Technische Universität Ilmenau
Institut für Volkswirtschaftslehre

Diskussionspapier Nr. 16

Wirtschaftspolitik für offene Kommunikationssysteme - Eine ökonomische Analyse am Beispiel des Internet

Torsten Steinrücken

März 1999

Institut für Volkswirtschaftslehre

Helmholtzplatz
Oeconomicum

D-98 684 Ilmenau

Telefon 03677/69-4032/-4034
Fax 03677/69-4203

ISSN 0949-3859

Inhaltsübersicht

Abkürzungsverzeichnis

Abb.	Abbildung
ARPANET	Advanced Research Projects Agency Network
ATM	Asynchoner Transfer Modus
Bd.	Band
bzw.	beziehungsweise
d.h.	das heißt
DNS	Domain Name System
E-Mail	Electronic Mail
et al.	et alia (und andere)
f.	und folgende Seite
ff.	und folgende Seiten
FTP	File Transfer Protocol
Hrsg.	Herausgeber
HTTP	Hypertext Transfer Protokoll
IP	Internet Protokoll
Jan.	Januar
Jg.	Jahrgang
Kbps	Kilobit pro Sekunde
Mbps	Megabit pro Sekunde
NSFNET	National Science Foundation Network
OECD	Organization for Economic Cooperation and Development
PEM	Privacy Enhanced Mail
PGP	Pretty Good Privacy
S.	Seite
SSL	Secure Socket Layer
SMTP	Simple Mail Transfer Protokoll
TCP/IP	Transmission Control Protokoll/Internet Protokoll
u.a.	unter anderem
UDP	User Data Protokoll
vgl.	vergleiche
vol.	volume (Band)
WIK	Wissenschaftliches Institut
WWW	World Wide Web

Abbildungsverzeichnis

I. Einleitung: Charakteristika offener Kommunikationssysteme

1. Vorbemerkungen

Das Angebot an Informationen hat sich in den letzten Jahren durch das Tempo des technischen Fortschritts im Informations- und Kommunikationsbereich in Teilen der Welt sprunghaft erhöht. Die Evolution von Industriegesellschaften hin zu Informationsgesellschaften ist dabei eng mit der Entwicklung neuer Technologien verbunden. Vor allem Kommunikationssysteme und Kommunikationsnetzwerke haben diese Entwicklung beschleunigt und zur Entstehung neuer Strukturen beigetragen. Gleichwohl die Nutzung und Verbreitung verschiedener Netzwerke und Kommunikationssysteme neue Chancen und Handlungsspielräume eröffnet, so sind mit dieser Entwicklung jedoch auch neue Probleme entstanden. In diesem Zusammenhang sollen im folgenden vor allem die wirtschaftspolitischen Herausforderungen dieser Entwicklung Beachtung finden[1]. Anliegen dieses Diskussionspapiers ist es dabei insbesondere, die ökonomischen und gesellschaftspolitischen Argumente für eine staatliche Aktivität in diesem Bereich darzustellen und sie aus ökonomischer Sicht kritisch zu hinterfragen. Im ersten Teil werden die ökonomischen Eigenschaften von Kommunikationsnetzwerken und -diensten sowie deren Implikationen für staatliches Handeln untersucht, daran anschließend erfolgt eine Betrachtung der Allokation von Mehrwertdiensten auf der Anwendungsebene des Internet. Die Beurteilung, wie eine effiziente staatliche Wirtschafts- und Wettbewerbspolitik in offenen Kommunikationsnetzwerken gestaltet werden sollte, setzt dabei nicht nur eine übergreifende Betrachtung der Notwendigkeiten, sondern auch der Möglichkeiten staatlicher Wirtschaftspolitik voraus.

2. Aufbau und Abgrenzung offener Kommunikationssysteme

Unter offenen Kommunikationssystemen sollen im folgenden jene Kommunikationssysteme verstanden werden, die prinzipiell für alle potentiellen Nutzer zugänglich sind und somit keinen klar abgegrenzten Teilnehmerkreis aufweisen[2]. Es sind ferner all jene Einrichtungen angesprochen, die eine zweiseitige Kommunikation zwischen den Netzteilnehmern erlauben. In der weiteren Analyse werden also keine Netze und Dienste Beachtung finden, die lediglich eine einseitige Informationsversorgung zu leisten vermögen (z.B. Hörfunk, TV)[3].

Dem Anspruch einer dialogorientierten Kommunikation werden eine Vielzahl verschiedener Systeme und Netzwerke gerecht[4], im vorliegenden Fall richtet sich die Betrachtung speziell auf das *Internet*, welches einen Verbund verschiedener dezentraler Netzwerke darstellt, die

[1] Vgl. Beck/Prinz (1997) S. 457, Für die Auswirkungen auf die Steuerpolitik siehe Soete/Kamp (1996) S. 353 ff., Soete/Weel (1998) S. 1 ff., Beck/Prinz (1997a) S. 87 ff., Horner/Owens (1996) S. 516, the Economist (31.05.97) S. 17-19.

[2] Geschlossene Netzwerke (z.B. Corporate Networks, unternehmensinterne Netzwerke) liegen also außerhalb der Betrachtung. Siehe zur Ökonomie von offenen Netzwerken Weinkopf (1993) S. 18 ff., Blind (1996a) S. 137 ff.

[3] Dieselbe Abgrenzung verwendet auch Blind (1996a) S. 142. Neuere technische Entwicklungen erlauben allerdings schon, daß der Nutzer über einen Rückkanal Einfluß auf TV- oder Hörfunkprogramme ausübt.

[4] Siehe zur Auflistung einzelner Netze und Dienste Ehlers (1994) S. 29, Blind (1996a) S. 141.

beim wechselseitigen Austausch der Daten das Konzept der Paketvermittlung nutzen. Voraussetzung für die Kommunikation zwischen verschiedenen Wirtschaftssubjekten über Kommunikationssysteme ist eine Infrastruktur, welche die Nutzung der vielfältigen Mehrwertdienstleistungen überhaupt ermöglicht. Neben der physischen Verbindung der Endgeräte (Datenstationen, Datenübertragungswege, Schalteinheiten) sind insbesondere die Regeln, die bei einem Kommunikationsvorgang die Art und Weise festlegen, wie Daten empfangen und transportiert werden, von besonderer Bedeutung[5]. Solche Regeln sind in den sogenannten *Kommunikationsprotokollen* verankert. Innerhalb eines Protokolls kann es eine Vielzahl von Schichten geben, wobei jede einzelne über bestimmte Funktionen verfügt und der jeweils nächst höheren Schicht spezielle Dienste zur Verfügung stellt. Um die Leistungen der obersten Protokollschicht in Anspruch nehmen zu können, bedarf es des Zusammenspiels aller Schichten. In der nachstehenden Grafik soll der Aufbau und die Nutzung eines solchen Kommunikationsprotokolls am Beispiel des TCP/IP Protokolls, auf dem die Internetkommunikation beruht, verdeutlicht werden.

TCP - Schichten	Protokolle/ Anwendungen	
Anwendungsschicht	Mehrwertdienste	z.B. Electronic Banking, Electronic shopping
	Erweiterte Netzdienste	z.B. World Wide Web, Gopher
	Grunddienste	FTP, DNS, SMTP,HTTP
Transportschicht	TCP, UDP	
Netzwerkschicht	Internet Protokoll	
Sicherungsschicht	Ethernet, FDDI, ATM etc.	
Bit - Übertragungsschicht	Kupfer, Glasfaser, Satellit etc.	

Abb. 1: Aufbau und Nutzung des TCP/IP Schichtenmodells[6]

Das oben vorgestellte TCP/IP Schichten-Konzept versucht, über eine vollständige Spezifikation der Schnittstellen zwischen den einzelnen Schichten, die Interoperabilität zwischen den verschiedenen Endgeräten zu sichern. Die vormals gegebene Bindung der Kommunikationstechnik an eine bestimmte Nutzungsform wird insofern bei offenen Kommunikationssystemen gegenstandslos. Die Grenze zwischen Netzen und Diensten gestaltet sich durch die Verwendung von Kommunikationsprotokollen mit Schichtenaufbau fließend. Eine Dienstleistung privater Anbieter kann im Prinzip auf jeder Netzebene definiert und bereitgestellt werden[7]. Im Hinblick auf das Internet können aufgrund dessen verschiedene Teilmärkte auf die Funktionsfähigkeit des Wettbewerbs hin untersucht werden. In der vorliegenden Arbeit soll diesbezüg-

[5] Vgl. Stahlknecht (1991) S. 129 ff., Hansen (1992) S. 645.

[6] Abbildung erstellt in Anlehnung an die Grafik bei Lux/Heinen (1997) S. 7.

[7] Vgl. Recke (1996) S. 1 ff.

lich nur der Markt für Informationsinhalte und Mehrwertdienstleistungen auf der Anwendungsebene des Internet betrachtet werden[8].

3. Ökonomische Eigenschaften offener Kommunikationssysteme

Kommunikationsnetzwerke bzw. -dienste können mit Hilfe der ökonomischen Theorie sowohl von der Kosten- als auch von der Nutzenseite her betrachtet werden[9]. Betrachtet man diese von der Kostenseite, so zeichnen sie sich durch einen hohen Fixkostenblock und geringe Grenzkosten zusätzlicher Netzanschlüsse aus[10]. Ausgehend von der Nutzenseite weisen Kommunikationsnetzwerke und -dienste zugleich Merkmale von privaten und öffentlichen Gütern auf[11]. So ist einerseits die gleichzeitige Nutzung durch mehrere Individuen möglich, die über eine geeignete technische Ausrüstung verfügen, andererseits treten aber in Kommunikationsnetzwerken und -diensten bei Überschreitung einer bestimmten Nutzerzahl Überfüllungserscheinungen auf, die die begrenzte Kapazität der Übertragungsinfrastruktur und Rivalität im Konsum signalisieren. Die technischen Eigenschaften von Kommunikationsnetzwerken und -diensten erlauben jedoch durch die Erhebung von Anschluß- oder Nutzungsgebühren[12] einen Konsumausschluß, so daß Zahlungsunwillige bei Überfüllungserscheinungen von der Nutzung ausgeschlossen werden können. Kommunikationsnetze und -dienste weisen aufgrunddessen die typischen Eigenschaften von Clubgütern auf, da Nichtrivalität im Konsum nur bis zu einer bestimmten Teilnehmerzahl gegeben ist und ein Nutzungsausschluß prinzipiell möglich ist.

4. Kompatibilität und positive Netzexternalitäten

Das Internet stellt einen internationalen Verbund zwischen verschiedenen Teilnetzen dar. Der individuelle Nutzen, den der einzelne Teilnehmer erzielen kann, entsteht neben der Informationsübertragung innerhalb des Teilnetzes wesentlich aus dem Anschluß an den Gesamtnetzverbund und der Nutzung der über diesen Verbund angebotenen Dienste[13]. Aus dieser komplementären Beziehung der Dienstleistungen resultiert die Existenz von *direkten positiven Netzeffekten*: Mit jedem zusätzlichen an das Netz angeschlossenen Rechner entstehen zum einen für alle bereits angeschlossenen Netzteilnehmer externe Effekte derart, daß der neue Netzteilnehmer zusätzliche Datenübertragungswege ermöglicht. Darüber hinaus erhöht aber jeder Neuanschluß den Wert des Netzes für die bereits angeschlossenen Teilnehmer auch dadurch, daß er neue Informationen bereitstellt und diese von den bereits im Netz befindlichen

8 Diese Abgrenzung macht deutlich, daß die wettbewerbspolitischen Probleme auf der Ebene des Netzzugangs durch die versuchte Monopolisierung seitens des Anbieters *Microsoft* und Probleme bei der *Vergabe von Domain Names* nicht berücksichtigt werden, da dies die Schicht der erweiterten Netzdienste betrifft. Vgl. zu diesen Problemkreisen Fichert (1998) S. 343 ff., Coates (1998) S. 1 ff.

9 Zur allgemeinen Charakterisierung von Netzen siehe Blankart/Knieps (1992) S. 74 ff.

10 Die hohen Fixkosten entstehen durch die Investitionen in die notwendige Übertragungs- und Vermittlungsinfrastruktur von Netzwerken.

11 Vgl. Blind (1996a) S. 143.

12 Siehe Liebowitz/Margolis (1994) S. 135 f.

13 Vgl. Rupp (1996) S. 12.

Teilnehmern genutzt werden können[14]. Hinzu kommen noch *indirekte positive Netzeffekte*, d.h. der individuelle Nutzen hängt auch noch deshalb positiv von der Gesamtzahl der Nutzer des Internet ab, weil mit ihr die Zahl der angebotenen sachlich differenzierten Systemkomponenten (z.B. der angebotenen Verschlüsselungsprogramme) steigt, wodurch für die Teilnehmer größere Wahlmöglichkeiten entstehen[15].

Beim Vorliegen von positiven Netzexternalitäten kann es sein, daß der individuelle Nutzen, einem Netz bzw. Dienst beizutreten, hinter dem gesamtwirtschaftlichen Nutzen zurückbleibt. Deshalb kann es zum Problem der *kritischen Masse*[16] von Netzteilnehmern innerhalb eines bestimmten Netzes kommen. Die Marktakzeptanz einer neuen Technologie hängt dann davon ab, wie verbreitet diese Technologie bereits ist. Wird die erforderliche Anzahl von Teilnehmern innerhalb einer bestimmten Zeit nicht überschritten, sinkt die Nutzerzahl wieder auf Null ab. Ist die kritische Masse hingegen überschritten, so übt die installierte Basis einen diffusionsfördernden Einfluß auf die weitere Entwicklung des kritischen Masse-Systems aus und es erfolgt ein Eintritt in eine Stabilitätsphase, in der die jeweilige Technologie mit hoher Wahrscheinlichkeit einen langfristigen Markterfolg erreichen wird[17]. Mit der kritischen Masse ist dann ein Diffusionsniveau erreicht, bei dem die subjektiven Wahrnehmungen der Mitglieder einer bestimmen Nachfragergruppe so gestaltet sind, daß die Technologie in ausreichendem Maße Nachfragesynergien selbst entfalten kann und in einer endlichen Zeitperiode ein Marktgleichgewicht erreicht wird[18]. Darüber hinaus kann beim Vorliegen von positiven Netzexternalitäten auch das Problem der *Netzzersplitterung* auftreten, falls bei mehreren gleichartigen Netzen die kritische Masse erreicht wird, aber wegen unterschiedlicher, inkompatibler Technologien die Vorteile der Netzexternalitäten nicht voll ausgeschöpft werden können[19].

5. Überfüllung und negative Netzexternalitäten

Das zunehmende Wachstum der Anzahl der Internetteilnehmer, verbunden mit dem explosionsartigen Anstieg der Netznutzung und der verstärkten Verwendung bandbreitenintensiver Dienste, wie dem World Wide Web oder der Internettelefonie, führt auch zu negativen externen Effekten: Netzüberlastung und daraus resultierende spürbare Verzögerungen[20] für alle Teilnehmer sind die offensichtlichsten. Das Internet in seiner derzeitigen Struktur hat die Ei-

14 Dies ist auf die Eigenschaft des Internet als Mehrwertdienstnetz zurückzuführen, in welchem jeder Netzteilnehmer die von anderen Nutzern bereitgestellten Informationen problemlos abrufen kann.

15 Dieser Zusammenhang kommt dadurch zustande, daß bei hohen Fixkosten der Produktion einer neuen Komponentenart (z.B. Software) die profitabel anbietbare Zahl der Arten mit der Anzahl der Nachfrager steigt. Vgl. Wöckner (1996) S. 260.

16 Vgl. Rohlfs (1974) S. 29 und Knorr (1993) S. 103

17 Vgl. Weiber (1992) S. 71 f., Witt (1997) S. 653 ff.

18 Siehe Rupp (1996) S. 14, Weiber S. 71.

19 Vgl. Blankart/Knieps (1992) S. 79.

20 Diese Verzögerungen entstehen bei Überfüllung zum einen dadurch, daß Pakete verlorengehen und wieder neu angefordert werden müssen und andererseits durch überlastete Router, welche die Weiterleitung verzögern.

genschaften eines klassischen Allmendegutes hinsichtlich der Nutzung der knappen Ressource „Bandbreite“. Es besteht Rivalität bezüglich der schnellen Übertragung von Datenpaketen, aber kein gänzlicher Ausschuß von der Übertragung. Mit dem Gutscharakter verbinden sich auch die „typischen“ Allokationsprobleme, die bei Allmendegütern auftreten. Durch den unregulierten Zugang zur Ressource „Übertragungskapazität“ werden traditionelle elastische[21] Anwendungen (z.B. E-Mail) verlangsamt und der Einsatz neuerer zeitkritischer Anwendungen (wie z.B. digitales Fernsehen in der Form von pay per view) teilweise verhindert[22].

Ziel einer Lösung für das Allokationsproblem sollte es daher sein, die auftretenden negativen externen Effekte weitestmöglichst zu internalisieren; d.h. die externen Kosten, die ein Teilnehmer durch Nutzung der Ressource allen anderen Nutzern aufbürdet, sollen dem Teilnehmer direkt zugerechnet werden[23]. Dies kann durch ein Preissystem, welches nicht nur den Netzzugang mit einem Preis belegt, sondern darüber hinaus auch den Nutzungsgrad bei Überfüllung tarifiert erreicht werden[24]. Die Einführung eines nutzungsabhängigen Preissystems setzt dabei individuelle pekuniäre Anreize für die Wirtschaftssubjekte, die dann die Möglichkeit haben, den Transport von Daten ihrer Zahlungsbereitschaft anzupassen. Ein nutzungsabhängiges Preissystem wird darüber hinaus auch neue Impulse für die stärkere Nutzung moderner Übertragungsformen generieren (z.B. Datenkomprimierung vor der Übertragung) und dadurch zu einer effizienten Nutzung der vorhandenen Bandbreite führen. Eine Sensibilisierung der Nutzer bezüglich der gesamten Kosten ihres Datentransports wird, aller Voraussicht nach, auch für die Entwicklung neuer Nutzungsformen des Internet von großer Bedeutung sein.

II. Tendenzen staatlicher Einflußnahme in offene Kommunikationssysteme

1. Grundlegende Gedanken zu staatlicher Wirtschaftspolitik

In einem marktwirtschaftlich orientierten Wirtschafts- und Gesellschaftssystem wird grundsätzlich davon ausgegangen, daß durch den Marktprozeß das beste Ergebnis automatisch realisiert wird. Es sind jedoch Bedingungen denkbar, in denen der Wettbewerb seiner Aufgabe nicht nachkommen kann. Dies kann daran liegen, daß *ökonomische Gründe* keinen funktionstüchtigen Wettbewerb zulassen, der effiziente[25] Ergebnisse erwarten läßt. So kann der Wettbewerbsprozeß fehlgeleitet werden, wenn eine Marktseite systematische Informationsvorsprünge bezüglich der Qualität von Gütern und Dienstleistungen besitzt. Hier kann die

[21] *Elastische* Anwendungen werden durch Überfüllungsprobleme nur verlangsamt. Für die Funktionsweise *unelastischer* Anwendungen ist es hingegen erforderlich, daß über die Dauer der Übertragung ein definierter Datendurchsatz garantiert ist.

[22] Vgl. Rupp (1996) S. 33.

[23] Vgl. Rupp (1996) S. 33.

[24] Zu Vorschlägen für ein nutzungsabhängiges Preissystem siehe Clark (1997) S. 215 ff., MacKie-Mason/ Murphy/Murphy (1997) S. 279 ff., Rupp (1996) S. 33 ff. und Grupta et al. (1997) S. 323 ff. Zu Problemen vgl. Sakar (1997) S. 497.

[25] Vgl. zur ökonomischen Effizienz Kallfass (1989) S. 5-18.

effizienzsichernde Funktion des Marktes nur durch die Schaffung geeigneter Regeln oder Institutionen realisiert werden. Weiterhin können durch marktwirtschaftliche Aktivitäten Fehlallokationen hervorgerufen werden, in dem Fall, wenn die privaten Anbieter nicht alle von ihren Konsum- oder Produktionsentscheidungen verursachten Kosten bzw. Nutzen in den individuellen Entscheidungen berücksichtigen. Staatliche Aktivitäten können diesbezüglich unter Umständen helfen, die Funktionsfähigkeit des Marktmechanismus in diesem Bereich zu verbessern[26].

Neben ökonomischen Argumenten können jedoch auch *gesellschaftspolitische Gründe* für staatliche Eingriffe in prinzipiell funktionierende Märkte sprechen. So ist es politisch unstrittig, daß die Sicherung individueller Persönlichkeitsrechte sowie die Durchsetzung der nationalen Rechtsordnung wesentliche Grundlagen für die Stabilität eines Gesellschaftssystems darstellen. Derartige gesellschaftspolitische Ziele können durchaus im Widerspruch zum Ziel der ökonomischen Wohlfahrtsmaximierung stehen. Aus ihrer besonderen Bedeutung für die Funktionsfähigkeit des Gesellschaftssystems ergibt sich aber, daß sie prinzipiell über dem Streben nach ökonomischer Wohlfahrtsmaximierung anzusiedeln sind[27].

2. Staatseingriffe aufgrund der ökonomischen Eigenschaften?

Die Ergebnisse des vorangegangenen Kapitels haben gezeigt, daß durch die Nutzung des Internet sowohl positive als auch negative Externalitäten auftreten. Eine Folge des Auftretens externer Effekte ist ein Abweichen des Marktergebnisses von einem gesamtwirtschaftlichen Optimum, die Marktallokation ist nicht effizient. Die privaten Anbieter berücksichtigen in diesem Fall nur einen Teil der von ihnen verursachten Kosten oder Nutzen. Die aufgezeigte Schwäche des Marktes im Fall externer Effekte kann dabei auf verschiedene Art und Weise geheilt werden. So argumentierte Pigou (1920), daß durch die Erhebung einer Steuer, in Höhe der Differenz zwischen sozialen und privaten Kosten, die Effizienz der Allokation wiederhergestellt werden kann. Eine andere Möglichkeit der Internalisierung externer Effekte hat Coase (1960) vorgestellt. Er zeigte, daß durch die Wahl eines entsprechenden Rechtssystems und die geeignete Definition von Handlungsrechten es möglich ist, die externen Effekte, bei Nichtexistenz von Transaktionskosten, in das Marktsystem zu internalisieren[28] und somit direkte Staatseingriffe unterbleiben können.

Angewand auf die *negativen externen Effekte* bei der Nutzung von Kommunikationsnetzwerken in Form von Datenstau und Wartezeiten stellt sich die Frage, ob der Markt von sich aus Lösungen findet, die zur Internalisierung der negativen externen Effekte beitragen. Generell kann eine nutzungsabhängige Preisgestaltung des Datentransports zur Internalisierung der externen Effekte führen. Die Abkehr vom derzeitig vorherrschenden Preissystem, bei dem der Nutzer an den Internetzugangsanbieter monatlich fixe Grundgebühren entrichtet, kann auf-

[26] Vgl. Fritsch/Wein/Ewers (1996) S. 211 ff. Neben asymmetrischer Informationsverteilung und externen Effekten kann auch die Vermachtung von Märkten zu ineffizienten Marktergebnissen führen.

[27] Vgl. Deutsches Institut für Wirtschaftsforschung (1996) S. 168.

[28] Siehe hierzu Coase (1960) S. 1 ff., Kohlhaas (1994) S. 358 ff. und Wegehenkel (1980) S. 9 ff.

grund der technischen Funktionsweise des internationalen Netzverbundes in einzelnen Teilnetzen oder Übertragungsstrecken des Internet vollzogen werden[29], ohne dabei das Funktionieren des gesamten Netzverbundes zu beeinträchtigen[30]. Das bedeutet, daß durch dezentrale Verhandlungen zwischen Nutzern und Internetzugangsanbierten die Anwendung eines effizienten Preissystems[31] vereinbart werden kann, welches geeignet ist, die auftretenden negativen externen Effekte zu internalisieren. Mit einer so geänderten Preisgestaltung der Nutzung können allerdings nur die externen Effekte bei Überfüllungserscheinungen des Netzwerks oder der Verbindung beseitigt werden, für die der einzelne Nutzer Gebühren zahlt. Datenstauprobleme in anderen Teilnetzen des Internet können weiterhin auftreten. Wenn also ein Nutzer Daten von einem Netzwerk oder Server abruft, wo der Datentransport noch nicht preissensibel transportiert wird, kann es selbst bei einer individuell hohen Zahlungsbereitschaft für den schnellen Datentransport noch zu Verzögerungen kommen. Die Änderung der Preissetzung in den einzelnen Subnetzen wird dann Raum greifen, wenn der Nutzenzuwachs der Teilnehmer größer ist als die Kosten für die Änderung des Preissystems. Die bei den Verhandlungen anfallenden Transaktionskosten für eine Modifikation des Tarifsystems dürften in der Regel niedrig ausfallen, da zwischen den Nutzern und den Internetzugangsanbierten derzeit schon vertragliche Beziehungen bestehen, in denen die Preise und Konditionen für den IP-Datentransport festgelegt sind. Aufgrund dessen ist eine Änderung der Tarifierung vermutlich nicht mit prohibitiv hohen Kosten verbunden. Ein staatlicher Eingriff zur Internalisierung der negativen externen Effekte ist insofern entbehrlich, da die Nutzer selbst die Möglichkeit haben, die bestehenden Allokationsineffizienzen durch private Verhandlungen zu beseitigen.

Allerdings könnte auch die Existenz von *positiven externen Effekten* nach kollektivem stattlichen Handeln verlangen[32]. So wird von einigen Autoren vorgeschlagen, durch den Einsatz von wirtschaftspolitischen Instrumenten (z.B. Ge- und Verbote, Steuern oder Subventionen) eine gesamtwirtschaftliche Wohlfahrtsverbesserung herbeizuführen und so Probleme, die aus den positiven Netzexternalitäten resultieren, zu beheben[33]. Diese Aktivitäten staatlicherseits sind durchaus umstritten[34], auf eine Anwendung beim Internet kann zudem verzichtet werden. So wurde das Startproblem bereits überwunden. Hierfür waren verschiedene Faktoren verantwortlich. So haben in der Aufbauphase des Internet die Absprachen zwischen verschiedenen amerikanischen Universitäten und Forschungseinrichtungen zur Nutzung einheitlicher (TCP/IP) Vermittlungsprotokolle zuvorderst dazu beigetragen, gleich zu Beginn, einer großen Anzahl von Nutzern den Zugang zu dem neuen Netzwerk zu ermöglichen. Die Verwendung

29 Ein solcher Preismechanismus ist bereits in Neuseeland in Nutzung. Vgl. Carter/Craeme (1995) S. 1 ff.

30 Das Internet entstand aus einem Forschungsprojekt der ARPA, welche das Ziel verfolgte, ein Computernetz zu schaffen, das auch bei teilweise zerstörten Leitungen noch nutzbar bleiben sollte.

31 In einer Spezifikation des Internet Protokoll wurde ein neu definiertes „Priority“ Feld eingefügt, welches eine Identifikation der Zustellpriorität beinhaltet und eine nutzungsabhängige Preissetzung prinzipiell ermöglicht Vgl. Rupp (1996) S. 51.

32 Siehe allgemein zur Behinderung der Funktionsweise von Marktsystemen aufgrund von Netzexternalitäten und mögliche wirtschaftspolitische Eingriffsmöglichkeiten Röver (1997) S. 33 ff.

33 Vgl. Röver (1997) S. 187 ff., Katz/Shapiro (1994) S. 112. Siehe zu Standardisierungstätigkeiten des Staates Thum (1995) S. 150 ff.

34 Siehe Liebowitz/Margolis (1994) S. 133 ff.

des TCP/IP Kommunikationsprotokolls geschah dabei schon von Anfang an im Hinblick darauf, einen Netzverbund mit anderen bereits bestehenden Netzen zu schaffen, anstatt ein neues separates Netz zu etablieren[35]. So wurde bereits mit dem Start des Internet das Problem der Netzzersplitterung durch die Verwendung eines offenen Protokolls gelöst, was die Kommunikation zwischen Rechnern und Netzen mit unterschiedlichen Hardwaresystemen und Netzwerkarchitekturen ermöglichte. Die Nutzung des neuen Netzes war also nicht an den Kauf spezieller Kommunikationshardware und Rechner gebunden, sondern es konnten bereits vorhandene, in ihrem Aufbau unterschiedliche Systeme Verwendung finden. Die Anbindung an den Internetverbund konnte so als Zusatzoption erfolgen, ohne das die gegenwärtige Nutzung der lokalen Netzwerke grundlegender Änderungen bedurfte[36]. Ein weiterer bedeutender Faktor, der den schnellen Aufbau einer Grundzahl an Nutzern ermöglichte, war die Subventionierung des NSFNET-Backbonenetzes durch die National Science Foundation[37]. Auf diese Weise wurde die Nutzung des Netzes verbilligt und für die Nachfrager ein zusätzlicher Anreiz geschaffen, sich dieser Technologie zuzuwenden. Die Überschreitung der kritischen Masse an Teilnehmern und das stürmische Wachstum des Internet soll anhand der Abb. 2 verdeutlicht werden. Es zeigt sich also, daß sich auch aus der Existenz von positiven Netzexternalitäten kein Grund für einen wirtschaftspolitischen Eingriff ableiten läßt[38].

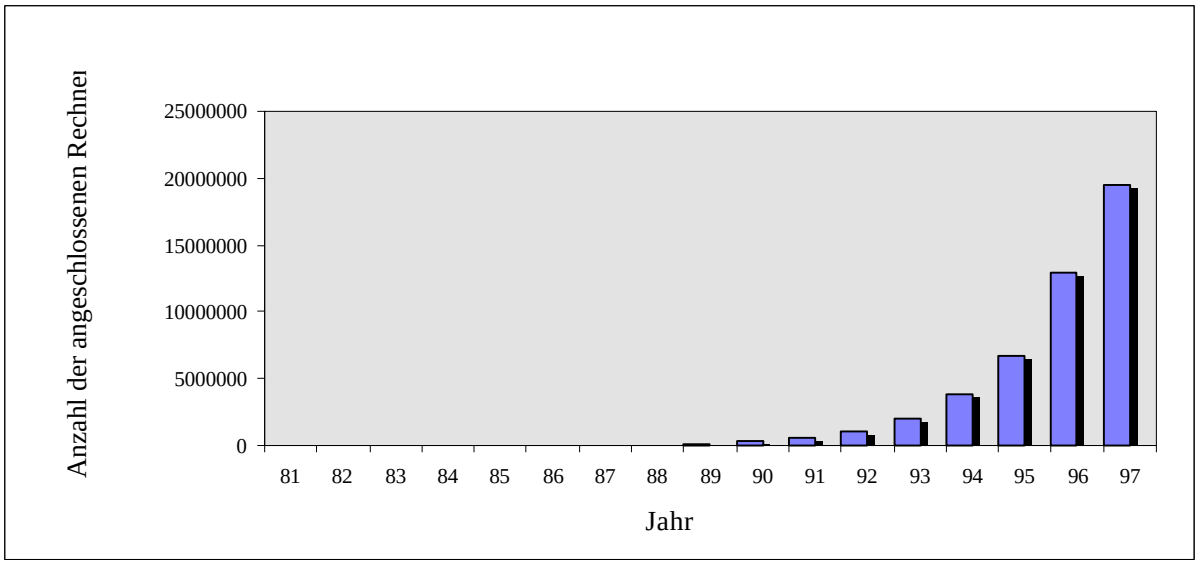

Abb. 2: Entwicklung der Anzahl am Internet angeschlossener Rechner[39]

35 Vgl. Rupp (1996) S. 15 ff.

36 Sollen zwei Netzwerke oder Rechner miteinander verbunden werden, die aufgrund ihrer Spezifikation Protokollübersetzungen in allen Schichten benötigen, so werden *Gateways* eingesetzt.

37 Vgl. Rupp (1996) S. 16.

38 Dagegen argumentiert Schickele (1996) S. 2 ff., daß eine Subventionierung des Internet (insbesondere der Netzinfrastruktur) durch den Staat für die weitere Entwicklung des Netzwerkes notwendig ist.

39 Grafik erstellt nach Daten des Merit Network Information Center. Vgl. http://nic.merit.edu/nsfnet/statistics/history.hosts.

3. Ordnungspolitik auf der Anwendungsebene des Internet

3.1 Anbieter und Nachfrager auf der Anwendungsebene des Internet

Unter Nutzung der globalen Netzinfrastruktur, der Grunddienste und der erweiterten Netzdienste (wie E-Mail und World Wide Web[40]) hat sich auf der Anwendungsebene des Internet in den letzten Jahren ein internationaler Markt für Mehrwertdienste entwickelt. Dieser wird derzeit vornehmlich durch den Handel von Dienstleistungen (z.B. Börseninformationen, Wetterbericht, Produktinformationen) und verschiedenen Waren (Texte, Bilder und Software) geprägt[41]. Das Spektrum der Angebote ist dabei vielfältig und reicht von einfachen Orientierungshilfen für die Suche im Netz bis hin zur Abwicklung von Finanzdienstleistungen („electronic banking“) oder Möglichkeiten zum elektronischen Kauf von Produkten („online shopping“)[42].

Anbieter dieser Waren oder Dienstleistungen sind einerseits kommerzielle Einrichtungen (z.B. Unternehmen, Content provider), als auch nicht-kommerzielle Anbieter wie Universitäten, Vereine oder Privatpersonen. Die offerierten Leistungen werden dabei auf Rechnern, die dem internationalen Netzverbund angeschlossen sind, bereitgestellt und können zu jeder Zeit von den *Nachfragern* abgerufen werden. Als solche treten private Nutzer, öffentliche Einrichtungen oder Unternehmen auf, die die verschiedenen im Internet angebotenen Leistungen zum Konsum oder als Vorleistung nutzen. Da es sich beim Internet um ein offenes Kommunikationssystem mit globaler Verbreitung handelt, können prinzipiell alle Wirtschaftssubjekte, die einen Zugang zum Netzwerk haben, als Anbieter oder Nachfrager auf diesem internationalen Markt auftreten. Dabei spielt es keine Rolle, an welchem Ort die verschiedenen Leistungen angeboten oder nachgefragt werden. Die Leistungen im internationalen Netzverbund sind entfernungsinsensitiv und ortsungebunden[43].

3.2 Ökonomische Gründe zur Rechtfertigung staatlicher Aktivität

Aufgrund der Vielzahl der Angebote an Mehrwertdiensten auf der Anwendungsebene des Internet kann die nachfolgende Betrachtung nur auf allgemeiner Ebene stattfinden. Aus ordnungspolitischer Sicht ist vor allem die Frage interessant, ob auf dieser Ebene die *Rahmenbedingungen* so gesetzt sind, daß Güter und Leistungen durch private Anbieter entsprechend den herrschenden Knappheiten alloziert werden können. Es zeigt sich allerdings, daß einer effizienten Allokation vor allem externe Effekte durch *Unsicherheiten bei der Netznutzung* und eine *asymmetrische Informationsverteilung* zwischen den Marktseiten bezüglich der Sicher-

40 Vgl. dazu Abb. 1 S. 2.

41 Vgl. Grimm (1997) S. 420.

42 Vgl. Beck/Prinz (1997) S. 458.

43 Vgl. Beck/Prinz (1997) S. 457 ff. Für physische Waren, die im Internet angeboten werden und deren Transport mit Kosten verbunden ist, spielt natürlich die Entfernung zwischen Anbieter und Nachfrager nach wie vor eine Rolle.

heit der angebotenen Dienstleistungen entgegenstehen und aus ökonomischer Sicht ein Abweichen vom Allokationsoptimum hervorrufen[44].

Prinzipiell kann eine *sichere Kommunikation* in offenen Netzwerken mit verschiedenen technischen und organisatorischen Mitteln hergestellt werden und äußert sich in vier Dimensionen: Verfügbarkeit, Integrität, Verbindlichkeit und Vertraulichkeit der kommunizierten Inhalte[45]. Diese allgemeinen Sicherheitsanforderungen an Datenübertragungen in Kommunikationssystemen werden auch an die im Internet abgewickelten Transaktionen von verschiedenen Benutzergruppen gestellt. Typische Internet-Übertragungen stellen derzeit jedoch ein nicht zu unterschätzendes Sicherheitsproblem dar, da eine elektronische Botschaft im Durchschnitt über 10 Rechner läuft und ohne großen Aufwand abgehört und kopiert werden kann[46]. Es existieren jedoch eine Reihe von Lösungsansätzen zur Gewährleistung oben genannter Sicherheitseigenschaften. So garantiert die Architektur des Internet als paketvermittelnde Kommunikation, daß beim Ausfall bestimmter Netzteile oder Kommunikationsverbindungen die gewünschten Informationspakete dennoch den Empfänger erreichen[47]. Ferner können verschiedene Sicherheitsmaßnahmen von den Dienstanbietern und Nutzern ergriffen werden, um ihre Kommunikation zu schützen. Hinsichtlich dieser Möglichkeiten, erscheint gegenwärtig die asymmetrische Verschlüsselung der Dateninhalte[48] als wirkungsvollste Maßnahme den Datenaustausch im Internet sicherer zu machen. Der Nutzen solcher Sicherheitsmaßnahmen liegt dabei in der Reduzierung des erwarteten Schadens, der bei einer Verletzung der Informationssicherheit auftreten kann[49]. Bestünde vollständige Transparenz über die Effizienz der Sicherheitsmaßnahmen, die Vertrauenswürdigkeit der Zertifizierungsinfrastruktur bei der Hinterlegung der öffentlichen Schlüssel und der Risiken bei der Nutzung des Internet, dann wird ein Anbieter solange das Ausmaß an Sicherheitsvorkehrungen seiner Dienstleistung erhöhen, bis die Kosten einer zusätzlich implementierten Sicherheitsvorkehrung für einen Teilnehmer mit dessen Zahlungsbereitschaft übereinstimmen.

Es zeigt sich allerdings mit Hinblick auf die technischen Gegebenheiten des Internet, daß eben jene Idealbedingungen für die Allokation von sicheren Mehrwertdiensten auf der Anwendungsebene nicht gegeben sind. Vielmehr liegt zwischen den Dienstanbietern und Nutzern ein unterschiedlicher Kenntnisstand bezüglich der implementierten Sicherungssysteme vor. Auf der Anbieterseite bestehen Anreize, die Informationsdefizite der Teilnehmer auszu-

44 Vgl. Blind (1996) S. 377 ff., Beck/Prinz (1997) S. 462 f.

45 Vgl. Kurth (1993) S. 85 ff.

46 Vgl. Rojas (1996) S. 229. Zu den einzelnen Sicherheitsmängeln im Internet siehe Wähner (1993) S. 350 f.

47 Bei Netzüberlastung kann es vorkommen, daß Pakete verlorengehen, diese werden dann selbständig vom TCP/IP Protokoll erneut angefordert.

48 Spontanen gesicherten Datenaustausch über Internet ermöglicht die *asymmetrische Kryptierung* (auch „public key“ Verfahren genannt). Jeder Kommunkationsteilnehmer besitzt dabei nur zwei Schlüssel: einen privaten und einen öffentlichen. Den privaten Schlüssel hält er geheim, der öffentliche wird wie in einem Telefonbuch für jedermann allgemein zugänglich gemacht. Die zu übermittelnde Nachricht kann mit jedem der beiden Schlüssel chiffriert werden, aber nur mit dem jeweils anderen Schlüssel wieder dechiffriert werden. Jede Veränderung der so übermittelten Nachricht führt dazu, daß sie nicht mehr zu entschlüsseln ist.

49 Vgl. Blind (1996) S. 379.

nutzen und die Aufwendungen für die Informationssicherheit ihrer Dienste zu senken[50]. Dies hat zur Folge, daß es zum Problem der *adversen Auslese*[51] kommt und sich ein volkswirtschaftlich ineffizientes Ausmaß an sicheren Diensten im Internet einstellt.

Das bloße Vorliegen von Informationsasymmetrien zwischen den Marktseiten rechtfertigt allein noch keinen staatlichen Eingriff[52], denn es existieren marktendogene Möglichkeiten, wie „Signalling[53]“ und „Screening[54]“, die dazu beitragen können, bestehende Asymmetrien zu verringern. Insbesondere vor dem Hintergrund, daß sowohl der Anbieter- als auch der Nachfragerseite durch das Informationsdefizit Wohlfahrtseinbußen entstehen, ist zu untersuchen, welche Möglichkeiten sich den Gruppen bieten, diese Informationsasymmetrien abzubauen. In der Regel haben die Benachteiligten die Möglichkeit, sich zusätzliche Informationen zu beschaffen, um ihren Informationsrückstand auszugleichen. Diese Strategie wird solange verfolgt, bis der Nutzenzuwachs weiterer Qualitätsinformationen kleiner ist als die zusätzlich einzusetzenden Suchkosten[55]. Dieser Vorgehensweise sind Grenzen gesetzt, wenn es der besser informierten Marktseite möglich ist, wichtige Informationen geheim zu halten. Oder wenn Spezialkenntnisse benötigt werden. Gerade die Beurteilung von Sicherheitsmaßnahmen im Internet konfrontiert den einzelnen Nutzer jedoch mit dem begrenzten Verständnis der komplexen Zusammenhänge und setzt seiner individuellen Informationsgewinnung Grenzen. Des weiteren muß mit der gezielten Verschleierung seitens der Anbieter gerechnet werden, Schwachstellen bezüglich der Sicherheit in ihren Dienstleistungen zu verbergen[56]. Auch wenn sich das Internet für die Informationsbeschaffung selbst bestens eignet, beispielsweise um Erfahrungswerte bezüglich der Sicherheitsvorkehrungen der einzelnen Dienste auszutauschen, so ist dennoch von solchen Suchstrategien kein genereller Abbau der Informationsasymmetrien zu erwarten.

Erfolgversprechender sind möglicherweise Garantieversprechen oder der *Aufbau von Reputation* durch die Anbieter. Solche Maßnahmen können helfen, die Qualitätsunkenntnis der Nachfrager abzubauen. Die Effizienz von Reputationsstrategien ist jedoch eingeschränkt, da die Nachfrager auch während des Nutzenzeitraums nur unzureichend die Produktqualität einschätzen können. Denn aus dem Nichteintritt eines Schadens bzw. dem Nichterkennen des Schadens kann nicht zwangsläufig auf die Güte der Sicherheitsmaßnahme geschlossen werden. Auch die Beteiligung an den Kosten bei einem Schadenseintritt wird höchstwahrscheinlich nicht von den Anbietern offeriert, da diese infolge der unvollkommenen Kenntnis des

50 Vgl. Beck/Prinz (1997) S. 463, Blind (1996) S. 380.

51 Vgl. zu asymmetrischer Informationsverteilung und Problemen der adversen Selektion Akerlof (1970) S. 236 ff., Hirshleifer/Riley (1979) S. 1375 ff.

52 Die Diagnose von Allokationsineffizienzen ist lediglich eine notwendige, keinesfalls eine hinreichende Bedingung für die Berechtigung staatlichen Handelns. Vgl. Weimann (1996) S. 102.

53 Siehe Spence (1973) S. 584 ff. zu Signallingstrategien.

54 Siehe zu Screeningstrategien Stiglitz (1975) S. 29 ff.

55 Vgl. Schulenburg (1993) S. 534.

56 Vgl. Blind (1996a) S. 210.

Bedrohungspotentials keine Garantie auf die hundertprozentige Gewährung der Informationssicherheit geben können[57].

Es zeigt sich, daß die marktendogenen Strategien nur unwesentlich zum Abbau der Informationsasymmetrien beitragen können und sich durch den Prozeß der adversen Selektion ein volkswirtschaftlich suboptimales Niveau an Sicherheit einstellen wird. Neben der asymmetrischen Informationsverteilung zwischen den Marktseiten können darüber hinaus auch Risiken bei der Kommunikation *negative externe Effekte* auslösen, die von den kommunizierenden Parteien oft nur unzureichend antizipiert werden[58]. Zur Reduzierung dieser Allokationsineffizienzen bieten sich staatlicherseits informatorische, ökonomische und ordnungsrechtliche Instrumente an, die nachfolgend vorgestellt und diskutiert werden sollen.

Es wurde ausgeführt, daß der unzureichende Informationszugang der Nachfrager zu einem ineffizienten Marktergebnis führen kann. Durch eine bessere und zuverlässigere Informationsversorgung ist es allerdings möglich, daß Entscheidungsverhalten der Marktteilnehmer zu verändern[59]. Ziel einer *staatlichen Informationspolitik* ist es in diesem Zusammenhang, die einzelnen Nachfrager in die Lage zu versetzen, sich über die angebotene Qualität der Dienste ein besseres Urteil zu bilden, und ihre Zahlungsbereitschaft dementsprechend anzupassen. Dazu können zwei Wege genutzt werden. Zum einen können die Diensteanbieter verpflichtet werden, über die Risiken bei der Kommunikation im Internet aufzuklären und die Wirksamkeit ihrer Sicherheitsmaßnahmen offenzulegen. Obwohl sich diese Lösung durch die kostengünstige Informationsgewinnung und -verbreitung durch die Anbieter auszeichnet, hat sie Nachteile. Denn den Anbieter liegen zum Teil auch nur unvollständige Informationen über die Risiken des Internet vor. Zudem sind Falschinformationen seitens der Anbieter von den Nachfragern und Kontrollbehörden nur schwer zu erkennen. Der andere Weg besteht darin, daß der Staat selbst entsprechende Informationen bereitstellt oder aber deren Bereitstellung iniziiert und damit den Nachfragern Zugang zu Informationen über mögliche Gefahren und die entsprechenden Gegenmaßnahmen ermöglicht[60]. So wäre mit Hinblick auf die Sicherheit im Internet denkbar, daß eine staatliche Institution oder andere, von den Anbietern unabhängige Dritte, anhand geeigneter Kriterien[61] die Stärke und Zuverlässigkeit der genutzten Sicherheitsmaßnahmen bewertet und die Ergebnisse den Nachfragern öffentlich zugänglich macht[62]. Diese Aufgabe können technische Überwachungsvereine oder für Deutschland das Bundes-

57 Siehe Blind (1996a) S. 211.

58 So können aufgrund von Sicherheitsmängeln Übermittlungsfehler bei der Netzkommunikation zweier Ärzte auftreten und Patienten u.U. falsch medikamentiert werden. Vgl. Beck/Prinz (1997) S. 463.

59 Vgl. Oberlack (1989) S. 72.

60 Vgl. Kuhlmann (1990) S. 116 ff., Blind (1996) S. 382, Blind (1996a) S. 224.

61 Für die USA z.B. sind solche Kriterien zur Bewertung von Sicherheitssystemen im sogenannten „Orange Book“ dargelegt und für Deutschland in den „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik“. Dabei werden 6 Bewertungsstärken von „ungeeignet“ bis „unüberwindbar“ definiert. Vgl. Kurth (1993) S. 115 ff.

62 Allerdings sind solche Produkttests nur mit bereits am Markt befindlichen Produkten durchführbar. Deshalb kann unter Umständen eine derartige Politik auch den Marktzutritt neuer Produkte erschweren. Vgl. Fritsch/ Wein/Ewers (1996) S. 229.

amt für Sicherheit und Informationstechnik wahrnehmen[63]. Vorstellbar wäre auch, daß eine staatliche Stelle alle verfügbaren Informationen über die Sicherheit bestimmter Internet-Dienste sammelt und damit die Suchkosten für interessierte Nachfrager reduziert. Es ist dabei nicht unbedingt nötig, daß alle Verbraucher die bereitgestellten Informationen nutzen. Auch wenn nur ein Teil der Nachfrager die verfügbaren Informationen in ihre Entscheidungen einbezieht, kann die durchschnittliche Qualität der Sicherheitsmaßnahmen in den angebotenen Dienstleistungen positiv beeinflußt[64] und so das Problem der adversen Auslese begrenzt werden. Es ist also möglich, durch eine staatliche Informationspolitik das Informationsdefizit der Nachfrager sowohl bezüglich der Sicherheitsvorkehrungen in den angebotenen Diensten als auch hinsichtlich der Risiken und Schadenseintrittswahrscheinlichkeiten bei der Datenübermittlung abzubauen. Indes ist eine staatliche Informationspolitik nicht geeignet, die negativen externen Effekte aus der Verletzung der Informationssicherheit zu internalisieren, da von ihr keine direkten Anreizwirkungen bzw. Sanktionen für die Wirtschaftssubjekte ausgehen[65]. Mit dieser staatlichen Maßnahme ist kein direkter Eingriff in den Marktprozeß verbunden, und die Kosten sind als relativ gering einzuschätzen. Es kann jedoch auch nicht sicher vorhergesagt werden, ob ein Abbau der Informationsasymmetrien tatsächlich stattfindet und die nationalen Internetnutzer der Sicherheit im Netz mehr Beachtung schenken und verstärkt sichere Dienste in Anspruch nehmen[66].

Neben informationspolitischen Maßnahmen können bei Sicherheitsrisiken auch andere staatliche Regelungen zum Abbau der externen Effekte und Informationsasymmetrien beitragen. Insbesondere eine spezifische Gestaltung des Haftungsrechts, die Subventionierung (Besteuerung) sicherer (unsicherer) Netzdienste und das Erlassen von gesetzlichen Mindestsicherheitsstandards können zur Erhöhung der Sicherheit im Netz führen. Bei der Anwendung dieser Instrumente auf die Mehrwertdienste im Internet treten jedoch Probleme auf, die die Wirkung dieser Instrumente unterminieren.

Die spezifische Ausgestaltung der Haftung stellt eine Möglichkeit dar, die Kosten auftretender Schäden zu internalisieren. Wichtig für die Wirkungsweise haftungsrechtlicher Regelungen ist, daß sich die Anbieter bereits vorher Erwartungen bilden, zu welchen Zahlungsverpflichtungen ihre Verhaltensweisen führen[67]. So können spezielle *Haftungsregeln* für die Anbieter[68] von Internet-Dienstleistungen Anreize darstellen, nur wirklich zuverlässige und sichere Dienste anzubieten, wodurch die Qualitätsunkenntnis der Nachfrager verringert und deren Zahlungsbereitschaft erhöht wird. Da aber nationale Haftungsregelungen nur auf im Inland

63 Vgl. Blind (1996) S. 382.

64 Vgl. Oberlack (1989) S. 73.

65 Vgl. Bind (1996) S. 382 ff. Zur Wirkungsweise von informationspolitischen Maßnahmen im Umweltbereich vgl. Wicke (1993) S. 285 f.

66 Vgl. Blind (1996) S. 382.

67 Vgl. Kohlhaas (1994) S. 366.

68 Es wäre auch denkbar, durch allgemeine Haftungsregeln für die *Nutzer* des Internet eine verstärkte Nachfrage nach sicheren Netzdiensten zu schaffen und dadurch das Ausmaß der externen Effekte zu begrenzen. Eine derartige Ausgestaltung des Haftungsrechts wird im weiteren aber nicht betrachtet, da die Anzahl der Teilnehmer zu groß und zu heterogen ist, so daß eine Überwachung sehr schwierig erscheint.

angebotene Dienstleistungen anwendbar sind, die Mehrzahl der Mehrwertdienstleistungen im Internet aber von ausländischen Anbietern offeriert werden, kann eine nationalstaatliche Regelung des Haftungsrechts nur eine *begrenzte Wirkung* auf das Sicherheitsniveau im Internet entfalten. Um Wettbewerbsverzerrungen auf dem Markt für Mehrwertdienstleistungen im Internet zwischen nationalen und internationalen Diensteanbietern durch eine unterschiedliche Ausgestaltung des Haftungsrechts zu vermeiden, müßten diesbezüglich möglichst international einheitliche rechtliche Rahmenbedingungen für bestimmte Dienstleistungen geschaffen werden. Da solche einheitlichen internationalen Rahmenbedingungen derzeit fern der Realität erscheinen und darüber hinaus die Feststellung und der Nachweis von Schäden schwierig ist[69], sollte auf den Einsatz dieses Instruments auf nationaler Ebene eher verzichtet werden.

Auch eine Besteuerungslösung ist mit verschiedenen praktischen Problemen bei der Umsetzung im Internet verbunden. So ist die Feststellung der Bemessungsgrundlage schwierig, da der Umfang der Informationsflüsse durch die derzeit noch nutzungsunabhängige Preissetzung für den Transport der Daten keinen Rückfluß auf den Ausmaß des Datentransfers eines Teilnehmers zuläßt. Zum anderen ist eine Kategorisierung der kommunizierten Inhalte nach der jeweiligen externen Schadenshöhe nicht durchführbar, weil dann jeder einzelne Kommunikationsvorgang daraufhin untersucht werden müßte, ob und inwieweit eine Verletzung der Informationssicherheit zu einer Schadenswirkung für Dritte führt. Ferner müßten die von einigen Teilnehmern bereits genutzten Verschlüsselungsverfahren in der Höhe des Steuertarifs positiv berücksichtigt werden, dessen Niveau allerdings nur willkürlich und ohne ökonomische Fundierung festgelegt werden kann[70]. Aufgrund der verschiedenen Probleme bei der Durchführung einer solchen Besteuerungslösung ist diese Regelung derzeit keine praktikable und ökonomisch effiziente Möglichkeit zur Internalisierung der externen Effekte bei Verletzungen der Informationssicherheit.

Eine *Subventionierung* von sicheren Mehrwertdiensten ist einerseits mit Belastungen des Staatshaushalts verbunden, und zum anderen sind die Ausgaben der Diensteanbieter für Sicherungssysteme und deren Implementation angesichts der Anzahl der Anbieter nicht einmal mit einem extrem hohen Verwaltungsaufwand kontrollierbar. Neben diesen praktischen Schwierigkeiten existieren auch aus ökonomischer Perspektive zahlreiche Vorbehalte gegenüber Subventionslösungen, da mit dem Einsatz dieses Instruments ein direkter Eingriff in den Preisbildungsprozeß stattfindet, welcher den Wettbewerb zwischen den Anbietern verzerrt. Ferner werden durch Subventionen Mitnahmeeffekte generiert[71], welche in diesem Fall die eigentlichen Verursacher der Externalitäten, die Anbieter und die Kommunikationsteilnehmer, begünstigen[72]. Diese Mitnahmeeffekte der informierten Nachfrager sind ökonomisch nicht zu rechtfertigen und im politischen Entscheidungsprozeß nur bedingt durchzusetzen. Darüber hinaus ist die Treffsicherheit einer Subventionslösung infolge der unzureichenden

69 Bei der Verletzung der Informationssicherheit treten häufig auch immaterielle Schäden auf, deren monetäre Bewertung schwierig ist.

70 Vgl. Blind (1996a) S. 243.

71 Vgl. Molitor (1990) S. 216.

72 Vgl. Blind (1996) S. 386.

Kenntnis der Grenznutzenverläufe gering und die mit Subventionen verbundenen Preismodifikationen können zu beträchtlichen Fehlentwicklungen führen[73]. Eine staatliche Subventionierung ist deshalb ebenso wie die Besteuerungslösung ungeeignet, zur Verbesserung der Informationssicherheit im Internet beizutragen.

Ein häufig angewandtes Instrument staatlicher Regulierungspolitik bei Sicherheitsrisiken ist das Erlassen von gesetzlichen *Mindestsicherheitsstandards*. Durch die Setzung dieser verbindlichen Sicherheitsstandards wird das Qualitätsspektrum eingeschränkt und damit die asymmetrische Informationsverteilung zuungunsten der Nachfrager abgebaut[74]. Des weiteren werden die negativen Externalitäten, die durch die Verletzung der Informationssicherheit verursacht werden, mit Hilfe von Sicherheitsstandards, die über den von den Teilnehmern gewünschten Informationssicherheitsniveau liegen, reduziert[75]. Unter Verteilungsgesichtspunkten ist die Festsetzung verbindlicher Mindestsicherheitsstandards gerechtfertigt, weil die Verursacher der Externalitäten (Anbieter und Kommunikationsteilnehmer) auch für die Internalisierungskosten herangezogen werden. Schließlich kann eine Vorgabe von Mindestsicherheitsstandards für Internet-Dienstleistungen auch dadurch gerechtfertigt werden, daß bei Schadensfällen immer auch immaterielle Nutzeneinbußen zu erwarten sind, die durch eine finanzielle Kompensation im Rahmen eines Haftungssystems nicht oder nur unzureichend entschädigt werden können. Bei einer Fehleinschätzung der gesellschaftlichen Präferenzen für die Informationssicherheit und der Festlegung zu niedriger oder zu hoher Mindeststandards können jedoch auch erhebliche Wohlfahrtsverluste ausgelöst werden[76]. So kann die Vorgabe genereller Mindeststandards dazu führen, daß Ressourcen für den Transport nichtschutzbedürftiger Informationen eingesetzt werden müssen.

Angewandt auf die Gegebenheiten des Internet können mit diesen ordnungsrechtlichen Geboten einerseits die einzelnen Nutzer des Internet unter Androhung von Sanktionen dazu gezwungen werden, nur Internet-Dienste mit bestimmten Sicherheitsvorkehrungen zu nutzen, oder die Anbieter von Diensten nur dann eine Zulassung zum Markt erhalten, wenn sie gewisse Mindestanforderungen bezüglich der Sicherheit erfüllen[77]. Beide Strategien sind jedoch mit verschiedenen Schwierigkeiten bei der Umsetzung verbunden. Die Möglichkeit, die nationalen Internetnutzer zu zwingen, nur Dienstleistungen mit einer vorgeschriebenen Mindestqualität zu nutzen, scheitert an der Notwendigkeit einer umfassenden Kontrollinfrastruktur, die wenigstens strichprobenartig die Transaktionen im Internet auf die Einhaltung der geforderten Standards hin überprüfen müßte. Eine solche Überwachung erscheint vor dem Hintergrund der dafür erforderlichen technischen und finanziellen Aufwendungen nicht praktikabel und ist

73 So ist beispielsweise in der Realität die Differenz zwischen sozialen und teilnehmerspezifischen Grenznutzen nahezu unmöglich zu bestimmen. Vgl. Blind (1996a) S. 114 f.

74 Knorr (1993) S. 44 f. spricht in einem allgemeineren Zusammenhang von Transaktionskostenersparnissen durch die Setzung von Mindeststandards. Siehe Blind (1996a) S. 254.

75 Siehe Kuhlmann (1989) S. 180.

76 Vgl. Blind (1996) S. 386. So kann die Vorgabe genereller Mindeststandards dazu führen, daß Ressourcen für den Transport nicht schutzbedürftiger Informationen eingesetzt werden.

77 Siehe zu Zulassungsbeschränkungen Fritsch/Wein/Ewers (1996) S. 225.

auch aus datenschutzrechtlichen Gründen abzulehnen[78]. Denn wenn eine Transaktion auf die Verwendung eines sicheren Verschlüsselungsmechanismus hin überprüft werden soll, so ist damit zwangsläufig die Offenlegung des Nachrichteninhalts verbunden.

Nationale Zulassungsbeschränkungen für Anbieter von unsicheren Netzdiensten auf der Anwendungsebene können aufgrund der offenen und internationalen Struktur des Internet nur die Sicherheit des nationalen Angebots beeinflussen. Werden jedoch nur inländische Diensteanbieter solchen Sicherheitsstandards unterworfen, führt dies zu einer Verteuerung ihrer Dienstleistungen und zur Verringerung der Wettbewerbsfähigkeit im internationalen Rahmen. Gerade auf dem elektronischen Markt mit seiner hohen Markttransparenz sollten deshalb Mindestvorgaben unter internationaler Abstimmung erfolgen, um Nachteile für nationale Anbieter zu verhindern. So geartete Vorgaben stellen einen ordnungspolitisch bedenklichen Eingriff in den Marktprozeß dar und sollten über das erforderliche Maß nicht hinausgehen. Deshalb sollten sich Zulassungsbeschränkungen nur auf bestimmte Dienstleistungen beschränken, bei denen durch die Verletzung der Informationssicherheit besonders starke externe Effekte auftreten. Mit einer solchen Einschränkung auf einzelne Dienstleistungen wird zugleich der Verwaltungsaufwand staatlicher Institutionen, die die jeweiligen Standards bestimmen, durchsetzen[79] und kontrollieren müssen, verringert.

Der eben dargestellte Instrumenteneinsatz zur Erhöhung der Sicherheit der angebotenen Dienstleistungen im Internet ist nur dann wirksam, wenn die verwendeten Verschlüsselungsverfahren zuverlässig funktionieren. Alle Chiffriermethoden, welche die Vertraulichkeit und Integrität mit Hilfe asymmetrischer Verfahren sicherstellen, können jedoch nur dann Informationssicherheit im Internet gewährleisten, wenn die öffentlichen Schlüssel der einzelnen Kommunikationsteilnehmer sorgfältig verwaltet werden[80]. Treten bei der Beglaubigung und Zertifizierung Unregelmäßigkeiten auf, kann dies zu erheblichen Beeinträchtigungen der Sicherheit führen und schwerwiegende negative Externalitäten auslösen. Zur Begrenzung dieser negativen Auswirkungen durch den mißbräuchlichen oder fahrlässigen Umgang mit den verwalteten Schlüsseln und zur Erhöhung der Markttransparenz der Nachfrager hinsichtlich der Zuverlässigkeit dieser Zertifizierungsstellen können wirtschaftspolitische Eingriffe gerechtfertigt werden. Da alle Nutzer identische Präferenzen bezüglich der sicheren Verwahrung ihrer Schlüssel haben, führen *Zulassungsbeschränkungen für die Betreiber von Zertifizierungsstellen* zum Ausschluß einer von allen unerwünschten Qualität[81]. Die Genehmigung zum Betrieb könnte dabei vom Nachweis einer bestimmten Mindestqualifikation abhängig gemacht werden, die beispielsweise eine Bescheinigung über die erforderliche Fachkunde, Zuverlässigkeit und Sicherheit der Anlagen verlangt[82]. Mit einer solchen Regelung können

78 Siehe zu Datenschutzaspekten Hamm (1997) S. 188.

79 Zu den verschiedenen Möglichkeiten der Durchsetzung von Standards vgl. Oberlack (1989) S. 19.

80 Siehe Grimm (1997) S. 31.

81 Siehe zu Zulassungsbeschränkungen Fritsch/Wein/Ewers (1996) S. 225.

82 Im neuen Informations- und Kommunikationsdienstegesetz, das am 13. Juni 1997 vom Bundestag beschlossen wurde und am 1. 8. 97 in Kraft trat, werden Genehmigungen zum Betrieb von Zertifizierungsstellen nur erteilt, wenn der Antragsteller gewisse Anforderungen erfüllt. Siehe § 4 SigG.

die Informationsmängel im Hinblick auf die Qualität von Zertifizierungsstellen behoben und das Vertrauen in die Leistungsfähigkeit von asymmetrischen Verschlüsselungsverfahren gestärkt werden. Als flankierende Maßnahme kann die Einführung einer Gefährdungshaftung[83]dazu beitragen, daß die Betreiber von Zertifizierungsstellen über das staatlich vorgeschriebene Niveau hinaus Vorkehrungen ergreifen, um die zuverlässige Verwahrung der Schlüssel zu verbessern. Die Kosten für eine Kontrolle und Durchsetzung dieser Mindestanforderungen sind dabei je nach Ausgestaltung des Standards eher gering, da sich voraussichtlich nur eine begrenzte Anzahl an hierarchisch organisierten[84], nationalen Zertifizierungsstellen herausbilden wird.

3.3 Gesellschaftspolitische Gründe

Die neuen Handlungsspielräume, die durch die Nutzung von modernen Kommunikationssystemen entstehen, und deren Auswirkungen auf die Gesellschaft, können auch Anlaß für eine staatliche Aktivität im angezeigten Bereich darstellen. Das Internet als diensteintegrierendes Netzwerk ermöglicht den Zugang zu und den Transport von verschiedenen Inhalten. Diese Nutzungsmöglichkeiten können zu Aktivitäten mißbraucht werden, die in den meisten Fällen durch nationales Recht allgemein verboten sind[85]. So eröffnet das Netz die Möglichkeit sowohl gesetzlich verbotene Inhalte über das Internet zu übertragen als auch Zugang zu illegalen oder jugendgefährdenden Inhalten[86] zu erlangen. Für die Untersuchung, welche staatlichen Aktivitäten geeignet erscheinen, nationalem Recht auch in offenen Kommunikationssystemen Geltung zu verschaffen, muß unterschieden werden zwischen Regelungen, die den *Zugang* zu illegalen Inhalten verhindern sollen, und jenen Maßnahmen, die den *Transport* gesetzwidriger Inhalte zu unterbinden suchen.

Um die Bereitstellung und Nutzung von *illegalen* und unerwünschten Informationen zu verhindern, wird von einigen Staaten die direkte Überwachung der über das Internet zugänglichen Inhalte erwogen und teilweise auch praktiziert[87]. So ist beispielsweise in Singapur der Zugang zum Internet nur über drei staatliche Online-Provider möglich, die indizierte Inhalte nicht an die Nutzer weiterleiten[88]. Eine solche Lösung setzt allerdings die Kenntnis und Einordnung aller unerwünschten und illegalen Informationsangebote voraus, die angesichts der Größe und Wachstum des Internet selbst mit einem extrem hohen Kostenaufwand durch eine

83 Siehe § 8 Abs. 3 und 18 des Regelungsvorschlags von provet (1996) zum Signaturgesetz. Dieser sieht für die Betreiber von Zertifizierungsstellen eine Gefährdungshaftung mit Haftungshöchstgrenze und Dekkungsvorsorge vor.

84 Eine Zertifizierung durch gegenseitiges Vorstellen im Netz (wie z.B. bei PGP) ist auch möglich, aber mit verschiedenen Unsicherheiten verbunden. Siehe Grimm (1996) S. 34.

85 Vgl. Mitteilung an das Europäische Parlament (1997) S. 6 f.

86 Siehe beispielsweise Grundgesetz für die Bundesrepublik Deutschland, Art. 5 Abs. 2 (Jugendschutz, Schutz der persönlichen Ehre).

87 An einer ähnlichen Regulierung der Inhalte im Internet sind z.B. China und Indonesien interessiert, allerdings erschwert die Größe dieser Länder eine solche Lösung.

Siehe http://www.d-comm.com/features/957.html.

88 Vgl. Newsbytes News Network vom 03. 06. 96 „Singapore to regulate user Internet access“ S. 1.

nationale Behörde allein nicht identifizierbar sind. Mag eine Überwachung der Angebote in öffentlichen Internet-Anwendungen (World Wide Web) noch teilweise möglich sein, so ist dies bei privaten Anwendungen (z.B. E-Mail) weitaus schwieriger. Aufgrund dessen kann es nicht gelingen, den Zugang zu entsprechenden Inhalten durch eine zentrale staatliche Kontrolle umfassend zu verhindern[89]. Folglich ist eine Zugangsbeschränkung nur zu den Inhaltsangeboten möglich, die den staatlichen Behörden bekannt sind. Darüber hinaus ist keine Differenzierung mit Hinblick auf die unterschiedliche Altersstruktur der Nutzer bei einer solch restriktiven Regelung möglich, so daß auch Erwachsenen der Zugriff auf lediglich für Kinder schädliche Inhalte verwehrt wird. Dies verstößt gegen die Konsumentensouveränität, da nicht mehr das einzelne Individuum über die subjektive Kategorie „Nutzen“ entscheidet, sondern dann der Staat diese Entscheidung trifft. Da eine direkte Überwachung der kommunizierten Inhalte die Freiheiten und Kommunikationsmöglichkeiten der einzelnen Nutzer deutlich einengen würde, sind in freiheitlich demokratischen Staaten Widerstände der Bürger zu erwarten, so daß eine solche Regulierung voraussichtlich auch politisch schwer durchsetzbar sein wird.

Wirkungsvollere Lösungen sind von einer teilweisen Selbstregulierung des Internet, in Verbindung mit ökonomischen Instrumenten, zu erwarten. Man muß dabei unterscheiden hinsichtlich Regelungen, die den Zugang zu illegalen Inhalten unterbinden, und Regelungen, die lediglich den Zugriff Minderjähriger auf bestimmte Inhalte verwehren. So ist es möglich, das Angebot von *illegalen* Inhalten zu erschweren, indem die Haftung[90] der Diensteanbieter ausgeweitet wird. So können diese nicht nur für eigene Inhalte, sondern auch für fremde Inhalte, die sie zur Nutzung bereitstellen[91], haftbar gemacht werden, sofern sie von den Inhalten Kenntnis haben und es ihnen technisch möglich ist, deren Nutzung zu verhindern[92]. Durch eine solche Ausgestaltung des Haftungsrechts besteht für einen nach Kostenminimierung strebenden Online-Provider ein Anreiz, die entsprechenden Inhalte vom Gebrauch auszuschließen, wenn die Kosten dafür unter den erwarteten Haftungsansprüchen liegen. Allerdings wird sich der Online-Diensteanbieter nur darauf beschränken, möglichst kostengünstig den Zugang zu den entsprechenden Inhalten zu verhindern und darüber hinaus keine weiteren eigenen Kontrollaktivitäten unternehmen. Aufgrund dessen sollte der Staat die Online-Diensteanbieter, aber auch die Nutzer des Internet anregen, verstärkt selbst Kontrollmaßnahmen durchzuführen. Eine derartige Selbstkontrolle ist durch die Schaffung einer Institution möglich, die den Diensteanbietern und Nutzern des Internet die Gelegenheit bietet, vermeintlich illegale Inhaltsangebote zu melden[93]. Diese Institution sollte diese Hinweise prüfen und bei Verdachtsbestätigung die Inhaltsanbieter über die Existenz von illegalem Material auf ihrem Server informieren. Kann das illegale Material nicht von dem Server entfernt werden,

89 Siehe Göckel (1996) S. 336 f.

90 Je nach den Umständen kann die Haftung dabei durch das Strafrecht, Zivilrecht oder Verwaltungsrecht des jeweiligen Landes erfolgen.

91 Dies gilt beispielsweise für Diensteanbieter, die Speicherkapazität auf ihrem Server bereitstellen (z.B. für Homepages oder Downloads). Dies ist eine gängige Praxis bei den sogenannten Presence Providern. Siehe Lux/Heinen (1997) S. 27.

92 Eine derartige Regelung wurde im deutschen Teledienstegesetz § 5 Abs. 2 vom 13. Juli 1997 verankert.

93 Eine solche Institution existiert auch schon in Deutschland in Form der FSM (Freiwillige Selbstkontrolle Multimedia) vgl. http://fsm.de und in England http://www.iwf.org.uk.

beispielsweise weil sich der Server in einem Land befindet, mit dem keine Kooperationsgemeinschaft besteht, oder weil das Material in dem betreffenden Land nicht illegal ist, könnte eine Sperrung des Zugangs beim Zugangsanbieter eine Alternative sein.

Die Kontrolle *legaler* Inhalte im Internet, die aus Gründen des Jugendschutzes nur volljährigen Nutzern zugänglich sein sollten, kann durch die Teilnehmer selbst erfolgen. Die Zensur findet dabei nicht an der Quelle statt (Verhinderung der Veröffentlichung des Materials), sondern beim Nutzer (Verhinderung des Zugangs Minderjähriger zu schädigendem Material). Hierzu werden die einzelnen Inhaltsangebote von den Anbietern oder anderen Institutionen mit Hilfe einer neutralen Kennzeichnung bewertet (z.B. nach Sprache, sexuellen Inhalt, Gewalt usw.). In Verbindung mit entsprechenden *Filterprogrammen* wird dann der einzelne Nutzer befähigt, durch die individuelle Setzung von Parametern den Zugang von Kindern oder Jugendlichen zu bestimmten Inhaltsangeboten zu beschränken[94]. Ein Inhaltsangebot wird für Minderjährige nur dann zugänglich, wenn es einerseits eine Kennzeichnung trägt und zum anderen im Rahmen der individuell gesetzten Parameter bleibt[95]. Damit ist es möglich, den volljährigen Wirtschaftssubjekten weiterhin die Kenntnisnahme des gewünschten Materials einzuräumen, jedoch Minderjährige von der Nutzung auszuschließen.

Durch eine Selbstkontrolle und teilweise Selbstregulierung kann erreicht werden, daß das Angebot und die Verbreitung von illegalen Inhalten eingeschränkt und der Zugang zu bestimmtem Material für Minderjährige verhindert wird. Die Treffsicherheit einer teilweisen Selbstregulierung hängt allerdings wesentlich von den individuellen Kontrollaktivitäten der einzelnen Nutzer und Diensteanbieter sowie von der Inhaltsbewertung und der Effizienz der speziellen Filterprogramme ab. Vorteile gegenüber einer direkten staatlichen Inhaltskontrolle liegen vor allem in der Zuordnung der Entscheidungskompetenz zu den einzelnen Nutzern, wodurch die Motivations- und Informationsvorteile auf dieser Ebene genutzt werden können. Ferner ist mit einer derartigen Lösung kein direkter Eingriff in die Funktionsweise des Marktes und die Autonomie der Individuen verbunden. Die spezielle Ausgestaltung des Haftungsrechts für Diensteanbieter setzt nur Rahmenbedingungen und beeinträchtigt damit den Marktprozeß nicht unmittelbar. Für das Funktionieren eines solchen Kontrollsystems ist es allerdings erforderlich, daß eine internationale Zusammenarbeit erfolgt. Insbesondere die Entwicklung und Anwendung von einheitlichen Standards zur Kennzeichnung der Inhalte und die Zusammenarbeit der verschiedenen Kontrollinstitutionen zur Verfolgung gesetzwidriger Inhaltsangebote setzen eine Abstimmung auf globaler Ebene voraus[96]. Als flankierende Maßnahme kann eine staatliche Informationspolitik dazu beitragen, die Sensibilität der Öffentlichkeit zu erhöhen und auf diesem Weg die Effektivität einer Selbstregulierung zu verbessern.

Es wurde bereits angedeutet, daß nicht nur der Zugang, sondern auch der *Transport* von illegalen oder jugendgefährdenden Inhalten über das Internet ein gesellschaftliches Problem dar-

94 Seit kurzem gibt es die „Platform for Internet Content Selection“ (PICS), ein System zur Kennzeichnung und Filterung von Internetinhalten. Siehe http://www.w3.org/PICS.

95 Vgl. Mitteilung an das Europäische Parlament (1997) S. 15.

96 Siehe Mitteilung an das Europäische Parlament (19977) S. 18.

stellt. Im Zusammenhang mit dem Auftreten von externen Effekten und asymmetrischer Informationsverteilung bezüglich der angebotenen Dienstleistungen wurde gezeigt, daß die Verwendung von starken Verschlüsselungsverfahren dazu beitragen kann, den Transport der Inhalte über das Netz sicherer zu machen. Durch die individuelle Nutzung moderner und extrem starker Verschlüsselungssysteme[97] ist es aber möglich, daß Probleme für die Gesellschaft auch aus der „zu sicheren" Datenübertragung entstehen. Denn mit der Verwendung von starken kryptografischen Verfahren wird die Verfolgung krimineller Aktivitäten, die über das Netz abgewickelt werden, unmöglich[98]. Zwar besteht nach wie vor die Möglichkeit, die Übertragung abzuhören, aber diese Daten sind wertlos, wenn sie chiffriert sind und die zugehörigen Schlüssel fehlen. Aufgrund dessen wird von einigen Staaten derzeit nicht die Verbreitung und Nutzung sicherer Datenübertragung im Internet unterstützt, sondern im Gegenteil der Einsatz kryptografischer Verfahren reguliert. Vor allem die bedenklichen Konsequenzen, die aus der Verbreitung und Nutzung moderner Verschlüsselungsverfahren für die innere und äußere Sicherheit des Staates erwachsen, werden dabei als Grund für eine staatliche Regulierung angeführt. In der gegenwärtigen internationalen Diskussion über die Regulierung des Internet werden vor allem zwei Instrumente, das generelle Verbot[99] und die Zulassung nur bestimmter Verschlüsselungsverfahren[100], als geeignet angesehen, staatlichen Institutionen die Möglichkeit der Datenüberwachung einzuräumen. Im folgenden soll untersucht werden, ob mit dem Einsatz dieser ordnungsrechtlichen Mittel im Internet die eben beschriebenen negativen Externalitäten eingeschränkt werden können und wie diese Handlungsalternativen zu bewerten sind.

Mit einem *Verbot von Kryptoverfahren* (Verschlüsselungsverfahren) soll den staatlichen Sicherheitsbehörden das Abhören des Fernmeldeverkehrs im Rahmen ihrer gesetzlichen Befugnisse erleichtert werden. Faktisch würde ein derartiges Verbot bewirken, daß flächendeckend allen Wirtschaftssubjekten verboten wird, ihre Daten autonom gegen den Zugriff Dritter zu sichern, um in wenigen Einzelfällen die staatliche Überwachung zu ermöglichen. Eine solche Regulierung ist verfassungsrechtlich und gesellschaftspolitisch nicht unbedenklich[101], erscheint bezüglich der Treffsicherheit und des Kontrollaufwandes hingegen ein geeignetes Instrument zu sein, die Kontrolle des Fernmeldeverkehrs durch Sicherheitsbehörden zu gewährleisten. Dieser Aspekt offenbart bei näherer Betrachtung aber Schwierigkeiten. Ein solches Verbot kann praktisch ohne größeren Aufwand von den Kommunikationsteilnehmern unterlaufen werden, da mit geringem Aufwand Schlüssel selbst herstellbar sind, aber auch

97 Als starke Verfahren werden derzeit Verschlüsselungsprogramme mit Schlüssellängen von mindestens 90 bit bei symmetrischen Verfahren und 1024 bit bei asymmetrischen Verfahren verstanden. Vgl. Rojas (1996) S. 238 f.

98 Zu denken ist hier insbesondere an Steuerhinterziehung, Geldwäsche oder auch die Verbreitung von illegalem und schädlichem Inhalt über das Internet.

99 In Frankreich wurde am 29. Dezember 1990 ein Gesetz erlassen, wonach die Verschlüsselungsanwendung einer Erlaubnis des Premierministers verlangt. Vgl. Hortmann (1997) S. 214 und Rihaczek (1996a) S. 484 ff.

100 Vgl. Bizer (1996) S. 10.

101 Eine solche Vorschrift wäre in Deutschland mit der Einschränkung des Grundrechts auf Wahrung des Fernmeldegeheimnisses (Art. 10 Abs. 1 GG) verbunden, denn es untersagt dem Internetnutzer, seine individuelle Kommunikation selbst zu schützen. Zur rechtlichen Diskussion siehe Bizer (1996) S. 11.

derzeit im Internet zu erhalten sind[102]. Da die Daten in digitaler Form übertragen werden, bieten sich den einzelnen Nutzern des Internet noch verschiedene Möglichkeiten der elektronischen Tarnung[103] zur Umgehung des staatlichen Verbots. Für eine Durchsetzung sind deshalb wirksame Kontrollen notwendig. Diese bedingen den Aufbau einer umfassenden Kontrollinfrastruktur, welche die einzelnen Transaktionen und Datenübertragungen der nationalen Nutzer des Internet auf die mißbräuchliche Verwendung von Verschlüsselungsverfahren hin überprüft. Eine derartige Überwachung der Datenkommunikation im Internet ist mit extrem hohen Kosten verbunden und wird mit Hinblick auf die technischen Gegebenheiten dennoch keine umfassende Kontrolle ermöglichen. Gerade die für die staatliche Überwachung relevanten Kreise, wie kriminelle Organisationen und extremistische Vereinigungen, werden sich im Falle eines Verbots nicht von der Verwendung aufwendiger Verschlüsselungsverfahren abhalten lassen, solange die Wahrscheinlichkeit der Entdeckung gering und der Nutzen aus der abhörsicheren Übertragung hoch ist[104]. Aufgrund dessen sollte auf ein generelles Verbot von Verschlüsselungsverfahren verzichtet werden[105], da hiermit ein starker Eingriff in die Entscheidungskompetenzen der Individuen verbunden ist, aber das gewünschte Ziel, die Überwachung der Kommunikation im Internet, mit einem so gearteten staatlichen Eingriff nicht erreicht werden kann[106]. Überdies werden die Wirtschaftssubjekte in Zukunft immer stärker auf die sichere Übertragung ihrer Daten über das Internet angewiesen sein, so daß durch ein solches Verbot die Entwicklung des elektronischen Marktes graduell gefährdet ist und die Schadenswirkungen für unbeteiligte Dritte aufgrund von Verletzungen der Informationssicherheit zunehmen werden.

Ein anderer Lösungsansatz wird durch die *Lizensierung von Verschlüsselungsverfahren* gewählt. Dabei werden nur solche Verfahren von einer Regulierungsbehörde genehmigt, die den Sicherheitsbehörden Möglichkeiten zum Dechiffrieren bieten. Zu diesem Zweck können unterschiedliche Wege beschritten werden. Man kann sich auf die Freigabe von, in ihrer Leistungsfähigkeit beschränkten, Kryptografieverfahren einigen, die durch leistungsfähige Rechnersysteme der Sicherheitsbehörden zu entschlüsseln sind[107], oder es werden nur solche Verfahren zugelassen, bei denen die verwendeten Schlüssel zentral aufbewahrt werden müssen,

102 Vgl. Winkel/Büllingen (1995) S. 46, Hamm (1997) S. 4 ff.

103 So kann mit modernen technischen Mitteln verschleiert werden, daß verschlüsselt wurde. Mit Hilfe der sogenannten Steganografie lassen sich chiffrierte Nachrichten unauffällig in harmlos wirkenden Dateien verstecken. Vgl. Gerling (1997) S. 200.

104 Vgl. Winkel/Büllingen (1995) S. 46.

105 Vgl. Bizer (1996) S. 12, Hamm (1997) S. 191.

106 Ein Kennzeichen moderner Rechtsstaaten ist die Garantie von Grund- und Menschenrechten als Abwehrrechte gegenüber staatlicher Gewalt. Einschränkungen sind begründungsbedürftig und unterliegen besonderen Rechtfertigungslasten. Rechtlich zulässig sind sie nur, wenn sie legitime Ziele mit Mitteln verfolgen, die tatsächlich geeignet sind, sie zu erreichen.

107 In Exportversionen von US-amerikanischer Software sind heute ausschließlich schwache Algorithmen oder kurze Schlüssellängen implementiert, damit amerikanische Geheimdienste die Möglichkeit zur Überwachung haben. Vgl. Hamm (1997) S. 188.

so daß im Bedarfsfall die Sicherheitsbehörden die Möglichkeit haben, nach einem festgelegten rechtlichen Verfahren auf die hinterlegten Schlüsseldublikate zuzugreifen[108].

Mit der Zulassung nur bestimmter Verschlüsselungsverfahren wird erreicht, daß die einzelnen Wirtschaftssubjekte ihre Kommunikation schützen können, gleichzeitig aber die Sicherheitsbehörden auch die Möglichkeit haben, die verschlüsselten Daten zu überwachen. Geeignete Sanktionsmechanismen müssen aber dafür sorgen, daß auch nur die gesetzlich zugelassenen Programme genutzt werden. Um die Nutzung nur bestimmter Verschlüsselungsverfahren zu garantieren kann einerseits der Vertrieb kontrolliert oder andererseits die einzelnen Transaktionen der Internetnutzer auf den Einsatz der zulässigen Verfahren hin überprüft werden. Wie schon bei der Durchsetzung des Verbots von Verschlüsselungsverfahren gezeigt, ist eine wirksame Kontrolle des Angebots oder der Verwendung von Verschlüsselungsverfahren im Internet nicht möglich. Da vielfältige Wege der Umgehung[109] einer solchen staatlichen Kryptoreglementierung bestehen, kann auch eine Verwendungsauflage nur sehr bedingt zur Begrenzung der negativen Auswirkungen, die aus der Nutzung extrem starker Verschlüsselungsverfahren erwachsen, beitragen. Bezieht man die Erfahrungen ein, die in den USA mit der Hinterlegung von Schlüsseldublikaten gesammelt wurden, läßt sich nicht ausschließen, daß sich auch hinsichtlich der Durchsetzbarkeit im politischen Prozeß Probleme ergeben werden[110]. Auch das Lizensierungsmodell erscheint aus den angegebenen Gründen deshalb nicht geeignet, die Probleme, die aus der Entwicklung und der Verbreitung der neuen Kryptoverfahren erwachsen, in vollem Umfang zu bewältigen. Angesichts der Tatsache, daß eine solche Regulierung einen starken Eingriff in die Entscheidungskompetenzen der Individuen, Grundrechte der Bürger und in den Marktprozeß darstellt, sprechen viele Argumente dafür, auch auf eine Regulierung durch Lizensierungsmaßnahmen seitens des Staates zu verzichten[111].

[108] Dies ist genau die Stoßrichtung des amerikanischen ESCROW-Programms („Clipper-Initiative“), das am 16. 4. 93 von Präsidenten Clinton angekündigt wurde und heftige Diskussionen auslöste. Vgl. Rihaczek (1996) S. 603.

[109] Neben der schon erwähnten Steganografie kann auch eine Nachricht „überschlüsselt“ werden. Dabei wird mit einem zugelassenen Verfahren der zu übertragende Text verschlüsselt, der vorher mit einem nicht lizensierten Verfahren chiffriert wurde. Bei einer Überwachungsmaßnahme würde zuerst die übertragene Nachricht entschlüsselt. Erst zu diesem Zeitpunkt fällt auf, daß ein nicht zugelassenes Verfahren genutzt wurde. Siehe Hamm (1997) S. 189.

[110] Die kann auch auf das in *Amerika* herrschende Demokrativerständnis und die liberale Bürgerrechtstradition zurückzuführen sein, im zentralistisch organisierten *Frankreich* wurde eine Lizensierung dagegen ohne größeren Protest hingenommen. Vgl. Rihaczek (1996) S. 484 ff., Winkel/Büllingen (1995) S. 48.

[111] Mit dem Beschluß des Informations- und Kommunikationsdienstegesetzes des Deutschen Bundestages am 1. 8. 97 wurde laut Art. 3 § 5 Abs. 4 auf eine Regulierung von Kryptierungsverfahren verzichtet.

III. Schlußbetrachtung

Insgesamt zeigt sich, daß verschiedene ökonomische und gesellschaftspolitische Gründe für staatliche Eingriffe in die Anwendungsebene des Internet sprechen können. Eine nähere Analyse unter Beachtung der technischen Eigenschaften des Internet ergab jedoch, daß einige wirtschaftspolitische Instrumente infolge der Struktur des Internet nicht die gewünschten Wirkungen erzielen werden. Zwar können Informationsasymmetrien und externe Effekte durch die spezifische Ausgestaltung des Haftungsrechts und die Setzung von Mindestsicherheitsstandards vermindert werden, allerdings erfordert der Einsatz dieser Instrumente gleichwohl internationale Vereinbarungen, da infolge der internationalen Verbreitung des Internet einzelstaatliche Regelungen das angebotene Sicherheitsniveau nur bedingt beeinflussen können, aber negative Auswirkungen auf die Wettbewerbsfähigkeit nationaler Anbieter haben. Einzig Mindestsicherheitsstandards für Zertifizierungsstellen und eine staatliche Informationspolitik, die einerseits die Nutzer des Internet für Sicherheitsfragen stärker sensibilisiert und andererseits den Teilnehmern ihre moralische Pflicht bei der Verfolgung von gesetzwidrigen Inhalten im Internet vor Augen führt, erscheinen notwendig und sinnvoll. Es können nicht alle auftretenden Allokationsineffizienzen auf der Anwendungsebene des Internet durch staatliche Aktivitäten geheilt werden. Es ist jedoch nicht auszuschließen, daß das gesteigerte Bewußtsein, welches der Sicherheit im Netz entgegengebracht wird, und die dynamische Entwicklung des Internet dazu führen werden, daß andere, neue Möglichkeiten des Marktes zur Beseitigung der Sicherheitsmängel gefunden werden.

Von einer staatlichen Regulierung des Einsatzes kryptografischer Verfahren sollte generell abgesehen werden, da der erhoffte Nutzen zur Bekämpfung der Kriminalität und die Verhinderung von Straftaten sich mit den derzeit verfügbaren Instrumenten nicht sicher erreichen läßt. Dies ist auf die Tatsache zurückzuführen, daß die vorgestellten Handlungsoptionen des Staates leicht umgangen werden können und aus technischer und finanzieller Sicht kaum kontrollierbar sind. Mit solchen Eingriffen wird darüber hinaus kein Vertrauen in die Sicherheit des Netzes aufgebaut, was die kommerzielle Verwendung und weitere Entwicklung des Internet negativ beeinflußt[112].

112 Werden auf innovationsdynamischen Märkten staatliche Regelungen nicht ständig neu angepaßt, können sie sich als Innovationsbremse erweisen. Da gerade das Internet derzeit - und wohl auch noch in absehbarer Zukunft - ein hohes Innovationstempo aufweist, sollten staatliche Eingriffe eingeschränkt werden, damit sie nicht die dynamische Entwicklung behindern.

Bibliographie

Ackerlof, G. (1970): The market for lemons: Qualitative uncertaintzy and the market mechanism, in: Quarterly Journal of Economics 84, S. 488-500.

Beck, Hanno und Aloys Prinz (1997): Die Welt am Netz: Wieviel Regulierung braucht das Internet?, in: Wirtschaftsdienst VIII, 1997.

Beck, Hanno und Aloys Prinz (1997a): Should the World be taxed? - Taxation and the Internet, in: Intereconomics, März/April, 1997 S. 87-92.

Bizer, Johann (1996): Kryptokontroverse - Der Schutz der Vertraulichkeit in der Telekommunikation, in: Datenschutz und Datensicherheit, Nr. 1, S. 5-12.

Blankart, Charles B. und Günther Knieps (1992): Netzökonomik, in: Jahrbuch für Neue Politische Ökonomie, Bd. 11, S. 73-87.

Blind, Knut (1996): Informationssicherheit in offenen Kommunikationssystemen: Eine staatliche Regulierungsaufgabe?, in: List Forum für Wirtschafts- und Finanzpolitik 22, Heft 4, S. 377-388.

Blind, Knut (1996a): Allokationsineffizienzen auf Sicherheitsmärkten - Ursachen und Lösungsmöglichkeiten, Fallstudie: Informationssicherheit in Kommunikationssystemen, Frankfurt am Main.

Carter, Michael und Graeme Guthrie (1995): Pricing the Internet: The New Zealand Experience, in: Christchurch, New Zealand, Diskussion Paper/Department of Economics, University of Canterbruy, 9501.

Clark, David (1997): Internt Cost Allocation and Pricing, in: Lee W. McKnight und Joseph P. Bailey (Hrsg.): Internet Economics, Cambridge.

Coase, R. H. (1960): The Problem of Social Cost, in: Journal of Law and economics, Nr. 3. S. 1-44.

Coates, Kevin (1998): Competing for the Internet, in: EC Competition Policy Newsletter, auch online verfügbar: http://europa.eu.int/en/comm/dg04/speech/eight/en/sp98006.htm

Deutsches Institut für Wirtschaftsforschung (1996): Beiträge zur Strukturforschung, Künftige Entwicklung des Medien- und Kommunikationssektors in Deutschland, Heft 162, Berlin.

Ehlers, St. (1994): Telekommunikation: Dienste, Übersichten, Entscheidungshilfen, Berlin.

Fichert, Frank (1998): Das Microsoft-Monopol: Herausforderung für die Wettbewerbspolitik, in: Wirtschaftsdienst VI, S. 343-347.

Fritsch, Michael, Ewers, Hans-Jürgen und Thomas Wein (1996): Marktversagen und Wirtschaftspolitik: mikroökonomische Grundlagen staatlichen Handelns, München.

Gerling, W. (1997): Verschlüsselungsverfahren, in: Datenschutz und Datensicherheit, Nr. 4.

Grimm, Rüdiger (1997): Electronic Commerce, in: Datenschutz und Datensicherheit, Nr. 7, S. 420.

Göckel, Andreas (1996): Inhaltsverantwortung im Internet, in: Archiv für Post und Telekommunikation, Nr. 4.

Grupta, Alok und Dale O. Stahl und Andrew B. Whinston (1997): Priorty Pricing of Integrated Services Networks, in: Lee W. McKnight und Joseph P. Bailey (Hrsg.): Internet Economics, Cambridge.

Hamm, Rainer (1997): Kryptokontroverse, in: Datenschutz und Datensicherheit, Nr. 21, S. 180-191.

Hansen, Hans Robert (1992): Wirtschaftsinformatik I, 6. Aufl. Stuttgart, Jena.

Hirshleifer, J. und John G. Riley (1979): The Analytics of Uncertainty and Information - An Expository Survey, in: Journal of Economic Literature, Vol. XVII, S. 1375-1421.

Horner, Frances M. und Jeffery Owens (1996): Tax and the Web: New Technology, Old Problems, in: Bulletin for International fiscal documentation: publication of the International Bureau of Fiscal Documentation, Bd. 50, Heft 11-12, S. 516-523.

Hortmann, Michael (1997): Kryptoregulierung weltweit - Überblick, in: Datenschutz und Datensicherheit, Nr. 21, s. 214-215.

Kallfass, Hermann H. (1989): Großunternehmen und Effizienz, Göttingen.

Katz, Michael und Carl Shapiro (1994): Systems Competition and Network Effects, in: Journal of Economic Perspectives, Vol. 8, Nr. 2, S. 93-115.

Knorr, Henning (1993): Ökonomische Probleme von Kompatibilitätsstandards: eine Effizienzanalyse unter besonderer Berücksichtigung des Telekommunikationsbereichs, Baden-Baden.

Knorr, Michael und Uwe Schläger (1997): Datenschutz bei elektronischem Geld - Ist das Bezahlen im Internet anonym?, in: Datenschutz und Datensicherheit, Nr. 7, S. 396-402.

Kohlhass, Michael (1994): Ökonomische Instrumente in der Umweltpolitik, in: Vierteljahreshefte zur Wirtschaftsforschung, S. 354-376.

Kuhlmann, Eberhard (1990): Verbraucherpolitik: Grundzüge ihrer Theorie und Praxis, München.

Kurth, Helmut (1993): Grundlagen der Informationssicherheit, in: Hartmut Pohl und Gerhard Weck (Hrsg.), Einführung in die Informationssicherheit, München.

Liebowitz, S. J. und Stephen E. Margolis (1994): Network Externality: An uncommmon Tragedy, in: Journal of Economic Perspectives, Vol. 8, Nr. 2, S. 133-150.

Lux, Harald und Irene Heinen (1997): Der Internetmarkt in Deutschland: Provider & Dienstleister, 2. Aufl., Heidelberg.

MacKie-Mason, Jeffrey K., Liam Murphy und John Murphy (1997): Responsive Pricing in the Internet, in: :Lee W. McKnight und Joseph P. Bailey (Hrsg.): Internet Economics, Cambridge.

Mitteilung an das Europäische Parlament (1997): Illegale und schädigende Inhalte im Internet, online verfügbar: http://www2.echo.lu/legal/de/internet/content/communic.html.

Molitor, Bruno (1990): Wirtschaftspolitik, 2. Aufl.

Newsbytes New Network vom 03. 06. 96: Singapore to regulate user Internet access, online verfügbar: http://www.nb-pacifica.com/reg/singaporetoregulateus_523.shtml.

Oberlack, Hans Günther (1989): Handelshemmnisse durch Produktstandards: ökonomische Aspekte ihrer Beseitigung, Hamburg.

OECD (1997): C/MIN(97)11 Global Information Infrastructure - Global Information Society (GII-GIS): Policy Recommendations for Action, Online verfügbar: www.oecd.org/sge/council/ministerial/papers/eng_cmin11.add.pdf.

Recke, Martin (1996): Der Umbruch der Medienpolitik im digitalen Zeitalter - Zur Regulierung der Medien und der Telekommunikation in Deutschland, online verfügbar: http://userpage.fu-berlin.de/~mr94/dipom/expose-0.9beta.html.

Rihaczek, Karl (1996): Die US-Kryptoinitiative, in: Datenschutz und Datensicherheit, Nr. 10, S. 602-605.

Rihaczek, Karl (1996a): Neue französische Kryptogesetzgebung, in: Datenschutz und Datensicherheit, Nr. 8, S. 484-489.

Rohlfs, Jeffery (1974): A Theory of Interdependent Demand for a Communications Service, in: Bell Journal of Economics and Management Science, Vol. 5 (1).

Rojas, Raul (1996): Elektronisches Geld im globalen Datennetz, in: PROKLA, Zeitschrift für kritische Sozialwissenschaft, Heft 103, 26. Jg., Nr. 2, S. 227-240.

Röver, Andreas (1997): Netzexternalitäten als Ursache für Marktversagen, Frankfurt am Main, Europäische Hochschulschriften: Reihe 5 Bd. 2072.

Rupp, Hans Björn (1996): Ein Preissystem für das Internet, Wissenschaftliches Institut für Kommunikationsdienste, Diskussionsbeitrag Nr. 164, Bad Honnef.

Sakar, Mitrabarun (1997): Internet Pricing: A Regulatory Imperative, in: Lee W. McKnight und Joseph P. Bailey (Hrsg.): Internet Economics, Cambridge.

Schickele, Sandra (1996): the Case for a public Subsidy of the Internet, online verfügbar: http://netec.mcc.ac.uk/WoPEc/data/papers/wopsonoma_001.html.

Soete, Luc und Karin Kamp (1996): The „Bit Tax“: the case for further research, in: Science and public Policy, Vol. 23, Nr. 6, S. 353-360, online verfügbar: http://www.ispo.cec.be/hleg/bittax.html.

Soete, Luc und Bar Ter Weel (1998): Globalization, Tax Erosion and the Internet, online verfügbar: http://netec.mcc.ac.uk/WoPEc/data/papers/dgrumamer1998026.html.

Spence, M. (1973): Job Market Signalling, in: Quarterly Journal of Economics, S. 113-116.

Stahlknecht, Peter (1991): Einführung in die Wirtschaftsinformatik, 5. Aufl., Berlin, Heidelberg, New York u.a..

Stiglitz, J. E. (1979): Information and Economic Analysis, in: Parkin, Michael und Nobay, A. R. (Hrsg.), Current Economic Problems, London, S. 27 ff.

The Economist (31. 05. 97): Taxes Slip Through the Net.

Thum, Marcel (1995): Netzwerkeffekte, Standardisierung und staatlicher Regulierungsbedarf, Tübingen.

Wegehenkel, Lothar (1980): Transaktionskosten, Wirtschaftssystem und Unternehmertum, Tübingen.

Weiber, Rolf (1992): Die Diffusion von Telekommunikation: Problem der kritischen Masse, Münster.

Weimann, Joachim (1996): Wirtschaftspolitik: Allokation und kollektive Entscheidung, Berlin.

Weinkopf, Marcus (1993): Ökonomie des ONP-Konzeptes, Wissenschaftliches Institut für Kommunikationsdienste Bad Honnef, Diskussionsbeitrag Nr. 118.

Wicke, L. (1993): Umweltökonomie, 4. Aufl., München.

Winkel, Olaf und Franz Büllingen (1995): Sicherheit in der Telekommunikation - Soziale, institutionelle und organisatorische Voraussetzungen der Implementation von Sicherheit in telematischen Netzwerken, Wissenschaftliches Institut für Kommunikationsdienste, Diskussionbeitrag Nr. 153, Bad Honnef.

Witt, Ulrich (1997): „Lock in“ vs. „critical masses“ - industrial change under network externalities, in: Internationale Journal of Industrial Organization, Vol. 15, No. 6, S. 753-775.

Wöckner, Bernd (1996): Standardisierungspolitik für die Informationsgesellschaft in: Jahrbuch für Nationalökonomie und Statistik, Bd. 215/3, S. 256-273.

Verweise auf Internet-Adressen

http://www.w3.org/PICS	Platform for Internet Content Selection
http://fsm.de	Freiwillige Selbstkontrolle Multimedia
http://www.iwf.org.uk	Internet Watch Foundation