APuZ
Aus Politik und Zeitgeschichte
30 – 31/2005 · 25. Juli 2005

Sicherheit im Internet

Beilage zur Wochenzeitung Das **Parlament**

Editorial

Die rasche Ausbreitung des Internets über geographische und administrative Grenzen hinweg hat ungeahnte individuelle Freiheiten eröffnet. Doch zugleich haben sich die Sicherheitsprobleme verschärft. Die Freiheit des weltweiten Datennetzes braucht Regeln. Einheitliche Identifikationen von Internetdiensten, eine kontrollierte, zertifizierte Vergabe von Domainadressen sowie digitale E-Mail-Signaturen können helfen, Missbrauch und kriminellen Machenschaften zu begegnen. Doch viele Nutzer bewegen sich sorglos im Netz – ohne individuelle Sicherheitsvorkehrungen. Die Vision eines zuverlässigen Netzes setzt dagegen auf verantwortliche und verlässliche Nutzer.

In der Wissensgesellschaft des 21. Jahrhunderts muss das Spannungsfeld von Copyright und seinen Schranken, von Verwertungsinteressen und Bürgerrechten neu vermessen werden. Ende Juni hat der Supreme Court der USA verfügt, dass amerikanische Hersteller von Tauschbörsenprogrammen zu Schadenersatz verurteilt werden können, weil sich mit der Software auch Raubkopien verbreiten lassen. Dieses Urteil legt das Urheberrecht ganz im Sinne der Musik- und Filmindustrie aus, die längst „Digitales Rechtemanagement“ einsetzen, um die unerwünschte Weitergabe von Werken zu erschweren.

Staatliche Eingriffe erscheinen indes weder zweckmäßig noch wünschenswert. Autoritär regierte Staaten haben sogar zu drakonischen Zensurmaßnahmen gegriffen: Das Internet provoziert neue Möglichkeiten zentralistischer Kontrolle. Dass das Netz künftig auch zur Kriegführung dienen kann, belegen die Sicherheitsdebatten über den internationalen Terrorismus.

Hans-Georg Golz

Esther Dyson

Das zuverlässige Netz

Essay

Während der Online Publishers Conference in Palm Beach (Florida) im November 2004 fragte jemand nach E-Mail-Marketing: „Zu große Ähnlichkeit mit Spam oder Phishing“, antworteten die Podiumsteilnehmer. Am selben Tag wollten wir einen Flug von Santa Fe nach Albuquerque (New Mexico) buchen. Aber die URL[1] für www.SantaFeShuttle.com führt automatisch zur Seite www.SandiaShuttle.com, eine ganz andere Fluggesellschaft als die, die wir wollten. Der Unterschied zwischen beiden ist nicht klar, wenn man sich im Netz befindet, aber er wird sehr deutlich, sobald man zum Flughafen kommt: Dort befinden sich die Schalter beider Gesellschaften direkt nebeneinander. Santa Fe Shuttle und Sandia Shuttle tragen gerade einen Rechtsstreit aus, in dem es um den Domainnamen geht.[2] Auf dem Flug nach Albuquerque schauten wir fern: eine Episode des Fernsehmagazins „60 Minutes“ von CBS, in der eine herzzerreißende Geschichte von entzweiten Familien erzählt wurde. Die beiden Schwestern waren zerstritten, weil die eine 50 000 Dollar unter dem Namen der anderen ausgegeben hatte. Eine uralte Geschichte, aber sie wurde aktuell, weil sie durch das modernste aller Übel, Identitätsdiebstahl, Nachrichtenwert erhielt.

Esther Dyson
B.A., geb. 1952; 1998 bis 2000 Gründungsvorsitzende der Internet Corporation for Assigned Names and Numbers (ICANN); seit 1983 Redakteurin und Herausgeberin des monatlichen Newsletters „Release 1.0“ bei CNET Networks.
104 Fifth Avenue, New York, NY 10011, USA.
edyson@release1-0.com

Das Internet ist heute ein Ort des Identitätsdiebstahls, und daher verliert es für viele zunehmend an Attraktivität. Das liegt an der Flut von Spam[3] und Phishing[4], an so genannten *joe jobs* (ahnungslose Nutzer erhalten Antwortnachrichten, die eigentlich für jemand anderen bestimmt sind), an infizierten Computern, die Spam, Viren, gefälschte E-Mails und Webseiten verschicken, und an allen anderen Arten von Datenmüll und Bedrohungen.

In diesem Zustand liegt eine gewisse Ironie, denn das Netz sollte eigentlich ein sichererer Ort sein als die reale Welt: Man muss nichts mit Fremden zu tun haben, wenn man es nicht will, und theoretisch sind alle Dinge auffindbar. Und es ist leichter, Fremde außen vor zu halten – wenn man das wünscht. Doch es ist gleichzeitig viel schwieriger, herauszufinden, mit wem man es jeweils wirklich zu tun hat. Das hat in unserer vertrauensseligen Welt zu einem sehr offenen Netz geführt, in dem sich Fremde tummeln. Doch wenn man die Prämissen verändert – nicht: jeder ist ein Fremder, sondern: Fremde werden ausgeschlossen –, kann man eine völlig andere Welt erschaffen: das zuverlässige Netz.

Was würde sich ändern? Systeme sollen künftig als geschlossene, nicht als offene beginnen. Jeder wird nur mit einem identifizierbaren, vertrauenswürdigen, zuverlässigen Gegenüber verkehren. Dieses Netz nenne ich *peer-to-peer accountable*, d. h., zwei miteinander verbundene Computer und ihre Nutzer agieren vertrauensvoll miteinander. Voraussetzung hierfür ist, dass es keiner staatlichen Regulierungen bedarf, um die geschlossene, sichere Welt des Internets als breiteren, aber von Regeln bestimmten öffentlichen Raum wieder zu eröffnen. Denn geographisch eingeschränkte Regierungen sind nur schlecht ausgestattet, um die Sicherheit in einem globalen Netz aufrechtzuerhalten; lokales, privates Handeln ist dazu viel besser geeignet. Das zuverlässige Netz berücksichtigt individuelle Vorlieben, es macht die Teilnehmer untereinander verantwortlich und nicht gegenüber

Übersetzung aus dem Englischen von Hans-Georg Golz, Bonn.

[1] *Uniform Resource Locator*, Fundort des Dokuments im Internet.

[2] Mit *Domain* bezeichnet man logische Subnetze innerhalb von Netzwerken. Im Internet ist die Domain die wichtigste Art der Organisation, sie bestimmt die Internetadresse.

[3] Unerwünschte Form von Massen-E-Mails; wörtlich eine Mischung aus *ham* und *spiced pork*, eine beliebte Frühstücksmahlzeit in den USA.

[4] Betrügerische Versuche, über das Internet den Nutzern Passworte und Geheimzahlen von Bankverbindungen zu entwenden; wörtlich eine Mischung aus *password* und *fishing*.

Regierungsvorgaben, die nicht jedem gefallen mögen. Die Nutzer können wählen, unter welchem Regime sie „leben“ möchten: Wer mehr Regulierung möchte, kann wählen, nur mit solchen Teilnehmern zu kommunizieren, die sich solchen Systemen unterwerfen möchten, während jene, die lügen und betrügen möchten, es mit solchen zu tun bekommen, die das ebenfalls tun.

Man kann beide Systeme anhand von verschiedenen Kriterien unterscheiden: an Reputationssystemen (*brands*) und vor allem anhand der Domainnamen, oder aber anhand von *certified-mailer*-Programmen, welche die Identität von E-Mail-Absendern verifizieren. Dabei können sich Regierungen hilfreich beteiligen, sowohl, indem sie den privaten Sektor zur Selbstregulierung bewegen, und sei es nur aus Furcht vor staatlichen Eingriffen, als auch, indem kriminelle Machenschaften im Netz strafverfolgt werden bzw. eine Wiedergutmachung eingetretener Schäden erwirkt wird, wo die Kräfte des Marktes versagen und Selbstregulierung diese Arbeit nicht erledigen kann.

Jede Art von Internet-Governance funktioniert besser, wenn sie *peer to peer* stattfindet oder auch nur gelegentlich zu erkennen und nicht zentralisiert ist. Mit angemessenen Informationen über ihre Gegenüber, verlässlichen Reputationssystemen sowie Schutztools und -diensten sind die Nutzer bestens ausgestattet, für sich selbst zu entscheiden oder diese Entscheidungen an bestimmte Instanzen zu delegieren, deren Zielen sie vertrauen und die wiederum verantwortlich (nach den Regeln des Wettbewerbs) gegenüber ihren Kunden handeln. Sie sind ebenfalls bestens ausgestattet, um Netzwerke kommunikativer Beziehungen zu knüpfen. Im zuverlässigen Netz geht es nicht nur darum, bestimmte Menschen auszuschließen, sondern vor allem darum, Menschen miteinander in Kontakt zu bringen.

Für dieses *peer-to-peer*-Paradies einer wirkungsvollen Internet-Governance benötigen wir vor allem zwei Dinge. Zum einen müssen Authentifizierungssysteme von Menschen und Institutionen gewährleisten, dass Reputation und die Regeln, nach denen sie sich verhalten, auf sichere Weise nur jenen Teilnehmenden zugeordnet werden, die sie sich auch verdient haben. Das erfordert bestimmte Tools und Dienste, die es Individuen und Organisationen ermöglichen, diese Informationen zu interpretieren. Nur mit einer solchen Infrastruktur der Authentifizierung ist es möglich, eine verlässliche Reputation der Teilnehmenden sowie Systeme der Verantwortlichkeit zu schaffen. Das bedeutet nicht, dass Anonymität im Netz künftig unmöglich sein soll – aber sie soll für jeden klar erkennbar sein, sodass sich Individuen entscheiden können, ob sie mit anonymen Nutzern überhaupt in Austausch treten möchten und ob und wann sie ihre eigene Identität offen legen möchten. (Dabei können durchaus auch anonyme Nutzer von solchen Empfehlungen profitieren, etwa wenn andere Individuen oder Organisationen für ein bestimmtes Verhalten des anonymen Teilnehmers beim Versenden von E-Mails, bei Bankgeschäften oder beim Posten von Beiträgen in Chatrooms bürgen.)

Zum anderen erweitert das zuverlässige Netz die Macht der Individuen, ihre eigene Wahl zu treffen, und zwar durch Software, Organisationen und Dienste, die dazu dienen, die Meinungen der Nutzer auszudrücken, ihre Marktmacht zu bündeln, ihre Reputation zu verbreiten und Verantwortlichkeit zu stärken. Hiermit sind Tools von Softwarehändlern gemeint, ebenso Reputationsdienste, die als Netzcommunities mit eigenen Regeln und Diensten das Verhalten ihrer Mitglieder beobachten und im Gegenzug bestimmte Privilegien zusichern. Diese Communities handeln im Auftrag der individuellen Teilnehmer, die sie gewählt haben, nicht etwa kollektiv im Auftrag aller Menschen, die in einem bestimmten geographischen Raum leben. In Extremfällen können diese Organisationen Individuen sogar dabei helfen, Ansprüche gegenüber Übeltätern geltend zu machen, oder sie können mit der Regierung zusammenarbeiten, um Betrug und andere Verbrechen zu verfolgen.

Das zuverlässige Netz ist eine Vision der Dezentralisierung. Viele Teilnehmer müssen zusammenwirken. Im Einzelnen geht es um Dienste, die es individuellen Nutzern ermöglichen, ihre Gegenüber sicher zu identifizieren und zur gleichen Zeit ihre eigene Identität zu schützen; es geht weniger um Biometrie, die es beispielsweise Unternehmen erlaubt, ihre Beschäftigten und ihre Kunden zu identifizieren. Im Mittelpunkt müssen Authentifizierungsstandards für den E-Mail-Verkehr, Domainauthentifizierungen, elektronische Signaturen, Reputationssysteme und die allge-

meine Netzsicherheit stehen. Die technischen Möglichkeiten dazu sind längst vorhanden.[5]

Insbesondere die Spam-Plage ist so schlimm geworden, dass sich einstige Konkurrenten längst zusammengetan haben. Spam ist ein gutes Beispiel für asymmetrischen Krieg – jede Einzellösung würde die Angriffe nur verstärken. Man benötigt stattdessen eine Art elektronisches Immunsystem, das kontinuierlich neue Antikörper entwickelt, um den neuen Bedrohungen begegnen zu können. Nur ein erster Schritt wäre die Authentifizierung, denn sie würde Mailempfängern (meist ein Internet-Serviceprovider oder ein Filter von Unternehmen) gestatten, *spoofing* zu unterbinden (das Benutzen einer falschen Absenderadresse einer Domain, die nicht verantwortlich für die Sendung ist).

Ferner wäre über eine pfadgestützte und eine signaturgestützte Authentifizierung von Domains nachzudenken. Erstere bezieht sich auf die Herkunft der E-Mail – meist auf die IP (*internet protocol*)-Adresse – und vergleicht sie mit einer Liste erlaubter IP-Adressen, die in den Namenssystemen der jeweiligen Domain aufgezeichnet sind. Die IP-Adresse ist nur sehr schwer zu fälschen, anders als der Domainname, von dem die Nachricht zu kommen scheint; hier genügt schon ein Abgleich mit der IP-Adresse (auch wenn weitergeleitete E-Mails das größte Problem darzustellen scheinen). Die Authentifizierung per Signatur schaut sich die Nachricht selbst an und sucht nach einer Unterschrift der Herkunftsdomain. Beide Methoden funktionieren ohne menschliche Intervention. Diese Authentifizierung ist der Schlüssel für jedes Reputationssystem. Derzeit ist sie an die Ebene der Domains gekoppelt, und in der Welt der E-Mails verfügen manche IP-Adressen bereits über eindeutige Reputationen (oft sind viele von ihnen mit einer einzigen Domain verbunden), während andere über Nacht wieder verschwinden.

Wie können wir das zuverlässige Netz schaffen? Vor allem müssen die Verkäufer von IT-Produkten versuchen, ihre Kunden zu viel größerer Vorsicht zu erziehen. Sie müssen Systeme verkaufen, die serienmäßig über Sicherheitseinstellungen verfügen, selbst wenn sie dadurch zunächst schwerer abzusetzen sind und die Zahl der Anrufe bei den Supporthotlines steigt. Die Kosten der Sicherheit müssen im Vordergrund stehen. Kann man den Kunden Sicherheit vor Spam und Viren als mehrwertsteigernd vermitteln? Es wird schwer, denn Verkäufer hassen es, Sicherheitslücken in ihren Produkten einzugestehen. Aber die Kosten der Unsicherheit sind auf lange Sicht viel höher.

Aber es geht nicht nur um die Händler. Die Serviceprovider, insbesondere die Kabelfirmen, verkaufen ihre Produkte und kümmern sich kaum um einen angemessenen Support. Sie beachten nicht, welche Art von anormalem Verkehr aus ihren Maschinen quellen kann. Ein großer Teil der Spammails wird über infizierte Rechner unschuldiger, schlimmer noch: sorgloser Nutzer versandt. Die Providergesellschaften sollten zumindest ansatzweise Verantwortung dafür verspüren, wie ihre Dienste letztlich genutzt werden. Wenn sie ihre Nutzer nicht besser kontrollieren und unterstützen, könnten sie unausweichlich auf schwarze Listen von *peer*-Netzwerken gelangen.

Die vielleicht wichtigste Gruppe bei der Durchsetzung des zuverlässigen Netzes sind die Registratoren von Domainnamen, denn erst sie ermöglichen eine Identität im Internet. Dieser Markt ist hart umkämpft.[6] Doch leider verläuft der Wettbewerb von oben nach unten: Die Registrierung läuft in erster Linie über den Preis, denn kein Wert wird hinzugefügt (etwa Reputation), und die Organisation zur Regelung der technischen Infrastruktur des Internets, insbesondere der Vergabe von Internetadressen (Internet Corporation for Assigned Names and Numbers/ICANN), differenziert die Produkte nicht, die sie verkauft. Die Idee, so genannte *top level domains* (die Endung einer URL, die angibt, ob der Server in einem Land steht oder zu einer Organisation gehört) zu sponsern, um die Träger dieser besonderen Adressen mit einem wichtigen Unterscheidungsmerkmal zu versehen, konnte nicht realisiert werden. Es ginge beispielsweise darum, die neue Endung „.tra-

[5] Vgl. dazu im Einzelnen Esther Dyson, The Accountable Net: Let's Take Back Paradise!, in: Release 1.0. Esther Dyson's Monthly Report, 22 (2004) 10, insbes. S. 4–30; www.release1–0.com.

[6] Ich trage eine Mitverantwortung als Gründungsvorsitzende der Internet Corporation for Assigned Names and Numbers (ICANN).

vel“ nur solchen Organisationen zur Verfügung zu stellen, die bestimmte, harte Kriterien erfüllen – eine wirkungsvolle Werbung, die Kunden Distinktion erlaubt hätte.

Domainnamen sind der Hauptort zur Gewährung dauerhafter Identität im Internet, doch sie sind viel zu leicht erhältlich. Ursprünglich war der Domainname eine Form der Präsenz, eine Art, sich selbst auszudrücken, und ein Medium für die Freiheit der Rede und der Information. Aber das Internet ist zunehmend zu einem Medium zur Informationssammlung (und des Geldverdienens) geworden. Ein dezentraler Markt muss lokal reguliert werden; doch das Geschäft mit den Domainnamen scheint keinerlei Regulierung zu unterliegen, und es verläuft mit nur wenig Selbstzurückhaltung. Wie Jon Callas, Geschäftsführer der Verschlüsselungssoftwarefirma Pretty Good Privacy (PGP) formuliert: „Wie kommen Spammer an legale Domains? Natürlich durch die Registrierungsbehörden. Warum ziehen wir diese Personen nicht zur Rechenschaft? Ist es nicht offensichtlich, dass jemand nichts Gutes im Schilde führt, wenn er die Domainnamen ‚drugs4u0000.biz‘ bis ‚drugs4u9999.biz‘ erwirbt? Spammer lassen buchstäblich tausende von Wegwerfadressen pro Monat registrieren. Für die Domainhändler ist das ein gutes Geschäft. Sie profitieren von den Phishers. Sie sind ebenso ein Teil des Spam-/Betrugssystems, wie Geldwäscher ein Teil des Drogenkartells sind.“

ICANN wollte eine staatliche Regulierung des Internets vermeiden, indem es auf *peer-to-peer*-Regulierung setzte und nicht etwa ganz auf Regulierung verzichten wollte. Aber obwohl die meisten es wohl gerne sähen, wenn der Markt bereinigt würde, möchte niemand den ersten Schritt tun. Weil der Domainname, den beispielsweise Juan’s Noble Name Registrar verkauft, derselbe ist, den man von Alice’s Deadbeat Domains erwerben kann, kann es sich Juan nicht erlauben, sich aus dem Geschäft zurückzuziehen, weil die Domainnamen, die er verkauft, nicht sein Eigentum sind. Sie enden auf „.com“ oder „.biz“, lassen aber nicht erkennen, wo sie erworben wurden.

Kurz gesagt, das heutige System der Domainnamenvergabe eignet sich nicht für die Vision des zuverlässigen Netzes. Auch die Hoffnung, dass neue *top level domains* wie „.biz“ und „.info“ differenziert und kontrolliert verkauft werden könnten, hat sich rasch zerschlagen. Es gibt eine größere Registrierungsagentur für die „.com“ *top level domain* – VeriSign/Network Solutions –, die aber den Verkauf der Adressen nach wie vor Registratoren überlässt. Diese wiederum sind ebenfalls nicht verantwortlich: Niemand sucht sich eine Adresse oder vermeidet sie auf der Basis des Registrators, bei dem sie erworben wurde.

Das geradezu als historisch zu bezeichnende Problem liegt darin, dass Domainnamen prinzipiell allen verfügbar sein sollen. Aber vielleicht handelt es sich bei einem Domainnamen eher um ein Privileg als um ein Recht – oder zumindest um ein Recht, das auf ehrenwerte, verantwortliche Weise genutzt werden muss. Wie Mailingdienste müssen Registratoren über Mittel verfügen, um ein verlässliches Feedback über ihre Kunden zu erhalten. Und wie Mailingdienste sollten sie Kunden, deren Integrität nicht festgestellt werden kann oder in Zweifel steht, keine Dienste verkaufen, denn die Nutzer würden solche Websites nicht länger aufsuchen, ebenso wie sie Post verweigern, je nach Ruf des Mailingdienstes. Zur Zeit sind Registratoren nicht mit den Namen verbunden, die sie registrieren. Der Domainmarkt basiert auf der Voraussetzung, dass man dieselbe Domain über verschiedene Registratoren erwerben kann. Es gibt keinerlei Qualitätskontrolle.

Ob neue, differenzierte *top level domains* so etwas leisten können, ist fraglich. Aber wenn die Gemeinschaft der Domainhändler und Website- bzw. Web-Hosting-Anbieter nicht rasch von den Reputationssystemen lernt, die Mailingdienste zu nutzen beginnen, könnten sie sich bald viel drakonischeren Formen des Feedbacks gegenübersehen – der staatlichen Regulierung. Ein wirklicher, auf Reputation und Qualitätskontrolle beruhender Wettbewerb unter den *top level domains* wäre keine Patentlösung, aber er wäre ein notwendiger erster Schritt, um das Netz auszumisten. Andernfalls wird die Öffentlichkeit künftig das Internet insgesamt für die Handlungen der Übeltäter verantwortlich machen – und möglicherweise würden die Rufe nach einer staatlichen Regulierung des Internets lauter.

Matthias Spielkamp

Die Zukunft der Ideen

In der „Rheinischen Zeitung“ vom 25. Oktober 1842 machte ein Journalist seinem Unmut Luft: „Man kann unmöglich auf elegantere und zugleich einfachere Weise das Recht der Menschen vor dem Recht der jungen Bäume niederfallen lassen“, hieß es dort mit weit mehr als einem Anflug von Sarkasmus. „Auf der einen Seite nach Annahme des Paragraphen steht die Notwendigkeit, daß eine Masse Menschen ohne verbrecherische Gesinnung von dem grünen Baum der Sittlichkeit abgehauen und als Raffholz der Hölle des Verbrechens, der Infamie und des Elends zugeschleudert werden. Auf der andern Seite nach Verwerfung des Paragraphen steht die Möglichkeit der Mißhandlung einiger jungen Bäume, und es bedarf kaum der Anführung! die hölzernen Götzen siegen, und die Menschenopfer fallen!“[1] Nicht nur die hölzernen Götzen siegten, sollte man hinzufügen, sondern auch die Waldeigentümer.

Matthias Spielkamp
geb. 1970; freier Journalist mit dem Spezialgebiet Immaterialgüter (Urheberrecht, Patente, Markenschutz); Immanuelkirchstraße 38, 10405 Berlin.
spielkamp@autorenwerk.de; www.immateriblog.de.

Karl Marx nahm seine Sprachmacht zusammen, um zu zeigen, wie einmal mehr die herrschende Klasse sich Gesetze schuf, die die Welt nach ihren subjektiven Interessen strukturierte. Ort der hitzigen Auseinandersetzungen an fünf Tagen im Herbst 1842: der Landtag der Preußischen Rheinprovinz. Ihr Objekt: das Holzdiebstahlsgesetz. Warum beschäftigte sich Marx damit? Weil es dort um eine der fundamentalen Kategorien moderner Gesellschaften ging: das Eigentum.

Was ist Eigentum?

Viele, die an Eigentum denken, denken an einen Gegenstand. Dieses Auto ist mein Eigentum, dieser Apfel, dieses Haus. Juristen, Soziologen oder Philosophen denken an etwas anderes. Sie haben, wenn sie den Begriff Eigentum hören, ein Verhältnis zwischen Menschen vor Augen, durch das festgelegt wird, wer das Eigentum an einem Gegenstand für sich in Anspruch nehmen kann. Mit dem Gegenstand selbst hat das wenig zu tun – so, wie es nichts mit dem Raffholz selber zu tun hatte, wer ein Eigentumsrecht daran beanspruchen konnte.

Bis zu jenen Tagen im Jahre 1842 war es üblich, dass niemand diesen Anspruch erhob. Fiel ein Ast von einem Baum zu Boden, wurde er aufgerafft von denen, die sich Feuerholz nicht leisten konnten. Das waren viele. Wurde jemand erwischt, wenn er einen Ast abschlug – oder gar einen ganzen Baum fällte –, wurde er vor Gericht gestellt. Der Baum und seine Zweige waren Eigentum desjenigen, dem der Wald gehörte, die Zweige, die am Boden lagen, nicht. So regelte es das Gesetz. Mit einer wie auch immer gearteten „Natur der Dinge“ hatte es nichts zu tun, dass ein Zweig, der am Boden lag, anderen Regeln unterworfen war als ein Zweig, der aus dem Stamm wuchs. Was man am Ergebnis der Debatte ablesen konnte: Das Gesetz wurde verabschiedet; von nun an war es ein Verbrechen gegen das Eigentum, im Wald Holz zu raffen. Wer Geld hatte, konnte Feuerholz vom Waldeigentümer kaufen. Wer kein Geld hatte, fror. An der Tatsache, dass im Wald tote Äste von den Bäumen zu Boden fielen, hatte sich – welch Wunder – durch das Gesetz nichts geändert.

Was hat der Titel dieses Beitrags mit den toten Ästen von Marx zu tun? Eine Menge. Denn wenn es um Ideen geht, geht es auch immer um das Eigentum an ihnen. Eine Idee, die ich habe, muss mir gehören, damit ich sie wirtschaftlich verwerten kann. Nur wenn ich das kann, werde ich es mir leisten können, eine Idee zu haben. Und je vollständiger mir eine Idee gehört, desto besser kann ich sie verwerten. Die Logik, die hinter Argumenten wie diesem steht, scheint auf den ersten Blick überzeugend, weil die Idee des Privateigentums so tief in unserer Gesellschaft verwurzelt ist wie kaum eine andere. Wir wachsen auf mit einem Schnuller im Mund, der mein ist und nicht dein, bekommen einen Schul-

[1] Karl Marx, Verhandlungen des 6. Rheinischen Landtags. Debatten über das Holzdiebstahlsgesetz, in: Marx-Engels Werke, Bd. 1, Berlin (Ost) 1988[15], S. 111.

ranzen, der mir gehört, nicht dir, und am Ende denken wir, dass eine Idee, die ich habe, auch mein unbeschränktes Eigentum sein muss. Diese Logik klingt überzeugend, aber sie ist falsch.

Eigentum ist ein Verhältnis zwischen Menschen. Es ist nicht überhistorisch, nicht naturgegeben. Es wird gestaltet von den Akteuren, die die Macht haben, in Gesellschaften ihre Interessen durchzusetzen. Das Pendel schwingt hin und her zwischen ihnen; mal können sich die einen durchsetzen, mal die anderen. Es gab Zeiten, in denen es üblich war, Menschen zum Eigentum zu rechnen – eine Vorstellung, die uns heute absurd erscheint. Ebenso, wie vielen die Vorstellung absurd erschien, an etwas ein Eigentum zu haben, das sich nicht anfassen lässt. Und dass Eigentumsrechte an diesen „immateriellen" Gütern sogar umfassender sein könnten als an materiellen.

Druckerpressen und metaphysische Bänder

Wenn man einen Anfang festmachen will, könnte man den Beginn dieser Entwicklung auf das Jahr 1469 datieren. In jenem Jahr verlieh der Rat von Venedig dem Drucker Johann von Speyer das „Recht zur ausschließlichen Ausübung des Buchdrucks" im Stadtstaat. Etwa 15 Jahre zuvor hatte Johannes Gensfleisch zur Laden, besser bekannt als Gutenberg, die erste Bibel mithilfe beweglicher Lettern gedruckt. Die Gutenberg-Bibel wird heute als der Beginn eines neuen Medienzeitalters gesehen, das eine bis dahin unvorstellbare Verbreitung von Informationen ermöglichte. Es bedurfte keiner Mönche mehr, die in mühevoller, wochen- bis monatelanger Handarbeit Texte abschreiben mussten.

Doch es gab noch eine Revolution, die sich hier anbahnte und die von den meisten Zeitgenossen unbemerkt blieb: die des Rechts. Denn eine Druckerpresse kostete eine Menge Geld. Und statt sich darauf zu verlassen, dass seine Bücher beim Kunden besser ankommen als die der Konkurrenz, beantragte Johann von Speyer ein Monopol auf den Buchdruck in Venedig, um erst gar keine Konkurrenz aufkommen zu lassen – ein Ausnahmerecht, das ihm der Rat auch gewährte. Ein persönlicher – und sicher auch geschäftlicher – Erfolg für Johann, aber wahrscheinlich ahnte nicht einmal er selbst, dass dieses Ereignis noch Jahrhunderte später als Geburtsstunde des Urheberrechts angesehen würde.

Mehr als 200 Jahre lang schützten die „Druckerprivilegien" nicht die Urheber, sondern das Geschäftsmodell der Buchdrucker und -verleger. Zu Beginn des 18. Jahrhunderts war die englische Regierung die erste, die diesem Zustand eine Ende zu bereiten versuchte. Die Gründe dafür waren vielfältig: Es lag weniger daran, dass sie die Autoren davor schützen wollte, sich mit einem Honorar abspeisen lassen zu müssen, um anschließend keinerlei Rechte mehr an ihren Werken zu haben. Vielmehr hatten die Buchdrucker zuviel Macht erlangt, die sich die Krone eigentlich nicht aus der Hand nehmen lassen wollte. Also verabschiedete die englische Regierung 1710 das Statute of Anne, benannt nach der damaligen Königin Anne Stuart. Darin findet sich ein Satz, der gerade heute wieder zu erhitzten Diskussionen unter Urheberrechtsexperten führt: Das erklärte Ziel des Statuts war „Encouragement of Learned Men to Compose and Write useful Books" – also gebildete Männer zu ermutigen, nützliche Bücher zusammenzustellen und zu schreiben.[2] Das Mittel dazu war der Schutz der Autorenrechte, sodass niemand mehr einfach Bücher nehmen und ohne Zustimmung des Autoren vervielfältigen konnte. Die Rechte der Autoren an ihren Texten waren Mittel zum Zweck: Die wirtschaftliche Sicherheit der „gebildeten Männer" sollte ein Fundament für Kreativität schaffen, nach dem Motto: Wenn ich leben kann von dem, was ich gern tue, dann tue ich es noch lieber. Ökonomen nennen das die Anreiztheorie.

Auf dem europäischen Kontinent sah man das ganz anders. „Das heiligste, berechtigtste, am wenigsten anfechtbare und persönlichste allen Eigentums ist das Werk, die Früchte des Denkens eines Schriftstellers"[3], schrieb Isaac Le Chapelier 1791 in seinem „Report Le Chapelier" an das Revolutionsparlament, aus dem das erste Dekret zum Urheberrecht in Frankreich hervorging. Möglicherweise hatte er Immanuel Kants Beitrag in der „Berlinischen Monatsschrift" vom Mai 1785 gelesen, in dem der Königsberger Philosoph ein selt-

[2] Vgl. Gillian Davies, Copyright and the Public Interest, London 2002, S. 15.
[3] Zit. nach: ebd., S. 137.

sames Gedankengebäude errichtet hatte, mit dem er die „Unrechtmäßigkeit des Büchernachdrucks“ – so der Titel – zu begründen versuchte. Es folgten ihm Fichte und Hegel, wenn auch nicht in ihrer Argumentation, so doch in ihrer Schlussfolgerung: Es gibt ein Eigentum, auf immer und unveräußerlich, des Urhebers, des Autors an seinem Werk.

Seitdem halten die Kontinentaleuropäer das Urheberrecht für eine Art weltlichen Ausdruck eines metaphysischen Bandes, das Autor und Werk untrennbar verbindet – und haben darüber oft genug das Weiterlesen vergessen. Denn bei Le Chapelier heißt es auch: „Jedoch ist es ein Eigentum, das in seinem Wesen völlig verschieden ist von anderen Eigentumsarten“, denn: „Aus der Natur der Sache heraus ist alles vorbei für Autoren und Verleger, sobald die Öffentlichkeit das Werk durch seine Publikation in Besitz genommen hat.“

Private Rechte und öffentliche Interessen

Denn auch das kontinentaleuropäische Urheberrecht hat die Aufgabe, einen Ausgleich zu schaffen zwischen den Interessen der Urheber und den Interessen der Öffentlichkeit. (Was übrigens auch für das wichtigste andere Immaterialgüterrecht gilt: das Patentrecht.) Zwar kann man dort, wo ein Urheberrecht im Wortsinn gilt, niemals das vollständige Recht an seinem Werk abtreten. Denn ein metaphyisches Band lässt sich schließlich nicht mit weltlichen Verträgen zerschneiden. Doch selten geht es beim Streit ums Urheberrecht um etwas anderes als Verwertungsrechte: Wer darf meinen Text drucken, wer mein Musikstück aufführen, wer mein Foto ausstellen? Darüber bestimmen zu können, ist das Verlangen der Urheber, denn dadurch verdienen sie Geld. Und diese Verwertungsrechte lassen sich sehr wohl abtreten. Sie sind es, die seit Jahrhunderten immer stärker ausgeweitet werden, und zwar in alle Richtungen: die Dauer des Schutzes, ihr Umfang und die Anforderungen, die erfüllt sein müssen, um in den Genuss des Urheberrechtsschutzes zu kommen.

So betrug die Schutzdauer in England, verliehen durch das Statute of Anne, 14 Jahre; sie konnte auf Antrag um weitere 14 Jahre verlängert werden. In den USA galten mit dem Copyright Act von 1790 ebenfalls 14 Jahre, die um weitere 14 verlängert wurden, wenn der Autor nach Ablauf der ersten Periode noch lebte und die Verlängerung beantragte. In Deutschland wurde am 11. Juni 1837 das „Preußische Gesetz zum Schutze des Eigenthums an Werken der Wissenschaft und Kunst gegen Nachdruck und Nachbildung“ erlassen. Schutzdauer: 30 Jahre *post mortem auctoris* (nach dem Tod des Autors). In den genannten Ländern gilt heute für Werke der Kunst und Literatur – und auch für viele andere – eine Schutzdauer von 70 Jahren nach dem Tod des Autors. Hätte eine derartige Schutzdauer zu Goethes Zeiten bestanden, wäre der „Werther“, den er im Alter von 25 Jahren veröffentlichte, 152 Jahre lang geschützt gewesen. Wird Benjamin Lebert so alt wie Goethe, würde sein Roman „Crazy“ eine Schutzdauer von 161 Jahren genießen.

Auch was den Schutzumfang anbelangt, sind die aktuellen Gesetze kaum mit ihren Vorgängern zu vergleichen. Im Preußischen Gesetz von 1837 heißt es: „Das Recht, eine bereits herausgegebene Schrift, ganz oder theilweise, von neuem abdrucken oder auf irgend einem mechanischen Wege vervielfältigen zu lassen, steht nur dem Autor derselben oder denjenigen zu, welche ihre Befugniß dazu von ihm herleiten.“[14] Um den Nachdruck ging es, nicht mehr. Heute kann ein Urheber bestimmen über die Vervielfältigung, Verbreitung, Ausstellung seines Werkes, ob es zum Vortrag, zur Aufführung und Vorführung kommt, in einer Funksendung oder durch Bild- und Tonträger veröffentlicht oder öffentlich zugänglich gemacht wird – womit vor allem die Publikation über das Internet gemeint ist.

Schließlich die Anforderungen: Musste in den USA anfangs ein Schöpfer noch jedes Werk, das er schützen wollte, beim Register of Copyrights anmelden, steht heute automatisch jede E-Mail, jede Notiz, die jemand auf eine Serviette kritzelt, unter dem Schutz des Copyrights. Auch in Deutschland muss kein Werk registriert werden, um geschützt zu sein. Was den Werkbegriff anbelangt, gilt zwar nach wie vor der Grundsatz, dass nur Schutz genießt, was eine entsprechende Gestaltungshöhe vorweisen kann; die Schwelle für diese Gestaltungshöhe ist jedoch im Laufe der Zeit vom Gesetzgeber und den Gerichten

[14] Ebd., S. 383.

so weit abgesenkt worden, dass heute unvergleichbar mehr Werke Urheberrechtsschutz genießen als im 19. Jahrhundert. Doch das ist immer noch nicht alles. Um zu verstehen, wie weit der Schutz der Urheberrechte tatsächlich geht – und was das bedeutet –, muss man auch einen Ausflug machen nicht nur in die Welt des Rechts, sondern auch der Technik. Einen Ausflug, wie ihn – ungewollt – Shawn Yeager vor zwei Jahren unternahm.

Meine Musik gehört mir nicht

Der IT-Berater Yeager war von den USA nach Kanada umgezogen, als sein Apple Powerbook den Geist aufgab. Eigentlich nicht weiter schlimm, eine Neuinstallation des Betriebssystems war für den Techniker kein Problem. Doch als er seine im iTunes Music Store gekaufte Musik, die digital auf seinem Computer gespeichert war, hören wollte, machte ihm die Software einen Strich durch die Rechnung: Die Songs müssten erst wieder freigeschaltet werden, um sicherzugehen, dass Yeager der rechtmäßige Besitzer der Stücke sei, teilte ihm sein Programm mit. Als wenn das nicht ärgerlich genug gewesen wäre, erlebte Yeager die nächste Überraschung beim Telefonat mit Apples Serviceteam: Die Musik sei nur für Bewohner der Vereinigten Staaten gedacht. So stehe es in den Geschäftsbedingungen. Da Yeager nicht mehr in den USA wohne, könne er die Songs leider nicht mehr abspielen.

Womit Yeager unbeabsichtigt aneinander geraten war, nennt man in der Branche Digitales Rechtemanagement (*Digital Rights Management*, DRM). Seine Gegner finden eher den Begriff Digitales Restriktionsmanagement angemessen. Nicht ohne Grund: Jedes einzelne Musikstück aus dem Apple Store ist DRM-kodiert. Das bedeutet, dass jede Datei nicht nur Musik enthält, sondern auch Informationen darüber, wie diese Musik zu nutzen ist: Darf das Stück nur auf dem Computer abgespielt werden, auf den es beim Kauf heruntergeladen worden ist? Darf es der Käufer auf CD brennen, auf einen MP3-Player überspielen, auf seinen Laptop übertragen? Wenn ja, wie oft? Eine solche Datei kann nicht mit einem beliebigen Programm geöffnet werden, sondern nur mit solchen, die die DRM-Informationen auch interpretieren können. Erkennt etwa Apples iTunes-Software, dass ein Musikstück bereits fünfmal auf unterschiedlichen Rechnern gespeichert wurde, weigert sie sich, dies ein sechstes Mal zu tun. Als Yeager nach seinem Powerbook-Crash das Betriebssystem neu installierte, interpretierte die iTunes-Software das so, als sei die Musik auf einen neuen Rechner kopiert worden. Also forderte das Programm Yeager auf, die Songs, für die er bezahlt hatte, neu freizuschalten – und das wurde ihm verweigert, weil seine Eigentumsrechte an den Songs außerhalb der USA nicht gültig waren. Yeager musste erkennen, dass er nicht die Songs besaß, sondern lediglich etwas Neues, schwer Fassbares, Ephemeres: ein Nutzungsrecht an Musik. Dieses Nutzungsrecht, und das war die zweite, größere – und folgenreichere – Überraschung, war ihm nur unter bestimmten Bedingungen übertragen worden. Also konnte es ihm auch wieder entzogen werden, wenn es dem tatsächlichen Inhaber des Rechts gefiel – also nicht Yeager, sondern Apple. Willkommen im digitalen Zeitalter.

Shawn Yeagers Erfahrung mit dem iTunes Music Store ist wie geschaffen dafür, zu verstehen, wie DRM funktioniert. Vor noch nicht allzu langer Zeit ging man, wenn man Musik hören wollte, in ein Geschäft und kaufte eine Platte, die man dann besaß. Man konnte sie anhören, verschenken, verkaufen, an Freunde verleihen, im Schrank verstauben lassen, als Bierdeckel benutzen, zerbrechen, wegwerfen. Oder, wenn man sie im Auto hören wollte oder im Ferienhaus, wo kein Plattenspieler stand, die Musik auf eine Kassette überspielen. Das hätten die Rechteinhaber zwar gern gesetzlich verboten gesehen, aber die Regierungen weigerten sich: Es wäre unmöglich gewesen, ein solches Verbot zu kontrollieren. Und damit wäre es „ebenso effektiv gewesen wie ein Verbot des Nasebohrens“, wie es Elmar Hucko, ehemals als Ministerialdirektor im Bundesjustizministerium zuständig für das Urheberrecht, ausdrückte.[5]

Doch heute wittern die Rechteinhaber die Chance, die Rechte der Kunden zu kontrollieren. Denn die Digitalisierung der Daten ist der Albtraum, der den Managern der großen Unterhaltungskonzerne den Schlaf raubt: Jede Kopie ist so gut wie das Original, Inhalte sind nicht mehr als Nullen und Einsen, die sich

[5] Das Urheberrecht kennt kein Recht auf Privatkopie, in: c't, Nr. 16 vom 26. 7. 2004.

umso schneller an jeden Ort der Welt übertragen lassen, je höher die Bandbreite der Internetanschlüsse ist – und die wächst mit einem gewaltigen Tempo. Eigentlich ein fantastisches Mittel, um vor allem die Vertriebskosten für die nunmehr körperlosen Güter zu verringern. Keine CD muss mehr gepresst, kein Booklet gedruckt werden, kein Lastwagen muss die Ware ausliefern an Ladengeschäfte, für die Miete und Lohnkosten anfallen.

Doch das ist nur die eine Seite der Medaille. Da die Manager der großen Unterhaltungskonzerne jahrelang auf sie starrten wie das Kaninchen auf die Schlange, kamen ihnen diejenigen zuvor, die keine Rücksicht nahmen auf Unternehmensstrukturen, Hierarchien und Entscheidungsabläufe der multinationalen Großunternehmen. Stattdessen entwickelten sie Software, mit der es möglich ist, die digitalisierten Songs und Filme sekundenschnell auffind- und abrufbar zu machen. In diesen *peer-to-peer*-Tauschbörsen, in denen Nutzer direkt miteinander kommunizieren, tummeln sich seitdem Millionen von Menschen, die Milliarden von Texten und Filmen, vor allem aber Musikstücke vervielfältigen, ohne die Rechteinhaber um Erlaubnis zu fragen.

Und dagegen könne man auch nichts tun – so lautet noch immer das Credo vieler *Digerati*, Netzbürger, die mit Stewart Brand die Ansicht vertreten, dass „Information frei sein will“ und es nichts gibt, was den Geist der Digitalisierung in der Flasche halten könne.[6] Egal, welchen Schutz das Urheberrecht biete: In einer Welt digitaler Güter könne auf lange Sicht kein Mensch mehr ausgeschlossen werden von der Teilhabe an ihnen. Denn von nun an sei es möglich, Bücher, Filme, Fotos, Musik und vieles andere mehr nahezu kostenlos zu vervielfältigen und zu vertreiben. Ganz im Sinne von John Perry Barlows „Cyberspace Manifesto“, in dem er das Ende der Regierungen der industrialisierten Welt, den „müden Giganten aus Fleisch und Stahl“, ausrief, sei auch das Ende der industriellen Inhalteanbieter gekommen.[7] Wissen sei ein öffentliches Gut, von dem niemand ausgeschlossen werden könne, vor allem dann nicht, wenn alle Inhalte in unkörperlicher Form vorliegen.

Fiktion der Nicht-Ausschließbarkeit

Ein folgenschwerer Irrtum. Denn menschlicher Erfindungsreichtum kennt keine Grenzen, wenn es darum geht, diesen Status der Nicht-Ausschließbarkeit, wie ihn Ökonomen nennen, zu überwinden, indem man exklusive Eigentumsrechte zuweist.[8] Technische Möglichkeiten und Regulierungsmaßnahmen wie das Urheber- und Patentrecht wurden entwickelt, um all jene von der Nutzung von Gütern auszuschließen, die nicht dafür bezahlen – weil sie nicht wollen oder können. Denn Nicht-Ausschließbarkeit ist alles andere als ein natürliches oder technisches Charakteristikum, sondern eine soziale und rechtliche Konstruktion, die aus politischen Auseinandersetzungen und normativen Entscheidungen hervorgeht.

Im Hinblick auf die so genannten immateriellen Güter – Musik, Filme, wissenschaftliche Erkenntnis – müsste diese Einsicht weitreichende Bedeutung haben. Denn gerade die Digitalisierung bietet die Chance, ein Ausmaß an Kontrolle über die Daten zu erlangen, das in der analogen Welt unvorstellbar gewesen ist. Wie im Beispiel des iTunes Music Stores: Die Software leistet weit mehr, als nur die Musik zu entschlüsseln und damit wieder hörbar zu machen: Sie kontrolliert, welche Rechte mit den Songs verbunden sind, also was die Nutzer damit machen dürfen. Dabei ist eine große Spannbreite denkbar, von „Nur einmal abspielbar am Geburtstag des Nutzers auf seinem eigenen Computer“ bis zu „Darf auf jedem Gerät unendlich oft gespielt und auf CD gebrannt werden“. Die zweite Variante hätte allerdings wenig Sinn, denn dann könnten die Anbieter die Inhalte gleich unverschlüsselt verkaufen. Tatsächlich träumen sie aber von Modellen, bei denen Songs für nur eine Party genutzt werden können, DVDs sich nur einmal abspielen lassen (damit man sie verschicken kann und der Kunde sie nicht in die Videothek zurückbringen muss) oder Käufer ein eBook kaufen, das sie zwar lesen, aber nicht ausdrucken können.

[6] Stewart Brand wurde durch die Gründung des Online-Diskussionsforum „The Well“ zu einem der Pioniere der Internetkommunikation.

[7] Vgl. John Perry Barlow, A Declaration of the Independence of Cyberspace, http://homes.eff.org/~barlow/Declaration-Final.html (5. 6. 2005).

[8] Vgl. Elmar Altvater: What happens when public goods are privatised?, www.rosalux.de/cms/fileadmin/rls_uploads/ wemgehoertdiewelt/altvater_ 0312.pdf (31. 4. 2005).

Das Problem an dieser Methode: Ein funktionierendes DRM entwickeln heißt zu versuchen, einen Menschen davon abzuhalten, sich die eigene Geldbörse zu stehlen, indem man sie an seiner Hose festbindet – wohl wissend, dass er ein Messer in der Tasche hat. Denn der potenzielle Angreifer ist der Kunde: Er besitzt das Medium, den geschützten Text, Film, Song, dazu das Programm, das den Inhalt schützen soll, den Computer, auf dem das Programm läuft, und den Schlüssel, um den Inhalt zu öffnen. Kryptografen sind sich einig, dass es mit dem PC, wie wir ihn kennen, nie möglich sein wird, ein erfolgreiches DRM-System zu etablieren. Schließlich hat der PC seinen Erfolg der Tatsache zu verdanken, dass er eine Universalmaschine ist. Man kann auf ihm Programme schreiben oder Texte, Musik komponieren oder Filme schneiden und E-Mails verschicken. Dass sein Besitzer zu diesem Zweck auf alle Bestandteile des Rechners zugreifen kann, ist eine grundlegende Idee dieses Systems.

Für diejenigen, die diese Technik einsetzen wollen – vor allem die Unterhaltungsindustrie –, ist diese Universalität die größte Bedrohung. Denn wenn Benutzer auf alles Zugriff haben, werden sie auch jeden Schutz überwinden können. Zwar kann man DRM-Hürden bauen, die es technischen Laien unmöglich machen, den Inhalt zu entschlüsseln. Doch Experten werden diese Hürden immer überwinden. Kombiniert mit einer Erkenntnis, die in Fachkreisen BORA (*break once, run anywhere*) genannt wird, ergibt das ein eindeutiges Szenario. BORA bedeutet, dass es für den Großteil der Nutzer nicht nötig ist zu wissen, wie man einen Kopierschutz umgeht. Es genügt, wenn es ein Experte tut und den entschlüsselten Inhalt in einer Tauschbörse zur Verfügung stellt. Zu dem Schluss, dass dieser Kampf mit technischen Mitteln nicht zu gewinnen ist, kamen selbst vier hochrangige Microsoft-Ingenieure in einer Studie, die als Darknet-Paper weltbekannt geworden ist.[9]

Trusted Computing

Doch so schnell lassen sich Unternehmen nicht entmutigen, wenn es darum geht, Erlösquellen ungekannten Ausmaßes zu erschließen. Ein Teil der Strategie, die Computerbauer und Inhalteanbieter daher einschlagen, um die Inhalte dennoch zu sichern, ist der Versuch, aus dem offenen System PC ein geschlossenes System zu machen, wie einen Videorecorder oder einen CD-Player. In der Trusted Computing Group haben sich mehr als 80 Firmen zusammengeschlossen, von Microsoft und Sony über IBM und Intel bis zu Fujitsu, Siemens und Philips, um dieses Ziel zu verwirklichen. Der Plan ist, in jeden PC ein Trusted Platform Modul (TPM) einzubauen – einen Chip, der als Herzstück einer komplizierten Architektur darüber wacht, dass die Nutzer mit ihren Daten nur tun, was die Verkäufer erlauben. Die ersten Geräte nach TPM-Spezifikation sind bereits seit einigen Jahren auf dem Markt. Ronald Rivest, Informatiker am Massachusetts Instutute of Technology und Mitentwickler des weltweit bekanntesten Verschlüsselungsalgorithmus RSA (Rivest-Shamir-Adleman): „Man muss sich das so vorstellen, als würde man eine virtuelle Set-Top-Box in seinen Computer einbauen, um damit Teile seines PCs an Leute zu vermieten, denen man nicht vertraut."[10] Gemeint sind die Unterhaltungsindustrie und Computerbauer. Oder, wie es der Cambridge-Mathematiker Ross Anderson ausdrückt: „Was heißt Trusted Computing? Dass ich meinem Computer vertrauen kann? Nein, es bedeutet, dass die Industrie meinem Computer vertrauen kann."[11]

Ebenso viel Energie wie auf die Technik verwenden die großen Unterhaltungskonzerne auf das weltweite Lobbying gegenüber den Gesetzgebern. Sie haben erreicht, dass Werke einen nie gekannten Schutz genießen. Nun haben sie es gegen den Willen von Bürgerrechtsorganisationen, Wissenschaftlern und Verbraucherschützern geschafft, alle Mitglieder der World Intellectual Property Organization mithilfe des WIPO Copyright Treaty von 1996 dazu zu verpflichten, in ihre jeweiligen Landesgesetze eine Klausel aufzunehmen, die es verbietet, DRM-Systeme zu

[9] Vgl. Peter Biddle u. a., The Darknet and the Future of Content Distribution, unveröff. Diskussionspapier ohne Jahresangabe, http://msl1.mit.edu/ESD10/docs/darknet5.pdf (5. 6. 2005).

[10] „The right way to look at this is you are putting a virtual set-top box inside your PC. You are essentially renting out part of your PC to people you may not trust." Rick Merritt, Cryptographers sound warnings on Microsoft security plan, in: EETimes Online vom 15. 4. 2003, www.eetimes.com/story/OEG20030415S0013 (5. 6. 2005).

[11] Im Gespräch mit dem Autor am 14. 1. 2004.

umgehen.[12] In Deutschland wurde diese Verpflichtung mit dem novellierten Urheberrechtsgesetz vom September 2003 erfüllt. Seitdem sind auch hierzulande zahlreiche im Prinzip legale Möglichkeiten, Medien zu nutzen, untersagt.

Eine erlaubte Kopie, die gleichzeitig verboten ist – das klingt nicht nur paradox, sondern ist es auch. Möchte beispielsweise eine Hochschullehrerin ihren Studierenden eine Sammlung von Liedausschnitten als Unterrichtsmaterial auf einer CD zur Verfügung stellen, ist eine solche Nutzung eigentlich durch § 46 des Urheberrechtsgesetzes („Sammlungen für Kirchen-, Schul- oder Unterrichtsgebrauch") gestattet. Ist aber ein Musikstück, das sie für ihre Auswahl verwenden möchte, auf einer DRM-geschützten CD veröffentlicht, besagt das Umgehungsverbot, dass sie diese Beschränkung nicht aushebeln darf. Das Umgehungsverbot wiegt schwerer als die Schranke des Urheberrechts.

Eigentlich sollte das Urheberrecht nie das Ziel haben, dem Schöpfer ein absolutes, unbeschränktes „Eigentum" an seinem Werk zu verschaffen. Im Gegenteil: Immer war es auch erklärtes Ziel, einen Ausgleich zu schaffen zwischen den individuellen Bedürfnissen der Schöpfer nach Entlohnung für ihre Leistungen auf der einen und dem öffentlichen Interesse einer Gesellschaft nach Zugang zu diesen Werken auf der anderen Seite. Für Unterricht und Forschung, Rechtspflege und Presseberichterstattung oder auch den privaten Gebrauch muss es Regeln geben, die es möglich machen, Werke zu nutzen, ohne jedes Mal den Rechteinhaber um Erlaubnis bitten zu müssen.

Und jahrhundertelang schien auch dem Gesetzgeber klar zu sein: ohne Zugang zu bestehender Kreativität und bekanntem Wissen keine neuen Kunstwerke, keine neuen Erkenntnisse – all das, was Isaac Newton im Kopf hatte, als er sagte: „Wenn ich weiter sehen konnte (als andere vor mir), dann deshalb, weil ich auf den Schultern von Giganten stehe." Ein Gleichnis übrigens, das vor ihm bereits Bernhard von Chartres im 12. Jahrhundert verwendet hatte. Der wiederum bezog sich auf Marcus Annaeus Lucanus, einen römischen Dichter des 1. Jahrhunderts.

[12] Art. 11, www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html#P87_12240 (5. 6. 2005).

Doch wenn es nach dem Willen der Rechteinhaber geht, wird in Zukunft am Fuße eines jeden Giganten, sei es Goethe oder Einstein, ein Automat stehen mit der Aufschrift: „Um sich auf die Schultern zu stellen, führen Sie bitte Ihre Kreditkarte ein. Wir buchen dann den Betrag ab, den wir für angemessen halten." Ein Vorhaben, das nur gelingen kann, wenn die Gesetzgeber mitspielen; was sie auch tun, zumindest in den meisten Industrienationen. Deutschland ist dabei keine Ausnahme.

Information will frei sein – und teuer

Womit wir wieder bei Stewart Brand angelangt wären. „Information wants to be free", hatte er gesagt, und er hätte sich mit diesem Ausspruch den Vorwurf grenzenloser Naivität eingehandelt, wenn er nicht die Einschränkung dieser These gleich mitgeliefert hätte. Information will frei sein, weil es so billig geworden ist, sie zu verteilen, zu kopieren und neu zu arrangieren – zu billig, um die Kosten noch zu messen, schrieb Brand vor fast zwei Jahrzehnten. Aber Information wolle auch teuer sein, fuhr er fort, denn sie kann unermesslich wertvoll sein für den Empfänger (und damit auch für den Verkäufer). Diese Spannung werde nie verschwinden, sondern zu endlosen, verdrehten Debatten führen über Preise, Urheberrechte, „geistiges Eigentum", weil jede Runde in der Entwicklung neuer Geräte die Spannung schlimmer werden lasse.[13]

Diese Vorhersage hat sich bewahrheitet. Die Frage, welche Grenzen des Eigentums an nichtfassbaren Gütern das öffentliche Wohl gebietet, ist noch immer ungelöst. Auf der Suche nach einer Antwort vor allem die Interessen der Rechteinhaber im Blick zu haben widerspricht fundamental der Idee einer Gesellschaft, die sich als demokratisch verfasst betrachtet. Dennoch ist es genau das, was der Gesetzgeber derzeit tut. Man kann, so würde es Marx wohl ausdrücken, unmöglich auf elegantere und zugleich einfachere Weise das Recht der Menschen vor dem Recht einer DVD niederfallen lassen.

[13] Vgl. Stewart Brand, The Media Lab. Inventing the Future at MIT, Chicago 1987, S. 202.

Thomas Hoeren

Urheberrecht in der Wissensgesellschaft

Das klassische Zivilrecht, voran das Bürgerliche Gesetzbuch (BGB), ist geprägt vom Primat der Warenproduktion, entsprechend den ökonomischen Verhältnissen am Ende des 19. Jahrhunderts. Im Vordergrund steht folglich der Erwerb von Sachen im Sinne von § 90 BGB. Diese Sachen sind eigentumsfähig; sie können verkauft, vermietet, verarbeitet oder umgebildet werden. Kaum brauchbar ist das BGB aber für die Zuordnung von Informationen, dem Grundstoff der modernen Informations- und Wissensgesellschaft.[1] Informationen sind als immaterielle Güter nicht eigentumsfähig. Eine Zuordnung von Rechten an Informationen wird zwar vom Bundesgerichtshof (BGH) über das Eigentum am Datenträger vorgenommen, doch dieser Ansatz erweist sich angesichts der abnehmenden Bedeutung von Datenträgern als fragwürdig. Auch die Zuordnung über den Schutz von Informationen als „Betriebsgeheimnisse" wird immer nebulöser, da die Grenzen zwischen geheimem und nicht geheimem Wissen immer fließender werden.

Thomas Hoeren
Dr. jur., geb. 1961; Professor für Informationsrecht und Rechtsinformatik; Mitherausgeber der Zeitschrift „Multimedia und Recht". Westfälische Wilhelms-Universität Münster, Institut für Informations-, Telekommunikations- und Medienrecht, Zivilrechtliche Abteilung, Leonardo-Campus 9, 48149 Münster.
hoeren@uni-muenster.de

In dieser Situation kommt dem Immaterialgüterrecht besondere Bedeutung zu. Insbesondere das Urheberrecht ermöglicht eine klare Zuordnung von Rechten an Informationen, sofern deren Auswahl oder Anordnung eine persönlich-geistige Schöpfung beinhaltet. Damit ist zwar noch kein Ausschließlichkeitsrecht an der Information, aber ein Schutz von Informationssammlungen begründet. Jüngste Tendenzen, die auf eine Erweiterung des immaterialgüterrechtlichen Schutzes hinauslaufen, sind kritisch zu beachten. So wird parallel zum urheberrechtlichen Schutz von Software auch die Möglichkeit eines erweiterten Schutzes über das Patentrecht diskutiert. Hinzu kommt das Markenrecht, das aufgrund seiner auf Ewigkeit angelegten Schutzrichtung die Schutzfristen des Urheberrechts unterlaufen kann.

Das deutsche Urheberrechtsgesetz (UrhG) stammt von 1965 und kann schon aufgrund seines Alters nicht auf das Internet bezogen sein. Daher müssen neuere Bestimmungen, insbesondere des internationalen Urheberrechts, ergänzend hinzugenommen werden. Dabei handelt es sich vor allem um den World Copyright Treaty (WCT) und den World Performers and Producers Rights Treaty (WPPT) sowie um die Richtlinie der EU zum Urheberrecht in der Informationsgesellschaft (InfoSoc-Richtlinie). Beim WCT und beim WPPT handelt es sich um völkerrechtliche Verträge, die im Rahmen der World Intellectual Property Organization (WIPO) im Dezember 1996 ausgehandelt worden sind. Sie sehen ein weites Vervielfältigungsrecht und ein neues „right of making available to the public" vor. Der WCT trat am 6. März 2002, der WPPT zum 30. Mai 2002 in Kraft.[2]

Die Vorgaben dieser Verträge sind EU-einheitlich nach langwierigen Verhandlungen geringfügig verändert in der InfoSoc-Richtlinie umgesetzt worden.[3]. In Deutschland erfolgte die Umsetzung mit Wirkung zum 13. September 2003.[4] Nach zwei Regierungsentwürfen war es wegen Bedenken des Bundesrates[5] zur

[1] Siehe zu diesem Themenbereich Jean Nicolas Druey, Information als Gegenstand des Rechts, Zürich–Baden-Baden 1995, insbes. S. 77, sowie Helmut F. Spinner, Die Wissensordnung, Opladen 1994.

[2] Zur Implementierung siehe www.ifpi.org/site-content/library/wipo-treaties-ratification-status.pdf.

[3] Siehe dazu auch Thomas Hoeren in: Multimedia und Recht (MMR), 3 (2000), S. 515. Zur Gesetzgebungshistorie: www.parlinkom.gv.at/pd/pm/XXII/I/his/000/I00040·html. Unter www.euro-copyrights.org findet sich ein Überblick über die Umsetzung der InfoSoc-Richtlinie in den EU-Mitgliedstaaten.

[4] Bundesgesetzblatt (BGBl), Nr. 46 vom 12. 9. 2003, S. 1774; Text: www.urheberrecht.org/topic/Info-RiLi/ent/11650.pdf. In Österreich trat die Novelle zum 1. 7. 2003 in Kraft: http://bgbl.wzo.at/pdf/2003a032.pdf.

[5] Regierungsentwurf vom 16. 8. 2002, Bundesratsdrucksache (BR-Drs.) 684/02, und Entwurf eines Gesetzes zur Regelung des Urheberrechts in der Informationsgesellschaft vom 6. 11. 2002, Bundestagsdrucksache (BT-Drs.) 15/38. Siehe die Unterrichtung

Anrufung des Vermittlungsausschusses gekommen. Noch offene Fragen, insbesondere bei der Ausgestaltung der Privatkopierfreiheit, werden jetzt im Rahmen eines „Zweiten Korbs“ diskutiert. Bis zum Juni 2004 haben elf Arbeitsgruppen unter Leitung des Bundesjustizministeriums (BMJ) über die Neuerungen beraten; ein erster Referentenentwurf existiert seit September 2004.[6] Kommt es zu Neuwahlen, ist unklar, ob und mit welchem Inhalt das Gesetz das Parlament passieren wird.

Der Umgang mit dem Urheberrecht

Welche Positionen lassen sich beim Umgang mit dem Urheberrecht unter den Bedingungen der Informationsgesellschaft identifizieren? Da ist zuerst die traditionelle Auffassung, die Auffassung der Orthodoxie, stark vertreten in Frankreich. Auch in Deutschland finden sich zahlreiche Vertreter dieses Modells. Es geht vom Begriff des *geistigen Eigentums* aus; das Urheberrecht soll daher primär die Interessen des Urhebers schützen.

Die Redeweise vom geistigen Eigentum ist insofern auffällig, als bereits Ende des 19. Jahrhunderts darauf hingewiesen worden ist, wie unklar dieses Konzept ist. Denn das Urheberrecht besteht nicht nur aus eigentumsähnlichen Elementen, sondern auch aus starken persönlichkeitsrechtlichen Facetten. Die Parallele zwischen dem Eigentum an materiellen Dingen und dem an geistigen Inhalten verkennt die vielfältigen Verflechtungen und Interdependenzen, in denen das Urheberrecht in der Auseinandersetzung mit der Allgemeinheit steckt. Die Orthodoxie erklärt jedoch jede vereinbarte Schranke geistigen Eigentums zu einer Ausnahmeregelung gegenüber dem allgemeinen Grundsatz des Urheberrechtsschutzes und lehnt eine verfassungsrechtliche Verankerung der Schranken ab. Die amerikanische Juristin Jane Ginsburg erklärte mit großer Verve bei einer Tagung der Association Littéraire et Artistique Internationale (ALAI) in New York, dass die Privatkopierfreiheit keinerlei verfassungsrechtlichen Hintergrund habe. Sie sei aus „mere pragmatism“ eingeführt worden. Die Konsequenz dieses Gedankens ist der Ansatz, dass Schranken jederzeit wieder abgeschafft werden können. Ein einfacher Federstrich des Gesetzgebers sei nötig, um – ohne Rekurs auf verfassungsrechtliche Zwänge – etwa die Privatkopierfreiheit aus dem UrhG zu verbannen. Eine weitere Konsequenz liegt auf der Hand: Natürlich sind die Schranken vertraglich abdingbar (d. h. durch eine freie Vereinbarung ersetzbar). Ausnahmen werden nur bei wenigen klar konturierten Fällen zugelassen, die sämtlich durch EU-Richtlinien vorgezeichnet worden sind.

Diesem traditionellen Modell steht ein anderes gegenüber, das insbesondere in den USA großen Zuspruch gefunden hat. Wie Artikel 1, Sect. 8 der US-Verfassung von 1787 betont, dient das Urheberrecht dem Wohl der Gesellschaft. Dahinter steckt das Leitbild, dass am Anfang der Grundsatz der *Informationsfreiheit* steht. Schon historisch sei das Urheberrecht ein Produkt der Neuzeit. Bis in das 18. Jahrhundert hinein seien Informationen als „common heritage of mankind“ angesehen worden. Das Urheberrecht sei insofern eine Ausnahmeerscheinung, und nicht die Schranken, sondern der Urheberrechtsschutz selbst sei eng auszulegen. Jede Ausdehnung und Erweiterung des Schutzes durch das Urheberrecht bedürfe der Rechtfertigung und sei nur in Ausnahmefällen zulässig.

Die Schranken hätten wiederum die Aufgabe, der Gesellschaft die informationelle Freiheit zurückzugeben, über die sie im ursprünglichen Zustand verfügt habe. Die Rechtsprechung könne daher durchaus Schranken über den Wortlaut hinaus erweitern und neue „erfinden“. Die Schranken des Urheberrechts seien sogar verfassungsrechtlich abgesichert, insbesondere vor dem Hintergrund der Informations- und Meinungsfreiheit. Sie stünden daher auch nicht jederzeit zur Disposition, und es sei nicht zulässig, durch vertragliche Regelungen die Schranken zu unterlaufen. Belgien beispielsweise hat sich in der Urheberrechtsszene profiliert, indem es alle Schranken zu zwingenden Rechtsbestimmungen erklärt hat.

Zwischen diesen beiden Extrempositionen – geistiges Eigentum vs. Informationsfreiheit – gibt es einen Mittelweg: Das Balance-

des Bundestages durch den Bundesrat über die Gründe für die Anrufung des Vermittlungsausschusses (BT-Drs. 15/1066 vom 27. 5. 2003).

[6] Zusammenfassung der Ergebnisse unter www.urheberrecht.org/topic/Korb-2/bmj/707.pdf; Referentenentwurf vom 27. 9. 2004, www.urheberrecht.org/topic/Korb-2/bmj/760.pdf.

modell versteht das Urheberrecht allgemein und wertungsfrei als *Immaterialgüterrecht.* Versuche zum Schutz des geistigen Eigentums und der Bindung des Urheberrechts an die Interessen der Allgemeinheit sind gleichrangig. Keine der beiden Seiten, weder der Urheber noch der Nutzer, hat Priorität. Wie das Bundesverfassungsgericht (BVG) immer wieder betont hat, bedarf es einer solchen Balance zwischen dem Schutz des Urhebers und den verfassungsrechtlich gesicherten Interessen der Allgemeinheit. Diese erfordert praktische Konkordanz: Gesetzgeber und Rechtsprechung sind aufgefordert, beide Schutzgüter zur optimalen Entfaltung zu bringen. Daher ist nicht jede Schrankenbestimmung verfassungsrechtlich abgesichert, etwa die Zitatfreiheit oder die Presseberichterstattung. Die einzelnen Schranken müssen auf ihren verfassungsrechtlichen Kern bezogen werden. Auch muss zwischen Urhebern und Verwertern unterschieden werden.

In Deutschland weist die Tendenz seit einigen Jahren in Richtung Balancemodell. So ging es in der Entscheidung des BVG vom 29. Juni 2000 in Sachen „Germania 3 Gespenster am Toten Mann“[7] nur vordergründig um den Streit zwischen den Erben Bertolt Brechts und dem Verleger des Dramatikers Heiner Müller um die Grenzen des Zitatrechts. Das BVG ging weit über diese Spezialthematik hinaus: „(M)it der Veröffentlichung (steht) ein Werk nicht mehr allein seinem Inhaber zur Verfügung (. . .). Vielmehr tritt es bestimmungsgemäß in den gesellschaftlichen Raum und kann damit zu einem eigenständigen, das kulturelle und geistige Bild der Zeit mitbestimmenden Faktor werden. Es löst sich mit der Zeit von der privatrechtlichen Verfügbarkeit und wird geistiges und kulturelles Allgemeingut (. . .). Diese gesellschaftliche Einbindung der Kunst ist damit gleichzeitig Wirkungsvoraussetzung für sie und Ursache dafür, dass die Künstler im gewissen Maß Eingriffe in ihre Urheberrechte durch andere Künstler als Teil der sich mit dem Kunstwerk auseinandersetzenden Gesellschaft hinzunehmen haben. Zur Bestimmung des zulässigen Umfangs dieser Eingriffe dienen die Schrankenbestimmungen des Urheberrechts (§ 45 ff. UrhG), die ihrerseits wieder im Lichte der Kunstfreiheit auszulegen sind und einen Ausgleich zwischen den verschiedenen – auch verfassungsrechtlich – geschützten Interessen schaffen müssen.“

Ein weiterer Argumentationsstrang findet sich in zwei weiteren Rechtsfällen. In der Entscheidung über Kopienversanddienste[8] unter Bezugnahme auf die Sozialbindung des Eigentums hat der BGH aus Art. 9 der Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst (RBÜ) und entsprechenden Regelungen des Übereinkommens der Welthandelsorganisation über handelsbezogene Aspekte des geistigen Eigentums (TRIPS) eine neue Schranke konturiert: „Der Schutz des Urheberrechts als geistiges Eigentum durch Art. 14 GG schließt zwar Schranken des Rechts aufgrund der Sozialpflichtigkeit des Eigentums nicht aus, verlangt aber auch, dass bei der inhaltlichen Auslegung des Urheberrechts sachgerechte Maßstäbe festgelegt werden, die eine der Natur der sozialen Bedeutung des Rechts entsprechende Nutzung und angemessene Verwertung sicherstellen (. . .). Beschränkungen des Nutzungsrechts im Hinblick auf das Allgemeinwohl müssen vom geregelten Sachbereich her geboten sein und dürfen nicht weiter gehen, als der Schutzzweck reicht, dem die Regelung dient. Eine übermäßige, durch den sozialen Bezug des Urheberrechts nicht geforderte Einschränkung kann nicht mit Art. 14 Abs. 2 GG gerechtfertigt werden.“

Noch deutlicher wurde der BGH in der Entscheidung über elektronische Pressespiegel.[9] Er begrüßte es, „dass ein im Rahmen der Schrankenregelungen der §§ 45 ff. UrhG verwendeter Begriff in Folge technischer Fortentwicklungen veralten kann“. Dem müsse gegebenenfalls durch eine extensive Auslegung Rechnung getragen werden. Doch „sind neben den Interessen des Urhebers die durch die Schrankenbestimmung geschützten Interessen zu beachten und ihrem Gewicht entsprechend für die Auslegung der gesetzlichen Regelung heranzuziehen“. Der BGH begründete erstmals ausdrücklich eine „ausnahmsweise extensive Auslegung einer Schrankenbestimmung“.

[7] Vgl. Gewerblicher Rechtsschutz und Urheberrecht (GRUR), 103 (2001), S. 194.

[8] Vgl. GRUR, 101 (1999), S. 707.

[9] Vgl. Wettbewerb in Recht und Praxis (WRP), (2002) 11, S. 1296. Zu elektronischen Pressespiegeln siehe auch weiter unten.

Zuletzt ist auf eine Entscheidung meines eigenen Senats, des Urheberrechtssenats beim Oberlandesgericht (OLG) Düsseldorf, hinzuweisen. Dieser hat sehr ausführlich geprüft, inwieweit wesentliche Grundgedanken des Urheberrechts vertraglich abdingbar seien. Anders als der BGH seinerzeit in der heute wohl veralteten Entscheidung über Honorarbedingungen beim NDR hat unser Senat bekräftigt, dass eine Abdingbarkeit bei individuellen Verträgen zwar weitgehend zu bejahen sei. Im Rahmen von Allgemeinen Geschäftsbedingungen (AGB) aber seien Schrankenbestimmungen nicht einfach dispositiv (d. h. verfügbar). Vielmehr flössen sie in vollem Umfang in die Inhaltskontrolle nach § 307 BGB ein, sodass die Schrankenbestimmungen demnach AGB-fest sind.

Es ist fraglich, ob das Balancemodell die zukünftige Diskussion beherrschen wird, denn zum einen sind die Modelle eins und zwei sehr solipsistisch auf sich bezogen und kämpfen mit Vehemenz gegen das jeweils andere. Die Diskussionen um *Open Source* und die Softwarepatentierungsrichtlinie zeigen, mit welch seriöser und manchmal auch fanatischer Energie beide Seiten gegeneinander vorgehen. Als Zweites wird Brüssel eine fatale Rolle spielen: Die InfoSoc-Richtlinie zeigt, wie unreflektiert und bestechlich die EU-Kommission das europäische Urheberrecht strukturiert hat. In der Richtlinie wird undifferenziert von „exceptions“ gesprochen. Man vermisst im gesamten Text auch nur einen Hauch von urheberrechtlicher Dogmatik, Reflexion oder Systematik, was die Schranken angeht. Es steht zu befürchten, dass Bemühungen um eine wissenschaftliche Klärung der Urheberrechtsfragen in Brüssel nicht gehört werden; die Kommission lässt sich offenbar lieber von der International Federation of the Phonographic Industry (IFPI) bedienen. Diese Tendenz zeigt sich bei Art. 6 Abs. 4 der InfoSoc-Richtlinie: Die dortigen Regelungen zur Absicherung der Schranken gegenüber übermächtigen Digital Rights Management Systems (DRM) sind technisch so ineffizient, dass jede Diskussion angesichts der Übermacht von DRM obsolet zu werden droht.

Internet und nationales Recht

Die Informationsindustrie ist ein international ausgerichteter Wirtschaftssektor. Informationen sind ihrer Natur nach ubiquitär; sie können ohne hohen Kostenaufwand reproduziert und in Bruchteilen von Sekunden über internationale Datennetze transferiert werden. Gerade Phänomene wie die Satellitenübertragung oder das Internet zeigen, dass nationale Grenzen keine besondere Bedeutung mehr haben. Es stellt sich die Frage, ob und wann das deutsche Urheberrecht bei Informationsprodukten überhaupt zur Anwendung kommt.

Das anwendbare Recht kann (scheinbar) vertraglich durch eine Rechtswahlklausel geregelt werden: Die Parteien vereinbaren die Anwendung einer bestimmten Urheberrechtsordnung auf ihre Rechtsbeziehungen. Nach Art. 27, 28 Einführungsgesetz zum BGB (EGBGB) unterliegt ein Vertrag vorrangig dem von den Parteien gewählten Recht. Das deutsche UrhG enthält jedoch zwingende Regelungen zu Gunsten des Urhebers, die durch eine Rechtswahlklausel nicht ausgehebelt werden können.[10] Hierzu zählen Urheberpersönlichkeitsrechte, der Zweckübertragungsgrundsatz, die Unwirksamkeit der Einräumung von Nutzungsrechten nach § 31 IV UrhG, die Regelungen zur angemessenen Vergütung von Urhebern und zur weiteren Beteiligung bei einem besonders erfolgreichen Werk (§ 32 UrhG) sowie das Rückrufrecht wegen gewandelter Überzeugung (§ 41 UrhG). Ferner gilt eine Rechtswahlklausel von vornherein nicht für das Verfügungsgeschäft, also die rechtliche Beurteilung der Übertragung von Nutzungsrechten.[11] Das UrhG findet folglich auch dann Anwendung, wenn geschützte Inhalte, die auf einem Server im Ausland abgelegt sind, in Deutschland zugänglich gemacht werden.[12]

Darüber hinaus ist zu beachten, dass allein das gewählte Recht für die vertraglichen Rechtsbeziehungen entscheidend ist. So werden die häufig auftretenden deliktischen (d. h. schuldhaft gesetzwidrigen) Rechtsfragen nicht dem gewählten Vertragsstatut unter-

[10] Vgl. hierzu Thomas Hoeren/Dorothee Thum, Internet und IPR – Kollisionsrechtliche Anknüpfungen in internationalen Datennetzen, in: Robert Dittrich (Hrsg.), Beiträge zum Urheberrecht V, Wien 1997, S. 78 – 98.

[11] Siehe auch BGH, Urteil vom 2. 10. 1997, in: MMR, 1 (1998), S. 35.

[12] Vgl. LG Hamburg, Urteil vom 5. 9. 2003, 308 O 449/03.

stellt, sondern nach dem Deliktstatut beurteilt. Wenngleich also umstritten ist, ob bei Urheberrechtsverletzungen auf die 1999 eingefügte Tatortregel des Art. 40 I EGBGB zurückgegriffen werden kann oder ob die Ausweichklausel des Art. 41 zur Anwendung gelangt,[13] gilt hier, dem geistigen Eigentum Rechnung tragend, nach allgemeiner Meinung das Schutzlandprinzip.[14] Anwendbar ist demnach das Recht des Staates, für dessen Gebiet Schutz gesucht wird, die *lex loci protectionis*.[15] Nach ihr richten sich, anders als bei der Verletzung von Sacheigentum, bei der Verletzung von Immaterialgüterrechten auch die kollisionsrechtlichen Vorfragen.[16] Hierzu zählen die Entstehung des Urheberrechts,[17] die erste Inhaberschaft am Urheberrecht und die Frage, ob und welche urheberrechtlichen Befugnisse übertragbar sind.[18]

Die Geltung des Schutzlandprinzips bereitet den Rechteverwertern im Internetbereich große Probleme. Diejenigen, die sich rechtmäßig verhalten wollen, müssen ihre Internetauftritte nach den Urheberrechtsordnungen all derjeniger Staaten ausrichten, in denen ihr Angebot abrufbar ist, da jeder dieser Staaten potenziell als Schutzland in Betracht kommt.[19] Damit würde aber jeder Internetauftritt zu einem rechtlich unmöglichen Unterfangen; denn zu einer effektiven Kontrolle seiner Rechtmäßigkeit müssten alle weltweit bekannten Urheberrechtsordnungen (technisch gesehen: alle Rechtsordnungen der Welt) berücksichtigt werden.

Elektronische Pressespiegel

Unter dem Gesichtspunkt des freien Informationszugangs regelt § 49 UrhG den uneingeschränkten Zugriff auf Beiträge vor allem aus der Tagespresse. Erst die Rechtsprechung hat aus dieser Bestimmung die „Pressespiegelbestimmung“ gemacht.[20] Interessant ist vor allem der Bereich der elektronischen Pressespiegel. Nach § 49 UrhG ist die Vervielfältigung und Verbreitung einzelner Artikel aus Zeitungen in anderen „Zeitungen und Informationsblättern“ sowie deren öffentliche Wiedergabe zulässig, sofern die Artikel politische, wirtschaftliche oder religiöse Tagesfragen betreffen und nicht mit einem Rechtsvorbehalt versehen sind. Fraglich ist, ob bei der Erstellung einer Pressespiegeldatenbank, die beispielsweise in einem Großunternehmen genutzt wird, diese von § 49 UrhG umfasst wäre, denn es ist, wie erläutert, nur die Verbreitung von Informationsblättern gestattet, die dem Tagesinteresse dienen. Es erscheint aber nicht wahrscheinlich, dass elektronische Pressespiegel tatsächlich nur für einen Tag benutzt und dann vernichtet oder unabhängig von den jeweils anderen tagesaktuellen Pressespiegeln aufbewahrt werden. Vielmehr wird eine Datenbank entstehen, die jederzeit, mit Suchfunktionen versehen, verfügbar wäre. Das Erfordernis der „Tagesinteressen“ wäre damit nicht mehr gegeben.[21]

Beim übernehmenden Medium muss es sich ebenfalls um „Zeitungen und Informationsblätter“ handeln. Abwegig erscheint die teilweise vertretene Ansicht, dass auch der selektive Ausdruck von gescannten Zeitungsartikeln aus einer zentralen Datenbank heraus unter § 49 UrhG falle.[22] Der Benutzer einer

[13] Vgl. hierzu Rolf Sack, Das internationale Wettbewerbs- und Immaterialgüterrecht, in: WRP, (2000) 3, S. 269 ff.

[14] Vgl. Entscheidungen des Reichsgerichts in Zivilsachen (RGZ), 129, 385, 388; BGH, Urteil vom 17. 6. 1989, vgl. dazu Entscheidungen des BGH in Zivilsachen (BGHZ), 118, 394, 397 f.; BGH, Urteil vom 2. 10. 1987, vgl. dazu BGHZ 126, 252, 255; BGHZ 136, 380, 385 f.; vgl. auch Julius von Staudinger/Bernd von Hoffmann, Kommentar zum BGB mit Einführungsgesetz und Nebengesetzen, Berlin 1998, Art. 38 EGBGB, Rdnr. 574.

[15] Vgl. R. Sack (Anm. 13), S. 269 f.

[16] Seit langem schon anderer Ansicht ist Haimo Schack, zuletzt in: MMR, 3 (2000), S. 59 und 63 f.

[17] So auch BGHZ 49, 331, 334 f.; vgl. dazu Praxis des Internationalen Privat- und Verfahrensrechts (IPRax), (1983), S. 178; OLG Frankfurt, in: Betriebs-Berater (BB), (1983), S. 1745; OLG München, in: GRUR, Internationaler Teil (Int.), (1990), S. 75.

[18] BGH, Urteil vom 2. 10. 1997 – I ZR 88/95, vgl. dazu MMR, 1 (1998), S. 35, Spielbankaffäre mit Anm. Schricker. Ähnlich auch LG Hamburg, Urteil vom 4. 9. 2001, vgl. dazu Neue Juristische Wochenschrift (NJW), 55 (2002), S. 623.

[19] Zu den Haftungsproblemen siehe allgemein Decker, in: MMR, 2 (1999), S. 7, und Arthur Waldenberger, Zur zivilrechtlichen Verantwortlichkeit für Urheberrechtsverletzungen im Internet, in: Zeitschrift für Urheber- und Medienrecht (ZUM), 41 (1997), S. 176.

[20] Gegen die Anwendung von § 49 Abs. 1 auf Pressespiegel vgl. Beiner, in: MMR, 2 (1999), S. 691, 695.

[21] Die Abgrenzung ist fließend, vgl. Georg Wallraf, Elektronische Pressespiegel aus der Sicht der Verlage, in: Zeitschrift für Medien- und Kommunikationsrecht (AfP), 30 (2000), S. 23–29.

[22] So Horst Eidenmüller, Elektronischer Pressespiegel, in: Computer und Recht (CR), 7 (1992), S. 321, 323.

Datenbank stellt sich doch eben nicht sein eigenes „Informationsblatt“ zusammen; der Verteilung von Kopien an Dritte geht keine vorherige Zusammenfassung in einem zentralen Primärmedium voraus. Wie Ulrich Loewenheim zu Recht feststellt,[23] fehlt es bei solchen Informationsdatenbanken daran, dass der Betreiber von sich aus und im eigenen Interesse informieren will. Der BGH hat eine Anwendung des § 49 Abs. 1 UrhG auf elektronisch übermittelte Pressespiegel für möglich erachtet.[24] Entscheidend sei, dass der Pressespiegel nach Funktion und Nutzungspotenzial im Wesentlichen einem herkömmlichen Pressespiegel entspricht. Dies setze voraus, dass der elektronische Pressespiegel nur betriebs- oder behördenintern und nur in einer Form zugänglich gemacht wird, die sich im Falle der Speicherung nicht zur Volltextrecherche eigne.

Zeitungsverleger haben die Pressemonitor Deutschland GmbH & Co. KG (PMG) gegründet, die ihre Pressespiegelrechte bündeln soll. Die PMG bietet elektronische Artikel und/oder Lizenzen von derzeit 410 Quellen aus 128 Verlagen für die Erstellung elektronischer Pressespiegel an. Strittig war lange Zeit, ob diese Organisation nicht ihrerseits als Verwertungsgesellschaft anzusehen ist, sodass eine Erlaubnis des Deutschen Patent- und Markenamtes (DPMA) eingeholt werden müsste.[25] Das Problem hat sich dadurch entschärft, dass die PMG seit kurzem zusammen mit der Verwertungsgesellschaft (VG) Wort im Bereich der Pressespiegelvergütung tätig ist. Die Auswirkungen der BGH-Entscheidung auf die Pressemonitoraktivitäten sind noch unklar. Ebenso zu klären ist, inwieweit die Rechtsprechung mit den Vorgaben der InfoSoc-Richtlinie kompatibel ist, die ausdrücklich keine Schranke zugunsten elektronischer Pressespiegel enthält.

[23] Vgl. Ulrich Loewenheim, Urheberrechtliche Grenzen der Verwendung geschützter Werke in Datenbanken, Stuttgart 1994, S. 76.

[24] Urteil vom 11. 7. 2002; vgl. dazu MMR, 5 (2002), S. 739, mit Anm. Thomas Hoeren und Arthur Waldenberger; CR, 17 (2002), S. 827, mit Bespr. Niemann, S. 817; Recht der Datenverarbeitung (RDV), 18 (2002), S. 306.

[25] Siehe zu den Rechtsauseinandersetzungen Bayerischer Verwaltungsgerichtshof, Beschluss vom 14. 3. 2002; vgl. dazu AfP, 32 (2002), S. 173 (nicht rkr.) zur Frage, ob und mit welchem Inhalt das DPMA über eine Untersagungsverfügung für Pressemonitore Pressemitteilungen herausgeben darf.

Elektronische Seminarapparate

Eine Schrankenregelung zugunsten von Unterricht, Wissenschaft und Forschung sieht der 2003 eingeführte § 52a UrhG vor. Durch diese Regelung soll die Nutzung von Werken im Rahmen kleiner Forschungs- und Lehrintranets verbotsfrei und gegen Pauschalvergütung zulässig sein. Diese Vorschrift erlaubt das zustimmungsfreie öffentliche Zugänglichmachen veröffentlichter kleiner Teile eines Werks, von Werken geringen Umfangs sowie einzelner Zeitungs- und Zeitschriftenbeiträge zur Veranschaulichung im Schul- und Hochschulunterricht für einen „bestimmt abgegrenzten Kreis“ von Unterrichtsteilnehmern oder von Personen für deren eigene wissenschaftliche Forschung.

Dabei muss die Zugänglichmachung zu dem jeweiligen Zweck geboten und zur Verfolgung nicht kommerzieller Zwecke gerechtfertigt sein. Nach § 52a UrhG fallen Filmwerke erst zwei Jahre nach Beginn der üblichen regulären Auswertung in Filmtheatern unter diese Schranke. Auch die mit der öffentlichen Zugänglichmachung im Zusammenhang stehenden Vervielfältigungen (z. B. Drucken, Speichern) sind von der Regelung umfasst, es ist jedoch eine Vergütung an die jeweiligen Verwertungsgesellschaften zu entrichten. Während bei Unterrichtszwecken der abgegrenzte Personenkreis durch die Unterrichtsteilnehmer hinreichend bestimmt ist, fragt sich, was unter einem „bestimmt abgegrenzten Personenkreis“ bei der Zugänglichmachung für Forschungszwecke zu verstehen ist. Eine offene Forschergruppe mit wechselnden Mitgliedern wird nicht gemeint sein. Die Mitglieder müssen sich dem Personenkreis vielmehr eindeutig zuordnen lassen, z. B. als Mitarbeiter eines Forschungsinstituts oder verschiedenster Einrichtungen, die in einem Team zusammenarbeiten.

Zugunsten des Personenkreises erlaubt die Vorschrift das Einstellen von urheberrechtlich geschützten Materialien in ein Newsboard oder eine Mailingliste. Dabei sind immer Quelle und Name des Urhebers anzugeben (§ 63 UrhG). Vorsicht ist geboten beim Einstellen ganzer oder wesentlicher Teile von Datenbanken (i. S. d. §§ 87a ff. UrhG) oder von Computerprogrammen (§§ 69a ff. UrhG). Diese Schutzgegenstände

unterliegen eigenen, sehr engen Schrankenregelungen; § 52a UrhG findet auf sie keine Anwendung.

Weitere Probleme bereitet die Filmauswertung im Rahmen von Intranets. Zu Unterrichts- und Forschungszwecken wird meist auf Dokumentarfilme zurückgegriffen. Bei diesem Genre fehlt es aber meist an der in § 52a vorausgesetzten „üblichen regulären Auswertung in Filmtheatern". Das Gesetz ist einseitig auf den Spielfilm bezogen. Insofern käme mangels Kinoauswertung eine Verwendung von Dokumentarfilmen im Rahmen von § 52a überhaupt nicht in Betracht. Denkbar ist allenfalls eine analoge Anwendung des Paragraphen auf die Fernsehauswertung oder die übliche Nutzung bei Filmfestivals; doch diese Auslegung geht über den (eng auszulegenden) Wortlaut der Vorschrift hinaus. Im Übrigen kann davon ausgegangen werden, dass dem Gesetzgeber die Besonderheiten des Dokumentarfilmmarktes nicht unbekannt waren, sodass es sich hierbei auch um eine bewusste Entscheidung zu Gunsten des Dokumentarfilms und gegen dessen Intranetverwendung handeln kann. Der § 52a UrhG soll nur befristet, bis Ende 2006 gelten. Eine solche Vorschrift mit Verfallsdatum ist ein gesetzgebungstechnisches Novum. Für Medienzentren an Universitäten ist es daher schwierig, diese Schranke wirklich zu nutzen, denn der Aufbau einer entsprechenden Intranetstruktur zieht sich naturgemäß über einige Jahre hin. Insofern könnte das „Geschenk an Forschung und Lehre" gerade dann obsolet werden, wenn es am dringendsten benötigt wird.

Im Rahmen der Novellierung des UrhG beim Zweiten Korb[26] wird überlegt, einen neuen § 52b in das Gesetz aufzunehmen. Dieser soll die Wiedergabe von Werken an elektronischen Leseplätzen in öffentlichen Bibliotheken regeln. Es soll zulässig sein, veröffentlichte Werke aus Bibliotheksbeständen in den Räumen öffentlich zugänglicher Bibliotheken an eigens dafür eingerichteten elektronischen Leseplätzen zur Forschung und für private Studien zugänglich zu machen, soweit dem keine vertraglichen Regelungen entgegenstehen. Es dürfen dann allerdings nicht mehr Exemplare eines Werkes an den eingerichteten elektronischen Leseplätzen gleichzeitig zugänglich gemacht werden, als der Bestand der Bibliothek umfasst. Für die Zugänglichmachung wäre eine angemessene Vergütung an eine Verwertungsgesellschaft zu zahlen. Dieser Regelungsvorschlag übernimmt Ideen aus der InfoSoc-Richtlinie. Allerdings wird von Bibliotheken und Wissenschaftsorganisationen die Enge der Vorschrift kritisiert. In der Tat ist die Beschränkung auf die im Bestand der Bibliothek befindlichen Exemplare kontraproduktiv, denn Sinn und Zweck eines elektronischen Lesezugriffs werden dadurch konterkariert.

[26] Referentenentwurf für ein Zweites Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft vom 27. 9. 2004; www.urheberrecht.org.

Privatkopien

Die Magna Charta der gesetzlichen Lizenzen findet sich in Form von § 53 UrhG, der weitgehend Vervielfältigungen zum eigenen Gebrauch auch ohne Zustimmung der Rechteinhaber zulässt. Kompensatorisch erhält der Urheber für den Rechteverlust einen Anspruch auf Vergütung (§§ 54, 54a UrhG), der seit 1985 hauptsächlich auf einen Anteil an der Geräte- und Leerkassettenabgabe gerichtet ist.[27] Nach § 53 UrhG ist es zulässig, einzelne Vervielfältigungsstücke eines Werkes zum privaten Gebrauch herzustellen oder herstellen zu lassen. Bei der Übertragung von Werken auf Bild- und Tonträger sowie bei der Vervielfältigung von Werken der Bildenden Künste ist die Herstellung durch andere aber nur zulässig, wenn sie unentgeltlich erfolgt.

Jedermann kann sich im Internet via File Transfer Protocol (FTP) und unter Berufung auf privaten Gebrauch fremdes Material herunterladen und kopieren. Er kann sich auch von Bibliotheken und Dokumentationsstellen Material kopieren und via Internet zusenden lassen, vorausgesetzt, dass diese Herstellung von Kopien durch andere unentgeltlich geschieht. Anderes gilt jedoch für die Verwendung von Datenbankwerken und Datenbanken, da deren Vervielfältigung – selbst zum Laden in den Arbeitsspeicher und auch zum Privatgebrauch – genehmigungspflichtig ist.[28] Eine Differenzierung nach der verwendeten Technik (analog oder digital) findet

[27] Zur Vorgeschichte siehe Kreile, in: ZUM, (1985), S. 609; Melichar, in: ZUM, (1987), S. 51; Nordemann, in: GRUR, 87 (1985), S. 837.

[28] OLG Hamburg, Urteil vom 22. 2. 2001; vgl. dazu ZUM, (2001), S. 512; MMR, 4 (2001), S. 533; CR, 16 (2001), S. 704, mit Anm. Dieselhorst.

nicht statt; die Privatkopierfreiheit umfasst auch digitale Kopien. Nicht erfasst hingegen ist die Erstellung von Kopien zu erwerbswirtschaftlichen Zwecken. Auch können nach herrschender Auffassung[29] nur natürliche Personen in den Genuss der Regelung kommen; damit scheidet eine Berufung auf diese Vorschrift für betriebsinterne Zwecke eines Unternehmens aus.

Strittig ist, inwieweit das Kopieren von Werken nur zulässig ist, wenn eine erlaubterweise hergestellte Vervielfältigung als Vorlage benutzt worden ist. Im Zusammenhang mit der Internettauschbörse Napster[30] wurde zum Beispiel die Auffassung vertreten, dass dieses Kriterium nach dem Wortlaut des § 53 UrhG nicht vorausgesetzt sei.[31] Die Gesetzesbestimmung sah in ihrer alten Fassung keinen Hinweis darauf vor, dass die Vorlage für die Kopie ihrerseits rechtmäßig erstellt sein müsste. Dieses Schweigen wurde dahingehend interpretiert, dass die Nutzung von P2P(*peer-to-peer*)-Diensten wie Kazaa zu privaten Kopierzwecken urheberrechtlich zulässig ist. Dies störte bei der letzten Novellierung des Gesetzes den Bundesrat, der in seiner Entschließung[32] die Reichweite der Privatkopierfreiheit auf Kopien von legal hergestellten Vorlagen beschränken will. Dieser Vorschlag wurde im Vermittlungsausschuss abgelehnt.

Erstaunlicherweise kam es in letzter Minute doch noch zu einer Änderung des § 53 Abs. 1 UrhG: So wurde kurzerhand verankert, dass die Privatkopierfreiheit ausnahmsweise nicht zum Tragen kommt, wenn zur Vervielfältigung „eine offensichtlich rechtswidrig hergestellte Vorlage" verwendet wird. Der Begriff ist neu und unkonturiert. Es bleibt unklar, auf welche Rechtsordnung hinsichtlich der Feststellung einer „offensichtlichen Rechtswidrigkeit" abzustellen ist. Insgesamt handelt es sich um einen Pyrrhussieg der Musikindustrie, denn vor der Novellierung konnte sie behaupten, dass die Privatkopierfreiheit eine rechtmäßige Vorlage voraussetze; jetzt ist dieser Einwand auf offensichtlich rechtswidrige Vorlagen beschränkt. Es sei darauf hingewiesen, dass P2P-Dienste nicht offensichtlich rechtswidrige Kanäle sind, sondern in vielfältiger Weise zu legalen Zwecken, etwa im Bereich der Wissenschaft, genutzt werden.

Weiter wird die Möglichkeit der Herstellung von Vervielfältigungen durch Dritte beibehalten, sofern dies unentgeltlich geschieht oder es sich um reprografische oder ähnliche Vervielfältigungen handelt. Die vorgeschlagene Regelung gewährleistet weiterhin, dass ein Versand von Kopien möglich bleibt. Als unentgeltlich im Sinne dieser Vorschrift sollen Vervielfältigungen auch dann anzusehen sein, wenn sie z. B. durch Bibliotheken gefertigt werden, die Gebühren oder Entgelte für die Ausleihe erheben, soweit die Kostendeckung nicht überschritten wird.

Die Reichweite von § 53 Abs. 1 UrhG wird aber durch die Neueinfügung des § 95b konterkariert. Sofern der Rechteinhaber technische Schutzmaßnahmen verwendet, sind öffentliche Multiplikatoren (wie z. B. Schulen oder Universitäten) geschützt, private Nutzer aber nicht. Aus dem Fehlen von § 53 Abs. 1 in § 95b Abs. 1 lässt sich also schließen, dass der Rechteinhaber nur technische Sperrmechanismen einsetzen muss, um § 53 Abs. 1 UrhG zu umgehen. Dieser „Trick" ist unerträglich. Dass das BMJ einer solchen Strategie rechtlichen Schutz gewähren will, ist ein Zugeständnis an die Musikindustrie. Es ist bedenklich, dass die Privatkopierfreiheit in § 95b Abs. 1 nicht genannt wird.[33] Denn damit ist die Regelung des § 53 UrhG ein zahnloser Tiger. Die Industrie kann privaten Nutzern das, was § 53 Abs. 1 UrhG ihnen bietet, durch den Einsatz technischer Schutzmechanismen wieder nehmen. Das BMJ erklärt auch nicht, warum die in Art. 6 Abs. 4 der InfoSoc-Richtlinie bestehende Option zugunsten privater Nutzer nicht ausgeschöpft wird. Dieses Geschenk für

[29] So am deutlichsten Norbert Flechsig, in: NJW, 38 (1985), 44 (1991), 47 (1994). Ähnlich auch Gerhard Schricker, Urheberrecht, Kommentar, München 1999, § 53 Rdnr. 7, mit weiteren Nachweisen.

[30] Siehe dazu A&M Records Inc v. Napster Inc, 114 F. Supp. 2d 896, in: GRUR Int., (2000), S. 1066, sowie die Entscheidung des US Court of Appeals for the Ninth Circuit vom 12. 2. 2001, in: GRUR Int., (2001), S. 355.

[31] So etwa Haimo Schack, Urheber- und Urhebervertragsrecht, Tübingen 2004[2], Rdnr. 496; Mönkemöller, in: GRUR, 102 (2000), S. 663, 667 f.; anderer Ansicht Leupold/Demisch, in: ZUM, (2000), S. 379, 383 ff.; Ulrich Loewenheim, in: G. Britz u. a. (Hrsg.), Grundfragen staatlichen Strafens. Festschrift für Heinz Müller-Dietz, München 2001, S. 415 ff.

[32] BT-Drs. 15/1066 vom 27. 5. 2003, S. 2.

[33] So auch Holznagel/Brüggemann, in: MMR, 6 (2003), S. 767 ff. Siehe auch Thomas Hoeren, Urheberrecht und Verbraucherschutz, Münster 2003.

die Musikindustrie geht an den verfassungsrechtlichen Vorgaben (Unverletzlichkeit der Wohnung; Informationsfreiheit) vorbei. Art. 6 Abs. 4 der InfoSoc-Richtlinie ist ein mühevoll errungener Kompromiss zu Gunsten privater Nutzer, der unbedingt der Umsetzung bedarf. Dem können nicht die Vorbehalte der Musikindustrie gegen die Gefahr des Hacking und unkontrollierten CD-Brennens entgegengehalten werden. Es bleiben hinreichende technische Möglichkeiten, die Zahl der Privatkopien technisch zu beschränken; im Übrigen erhält die Musikindustrie über die Geräte- und Leerkassettenabgabe eine nicht unbeträchtliche Kompensation. Man könnte allenfalls darüber nachdenken, diese Kompensation zu erhöhen.

Die Schutzlücke kann auch nicht dadurch kompensiert werden, dass das Umgehen technischer Maßnahmen zum eigenen privaten Gebrauch strafrechtlich freigestellt wird (§ 108b Abs. 1). Denn zivilrechtliche Sanktionen bleiben bestehen und können für den Betroffenen sehr hart sein. Auch entsteht in der Öffentlichkeit der Eindruck, dass das Umgehen von Schutzmechanismen zur Erstellung privater Kopien strikt verboten sei, was aber angesichts der Regelung des § 53 Abs. 1 UrhG nicht zutrifft. Man fragt sich, worin der Unrechtsgehalt des Umgehens zu privaten Zwecken besteht, ist doch das Einfügen technischer Sperren in diesem Bereich das eigentliche Unrecht.

Kopienversanddienste

In jüngster Zeit wurde um die Zulässigkeit von Kopierdiensten gerungen, die von größeren Bibliotheken und Unternehmen angeboten werden.[34] Der BGH hat in zwei Verfahren gegen kommerzielle Recherchedienste entschieden, dass das Angebot von Recherche und Erstellung von Kopien aus einer Hand nicht von den Schranken des Urheberrechts gedeckt sei. Die Klagen richteten sich jeweils gegen die CB-Infobank, die angeboten hatte, aus ihrem umfangreichen Pressearchiv Rechercheaufträge zu erfüllen und Kopien gleich mit anzufertigen. Dabei berief sie sich in erster Linie auf § 53 Abs. 2 UrhG. Die Vorinstanzen hatten voneinander abweichende Urteile erlassen. Der BGH hat klargestellt, dass bei einem Recherche- und Kopierauftrag das UrhG nicht zur Anwendung komme, weil die Kopiertätigkeit der Informationsstelle nicht für den Auftraggeber, sondern in eigener Sache geschehe. Die Bank könne sich deshalb nicht auf eine Privilegierung berufen. Der Kunde andererseits, der sich auf die Schranke hätte berufen können, habe weder kopiert noch kopieren lassen.[35]

Bei öffentlichen Bibliotheken und sonstigen der Öffentlichkeit zugänglichen Einrichtungen unterscheidet sich die Rechtslage von der kommerzieller Informationsdienste. Dies gilt insbesondere, wenn auch die Recherche- und Auswahlleistung beim Besteller liegt. In einer spektakulären Grundsatzentscheidung[36] hat der BGH entschieden, dass solche Einrichtungen weder in das Vervielfältigungs- noch in das Verbreitungsrecht des Urhebers eingreifen, wenn sie auf eine Einzelbestellung hin Vervielfältigungen einzelner Zeitschriftenbeiträge anfertigen und im Wege des Post- oder Faxversandes übermitteln. In einem solchen Fall sei aber in rechtsanaloger Anwendung von §§ 27 Abs. 2 und 3, 49 Abs. 1, 54a Abs. 2 und 54h Abs. 1 UrhG ein Anspruch des Urhebers auf angemessene Vergütung zuzuerkennen, der nur durch eine Verwertungsgesellschaft geltend gemacht werden könne. Die Anerkennung eines solchen Anspruchs sei angesichts der technischen und wirtschaftlichen Entwicklung geboten, um den Anforderungen des Art. 9 RBÜ, der Art. 9 und 13 des TRIPS-Übereinkommens, der Eigentumsgarantie des Art. 14 GG sowie dem urheberrechtlichen Beteiligungsgrundsatz Rechnung zu tragen. Vor diesem Hintergrund sei eine analoge Anwendung aller Regelungen im UrhG, in denen einem Rechte-

[34] Diese Problematik ist der Hintergrund für das Gutachten, das Ulrich Loewenheim im Auftrag der Zeitungsverlegerverbände erstellt hat; siehe ders., Urheberrechtliche Grenzen der Verwendung geschützter Werke in Datenbanken, Stuttgart 1994.

[35] Vgl. dazu Zeitschrift für Wirtschafts- und Bankrecht (WM), (1997), S. 731, CB-Infobank I, sowie ebd., S. 738, CB-Infobank II. Ähnlich auch LG Frankfurt, Urteil vom 25. 10. 2001, vgl. dazu AfP, 31 (2001), S. 526; MMR, 5 (2002), S. 488 für elektronische Pressespiegel.

[36] BGH, Urteil vom 25. 2. 1999 – I ZR 118/96, vgl. dazu Kommunikation & Recht (K&R), (1999), S. 413. Gegen das Urteil haben beide Parteien Verfassungsbeschwerde eingelegt. Vgl. auch die (gegensätzlichen) Anmerkungen zu diesem Urteil von Thomas Hoeren, in: MMR, 2 (1999), S. 665, und Ulrich Loewenheim, in: ZUM, 43 (1999), S. 574.

inhaber im Bereich der Schranken Vergütungsansprüche zugebilligt werden, geboten.

Ausführlich nimmt der BGH auf die Möglichkeiten des Internets und des Zugriffs auf Datenbanken (im Sinne von Onlinekatalogen und hinsichtlich der dadurch wesentlich erleichterten und erweiterten Recherchemethoden) Bezug. Offen bleibt, ob der BGH nur den Kopienversand per Post und Fax ausnehmen will oder ob die Entscheidungsgründe auch auf den Onlineversand (der nicht Gegenstand des Verfahrens war) übertragen werden können. Nach Auffassung des OLG Köln fällt ein Internetsuchdienst, durch den man Zeitungsartikel mittels Deep-Links auffinden kann, unter § 53 Abs. 2 UrhG.[37] Der Nutzer verwende den Suchdienst nur zum eigenen Gebrauch; daran ändere auch die Beteiligung des Betreibers des Suchdienstes nichts.

Im Rahmen der Novellierungsüberlegungen zum Zweiten Korb[38] soll die Zulässigkeit von Kopienversanddiensten geregelt werden. Nach § 53a des Entwurfs soll die Versendung im Wege des Post- oder Faxversandes durch öffentliche Bibliotheken zulässig sein, sofern sich der Besteller auf einen durch § 53 UrhG privilegierten Zweck berufen kann. Die Vervielfältigung und Verbreitung in sonstiger elektronischer Form wird auf grafische Dateien beschränkt. Eine solche Versendung kommt aber nur in Betracht, wenn die Beiträge von Mitgliedern der Öffentlichkeit nicht von Orten und zu Zeiten ihrer Wahl mittels einer vertraglichen Vereinbarung erworben werden können. Mit diesen Beschränkungen hat sich der Kopienversand von öffentlichen Bibliotheken weitgehend erledigt.

Technische Selbsthilfe

Die globale Verbreitung des Internets und die territoriale Anknüpfung des Urheberrechts stehen im Widerspruch zueinander; dieser führt in der Praxis zu erheblichen Irritationen. Die Probleme lassen sich nur eingeschränkt durch gesetzliche Ausnahmebestimmungen (*statutory licensing*) oder die Zwischenschaltung von Verwertungsgesellschaften (*collective licensing*) lösen. Auch das *single licensing* erweist sich als zeitraubender Lösungsansatz, muss doch mit jedem Rechteinhaber ein Vertrag geschlossen werden.

Es verwundert daher nicht, dass die Industrie zur Selbsthilfe übergeht: Mit *Code-as-code*-Verfahren wird der Programmiercode zur Kodifikation. An die Stelle gesetzlicher Vorgaben treten technische Standards, Kopierschutzmechanismen und Copyright-Management-Systeme (CMS). Hierzu zählen: *Dongles*, kleine Steckmodule, die zum Schutz vor unberechtigter Softwarenutzung auf den Parallelports der Rechner angebracht werden und dadurch erst die Nutzung des Computerprogramms ermöglichen; RPS, das *Rights Protection System* der IFPI, ein System zur Sperrung des Zugriffs auf urheberrechtsverletzende Websites; *Regional Encoding Enhancements*, eine territorial-bezogene Beschränkung der Nutzungsmöglichkeiten einer CD; das *Serial Copy Management System* (SCMS), das die Verwendung kopierter CDs verhindert.

Zum Bereich der technischen Selbsthilfe hat die EU eine Reihe von Regelungen erlassen. Zu bedenken sind zunächst die Bestimmungen in der Softwareschutzrichtlinie über den Schutz vor Umgehungstools (Art. 7 Abs. 1 lit. c).[39] Hinzu kommt die Richtlinie 98/84/EG über den rechtlichen Schutz von zugangskontrollierten Daten und von Zugangskontrolldiensten.[40] Diese regelt nicht nur den Bereich des Pay-TV, sondern aller Zugangskontrolldienste (Art. 2 lit. a). Nach Art. 4 dieser Richtlinie müssen die Mitgliedsstaaten „illicit devices" verbieten. Solche sind in Art. 2 lit. (e) definiert als „any equipment or software designed or adapted to give access to a protected service in an intellegible form without the authorisation of the service provider". Die Richtlinie ist im März 2002 durch das Gesetz zum Schutz von zugangskontrollierten Diensten und Zugangskontrolldiensten (Zugangskontrolldiensteschutzgesetz/ZKDSG) in deutsches Recht umgesetzt worden.[41] Verboten ist danach die gewerbs-

[37] Urteil vom 27. 10. 2000; vgl. dazu K&R, (2001), S. 327, und NJW-Rechtsprechungs-Report, (2001), S. 904.

[38] Referentenentwurf (Anm. 26).

[39] Siehe dazu vor allem Raubenheimer, in: CR, 9 (1994), S. 129 ff.

[40] EU-Amtsblatt Nr. L 320/54 vom 28. 11. 1998.

[41] BGBl 2002 I v. 22. 3. 2002, 1090 f.; http://217.160.60.235/BGBL/bgbl1f/bgbl102019s1090.pdf. Siehe dazu Bär/Hoffmann, in: MMR, (2002), S. 654 ff., und ausführlich Christian Dressel/Hauke Scheffler (Hrsg.), Rechtsschutz gegen Dienstepiraterie. Das ZKDSG in Recht und Praxis, München 2003.

mäßige Verbreitung von „Vorrichtungen“, die dazu bestimmt sind, den geschützten Zugang von Fernseh- und Radiosendungen sowie von Tele- und Mediendiensten zu überwinden.

Hinzu kommt die jüngst verabschiedete Richtlinie zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft. Die InfoSoc-Richtlinie verpflichtet die Mitgliedstaaten zu einem angemessenen Rechtsschutz gegen die Umgehung wirksamer technischer Maßnahmen durch eine Person, der bekannt ist oder den Umständen nach bekannt sein muss, dass sie dieses Ziel verfolgt (Art. 6 Abs. 1). Allerdings ist ein solcher Schutz problematisch, wo die technischen Schutzsysteme gesetzliche Vorgaben unterminieren. Das ist zum Beispiel bei SCMS der Fall, sofern das gesetzlich erlaubte Erstellen privater Kopien technisch unmöglich gemacht wird. Ähnliches gilt für die *Regional Encoding Enhancements*, die mit dem Erschöpfungsgrundsatz (§ 17 Abs. 2 UrhG) und dem Prinzip der Warenverkehrsfreiheit kollidieren. Nach Art. 6 Abs. 4 S. 1 der InfoSoc-Richtlinie treffen die Mitgliedstaaten auch Schutzmaßnahmen gegen technische Sperren, sofern diese den gesetzlichen Schranken widersprechen.

Für das Verhältnis zur Privatkopierfreiheit sieht Art. 6 Abs. 4 S. 2 allerdings nur noch vor, dass ein Mitgliedstaat hier tätig werden „kann“ („may“). Es wird künftig möglich sein, dass technische Sperren das Erstellen privater Kopien verhindern und die EU-Staaten hier nicht zum Schutz des Endnutzers vorgehen. Im Übrigen können die Rechteinhaber solche Sperren auch setzen, wenn sie selbst die Vervielfältigung zum privaten Gebrauch ermöglichen (Art. 6 Abs. 4 S. 2 a. E.).

Stephan Blancke

Information Warfare

Sämtliche Signale werden unverständlich, da niemand weiß, wo die wirkliche Macht liegt.

Robert Anton Wilson, Die Illuminati-Papiere, Berkeley 1980

Die in den Medien häufig erwähnte Information Warfare (IW) wird selten differenziert erklärt und ist nur sperrig als „elektronische Kriegführung mit Informationen“ übersetzbar. Das strategische Interesse sowie die militärische Intention, die hinter IW stehen und die unter Umständen die globale Kommunikation über das Internet beeinträchtigen können, werden kaum thematisiert. Die Folge ist, dass IW bisher nicht adäquat in den Bemühungen zur Entspannung und Abrüstung berücksichtigt wurde.[1] Ein Grund für die sich relativ ungestört entwickelnde IW-Szene sind auch die nur vagen Vorstellung von Operationen militärischen Charakters, die sich im Internet abspielen sollen. Mit IW wird zunächst kein praktisches Instrumentarium beschrieben, denn es existiert kein definiertes und empirisch basiertes Konzept. Vielmehr müssen alle Formen des Informationsaustausches und der Interaktion zwischen Individuen und Strukturen der Informationstechnologie betrachtet werden.[2]

Stephan Blancke
Dipl.-Verwaltungswirt (FH), Dipl.-Politologe, geb. 1969; Doktorand am Otto-Suhr-Institut für Politikwissenschaft, Freie Universität Berlin, Ihnestraße 1, 14195 Berlin.
stephan.blancke@web.de

Als der Begriff des „Information War“ in der Literatur auftauchte, war zunächst die Manipulation der Menschen durch die Medien, also der zivile Aspekt, gemeint.[3] Mit

[1] Vgl. Forschungsgruppe Informationsgesellschaft und Sicherheitspolitik (FoG:IS), Information Warfare. Die Rüstungskontrolle steht vor neuen Herausforderungen, Arbeitspapier Nr. 2, Berlin 2000.
[2] Vgl. Martin Libicki, What is Information Warfare?, Washington 1996.
[3] Vgl. Dale Minor, The Information War, New York 1970.

dem Aufkommen leistungsfähiger Rechnersysteme entstand jedoch die Grundlage für eine effektive elektronische Kriegführung, die über die bis dahin angewandten Methoden – z. B. die Störung des gegnerischen Radars – hinausging und deren Bedeutung rasch deutlich wurde: „Electronic warfare is a relatively new but utterly deadly battlefield, where victory or defeat may come in a matter of seconds or even microseconds. Electronic intelligence is vital to survival in this struggle."[4]

Parallel zur technologischen und kulturellen Entwicklung entstanden neue Forschungsvorhaben und Institute, die sich mit Kybernetik und Systemtheorien, vernetzten Rechnersystemen und schließlich der Verwundbarkeit dieser Strukturen unter kriegerischen Bedingungen befassten. Eines der ersten dezentralen Rechnersysteme war in den frühen sechziger Jahren das Semi-Automatic Ground Environment Air Defense System (SAGE), das dem US-Militär unterstellt war. Die in den späten fünfziger Jahren gegründete Advanced Research Projects Agency (ARPA) bildete mit dem hauseigenen Arpanet die Grundlage für das Internet der heutigen Zeit.[5]

Parallel zu diesen Entwicklungen wuchs der Wert von Informationen und ihr Einfluss auf die Akteure militärischer Szenarien.[6] In den Computerlabors erkannte man, welche Bedeutung rechnergestützte Informationen besitzen konnten: „Man kann nämlich aus jedem guten Informationssystem ein Instrument zur Desinformation machen (...). Kommunikation ist Macht und Information ist Macht."[7] Es lässt sich eine kausale Kette zwischen der 1946 als Thinktank von Mathematikern gegründeten RAND Corporation und dem heutigen globalen Netz zur Erfassung von Informationen, Echelon, herstellen.[8]

[4] William V. Kennedy, Intelligence Warfare, New York 1987.
[5] Vgl. Lutz Dammbeck, Das Netz – die Konstruktion des Unabombers, Hamburg 2004.
[6] Vgl. Manuel De Landa, War in the Age of Intelligent Machines, New York 1991.
[7] Jaques Valle, The Network Revolution, Berkeley 1982.
[8] Vgl. Christiane Schulzki-Haddouti (Hrsg.), Bürgerrechte im Netz, Bonn 2003.

IW wird in den aktuellen Diskussionen in mehrere Kategorien unterteilt, die sich in ihrer technischen Durchführung überschneiden können. So wird von Command-And-Control-, Intelligence-Based-, Electronic-, Psychological-, Hacker-, Economic-, Information- und schließlich Cyber-Warfare gesprochen.[9] Diese Auflistung verdeutlicht die Versuche, eine gültige Definition zu finden. Es gibt weitere Unklarheiten, die sich auf die Intention von IW und die Identifikation und Bewertung von Störungen elektronischer Kommunikationsverbindungen beziehen: Handelt es sich um einen Hackerangriff, d. h., steht dahinter eine eventuell politisch unmotivierte Einzelperson, oder wird im Auftrag eines dem Angreifer unbekannten Geldgebers gearbeitet? Hat der Auftraggeber politische, wirtschaftliche oder rein persönliche Gründe? Wo liegen die qualitativen Unterschiede zwischen dem folgenlosen Eindringen einerseits und dem bewussten Zerstören einer elektronischen Infrastruktur andererseits? Lassen sich terroristische Verbindungen herstellen? Handelt es sich um eine terroristische Struktur, die weltweit operiert und sich für die Verbreitung einer (religiösen) Weltanschauung einsetzt, oder um eine Gruppierung, die von einem Staat gesponsert oder beherbergt wird?

Methoden und Ziele

Angesichts dieser Unklarheiten erscheint es sinnvoll, sich neben den Methoden auf die Ziele von IW zu konzentrieren: die Manipulation des ungestörten, weltweiten Informationsaustauschs. IW zielt darauf ab, unter Ausnutzung schneller, hoch technisierter Informationsverarbeitung die Verfügbar- und Unversehrbarkeit von zivilen und/oder militärischen Informationen sowie die Integrität der gegnerischen Kommunikationsressourcen in Frage zu stellen. Dieses Konzept ist nicht neu, gewinnt aber angesichts der zunehmenden Vernetzung und Digitalisierung an Relevanz.

IW zielt nicht unbedingt auf die materielle Zerstörung militärischer oder ziviler Güter. Es geht vielmehr darum, die Informationen, die zur Aufrechterhaltung eines militärischen oder zivilen Systems benötigt werden, zu stören oder zu eliminieren. Ein gestörter Funk-

[9] Vgl. www.georgetown.edu (18. 11. 2003).

spruch an die Besatzung eines U-Bootes gehört ebenso zu IW wie die Ausschaltung der Steuerungssoftware eines Atomkraftwerks.[10] Während frühere Methoden von IW z. B. Flugblätter oder Störsender darstellten, hat IW heute unter Umständen umfassende Konsequenzen für Unbeteiligte: Die Zahl der Personen, die an manipulierbarer Technik partizipieren oder von ihr abhängen, ist bei weitem höher als noch vor wenigen Jahrzehnten. Das bedeutet etwa, dass gefälschte Reportagen, die über das Fernsehen ausgestrahlt werden, einen weitaus größeren Einfluss haben als die Aktivitäten von Störsendern im Zweiten Weltkrieg.[11] Aufgrund der hohen Vernetzungsdichte können zahlreiche Unbeteiligte von Attacken auf Internetserver betroffen sein, ohne dass ein kausaler Zusammenhang zwischen diesen Personen und den Interessen eines Angreifers hergestellt werden könnte.

Zur Umsetzung von IW sind aufeinander basierende Information Operations (IO) notwendig:[12]

– Die Sammlung von möglichst umfassenden Informationen über den Gegner, wobei das Wissen über Informationsabläufe und Kommunikationsstrukturen Priorität genießt. Dabei wird unterschieden zwischen Software (Programme, Tools, Schwachstellen von Verschlüsselungstechniken) und Hardware (Rechenzentren, Führungsstäbe, Kommunikationsbunker, Radio- und Fernsehstationen, Satelliten, Kabelschächte). Die Sammlung und Weitergabe dieser Informationen (*collection* und *dissemination*) kann über staatliche Geheimdienststrukturen oder durch private, speziell beauftragte Unternehmen erfolgen.[13]

– Die Manipulation, Kontrolle, Störung oder Vernichtung der gegnerischen Informationsflüsse. Die ins Visier geratene Soft- und Hardware kann mit Systemen angegriffen werden, die ebenfalls in Soft- (Propaganda aller Art, Serverattacken, Vireneinschleusung) und Hardware (Zerstörung der Hardware, Einsatz von satellitengesteuerten Raketen) unterteilt werden. Auch die Ausschaltung einzelner Personen kann zu Methoden der IW gezählt werden.[14]

Daraus folgt, dass das Scannen nach Schwachstellen in einem System bereits eine erste, unumgängliche Operation darstellt, um einen Angriff auszuführen.[15] Die so gewonnenen Erkenntnisse können vielfältiger Natur sein: Namen, Position und Zugangsmöglichkeiten, Erreichbarkeit einzelner Personen; Tätigkeiten, Aktivitäten (inhaltlich und zeitlich), Örtlichkeiten; Anbindung des gescannten Objektes an andere Strukturelemente und die erforderliche Energieversorgung; Wirkungsebene, Zielrichtung und Zielobjekt; Strategien und Verhaltensweisen. Mithilfe des Scannens können Personen herausgefiltert werden, die für eine IO in Frage kommen. Dabei ist offen, ob die Informationswege dieser Einzelperson gestört oder manipuliert werden sollen oder ob diese Person durch eine geheimdienstliche Operation für eine Zusammenarbeit gewonnen werden kann. Dieser Schritt hängt von der Intention des Angreifers ab, denn ein Scanning mit terroristischem Hintergrund wird nur selten das Ziel einer Kontaktanbahnung haben. Das heißt, dass für diese Operationen die *counter-intelligence*-Strukturen eines Staates geeignet sind.[16]

Neben diversen Verfahren auf der Softwareebene, welche die Kommunikationswege nutzen, um diese auf der gegnerischen Seite unbrauchbar zu machen, sind direkte militäri-

[10] Vgl. John Ferris, Netcentric Warfare, C4ISR and Information Operations. Toward a revolution in military intelligence?, in: L.V. Scott/Peter Jackson (Hrsg.), Understanding Intelligence in the Twentyfirst Century. Journeys in Shadows, London 2004, S. 54 ff.

[11] Vgl. auch Thymian Bussemer, Medien als Kriegswaffe. Eine Analyse der amerikanischen Militärpropaganda im Irak-Krieg, in: Aus Politik und Zeitgeschichte (APuZ), 53 (2003) 49–50, S. 20–28.

[12] Zum Begriff Information Operations siehe u. a. Department of Defence Operations Policy, www.crows.org/about/Io.htm (3. 12. 2003).

[13] Vgl. Michael Herman, Intelligence Power In Peace And War, Cambridge 1996. Insbesondere auf der technischen Ebene gibt es im privaten Sektor einen qualitativen Vorsprung, so dass eine Kooperation unumgänglich erscheint.

[14] Vgl. Roy Godson, Dirty Tricks Or Trump Cards. US Covert Action And Counterintelligence, Washington 1995; Department of Defense, Joint Publication 1–02 vom 12. 4. 2001, www.dtic.mil (24. 11. 2003).

[15] Vgl. Clay Wilson, Computer Attacks and Cyber Terrorism. Vulnerabilities and Policy Issues for Congress (Congressional Research Service Report for Congress, RL32114), Appendix A – Planning a Computer Attack, Washington 2005, S. 36 ff.

[16] Counter-Intelligence ist von Counter-Espionage zu unterscheiden: Letztere dient der Spionageabwehr auf dem eigenen Staatsgebiet, während Erstere die Infiltration gegnerischer Intelligence-Strukturen, auch jenseits des eigenen Staatsgebietes, zum Ziel hat.

sche Angriffe auf entsprechende Strukturen möglich.[17] Dabei können konventionelle Waffen oder Spezialkommandos eingesetzt werden, die damit Instrumente von IW werden. Jedoch können auch Waffensysteme verwendet werden, deren Einsatz besonderen Bestimmungen unterliegt. Diese militärischen Operationen können Merkmale eines *low-intensity*-Konfliktes zeigen und teilweise in den Bereich der asymmetrischen Kriegführung fallen.[18]

Zu diesen Systemen zählen auch Atomwaffen. Im Zusammenhang mit IW ist in erster Linie nicht der Bodeneinsatz, sondern die Zündung eines Sprengsatzes in bis zu 500 Kilometern Höhe gemeint. Bei der Kernspaltung wird ein kurzfristiger elektromagnetischer Puls (EMP) erzeugt, der weitflächig elektronische Komponenten unbrauchbar macht.[19] Ein einzelner EMP kann theoretisch einen gesamten Kontinent und zivile wie militärische Ziele betreffen. Die für den Internetverkehr notwendige Infrastruktur ist nur mit sehr großem Aufwand abzuschirmen, eine nahezu unlösbare und kaum finanzierbare Aufgabe. Auch mobile elektronische Komponenten in Flugzeugen, Schiffen und Raketen würden gestört werden.

Der Bodeneinsatz von Atomwaffen, wie er von den USA mit so genannten *mini-nukes* geplant wird, hat in erster Linie jene Ziele im Visier, die für moderne Kriegführung unerlässlich sind: in großer Tiefe befindliche Führungsbunker, Kommunikationswege und Infrastrukturen. Eine derartige Waffe ist geradezu prädestiniert für den Einsatz in einer IO.[20] Neue Entwicklungen betreffen Waffensysteme, die Mikrowellen produzieren und damit ebenfalls elektronische Komponenten ausschalten können. Die USA sollen *non-nuclear electromagnetic pulse warheads* im ersten Golfkrieg gegen die irakische Infrastruktur eingesetzt haben.[21] Ferner wird an der Entwicklung von Mikrowellenkanonen gearbeitet, die unter großem Energieverbrauch innerhalb von Sekundenbruchteilen einen Puls produzieren, dessen Frequenzen geeignet sind, elektronische Komponenten unbrauchbar zu machen. Intensive Forschungen dazu werden auch in Deutschland geleistet.[22] Zusätzlich zur Kanonenvariante sollen mobile und kleinere Waffensysteme, die auf dieser Technologie beruhen, entwickelt werden.[23]

Die Gefährdung des Internets

Unabhängig von der Frage nach der Gefährdung des Internets als Kommunikationsnetzwerk muss der Einsatz der beschriebenen Waffensysteme so gestaltet werden, dass die eigenen Kommunikationswege nicht beeinträchtigt werden. Insofern müssen die IO punktuell, d. h. möglichst im Zielland realisiert werden. Die Ausschaltung eines Rootservers – eines der weltweit 13 Internetzentralrechner – würde den Internetverkehr nur unerheblich beeinträchtigen; die auch nur temporäre Blockade aller weltweiten Standpunkte hingegen wäre bezüglich der eigenen internetbasierten Kommunikation autodestruktiv und im Übrigen schwierig durchzuführen, da die Systeme erheblich abgesichert sind.[24]

Praktikabler wären gezielte Angriffe auf einzelne Komponenten, wobei der Softwareeinsatz unauffälliger durchgeführt werden kann und sich in einer rechtlich vorteilhafteren, schwer nachweisbaren Situation befindet. Das Ziel sollte eng gefasst und – vor einer konventionellen militärischen Gewaltanwendung – mit geringstmöglicher Mittelsignifikanz angegriffen werden, um jede Identifikation zu erschweren. Hingegen würden terroristische bzw. nichtstaatliche IO entweder Einzelobjekte des Gegners betreffen oder aber die betroffenen Sozialstrukturen angreifen. Dafür kämen insbesondere Infrastrukturen des zivilen Sektors in Frage: Grundversorgung (Energie, Nahrung, Medizin), Medien, Verkehr. Britische Geheimdienste befürchten insbesondere Angriffe, die sich

[17] Vgl. Edwin L. Armistead, Information Operations. Warfare and the Hard Reality of Soft Power, Dulles 2004.

[18] Vgl. Bernd Jakob, Geheime Nachrichtendienste und Globalisierung, Frankfurt/M. 1999, S. 195 ff.

[19] Es gibt verschiedene Arten eines EMP sowie diverse Techniken, diesen zu erzeugen, vgl. www.fas.org.

[20] Vgl. Markus Becker, Forscher entwerfen Bushs nukleare Sense, in: Spiegel Online, www.spiegel.de (12. 11. 2003).

[21] Vgl. u. a. High-power microwave (HPM)/E-Bomb, www.globalsecurity.org (6. 11. 2003).

[22] Siehe www.pulsed-power.de.

[23] Vgl. Georg Schöfbänker, Computer-Netzwerk-Attacken und Mikrowellenkanonen, www.heise.de (24. 11. 2003).

[24] Vgl. Jonathan Adams/Fred Guterl, Bringing Down The Internet, in: Newsweek vom 3. 11. 2003, S. 50 ff.; siehe auch www.root-servers.org.

gegen zivile, offene Kommunikationsstrukturen richten.[25] Derartige IO könnten auch das Ziel haben, die „gegnerischen Hacker“ zu provozieren oder einzuschüchtern.[26]

Simulationen zeigen, dass auch bei einzelnen Ausfällen die Kommunikation weiter funktionstüchtig ist – insbesondere bei einer dichten Vernetzung aller Komponenten, über die der Datentransport läuft.[27] Es müssten zahlreiche und zeitgleiche, abgestimmte Angriffe erfolgen, die den Datenverkehr mit Software blockieren und mit physischer Gewalt relevante Schnittstellen zerstören. Im Gegensatz zu einzelnen Gruppierungen ist es für staatliche Akteure einfacher, dieses Ziel zu realisieren: So wird regelmäßig kritisiert, dass der überwiegende Teil der für den Datenverkehr wichtigen Rootserver in den USA steht und bei Belieben abgeschaltet werden könnte. Ein geringer Programmieraufwand könnte sämtliche Internetauftritte eines Landes von den Monitoren verschwinden lassen. Mit einem Eingriff in das internationale Telefonnetz deaktivierten die USA im November 2001 den somalischen Provider Somalia Internet Company, dem terroristische Verwicklungen vorgeworfen wurden.

Allerdings wird die Kommunikation über das Internet derzeit weniger gezielt attackiert als vielmehr unter kriminellen oder religiösen Aspekten missbraucht. Für die kontinuierliche Zunahme der Manipulationen sind Gruppen der organisierten Kriminalität verantwortlich, die systematisch Sicherheitslücken bei Firmen und Banken ausnutzen.[28] Neben Wirtschaftsspionage geht es auch um Eingriffe in die boomende Internettelefonie.[29] Im Gegensatz dazu bereiten sich bestimmte Staaten darauf vor, im Internet selbst Eingriffe vornehmen zu können. Nordkorea beschäftigt sich mit der Ausbildung von Experten für den Cyberwar, der eine Alternative für die kostspielige konventionelle Kriegführung darstellt.[30] Ebenso bestätigt Zhang Zhaozhong, Direktor der chinesischen National Defense University, Experten aus der sehr aktiven chinesischen Hackerszene rekrutieren zu wollen. Einen Einblick in die durchgeführten IO erhält man meist erst dann, wenn sie scheitern, so z. B. bei chinesischen Angriffen auf deutsche oder südkoreanische Server.

Die USA arbeiten seit geraumer Zeit am Aufbau eines neuen weltweiten Kommunikationsnetzes – Global Information Grid (GIG) genannt –, das unabhängig vom Internet arbeiten soll, sowie an einer speziellen militärischen Einheit, dem Joint Functional Component Command for Network Warfare (JFCCNW). Dessen Mitglieder rekrutieren sich aus CIA, NSA, FBI und den Militärgeheimdiensten. Unabhängig davon existieren weitere staatliche Projekte, die im Umfeld krimineller Attacken auf Internetstrukturen ermitteln.[31] Die Entwicklung zeigt, dass es sich um eine Symbiose privatwirtschaftlicher, akademischer und sonstiger staatlicher Institutionen handelt, die an der Entwicklung von progressiven Open-Source-Lösungen oder alternativen Rootserversystemen wie dem Open Root Server Network (ORSN) kaum Interesse haben.[32] Zum einen geht es um den Bestand von Softwaremonopolen, zum anderen um die Möglichkeit der Einflussnahme auf Kommunikationsstrukturen und damit um die Funktionsfähigkeit des Internets. Die Realisierung des Network Centric Warfare verlangt uneingeschränkten Zugriff staatlicher Stellen auf alle Informationskanäle im Operationsgebiet.

Neben dem gestörten Informationsaustausch ist auch eine unterbundene Information Bestandteil von IW. Ambitionierte Staaten wie die USA oder die Volksrepublik China versuchen, effektive Verschlüsselungssoftware zu verbieten oder mit umfassenden

[25] Die sporadischen Energieausfälle in den USA und Südkanada sind nach offiziellen Verlautbarungen zwar nicht auf Angriffe von Hackern zurückzuführen, es gibt aber auch gegenteilige Ansichten, die z. B. den MSBlast-Wurm („Blaster“) für die Ausfälle verantwortlich machen, vgl. Brian Krebs, Hackers Did Not Cause Blackout – Report, www.washingtonpost.com (20. 11. 2003); Bruce Schneier, Internet worms and critical infrastructure, http://news.com (16. 12. 2003).

[26] Vgl. Ellen Messmer, The e-jihad. When middle east conflict goes electronic, http://napps.nwfusion.com (16. 12. 2003).

[27] So z. B. das Modell INESS des Forschungszentrum Jülich, www.fz-juelich.de.

[28] Vgl. Computer Crime Research Center, Russian hackers unite in organized criminal groups, www.crime-research.org (20. 4. 2005).

[29] Siehe den aktuellen CyberCrime Report 2005, www.infosec.co.uk (26. 4. 2005).

[30] Vgl. Joseph S. Bermudez Jr., The Armed Forces of North Korea, London 2001.

[31] Vgl. U.S. Cyber-Crime Unit Focuses on Russian Hackers, www.mosnews.com (13. 5. 2005).

[32] Vgl. www.wired.com.

Firewalls den Zugriff ihrer Bürger auf Informationen zu verhindern. An der Entwicklung von Technologien wie Quantenrechnern und selbstlernenden Netzwerken beteiligen sich zahlreiche Firmen, die von der boomenden Nachfrage nach der Informationsüberlegenheit profitieren.[33] Auf Konferenzen wie der „Information Operations Europe 2005" stellen Militärs, Politiker und Wissenschaftler neue Technologien und Taktiken vor und diskutieren den Umgang mit Medien und die Notwendigkeit dosierter Informationen.[34]

Rechtliche Situation

Der Kampf um Informationen findet überwiegend in einer Grauzone statt. Nur selten werden rechtswidrige Operationen wie z. B. Lauschangriffe auf die UNO und auf Generalsekretär Kofi Annan bekannt. Die umfassende Überwachung des Internetverkehrs durch Geheimdienste wie die NSA wird erst dann deutlich, wenn bestimmte Personen und ihre Konversation betroffen sind – wie z. B. Mohammed Momin Khawaja, der die Deaktivierung eines chinesischen Satelliten via Laptop und Mobiltelefon demonstrieren wollte und 2004 wegen angeblicher terroristischer Motive angeklagt wurde.

Aus rechtlicher Sicht stellt IW Neuland dar, und der Umgang mit IO birgt große Schwierigkeiten. Man kann nicht davon ausgehen, dass sich die Protagonisten von IW auf eine gesicherte Rechtsbasis berufen können. Alle dargestellten Aktivitäten können daher nur innerhalb des geltenden Völkerrechts bewertet werden. Die zunehmenden Attacken im Internet erhöhen den Druck auf die Staatengemeinschaft, präzisere Regelungen zu etablieren. Weiterhin wird deutlich, dass eine Aufstockung der Ermittlungsbehörden allein nicht dem Rechtsmangel abhelfen kann.[35] Vielmehr betont die Ausweitung staatlicher Eingriffe in die informationelle Selbstbestimmung, basierend lediglich auf einer angeblich omnipräsenten Terrorgefahr, die Notwendigkeit internationaler Vereinbarungen. In den meisten Publikationen über IW werden die neuen Möglichkeiten und Techniken in einer oft euphemistischen Art und Weise beschrieben, die rechtlichen Aspekte jedoch kaum behandelt. Umfassende Zusammenstellungen von Gesetzestexten und Vereinbarungen zur Waffenkontrolle führen den Begriff des IW nicht auf; lediglich *electronic warfare* wird erwähnt.[36] Dabei stehen technische Fragen wie die Möglichkeiten von Militärsatelliten oder die Verwendung moderner Kommunikationsformen durch Terroristen im Vordergrund. Immerhin wird unter dem Schlagwort „Network Centric Operations" nach „Breaking the backbone" gefragt.[37] Relevante Handbücher militärischer Organisationen kennen IW und die rechtliche Problematik entweder nicht oder erwähnen nur kurz die dafür verantwortliche Institution, oder aber der Begriff wird als Instrument der Militärlogistik jenseits rechtlicher Anforderungen und Verantwortungen definiert.[38] Eine IO wird derzeit nicht als militärische Operation, sondern als technisches, unter rechtlichen Gesichtspunkten quasi wertfreies Phänomen betrachtet.

Aus völkerrechtlicher Sicht ist jedoch die Unterscheidung von staatlichen und privaten Akteuren notwendig, da ein Staat nicht für die Aktionen privater Akteure verantwortlich ist – es sei denn, dass er das offensichtlich unzulässige Handeln privater Akteure toleriert oder gar fördert. In einem solchen Fall würde er für solche Informationsoperationen verantwortlich gemacht werden können. IW kann derzeit jedoch nur von staatlichen Strukturen effektiv geleistet werden, so dass diese hier im Vordergrund stehen müssen.[39]

Im Gegensatz zur defensiven IO, die in unterschiedlicher Intensität völkerrechtlich zulässig sein kann, kommt für eine offensive IO der Art. 2, Ziff. 4 der Satzung der Vereinten Nationen (SVN) in Frage, denn hier wird

[33] Anschaulich dafür sind z. B. die Werbeanzeigen in C4ISR, dem Journal Of Net-Centric Warfare der Defense News Media Group (USA).
[34] Vgl. www.defenceiq.com/2360a (17. 5. 2005).
[35] Vgl. G5 nations propose terrorist watch centre, http://jir.janes.com (14. 4. 2005).
[36] Vgl. Jozef Goldblat, Arms Control. The New Guide to Negotiations and Agreements. Fully Revised and Updated Second Edition with New CD-ROM Documentation Supplement, London 2002.
[37] Vgl. The International Institute for Strategic Studies (IISS), The Military Balance 2004/ 2005, London 2004.
[38] Vgl. NATO Office of Information and Press, NATO Handbook, Brüssel 2001, S. 324; Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1–02, Version September 2003.
[39] Vgl. Vulnerability. What are Al Qaeda's Capabilities?, http://www.pbs.org (18. 12. 2003).

jede Androhung oder Anwendung von Gewalt untersagt. Ob eine solche stattgefunden hat, entscheidet der Sicherheitsrat der Vereinten Nationen (VN). Nach der Feststellung hat der betroffene Staat nach Art. 51 SVN das Recht auf Selbstverteidigung. Wann liegt eine offensive, aggressive IO im Sinne einer Gewaltanwendung vor? Das Völkerrecht denkt bei dem Begriff der Aggression an Waffeneinsatz und militärische Gewalt. Die Resolution der VN vom 14. Dezember 1974 führt als Beispiele Blockaden der Häfen und Küsten und Verletzung der Integrität des staatlichen Territoriums auf.[40]

Unter heutigen Umständen könnte eine solche Auflistung die Durchführung von IO beinhalten, denn die Blockade und die Störung der Informations- und Kommunikationsnetze können gleiche oder noch verheerendere Folgen haben.[41] Da „Waffe" nicht eindeutig zu definieren ist, kann darauf zu Gunsten des Resultats des Mitteleinsatzes verzichtet werden, etwa wenn mit einer IO – ebenso wie mit konventionellen Waffen – Zerstörung oder Beeinträchtigung des Gegners sowie eigene Vorteilsnahme beabsichtigt sind. Damit wird auch die Selbstverteidigung eines Staates gegen eine IO zulässig. Allerdings muss der Grundsatz der Verhältnismäßigkeit gewahrt bleiben; das Mittel der Selbstverteidigung orientiert sich an den durch die IO erzeugten Schäden.

Doch lassen sich die IO bzw. der Angriff eindeutig verifizieren? Kann bei einem Softwareeinsatz die verantwortliche Quelle identifiziert werden? Darf auf die IO mit den gleichen Mitteln geantwortet werden? Wie intensiv darf der Gegenschlag gestaltet sein? Wie verhält sich der angegriffene Staat, wenn im Rahmen einer IO die Kommunikationsstrukturen eines anderen, unbeteiligten Staates missbräuchlich verwendet werden? Ist der angegriffene Staat technologisch so ausgerüstet, dass er eine Gegenoperation führen kann? Darf er sich ansonsten mit konventionellen militärischen Mitteln verteidigen? Sind die gegen einen Staat gerichteten IO nach dem Völkerrecht zulässig, d. h., handelt es sich eventuell um (zulässige) Propaganda, die desinformieren soll, oder handelt es sich um (unzulässige) Propaganda, die z. B. die gegnerische Staatsführung beleidigt oder die Bevölkerung zu subversiven Handlungen aufruft?[42]

Diese wenigen Punkte zeigen, in welch unklarer Situation sich IO und ihre Abwehr bewegen. Das führt zwangsläufig dazu, dass der Rechtsrahmen sehr weit interpretiert wird. Erschwerend kommt hinzu, dass zahlreiche Staaten nicht adäquat und in völkerrechtlich zulässiger Form auf eine IO reagieren können: So ist z. B. die Retorsion (erlaubter Eingriff in den Rechtskreis eines anderen zur Wiedergutmachung eines durch ihn zugefügten Unrechts) für finanziell schwache Staaten kaum durchführbar.[43] Dieses Unvermögen des adäquaten Antwortens wird in einem konventionellen militärischen Konflikt völlig legitim ausgenutzt, aber im Rahmen einer IO sind die Grenzen zwischen offener, rechtlich festgelegter Konfliktaustragung und versteckter Provokation fließend, sodass eine Eskalation denkbar ist. Staaten, die z. B. international weitgehend isoliert sind oder sich in einem ungleichförmigen Transformationsprozess befinden, könnten dazu neigen, Gefühle der vermeintlichen oder tatsächlichen (technischen) Unterlegenheit mit gefährlichen, auch unkonventionellen Überreaktionen zu kompensieren.[44]

Auch geheimdienstliche Operationen, die unter bestimmten Bedingungen völkerrechtlich zulässig sind, können IO darstellen, z. B. wenn gegnerische Datenbanken gescannt werden. Die Gefahr, dass dieser Vorgang von der Gegenseite analysiert wird, ist gerade bei jenen Staaten gewachsen, die man gewöhnlich als technische Entwicklungsländer betrachtet. Das Beschaffen der notwendigen Informa-

[40] Vgl. Nicolas Nyiri, The United Nations' Search for a Definition of Aggression, Resolution 3314 (XIX), New York 1989.

[41] Vgl. Kent Anderson, Intelligence-Based Threats Assessment for Information Networks and Infrastrucures, Portland 1998, http://www.aracnet.com (18. 12. 2003).

[42] Unter diesem Gesichtspunkt sind z. B. die IO der USA gegen die irakische Regierung 2003 kritisch zu bewerten.

[43] Dabei handelt es sich um eine sog. „unfreundliche Handlung", die dem Völkerrecht aber nicht widerspricht, also z. B. die Ausweisung von Diplomaten oder die Aussetzung von Zahlungen.

[44] So kann z. B. die bekundete Entwicklung von nordkoreanischen Atomwaffen als übersensible Reaktion der weitgehend abgeschotteten Regierung auf vermutete oder tatsächliche ausländische Provokationen gewertet werden: John B. Garrick/Willard C. Gekler (Hrsg.), The Analysis, Communication and Perception of Risk, New York 1991.

tionstechnologie ist seit dem Ende des Kalten Krieges relativ einfach geworden. Entweder werden entsprechende Spezialisten auf dem Weltmarkt „eingekauft“, oder es werden eigene IW-Strukturen entwickelt.[45] Proportional zu den militärischen Kapazitäten holen diese Staaten auch im Intelligence-Sektor und den angegliederten IW-Strukturen massiv auf; hier steht China neben den USA und Russland weltweit bereits an dritter Stelle.[46] Horchposten wie z. B. in Bejucal auf Kuba werden von China systematisch mit Technologie nachgerüstet. Zudem werden eigene Internetdienste entwickelt, um die Kontrolle über die nationale Kommunikation und ihre „subversiven“ Begleiterscheinungen zu erlangen.[47]

Weiterhin steigt im Rahmen von Konflikten, die von staatlichen IO begleitet werden, die Zahl der nichtstaatlichen IO. Dieses Phänomen konnte z. B. bei Spannungen zwischen den USA und China anlässlich gegenseitiger Spionageaktivitäten, beim Jugoslawienkrieg oder dem Angriff der USA auf den Irak beobachtet werden. Solche Situationen könnten eskalieren.[48] Ferner bedienen sich nichtstaatliche Akteure zwar moderner Technologie, orientieren sich aber noch weniger als Staaten an völkerrechtlichen Bestimmungen und agieren daher weitgehend unberechenbar. Insofern sollten ausgewählte, verletzbare Strukturen, die gewöhnlich bei zwischenstaatlichen Konflikten verschont werden, im allgemeinen Interesse besonders geschützt werden.[49]

Schlussfolgerungen

Alle an elektronischer Kommunikation beteiligten Akteure suchen Schutzmechanismen, um im *worst case scenario* bestehen zu können. Dabei werden neue Firewalls entwickelt oder internetähnliche Strukturen kostspielig konstruiert, um sie mit Attacken zu testen und wieder zu zerstören.[50] Insbesondere bei den staatlichen Stellen steht die Sorge um mögliche terroristische Angriffe auf die „nationale Sicherheit“ im Allgemeinen und das Internet im Speziellen im Vordergrund; eine Furcht, die von der US-Regierung aus unterschiedlichen Gründen geschürt wird. Doch weniger als ein Prozent aller registrierten Attacken auf das Internet in den USA haben ihren Ursprung in jenen Ländern, die der „Achse des Bösen“ zugerechnet werden; den Großteil stellen Angriffe dar, die innerhalb der USA geführt und „traditionellen“ Hackern zugerechnet werden können.[51] Die massive Einschränkung von Bürgerrechten, etwa mit dem Patriot Act, erscheint angesichts dessen als kaum gerechtfertigt.

Einer der Gründe für die ansteigenden Angriffe auf Internetkomponenten ist die rigorose Microsoft-Monokultur: 94 Prozent aller PCs weltweit verwenden als Betriebssystem das Microsoftprodukt Windows, dessen Verwundbarkeit sich täglich aufs Neue zeigt. Ein erster Schritt könnte der forcierte Einsatz alternativer Systeme sein, um die Abwehroptionen gegenüber Angriffen variabler zu gestalten. Welche Komponenten der Kommunikationsstruktur haben besonderen Status? Dazu gehören in erster Linie Versorgungseinrichtungen des öffentlichen Lebens, deren Ausfall zu Unruhe und Fragmentierung innerhalb der Gesellschaft führen könnte, ferner innerstaatliche Sicherheitsinstitutionen, denn innere Stabilität ist in den westlichen Staaten eher gefährdet und daher bevorzugter zu schützen als militärische Sicherheit.

Derzeit sind relevante militärische Angriffe auf westliche Staaten nicht realisierbar. Potenzielle Akteure wären kaum zu kurzfristigen Aktionen mit großer Schadenswirkung fähig, sondern benötigten eine monatelange Vorbereitungsphase; es müssten zivile und staatliche Institutionen wie Energieversorgung, Krankenhäuser, Verkehrssysteme, Industrie, Finanzmärkte, Telefonverbindungen, Polizeiwachen und Gefängnisse berücksich-

[45] Vgl. Florian Rötzer, Phantome der Konflikte im Informationszeitalter: Nordkorea, der Cyberwar und die Atomwaffen, www.heise.de (11. 12. 2003); Yoo Yong-won, North Building Up Hacking Capability, http://english.chosun.com (11. 12. 2003).

[46] IOSS (Interagency OPSEC [Operations Security] Support Staff), Intelligence Threat Handbook 2004 (USA).

[47] Vgl. North Korea launches ‚secure‘ email, in: ZDNet Week, http://news.zdnet.co.uk (3. 12. 2003).

[48] Vgl. Wayne Michael Hall, Stray voltage. War in the information age, Annapolis 2003.

[49] Ein Beispiel hierfür sind die großen Unterwasserkabel, die einem besonderen völkerrechtlichen Schutz unterworfen sind, www.cybergeography.org (16. 5. 2005).

[50] Vgl. Carrie Kirby, Researchers to build model of Internet – to destroy it, in: Seattle Post-Intelligencer, http://seattlepi.nwsource.com (10. 11. 2003).

[51] Vgl. Fighting the worms of mass destruction (Special Report. Internet Security), in: The Economist vom 29. 11. 2003, S. 75 ff.

tigt werden.[52] Zum Schutz muss eine parallele Kommunikationsstruktur bereitgestellt werden, die unabhängig vom Internet und bekannten Netzwerken arbeiten kann. Grundsätzlich sollten aufwendige elektronische Strukturen überdacht werden, da Komplexität eng verbunden ist mit Instabilität und Verlust von Effektivität.

Die Ausführungen haben gezeigt, dass sich IO auf einem rechtlich unklaren Terrain bewegen und dazu führen können, eine angespannte Situation zur Eskalation zu bringen. Auch im Bereich der IO muss daher die Vermeidung von Konflikten Vorrang genießen; die Defizite in der internationalen Rechtsprechung und ihrer Durchsetzung sollten nicht durch weitere Fehlentwicklungen vergrößert werden.[53] Grundsätzlich ist die Androhung oder die Anwendung von Waffensystemen – auch im Rahmen von IW – durch das Völkerrecht verboten, wenn dadurch der betroffene Akteur in seiner Handlungsfreiheit eingeschränkt, Gewalt ausgeübt und ein Schaden erzielt wird.[54] Die völkerrechtlichen Begriffe des Interventions- und Schädigungsverbots beziehen sich auf Handlungen, die unter dem Niveau einer direkten, bewaffneten Auseinandersetzung stattfinden. Diese Verbote eignen sich, die rechtliche Fragwürdigkeit von einzelnen IO zu unterstreichen. Durch diese werden fremde Kommunikationsstrukturen „betreten", d. h., die IO richtet sich gegen ein Rechtsobjekt, das nicht im eigenen Verfügungsbereich liegt. Abgesehen von den möglichen materiellen Schäden wird das souveräne Verfügen über diese Rechnerstruktur grundsätzlich in Frage gestellt.[55] Die Gefahr, dass diese Situation angesichts der zunehmenden technischen Vernetzung der Staaten untereinander eintritt, könnte durch ein Verbot oder eine ausdrückliche Regulierung minimiert werden. Denkbar wäre auch die Formulierung einer spezifischen Nichtangriffserklärung, die sich auf IO beschränkt.

Notwendig ist ferner eine internationale Abgleichung der Definitionen und ein Verhaltenskodex, der bestimmte Manipulationen innerhalb einer Struktur entweder ächtet oder verbietet und darauf basierend Sanktionen ermöglicht. Bei der Diskussion um Abrüstung auf dem Gebiet der IW ist die explizite Feststellung notwendig, dass nicht unbedingt nur „virtuelle Waffensysteme" eingesetzt, sondern auch militärische Operationen durchgeführt werden können. Der Glaube, dass es sich bei IW um „saubere" und „unblutige" Maßnahmen handelt, ist ein verhängnisvoller Irrglaube.[56]

Da eine internationale Kommunikationsstruktur unverzichtbarer Teil der globalen Wirtschaft und Kultur ist, sollte eine internationale Regelung erarbeitet werden, welche provokative IO verbietet und die Institutionalisierung einer bei den VN angesiedelten Behörde ermöglicht, um effektiv die internationalen Informationsströme zu überwachen. Dabei könnte es sich um eine Intelligence-Struktur handeln, deren Fehlen im Zusammenhang mit den *early-warning capacities* der VN ohnehin beklagt wird.[57] Ferner müsste der Zusammenhang von IW-Kapazitäten und Abrüstungsfragen deutlicher hergestellt werden. Ansonsten wird auch in diesem Bereich aufgerüstet werden.[58] In diesem Zusammenhang muss sich die internationale Rechtsprechung mit der Relation zwischen Spionage und IO befassen, denn bislang ist völlig unklar, ob z. B. das Scannen von gegnerischen Datenbanken eine erlaubte Handlung oder einen illegalen Eingriff darstellt. Schließlich soll darauf hingewiesen werden, dass jene Staaten, die nicht über ausreichende technische IW-Kapazitäten verfügen, im Falle einer gegen sie gerichteten IO zu konventionellen Mitteln der Selbstverteidigung greifen könnten.

[52] Vgl. Prime Minister's Strategy Unit, Countries at Risk of Instability, www.strategy.gov.uk (26. 4. 2005).
[53] Vgl. Patricia Schneider/Kristina Thony/Erwin Müller (Hrsg.), Frieden durch Recht. Friedenssicherung durch internationale Rechtsprechung und Rechtsdurchsetzung, Baden-Baden 2003.
[54] Vgl. Lawrence Greenberg/Seymor Goodman/Kevin Soo Hoo, Information Warfare and International Law, www.dodccrp.org (17. 12. 2003).
[55] Vgl. Thorsten Stein/Thilo Marauhn, Völkerrechtliche Aspekte von Informationsoperationen, in: Zeitschrift für ausländisches öffentliches Recht und Völkerrecht, Nr. 60, (2000), S. 1–40.
[56] Vgl. Daniel Heller, Information Warfare und behördliche Informationsführung, in: Verein Sicherheitspolitik und Wehrwissenschaft (Hrsg.), Sicherheitspolitische Information, Zürich 2003, S. 10.
[57] Vgl. International Commission On Intervention And State Sovereignty, The Responsibility To Protect (Report), Ottawa 2001, S. 21 f.
[58] Vgl. Desmond Ball, China pursues space-based intelligence gathering capabilities, in: Jane's Intelligence Review, Dezember 2003, S. 36 ff.

Stephan Zeidler

Zensur im Internet

Das Internet hat sich zum führenden globalen Kommunikationsmedium entwickelt. In fast allen Ländern der Erde stehen Internetzugänge zur Verfügung. Nicht nur Privatpersonen nutzen das Netz, vielmehr sind es zunehmend auch Menschenrechtsorganisationen, Menschenrechtsverteidiger und Journalisten, die online Informationen aus ihren Heimatländern austauschen. Gerade der schnelle Datenaustausch wird aber von vielen Regierungen als Gefährdung der eigenen Machtposition angesehen. Daher versuchen insbesondere autoritäre und diktatorische Regime, den Zugang zum Internet zu kontrollieren und zu reglementieren.

Stephan Zeidler
Dr. phil., geb. 1969; Historiker; wissenschaftlicher Referent bei einem Mitglied des Deutschen Bundestages.
Uhlandstraße 11, 13156 Berlin.
s.zeidler@gmx.de

Grundvoraussetzung der Zensur von Internetinhalten (Content) und der Kontrolle des E-Mail-Verkehrs der Nutzer (User) sind die technischen Zugriffsmöglichkeiten staatlicher Behörden auf den Datenverkehr in einem Land. Je geringer die Zahl der Internet-Service-Provider (ISP) ist, umso größer sind für Polizei und Strafverfolgungsbehörden die Möglichkeiten, das Netz zu überwachen. Die einfachste und effektivste Kontrolle kann dann erfolgen, wenn nur derjenige einen Internetzugang erhält, der als systemtreuer Unterstützer gilt. So ist es z. B. in Turkmenistan nicht möglich, einen privaten Internetzugang zu erhalten, sodass nur wenigen tausend Menschen ein Zugriff über dienstlich genutzte Geräte möglich ist.[1]

Während diese Methode auf dem weitgehenden Ausschluss der Bürger eines Landes vom Internet beruht, sind viele Regierungen bei der Internetkontrolle „fortschrittlicher". Sie bemühen technische Methoden, um das Surfverhalten ihrer Einwohner zu regulieren und zu zensieren. Die technisch einfachste, aber auch am wenigsten effektive Methode besteht darin, dass Regierungsstellen die ISP anweisen, bestimmte Internetadressen (Domains) zu filtern und sie auf andere, regierungskonforme Seiten umzuleiten.[2] Dieses System hat sich vor allem in Usbekistan durchgesetzt, wo der staatliche Internetprovider weitgehende Kontrolle auch über andere Firmen ausüben kann.[3] Chinesische Surfer werden dagegen häufig mit technischen Fehlermeldungen konfrontiert, die dem User suggerieren sollen, dass die angeforderte Seite nicht (mehr) existiert. Allerdings lassen sich solche Manipulationen durch versierte Benutzer mit relativ wenig Aufwand umgehen.[4]

Aufwändiger ist die Filterung einzelner Seiten bzw. Seiteninhalte, die unerwünschte Texte enthalten. So lassen sich manche Seiten verschiedener Anbieter nur teilweise darstellen, und das auch nur, solange sie nicht zensierte Begriffe wie „Menschenrechte" oder „Meinungsfreiheit" beinhalten. Moderne Content-Filter-Software lässt solchen Websites keine Chance und blockiert sie sofort. Selbst per se „unpolitische" Suchportale wie Google sind etwa für Internetnutzer in China nur dann erreichbar, wenn nicht entsprechende Begriffe gesucht werden.[5] An den zentralen Übergabepunkten des chinesischen Internets setzen Filter an, um den Datenverkehr zu kontrollieren und insbesondere ausländische Seiten zu blockieren, sobald diese nicht genehmigte Inhalte anbieten. Allerdings hat sich dieses Kontrollbedürfnis der chinesischen Behörden bereits negativ ausgewirkt: Aufgrund der Vielzahl von Usern kommen die Server und Filter beim Datentransport kaum mehr hinterher, sodass das gesamte Netz in den Spitzenzeiten langsam wird, weil zu viele Daten kontrolliert und gefiltert werden müssen. Vor dem Hintergrund der wirtschaftlichen Expansion ist die eingeschränkte Nutzung des Internets in China kontraproduktiv.[6]

[1] Vgl. Reporters without Borders, The Internet under Surveillance, Turkmenistan, in: www.rsf.org/article.php3?id_article=10684.
[2] Vgl. Florian Rötzer, Verschlossene Türen im virtuellen Raum der Globalität, in: Das Parlament, Nr. 31/32 vom 26.7./2. 8. 2004, S. 18.
[3] Vgl. Reporters without Borders (Anm. 1), Uzbekistan, in: www.rsf.org/article.php3?id_article=10687
[4] Vgl. Zensur im Internet, in: http://de.wikipedia.org/wiki/Zensur_im_Internet, mit weiteren Hinweisen zur Umgehung von Zensurmethoden.
[5] Vgl. Zensierte Suche, in: Der Tagesspiegel vom 3. 10. 2004. Vgl. auch Niels Gründel, Google im Visier, in: www.netzkritik.de/art/283.shtml
[6] Vgl. Web-Zensur verlangsamt Chinas Netz, in: www.netzeitung.de/internet/229564.html.

Daneben erfolgt die Kontrolle vor allem über den Zugang zum Internet. So verpflichten viele Regierungen die ISP, genaue Aufzeichnungen über das Surfverhalten ihrer Kunden anzulegen, um entsprechende Beweise für den Besuch missliebiger Seiten zu erhalten.[7] Ein Nutzer muss damit rechnen, dass er Besuch von Polizei und Justiz erhält, wenn er sich etwa die Seiten von Menschenrechtsorganisationen oder politischen Dissidenten ansieht. Aber nicht nur das Surfen im Web, sondern auch der persönliche E-Mail-Verkehr wird häufig überwacht, um gegen Oppositionelle oder Menschenrechtsverteidiger vorzugehen. Da die meisten E-Mail-User auf den Einsatz effektiver Verschlüsselungstechniken verzichten, ist es für die Sicherheitsbehörden einfach, den E-Mail-Verkehr „abzuhören" und die Versender oder Empfänger ausfindig zu machen.

Die Lage in China

Vor allem die kommunistischen Regime in China, Nordkorea, Vietnam und Kuba verfolgen das Ziel, eine möglichst umfassende Beherrschung von Medienangeboten und Internetseiten zu erreichen. Während Nordkorea und Vietnam sich aufgrund ihrer wirtschaftlichen Struktur als ziemlich rückständig erweisen und bislang kaum auf moderne Technologien zurückgreifen können, hat China den Anschluss zum Weltmarkt gefunden und nutzt das Internet, um seine wirtschaftliche Potenz zu vergrößern. Jedoch steigt in jüngster Zeit die Zahl der Internetnutzer in China nicht mehr so rapide an. Die Gründe dafür liegen vor allem in der immer rigideren Kontrolle des Zugangs zum Internet über die Zuteilung von Anschlüssen und Nutzerberechtigungen.[8]

Doch trotz der Kontrollen ist die Zahl der Nutzer inzwischen auf fast 100 Millionen angestiegen, und ein Ende des Booms ist nicht abzusehen. Die Interessenschwerpunkte sind dabei neben kommerziellen Angeboten wie Handel oder Online-Banking auch Unterhaltung oder Jobangebote. Während solche Internetseiten von der staatlichen Zensur akzeptiert sind und keinen Verboten unterliegen, ist vor allem die Beschaffung ungefilterter Nachrichten aus dem Web heikel. Auch die Verbreitung von Informationen über das Web wird von den Behörden äußerst argwöhnisch beobachtet und führt sehr schnell zu Konflikten mit der Staatsmacht. Aufgrund zahlreicher „Gummiparagraphen" im chinesischen Strafgesetzbuch ist es leicht, Internetnutzer etwa wegen „konterrevolutionärer Vergehen", „Aufruf zur Subversion" oder „Weitergabe von Staatsgeheimnissen" zu verhaften und anzuklagen.[9]

In den neunziger Jahren hat die Regierung einen Katalog verbotener Inhalte von Websites erlassen. Unzulässig ist danach jede Information, die „(1) den in der Verfassung festgelegten Grundprinzipien widerspricht, (2) die nationale Sicherheit gefährdet, Staatsgeheimnisse preisgibt, die Regierung umstürzt, die Einheit des Landes zerstört, (3) der Ehre und den Interessen des Staates schadet, (4) zu ethnischem Hass und ethnischer Diskriminierung aufstachelt, die Einheit der Nationalitäten [Chinas] zerstört, (5) der Religionspolitik des Staates schadet, böse Kulte oder feudalen Aberglauben propagiert, (6) Gerüchte verbreitet, die gesellschaftliche Ordnung stört, die gesellschaftliche Stabilität untergräbt, (7) Unzucht, Pornographie, Glücksspiel, Gewalt, Mord, Terror verbreitet oder zu Verbrechen anstiftet, (8) andere Personen beleidigt oder verleumdet, den legitimen Rechten und Interessen anderer Personen schadet, (sowie) (9) andere Inhalte, die durch das Gesetz oder Verwaltungsvorschriften verboten sind"[10].

Ein ähnlicher Katalog mit „Bestimmungen für das Publikationswesen" wurde 1997 auch für andere Medien erlassen, um dort ebenso scharf kontrollieren zu können. Auf der Grundlage dieser Bestimmungen lässt sich in China nahezu jede oppositionelle Meinungsäußerung verbieten, da jegliche politische Handlung unter die besonders in den ersten drei Punkten aufgeführten Vergehen subsumiert werden kann.

[7] Vgl. Klaus Boldt, Ein historischer Trend, der nicht aufgehalten werden kann. Zensurversuche stoßen im Internet-Zeitalter an ihre Grenzen, in: www.epo.de/specials/zensur_internet.html.

[8] Vgl. 87 Millionen Chinesen sind online, in: www.heise.de/newsticker/meldung/49283.

[9] Vgl. Chinas Internet wächst trotz Zensur, in: www.netzeitung.de/internet/323055.html.

[10] Zit. nach Gudrun Wacker, Widerstand ist zwecklos: Internet und Zensur in China, in: Günter Schucher (Hrsg.), Asien und das Internet, Hamburg 2002, S. 70–96, Zitat: S. 77 ff.

Bereits vor einigen Jahren hat die Regierung begonnen, in Anlehnung an das berühmte historische Bauwerk eine „Great Firewall“ zu ziehen, um die Einwohner des Landes vor unerwünschten Informations- und Unterhaltungsangeboten zu „schützen“.[11] Diese „virtuelle Mauer“ versucht, den Informationsfluss ins Land zu regulieren oder gar zu unterbinden. Sie wird unterstützt durch spezielle Polizeieinheiten zur Überwachung des Cyberspace.[12] Betroffen sind vor allem ausländische Websites, da chinesische Webangebote von den Behörden registriert und genehmigt werden müssen.[13] Unter dem Vorwand des Kampfs gegen Pornographie wurden allein im Jahr 2004 mehrere tausend ausländische Internetseiten gesperrt und im Zuge der gleichen Kampagne rund 8600 Internetcafés geschlossen.[14] Während das Verbot der Pornographie jedoch nur ein Nebenschauplatz ist, um das von der kommunistischen Regierung propagierte Moralverständnis nicht zu untergraben, liegt das eigentliche Interesse der Behörden in der Überwachung von Dissidenten und kritischen Intellektuellen.

Insbesondere Veröffentlichungen mit politischen Äußerungen zur Demokratiebewegung in China oder Forderungen nach einer weiteren Öffnung des Landes führen unweigerlich zur Unterdrückung solcher Nachrichten. Noch über 15 Jahre nach der blutigen Niederschlagung der Demokratiebewegung auf dem Tiananmen-Platz in Peking sind Artikel oder Berichte über die damaligen Vorgänge strengstens verboten und führen zur Verhaftung der Autoren.[15] Auch die Beschaffung von Nachrichten aus dem Ausland wird zunehmend erschwert, seit die Zensurbehörden den Zugang zu „Google News“ blockieren. Google selbst stand in der Kritik, weil die Betreiber auf die chinesische Zensur von sich aus reagierten und für das Land nur noch eine von Google selbst zensierte Version anboten, die den Machthabern mehr zusagte. Eine ähnliche Selbstzensur ist aber auch von anderen großen Portalen wie etwa sina.com bekannt, die sich dadurch vor dem Verbot retteten.[16]

Zunehmend geraten jedoch nicht nur politisch motivierte Websites oder Nachrichten ins Blickfeld der chinesischen Zensurbehörden. Auch die Internetseiten von Kirchen und Religionsgemeinschaften – gleich welcher Ausrichtung – werden streng beobachtet, oder ein Zugriff darauf wird verhindert. Betroffen sind davon vor allem Inhalte zum tibetischen Buddhismus und dem Dalai Lama, zur Falun-Gong-Bewegung, aber auch der muslimischen Minderheit der Uiguren in der Provinz Xinjiang sowie zu anderen islamischen Organisationen, die als Gefahr für die kommunistische Regierung angesehen werden. Hinzu kommen auch weitere katholische Seiten aus dem Ausland, die häufig die mangelnde Religionsfreiheit in China kritisieren.[17]

Hier wird deutlich, welch geringen Stellenwert grundlegende, individuelle Menschenrechte wie das Recht auf freie Meinungsäußerung, Religionsfreiheit sowie Pressefreiheit in China haben.[18] Zwar schützt die Anonymität des Internets die Nutzer bis zu einem gewissen Grad, der Zwang zur Registrierung bei der Zulassung und die Kontrolle der zahllosen Internetcafés macht ein Aufrechterhalten der Anonymität und damit auch des Rechts auf freie Meinungsäußerung kaum möglich.[19] Inzwischen hat sich China nach Ansicht der Organisation „Reporter ohne Grenzen“ zum größten Gefängnis für Cyber-Dissidenten entwickelt: Allein im Jahr 2004 wurden in der Volksrepublik über 60 verhaftete Dissidenten registriert, die allein aufgrund von Internetvergehen inhaftiert worden sind.[20] Wie kritisch die Situa-

[11] Vgl. David Banisar, „Great Firewall“ in China: Dissidenten im Internet, in: www.epo.de/specials/md_firewall.html.
[12] Vgl. Gudrun Wacker, Hinter der virtuellen Mauer. Die VR China und das Internet (Berichte des Bundesinstituts für ostwissenschaftliche und internationale Studien), Köln 2000, S. 35.
[13] Vgl. Ralf Lehnert, China: Mächtige digitale Mauer, in: www.deutsche-welle.de, Meldung v. 22. 6. 2004.
[14] Vgl. China blockiert ausländische Websites, in: www.heise.de/newsticker/meldung/49381.
[15] Vgl. China geht gegen Intellektuelle wegen Internet-Artikel vor, in: www.heise.de/newsticker/meldung/54216.
[16] Vgl. China blockiert Google-News, in: www.spiegel.de/netzwelt/politik/0,1518,330328,00.html.
[17] Vgl. Felix Corley/Magda Hornemann, CHINA: Government blocks religious websites, in: http://forum18.org/Archive.php?article_id=366;
[18] Vgl. Martin Woesler, Das Internet und die Menschenrechte in China, S. 319 f., in: Hauke Brunkhorst/Matthias Kettner (Hrsg.), Globalisierung und Demokratie. Wirtschaft, Recht, Medien, Frankfurt/M. 2000, S. 310–329.
[19] Vgl. Fritjof Meyer, Chinas Staatsfeind, in: www.spiegel.de/netzwelt/politik/0,1518,2922116,00.html.
[20] Vgl. Reporters without Borders (Anm. 1), China, in: www.rsf.org/article.php3?id_article=10749.

tion ist, verdeutlicht eine Meldung von Anfang März 2005: Danach hatten chinesische Behörden einem Anwalt, der Internetautoren und -journalisten vor Gericht verteidigt hatte, ein einjähriges Berufsverbot angedroht.[21]

Die Lage in Nordkorea, Kuba und Vietnam

Vor allem Nordkorea schirmt sich gegen Einflüsse und Kontakte von und nach außen ab. Dies betrifft jedoch nicht nur Nachrichten zum Thema Internetzensur, sondern auch alle anderen Bereiche des Lebens in dem Land. Sämtliche Medien unterliegen strengster Kontrolle, und bereits kleinste Unregelmäßigkeiten bedeuten für Journalisten nicht selten Haftstrafen und Umerziehungslager.[22] Die Behörden sind nicht auf umfangreiche Zensur- und Überwachungsmaßnahmen angewiesen: Nur wenige tausend handverlesene Bürger mit Loyalität zu Staat und Partei haben überhaupt einen Zugang zum Internet oder können E-Mails nutzen. Kontakte außerhalb des Landes gibt es fast ausschließlich zu Einrichtungen in der Volksrepublik China. Für die Regierung wurde von einem deutschen Unternehmen mit dem Aufbau eines Intranets begonnen, das jedoch aufgrund deutscher Ausfuhrverbote für technische Geräte in der Bundesrepublik gehostet ist (der Server befindet sich in Deutschland), sodass die Daten per Satellit nach Nordkorea transportiert werden müssen. Wie unterentwickelt das Land in Sachen Internet ist, zeigt sich auch daran, dass der Länderdomainname .kp bisher nicht von der internationalen Vergabeorganisation ICANN registriert wurde.[23] Die gespannte politische Situation des Landes, insbesondere die Auseinandersetzung mit den USA über den Bau von Kernwaffen, lässt für die nähere Zukunft kaum eine positive Entwicklung erwarten.

Sehr ähnlich gestaltet sich auch die Situation in Kuba. Der Zugang zum Internet ist auf wenige Bürger beschränkt. Computer sind kaum zu erwerben, und der E-Mail-Verkehr wird streng überwacht. Im Jahr 2000 wurde sogar ein Ministerium gegründet, dessen Aufgabe die Überwachung und Regulierung von Netzwerken und Telekommunikation ist. Den meisten Bürgern ist nur ein von der Regierung erarbeitetes und autorisiertes Intranet zugänglich, während der Weg in das World Wide Web versperrt ist und nur Touristen offen steht.[24] Illegale Computer- und Internetnutzung wird von den Behörden streng verfolgt und geahndet.

Die Situation in Vietnam ähnelt stark der in China. Wie in dem großen Nachbarland steht die Regierung vor dem Dilemma, einerseits die Nutzung und Verbreitung des Internets zu fördern, um wirtschaftliche Vorteile zu gewinnen. Dazu wurden auch erste Breitbandverbindungen (ähnlich einer DSL-Verbindung in Deutschland) eingerichtet, um den Datentransfer zu beschleunigen und mehr User an das Netz anzubinden. Andererseits birgt jeder Ausbau die Gefahr in sich, dass oppositionelle und regimekritische Stimmen sich verbreiten. Wie China reagierte auch die vietnamesische Staatsführung mit der Einrichtung einer Spezialpolizeieinheit, um „Cyber-Kriminelle“ zu jagen.[25] So werden vor allem regimekritische Websites und Angebote von Menschenrechtsorganisationen wie Reporter ohne Grenzen durch Filter und Firewalls blockiert. Hinzu kommen Seiten von vietnamesischen Dissidenten im Exil, die die Zustände in ihrer Heimat anprangern. Um die Nutzer bereits bei der Suche nach Informationen zu lenken, haben die Zensurbehörden eine eigenständige Suchmaschine entwickelt, die gezielt zu offiziellen oder staatlich registrierten Internet-Seiten führt.

Im Frühjahr 2004 hat die vietnamesische Regierung mit einer Kampagne begonnen, um die Überwachung der Nutzer zu verschärfen. Ähnlich wie in China wird mit weit auslegbaren Paragraphen und Straftatbeständen gearbeitet, um bereits bei geringsten Vergehen mit Haftstrafen reagieren zu können. Auch hier stehen die Gefährdung der nationalen Sicherheit oder mögliche Störungen der öffentlichen Ordnung im Vordergrund, um jede kritische Äußerung zu verfolgen.[26] Besucher von Inter-

[21] Vgl. Berufsverbot für Anwalt von Internet-Autoren in China angedroht, in: www.heise.de/newsticker/meldung/56947.
[22] Vgl. Vincent Brossel, North Korea. Journalism in the service of a totalitarian dictatorship. Fact-finding mission, in: www.rsf.org.
[23] Vgl. Reporters without Borders (Anm. 1), North Korea, in: www.rsf.org/article.php3?id_article=10798.
[24] Vgl. ebd., www.rsf.org/article.php3?id_article=10611.
[25] Vgl. ebd., Vietnam, in: www.rsf.org/article.php3?id_article=10778.
[26] Vgl. Vietnam verschärft Internet-Kontrolle, in: www.netzeitung.de/internet/286405.html.

netcafés müssen sich beim Betreten registrieren lassen und ihre Ausweise vorlegen, um eine nachträgliche Identifizierung bei Aufrufen illegaler Seiten zu ermöglichen.

Aus Vietnam kamen in der jüngsten Vergangenheit wiederholt Nachrichten über die Verurteilung von Cyber-Dissidenten. So wurde 2003 ein Mann verhaftet, weil er einen Text der amerikanischen Botschaft über Demokratie in seine Heimatsprache übersetzt und über E-Mail verteilt hatte.[27] Die verschärften Zensurmaßnahmen aus dem Jahr 2004 lassen daher kaum Hoffnung zu, dass ein Wandel in absehbarer Zeit zu erwarten ist.

Arabische und islamische Staaten

Auch in vielen arabischen und islamisch geprägten Ländern hat sich die Zensur des Internets in den letzten Jahren stark ausgeweitet. Gerade diese Zensurpolitik hat die „digitale Spaltung" in Arm und Reich verstärkt. Eine von der Menschenrechtsorganisation Arabic Portal for Human Rights Information vorgelegte Studie[28] zur Nutzung des Internets in verschiedenen arabischen Staaten belegte, dass „neben Armut und Analphabetismus vor allem politische Repression für die langsame Entwicklung verantwortlich" ist.[29] Auch die Vereinten Nationen haben in einem Bericht zur Entwicklung in diesen Ländern festgestellt, dass mangelnde Bildung sowie der häufig nicht vorhandene Zugang zum Internet und die Zensur eine Ursache für das Zurückbleiben der wirtschaftlichen und gesellschaftlichen Entwicklung seien.[30]

Dagegen beschreiten Staaten wie Tunesien oder der Iran einen anderen Weg. Hier haben sich in den letzten Jahren zwar die Möglichkeiten, das Internet zu nutzen, durch zahlreiche Internetcafés oder Internetanschlüsse an Schulen und Hochschulen stark verbessert. Damit einher ging jedoch auch eine nahezu ausufernde Zensur von Websites und eine verstärkte Kontrolle der Nutzer in den Cafés. Gerade Tunesien hat sich in diesem Bereich einen zweifelhaften Ruf erworben. Zum einem hat die Regierung unter Staatspräsident Ben Ali die Infrastruktur der staatlichen Telekommunikationssysteme ausgebaut, neue Internetcafés eingerichtet und die Möglichkeiten zum Surfen erweitert. Zum anderen aber dürfen die Nutzer nur das sehen, was den staatlichen Zensurbehörden gefällt und was nicht die „nationale Sicherheit" gefährdet. Vor allem ausländische Medien mit Berichten zur Menschenrechtssituation und kritische Artikel zur Politik der Regierung werden blockiert und sind nicht frei zugänglich. Wie in vielen anderen Ländern auch ist ein Besuch eines Internetcafés nur nach behördlicher Registrierung möglich.[31] Bezug nehmend auf den recht frühen Anschluss Tunesiens an das Internet (1991) urteilte das Arabic Portal for Human Rights Information: „Tunisia: The First, The Worst."[32] Verstöße gegen die strengen Gesetze führen auch in Tunesien unweigerlich zu Verhaftungen. Erst im Frühjahr 2004 wurden mehrere Personen zu Gefängnisstrafen zwischen 19 und 26 Jahren verurteilt, weil sie verbotene Dokumente aus dem Web heruntergeladen hatten.[33]

Ähnlich scharf geht die iranische Regierung gegen Kritiker vor. Zuletzt wurden auch dort wiederholt Journalisten wegen ihrer Arbeit sowie Autoren aufgrund ihrer Veröffentlichungen in Weblogs[34] verhaftet und zu langjährigen Haftstrafen verurteilt.[35] Begründet werden Zensur und Verhaftungen auch hier mit Verstößen gegen die nationale Sicherheit oder mit der Verletzung religiöser Gefühle.[36]

[27] Vgl. Amnesty kämpft in Vietnam für Meinungsfreiheit im Internet, in: www.netzeitung.de/internet/244218.html; Der Spiegel vom 1. 9. 2003.
[28] Vgl. The Internet in the Arab World. A New Space of Repression? Overview, in: www.hrinfo.net/en/reports/net2004/intro.shtml.
[29] Vgl. Internet-Kontrolle verschärft digitale Kluft in arabischen Staaten, in: www.heise.de/newsticker/meldung/48705.
[30] Vgl. Christian Buck, UNO dokumentiert den Niedergang der Araber. Entwicklungsbericht stellt den Machthabern ein vernichtendes Zeugnis aus – Eklatante Bildungsdefizite, in: Die Welt vom 3. 1. 2004.
[31] Vgl. Ralf Lehnert, Tunesien: Schöne neue Cyberwelt?, in: www.deutsche-welle.de, Meldung vom 22. 6. 2004.
[32] The Internet in the Arab World. A New Space of Repression? Tunisia, in: www.hrinfo.net/en/reports/net2004/tunis.shtml.
[33] Vgl. Tunesisches Gericht verhängt lange Haftstrafen wegen Internet-Lektüre, in: www.heise.de/newsticker/meldung/46548.
[34] Vgl. Aktion für verhaftete iranische Blogger, in: www.heise.de/newsticker/meldung/56669.
[35] Vgl. Europas Internet-Medien fordern Freilassung von Journalisten, in: www.spiegel.de/kultur/gesellschaft/0,1518,324125,00.html.
[36] Vgl. Netz-Zensur im Iran: Kulturelle Vorbehalte, in: www.heise.de/newsticker/meldung/42865.

Geradezu absurd mutet die Situation in Saudi-Arabien an. Mit Hilfe deutscher Unternehmen[37] hat das saudische Königshaus eines der weltweit besten Filtersysteme aufbauen lassen, um große Bereiche des Internets zu sperren. Betroffen sind davon vor allem Seiten mit den Themen Politik, Sexualität, Religion und Menschenrechte.[38] Selbst unverdächtige Websites wie die des amerikanischen Musikmagazins „Rolling Stone" stehen auf dem Index. Besonders betroffen sind vor allem Seiten, die sich mit Frauenrechten oder mit Homosexualität beschäftigten. Da Letztere in Saudi Arabien verboten und mit körperlichen Strafen wie Auspeitschen bedroht ist, dürfen solche Webinhalte nicht zugänglich sein.[39] Diese Verbote werden von vielen Saudis jedoch häufig umgangen. Zwar erlauben die Filter normalerweise kaum einen Zugriff auf gesperrte Seiten. Inzwischen hat sich jedoch eine Art „Schwarzmarkt" unter Hackern ausgebreitet, die bereit sind, für ein paar Dollar Seiten zu hacken und den Lesern zugänglich zu machen. Das Hacken der Seiten ist nicht verboten und wird auch nicht verfolgt. Viele Einwohner des Landes sind auf das Netz angewiesen, da viele politische Betätigungen, aber auch zahlreiche Freizeitvergnügungen aufgrund der strengen, religiös begründeten Moralvorstellungen verboten sind.[40]

Zensur oder Freiheit?

Die Zukunft des Internets als Kommunikationsmedium, das auch politische Diskussion und kritische Berichterstattung zulässt, hängt stark davon ab, wie die Regierungen einzelner Länder mit Zensur umgehen. In den letzten Jahren hat sich der Wille zur Zensur und zur Blockade unerwünschter Inhalte eher verstärkt als abgeschwächt. Dies lässt befürchten, dass die Arbeit im Internet für Onlinejournalisten, Menschenrechtsgruppen und politische Dissidenten schwerer wird denn je. Der User unterliegt stärkeren Kontrollen und wird beim Surfen beobachtet, registriert und auch verfolgt, wenn er „illegale" Inhalte aufruft. Selbst in Ländern wie Russland, das man bereits auf dem Weg zu einer Demokratie nach westlichen Maßstäben wähnte, ist der Drang nach Zensur gewachsen.[41] In den USA wird angesichts der erhöhten Sicherheitsbedürfnisse nach den Terroranschlägen 2001 die Einschränkung von Meinungs- und Pressefreiheit von vielen Menschen kaum als Problem wahrgenommen.[42]

Dennoch ist in der politischen Diskussion die Tendenz wahrnehmbar, sich dem weltweiten Zensurproblem zu stellen und Gegenmaßnahmen zu ergreifen. Im Februar 2005 legte der Europarat einen Entwurf für eine Erklärung vor, die Menschenrechte im Internet besonders betont und zu deren Schutz aufruft.[43] Auch in Deutschland wurde ein entsprechender Antrag in den Bundestag eingebracht, aber von der Regierungskoalition zunächst abgelehnt.[44] Inwieweit die Initiative Erfolg haben wird, bleibt abzuwarten. In den USA ist man in der Diskussion schon weiter: Dort wurde bereits eine Behörde eingerichtet, die zensierte Inhalte den Bürgern anderer Länder zugänglich machen soll. Grundlage dafür ist der Global Internet Freedom Act, den zwei Kongressabgeordnete vor einigen Jahren initiiert haben.[45] Ähnliche Initiativen, die einen Zugriff auf im Ausland gesperrte Seiten ermöglichen könnten, sind in Deutschland bisher nicht zu verzeichnen.

[37] Vgl. Mit Allah und den Deutschen, in: Die Tageszeitung vom 22. 8. 2002.
[38] The Internet in the Arab World. A New Space of Repression? Saudi Arabia, in: www.hrinfo.net/en/reports/net2004/saudi.shtml.
[39] Vgl. Reporters without Borders (Anm. 1), Saudi Arabia, in: www.rsf.org/article.php3?id_article=10766.
[40] Vgl. Oliver Eberhardt, Den zensierten Internetzugang zahlt das Königshaus, in: www.telepolis.de/r4/artikel/14/14928/1.html.
[41] Vgl. Katja Seefeldt, Großreinemachen auf der Müllhalde Internet, in: www.telepolis.de/deutsch/inhalt/on/17663/1.html; Putins Pressionen. Wird nach dem Fernsehen das Internet zensiert?, in: Süddeutsche Zeitung vom 4. 6. 2004.
[42] Vgl. Florian Rötzer, Staatliche Zensur nicht so schlimm, in: www.telepolis.de/r4/artikel/19/19358/1.html; Michael Voegger, Krieg mit Filter, in: www.spiegel.de/netzwelt/politik/0,1518,330668,00.html.
[43] Vgl. Stefan Krempl, Der Europarat will die Menschenrechte im Cyberspace retten, in: www.telepolis.de/r4/artikel/19/19396/1.html.
[44] Vgl. Antrag der CDU/CSU-Fraktion, Presse- und Meinungsfreiheit im Internet weltweit durchsetzen – Journalisten, Menschenrechtsverteidiger und private Internetnutzer besser schützen, in: Bundestagsdrucksache 15/3709.
[45] Vgl. Neue US-Behörde soll Internet-Zensur anderer Nationen verhindern, in: www.heise.de/newsticker/meldung/38667.

Herausgegeben von
der Bundeszentrale
für politische Bildung
Adenauerallee 86
53113 Bonn.

Redaktion
Dr. Katharina Belwe
Dr. Hans-Georg Golz
(verantwortlich für diese Ausgabe)
Dr. Ludwig Watzal
Hans G. Bauer
Andreas Kötzing (Volontär)
Telefon: (0 18 88) 5 15-0
oder (02 28) 36 91-0

Internet
www.bpb.de/publikationen/apuz
E-Mail: apuz@bpb.de

Druck
Frankfurter Societäts-
Druckerei GmbH,
60268 Frankfurt am Main

Vertrieb und Leserservice
Die Vertriebsabteilung der
Wochenzeitung Das **Parlament**
Frankenallee 71–81,
60327 Frankfurt am Main,
Telefon (0 69) 75 01-42 53,
Telefax (0 69) 75 01-45 02,
E-Mail: parlament@fsd.de,
nimmt entgegen:

- Nachforderungen der Zeitschrift Aus Politik und Zeitgeschichte
- Abonnementsbestellungen der Wochenzeitung einschließlich APuZ zum Preis von Euro 19,15 halbjährlich, Jahresvorzugspreis Euro 34,90 einschließlich Mehrwertsteuer; Kündigung drei Wochen vor Ablauf des Berechnungszeitraumes;
- Bestellungen von Sammelmappen für APuZ zum Preis von Euro 3,58 zuzüglich Verpackungskosten, Portokosten und Mehrwertsteuer.

ISSN 0479-611 X

APuZ

Nächste Ausgabe 32–33/2005 · 8. August 2005

Bundestagswahl 2005

Sicherheit im Internet

APuZ 30 – 31/2005