris, Charles W. (1966): *Foundations of the Theory of Signs*. Chicago, IL: University of Chicago Press.

Murauer, Johann (2001): *Informationsflussorientierte Verfahren zum Zugriffschutz in Computersystemen*. Linz, Johannes-Kepler-Universität, Dissertation.

Musgrave, Richard A. (1957): A Multiple Theory of Budget Determination. In: *FinanzArchiv* 17 (3), 333 – 243.

Musgrave, Richard A. (1959): *The Theory of Public Finance. A Study in Public Economy*. New York, NY: McGraw-Hill.

Nash, Andrew; Duane, William; Joseph, Celia; Brink, Derek (2002): *PKI. E-Security implementieren*. Bonn: mitp-Verlag.

Nash, John F. (1951): Non-Cooperative Games. In: *Annals of Mathematics* 54, 286 – 295.

Negroponte, Nicholas (1995): *Being Digital*. London: Hodder & Stoughton.

Newman, Abraham L. (2007): Protecting Privacy in Europe: Administrative Feedbacks and Regional Politics. In: Meunier, Sophie; McNamara, Kate (Hrsg.): *Making History: The State of the European Union*. Oxford: Oxford University Press.

Newman, Abraham L.; Bach, David (2004): Self-Regulatory Trajectories in the Shadow of Public Power: Resolving Digital Dilemmas in Europe and the United States. In: *Governance* 17 (3), 387 – 413.

Nichols, Gerald E. (1987): On the Nature of Management Information. In: Galliers, Robert (Hrsg.): *Information Analysis. Selected Readings*. Sydney: Addison-Wesley, 7 – 17.

Nissen, Hans J.; Damerow, Peter; Englund, Robert K. (2004): *Informationsverarbeitung vor 5000 Jahren. Frühe Schrift und Techniken der Wirtschaftsverwaltung im alten Vorderen Orient*. Hildesheim: Franzbecker.

Nora, Simon; Minc, Alain (1979): *Die Informatisierung der Gesellschaft. Herausgegeben von Uwe Kalbhen*. Frankfurt a. M.: Campus.

Nordhaus, William D. (2000): Globale öffentliche Güter. In: Krull, Wilhelm (Hrsg.): *Zukunftsstreit*. Weilerswist: Velbrück Wissenschaft, 187 – 201.

North, Douglas (1991): Institutions. In: *Journal of Economic Perspectives* 5, 97 – 112.

Northcutt, Stephen; Novak, Judy (2001): *IDS: Intrusion Detection Systeme. Spurensuche im Internet*. Bonn: mitp-Verlag.

Noyce, Robert N. (1980): Microelectronics. In: Forester, Tom (Hrsg.): *The Microelectronics Revolution*. Oxford: Blackwell, 29 – 41.

Nye, Joseph S. (2004): *Power in the Global Information Age. From realism to globalization*. London: Routledge.

OECD (2012): *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy. OECD Digital Economy Papers No. 211*. <`http://dx.doi.org/10.1787/5k8zq92vdgtl-en`>. Online-Ressource.

Olson, Mancur (1965): *The Logic of Collective Action. Public Goods and the Theory of Groups*. Cambridge, MA: Harvard University Press.

Oppenheim, Paul; Putnam, Hilary (1958): Unity of Science as a Working Hypothesis. In: Feigl, Herbert; Scriven, Michael; Maxwell, Grover (Hrsg.): *Concepts, Theories, and the Mind-Body-Problem. Minnesota Studies in the Philosophy of Science*. Minneapolis, MN: University of Minnesota Press, 3 – 36.

Ortega y Gasset, José (1978): Betrachtungen über die Technik. In: Ortega y Gasset, José (Hrsg.): *Gesammelte Werke. Bd. 4*. Stuttgart: Deutsche Verlags-Anstalt, 7 – 69.

Ostrom, Elinor (1993): *Governing the Commons. The Evolution of Institutions for Collective Action*. Cambridge, UK: Cambridge University Press.

Ostrom, Elinor (2002): Property-Rights Regimes and Common Goods: A Complex Link. In: Héritier, Adrienne (Hrsg.): *Common Goods. Reinventing European and International Governance*. Lanham: Rowman & Littlefield, 29 – 57.

Pappi, Franz U. (1987): Die Netzwerkanalyse aus soziologischer Persektive. In: Pappi, Franz U. (Hrsg.): *Methoden der Netzwerkanalyse*. München: Oldenbourg, 11 – 37.

Parsons, Talcott (1951): *The Social System*. Glencoe, IL: Free Press.

Parsons, Talcott (1971): *The System of Modern Societies*. Englewood Cliffs, NJ: Prentice Hall.

Pattberg, Philipp (2005): The Institutionalization of Private Governance: How Business and Nonprofit Organizations Agree on Transnational Rules. In: *Governance* 18 (4), 399 – 429.

Pawlak, Patryk; Wendling, Cécile (2013): Trends in cyberspace: can governments keep up? In: *Environment Systems and Decisions* 33 (4), 536 – 543.

Peirce, Charles S. (1998a): *Phänomen und Logik der Zeichen.* Frankfurt a. M.: Suhrkamp.

Peirce, Charles S. (1998b): A Sketch of Logical Critics. In: Peirce Edition Project (Hrsg.): *The Essential Peirce. Selected Philosophical Writings. Vol. 1, 1867–1893.* Bloomington: Indiana University Press, 451 – 462.

Peirce, Charles S. (1878): How to Make Our Ideas Clear. In: *Popular Science Monthly* (12), 286 – 302.

Peltzman, Sam (1993): George Stigler's Contribution to the Economic Analysis of Regulation. In: *Journal of Political Economy* 101 (5), 818 – 832.

Perrow, Charles (1996): Eine Gesellschaft von Organisationen. In: Kenis, Patrick; Schneider, Volker (Hrsg.): *Organisation und Netzwerk. Institutionelle Steuerung in Wirtschaft und Politik.* Frankfurt a. M.: Campus, 75 – 121.

Perrow, Charles (2002): *Organizing America. Wealth, Power, and the Origins of Corporate Capitalism.* Princeton, NJ: Princeton University Press.

Petrovic, Otto; Ksela, Michael; Fallenböck, Markus; Kittl, Christian (Hrsg.) (2003): *Trust in the Network Economy.* Wien: Springer.

Pfister, Christa (2007): *Hacking. Die Schweizer Hacking-Strafnorm (Art. 143bis StGB) im Vergleich mit den Bestimmungen der Cybercrime Convention, des Rechts der Europäischen Union, des deutschen und des österreichischen Strafrechts.* Zürich, Universität Zürich, Dissertation.

Philippsohn, Steven (2001): Trends In Cybercrime: An Overview Of Current Financial Crimes On The Internet. In: *Computers & Security* 20 (1), 53 – 69.

Phillips, John T. (2002): Privacy vs. Cybersecurity. In: *Information Management Journal* 36 (3), 46 – 49.

Popper, Karl R. (1934): *Logik der Forschung.* Wien: Springer.

Popper, Karl R. (1972): *Objective Knowledge: An Evolutionary Approach.* Oxford: Oxford University Press.

Popper, Karl R. (1994): *Alles Leben ist Problemlösen: Über Erkenntnis, Geschichte und Politik.* München: Piper.

Porat, Marc U. (1977): *The Information Economy: Definition and Measurement.* Washington, DC: US Government Printing Office.

Poullet, Yves (2004): The Fight against Crime and/or the protection of Privacy: A Thorny Debate! In: *International Review of Law, Computers & Technology* 18 (2), 251 – 273.

Powell, Walter W. (1996): Weder Markt noch Hierarchie: Netzwerkartige Organisationsformen. In: Kenis, Patrick; Schneider, Volker (Hrsg.): *Organisation und Netzwerk. Institutionelle Steuerung in Wirtschaft und Politik.* Frankfurt a. M.: Campus, 213 – 272.

Powell, Walter W.; Clemens, Elisabeth S. (Hrsg.) (1998): *Private Action and the Public Good.* New Haven, CT: Yale University Press.

Price, E. M.; Verhulst, Stefaan G. (2000): In search of the self: charting the course of self-regulation on the Internet in a global environment. In: Marsden, Christopher T. (Hrsg.): *Regulating the Global Information Society.* London: Routledge, 57 – 78.

Putnam, Robert D. (1993): *Making Democracy Work. Civic Traditions in Modern Italy.* Princeton, NJ: Princeton University Press.

Putnam, Tonya L.; Elliott, David D. (2001): International Responses to Cyber Crime. In: Sofaer, Abraham D.; Goodman, Seymour E. (Hrsg.): *The Transnational Dimension of Cyber Crime and Terrorism.* Stanford, CA: Hoover Institution Press, 35 – 67.

Raab, Charles D. (1993): The Governance of Data Protection. In: Kooiman, Jan (Hrsg.): *Modern Governance. New Government – Society Interactions.* London: Sage, 89 – 103.

Raab, Charles D. (2006): The Governance of Global Issues: Protecting Privacy in Personal Information. In: Koenig-Archibugi, Mathias; Zürn, Michael (Hrsg.): *New Modes of Governance in the Global System. Exploring Publicness, Delegation and Inclusiveness.* Basingstoke: Palgrave Macmillan, 125 – 153.

Raepple, Martin (2001): *Sicherheitskonzepte für das Internet. Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung.* Heidelberg: dpunkt-Verlag.

Rammert, Werner (1999): *Technik: Stichwort für eine Enzyklopädie.* Berlin, Technische Universität Berlin, Institut für Sozialwissenschaften, Working Paper.

Rammert, Werner (2000): *Technik aus soziologischer Perspektive 2: Kultur – Innovation – Virtualität.* Wiesbaden: Westdeutscher Verlag.

Rammstedt, Otthein (1992): Risiko. In: Ritter, Joachim; Gründer, Karlfried (Hrsg.): *Historisches Wörterbuch der Philosophie. Bd. 8.* Basel: Schwabe & Co., 1045 – 1051.

Randazzo, Marisa R.; Keeney, Michelle; Kowalski, Eileen; Cappelli, Dawn; Moore, Andrew (2004): *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector.* <`http://www.secretservice.gov/ntac/its_report_040820.pdf`>. Online-Ressource, Abruf: 05.01.2006. Studie des U.S. Secret Service in Zusammenarbeit mit dem CERT/CC.

Rathmell, Andrew (2001): Protecting Critical Information Infrastructure. In: *Computers & Security* 20 (1), 43 – 52.

Ratzel, Max-Peter (2004): Kriminalitätsbekämpfung im Internet. Konzepte, Strategien, Handlungsempfehlungen aus polizeilicher Sicht. In: von Knop, Jan; Frank, Hans (Hrsg.): *Netz- und Computersicherheit. Sind wir auf einen Angriff auf unsere Informationssysteme und Informations-Infrastrukturen vorbereitet?* Bielefeld: Bertelsmann, 137 – 148. Kongressband 2003 der Bundesakademie für Sicherheitspolitik und der Heinrich-Heine-Universität Düsseldorf.

Reindl, Josef (1998): Partikularstaatliche Politik und technische Dynamik: Die drahtgebundene Telegraphie und der Deutsch-Österreichische Telegraphenverein von 1850. In: Teuteberg, Hans-Jürgen; Neutsch, Cornelius (Hrsg.): *Vom Flügeltelegraphen zum Internet. Geschichte der modernen Telekommunikation.* Stuttgart: Steiner, 27 – 46.

Reinermann, Dirk; Weber, Joachim (2004): Analyse Kritischer Infrastrukturen. In: von Knop, Jan; Frank, Hans (Hrsg.): *Netz- und Computersicherheit. Sind wir auf einen Angriff auf unsere Informationssysteme und Informations-Infrastrukturen vorbereitet?* Bielefeld: Bertelsmann, 309 – 320. Kongressband 2003 der Bundesakademie für Sicherheitspolitik und der Heinrich-Heine-Universität Düsseldorf.

Reinicke, Wolfgang H. (1998a): *Global Public Policy. Governing without Government?* Washington, DC: Brookings Institution.

Reinicke, Wolfgang H. (1998b): Hands on the Bridge. In: *World Link* (1/2), 40 – 42.

Reinicke, Wolfgang H. (1999): The Other World Wide Web: Global Public Policy Networks. In: *Foreign Policy* (Winter 1999/2000), 44 – 57.

Reinicke, Wolfgang H.; Benner, Thorsten; Witte, Jan M. (2001): Global Public Policy: Globalisierung gestalten durch globale Politiknetzwerke. In: Oberreuter, Heinrich; Piazolo, Michael (Hrsg.): *Global Denken. Die Rolle des Staates in der internationalen Politik zwischen Kontinuität und Wandel.* München: Olzog, 265 – 277.

Reitinger, Philip (2000): Encryption, Anonymity and Markets: Law enforcement and technology in a free market virtual world. In: Thomas, Douglas; Loader, Brian D. (Hrsg.): *Cybercrime: Law enforcement, security and surveillance in the information age.* London: Routledge, 132 – 152.

Rheingold, Howard (1995): *Virtuelle Welten. Reisen im Cyberspace.* Reinbek bei Hamburg: Rowohlt.

Rhodes, Rod A. W. (1996): The New Governance: Governing without Government. In: *Political Studies* 44, 652 – 667.

Rhodes, Rod A. W. (1997): *Understanding Governance: Policy Networks, Reflexivity, and Accountability.* Buckingham, PA: Open University Press.

Richardson, George B. (1972): The Organization of Industry. In: *Economic Journal* 82, 883 – 896.

Richter, Wolfram F.; Wiegard, Wolfgang (1993): Zwanzig Jahre „Neue Finanzwissenschaft“. Teil I: Überblick und Theorie des Marktversagens. In: *Zeitschrift für Wirtschafts- und Sozialwissenschaften* (113), 169 – 224.

Riepl, Wolfgang (1913): *Das Nachrichtenwesen des Altertums. Mit besonderer Rücksicht auf die Römer*. Leipzig: Teubner.

Rifkin, Jeremy (2000): *Access. Das Verschwinden des Eigentums*. 2. Frankfurt a. M.: Campus.

Rinaldi, Steven M.; Peerenboom, James P.; Kelly, Terrence K. (2001): Identifying, Understanding, and Analyzing Critical Infrastructure Dependencies. In: *IEEE Control Systems Magazine* 21 (6), 11 – 25.

Risse-Kappen, Thomas (1995): Structures of governance and transnational relations: what have we learned? In: Risse-Kappen, Thomas (Hrsg.): *Bringing transnational relations back in: non-state actors, domestic structures and international institutions*. Cambridge, UK: Cambridge University Press, 280 – 313.

Roberts, Alasdair (2001): The informational commons at risk. In: Drache, Daniel (Hrsg.): *The Market or the Public Domain*. London, UK: Routledge, 175 – 201.

Ronit, Karsten; Schneider, Volker (1999): Global Governance through Private Organizations. In: *Governance* 12, 243 – 266.

Ronit, Karsten; Schneider, Volker (2000a): Private organizations and their contribution to problem-solving in the global arena. In: Ronit, Karsten; Schneider, Volker (Hrsg.): *Private Organizations in Global Politics*. London: Routledge, 1 – 33.

Ronit, Karsten; Schneider, Volker (Hrsg.) (2000b): *Private Organizations in Global Politics*. London: Routledge.

Rosenau, James N.; Czempiel, Ernst-Otto (Hrsg.) (1992): *Governance without Government: Order and Change in World Politics*. Cambridge, MA: Cambridge University Press.

Roth, Gerhard; Schwegler, Helmut (1995): Das Geist-Gehirn-Problem aus der Sicht der Hirnforschung und eines nicht-reduktionistischen Physikalismus. In: *Ethik und Sozialwissenschaften* 6 (1), 69 – 77.

Rubin, Michael R.; Huber, Mary T. (1986): *The Knowledge Industry in the United States 1960 – 1980*. Princeton: Princeton University Press.

Rustemeyer, Frank (2004): Der Mitarbeiter – ein zentraler Risikofaktor für die IT-Sicherheit? In: von Knop, Jan; Frank, Hans (Hrsg.): *Netz- und Computersicherheit. Sind wir auf einen Angriff auf unsere Informationssysteme und Informations-Infrastrukturen vorbereitet?* Bielefeld: Bertelsmann, 239 – 254. Kongressband 2003 der Bundesakademie für Sicherheitspolitik und der Heinrich-Heine-Universität Düsseldorf.

Salus, Peter H. (1995): *Casting the Internet: From ARPANET to Internet and Beyond*. Reading, MA: Addison-Wesley.

Salzmann, Oliver; Steger, Ulrich; Ionescu-Somers, Aileen (2008): Determinants of corporate sustainability management: An empirical contingency approach. In: *Zeitschrift für Betriebswirtschaft: Corporate Social Responsibility* (Special Issue 3), 1 – 22.

Samuelson, Paul (1954): Diagrammatic Exposition of a Theory of Public Expenditure. In: *Review of Economics and Statistics* 36 (4), 387 – 389.

Sandler, Todd (2004): *Global Collective Action*. Cambridge, UK: Cambridge University Press.

Sandmo, Agnar (2003): International Aspects of Public Goods Provision. In: Kaul, Inge; Conceição, Pedro; Le Goulven, Katell; Mendoza, Ronald U. (Hrsg.): *Providing Global Public Goods. Managing Globalization*. New York, NY: Oxford University Press, 112 – 130.

Saussure, Ferdinand de (1931): *Grundfragen der allgemeinen Sprachwissenschaft*. Berlin: de Gruyter.

Scharpf, Fritz W. (1991): Die Handlungsfähigkeit des Staates am Ende des zwanzigsten Jahrhunderts. In: *Politische Vierteljahresschrift* (32), 621 – 634.

Scharpf, Fritz W. (1994a): *Efficient Self-Coordination in Policy Networks. A Simulation Study*. Köln, Max-Planck-Institut für Gesellschaftsforschung, Discussion Paper.

Scharpf, Fritz W. (1994b): Politiknetzwerke als Steuerungssubjekte. In: Derlien, Hans U.; Gerhardt, Uta; Scharpf, Fritz W. (Hrsg.): *Systemrationalität und Partialinteresse. Festschrift für Renate Mayntz*. Baden-Baden: Nomos, 381 – 407.

Scharpf, Fritz W. (2000): *Interaktionsformen. Akteurzentrierter Institutionalismus in der Politikforschung*. Opladen: Leske + Budrich.

Schaumüller-Bichl, Ingrid (1992): *Sicherheitsmanagement. Risikobewältigung in informationstechnologischen Systemen*. Mannheim: BI-Wissenschaftsverlag.

Scheele, Ulrich (1993): *Privatisierung von Infrastruktur. Möglichkeiten und Alternativen*. Köln: Bund-Verlag.

Schäfer, Günter (2003): *Netzsicherheit. Algorithmische Grundlagen und Protokolle*. Heidelberg: dpunkt-Verlag.

Schimank, Uwe (1992): Erwartungssicherheit und Zielverfolgung. Sozialität zwischen Prisoner's Dilemma und Battle of the Sexes. In: *Soziale Welt* 43, 182 – 200.

Schimank, Uwe (2002): Organisationen: Akteurkonstellationen – Korporative Akteure – Sozialsysteme. In: Allmedinger, Jutta; Hinz, Thomas (Hrsg.): *Organisationssoziologie*. Wiesbaden: Westdeutscher Verlag, 29 – 54.

Schimank, Uwe (2003): Das Wechselspiel von Intentionalität und Transintentionalität im Institutionalismus und in der Organisationsforschung. In: Greshoff, Rainer; Kneer, Georg; Schimank, Uwe (Hrsg.): *Die Transintentionalität des Sozialen. Eine vergleichende Betrachtung klassischer und moderner Sozialtheorien.* Wiesbaden: Westdeutscher Verlag, 246 – 277.

Schmidt, Susanne K.; Werle, Raymund (1992): *Koordination und Evolution: Technische Standards im Prozeß der Entwicklung technischer Systeme.* Köln, Max-Planck-Institut für Gesellschaftsforschung, Discussion Paper.

Schmidt, Susanne K.; Werle, Raymund (1998): *Coordinating Technology. Studies in the International Standardization of Telecommunications.* Cambridge, MA: MIT Press.

Schmitter, Philippe C. (1977): Modes of Interest Intermediation and Models of Societal Change in Western Europe. In: *Comparative Political Studies* 10, 7 – 38.

Schmitter, Philippe C. (1979): Still the Century of Corporatism? In: Schmitter, Philippe C.; Lehmbruch, Gerhard (Hrsg.): *Trends Toward Corporatist Intermediation.* London: Sage, 7 – 52.

Schmitz, Walter (2004): Kritische Infrastrukturen: Bedrohungsanalyse und Handlungsbedarf. In: von Knop, Jan; Frank, Hans (Hrsg.): *Netz- und Computersicherheit. Sind wir auf einen Angriff auf unsere Informationssysteme und Informations-Infrastrukturen vorbereitet?* Bielefeld: Bertelsmann, 275 – 307. Kongressband 2003 der Bundesakademie für Sicherheitspolitik und der Heinrich-Heine-Universität Düsseldorf.

Schneider, Volker (1989): *Technikentwicklung zwischen Politik und Markt: Der Fall Bildschirmtext.* Frankfurt a. M.: Campus.

Schneider, Volker (1991): The Governance of Large Technical Systems: The Case of Telecommunications. In: La Porte, Todd R. (Hrsg.): *Responding to Large Technical Systems: Control or Anticipation.* Dordrecht: Kluwer, 19 – 42.

Schneider, Volker (1993): Networks and Games in Large Technical Systems. In: Scharpf, Fritz W. (Hrsg.): *Games in Hierarchies and Networks.* Frankfurt a. M.: Campus, 251 – 286.

Schneider, Volker (1999): *Staat und Technische Kommunikation. Die politische Entwicklung der Telekommunikation in den USA, Japan, Grossbritannien, Deutschland, Frankreich und Italien.* Opladen: Westdeutscher Verlag.

Schneider, Volker (2000a): Evolution in Cyberspace: The Adaption of National Videotext Systems to the Internet. In: *Information Society* 16 (4), 319 – 328.

Schneider, Volker (2000b): Global Economic Governance by Private Actors: The International Chamber of Commerce. In: Greenwood, Justin; Jaycek, Henry (Hrsg.): *Organized Business and the New Global Order.* London: Mac Millan, 223 – 240.

Schneider, Volker (2000c): Organisationsstaat und Verhandlungsdemokratie. In: Werle, Raymund; Schimank, Uwe (Hrsg.): *Gesellschaftliche Komplexität und kollektive Handlungsfähigkeit.* Frankfurt a. M.: Campus, 243 – 269.

Schneider, Volker (2002): Private Actors in Political Governance: Regulating the Information and Communication Sectors. In: Grote, Jürgen R.; Gbikpi, Bernard (Hrsg.): *Participatory Governance. Political and Societal Implications.* Opladen: Leske + Budrich, 245 – 264.

Schneider, Volker (2003): Akteurkonstellationen und Netzwerke in der Politikentwicklung. In: Schubert, Klaus; Bandelow, Nils (Hrsg.): *Lehrbuch der Politikfeldanalyse.* München: Oldenbourg, 107 – 145.

Schneider, Volker (2004a): Großfirmen in Politiknetzwerken: Zum Bedeutungsgewinn des „Corporate Lobbying" im Kontext von Europäisierung und Internationalisierung. In: Henning, Christian H. C. A.; Mehlbeck, Christian (Hrsg.): *Interdisziplinäre Sozialforschung. Theorie und empirische Anwendungen.* Frankfurt a. M.: Campus, 225 – 244.

Schneider, Volker (2004b): Organizational Governance – Governance in Organisationen. In: Benz, Arthur (Hrsg.): *Governance – Regieren in komplexen Regelsystemen.* Wiesbaden: VS Verlag, 173 – 192.

Schneider, Volker (2004c): State Theory, Governance and the Logic of Regulation and Administrative Control. In: Warntjen, Andreas; Wonka, Arndt (Hrsg.): *Governance in Europe.* Baden-Baden: Nomos, 25 – 41.

Schneider, Volker (2004d): The Transformation of the State in the Digital Age. In: Puntscher Riekmann, Sonja; Mokre, Monika; Latzer, Michael (Hrsg.): *The State of Europe. Transformations of Statehood from a European Perspective.* Frankfurt a. M.: Campus, 51 – 72.

Schneider, Volker (2005): *Policy-Networks in a Systemic Perspective. A New Look at an Old Data Set.* Konstanz, Universität Konstanz, unveröffentlichtes Papier zur 5. POLNET Summer School on the Analysis of Political and Managerial Networks an der Universität Tilburg, 18 – 23 September 2005.

Schneider, Volker (2006): Über die Natur der Sozialwissenschaften. Die Perspektive des Wissenschaftsphilosophen Mario Bunge. In: Soeffner, Hans-Georg; Herbrik, Regine (Hrsg.): *Soziologische Revue, Sonderheft 6, „Wissenssoziologie"* Bd. 28. München: Oldenbourg, 111 – 121.

Schneider, Volker; Dang-Nguyen, Godefroy; Werle, Raymund (1994): Corporate Actor Networks in European Policy Making: Harmonizing Telecommunications Policy. In: *Journal of Common Market Studies* 32, 473 – 498.

Schneider, Volker; Hyner, Dirk (2006): Security in Cyberspace: Governance by Transnational Policy Networks. In: Koenig-Archibugi, Mathias; Zürn, Michael (Hrsg.): *New Modes*

of Governance in the Global System. Exploring Publicness, Delegation and Inclusiveness. Basingstoke: Palgrave Macmillan, 154 – 176.

Schneider, Volker; Janning, Frank (2006): *Politikfeldanalyse. Akteure, Diskurse und Netzwerke in der öffentlichen Politik.* Wiesbaden: VS Verlag.

Schneider, Volker; Kenis, Patrick (1996): Verteilte Kontrolle: Institutionelle Steuerung in modernen Gesellschaften. In: Kenis, Patrick; Schneider, Volker (Hrsg.): *Organisation und Netzwerk. Institutionelle Steuerung in Wirtschaft und Politik.* Frankfurt a. M.: Campus, 9 – 43.

Schneider, Volker; Mayntz, Renate (1995): Akteurzentrierter Institutionalismus in der Technikforschung. Fragestellungen und Erklärungsansätze. In: Kubicek, Herbert; Müller, Günter; Klumpp, Dieter; Neumann, Karl-Heinz; Raubold, Eckart; Rossnagel, Alexander (Hrsg.): *Jahrbuch Technik und Gesellschaft*, 107 – 130.

Schneider, Volker; Ronit, Karsten (1999): Die Quadratur des Kreises? Der Beitrag transnationaler Unternehmerorganisationen zur Produktion globaler öffentlicher Güter. In: Honegger, Claudia; Hradil, Stefan; Traxler, Franz (Hrsg.): *Grenzenlose Gesellschaft? Verhandlungen des 29. Kongresses der Deutschen Gesellschaft für Soziologie, des 16. Kongresses der Österreichischen Gesellschaft für Soziologie, des 11. Kongresses der Schweizerischen Gesellschaft für Soziologie in Freiburg i. Br. 1998.* Opladen: Leske + Budrich, 258 – 373.

Schneider, Volker; Tenbücken, Marc (Hrsg.) (2004): *Der Staat auf dem Rückzug. Die Privatisierung öffentlicher Infrastrukturen.* Frankfurt a. M.: Campus.

Schuler, Douglas; Day, Peter (Hrsg.) (2004): *Shaping the Network Society. The New Role of Civil Society in Cyberspace.* Cambridge, MA: MIT Press.

Schulz, Wolfgang; Held, Thorsten (2002): *Regulierte Selbstregulierung als Form modernen Regierens.* Hamburg, Hans-Bredow-Institut, Arbeitspapier.

Schulze, Tillmann (2006): *Bedingt abwehrbereit. Schutz kritischer Informations-Infrastrukturen in Deutschland und den USA.* Wiesbaden: VS Verlag.

Schulzki-Haddouti, Christiane (2000): E-Commerce: Prüfstein für die transatlantischen Beziehungen. In: *Internationale Politik* (3), 19 – 24.

Schumpeter, Joseph A. (1942): *Capitalism, Socialism and Democracy.* New York, NY: Harper & Brothers.

Schwartau, Winn (2000): *CyberShock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Disruption.* New York, NY: Thunder's Mouth Press.

Schwegler, Helmut (1992): Systemtheorie als Weg zur Vereinheitlichung der Wissenschaften? In: Krohn, Wolfgang; Küppers, Günter (Hrsg.): *Emergenz: Die Entstehung von Ordnung, Organisation und Bedeutung.* Frankfurt a. M.: Suhrkamp, 27 – 56.

Schwenk, Jörg (2002): *Sicherheit und Kryptograhie im Internet. Von sicherer E-Mail bis zu IP-Verschlüsselung.* Braunschweig: Vieweg.

Semar, Wolfgang (2001): *Eine empirische Studie über die Auswirkungen elektronischer Märkte für eine Region: am Beispiel der Stadt Pfullendorf.* Konstanz, Universität Konstanz, Dissertation.

Shackelford, Scott J. (2014): Beyond the New 'Digital Divide': Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity. In: *Stanford Journal of International Law* 50 (1), 119 – 184.

Shannon, Claude E. (1948): A Mathematical Theory of Communication. In: *Bell Systems Technical Journal* 27, 379 – 423, 623 – 656.

Shannon, Claude E.; Weaver, Warren (1949): *The Mathematical Theory of Communication.* Urbana, IL: University of Illinois Press.

Sieber, Ulrich (1996): Mißbrauch der Informationstechnik und Informationsstrafrecht. Entwicklungstendenzen in der internationalen Informations- und Risikogesellschaft. In: Tauss, Jörg; Kollbeck, Johannes; Mönikes, Jan (Hrsg.): *Deutschlands Weg in die Informationsgesellschaft. Herausforderungen und Perspektiven für Wirtschaft, Wissenschaft, Recht und Politik.* Baden-Baden: Nomos, 608 – 651.

Sieber, Ulrich (1998): *Legal Aspects of Computer-Related Crime in the Information Society. The COMCRIME Study for the European Commission.* <`http://www.jura.uni-muenchen.de/sieber/article/comcrime/comcrime_www.pdf`>. Online-Ressource, Abruf: 03.03.2006.

Sieber, Ulrich (1999): *Verantwortlichkeit im Internet. Technische Kontrollmöglichkeiten und multimediarechtliche Regelungen.* München: Beck.

Sieber, Ulrich (2008): Mastering Complexity in the Global Cyberspace: The Harmonization of Computer-Related Criminal Law. In: Delmas-Marty, Mireille; Pieth, Mark; Sieber, Ulrich (Hrsg.): *Les chemins de l'Harmonisation Pénale. Collection de L'UMR de Droit Comparé de Paris, Bd. 15.* Paris: Société de législation comparée, 127 – 202.

Sieber, Ulrich; Nolde, Malaika (2008): *Sperrverfügungen im Internet. Nationale Rechtsdurchsetzung im globalen Cyberspace?* Berlin: Duncker & Humblot.

Simon, Herbert A. (1996): Organisationen und Märkte. In: Kenis, Patrick; Schneider, Volker (Hrsg.): *Organisation und Netzwerk. Institutionelle Steuerung in Wirtschaft und Politik.* Frankfurt a. M.: Campus, 47 – 74.

Simonis, Ernst (Hrsg.) (1977): *Infrastruktur. Theorie und Politik.* Köln: Kiepenheuer & Witsch.

Singh, Simon (2000): *The Code Book. The Science of Secrecy from Ancient Egypt to Quantum Cryptography.* New York, NY: Anchor Books.

Slaughter, Anne-Marie (2004): *A New World Order*. Princeton, NJ: Princeton University Press.

Smith, Adam (1991): *The Wealth of Nations*. New York, NY: Knopf.

Smith, D. (2004): Cybercriminal impacts on online business and consumer confidence. In: *Online Information Review* 28 (3), 224 – 234.

Sofaer, Abraham D. (2001): Toward an International Convention on Cyber Security. In: Sofaer, Abraham D.; Goodman, Seymour E. (Hrsg.): *The Transnational Dimension of Cyber Crime and Terrorism*. Stanford, CA: Hoover Institution Press, 221 – 248.

Sofaer, Abraham D.; Goodman, Seymour E. (2001a): Cyber Crime and Security: The Transnational Dimension. In: Sofaer, Abraham D.; Goodman, Seymour E. (Hrsg.): *The Transnational Dimension of Cyber Crime and Terrorism*. Stanford, CA: Hoover Institution Press, 1 – 34.

Sofaer, Abraham D.; Goodman, Seymour E. (Hrsg.) (2001b): *The Transnational Dimension of Cyber Crime and Terrorism*. Stanford, CA: Hoover Institution Press.

Sokal, Robert R.; Sneath, Peter H. A. (1963): *Principles of Numerical Taxonomy*. New York, NY: Freeman.

Spafford, Eugene H. (1991): *The Internet worm incident. Technical Report CSD-TR-933*. < `http://homes.cerias.purdue.edu/~spaf/tech-reps/933.pdf` >. Online-Ressource, Abruf: 24.01.2006. Purdue University.

Spinello, Richard A. (2002): *CyberEthics: Morality and Law in Cyberspace*. Sudbury, MA: Jones and Bartlett.

Sprinkel, Shannon C. (2002): Global Internet Regulation: The Residual Effects of the 'ILoveYou' Computer Virus and the Draft Convention on Cyber-Crime. In: *Suffolk Transnational Law Review* 25 (3), 491 – 514.

Stehr, Nico (1994): *Arbeit, Eigentum und Wissen. Zur Theorie von Wissensgesellschaften*. Frankfurt a. M.: Suhrkamp.

Stehr, Nico (2000): *Die Zerbrechlichkeit moderner Gesellschaften*. Weilerswist: Velbrück Wissenschaft.

Stehr, Nico (2001a): Moderne Wissensgesellschaften. In: *Aus Politik und Zeitgeschichte* 36, 7 – 14.

Stehr, Nico (2001b): *Wissen und Wirtschaften. Die gesellschaftlichen Grundlagen der modernen Ökonomie*. Frankfurt a. M.: Suhrkamp.

Stelzer, Dirk (2000): Digitale Güter und ihre Bedeutung in der Internet-Ökonomie. In: *WISU – Das Wirtschaftsstudium* (6), 835 – 842.

Stigler, George J. (1961): The economics of information. In: *Journal of Political Economy* (3), 213 – 225.

Streeck, Wolfgang (1983): Interessenverbände als Hindernisse und Vollzugsträger öffentlicher Politik. In: Scharpf, Fritz W.; Brockmann, Marlene (Hrsg.): *Institutionelle Bedingungen der Arbeitsmarkt- und Beschäftigungspolitik*. Frankfurt a. M.: Campus, 181 – 198.

Streeck, Wolfgang (Hrsg.) (2006): *Governing Interests. Business associations facing internationalization*. London: Routledge.

Streeck, Wolfgang; Schmitter, Philippe C. (Hrsg.) (1985): *Private Interest Government. Beyond Market and State*. London: Sage.

Streeck, Wolfgang; Schmitter, Philippe C. (1996): Gemeinschaft, Markt und Staat – und die Verbände? Der mögliche Beitrag von Interessenregierungen zur sozialen Ordnung. In: Kenis, Patrick; Schneider, Volker (Hrsg.): *Organisation und Netzwerk* Bd. 25. Frankfurt a. M.: Campus, 123 – 164.

Sydow, Jörg (1996): Virtuelle Unternehmung: Erfolg als Vertrauensorganisation? In: *Office Management* 44 (7/8), 10 – 13.

Teuteberg, Hans-Jürgen; Neutsch, Cornelius (Hrsg.) (1998): *Vom Flügeltelegraphen zum Internet. Geschichte der modernen Telekommunikation*. Stuttgart: Steiner.

Thatcher, Mark (1998): The Development of Policy Network Analyses: From Modest Origins to Overarching Frameworks. In: *Journal of Theoretical Politics* 10 (4), 389 – 416.

Thomas, Douglas; Loader, Brian D. (2000): Introduction. In: Thomas, Douglas; Loader, Brian D. (Hrsg.): *Cybercrime: Law enforcement, security and surveillance in the information age*. London: Routledge, 1 – 13.

Thurner, Paul W.; Stoiber, Michael; Weinmann, Cornelia (2005): Informelle transgouvernementale Koordinationsnetzwerke der Ministerialbürokratie der EU-Mitgliedstaaten bei einer Regierungskonferenz. In: *Politische Vierteljahresschrift* 46 (4), 552 – 574.

Toffler, Alvin (1980): *The Third Wave*. New York, NY: Bantam Books.

Turing, Alan M. (1937): On computable numbers, with an application to the Entscheidungsproblem. In: *Proceedings of the London Mathematical Society* 42, 230 – 254.

Turkle, Sherry (1997): *Life on the screen: Identity in the Age of the Internet*. London: Phoenix.

Ulrich, Otto (2002): IT-Sicherheit als didaktische Aufgabe. In: Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *Mit IT-Sicherheit gegen Internet-Kriminalität?!* Ingelheim: SecuMedia, 71 – 81.

UNCTAD (2006): *United Nations Conference on Trade and Development. Information Economy Report 2006. The Development Perspective*. New York, NY: United Nations.

US Department of Homeland Security (2003): *The National Strategy to Secure Cyberspace.* <http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf>. Online-Ressource, Abruf: 08.03.2008.

van Creveld, Martin (2004): The Fate of the State. In: Puntscher Riekmann, Sonja; Mokre, Monika; Latzer, Michael (Hrsg.): *The State of Europe. Transformations of Statehood from a European Perspective.* Frankfurt a. M.: Campus, 33 – 50.

van Laak, Dirk (1999): Der Begriff „Infrastruktur" und was er vor seiner Erfindung besagte. In: Scholtz, Gunter (Hrsg.): *Archiv für Begriffsgeschichte* Bd. 41. Bonn: Bouvier, 280 – 299.

Venables, William N.; Ripley, Brian D. (2002): *Modern Applied Statistics with S-PLUS.* New York, NY: Springer.

Verba, Sidney (1967): Some Dilemmas in Comparative Research. In: *World Politics* 20 (1), 111 – 127.

Vielhauer, Claus; Steinmetz, Ralf (2001): Sicherheitsaspekte biometrischer Verfahren: Klassifizierung von sicherheitsrelevanten Vorfällen und wesentlicher Größen zur Beurteilung der Funktionssicherheit. In: Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *2001 – Odyssee im Cyberspace? Sicherheit im Intenet!* Ingelheim: SecuMedia Verlag, 127 – 140.

Voiskounsky, Alexander E.; Babaeva, Julia D.; Smyslova, Olga V. (2000): Attitudes towards computer hacking in Russia. In: Thomas, Douglas; Loader, Brian D. (Hrsg.): *Cybercrime: Law enforcement, security and surveillance in the information age.* London: Routledge, 56 – 84.

von Bertalanffy, Ludwig (1956): General Systems Theory. In: *General Systems* 1, 1 – 10.

von Bertalanffy, Ludwig (1968): *General Systems Theory. Foundations, Developments, Applications.* New York, NY: Braziller.

von Bertalanffy, Ludwig (1972): Äquifinalität (Lexikonbeitrag). In: Ritter, Joachim (Hrsg.): *Historisches Wörterbuch der Philosophie. Band I.* Basel: Schwabe, 478.

von Humboldt, Wilhelm (1851): *Ideen zu einem Versuch, die Gränzen der Wirksamkeit des Staats zu bestimmen.* Breslau: Eduard Trewendt.

Walden, Ian (2005): Crime and Security in Cyberspace. In: *Cambridge Review of International Affairs* 18 (1), 51 – 68.

Wall, David S. (2007): *Cybercrime. The Transformation of Crime in the Information Age.* Cambridge, MA: Polity Press.

Ward, Joe H. (1963): Hierarchical grouping to optimize an objective function. In: *Journal of the American Statistical Association* 58, 236 – 244.

WATTS, Duncan J. (1999): *Small Worlds. The Dynamics of Networks between Order and Randomness.* Princeton, NJ: Princeton University Press.

WEBER, Max (1980): *Wirtschaft und Gesellschaft.* Tübingen: Mohr.

WEBSTER, Frank (2002): *Theories of the Information Society. Second Edition.* London: Routledge.

WEIMANN, Joachim (2004): *Wirtschaftspolitik. Allokation und kollektive Entscheidung.* 3. Berlin: Springer.

WEINGART, Peter (1989): „Großtechnische Systeme" – ein Paradigma der Verknüpfung von Technikentwicklung und sozialem Wandel. In: WEINGART, Peter (Hrsg.): *Technik als sozialer Prozeß.* Frankfurt a. M.: Suhrkamp, 174 – 196.

WELLMAN, Barry; SALAFF, Janet; DIMITROVA, Dimitrina; GARTON, Laura; GULIA, Milena; HAYTHORNTHWAITE, Caroline (1996): Computer Networks as Social Networks: Collaborative Work, Telework, and Virtual Community. In: *Annual Review of Sociology* 22, 213 – 238.

WENNERSTRÖM, Erik (2004): EU-legislation and Cybercrime: A Decade of European Legal Developments. In: *Scandinavian Studies in Law* 47, 451 – 470.

WERLE, Raymund (1999): Zwischen Selbstorganisation und Steuerung. Geschichte und aktuelle Probleme des Internet. In: WILKE, Jürgen (Hrsg.): *Massenmedien und Zeitgeschichte.* Konstanz: Universitätsverlag Konstanz, 499 – 517.

WERSIG, Gernot (2000): *Informations- und Kommunikationstechnologien. Eine Einführung in Geschichte, Grundlagen und Zusammenhänge.* Konstanz: Universitätsverlag Konstanz.

WHINE, Michael (2000): Far right extremists on the Internet. In: THOMAS, Douglas; LOADER, Brian D. (Hrsg.): *Cybercrime: Law enforcement, security and surveillance in the information age.* London: Routledge, 234 – 250.

WIEDEMANN, Peter (2000): Tatwerkzeug Internet: Ein Überblick über das System und seine kriminelle Nutzung. In: *Kriminalistik* (4), 229 – 239.

WIENER, Norbert (1962): *Cybernetics: Or control and communication in the animal and the machine.* Cambridge, MA: MIT Press.

WIENER, Norbert (1966): *Mensch und Menschmaschine. Kybernetik und Gesellschaft.* Frankfurt a.M.: Athenäum.

WIESENTHAL, Helmut (2000): Markt, Organisation und Gemeinschaft als „zweitbeste" Verfahren sozialer Koordination. In: WERLE, Raymund; SCHIMANK, Uwe (Hrsg.): *Gesellschaftliche Komplexität und kollektive Handlungsfähigkeit.* Frankfurt a. M.: Campus, 44 – 73.

WILDE, Erik (1999): *World Wide Web: Technische Grundlagen.* Berlin: Springer.

WILLIAMS, Michael R. (1997): *A History of Computing Technology.* New York, NY: John Wiley & Sons.

WILLIAMSON, Oliver E. (1985): *The Economic Institutions of Capitalism.* New York, NY: Free Press.

WILLIAMSON, Oliver E. (1996): *The Mechanisms of Governance.* Oxford: Oxford University Press.

WILLKE, Helmut (2000): *Systemtheorie I: Grundlagen.* Stuttgart: Lucius & Lucius.

WILLKE, Helmut (2001): *Systemisches Wissensmanagement.* Stuttgart: Lucius & Lucius.

WINDELBAND, Wilhelm (1919): *Präludien. Aufsätze und Reden zur Philosophie und ihrer Geschichte.* Tübingen: Mohr.

WINKEL, Olaf (2000): Sicherheit in der digitalen Informationsgesellschaft: IT-Sicherheit als politisches, ökonomisches und gesellschaftliches Problem. In: *Aus Politik und Zeitgeschichte* (41/42), 19 – 30.

WISHART, David (1969): An algorithm for hierarchical classification. In: *Biometrics* (25), 165 – 170.

WITTE, Martin J.; REINICKE, Wolfgang H.; BENNER, Thorsten (2000): Beyond Multilateralism: Global Public Policy Networks. In: *Politik und Gesellschaft* (2), 176 – 188.

WITTFOGEL, Karl A. (1962): *Die orientalische Despotie: Eine vergleichende Untersuchung totaler Macht.* Köln: Kiepenheuer & Witsch.

WOLFF, Brigitta; NEUBURGER, Rahild (1995): Zur theoretischen Begründung von Netzwerken aus Sicht der Neuen Institutionenökonomik. In: JANSEN, Dorothea; SCHUBERT, Klaus (Hrsg.): *Netzwerke und Politikproduktion. Konzepte, Methoden, Perspektiven.* Marburg: Schüren, 74 – 94.

YAR, Majid (2006): *Cybercrime and Society.* London: Sage.

YIN, Robert K. (2003): *Case Study Research. Design and Methods.* Thousand Oaks, CA: Sage.

ZÜRN, Michael (1992): *Interessen und Institutionen in der internationalen Politik. Grundlegung und Anwendungen des situationsstrukturellen Ansatzes.* Opladen: Leske + Budrich.

ZÜRN, Michael (1998): *Regieren jenseits des Nationalstaates.* Frankfurt a. M.: Suhrkamp.

ZÜRN, Michael (2001): Regieren im Zeitalter der Denationalisierung. In: OBERREUTER, Heinrich; PIAZOLO, Michael (Hrsg.): *Global Denken. Die Rolle des Staates in der internationalen Politik zwischen Kontinuität und Wandel.* München: Olzog, 216 – 232.

ZÜRN, Michael; WALTER, Gregor; DREHER, Sabine; BEISHEIM, Marianne (2000): *Postnationale Politik? Über den politischen Umgang mit den Denationalisierungsherausforderungen Internet, Klima und Migration*, Universität Bremen, InIIS-Arbeitspapier Nr. 18.