Walter, Gregor

Research Report

Internetkriminalität: Eine Schattenseite der Globalisierung

SWP-Studie, No. S 16/2008

Provided in Cooperation with:
Stiftung Wissenschaft und Politik (SWP), German Institute for International and Security Affairs, Berlin

Suggested Citation: Walter, Gregor (2008) : Internetkriminalität: Eine Schattenseite der Globalisierung, SWP-Studie, No. S 16/2008, Stiftung Wissenschaft und Politik (SWP), Berlin

This Version is available at:
https://hdl.handle.net/10419/252674

SWP-Studie
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale
Politik und Sicherheit

Gregor Walter

Internetkriminalität

Eine Schattenseite der Globalisierung

S 16
Juni 2008
Berlin

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3–4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1611-6372

Inhalt

Dr. Gregor Walter ist Wissenschaftlicher Assistent an der Arbeitsstelle Transnationale Beziehungen, Außen- und Sicherheitspolitik des Otto-Suhr-Instituts für Politikwissenschaft der Freien Universität Berlin

Internetkriminalität. Eine Schattenseite der Globalisierung

Das Internet ist eine bemerkenswerte Erfolgsgeschichte. In knapp dreißig Jahren ist eine vollständig neue Kommunikationsinfrastruktur entstanden, die auf digitalem Wege inzwischen weit über eine Milliarde Menschen weltweit miteinander verbindet und aus Lebens- und Arbeitswelt kaum noch wegzudenken ist. Von den täglichen E-Mails bis zum Online-Shopping, von der Bahnauskunft bis zum »E-Learning« und vom Spiel in virtuellen Welten bis zum »Electronic Banking«: Das Internet hat vielen herkömmlichen Transaktionen eine neue digitale Plattform gegeben und es hat etliche gänzlich neue Kommunikationsformen geschaffen.

Dabei ist das Internet im Wortsinne »grenzenlos«. Es kennt kein »innen« und »außen«, keine Zöllner und Schmuggler, keine Auslandstarife und -zuschläge und auch keine der feinen Trennlinien, die unsere geographischen Weltkarten und unser politisches Denken üblicherweise strukturieren. Das Internet ist ein einziger globaler sozialer Raum, in dem täglich Milliarden von Transaktionen stattfinden – wahrhaftig ein Paradebeispiel der Globalisierung.

Dieses neue Medium hat jedoch auch seine »dunkle Seite«. Ein signifikanter Teil der oben erwähnten Transaktions- und Kommunikationsvorgänge findet in einer Grauzone statt oder ist nach nationalen oder internationalen Standards illegal. Herkömmliche kriminelle Transaktionen lassen sich nun auch digital »online« abwickeln, und auch für gesetzwidrige Handlungen hat das Internet ganz neue Kommunikationsformen geschaffen. Dementsprechend reicht das Spektrum der Internetkriminalität von auch vor dem Webzeitalter bekannten Straftaten wie Volksverhetzung und Kinderpornographie über neue Formen des Betrugs bis hin zu unerwünschten Werbe-E-Mails (»Spam«), Computerviren und Bedrohungen durch »Cyberterrorismus«, für den Informationsgesellschaften besonders anfällig sind. Dabei treffen im Internet mit Globalisierung und Digitalisierung zwei Prozesse zusammen, die jeder für sich genommen bereits die Prävention und Verfolgung kriminellen Verhaltens erschweren, sich aber in dieser negativen Wirkung auch noch wechselseitig verstärken. Ein digitales Medium macht es möglich, sehr große Informationsmengen in sehr kurzer Zeit und mit minimalem Auf-

wand zu übertragen, zu vervielfachen und zu manipulieren. Dies allein ist unter der Perspektive illegaler Transaktionsformen bereits äußerst problematisch. Es ist zum Beispiel extrem schwierig, der Flut unerwünschter Mails oder der Ausbreitung von Computerviren einen Riegel vorzuschieben. Hinzu kommt jedoch, dass das Internet einen homogenen grenzüberschreitenden Raum darstellt, in dem sich Regelungen, die für einen nationalen Handlungsraum gedacht waren, nur sehr schwer implementieren lassen.

Die vorliegende Studie widmet sich diesen »Schattenseiten« des Internets. Sie gibt einen systematischen Überblick über die verschiedenen Spielarten der Internetkriminalität. Es zeigt sich, dass bei einer ganzen Reihe verschiedener Transaktionsformen mittlerweile besorgniserregende Trends zu beobachten sind. Trotzdem ist der Versuch der Bekämpfung der verschiedenen Formen der Internetkriminalität keineswegs aussichtslos. Konkret empfiehlt die Studie, die Harmonisierung des internationalen Rechts weiter voranzutreiben und in Deutschland sowohl staatlicherseits als auch bei den entsprechenden nichtstaatlichen Initiativen Kompetenzen zu bündeln und klar erkennbare Ansprechpartner zu schaffen. Die nationalen Regelungen sollten maßvoll und unter systematischer Berücksichtigung erstens der Möglichkeiten und Grenzen der internationalen Rechtsangleichung, zweitens der Durchsetzbarkeit und drittens der Vereinbarkeit mit den zentralen Grundrechten im Informationszeitalter an die besonderen Herausforderungen durch das Internet angepasst werden.

Das Internet

Das Internet als globalisiertes Medium

Ohne weiter auf technische Details einzugehen, lässt sich konstatieren, dass das Internet zwei strukturelle Eigenschaften aufweist, die beide entscheidend dazu beitragen, dass die Bekämpfung illegaler Handlungen bzw. solcher Handlungen, die sich in einer rechtlichen Grauzone bewegen, signifikant erschwert wird: Das Internet ist zum einen ein *globalisiertes* und zum anderen ein *digitales* Medium.

Zunächst ist zu betonen, dass es sich beim Internet zwar nicht um ein globales, wohl aber um ein sehr stark *globalisiertes Medium* handelt. Ursprünglich entstanden ist das Netzwerk in den USA, wo das Pentagon Anfang der 1960er Jahre eine Möglichkeit schaffen wollte, die Großcomputer jener externen Forschungseinrichtungen miteinander zu verknüpfen, die die Aufträge der »Advanced Research Projects Agency (ARPA)« des Verteidigungsministeriums bearbeiteten.[1] Diese neue Kommunikationsform erwies sich insbesondere für Wissenschaftler als so nützlich, dass schon 1973 in London der erste internationale »Host« (Teilnehmer) dieses sogenannten »Arpanet« entstand. Dabei wurde eine universelle, kostenlos erhältliche Kommunikationssprache – das »TCP/IP-Protokoll« – verwendet, die es praktisch jedem anderen netzwerkfähigen Computer der Welt erlaubte, sich mit dem Arpanet zu verbinden. Dies machte erstmals eine Verbindung *zwischen* Computernetzen möglich; es entstand ganz wortwörtlich ein »Inter-Net«.

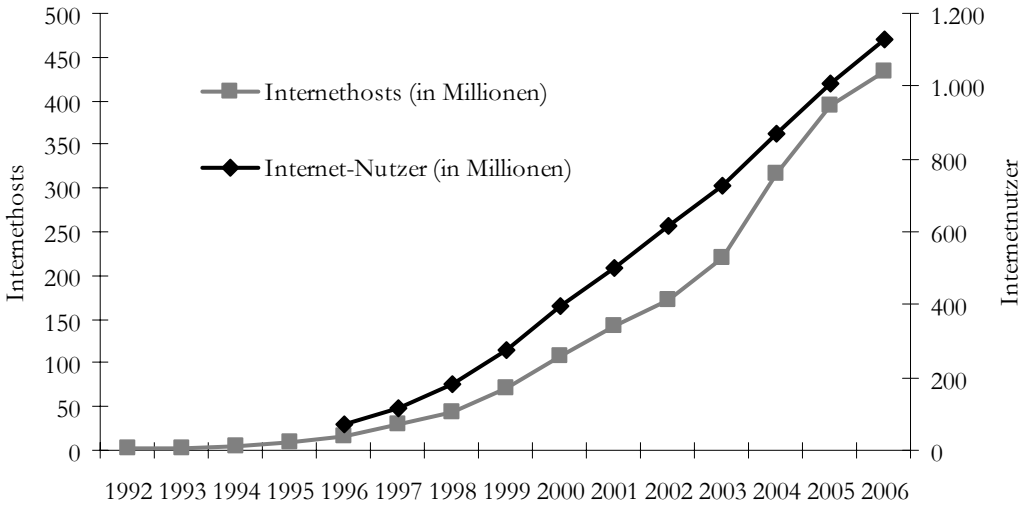
Ab den achtziger Jahren war es vor allem der internationale Wissenschaftsbereich, der die Verbreitung des Netzes stetig vorantrieb. 1991 entstand am Nuklearforschungszentrum CERN das grafikorientierte »World Wide Web« (WWW). Es stellte einen weiteren Quantensprung in der Entwicklung des Internets dar, denn es erlaubte auch Nutzern ohne jede Vorkenntnisse, auf die wachsenden Informationsressourcen des Netzes über eine einfache benutzerfreundliche Oberfläche zuzugreifen. Damit wurde zunehmend auch das enorme ökonomische Potential deutlich, das die neue Kommunikationsform für den Datenaustausch zwischen Unternehmen und Unternehmensteilen, aber insbesondere auch für Marketing, Verkauf und das Angebot verschiedenster Dienstleistungen besaß. In der Folge entstand ein neuer und äußerst dynamischer Markt, in dem jedermann gegen Gebühren Zugang zur TCP/IP-Kommunikation bzw. zum WWW erhalten konnte. Schon 1997 waren Computer aus praktisch allen Ländern der Erde mit dem Internet verbunden. Das Internet hat sich fast explosionsartig ausgebreitet und wird derzeit von weit über einer Milliarde Menschen weltweit genutzt (vgl. Schaubild 1, S. 8).

Allerdings sind diese Nutzer keineswegs gleichmäßig über den Globus verteilt. Das Internet teilt damit eine Eigenschaft anderer Globalisierungsphänomene. Zwar sind fast alle Staaten der Welt in irgendeiner Form mit dem Internet verbunden; die Anschlussdichte pro Einwohner variiert jedoch extrem stark (vgl. dazu Karte 1, S. 9). Während der Anteil der Internetnutzer in Nordamerika, Europa und Australien sehr hoch ist, sind es in Afrika und Asien hauptsächlich die Küstenstädte und internationalen Handelsgebiete, die in nennenswertem Umfang Zugang zum Web haben. Besonders in Afrika ist die Anschlussdichte – mit Ausnahme Südafrikas – sehr gering. Noch 2005 beschränkte sich beispielsweise die gesamte Verbindung der Demokratischen Republik Kongo mit ihren gut 55 Millionen Einwohnern zum Internet auf rund 163 Internethosts in Kinshasa. Dieser Umstand wird in der Regel als »Digital Divide« (oder auf Deutsch »Digitale Kluft« oder »Digitale Spaltung«) bezeichnet. Er teilt die Welt in diejenigen, die von der Informationsrevolution profitieren, und diejenigen, die nicht daran teilhaben.[2] Das Internet ist also nicht global.

1 Zur Geschichte und Entwicklung des Internets vgl. insbesondere Katie Hafner/Matthew Lyon, *Where Wizards Stay Up Late. The Origins of the Internet*, New York 1998, und Robert H. Zakon, *Hobbes' Internet Timeline v8.2*, <www.zakon.org/robert/internet/timeline/> (Zugriff 14.4.2008).

2 Der Begriff des »Digital Divide« bezieht sich daher nicht nur auf das Internet, sondern auch auf andere moderne Kommunikationsmittel wie PCs oder Handys. Teilweise wird er auch auf die hochvernetzten Länder selbst angewendet, um anzudeuten, dass auch innerhalb der betreffenden Gesellschaften die Chancen, an neuen Informationstechnologien zu partizipieren, ungleich verteilt sind, vgl. dazu z.B. Deutscher Bundestag (Hg.), *Schlussbericht der Enquete-Kommission: Globalisierung der Weltwirtschaft – Herausforderungen und Antworten*, BT-Drucksache 14/9200, 12.6.2002, S. 269–272.

Schaubild 1
Internethosts und Internetnutzer 1992–2006



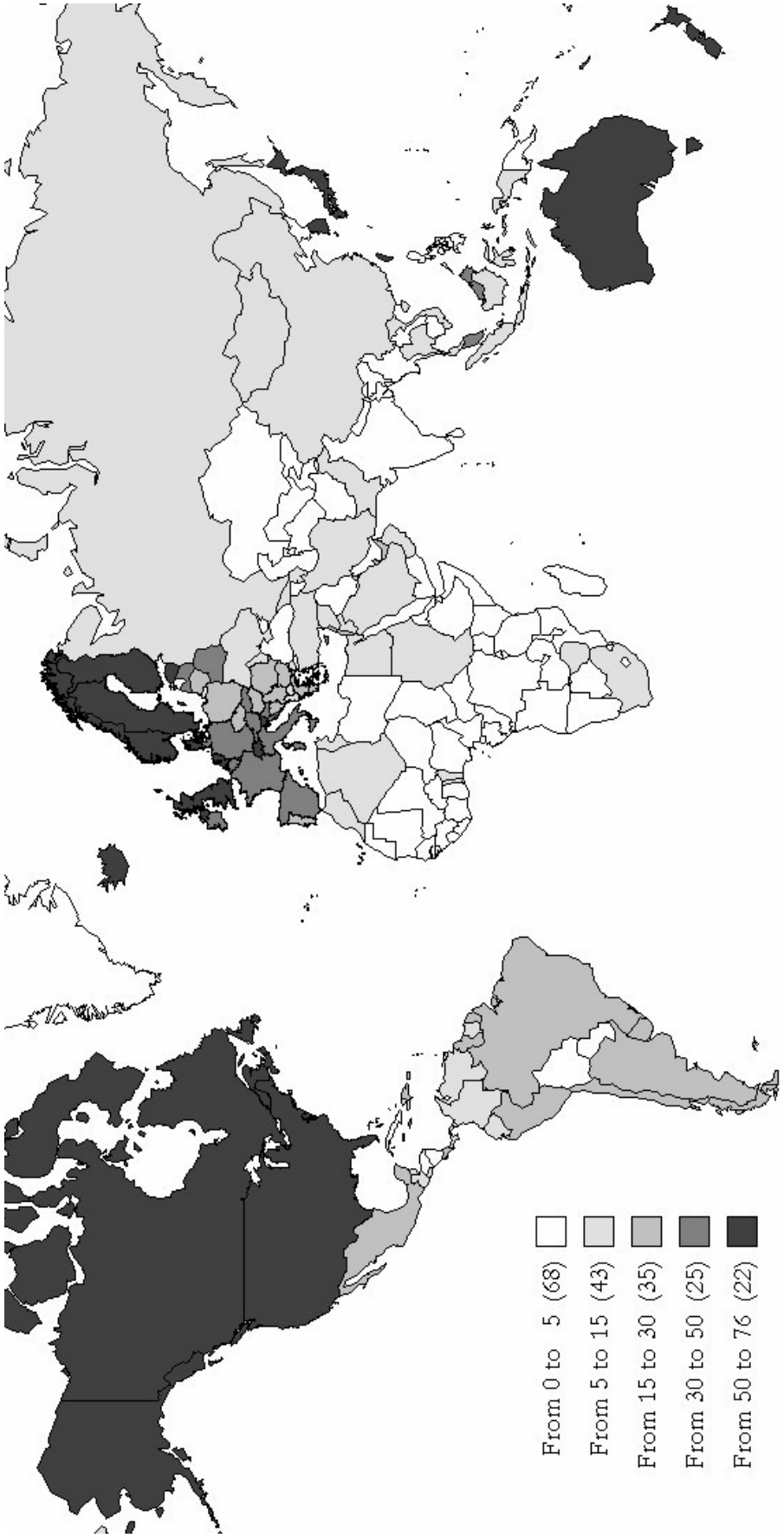
Quelle: Internet System Consortium, *ISC Internet Domain Survey*, <www.isc.org/ops/ds/> (Zugriff 14.4.2008); International Telecommunication Union, *Key Global Telecom Indicators for the World Telecommunication Service Sector*, <www.itu.int/ITU-D/ict/statistics/at_glance/KeyTelecom99.html> (Zugriff 14.4.2008).

Es ist allerdings fast vollständig *globalisiert*, denn es kennt keine nationalstaatlichen Grenzen. Dort, wo das Internet eine hohe Verbreitung hat, schafft es einen homogenen Raum, für den die herkömmlichen nationalstaatlichen Grenzziehungen keinerlei Bedeutung haben. Die Geschichte der technischen Entwicklung des Internets zeigt, dass es vor allem um die *Verbindung* von Kommunikationsnetzwerken ging und sich diese Verbindungen sehr bald wie selbstverständlich über nationale Grenzen hinweg ausbreiteten. Das war auch nicht verwunderlich, denn zwischen einer TCP/IP-Verbindung zwischen Kalifornien und New York und einer zwischen New York und London bestand technisch gesehen kein Unterschied. Anders als bei anderen Infrastrukturen gab es am Anfang keine verschiedenen nationalen Systeme (wie bei Telefon, Post, Bahn), die dann über internationale Abkommen und Standards hätten miteinander verbunden bzw. kompatibel gemacht werden müssen. Für das Internet war die Verbindung unterschiedlichster Kommunikationsnetzwerke vielmehr die zentrale *raison d'être*.

Wenn man annimmt, dass der Grad der Globalisierung über die Differenz der Kosten für binnenstaatliche und grenzüberschreitende Transaktionen sinnvoll gemessen werden kann (um wie viel teurer und aufwendiger sind z.B. Auslandsgeschäfte, internationale Telefongespräche, Auslandsreisen etc. im Vergleich zu den entsprechenden Interaktionen innerhalb eines Landes?),[3] muss man zu dem Ergebnis kommen, dass das Internet ein perfekt globalisiertes Medium darstellt. Im Internet ist die Differenz der Kosten zwischen binnenstaatlichen und grenzüberschreitenden Transaktionen null. Es ist sogar denkbar, dass der Abruf von Informationen aus einem Land mit hoher Internetanschlussdichte (wie sie z.B. in Finnland, Singapur, den Bahamas oder den USA gegeben ist) schneller erfolgt als von einem Computer im Inland, der mit nur geringer Bandbreite[4] mit dem Internet verbunden ist. Vergleicht man diese Eigenschaft mit herkömmlichen Kommunikations- und Transaktionsformen (mit Post oder Telefonie, aber auch mit internationalem Handel oder Investitionen) wird schnell deutlich, wie ungewöhnlich diese Struktureigenschaft des Netzes ist. Wir halten es für völlig normal, dass ein Brief, ein Telefongespräch, eine Reise, aber auch ein Handelsgeschäft oder ein Investitionsvorhaben deutlich teurer und aufwendiger ist, wenn das Ziel außerhalb der nationalstaatlichen Grenzen liegt, und zwar in der Regel umso teurer, je weiter die

3 Jeffrey A. Frieden/Ronald Rogowski, »The Impact of the International Economy on National Policies. An Analytical Overview«, in: Robert O. Keohane/Helen Milner (Hg.), *Internationalization and Domestic Politics*, Cambridge 1996, S. 26.
4 Unter »Bandbreite« versteht man die Geschwindigkeit, mit der Daten in einem Netzwerkabschnitt übertragen werden können.

Karte 1
Internetnutzer in Prozent der Bevölkerung (2005)



Quelle: International Telecommunication Union, *ITU ICT Eye*, <www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx> (Zugriff 14.4.2008)

entsprechende Transaktion reicht. Das Internet dagegen ist ein einziger Handlungsraum, dessen Grenzen nicht nur über den Nationalstaat hinausreichen, sondern völlig unabhängig von den nationalstaatlichen Grenzen sind und sich allein durch den globalen »Digital Divide« definieren. Das Internet hat somit eine Struktur, die unserer gängigen politisch-geographischen Vorstellung der Welt gänzlich widerspricht. Hinzu kommt, dass das Internet von Anfang an anders als andere Infrastruktursysteme nicht in der Regie staatlicher Institutionen stand. Der ursprüngliche Auftrag des Pentagon spielte in der weiteren Entwicklung des Internets nur noch pro forma eine Rolle. Die Wissenschaftler und Unternehmen, die zu seiner Ausbreitung maßgeblich beitrugen, agierten abseits aller staatlichen Regulierungsbehörden.

Im Hinblick auf »graue« oder illegale Transaktionen hat dieser Charakter des Internets als globalisiertes Medium eine Reihe von problematischen Implikationen: *Erstens* existieren weder physisch-geographische noch irgendwelche anderen Grenzlinien, an denen sich Kommunikationstransaktionen innerhalb des Internets in irgendeiner Form kontrollieren ließen. Die Möglichkeit einer »Grenz-« oder »Zollkontrolle« wie in der physischen Welt beim Warenhandel oder bei Reisen und Verkehr besteht dort nicht. *Zweitens* gibt es auch keine wie immer geartete zentrale Organisation, die in irgendeiner Form als Kontrollinstanz agieren könnte, denn das Internet funktioniert, ohne dass es ein Äquivalent zu den ehemals staatlichen nationalen Post- oder Telekommunikationsunternehmen oder den entsprechenden Regulierungsbehörden gäbe.[5] Gleichzeitig existiert *drittens* eine fundamentale Diskrepanz zwischen dem homogenen Raum »Internet« und den rechtlich und politisch völlig inhomogenen Räumen, in denen die Nutzer »offline« leben. Das Internet »schließt« die Rechtssysteme der beteiligten Länder quasi »kurz«. Was nach den Regeln eines Staates legal ist, kann nach denen eines anderen illegal sein. Solange diese Rechtsräume halbwegs voneinander getrennt sind oder sich an ihren Grenzen kontrollieren lassen, ist das unproblematisch. Ein einziger, gemeinsamer Transaktionsraum mit unterschiedlichen Normen schafft jedoch automatisch zahlreiche Schwierigkeiten und Konflikte.

5 Es gibt zwar mit der Internet Corporation for Assigned Names and Numbers (ICANN) eine äußerst interessante hybride staatlich-nichtstaatliche Organisation, die sich mit zentralen Internetbelangen befasst, aber deren Autorität bezieht sich nur auf sehr wenige, eher technische Regelungsprobleme.

Und *viertens* schließlich sind die Akteure des homogenen Raums »Internet« gegenüber den weitgehend national gebundenen Justiz- und Polizeibehörden deutlich im Vorteil. Während beispielsweise eine illegale Transaktion durch nur wenige Mausklicks Dutzende von Grenzen überschreiten kann, steigt der Aufwand bei der Strafverfolgung exponentiell.

Das Internet als digitales Medium

Zu diesem globalisierten Charakter des Internets kommt ein zweites, mindestens ebenso ambivalentes Strukturmerkmal. Das Internet ist ein computerbasiertes Netzwerk, das Informationen in digitaler Form elektronisch verarbeitet. Diese »digitale Welt« hat eine Reihe von Eigenschaften, die sie gegenüber der »normalen Welt« absetzen:

Erstens gilt für digitale Daten eine sehr hohe *Verarbeitungs- und Transportgeschwindigkeit*. Ein Mikroprozessor in einem derzeit handelsüblichen Computer für den Massenmarkt führt mehrere Milliarden Maschinenbefehle pro Sekunde aus und verfügt über Speicherkapazitäten im Bereich von Dutzenden von Milliarden Zeichen (äquivalent in etwa einer Etage in einer Bibliothek). Gleichzeitig stehen in einem Land wie Deutschland für Privatnutzer mittlerweile praktisch flächendeckend Anschlussmöglichkeiten an das Internet zur Verfügung, die Transferraten von über 350 000 Zeichen pro Sekunde bewältigen. Das entspricht dem Text der Bibel in circa zehn Sekunden. Zweitens besteht bei digitalen Daten die Möglichkeit der *uneingeschränkten Vervielfachung*. Das bedeutet, dass von jedem Datensatz mit sehr geringem Aufwand Kopien hergestellt werden können, die weder das Original beeinträchtigen noch zu einem Qualitätsverlust bei der Kopie führen. Drittens zeichnen sich digitale Daten – die entsprechende technische Expertise vorausgesetzt – durch *leichte Manipulierbarkeit* aus. Es ist gerade einer der zentralen Vorteile digitaler Technologie, dass Informationen sehr leicht modifiziert, ergänzt oder gelöscht werden können. Auch hier sind die entsprechenden Transaktionskosten aufgrund der inzwischen hoch entwickelten Datenverarbeitungstechnik ausgesprochen gering.

Bei der Bewertung der Tragweite dieser Eigenschaften muss zusätzlich berücksichtigt werden, dass heute immer mehr Informationen in digitaler Form vorliegen oder sich leicht digitalisieren lassen. Das gilt zum einen für Medien wie Bücher und Schriften, Tondokumente, Bilder, Filme, TV-Programme und andere,

die durch die Digitalisierung zu immateriellen Gütern werden. Zum anderen liegen immer mehr persönliche Daten (Bank- und Kreditkarteninformationen, medizinische Informationen, Versicherungsinformationen u.Ä.) in digitaler Form vor und werden immer mehr Produktions- und Verwaltungsprozesse auf Basis digitaler Daten gesteuert. Das Ausmaß der Digitalisierung illustriert eine Schätzung, wonach bereits 2002 weltweit auf Computerfestplatten 1200 mal mehr neue Informationen generiert wurden als in allen Papiermedien (Bücher, Zeitungen, Zeitschriften, Bürodokumente etc.) zusammen.[6] Für das Internet als digitales Medium bedeutet dies, dass gewaltige Mengen dieser Informationen in kurzer Zeit versendet, vervielfacht, verarbeitet und – von Experten – auch manipuliert werden können. Die entsprechenden Transaktionen sind nur mit erheblichem Aufwand und Fachwissen zu kontrollieren. Hinzu kommt, dass es ein grundsätzliches Gefälle zwischen der Geschwindigkeit digitaler Transaktionen und polizeilichen Kontroll- und Sanktionsmechanismen gibt, die – aus guten Gründen – ihrerseits rechtsstaatlichen Kontrollmechanismen unterliegen und daher Zeit benötigen. Der digitale Charakter des Internets schafft daher günstige Voraussetzungen für die Herausbildung einer »Dunkelzone« außerhalb der Reichweite der etablierten Kontroll- und Sanktionsmechanismen von Polizei und Justiz.

Zusammenfassend lässt sich festhalten, dass das Internet sowohl als globalisiertes wie auch als digitales Medium zu charakterisieren ist. Vom Standpunkt der Prävention bzw. Sanktionierung halblegaler oder illegaler Transaktionen ist jede dieser beiden Eigenschaften für sich genommen bereits problematisch. Hinzu kommt jedoch, dass sie sich gegenseitig verstärken. Die Geschwindigkeit und Leichtigkeit, mit der digitale Daten verarbeitet, versendet, vervielfacht und manipuliert werden können, ist unter dem Gesichtspunkt der Strafverfolgung umso problematischer, wenn die Verarbeitung und Manipulation an wechselnden geographischen Orten unter Einbeziehung von Computern in allen möglichen Ländern stattfinden können. Kurzum, die Digitalität alleine erzeugt schon günstige Bedingungen für die Ausbreitung einer Dunkelzone an Transaktionen. Nimmt man den globalisierten Charakter des Internets hinzu, bedeutet dies, dass diese Dunkelzone in einem »grenzenlosen« Raum jenseits der unterschiedlichen Rechts- und Sanktionssysteme liegt, in dem geographische Orte oder Entfernungen eine völlig untergeordnete Rolle spielen und die typischerweise an einzelstaatliche Strukturen gebundene Maßnahmen zur Strafprävention und Strafverfolgung erheblich erschwert.

6 Vgl. Peter Lyman/Hal R. Varian, *How Much Information?*, Berkeley 2003, <www2.sims.berkeley.edu/research/projects/how-much-info-2003/> (Zugriff 14.4.2008).

Formen der Internetkriminalität

Im Folgenden wird konkretisiert, welche problematischen Transaktionsformen es im Internet gibt, und gleichzeitig bewertet, wie schwerwiegend diese jeweils sind. Der Begriff der »Kriminalität« wird dabei bewusst weit gefasst und bezieht sich hier nicht nur auf strafrechtlich relevante Tatbestände, sondern auch auf andere Deliktsformen, die in das Privatrecht hineinreichen. Es geht also ganz allgemein um Regelverletzungen im Internet.

Einschränkend muss noch vorausgeschickt werden, dass es schwierig ist, verlässliche (und idealiter international vergleichbare Daten) zu den unterschiedlichen Problembereichen zu finden. Das erklärt sich zum einen mit der globalisierten Struktur des Netzes (es gibt eben keine Zentralinstanz, die entsprechende Daten erheben könnte), zum anderen sind sich Beobachter darüber einig, dass bei der Internetkriminalität eine erhebliche Dunkelziffer existiert, da nur ein Bruchteil der problematischen Transaktionen in irgendeiner Form aktenkundig wird und/oder in Statistiken auftaucht.[7] Man kann also davon ausgehen, dass es sich bei den hier präsentierten Daten zumeist um eher zurückhaltende Schätzungen handelt.

Die Formen von Regelverletzungen im Internet sind sehr vielfältig. Zur besseren Übersicht soll daher die folgende Systematisierung dienen, die zum einen nach der Motivation derjenigen fragt, die entsprechende Transaktionen vornehmen, und zum anderen danach unterscheidet, welche Rolle das Internet für eine solche Transaktion spielt. Was die Motivation angeht, so kann zwischen *ökonomischen* und *nichtökonomischen* Intentionen unterschieden werden. Das Internet kann in beiden Fällen entweder nur als *Medium* für eine Art von Transaktion dienen, die prinzipiell auch »offline« durchgeführt werden könnte, oder es ist selbst *Zentrum und Ziel* der entsprechenden Handlungen. Kreuzt man diese beiden Dimensionen, ergeben sich vier Typen der Internetkriminalität, die in Tabelle 1 systematisiert dargestellt sind.

Tabelle 1
Systematik von Formen der Internetkriminalität

		Rolle des Internets	
		Medium	*Zentrum/Ziel*
Motivation	*Ökonomisch*	»Traditionelle« Kriminalität	Internetkriminalität i.e.S.
	Nichtökonomisch	Inhaltsbezogene Rechtsverletzungen	Cyberterrorismus

Traditionelle Kriminalität via Internet

Bei ökonomisch motivierter, »traditioneller« Kriminalität via Internet handelt es sich einerseits um Formen von Betrug und Fälschung, wie sie auch bei Transaktionen außerhalb des Internets vorkommen, und andererseits um Urheberrechtsverletzungen. Bei *Betrug und Fälschung* fungiert das Internet lediglich als Medium des eigentlichen Vorgangs. Den Tätern geht es um die Erzielung eines finanziellen Vorteils, der sich »offline« in Bargeld umsetzen lässt. In diesem Fall macht sich der digitale Charakter des Netzes besonders stark bemerkbar: Vor allem die Manipulierbarkeit elektronischer Daten, gekoppelt mit der hohen Anzahl von ökonomischen Transaktionen, die über das Internet ablaufen, und der relativen Anonymität des Netzes, eröffnet hier bei entsprechender krimineller Energie und entsprechendem technischen Sachverstand große Möglichkeiten. Der globalisierte Charakter des Internets verschärft das Problem, da sich die Täter gezielt grenzüberschreitender Handlungsformen bedienen können, um den Nachvollzug ihrer Aktivitäten zu erschweren. Unter diese Formen »traditioneller« Kriminalität fällt neben Betrug und Fälschung in Zusammenhang mit Kreditkarten, »Debitkarten« (wie EC-Karten), manipulierten Rechnungen, zweifelhaften Warenangeboten oder betrügerischen Versteigerungen (Online-Auktionen) auch Geldwäsche. Zumindest teilweise ist dabei auch von Organisierter Kriminalität auszugehen. Der Einfallsreichtum der Betrüger ist groß. Ein bekanntes Beispiel ist die Methode der sogenannten »Nigeria-Connection«: Per E-Mail bieten Unbekannte den Empfängern an, vom Transfer von

7 Vgl. z.B. »›Ein riesiges Dunkelfeld‹. Kriminalität im Internet« [Interview mit dem Kriminologen Frank Robertz], in: *Süddeutsche Zeitung*, 10.1.2007, <www.sueddeutsche.de/computer/artikel/655/97558/> (Zugriff 14.4.2008).

Millionensummen illegaler Gelder aus Afrika zu profitieren, wobei sich nach der Anbahnung des Kontakts herausstellt, dass in Vorleistung gegangen werden muss, um die Kosten des Transfers abzudecken.[8] Andere Verfahren sind raffinierter und machen sich systematisch den grenzüberschreitenden Charakter von Internettransaktionen zunutze. So melden sich zum Beispiel beim Online-Warenverkauf Interessenten aus dem Ausland, bieten einen guten Preis und zahlen per Scheck, der sich nach Übergabe der Ware als ungedeckt herausstellt. Das Problem liegt hierbei darin, dass internationale Schecks zunächst vorläufig gutgeschrieben werden und für den Verkäufer damit alles in Ordnung scheint, während sich die Banken vorbehalten, die Gutschrift bei negativer Prüfung rückgängig zu machen. Eine solche Prüfung dauert im grenzüberschreitenden Bankverkehr jedoch in der Regel sehr lange, so dass die Übergabe der Ware häufig längst erfolgt ist.[9]

Wie aber unterscheidet sich »traditioneller«, ökonomisch motivierter Betrug von den entsprechenden Internetdelikten? Beide Kriminalitätsformen sind in der Tat schwierig voneinander abzugrenzen, weil die eine sich eben nur darin abhebt, dass das Internet hier als ein spezielles Kommunikationsmittel eingesetzt wird. In den USA wird diese Unterscheidung durch die Nutzer selbst vorgenommen: Dort existiert – auf der Basis einer Kooperation zwischen dem FBI und dem National White Collar Crime Center (NW3C) – ein »Internet Crime Complaint Center« (IC3), dem individuelle Beschwerden über Internet-Betrugsfälle gemeldet werden können und das diese Anzeigen nach einer Vorprüfung an die zuständigen Justizverfolgungsbehörden weiterleitet. Die Zahl der beim IC3 eingegangenen Klagen über Betrug hat sich von anfänglich rund 17 000 auf mittlerweile deutlich über 200 000 pro Jahr gesteigert, wobei die geschätzte Schadenssumme 2006 bei knapp 200 Millionen US-Dollar lag.[10] Die Federal Trade Commission (FTC) hat mit dem »Consumer Sentinel« schon Ende der neunziger Jahre ebenfalls eine Beschwerdestelle eingerichtet. Sie kommt auf ähnliche Fallzahlen wie das IC3, schätzt aber die Schadenssumme mit fast 600 Millionen US-Dollar bedeutend höher.[11]

In Deutschland erfasst die Polizeiliche Kriminalstatistik des Bundeskriminalamts seit 2004 gesondert Straftaten mit dem »Tatmittel Internet«. Allerdings ist die entsprechende Klassifizierung bisher noch nicht in allen Bundesländern umgesetzt worden. Die vorliegenden Zahlen zeigen jedoch, dass zwischen 2005 und 2006 der Anteil des Internet-Betrugs an allen Betrugsdelikten deutlich gestiegen ist und mittlerweile bei 13 Prozent liegt (in der Unterkategorie des Warenbetrugs sogar bei 63%).[12] Diese Zahlen legen nahe, dass der schon länger beobachtete Trend einer Zunahme der Betrugsdelikte (die diesbezüglichen Fallzahlen der Kriminalstatistik haben sich zwischen 1993 und 2005 fast verdoppelt) auch etwas mit der Verbreitung des Internets zu tun hat. Bemerkenswert ist dabei, dass diese Daten vor dem Hintergrund einer allgemein stagnierenden oder sogar rückläufigen Entwicklung der Gesamtzahl der Straftaten in der Kriminalstatistik zu sehen sind.[13] Dies lässt vermuten, dass die relative Bedeutung des Betrugs mit der kontinuierlichen Ausdehnung des »E-Commerce« weiter ansteigen wird. Der Befund deutet jenseits der absoluten Zahlen auch darauf hin, dass in dem Maße, wie sich ökonomische Aktivitäten ins Internet verlagern, der Anteil krimineller Transaktionen steigt, da die Voraussetzungen dafür im »Cyberspace« besonders günstig sind.

Urheberrechtsverletzungen sind die zweite, innerhalb des Internets besonders virulente Deliktgruppe, die in den Bereich der »traditionellen Kriminalität« fällt. Sie beziehen sich auf Mediendaten aller Art (Textdokumente, Musik, vor allem im sogenannten »MP3«-Format[14], und Filme) sowie auf Software. Das Internet ist

8 Bundeskriminalamt, *Erhalt betrügerischer Angebotsschreiben*, Wiesbaden 2007, <www.bka.de/profil/faq/hinweise/angebot.html> (Zugriff 14.4.2008).

9 Bundeskriminalamt, *Warnung vor Betrug beim Auto-Verkauf / Bezahlung mit ungedeckten Schecks*, Pressemitteilung vom 13.8.2004, Wiesbaden, <www.bka.de/pressemitteilungen/2004/pm130804.html> (Zugriff 14.4.2008).

10 Internet Crime Complaint Center, *Internet Crime Report 2006*, <http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf> (Zugriff 14.4.2008).

11 Federal Trade Commission, *Consumer Fraud and Identity Theft Complaint Data*, Washington 2007, <www.consumer.gov/sentinel/trends.htm> (Zugriff 25.7.2007).

12 Bundeskriminalamt, *Polizeiliche Kriminalstatistik 2006*, Wiesbaden 2006.

13 Vgl. Werner Rüther, »Betrugsdelikte im Internet. Zum aktuellen Stand des empirischen Wissens aus kriminologischer Sicht«, in: Deutsches Forum für Kriminalprävention (Hg.), *Internet-Devianz*, Berlin 2006, S. 70–72.

14 »MP3« bezeichnet ein ursprünglich vom Fraunhofer-Institut in Erlangen entwickeltes Kompressionsverfahren, das es möglich macht, die Dateigröße von Musikstücken ohne merklichen Qualitätsverlust auf bis zu 10% des Ausgangsniveaus zu reduzieren. Dadurch werden Speicherung, Kopie und Transfer im Vergleich zur CD erheblich vereinfacht (mit allen entsprechenden Konsequenzen für den Urheberrechts-

sowohl für Software als auch für Medien ein idealer Verteilungs- und Transportkanal. In vielen Fällen wirkt sich das für die Urheber jedoch negativ aus, weil ihre geistigen Leistungen zwar weit verbreitet werden, es ihnen jedoch nicht gelingt, ihre Rechte geltend zu machen. Urheberrechtsverletzungen sind im Sinne der obigen Systematik der »traditionellen« Kriminalität strukturell ähnlich: Das Internet dient auch hier primär als Transportmedium und die Motivation ist zumeist ökonomisch. Die meisten Urheberrechtsverletzungen in Form von illegalen Kopien werden allerdings nicht begangen, weil die Täter einen kurzfristigen Gewinn suchen, sondern weil sie Kosten vermeiden wollen.

Der digitale Charakter des Internets ist hier von besonderer Relevanz. In kürzester Zeit können illegale Kopien von Software oder Medien ohne Qualitätsverlust millionenfach hergestellt und weltweit verteilt werden. Ende der neunziger Jahre wurde die Internet-Musiktauschbörse »Napster« zum Schlagwort für das, was manche als den Anfang vom »Ende der Musikindustrie«[15] sehen. Beim Medium Film dominieren wegen der Datenmenge bislang noch Kopien von DVDs (»Hard Goods Piracy«), [16] aber seit Anfang der 2000er gibt es auch in diesem Bereich sogenannte »Peer-to-Peer«-Netzwerke, in denen jeder Teilnehmer gleichzeitig Anbieter und Nachfrager ist und keine Abhängigkeit von einem zentralen Server existiert. Dadurch können auch sehr große Datenmengen sehr schnell verteilt werden und eine Kontrolle an einem zentralen Server (wie noch bei Napster) ist nicht mehr möglich. Der globalisierte Charakter des Netzes wirkt auch hier problemverschärfend: Zum einen, weil Reichweite und Potential des Verteilungsnetzes erheblich erhöht werden; zum anderen aber auch, weil die urheberrechtlichen Regelungen und ihre Grenzen bzw. Ausnahmen nicht in allen Ländern den gleichen Prinzipien folgen.[17]

Über das Ausmaß dieses Phänomens liegen eine ganze Reihe von Daten vor, die zumeist von den betroffenen Industriezweigen selbst stammen und von neutralen Beobachtern daher zum Teil als fragwürdig eingestuft werden. Das Grundproblem besteht darin, dass unklar ist, inwieweit der Nutzer einer Raubkopie ein legaler Kunde hätte sein können. Die Business Software Alliance (BSA) beispielsweise, ein Verband der weltgrößten Softwarehersteller, nennt für den Bereich *Software* die gewaltige Zahl von weltweit 40 Milliarden US-Dollar Verlust (»loss«), der allein im Jahr 2006 durch Softwarepiraterie »online« und »offline« entstanden sei. Über 1,6 Milliarden sollen die Schäden allein in Deutschland betragen.[18] Erstens wäre eine bessere Formulierung als »Schaden« wohl »entgangener Umsatz« und zweitens gibt es deutliche Hinweise darauf, dass diese Zahlen viel zu hoch angesetzt sind.[19] Was die *Musiksparte* betrifft, geht die International Federation of the Phonographic Industry (IFPI) bei ihren Schätzungen etwas vorsichtiger vor. Sie berechnet nicht die finanziellen Einbußen, sondern nur den Umsatz an Musiktiteln, und kommt so zu dem Schluss, dass 2005 etwa 20 Milliarden Titel weltweit illegal aus dem Internet bezogen wurden, sei es über Websites, »Peer-to-Peer«-Börsen oder über andere Kanäle.[20] Für Deutschland liegen die entsprechenden Zahlen (die zumeist auf Umfragen beruhen) bei mehreren Hundert Millionen, wobei die Zahl der Personen, die illegale Downloads durchführen, mit deutlich über sieben Millionen (fast 9 Prozent der Bevölkerung!) angesetzt wird.[21] Einige Studien kommen zu dem Ergebnis, dass der Musikmarkt zwischen 1998 und 2002 weltweit durch Internet-Downloads um 20 Prozent

schutz).

15 Janko Röttgers, *Mix, Burn & R.I.P. – Das Ende der Musikindustrie*, Hannover 2003.

16 2005 beispielsweise stammten in Deutschland »nur« 19% der gebrannten Spiel- oder Kinofilme von Internettauschbörsen oder Homepages bzw. Webservern, vgl. dazu Filmförderungsanstalt, *Brennerstudie 2005. Kopieren und Download von Spiel-/Kinofilmen*, Berlin 2006, <www.ffa.de/downloads/publikationen/brenner_studie4.pdf> (Zugriff 14.4.2008).

17 So knüpft das Urheberrecht wortwörtlich am Schöpfer eines Werkes an, während das im angloamerikanischen Raum geläufige »Copyright« sich stärker auf eine Verwertungsperspektive bezieht.

18 Business Software Alliance (BSA), *Fourth Annual BSA and IDC Global Software Piracy Study*, <http://w3.bsa.org/globalstudy//upload/2007-Global-Piracy-Study-EN.pdf> (Zugriff 14.4.2008).

19 Der Verlust wird dabei über die Divergenz zwischen PC-Verkäufen und Softwareverkäufen geschätzt. Aus den legal betriebenen PCs wird ein »Mittelwert« der Softwareausstattung ermittelt und auf die Zahl aller verkauften PCs angewendet. Der Vergleich mit den tatsächlichen Software-Verkäufen ergibt dann denn Verlust. Es ist allerdings äußerst fragwürdig, ob dieser »Mittelwert« tatsächlich für alle PCs plausibel ist, vgl. »Dodgy Software Piracy Data«, in: *The Economist*, 19.5.2005.

20 International Federation of the Phonographic Industry (IFPI), *The Recording Industry 2006 Piracy Report. Protecting Creativity in Music*, London 2006.

21 IFPI, *Internet Piracy in Germany*, 2005, <www.ifpi.org/content/section_news/20050412i.html> (Zugriff 25.7.2007).

geschrumpft ist;[22] im Hinblick auf Deutschland berichtet die IFPI sogar von Rückgängen um 30 Prozent zwischen 1997 und 2004.[23] Allerdings sind auch diese Werte äußerst umstritten, und es gibt Experten, die bestreiten, dass es überhaupt einen statistisch nachweisbaren Zusammenhang zwischen Download-Verhalten und dem Kauf von Musik-CDs gibt.[24] Die Verluste durch Internetpiraterie im Bereich *Film* werden von der Motion Picture Association (MPA), dem Dachverband der Film- und Fernsehindustrie, auf Basis von Umfragen unter ihren Mitgliedsfirmen auf 2,3 Milliarden US-Dollar taxiert.[25] Wird die gesamte Wertschöpfungskette (Distributoren, Kinos, Videoverleih und »Pay-per-view«) miteinbezogen, so summiert sich der entgangene Umsatz nach Berechnungen der MPA sogar auf 7,1 Milliarden US-Dollar. Die entsprechenden Zahlen für Deutschland liegen bei insgesamt über 180 Millionen US-Dollar.

Zusammenfassend lässt sich festhalten, dass sowohl bei Software als auch bei Medien Raubkopien millionenfach im Internet kursieren bzw. über das Internet verteilt werden. Urheberrechtsverletzungen sind mit Hilfe des Internets, vor allem in jüngeren Bevölkerungskreisen, zum Massendelikt geworden. Die Höhe der dabei entstehenden Schäden für die betroffenen Wirtschaftszweige ist stark umstritten. Während die Industrie mit sehr hohen Zahlen operiert, scheint sich unter den damit befassten Wissenschaftlern ein Konsens abzuzeichnen, wonach illegale Downloads zwar in der Tat die Produzenten schädigen, aber in weit geringerem Umfang als üblicherweise von den Unternehmen selbst angenommen.[26] Unstrittig ist die Einschätzung, dass sich das Problem mit der weiteren weltweiten Verbreitung des Internets und der steigenden Verfügbarkeit von Breitbandzugängen verschärfen wird.

Inhaltsbezogene Rechtsverletzungen

Diese Art von Rechtsverletzungen bezieht sich auf die Inhalte, die über das Internet kommuniziert werden, sei es als Text, Bild, Ton oder Film. Solchen Inhalten sind – trotz des in westlichen Demokratien universellen Prinzips der Meinungsfreiheit – legale Schranken gesetzt. Im Kontext des Internets sind dabei zwei Arten von Inhalten besonders relevant, denen gemeinsam ist, dass erstens die Motivation der Rechtsverletzung im Unterschied zur traditionellen Kriminalität zumeist nicht ökonomischer Natur ist und zweitens das Internet – anders als bei der Internetkriminalität im engeren Sinne – primär als Transportmittel dient. Zum einen geht es um politisch motivierte Äußerungen, insbesondere um rechts- und linksextremistisches Propagandamaterial, Aufstachelung zum Rassenhass, Herabwürdigung und Diskriminierung von Minderheiten oder Informationen über terroristische Methoden, und zum anderen um sexuell motivierte Kommunikation, wobei im Zusammenhang mit dem Internet Kindesmissbrauch und Kinderpornographie besondere Aufmerksamkeit erfahren haben, aber auch andere Pornographieformen eine Rolle spielen. Auf der Seite der Anbieter liegen dabei durchaus auch ökonomische Motive vor, aber das Ausmaß des Problems lässt sich nur mit der sexuellen Motivation der Nutzer erklären.

Beide Arten inhaltsbezogener Rechtsverletzungen sind nicht neu. In der historischen Entwicklung sind die Grenzen dessen, was an politischen oder sexuellen Inhalten uneingeschränkt kommuniziert werden kann, immer wieder anders gezogen worden. Quasi parallel dazu hat es immer Versuche gegeben, die entsprechenden Verbotslinien zu überschreiten, und diese Versuche haben sich auch immer jener »modernen« Kommunikationsmittel bedient, die in der jeweiligen Epoche zur Verfügung standen.[27] Auch Kinderpornographie und die Verletzung des Jugendschutzes sind nicht erst seit dem Internet ein signifikantes Problem, und auch bei der politisch motivierten Kommunikation gab es schon in der Vergangenheit immer wieder Rechtsverletzungen. So galt das benachbarte Dänemark mit seiner vergleichsweise liberalen

22 Martin Peitz/Patrick Waelbroeck, »The Effect of Internet Piracy on Music Sales: Cross Section Evidence«, in: *Review of Economic Research on Copyright Issues*, 1 (2004) 2, S. 71–79.
23 IFPI, *Internet Piracy in Germany* [wie Fn. 21].
24 Felix Oberholzer/Koleman Strumpf, »The Effect of File Sharing on Record Sales. An Empirical Analysis«, in: *Journal of Political Economy*, 115 (2007) 1, S. 1–42.
25 Motion Picture Association (MPA), *The Cost of Movie Piracy*, 3.5.2006, <www.mpaa.org/leksummaryMPA%20revised.pdf> (Zugriff 14.4.2008).
26 Daniel Gross, »Does a Free Download Equal a Lost Sale?«, in: *The New York Times*, 21.11.2004.

27 Manche Historiker gehen so weit zu behaupten, dass insbesondere sexuell motivierte Kommunikation schon seit den Zeiten des Buchdrucks ein Motor der technologischen Innovation in der Kommunikationstechnik gewesen sei, vgl. Jonathan Coopersmith, »Pornography and Progress«, in: *ICON* (published by the International Committee for the History of Technology), 4 (1998), S. 94–125.

Gesetzgebung bereits vor der Ausbreitung des Internets als »Einfallstor« für den Schmuggel rechtsradikalen Propagandamaterials nach Deutschland.[28] Neu ist jedoch, dass durch das Internet sowohl die Transaktionskosten als auch das Strafverfolgungsrisiko für inkriminierte Kommunikationsformen stark gesunken sind. Das Netz ist dabei von ganz besonderer Brisanz, weil sich Inhalte hier ausgesprochen schlecht kontrollieren lassen. Üblicherweise sind die Verteiler von Informationen (von Verlagen und Druckereien bis zu Kioskbetreibern) die Anknüpfungspunkte, an denen regulative Maßnahmen zur Restriktion von verbotenen Inhalten ansetzen. Im Internet fallen derartige »Mittler« zwischen Kommunikationsteilnehmern jedoch entweder ganz weg oder sie befinden sich im Ausland und damit möglicherweise in einer Rechtssphäre, die sehr viel schwerer zugänglich ist oder in der entsprechende Inhalte gar nicht illegal sind. Gleichzeitig ist die Überwachung der Kommunikationsflüsse schwierig. Man kann zur Kontrolle nur an den Millionen von »Sendern« und »Empfängern« ansetzen, die auf der ganzen Welt verstreut sein können und bei denen – selbst wenn man ihrer habhaft wird – häufig unklar ist, ob und wann ein Regelbruch bezüglich eines inkriminierten Inhalts vorliegt und welche Regel auf sie anwendbar ist.[29]

Zwar erschweren die oben genannten technischen Eigenschaften der digitalen Internetkommunikation die Kontrolle der Inhalte erheblich, aber besonders ungünstig wirkt sich bei den inhaltsbezogenen Regelverletzungen der globalisierte Charakter des Netzes aus. Das Grundproblem besteht hier in der Divergenz zwischen dem homogenen Kommunikationsraum »Internet« und den völlig inhomogenen Rechtsräumen in den verschiedenen Ländern, die über das Internet quasi »kurzgeschlossen« werden. Die Grenzen legaler Kommunikation werden von Staat zu Staat sehr unterschiedlich bestimmt. Deutschland beispielsweise hat aufgrund seiner Vergangenheit vergleichsweise restriktive Regelungen im Bereich der politischen Meinungsäußerung. Das »Verbreiten von Propagandamitteln« und das »Verwenden von Kennzeichen verfassungsfeindlicher Organisationen« sind hier strafbewehrt, ebenso wie die Tatbestände »Volksverhetzung«, »Aufstachelung zum Rassenhass« und »Leugnung des Holocaust«.[30] Ähnliche Gesetze existieren in schwächerer Form auch in anderen Staaten wie zum Beispiel in Kanada, Großbritannien, Irland oder den skandinavischen Ländern, wo entsprechende Inhalte als »Hate Speech« bezeichnet werden. Am Ende der Skala rangieren die USA, in denen es keinerlei derartige Einschränkungen gibt und wo das in der Verfassung verankerte Prinzip der »Free Speech« einen sehr hohen Stellenwert genießt. Das Internet macht es möglich, dass diese Regelungsdivergenzen systematisch gegeneinander ausgespielt werden. So kann sich beispielsweise ein deutscher Rechtsradikaler rechtswidrige Inhalte von Servern in den USA besorgen, Webseiten dorthin auslagern und überall auf der Welt mit Gleichgesinnten kommunizieren. Aufgrund des geringen technischen Aufwands lässt sich die Kommunikation in wenigen Minuten praktisch an einen anderen Ort verlagern. Zwar hat die deutsche Rechtsprechung inzwischen sogar höchstrichterlich festgestellt, dass auch das Einstellen gesetzwidriger Inhalte ins Internet auf Servern im Ausland in Deutschland strafbar ist,[31] rechtspraktisch ist dies jedoch kaum von Belang, weil man der Täter nur äußerst selten habhaft werden wird.

Die Regelungen bei sexuell motivierter Kommunikation sind weltweit sicherlich noch divergenter (man vergegenwärtige sich nur die Unterschiede zwischen beispielsweise Saudi-Arabien und Dänemark), im OECD-Rahmen jedoch im Vergleich zu denen zur politisch motivierten Kommunikation ziemlich ähnlich. Viele Rechtssysteme machen einen Unterschied zwischen »normaler« Pornographie einerseits (die prinzipiell legal, aber durch Jugendschutzeinschränkungen reglementiert ist) und Sonderformen der Pornographie wie zum Beispiel Gewalt-, Kinder- oder Tierpornographie (die generell verboten sind). Hinzu kommen im Falle der Kinderpornographie in der Regel korrelierende Bestimmungen, die die Anbahnung des Kindesmissbrauchs unter Strafe stellen, der

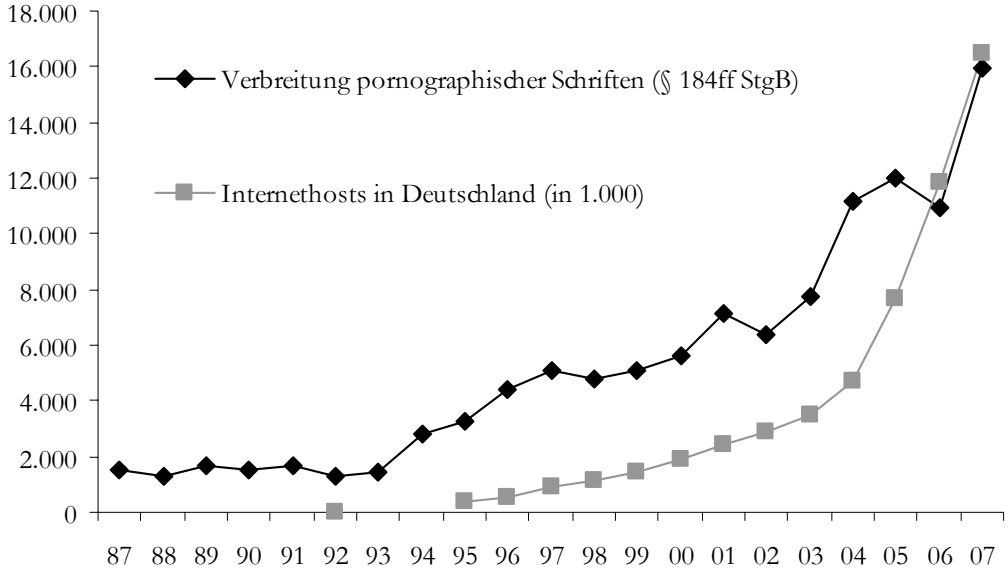
28 Vgl. Deutsche Welle, Monitor-Dienst (Hg.): *Die neo-nazistische Propaganda aus dem Ausland nach Deutschland. Internet, ausländische Flugschriften, internationale Kontakte, Skinhead-Konzerte*, Deutsche Welle 2000.

29 Autoritäre Regime unternehmen durchaus den Versuch, die im Internet verbreiteten Inhalte umfassend zu kontrollieren. Zu nennen sind dabei u.a. Länder wie Bahrain, Burma, Iran, Saudi-Arabien, Singapur und die Vereinigten Arabischen Emirate. Am erfolgreichsten sind diese Versuche in China – allerdings um den Preis einer gewaltigen Bürokratie und massiver Einschränkungen der Informationsfreiheit, vgl. dazu OpenNet Initiative, *Internet Filtering in China in 2004–2005: A Country Study*, 2005, <www.opennetinitiative.net/studies/china/> (Zugriff 14.4.2008).

30 U.a. geregelt in §§ 86, 86a, 130 des Strafgesetzbuchs.

31 Einschlägig ist hier ein Urteil des Bundesgerichtshofs (BGH) gegen einen australischen Holocaust-Leugner, vgl. BGH, Urteil vom 12.12.2000, 1 StR 184/00.

Schaubild 2
Straftaten im Zusammenhang mit der Verbreitung pornographischer Schriften und Ausbreitung des Internets in Deutschland



Quelle: für Internethosts wie Schaubild 1; Bundeskriminalamt, *Polizeiliche Kriminalstatistik*, <www.bka.de/pks/> (Zugriff 14.4.2008)

hinter jeder entsprechenden photographischen Abbildung steht.

Insbesondere die Verbreitung von *pornographischem Material* hat dem Internet in seinen ersten Jahren als Massenmedium einen schlechten Ruf beschert. Es galt als »weder sauber noch sicher« oder gar in Gänze als »Schmuggelpfad für Schmuddelkram«.[32] Mittlerweile ist aufgrund der explosionsartigen Ausbreitung des Netzes davon auszugehen, dass der Anteil derartiger Inhalte am gesamten Kommunikationsaufkommen eher gering ist. Das bedeutet freilich nicht, dass für diesen Bereich Entwarnung gegeben werden könnte. Im Hinblick auf Kinderpornographie, die wie oben skizziert in den meisten Ländern geächtet ist, sprach der Europarat 2004 von einem enormen Wachstum. Das jährliche Umsatzvolumen des entsprechenden kommerziellen Marktes im Internet schätzte er auf zwischen 7 und 20 Milliarden Euro.[33] Für den Zeitraum 2004 bis 2006 konstatiert die private britische »Internet Watch Foundation« einen Anstieg der von ihr identifizierten Internetseiten mit Bezug auf Kindesmissbrauch von 3433 auf 10656.[34] Vor diesem Hintergrund ist es wohl weniger der gestiegenen Effektivität als vielmehr der gewaltig gestiegenen Zahl entsprechender Internetangebote geschuldet, wenn in letzter Zeit bei groß angelegten Polizeiaktionen immer ausgedehntere Pädophilennetzwerke im Internet aufgedeckt wurden. So galt es im Juni 2007 als Meilenstein, als Strafverfolgungsbehörden über 700 Personen aus 35 Ländern ermitteln konnten, die bei einem Verteilerring für kinderpornographisches Material mitgemacht hatten.[35] Bereits im August 2007 wurde diese Zahl jedoch weit in den Schatten gestellt, als das LKA Baden-Württemberg bekanntgab, ihm sei via Internet die Identifikation von über 4000 Tatverdächtigen aus 106 Staaten gelungen.[36] Auch die deutsche Kriminalstatistik registriert eine äußerst problematische Entwicklung. So haben Straftaten im Zusammenhang mit

32 *Süddeutsche Zeitung*, 29.8.1996, S. 4, und *Süddeutsche Zeitung*, 10.2.1996, S. 9. Für den Beginn der entsprechenden Debatte in den USA vgl. »On a Screen Near You: Cyberporn«, in: *Time Magazine*, 7.3.1995, S. 1.

33 Council of Europe, *Organised Crime Situation Report 2004. Focus on the Threat of Cybercrime*, Straßburg 2004, S. 154.

34 Internet Watch Foundation, *Annual and Charity Report 2006*, Cambridge, UK, 2007, <www.iwf.org.uk/documents/20070412_iwf_annual_report_2006_(web).pdf> (Zugriff 14.4.2008).

35 Child Exploitation and Online Protection Centre (CEOP), *Global Online Child Abuse Network Smashed. CEOP Lead International Operation into UK based Paedophile Ring*, Pressemitteilung vom 18.6.2007.

36 Landeskriminalamt Baden-Württemberg, *Bislang größter Ermittlungserfolg baden-württembergischer Strafverfolgungsbehörden im Kampf gegen Pädokriminelle*, Pressemitteilung vom 17.8.2007.

der Verbreitung pornographischer Schriften in den vergangenen 15 Jahren drastisch zugenommen, das heißt in genau jenem Zeitraum, in dem sich auch das Internet stark ausgebreitet hat (vgl. Schaubild 2, S. 17). Für 2006 wies die Statistik dabei auch erstmals explizit aus, dass fast zwei Drittel der entsprechenden Straftaten mit dem »Tatmittel Internet« begangen wurden.

Weit weniger Beachtung als diesen Sonderformen illegaler Kommunikation wird in der Regel der Entwicklung im Bereich der »normalen« Pornographie geschenkt. Das ist umso erstaunlicher, als das Internet hier dazu geführt hat, dass die existierenden Jugendschutzbestimmungen praktisch komplett ausgehebelt worden sind. Ohne dass dies quantitativ zu spezifizieren wäre, ist offensichtlich, dass es jedem Kind oder Jugendlichen mit einem Minimum an Internetexpertise ohne Schwierigkeiten möglich ist, in fast beliebiger Menge auf Material zuzugreifen, das nach den Jugendschutzbestimmungen nicht in seine Hände gelangen sollte. Nach deutschem Recht sind die Anbieter von pornographischen Online-Inhalten genauso an die Jugendschutzregelungen gebunden wie die Betreiber von entsprechenden Verlagen, Läden oder Videoverleih-Geschäften. Der Bundesgerichtshof hat erst kürzlich noch einmal klargestellt, dass diese Anbieter tatsächlich effektive Zugangskontrollen installieren müssen.[37] Aber Websites mit pornographischem Material sind häufig im Ausland registriert (dafür reicht eine Eintragung mit dem Domainnamen ».com«), wo entweder andere Gesetze gelten oder sie nur unter größten Schwierigkeiten zur Verantwortung gezogen werden können. Sehr häufig ist es so, dass derartige Websites es mit einem Hinweis auf die folgenden Inhalte auf der ersten Seite bewenden lassen, was Jugendliche eher anziehen als abschrecken dürfte. Hier zeigt sich das typische Muster der inhaltsbezogenen Regelverletzungen im Internet: Das Netz macht aus den unterschiedlichen nationalen Gesetzessystemen einen einzigen Raum, in dem de facto rechtlich nur noch der kleinste gemeinsame Nenner gilt.

Ganz Ähnliches lässt sich in Bezug auf Rechtsverletzungen im Bereich der *politischen Kommunikation* beobachten. Relevant ist das Internet hier vor allem als Interaktionsplattform für Links- und Rechtsradikale sowie für terroristische Organisationen. Es kann eine ganze Reihe von Funktionen von erfüllen, so zum Beispiel:

- als Medium zur Verbreitung von Informationen/Propaganda in Bild, Ton und Text,
- als Marktplatz für den Versand von Materialien/Werbeträgern/Musik und Ähnlichem,
- als Plattform für Online-Spiele oder Spiele-Download mit entsprechenden Inhalten,
- als Basis für die Rekrutierung von Mitgliedern/Sympathisanten
- und für die Motivierung/»Weiterbildung« dieser Mitglieder/Sympathisanten sowie
- als Forum für die Kommunikation der Mitglieder/Sympathisanten untereinander (z.B. zur Koordination von Veranstaltungen/Aktionen etc., zur klandestinen Kommunikation unter Verwendung hochsicherer kryptographischer Verfahren etc.).

Die Kommunikation kann technisch über Webseiten, über E-Mails, aber auch über sogenannte »Newsgroups« (eine Art globales »Schwarzes Brett«), über Diskussionsforen oder (wie bei den Urheberrechtsverletzungen) über »Peer-to-Peer«-Netzwerke stattfinden. In jüngster Zeit immer beliebter ist auch die Nutzung von Videoportalen wie zum Beispiel »Youtube«.[38] Der Bundesinnenminister stellt dazu im Vorwort des Verfassungsschutzberichts 2006 fest, das Internet sei »ein gigantisches Forum: Es ist Kommunikationsplattform, Werbeträger, Fernuniversität, Trainingscamp und *think tank* in einem«.[39] Allein bei den Websites geht der Verfassungsschutz für 2006 von etwa 1000 rechtsextremistischen Internetpräsenzen aus, die von Deutschen betrieben werden.[40] Das Simon-Wiesenthal-Center in Los Angeles berichtet in der 2007er Ausgabe seines Jahresberichts *Digital Hate and Terrorism* von über 7000 Websites weltweit, die rassistische, antisemitische, volksverhetzende oder terroristische Inhalte verbreiten.[41] Gerade im Bereich des Rechtsradikalismus ist die Auslagerung von Informationen bzw. Server-Diensten in die USA häufig das Mittel der Wahl, da die Verantwortlichen dort keine Strafverfolgung befürchten müssen und ihnen gleichzeitig eine exzellente Infrastruktur zur Verfügung steht. Für islamistische terroristische Gruppie-

37 BGH, *Bundesgerichtshof: Führendes Altersverifikationssystem für Internetzugang unzureichend*, Pressemitteilung 149/2007 vom 19.10.2007.

38 Vgl. »Youtube verbreitet rechtsradikale Videos«, in: *Süddeutsche Zeitung*, 27.8.2007.

39 Bundesministerium des Innern (BMI), *Verfassungsschutzbericht 2006*, Berlin 2007, S. 4.

40 Ebd., S. 53.

41 Simon Wiesenthal Center 2007, *Digital Terrorism and Hate 2007. Growing Menace of Digital Terrorism and Hate Exposed in New SWC Interactive Report*, Pressemitteilung vom 7.6.2007.

rungen sind die USA naturgemäß nicht attraktiv, aber auch ohne diese Möglichkeit handelt es sich beim Internet in den Worten des BKA-Präsidenten Jörg Ziercke mittlerweile um »das entscheidende Kommunikationsmittel des internationalen Terrorismus«.[42] Auch der Verfassungsschutz attestiert dem Netz eine große und ständig weiter steigende Bedeutung für »Radikalisierung, Motivierung und Rekrutierung«[43] von Mitgliedern und Sympathisanten terroristischer Organisationen. Studien berichten von über 5000 Websites, Onlineforen und »Chatrooms«, die von Terroristen oder deren Sympathisanten betrieben oder benutzt werden.[44] Praktisch alle relevanten terroristischen Organisationen bedienen sich heute des Internets. Dies steht in einem starken Kontrast zu der Tatsache, dass es in Deutschland erst 2007 zum ersten und bisher einzigen Strafverfahren wegen der Verbreitung islamistischer Terrorpropaganda im Internet gekommen ist.[45]

Internetkriminalität im engeren Sinne

Unter Internetkriminalität im engeren Sinne werden hier Kriminalitätsformen gefasst, deren primäre Motivation zwar ebenfalls ökonomischer Natur ist, für die das Internet jedoch eine andere Rolle spielt als für die bisher diskutierten Delikte. Für Internetkriminalität im engeren Sinne ist das Netz nicht nur bloßes Transportmedium für eine strafbare Handlung, sondern das Internet selbst und die Hardware seiner Infrastruktur sind Ziel und Kern der entsprechenden Transaktionen, das heißt diese richten sich unmittelbar auf das Netz und seine Komponenten, auf die Computer der Nutzer oder auf deren Daten. Der Europarat hat diese Delikte als Angriffe auf die Vertraulichkeit, Integrität und Verfügbarkeit von Computersystemen und Daten unter der Formel der sogenannten *C.I.A. offences* (»offences against confidentiality, integrity, and availability of computer systems, networks, and computer data«) subsumiert.[46] Diese Variante der Internetkriminalität tritt in vielfältigen technischen Erscheinungsformen auf. Es lassen sich dabei insbesondere drei Grundarten differenzieren:

- »*Spam*«: Dieser Begriff bezeichnet unerwünschte E-Mails,[47] die zumeist Werbung für dubiose Produkte oder Dienstleistungen enthalten (wie zum Beispiel nicht-existierende Generika von Viagra oder fragwürdige Kreditangebote);
- »*Malware*«: Hierbei handelt es sich um Software, die ohne Wissen und Zustimmung des Nutzers in einen Computer eingeschleust wird und dort Schäden verursacht und/oder sich unter Rückgriff auf E-Mail-Daten des Computers selbst weiterverbreitet. Unterformen von *Malware* werden als »Viren«, »Würmer« und »Trojanische Pferde« bezeichnet;
- »*Spyware*«: Dies ist der Oberbegriff für (z.B. per E-Mail implantierte) Software, die das Ziel hat, private Daten auszuspähen. Dabei kann es um die Kontodaten des Computerbesitzers, aber auch schlicht um dessen Gewohnheiten der Internetnutzung gehen.

Diese drei Grundformen lassen sich auf verschiedene Arten und Weisen kombinieren. So kann beispielsweise Spam-E-Mail trojanische Pferde enthalten, die Spyware installieren. Umgekehrt können bestimmte Typen von Viren oder trojanischen Pferden dazu verwendet werden, Spam zu verbreiten. Unter den vielfältigen Formen, in denen sich Internetkriminalität im engeren Sinne manifestiert, sind drei von besonderer Bedeutung:

- »*Phishing*«: Unter diesem Begriff werden alle Aktivitäten zusammengefasst, die dem Ausspionieren oder/und dem Missbrauch vertraulicher Daten, vor allem im Kontext von »E-Commerce« und »Online-Banking«, dienen.
- »*Botnets*«: Sie stellen eine besondere Form von »Malware« dar. Botnets verbinden die infizierten Rechner untereinander und machen sie fernsteuerbar (»Zombie-Computer«), so dass von diesen Rechnern aus gemeinsam (und ohne Wissen der Besitzer) koordinierte Attacken auf andere Computersysteme durchgeführt werden können. Botnets sind zum Beispiel für circa 80 Prozent der Verteilung von Spam verantwortlich, aber auch äußerst effektiv für die Ausführung sogenannter

42 Deutschlandradio Kultur, »BKA-Präsident: ›Internet ist das Tatmittel der Zukunft‹. Ziercke hält Online-Durchsuchung für unerlässlich«, <www.dradio.de/dkultur/sendungen/interview/590511/> (Zugriff 14.4.2008).

43 BMI 2007, Fn. 55, S. 218.

44 Gabriel Weimann, »Online Terrorism – Modern Terrorists and the Internet«, in: Sonja Glaab (Hg.), *Medien und Terrorismus – Auf den Spuren einer symbiotischen Beziehung*, Berlin 2007, S. 51.

45 Erster Prozess wegen Terrorwerbung übers Internet, dpa-Meldung vom 26.4.2007.

46 Vgl. Council of Europe, *Convention on Cybercrime*, Chapter II, Section 1, Title 1.

47 Die Bezeichnung »Spam« geht auf einen Sketch aus der englischen Comedyserie »Monty Python's Flying Circus« aus den siebziger Jahren zurück, in dem der Markenname eines Dosenfleisches (»SPAM«) bis zur Absurdität wiederholt wurde.

- »*Denial of Service Attacks (DoS)*«: Damit bezeichnet man Angriffe auf die Verfügbarkeit eines Computers, Systems oder Dienstes. Ein solcher Angriff kann beispielsweise ausgeführt werden, indem ein Webserver so stark mit Anfragen überschwemmt wird, dass er weitere Anfragen blockiert oder abstürzt und daher für niemanden mehr erreichbar ist. *Denial of Service Attacks* eignen sich beispielsweise zur Erpressung von Firmen, die wirtschaftlich von ihrer Webpräsenz bzw. ihrer Erreichbarkeit per Internet abhängig sind.

Diese Formen der Kriminalität sind nur in einem digitalen Medium wie dem Internet denkbar, denn sie setzen unmittelbar an der computergestützten Datenverarbeitung an und nutzen systematisch die geringen Transaktionskosten, die leichte Manipulierbarkeit elektronischer Daten und die Unkenntnis (und teilweise auch Naivität) ungeschulter Nutzer. Bei Spam-Mails beispielsweise wirkt es sich verheerend aus, dass die Transaktionskosten der elektronischen Kommunikation so niedrig sind. Auch bei Millionen von E-Mails ist der Aufwand des Versands minimal, so dass sich unerwünschte elektronische Werbesendungen selbst dann lohnen, wenn unter Hunderttausenden von Empfängern nur einige wenige reagieren und auf das (meist betrügerische) Angebot hereinfallen. Der große Vorteil der E-Mail als schnelles und äußerst preisgünstiges Kommunikationsmedium wandelt sich hier in einen gravierenden Nachteil zum Schaden aller Internetnutzer.

Die mit diesen Formen der Internetkriminalität einhergehenden Probleme haben mittlerweile eine beachtliche Dimension erlangt. Das *Spam*-Volumen beispielsweise ist schlicht gigantisch. Geschätzte 80 Prozent des Datenverkehrs im Internet bestehen aus E-Mails und davon waren nach Schätzungen im Jahr 2006 wiederum über 80 Prozent Spam.[48] Stimmen diese Berechnungen, dann machen Spam-Mails heute über 60 Prozent des gesamten Datenverkehrs im Internet aus. Legt man hinsichtlich des absoluten Datenvolumens die mittlerweile sicherlich längst überholten Zahlen von 2002 zugrunde,[49] so würde das bedeuten, dass täglich fast 50 Milliarden unerwünschte Nachrichten versendet werden, die hintereinander ausgedruckt der halben Distanz zwischen Erde und Sonne entsprächen (ca. 75 Millionen Kilometer)! Die Datenkanäle des Internets werden somit in großem Umfang mit Spam-Daten überschwemmt und blockiert. Darüber hinaus binden die unerwünschten Nachrichten entweder die Aufmerksamkeit und Arbeitszeit der Internetnutzer, oder sie müssen durch Schutzmechanismen (Firewalls und Filter) die ihrerseits signifikante Kosten verursachen, aussortiert werden. Die Europäische Kommission veranschlagte die Gesamtkosten der durch Spam verursachten Schäden im Jahr 2001 auf über 10 Milliarden Euro weltweit.[50] 2005 war die geschätzte Summe bereits auf 39 Milliarden Euro angestiegen, wobei 3,5 Milliarden Euro allein auf Deutschland entfielen.[51]

Bei *Malware* handelte es sich ursprünglich zumeist um Computerviren, die in einer Vielzahl der Fälle allein deshalb programmiert wurden, um das technische Know-how ihrer Urheber zu demonstrieren. Das »Form-Virus« aus dem Jahr 1990 beispielsweise mutet aus heutiger Perspektive als harmlose Spielerei an. Es machte sich einmal im Monat über Tastaturklicks bemerkbar, enthielt in seinem eigenen Code die Meldung: »The FORM-Virus sends greetings to everyone who's reading this text«, verursachte sonst aber kaum Nebeneffekte. Mittlerweile ist Malware wesentlich elaborierter und bösartiger geworden. Die Entwicklung hat Software hervorgebracht, die erstens zu ihrer Weiterverbreitung selbst aktiv wird (dies gilt vor allem für sogenannte »Würmer«), zweitens auf den infizierten Geräten massive Schäden anrichten kann und drittens systematisch für kriminelle Zwecke eingesetzt wird. Bereits rein quantitativ ist das Aufkommen an Malware erheblich. In den letzten Jahren pendelte der Anteil Malware-verseuchter E-Mails am gesamten Mailverkehr nach Schätzungen der Sicherheitsfirma *MessageLabs* weltweit zwischen 1,5 und 3 Prozent. In absoluten Zahlen bedeutet das Hunderte von Millionen von verseuchten E-Mails. Deutschland liegt dabei mit 8 Prozent für 2005(!) und über 3 Prozent

48 Vgl. Message Labs, *MessageLabs Intelligence: 2006 Annual Security Report. A Year of Spamming Dangerously: The Personal Approach to Attacking*, Gloucester 2006, <www.messagelabs.com/mlireport/2006_annual_security_report_5.pdf> (Zugriff 14.4.2008).

49 2002 wurden weltweit geschätzte 440 000 Billionen Zeichen als E-Mail versendet, vgl. Lyman/Varian, *How Much Information?* [wie Fn. 6].

50 European Commission, *Data Protection: »Junk« E-mail Costs Internet Users 10 billion a Year Worldwide – Commission Study*, Pressemitteilung vom 2.2.2001. Damals galt dieser Wert als konservative Schätzung.

51 Europäische Kommission, *Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über die Bekämpfung von Spam-, Späh- und Schadsoftware,* Brüssel 2006, KOM (2006) 688, 15.11.2006.

für 2006 jeweils deutlich über dem Durchschnitt.[52] Dabei sind es keineswegs nur einige wenige Viren, die auf diese Weise millionenfach verbreitet werden. Die internationale Softwarefirma *Symantec*, einer der weltweit größten Anbieter von Virenschutzprogrammen, berichtet, sie habe allein 2006 über 15 000 *neue Varianten* von Viren, Würmern und trojanischen Pferden identifiziert.[53] Außerordentlich alarmierend ist die neue Qualität der oben beschriebenen »Botnets«. Diese verborgenen Netzwerke bieten sich für kriminelle Aktivitäten besonders an, weil das Risiko der Enttarnung des eigentlichen Urhebers äußerst gering ist, denn der Angriff erfolgt »ferngesteuert« von Tausenden fremder Computer aus. Botnets eignen sich nicht nur hervorragend für die Verteilung von Spam, sondern können zum Beispiel auch für die schon erwähnten DoS-Attacken eingesetzt werden, die wiederum für Erpressungen oder zum Ausschalten der Webseiten von Konkurrenten dienen. Beunruhigend ist, dass mittlerweile ganz offensichtlich ein Markt entstanden ist, auf dem Botnets für kriminelle Zwecke »gemietet« werden können, wobei ein Angriff mit mehreren Tausend Computern zwischen 500 und 1500 US-Dollar kosten soll. 2004 wurde der Fall einer britischen Firma für Online-Sportwetten bekannt, die Opfer eines entsprechenden Erpressungsversuchs wurde. Die Täter verlangten ein Lösegeld dafür, dass sie die Webseite der Firma *nicht* durch eine Botnet-DoS-Attacke lahmlegen, was der Wettfirma natürlich massive Verdienstausfälle beschert hätte.[54] Wie viele derartige Fälle nicht bekannt geworden sind und möglicherweise erfolgreich waren, lässt sich kaum abschätzen.[55] Äußerst aufschlussreich ist jedoch eine Zahl aus dem Frühjahr 2007, der zufolge nach derzeitigem Konsens unter den Experten auf circa 11 Prozent aller mit dem Internet verbundenen Computer Botnet-Clients installiert sind. Das wären nach dem jüngsten Stand mindestens 50 bis 60 Millionen Rechner weltweit, was ein enormes Potential für kriminelle Aktivitäten dieser Art darstellen würde.[56] Deutschland rangierte 2007 nach Angaben von *Symantec* bei den mit Botnets infizierten Computern international auf Platz 4 und findet sich generell bei den Malware-Aktivitäten regelmäßig unter den ersten drei bis vier Staaten – sowohl als Quelle entsprechender Angriffe als auch als deren Ziel.[57]

Eine zunehmende Relevanz hat auch *Spyware*, die dem Ausspähen vertraulicher Informationen dient. Zwar sind ganz verschiedene Formen von Spyware denkbar – und auch kommerzielle Softwarehersteller werden gelegentlich der Verteilung von Spyware beschuldigt, wenn sie Informationen über das Verhalten von Nutzern sammeln. Besonders problematisch ist Spyware aber im Zusammenhang mit »Phishing«. Dabei geht es um das Ausspähen von Kreditkarteninformationen, »Personal Identification Numbers« (PINs) und Transaktionsnummern (TANs), wie sie im Online-Banking üblich sind, Versicherungsdaten und Ähnlichem. Durch Phishing gewonnene Daten werden dann zumeist im Rahmen »traditioneller Kriminalität« genutzt, um Gelder umzulenken, Überweisungen zu tätigen, Einkäufe vorzunehmen und so weiter. Die Urheber von Phishing-Attacken versenden E-Mails (letztlich also Spam), in denen entweder der Empfänger direkt zur Preisgabe vertraulicher Informationen aufgerufen wird oder die einen Link auf eine Website enthalten. Dabei handelt es sich dann um die manipulierte Kopie einer echten Homepage, zum Beispiel einer Bank, wo der Nutzer seine vertraulichen Informationen eingeben soll. In der E-Mail wird dem Adressaten beispielsweise mitgeteilt, es sei zum Zwecke einer »Sicherheitsprüfung« notwendig, auf der entsprechenden Website die geheimen Daten anzugeben.

Bei einer noch gefährlicheren Variante des Phishing, dem sogenannten »Pharming«, wird auf diese Art von E-Mail-Kontakt verzichtet und der Internetzugang des Nutzers über Malware direkt manipuliert. Wenn dieser wie gewohnt beispielsweise die Website seiner Bank aufrufen will, wird er unbemerkt über eine Manipulation der Internetadresse der Bank auf eine gefälschte Version der Bank-Homepage umgelenkt. In Deutschland wurde die im Online-Geschäft sehr aktive Postbank bereits häufiger Opfer von Phishing-Attacken,[58] aber selbst die Website des Bundeswirt-

52 MessageLabs, *MessageLabs Intelligence: 2006 Annual Security Report* [wie Fn. 48].

53 Symantec Corporation, *Symantec Internet Security Threat Report. Trends for July–December 06*, Volume XI, März 2007, <http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf> (Zugriff 14.4.2008).

54 »How Zombie Networks Fuel Cybercrime«, in: *New Scientist*, 3.11.2004.

55 Symantec zumindest hat über ihre Produkte für das Jahr 2006 durchschnittlich über 5500 DoS-Attacken pro Tag registriert, vgl. Symantec Corporation, *Symantec Internet Security Threat Report* [wie Fn. 53].

56 »Attack of the Zombie Computers is a Growing Threat, Experts say«, in: *The New York Times*, 7.1.2007.

57 Symantec Corporation, *Symantec Internet Security Threat Report* [wie Fn. 53].

58 Postbank, *Postbank ergreift Maßnahmen gegen Phishing*, Pressemitteilung vom 2.5.2005.

schaftsministeriums wurde 2007 gefälscht. Den Besuchern der Homepage wurde eine Steuerrückzahlung angekündigt, zu welchem Zweck sie ebenfalls ihre Bankkontodaten angeben sollten.[59] *MessageLabs* schätzt den weltweiten Anteil von Phishing-Mails an allen Spam-Mails im letzten Quartal 2006 auf beinahe 25 Prozent.[60] Angesichts des gewaltigen Spam-Volumens bedeutet dies Milliarden von Phishing-Mails. Dabei ist neben diesem ungeheuren Aufkommen vor allem bemerkenswert, dass *Symantec* für 2006 über 300 000 *verschiedene Arten* von Phishing-Mails identifizieren konnte.[61] Selbst wenn nur ein verschwindend geringer Teil dieser Mails zum Erfolg führt und Nutzer tatsächlich vertrauliche Daten preisgeben, ist der potentielle Schaden enorm. Wie gesehen, gehören zum Phishing-System aber nicht nur die betrügerischen E-Mails sondern auch die gefälschten Webseiten, auf die die Nutzer mit Hilfe der E-Mails oder der Webadressen-Manipulation gelenkt werden. In diesem Zusammenhang fällt auf, dass Deutschland nach Schätzungen von *Symantec* mit 11 Prozent der Phishing-Sites im letzten Quartal 2006 weltweit auf Platz 2 stand.[62] Der tatsächliche Schaden, der durch Phishing entsteht, lässt sich auf der Basis dieser blanken Zahlen nur schwer ermessen, sollte aber im Rahmen der Erhebungen zur traditionellen Kriminalität zumindest teilweise berücksichtigt worden sein.

Als Zwischenresümee lässt sich festhalten, dass alle drei hier untersuchten Varianten der Internetkriminalität im engeren Sinne – Spam, Malware und Spyware – große Probleme aufwerfen. Die vorliegenden Daten zeigen zudem, dass Deutschland zur Weltspitze der von dieser Art von Internetkriminalität betroffenen Länder gehört. Dieser Befund macht vor allem deshalb nachdenklich, weil im Bereich der Kommunikationssicherheit inzwischen ein äußerst dynamischer Markt entstanden ist und zahlreiche Firmen professionelle Schutzlösungen anbieten. Zwei Schlussfolgerungen drängen sich auf: Entweder werden längst nicht von allen Nutzern (vor allem im privaten Bereich) entsprechende Abwehrprogramme verwendet und/oder die existierenden Programme sind nicht in der Lage, die skizzierte Entwicklung effektiv einzudämmen. Der Ausgang des »Katz-und-Maus-Spiels« zwischen dem technischen Erfindergeist der Täter und dem der Sicherheitsfirmen ist derzeit auf alle Fälle noch offen.

59 Bundeswirtschaftsministerium (BMWi), *Warnung: Gefälschte BMWi-Mails im Umlauf*, Pressemitteilung vom 2.8.2007.
60 MessageLabs, *MessageLabs Intelligence: 2006 Annual Security Report* [wie Fn. 48].
61 Symantec Corporation, *Symantec Internet Security Threat Report* [wie Fn. 53], S. 65.
62 Ebd., S. 70.

»Cyberterrorismus«

Unter »Cyberterrorismus« lassen sich alle terroristischen Aktivitäten fassen, deren Ziel Informationsnetzwerke sind. Der Begriff bezeichnet also nicht die Kommunikation »normaler« Terroristen untereinander, bei der das Internet lediglich als Transportmedium dient. (Diese Kommunikation fällt in der hier verwendeten Systematik unter die bereits diskutierten inhaltsbezogenen Rechtsverletzungen). Wie bei anderen Formen des Terrorismus handelt es sich beim Cyberterrorismus um eine Gewaltstrategie zur Durchsetzung politischer Ziele, die systematisch auf die Verbreitung von Angst und Schrecken setzt.[63] Das Internet ist dabei jedoch entweder selbst das Angriffs*ziel* oder das Angriffs*mittel*, das gegen eine andere Kommunikationsinfrastruktur eingesetzt werden soll.

Wie aber lassen sich durch eine virtuelle »Informationsattacke« relevante reale Schäden erzeugen und Angst und Schrecken verbreiten? In diesem Zusammenhang ist der Begriff der »kritischen Infrastruktur« von großer Bedeutung. Er bezieht sich auf Elemente der Infrastruktur eines Landes, die einerseits von essentieller Bedeutung sind und deren Ausfall oder Schädigung erhebliche Konsequenzen nach sich zöge, die andererseits aber auch in hohem Maße verwundbar sind. 1995 berief der damalige US-Präsident Clinton eine »President's Commission on Critical Infrastructure Protection (PCCIP)« ein, die 1997 einen Abschlussbericht vorlegte.[64] Dieser Bericht gilt als eine der ersten Publikationen, die die Felder »kritischer Infrastruktur« definiert.[65] Demnach gehören dazu insbesondere:

- Kommunikationsnetze im Bank- und Finanzwesen,
- Energieversorgungsnetze (Elektrizität, Gas, Öl),
- Wasserversorgungsnetze,
- Verkehrsdienste (insbesondere Flugsicherheit und Bahn),

63 Vgl. zur Definition des Terrorismus Ulrich Schneckener, *Transnationaler Terrorismus. Charakter und Hintergründe des »neuen« Terrorismus*, Frankfurt 2006, S. 21.
64 President's Commission on Critical Infrastructure Protection, *Critical Foundations. Protecting America's Infrastructures. The Report of the President's Commission on Critical Infrastrucuture Protection*, Washington 1997.
65 In Deutschland setzte 1997 mit der Konstituierung der »Arbeitsgruppe KRITIS« ein sehr ähnlicher Prozess ein.

- Notfallsysteme und -dienste (Rettungsdienste, technische Dienste) und
- Kommunikationssysteme von Regierung und Verwaltung.

Die Aufzählung macht deutlich, dass es einerseits unmittelbar um (digitale) Kommunikationsnetzwerke geht (Banken, Finanzen, Regierung und Verwaltung), und andererseits um Infrastrukturelemente, die in erheblichem Umfang von digitalen Kommunikationsnetzwerken abhängig sind bzw. auf der Basis digitaler Informationsverarbeitung gesteuert werden. Das Internet selbst bzw. andere Telekommunikationsinfrastrukturen wären zwischenzeitlich noch hinzuzufügen, denn in dem Maße, wie sich Transaktionen ins Internet verlagern, wird auch das Netz selbst zur kritischen Infrastruktur. Ein signifikanter Teil der »critical infrastructure« beruht somit auf einer »critical information infrastructure«, und genau diese ist im Rahmen des »Cyberterrorismus« potentiell angreifbar. Gelänge es Terroristen beispielsweise, die globale Kommunikation im Finanzsektor zu stören oder zu manipulieren, hätte dies innerhalb kürzester Zeit gravierende Auswirkungen nicht nur auf die internationalen Finanzmärkte, sondern mittelbar auch auf die makroökonomische Stabilität einer großen Anzahl von Volkswirtschaften. Ebenso ist offensichtlich, dass ein »Hack« in der Steuerungseinrichtung eines Atomkraftwerks oder die Manipulation eines Flugsicherungssystems verheerende Folgen hätte. Die entscheidende Frage lautet, inwieweit die entsprechenden Informationssysteme vom Internet aus angreifbar sind. Idealiter besteht zwischen einer »kritischen Informationsinfrastruktur« und dem Internet keinerlei Verbindung, so dass auf diesem Wege auch niemand »von außen« eindringen kann. In der Praxis sind Kommunikationsnetzwerke jedoch vielfach »perforiert« bzw. weisen Schnittstellen zur »Außenwelt« – und das bedeutet zumeist zum Internet – auf. Genau hier liegen die potentiellen Angriffspunkte des Cyberterrorismus.

Der globalisierte Charakter des Internets wirkt auch hier problemverschärfend. In dem Moment, wo eine kritische Informationsinfrastruktur eine Schnittstelle zum Internet hat, ist sie praktisch von jedem Ort der Welt aus angreifbar. Hinzu kommt, wie auch schon bei anderen Kriminalitätsformen, dass die Prävention und die Verfolgung entsprechender Aktivitäten im globalisierten Raum des Internets erschwert ist und die Täter ihre Spuren leichter verschleiern können.

Das Ausmaß des Risikos Cyberterrorismus abzuschätzen ist fast unmöglich, weil derartige Angriffe bislang weitgehend ausgeblieben oder nicht bekannt geworden sind. Der Hinweis darauf, dass Bedrohungen immer auch etwas mit Wahrnehmung zu tun haben und es – ausgehend von den USA – einen von politischen Interessen geleiteten Prozess gab, in dem die Gefahr eines »Cyberterrorismus« überhaupt erst formuliert wurde, ist sicher richtig. Kritisch sind auch die metaphorisch-manipulativen Begrifflichkeiten wie »electronic Pearl Harbor« oder »electronic 9/11« zu sehen, die in diesem Zusammenhang geprägt wurden.[66] Andererseits ist auch richtig, dass die Abhängigkeit kritischer Infrastrukturen von digitaler Kommunikation bereits jetzt sehr hoch ist, dass es in der Regel Schnittstellen zum Internet gibt und das Internet selbst zu einer kritischen Infrastruktur geworden ist. Konkrete Beispiele für entsprechende Angriffe gab es bisher vor allem in Form von politisch motivierten DoS-Attacken, bezogen sich also auf die Internetkommunikation selbst (und weniger auf andere kritische Infrastrukturen). Dies war zum Beispiel Ende Januar 2006 der Fall, als im Kontext des »Karikaturenstreits« die Website der dänischen Zeitung *Jyllands-Posten* manipuliert und lahmgelegt wurde. Ähnliches war schon früher im Zuge zum Beispiel des Kosovo-Krieges mit Webseiten der NATO oder des US-amerikanischen Verteidigungsministeriums geschehen. Diese Attacken lassen sich jedoch kaum als Manifestationen eines Cyberterrorismus im dargelegten Sinne verstehen. Es handelt sich dabei eher um die »Online«-Korrelate einer ansonsten primär mit traditionellen Mitteln geführten Auseinandersetzung, deren Schadenwirkung virtuell und äußerst begrenzt bleibt.

Deutlich gravierender waren die koordinierten virtuellen Attacken auf die Kommunikationsinfrastruktur in Estland im Mai 2007. Im Kontext einer Auseinandersetzung zwischen Estland und Russland über die Versetzung eines sowjetischen Kriegsdenkmals wurden damals verschiedene Einrichtungen Estlands zum Ziel massiver DoS-Attacken, wobei es starke Hinweise darauf gibt, dass diese von Russland ausgingen. Die Täter bedienten sich dabei jedoch auch Botnets, so dass die Palette der Herkunftsländer der angreifenden Rechner von den USA bis nach Vietnam reichte. Im Ergebnis waren unter anderem die Banken Estlands zeitweise nicht mehr erreichbar, was aufgrund der sehr hohen Internetabhängigkeit des Landes dazu führte, dass zum Beispiel elektronische Überweisungen oder Bezahlvorgänge (in Supermärkten oder an

66 Ralf Bendrath, »The Cyberwar Debate. Perception and Politics in U.S. Critical Infrastructure Protection«, in: *Information & Security*, 7 (2001), S. 80–103.

Tankstellen) nicht mehr möglich waren. Regierungs- und Behördenseiten waren ebenfalls zeitweilig gestört, und auch die Notrufnummer war nicht mehr funktionsfähig. Die Regierung reagierte mit der Abtrennung Estlands vom weltweiten Internet, was seinerseits Schäden, zum Beispiel im Bankbereich nach sich zog.[67]

Das Beispiel Estland macht deutlich, was es bedeutet, wenn das Internet selbst zur kritischen Infrastruktur wird. Und noch ein anderer Aspekt ist im Zusammenhang mit diesem Fall signifikant: So spricht viel dafür, dass Botnets zum Zwecke der Durchführung solcher Angriffe immer häufiger vermietet werden.[68] Das würde bedeuten, dass es terroristischen Akteuren, die selbst nicht über ein hinreichendes technisches Know-how verfügen, möglich wäre, dieses unkompliziert auf einem »Markt für Internetkriminalität« einzukaufen.

Festzuhalten bleibt zweierlei: Einerseits ist das Schadenspotential durch Cyberterrorismus durch die gewachsene Bedeutung digitaler Kommunikationsnetzwerke schon jetzt relativ hoch und wird aller Voraussicht nach weiter steigen. Das Beispiel Estlands zeigt, dass mit der Nutzung des Internets die potentielle Verwundbarkeit signifikant steigt, selbst wenn andere kritische Infrastrukturen effektiv abgeschirmt sein sollten. Andererseits sind bisher Fälle von Cyberterrorismus kaum bekannt geworden. Dies mag zum einen mit der Verfügbarkeit der entsprechenden technischen Expertise zu tun haben, zum anderen ist die symbolische Wirkung, die sich durch einen unmittelbaren Gewaltakt erzielen lässt, höher als bei Angriffen, die »nur« im virtuellen Raum stattfinden. Ein Bombenanschlag ist nach Maßgabe terroristischer Logik daher deutlich »effektiver« als eine DoS-Attacke. Das strategische Kalkül der Täter könnte sich allerdings mit der steigenden Abhängigkeit von internetgestützter Kommunikation und einer entsprechend gestiegenen Verwundbarkeit ändern.

67 »Estland im Visier. Ist ein Internetangriff der Ernstfall?«, in: *Frankfurter Allgemeine Zeitung*, 18.6.2007, S. 6; Brian Krebs, »Estonia Incident Demonstrated Power of Russia-Based Cyber Networks«, in: *Washington Post*, 13.10.2007.

68 Peter Warren, »Hunt for Russia's Web Criminals«, in: *The Guardian*, 15.11.2007

Reaktionsmöglichkeiten

Aus dem Überblick über die Varianten der Internetkriminalität und deren Entwicklung lassen sich folgende Schlüsse ziehen: In allen hier untersuchten Problembereichen gibt es eine immense Zahl von »grauen« oder illegalen Transaktionen, die milliardenschwere Schäden verursachen. Zudem lassen alle Trends, wo immer solche identifiziert werden konnten, einen weiteren Anstieg der kriminellen Aktivitäten befürchten. Lediglich im Bereich des »Cyberterrorismus« fehlen bisher spektakuläre Fälle, aber hier ist zumindest von einem erheblichen Gefahrenpotential auszugehen, das in dem Maße steigen dürfte, in dem die Bedeutung des Internets weiter zunimmt. Gleichwohl ist es nicht so, dass man dazu verdammt wäre, der oft beschworenen Entwicklung des Internets zum »rechtsfreien Raum« passiv zuzusehen. Es ist wichtig, sich klarzumachen, dass das Internet grundsätzlich eine technische Struktur ist, die mit politischem Willen gestaltet werden kann. Die »chinesische Lösung« der intensiven Kontrolle um den Preis des massiven Eingriffs in die persönliche Freiheit ist genauso möglich wie die amerikanische Variante des weitgehenden Laissez-faire, die mit hohen Kriminalitätsraten einhergeht. Das Internet ist sehr wohl regulierbar; die entscheidende Frage lautet vielmehr: Wo liegt der rechtlich mögliche und politisch konsensfähige Mittelweg zwischen Überwachung und Zensur zur Eindämmung der Kriminalität einerseits und dem Eingriff in die Meinungsfreiheit, Handlungsfreiheit und Datenschutz andererseits? Es geht somit nicht darum, ob reguliert werden *kann*, sondern wie und um welchen Preis reguliert werden *soll*.

Diese Grundüberlegung soll anhand der beiden oben erwähnten Prozesse illustriert werden, die sich im Internet überschneiden: Digitalisierung und Globalisierung. Im Hinblick auf die Frage, welche Möglichkeiten es gibt, um auf die Internetkriminalität zu reagieren, lautet dabei die erste Schlussfolgerung: *Digitalisierung ist eine Herausforderung aber auch eine Chance*. Wie eingangs dargelegt, erschwert die Digitalisierung, die zu gewaltigen Mengen »flüchtiger« oder »virtueller« Daten führt, die mit sehr großer Geschwindigkeit verarbeitet werden können, zweifelsohne die (Um-)Formulierung und Implementation von Regeln, die für ein analoges, langsameres und »greifbareres« Zeitalter gedacht waren. Aber gleichzeitig gibt die Digitalisierung den Regelsetzern und -durchsetzern auch neue Möglichkeiten an die Hand und zwingt sie dazu, die bisherigen Regeln und Regelungsmodi unter veränderten Rahmenbedingungen kritisch zu überdenken. Dies ist ein Aspekt, der in einer bisher weitgehend defensiv geführten Diskussion häufig unterbewertet wird.

Die zweite Schlussfolgerung lautet: *Das Internet ist globalisiert, aber es ist nicht entterritorialisiert*. Es trifft zwar zu, dass – wie oben gezeigt – das Internet keine Grenzen kennt und einen homogenen Handlungsraum darstellt. Aber es ist gleichzeitig wichtig, sich in Erinnerung zu rufen, dass das Netz mit der realen Welt durchaus physisch verbunden ist. Jeder »Internethost« hat einen konkreten Standort, jeder Internetnutzer ebenfalls und alle Daten sind zu einem bestimmten Zeitpunkt t an einem Ort x gespeichert. Diese territoriale Bindung lässt sich über die Internetadresse eines Rechners und über die Daten von Internet-Service-Providern auch ohne weiteres lokalisieren. Das Internet liegt nicht komplett jenseits der physischen Welt und damit auch nicht jenseits der Regelsysteme, die für die physische Welt erdacht worden sind.

Der Begriff Internetkriminalität in dem Sinne, wie er hier gebraucht wird, bezieht sich auf Rechtsverletzungen, bei denen das Internet entweder als bloßes Medium dient oder selbst Ziel der entsprechenden Aktivitäten ist. Rechtsverletzungen haben allgemein etwas mit Rechtssetzung bzw. Verregelung und mit Implementation von Normen (inklusive der Sanktionierung von Regelverletzungen) zu tun. Die Digitalisierung fordert vor allem dazu heraus, über die Formen nachzudenken, in denen Verregelung und Implementation erfolgen. Demgegenüber zwingt die Tatsache der Globalisierung in erster Linie dazu, bei der Konzeptualisierung der Reaktionsformen neben der nationalen systematisch eine internationale Ebene zu berücksichtigen. Fasst man diese beiden Überlegungen unter die Begriffe »Reaktionsart« und »Reaktionsebene« ergibt sich eine Systematik möglicher Reaktionen auf Internetkriminalität, die die folgende Tabelle 2 veranschaulicht.

Tabelle 2
Systematik möglicher Reaktionen auf Internetkriminalität

		Reaktionsart	
		Verregelung	*Implementation*
Reaktionsebene	*International*	Integration	Kooperation
	National	Adaption	Innovation

Integration: Internationale Harmonisierung von Regelungen

Es liegt nahe, dass der Homogenität des Handlungsraums »Internet« eine möglichst große Homogenität der verschiedenen internationalen Regelungen entsprechen sollte. Wenn die Transaktionen im Internet zunehmend den nationalen Raum überschreiten, können mittels einer internationalen Rechtsangleichung Transaktions- und Regelungsraum wieder zur Deckung gebracht werden. In der Praxis ist dies mit all jenen Schwierigkeiten verbunden, die jede internationale Kooperation gewöhnlich kennzeichnen (Konsenserfordernisse, Schwerfälligkeit der Verhandlungsführung etc.). Trotzdem ist in diesem Bereich bereits einiges geleistet worden. Besonders hervorzuheben ist die Budapester Konvention (oder »Cybercrime Convention«) des Europarats von 2001. Sie stellt das erste Rechtsdokument dar, das explizit der internationalen Harmonisierung all jener einzelstaatlichen Regelungen diente, die der Internetkriminalität entgegenwirken sollen. Sie hat zum einen erstmals einheitliche Definitionen und eine wichtige Systematisierung der verschiedenen Formen der Internetkriminalität geliefert und zum anderen einen Minimalkonsens darüber hergestellt, was »Cybercrime« eigentlich bedeutet. Die Konvention wurde zunächst von 27 Mitgliedstaaten des Europarats und von den »Beobachtern« USA, Kanada, Japan und Südafrika unterzeichnet und ist 2004 nach der Ratifikation durch die ersten fünf Unterzeichnerländer in Kraft getreten. Mitte 2007 hatten schon 43 Länder die Konvention unterzeichnet und 21 ratifiziert. Deutschland hat – obwohl es zu den Erstunterzeichnern gehörte – den Ratifikationsprozess allerdings bis Anfang 2008 nicht abgeschlossen. Was die hier betrachteten Formen von Internetkriminalität betrifft, vor allem die Internetkriminalität im engeren Sinne und die inhaltsbezogenen Rechtsverletzungen im Bereich der Kinderpornographie, ist das Budapester Abkommen *das* internationale Referenzdokument.

Die Konvention verweist zwar auch auf Verletzungen des Urheberrechtsschutzes, aber für die in diesen Bereich fallenden Gebiete sind die im Rahmen der WTO, der WIPO und der EU vereinbarten Regelungen einschlägiger. Die internationale Standardisierung des Urheberrechts ist (insbesondere im Vergleich zur politischen Kooperation in anderen Problembereichen der Internetkriminalität) nicht zuletzt auf Betreiben der betreffenden Industriezweige sehr weit vorangeschritten. Schon 1994 wurde mit Gründung der Welthandelsorganisation (WTO) auch das TRIPS-Abkommen unterzeichnet, das Mindeststandards für handelsbezogene Aspekte der Rechte des geistigen Eigentums definiert hat. Zwei Jahre später verabschiedete die World Intellectual Property Organization (WIPO) den »WIPO-Urheberrechtsvertrag« (WIPO Copyright Treaty, WCT), der ausdrücklich der Anpassung des Urheberrechts an für das Informationszeitalter dienen sollte. Der WCT wurde mittlerweile sowohl in den USA (mit dem Digital Millennium Copyright Act [DMCA] von 1998) als auch in der Europäischen Union (mit der EU-Urheberrechtsrichtlinie von 2001[69]) umgesetzt. In Deutschland wiederum hat die EU-Richtlinie im Jahr 2003 zu einer ersten Reform des Urheberrechts geführt. Eine weitere Novelle, die unter anderem das Herunterladen offensichtlicher Raubkopien aus »Peer-to-Peer«-Netzwerken für illegal erklärt, wurde Anfang Juli 2007 vom Bundestag verabschiedet.[70] Insgesamt weisen die Regelungen für den Urheberrechtsschutz einen Grad an Harmonisierung auf, der deutlich über demjenigen liegt, der für die Regelungsbereiche der »Cybercrime Convention« erreicht worden ist.

Häufig wird im Zusammenhang mit Internetkriminalität das Argument vorgebracht, dass internationale Harmonisierungsbestrebungen nur dann sinnvoll sein könnten, wenn wirklich alle Staaten daran beteiligt sind, denn angesichts der extrem niedrigen Transaktionskosten beim digitalen Datentransfer sei es für die betreffenden Akteure ein Leichtes, Daten in einen Staat zu verlagern, der an der Harmonisierung nicht teilhat und insofern einen »sicheren Hafen« darstellt. Da es für die Internetnutzer ohne Belang sei, woher die Daten kommen, seien solche nicht-universellen Konventionen somit zur Ineffektivität verurteilt. Global gültige Regelungen seien aber kaum zu erreichen. Dem lässt sich entgegenhalten, dass dieses Argument

69 Richtlinie 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft.
70 Bundesministerium der Justiz, *Bundestag beschließt Novelle des Urheberrechts*, Berlin 2007, Pressemitteilung vom 5.7.2007.

allenfalls auf bestimmte Formen von Internetkriminalität zutreffen kann, insbesondere auf Urheberrechtsverletzungen und inhaltsbezogene Rechtsverletzungen, bei denen größere Datenmengen auf bestimmten Servern abgelegt werden. Diejenigen Rechtsverletzungen, die sich auf Transaktionen wie »Phishing« oder auch »Cyberterrorismus« beziehen, sind davon kaum betroffen. Vor allem aber gilt, dass es eine erhebliche Wirkung hat, wenn diejenigen Staaten, die eine gut ausgebaute Internetinfrastruktur aufweisen, regulativ voranschreiten, denn erstens erfüllen sie eine Vorbildfunktion (auch bei der »Cybercrime-Convention« haben sich etliche Staaten erst nachträglich angeschlossen) und zweitens sinkt die Attraktivität von Datenverlagerungen deutlich, wenn man die »dichten« Zonen des Internets verlässt. Das Internet mag keine Grenzen kennen, aber es gibt sehr wohl ein »Zentrum« und eine »Peripherie«, definiert durch die Anschlussdichte und die »Bandbreite«, sprich die Datenübertragungsrate der jeweiligen Verbindungen.

Daraus ergeben sich unmittelbar zwei Konsequenzen: Erstens ist es ein wichtiges Ziel, die Harmonisierung der Definition und Inkriminierung bestimmter Transaktionsformen im Internet weiter voranzutreiben. So verfügen bisher nur 36 Staaten weltweit überhaupt über eine eigene rechtsverbindliche Definition von Kinderpornographie und nur 10 über gesetzliche Bestimmungen, wonach Internet-Service-Provider kinderpornographische Abbildungen automatisch zur Anzeige bringen müssen.[71] Selbst innerhalb Europas ist man sich noch nicht einmal über die Definition des Begriffs »Kind« einig. Zweitens: Bei jedem derartigen Regelungsversuch ist es von großer Bedeutung, die Reichweite der internationalen Harmonisierung möglichst auszudehnen, wobei diejenigen Länder mit einem signifikanten Anteil am globalen Internet Priorität genießen. In diesem Fall ist die absolute, nicht die relative Anzahl von Internethosts ein sinnvoller Indikator. Allein in den G8-Staaten sind fast 75 Prozent aller Internethosts registriert (Stand: Januar 2007). Deshalb gilt: Wenn nur die G8-Staaten die Harmonisierung ihrer Regelungen vorantreiben, ist bereits sehr viel erreicht. Wendet man diese Logik auf die Budapester Konvention an, wird allerdings deutlich, dass es zumindest einen Bereich gibt, wo es auch in Zukunft sehr schwer sein wird, signifikante Fortschritte zu erzielen: Bei den inhaltsbezogenen Regelverletzungen dürften die USA kaum bereit sein, von ihren »Free Speech«-Prinzipien abzurücken.[72] Sie haben im Rahmen der Budapester Verhandlungen verhindert, dass Regelungen zu »Hate Speech« in den Haupttext der Konvention aufgenommen werden. Die übrigen Staaten haben sich daraufhin auf ein entsprechendes Zusatzprotokoll für rassistische und xenophobe Kommunikationsinhalte geeinigt, das inzwischen auch 30 Staaten unterzeichnet haben. Aber ohne die Teilnahme der USA mit ihrer großen Bedeutung innerhalb der Gesamtinfrastruktur des Netzes wird dieses Protokoll in seiner Effektivität auf absehbare Zeit begrenzt bleiben.

Die internationale Harmonisierung der Regelungen zur Bekämpfung der Internetkriminalität bleibt ein wichtiges Desiderat, auch wenn für einige Bereiche bereits erste Fortschritte erreicht worden sind. Künftig gilt es, *weitere Regelungsbereiche zu harmonisieren* und *möglichst viele Länder zur Übernahme der harmonisierten Regelungen zu bewegen*. Besonders wichtig ist es, diejenigen Staaten zu integrieren, die eine zentrale Rolle als Standorte für Internetkommunikation spielen. Umgekehrt bedeutet dies aber auch, dass jene Bereiche, in denen sich kein Konsens unter den »großen Internetländern« finden lässt, sich letztlich kaum wirkungsvoll werden verregeln lassen.

Kooperation: Internationale Zusammenarbeit bei der Implementation

Das unmittelbare Pendant zur »Harmonisierung« ist die internationale Kooperation bei der Implementation von Regelungen zur Bekämpfung der Internetkriminalität und bei der Rechtsdurchsetzung und Sanktionierung. Hier sind verschiedene Formen der internationalen Abstimmung denkbar: Zum einen gibt es zahlreiche Möglichkeiten der Kooperation zwischen staatlichen Instanzen, zum anderen können aber auch private Akteure entweder mit oder ohne staatliche Institutionen grenzüberschreitend zusammenarbeiten.

Auf staatlicher Ebene sind es vor allem die Justiz- und Strafverfolgungsbehörden, die ihr Vorgehen

71 International Centre for Missing & Exploited Children, *Child Pornography: Model Legislation & Global Review 2006*, Alexandria, VA, 2006, <www.icmec.org/en_X1/pdf/English_2nd_Edition.pdf> (Zugriff 14.4.2008).

72 Nach dem 11. September hat es in den USA im Rahmen der Terrorbekämpfung zwar marginale Einschränkungen des »Free Speech«-Prinzips gegeben, aber substantielle Regelungen, die wie in anderen Ländern auf breiter Ebene Äußerungsdelikte definieren würden, spielen in der politischen Diskussion praktisch keine Rolle.

koordinieren sollten. Für Deutschland ist dabei an erster Stelle die bewährte und in den letzten Jahren weiter ausgebaute Kooperation im Rahmen der »Dritten Säule« der EU zu nennen. Insbesondere die Einheit für justizielle Zusammenarbeit (Eurojust) und Europol (aber auch Interpol) spielen eine wichtige Rolle bei der Koordination von Polizeiaktionen – speziell im Bereich der Kinderpornographie. Im Juni 2005 arbeiteten bei einer solchen Operation erstmals die Strafverfolgungsbehörden von 13 europäischen Staaten unter der Regie von Europol zusammen.[73] Mittlerweile hat es zahlreiche weitere Aktionen dieser Art gegeben. Zuletzt wurde im November 2007 ein spektakulärer Schlag gegen einen Kinderpornographie-Ring im Internet bekannt, bei dem circa 2500 Verdächtige identifiziert werden konnten. 19 nationale Polizeibehörden waren unter der Leitung von Eurojust und Europol daran beteiligt.[74]

Jenseits der EU hat die G8 seit 1997 eine »Subgroup on High-Tech Crime« etabliert, die ihrerseits die Einrichtung eines Informationsnetzwerks vorangetrieben hat, über das die Mitgliedstaaten Informationen über alle Arten von Internetkriminalität kurzfristig und rund um die Uhr austauschen können. In Deutschland dient eine eigene Stelle des BKA als »Point of Contact« dieses Netzwerks. Mittlerweile sind mehr als 40 Staaten Mitglieder dieser Struktur. Die Vernetzung ist ein Beleg dafür, wie die Digitalisierung auch für die Bekämpfung der Internetkriminalität neue Möglichkeiten schafft.

Ein Beispiel für eine grenzüberschreitende Zusammenarbeit von staatlichen und nichtstaatlichen Stellen findet sich im Kontext der EU-Initiative »Safer Internet Action Plan.«[75] Mit Mitteln dieses Programms wird die »International Association of Internet Hotlines (INHOPE)« finanziell unterstützt, in der private und öffentliche Organisatoren von Telefon- bzw. Internet-Hotlines aus 18 europäischen Ländern kooperieren. INHOPE nimmt Beschwerden über illegale Kommunikationsinhalte entgegen, Schwerpunkt ist die Bekämpfung der Kinderpornographie. Ein rein privates Modell internationaler Zusammenarbeit ist die »Platform for Internet Content Selection (PICS)«, ein Projekt, bei dem Webseiten nach einem internationalen Standard gekennzeichnet werden, um zum Beispiel jugendgefährdende Inhalte aus dem Internetangebot auszufiltern. Getragen wird PICS vom »World Wide Web Consortium (W3C)«, einem Zusammenschluss von mehr als 400 Internet- und Kommunikationsfirmen weltweit.

Die oben genannten Beispiele internationaler Kooperation sind zweifelsohne zu begrüßen, aber in Anbetracht der diagnostizierten Trends ist diese Form der Zusammenarbeit ganz offensichtlich nicht hinreichend. Noch immer gelingt es Internetkriminellen viel zu leicht und viel zu schnell, sich in den »grenzenlosen Raum« des Internets zurückzuziehen bzw. ihre Identität und ihre Transaktionen zu verschleiern. Das gilt insbesondere für Internetkriminalität im engeren Sinne, aber auch für »traditionelle Kriminalität« und zumindest einige Formen der inhaltsbezogenen Rechtsverletzungen. Daher kann die Handlungsempfehlung nur lauten: *Mehr vom Gleichen!* Angesichts der universalen Struktur des Netzes darf internationale Kooperation nicht die Ausnahme sein, sondern muss zum Regelfall werden. Das Ziel sollte sein, fast ebenso schnell international reagieren zu können, wie die illegalen Transaktionen Grenzen überschreiten.

Adaption: Anpassung nationaler Regelungen

Deutschland hat frühzeitig damit begonnen, sein Rechtssystem an die Herausforderung der Digitalisierung anzupassen. Seit Mitte der achtziger Jahre gibt es im deutschen Strafrecht spezifische Bestimmungen zur Computerkriminalität. Darunter fallen beispielsweise Regelungen gegen das, was man mittlerweile als »Phishing« bzw. »traditionelle Kriminalität via Internet« bezeichnen würde (§§ 202a/b und 263 StGB), oder einige Verbote, die sich heute unter der Rubrik »Internetkriminalität im engeren Sinne« subsumieren lassen (z.B. »Datenveränderung« und »Computersabotage« nach §§ 303a/b StGB). Kurz vor und nach der Jahrtausendwende sind eine ganze Reihe weiterer Neuerungen und Änderungen in den bestehenden Regelkatalog aufgenommen worden. Erwähnenswert ist in diesem Zusammenhang vor allem das »Informations- und Kommunikationsdienste-Gesetz (IuKDG)« von 1997, das nicht nur in seinem ersten Teil, dem neuen »Teledienstegesetz« (TDG), die rechtliche Verantwortlichkeit für Kommunikationsinhalte im Internet regelte, sondern auch im StGB, im Urheberrecht und im Jugendschutzgesetz etliche Anpassungen

73 European Law Enforcement Cooperation (Europol), *Annual Report 2005*, Den Haag 2006, S. 7.

74 Europol, *Worldwide Child Sex Offender Network Dismantled*, Presseerklärung vom 5.11.2007, <www.europol.europa.eu/index.asp?page=news&news=pr071105.htm> (Zugriff 14.4.2008).

75 Mittlerweile wurde der »Plan« abgelöst durch das »Safer Internet plus Programme« für 2005–2008.

vornahm und damit die Anwendbarkeit der vorhandenen Normen auf das Internet sicherstellte. Wichtig waren auch die im Jahr 2002 vorgenommenen Änderungen an der Strafprozessordnung, denen zufolge Internet-Service-Provider nun verpflichtet sind, auf Anfrage durch die Strafverfolgungsbehörden die IP-Adressen und damit die Adressen der Anschlussinhaber offenzulegen, die an illegalen Transaktionen beteiligt waren (§§ 100g/h StPO). Weitere neue Regelungen finden sich zum Beispiel in der 2004 überarbeiteten Fassung des »Gesetzes gegen den unlauteren Wettbewerb« (UWG), in der die Illegalität von »Spam« klargestellt wird (§ 7) oder in den Überarbeitungen der strafrechtlichen Bestimmungen im Bereich der Kinderpornographie aus demselben Jahr (§ 184b StGB). Auch das Urheberrecht ist 2003 und erneut 2007 überarbeitet und an die spezifischen Herausforderungen angepasst worden, die von der Digitalisierung im Allgemeinen und dem Internet im Besonderen ausgehen. Hinzu kommen richterrechtliche Weiterentwicklungen des bestehenden Regelkatalogs, die allerdings nicht ganz unumstritten sind, wie zum Beispiel die bereits erwähnte Entscheidung des BGH aus dem Jahr 2000, wonach auch das Einstellen illegaler Inhalte auf Internetservern im Ausland durch Ausländer in Deutschland strafbar ist.[76]

Insgesamt lässt sich resümieren, dass es auf dem Gebiet des Rechts einige Baustellen gibt, von denen ein Teil wohl auch noch längere Zeit bestehen bleiben wird. So müssen zum Beispiel die vorhandenen Gesetze kontinuierlich an die sich ändernden technischen Gegebenheiten angepasst, die existierenden Regelungen weiter konkretisiert und nicht zuletzt die erwähnte Budapester Konvention ratifiziert und umgesetzt werden. Über das gesamte Spektrum der Internetkriminalität hinweg gesehen gibt es derzeit in Deutschland jedoch nur noch vergleichsweise geringe rechtliche Unsicherheiten. Dass entsprechende Transaktionen nach deutschem Recht tatsächlich Regelverstöße darstellen, ist – bei allen Problemen im Detail – relativ klar. Zwei Aspekte sind jedoch anzumerken:

Erstens: Es gibt zwar Bereiche, wo die Überarbeitung des nationalen Rechts auf internationale Initiativen zurückgeht (beim Urheberrechtsschutz waren es die WTO, die WIPO und die EU, bei der Budapester Konvention der Europarat), aber insgesamt ist die Anpassung nationaler Regelungen bisher wesentlich intensiver betrieben worden als die internationale Harmonisierung. Dieses *Missverhältnis zwischen Integration und Adaption* ist angesichts der grenzüberschreitenden Struktur des Internets äußerst problematisch. Es hilft beispielsweise wenig, wenn die Verteilung von »Spam« zwar nach deutschem Recht eindeutig illegal ist, aber vom Ausland aus massenhaft ungestört erfolgt und deutsche Nutzer behindert. Ebenso hat das TDG zwar klargestellt, dass Internet-Zugangsprovider nicht für Inhalte verantwortlich sind, die sie lediglich durchleiten. Die Tatsache jedoch, dass man die Provider für diejenigen Inhalte, die sie im Ausland einspeisen, nur schwer zur Verantwortung ziehen kann, impliziert aber gleichzeitig, dass man heute nach deutschem Recht illegale Inhalte massenhaft hinnehmen muss. Jeder nationale Anpassungsschritt müsste daher daraufhin untersucht werden, ob er sich im einzelstaatlichen Rahmen implementieren bzw. effektiv durchsetzen lässt. Wenn dies nicht der Fall ist, müssen die politischen Verantwortlichen prüfen, welche internationalen Harmonisierungs- oder Kooperationsmaßnahmen erforderlich sind, um die Durchsetzung des Rechts zu gewährleisten.

Zweitens: An das oben genannte Argument knüpft sich die Frage, inwieweit die Möglichkeit der *Rechtsdurchsetzung ein Kriterium für die Regelanpassung* sein sollte. Zwei Probleme stellen sich hier: Es ist absehbar, dass im Bereich der politisch motivierten Äußerungsdelikte eine internationale Harmonisierung nur auf einem Regelungsniveau deutlich unterhalb der deutschen Standards möglich sein wird und sich die USA nicht einmal an einem solchen Konsens beteiligen würden. Das bedeutet, dass man nach deutschem Recht illegale Transaktionen selbst dann nicht wirksam wird verhindern können, wenn deutsche Internetnutzer daran beteiligt sind. Ebenso ist offensichtlich, dass sich die Bestimmungen zum Urheberrechtsschutz in ihrer jetzigen Form nicht durchsetzen lassen werden. Die entsprechenden rechtlichen Überarbeitungen in den Jahren 2003, 2007 und 2008 haben die Rechte der Urheber und Verwerter zwar bestätigt und gestärkt, im Ergebnis aber haben sie vor allem bestimmte Transaktionen, die millionenfach insbesondere von jungen Leute durchgeführt werden, rechtlich zu »bagatellartigen Massendelikten«[77] gemacht. Im Juli 2007 hat es das Amtsgericht Offenburg in einem Filesharing-Fall wegen offensichtlicher Unverhältnismäßigkeit abgelehnt, die Adressen von Internetnutzern über die IP-Adressdaten nach § 100g StPO zu

76 Vgl. BGH, Urteil vom 12.12.2000, 1 StR 184/00.

77 Vgl. Rüther, »Betrugsdelikte im Internet« [wie Fn. 13], S. 81.

ermitteln.[78] In der Folge forderten die betroffenen Branchen (vor allem die Musik- und Filmproduzenten) vom Gesetzgeber, eine Regelung zu schaffen, die ihnen auch ohne Strafverfahren erlauben würde, an solche Adressen zu kommen, um ihre zivilrechtlichen Ansprüche durchzusetzen. Aus gutem Grund waren diese Forderungen allerdings äußerst umstritten.[79] Trotzdem hat der Bundestag im April 2008 eine entsprechende Regelung verabschiedet, die jedoch entgegen den Wünschen der Industrie einen Richtervorbehalt und eine Einschränkung auf Rechteverletzungen im »gewerblichen Ausmaß« vorsieht.[80] Eine Prozessflut und ein kaum lösbarer Streit über die Definition des »gewerblichen Ausmaßes« und über die tatsächliche Schadenshöhe sind abzusehen. Darüber hinaus werden sich früher oder später ohne Zweifel technische Wege finden, wie »Downloader« ihre Identität verschleiern können. Beim Urheberrecht kommt hinzu, dass den meisten Jugendlichen ein Unrechtsbewusstsein vollständig abgeht und bezweifelt werden darf, dass Maßnahmen wie die Kampagne »Kopien brauchen Originale« des Bundesministeriums der Justiz (BMJ) oder gar »Raubkopierer sind Verbrecher« (getragen von Verbänden der Filmindustrie) tatsächlich dazu beitragen, ein solches Bewusstsein zu schaffen. Beim Urheberrechtsschutz wie bei den politisch motivierten Äußerungsdelikten stellt sich daher die Frage, ob mit den jeweiligen Rechtsanpassungen den dahinter stehenden Rechtsgütern tatsächlich entsprochen worden ist. Das klassische Motto der Rechtsanpassungen in den letzten 15 Jahren lautete: »Was offline illegal ist, ist auch online illegal.« Bei dieser Form der Adaption wird sich aber langfristig die Frage nicht vermeiden lassen, ob offline auf Dauer illegal bleiben kann, was sich online nicht durchsetzen lässt. Letztlich steht die Glaubwürdigkeit von Normen, die sich nicht implementieren lassen, zur Disposition. Es ist sinnvoll, bei Rechtsanpassungen die Möglichkeit der Rechtsdurchsetzung immer mitzudenken und gegebenenfalls regulative Alternativen ins Auge zu fassen. Konkret könnte man fragen: Wie kann man in Zeiten des Internets den Rechtsradikalismus wirksam bekämpfen? Oder: Wie kann man im digitalen Zeitalter die Rechte der Urheber wahren? Stattdessen ist bisher häufig einfach das bestehende Recht angepasst und fortgeschrieben worden.

Innovation: Neue Modelle der Implementation

Es ist umso ratsamer, sich die oben angemahnte Perspektive zu eigen zu machen, weil sich manche Regelungen in Zeiten der Globalisierung und Digitalisierung eben nicht mehr implementieren lassen, indem man allein auf traditionelle Mechanismen wie bürokratische Verwaltung bzw. juristische Mittel baut. Ein Beispiel aus dem Bereich des Jugendschutzes kann diese Problematik schlaglichtartig beleuchten. Hier haben Gerichte versucht, verstärkt die Internet-Service-Provider in die Pflicht zu nehmen, um den Zugang zu bestimmen Seiten zu sperren, weil man der Anbieter jugendgefährdender Inhalte im Ausland nicht habhaft werden kann.[81] Die technische Effektivität solcher Sperren muss jedoch bezweifelt werden, und in den bisherigen Fällen war es so, dass die Wirkung der Blockademaßnahme in keinem Verhältnis zum Volumen des im Internet nach wie vor frei erhältlichen jugendgefährdenden Materials stand.[82]

Dieser Fall illustriert, dass bei der Implementation von Regelungen zur Bekämpfung der Internetkriminalität notwendigerweise neue Wege gegangen werden müssen und ein erhebliches Maß an Innovation gefordert ist. In der Tat gibt es schon einige bemerkenswerte Initiativen: In den letzten 15 Jahren sind mit Blick auf die Herausforderungen durch das Internet in Deutschland Institutionen und Verfahren entstanden, die durchaus als innovativ gelten dürfen: So wurde bereits 1991 ein eigenes *Bundesamt für Sicherheit in der Informationstechnik* (BSI) geschaffen. Das BSI greift weder regulativ ein, noch implementiert es im klassischen Sinne. Stattdessen prüft es, berät es, zertifiziert es und informiert es in allen Sicherheitsbelangen der elektronischen Datenverarbeitung, und es konzipiert darüber

78 Beschluss des Amtsgerichts Offenburg, Az4 Gs 442/07.

79 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit: Schaar gegen Direktzugriff der Musik- und Filmindustrie auf Internetnutzungsdaten, Pressemitteilung vom 20.6.2007.

80 Bundesministerium der Justiz, *Bundestag verabschiedet Gesetz zum Schutz geistigen Eigentums*, Pressemitteilung vom 11.4.2008.

81 Vgl. z.B. Heise News 2007: *Arcor muss YouPorn sperren*, 19.10.2007, <www.heise.de/newsticker/meldung/97676> (Zugriff 11.11.2007).

82 Außerdem ist es nicht ohne Ironie, dass solche Maßnahmen bisher vor allem dann in die Diskussion kamen, wenn deutsche Anbieter pornographischer Produkte sich auf das Wettbewerbsrecht beriefen und in der freien Verfügbarkeit entsprechenden Materials im Internet einen unfairen Wettbewerbsnachteil sahen, Stefan Krempl, »Sperren für den Jugendschutz. Schlammschlacht in der Erotik-Branche«, in *c't*, 23/2007, S. 88–89.

hinaus auch eigene Sicherheitslösungen. Das Bundesamt ist damit eine in Europa weitgehend einmalige Institution, der vor allem bei der Bekämpfung der Internetkriminalität im engeren Sinne und des Cyberterrorismus eine große Bedeutung zukommt. Angesichts der Tatsache, dass es erstens bisher primär die private Industrie ist, die (kostenpflichtige) Lösungen für die Probleme der Internetkriminalität im engeren Sinne bereitstellt, und es zweitens nicht sicher ist, ob die Wirtschaft allein in der Lage ist, die Gefahren effektiv abzuwehren, scheint es angeraten, das *BSI in seinen Kompetenzen zu stärken, seine Finanzierung zu erhöhen und seine Kooperation mit der Wirtschaft und mit internationalen Partnern auszubauen*.

Auch im Bereich der Polizeiarbeit hat man versucht, sich den durch das Internet veränderten Gegebenheiten anzupassen. Im Laufe der neunziger Jahre gab es parallel zur Ausbreitung des Internets verschiedene Initiativen zunächst der Landeskriminalämter, im Internet aktiv zu werden. Bayern etwa gehörte zu den ersten Bundesländern, die eine »Streife im Internet« einführten, bei der Beamte das Netz ohne konkreten Anlass oder Verdacht nach illegalen Angeboten oder sonstigen Spuren von Straftaten durchforsten. 1999 wurde dann auch beim BKA eine »Zentralstelle für anlassunabhängige Recherche in Datennetzen (ZaRD)« eingerichtet. Erwähnenswert ist auch das Gemeinsame Internetzentrum (GIZ), das Anfang 2007 in Berlin gegründet wurde. Dort arbeiten Mitarbeiter des Bundesamts für Verfassungsschutz, des Bundeskriminalamts, des Bundesnachrichtendiensts, des Militärischen Abschirmdiensts und des Generalbundesanwalts bei der Bekämpfung von Extremismus und Terrorismus zusammen. Die Aktivitäten der Landeskriminalämter gibt es jedoch nach wie vor, und sie führen teilweise auch zu spektakulären Erfolgen.[83] Trotzdem erscheint eine *Bündelung der Aktivitäten* bei einer gleichzeitigen Verlagerung der entsprechenden Ressourcen sinnvoll. Gegenüber Kriminalitätsformen, für die Grenzen eine derart geringe Rolle spielen, wirkt die deutsche föderale Kompetenzverteilung in den Bereichen Polizeiarbeit und Strafverfolgung anachronistisch. Eine Bündelung der Kompetenzen könnte erstens die Effizienz erhöhen (Doppelungen bei den Suchaktionen könnten vermieden werden, die technische Kompetenz und Reaktionsgeschwindigkeit ließen sich erhöhen), und zweitens würde die internationale Kooperation erleichtert, weil es in Deutschland nur noch einen einzigen Ansprechpartner gäbe.

Änderungen an der StPO haben weitere Innovationen in der Polizeiarbeit möglich gemacht. Ein Beispiel ist die nun zulässige Aufklärung von Computerstandorten über IP-Adressinformationen der Provider (siehe oben, S. 29.). Gegenwärtig wird diskutiert, ob Verfassungsschutz und Strafverfolgungsbehörden das Recht zu »Online-Durchsuchungen« bekommen sollen, was die Ausspähung von Computerdaten über das Internet ohne Wissen des jeweiligen PC-Nutzers erlauben würde. Weil eine Software, die diesen Zweck erfüllt, technisch Ähnlichkeit mit »Malware« hätte, sprach man auch vom »Bundestrojaner«. Allerdings ist die Einführung der »Online-Durchsuchung« sehr umstritten. Während das Bundesinnenministerium argumentiert, diese Ermittlungsmöglichkeit sei in Zeiten der Internetkriminalität vor allem bei der Straf- und Terrorprävention ein unverzichtbares Werkzeug, sehen Gegner die Einführung solcher Maßnahmen als »Schritt in den Überwachungsstaat«. Das Bundesverfassungsgericht hat das Instrument der »Online-Durchsuchung« in einem Urteil über eine Novelle des nordrhein-westfälischen Verfassungsschutzgesetzes zwar prinzipiell für verfassungsrechtlich möglich erklärt, ihr jedoch gleichzeitig enge Grenzen gezogen. Das Gericht ging dabei davon aus, dass als Teil des allgemeinen Persönlichkeitsrechts ein Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme existiert.[84] Am Fall der Online-Durchsuchung wird exemplarisch deutlich, dass die Politik eine Wahl treffen muss zwischen dem technisch möglichen Maß an Kontrolle einerseits und dem Gebot der Wahrung der Grundfreiheiten und -rechte andererseits. Im vorliegenden Fall hat das Verfassungsgericht allerdings deutlich gemacht, dass eine freiheitliche Verfassung dieser Wahlmöglichkeit Grenzen setzt. Es empfiehlt sich, in Zukunft bereits im politischen Prozess eine abgewogene Entscheidung zu treffen, damit diese Grenzziehung nicht immer wieder dem Verfassungsgericht überlassen bleibt.

Darüber hinaus haben sich vor allem im Zusammenhang mit inhaltsbezogenen Regelverletzungen diverse Formen der Zusammenarbeit zwischen Staat und Wirtschaft entwickelt – entweder in Gestalt von »Public-Private-Partnerships (PPPs)« oder von Selbst-

83 Wie z.B. bei der Aktion des baden-württembergischen LKA gegen Kinderpornographie im Jahr 2007, vgl. Fn. 36.

84 Bundesverfassungsgericht, *Vorschriften im Verfassungsschutzgesetz NRW zur Online-Durchsuchung und zur Aufklärung des Internet nichtig*, Pressemitteilung vom 27.2.2008, Karlsruhe 2008, <www.bundesverfassungsgericht.de/pressemitteilungen/bvg08-022.html> (Zugriff 14.4.2008).

regulierungsmodellen, die sich teilweise an die in Deutschland im Medienbereich üblichen Strukturen der staatlich-privaten Koregulierung anlehnten. Bereits 1997 wurde nach dem Vorbild der Filmwirtschaft ein Verein »Freiwillige Selbstkontrolle Multimedia-Diensteanbieter (FSM)« gegründet, der die Anbieter von Online-Inhalten unter dem Aspekt der Einhaltung des Jugendschutzes berät und mit der Bundesprüfstelle für jugendgefährdende Medien (BPjM; vor 2003 »Bundesprüfstelle für jugendgefährdende Schriften«) zusammenarbeitet. Ein weiteres Beispiel ist das Netzwerk »Klicksafe.de«, das auf eine Initiative des »Safer Internet«-Programms der Europäischen Kommission zurückgeht und dessen Aufgabe vor allem darin besteht, über Internetgefährdungen aufzuklären und die Kompetenz der Nutzer im Umgang mit dem neuen Medium zu erhöhen. Ähnliche Ziele verfolgt auch der Verein »Deutschland sicher im Netz«, in dem sich große IT-Firmen, die FSM und Bitcom (der Branchenverband der Telekommunikationswirtschaft) zusammengeschlossen haben und der mit dem Bundesinnenministerium kooperiert.[85]

Die Beispiele zeigen bereits, worin das Grundproblem in diesem Bereich liegt: Die Landschaft der Initiativen zum Jugendschutz im Internet, zur Aufklärung und Weiterbildung der Nutzer und zur Erhöhung der Medienkompetenz ist sehr stark zerklüftet. Allein in der Initiative »Klicksafe.de« kooperieren nicht weniger als 39 Partnerunternehmen, -organisationen und -verbände. Aus Sicht der Nutzer ist weitgehend unklar, an welche Stelle man sich mit einer Beschwerde wenden kann. Da Internetkriminalität nur aussichtsreich bekämpft werden kann, wenn der einzelne Internetnutzer Mitverantwortung übernimmt, wäre es zweckmäßig, wenn es eine *zentrale Informations- und Beschwerdestelle für alle Formen der Internetkriminalität* gäbe, die als »Leuchtturm« fungieren könnte und sicherstellen würde, dass die entsprechenden Hinweise an die zuständigen Firmen, Einrichtungen und Behörden weitergegeben werden. Ob diese Institution staatlich oder nichtstaatlich getragen ist, dürfte von nachrangiger Bedeutung sein.

Schließlich ist darauf hinzuweisen, dass es neben den erwähnten Maßnahmen dringend geboten ist, den Kenntnisstand über Internetkriminalität zu erhöhen. Die Anzahl entsprechender Studien ist gering und in den meisten vorliegenden Untersuchungen werden nur kleinere Teilaspekte der Internetproblematik beleuchtet. Zudem ist die Datenlage teilweise ausgesprochen dürftig bzw. zweifelhaft. Die Palette der in diesem Kontext notwendigen Forschungsarbeiten reicht von kriminologischen Hintergrundanalysen zu den »Tätern« über ökonomische Untersuchungen zu den Effekten der Internetkriminalität bis zu sozialwissenschaftlichen Studien zu möglichen innovativen Regelungsformen und Modellen der internationalen Kooperation. Neben den oben skizzierten Maßnahmen ist daher die *Förderung der Forschung zur Internetkriminalität* ein sehr wichtiges und bisher eher vernachlässigtes Instrument, um dem Problem zu begegnen. Das 2007 aufgelegte Programm der Bundesregierung zur Sicherheitsforschung dürfte hier kaum Fortschritte bringen, da es primär auf klassische Sicherheitsfragen (Katastrophenschutz, Gefahrstoffsicherung, Schutz von Verkehrsinfrastrukturen etc.) ausgerichtet ist.

85 BMI, *Bundesinnenministerium und »Deutschland sicher im Netz« vereinbaren Kooperation*, Pressemitteilung vom 20.6.2007.

Fazit und politische Empfehlungen

Das Internet hat die Lebens- und Arbeitswelt grundlegend verändert. Für Millionen von Menschen ist es aus dem Alltag nicht mehr wegzudenken, und es ist davon auszugehen, dass seine Bedeutung weiter zunehmen wird. Gleichzeitig nehmen jedoch auch die Bedrohungen zu, die uns in Form der Internetkriminalität begegnen. Das Internet stellt dabei eine besondere Herausforderung dar, denn in diesem Medium überschneiden sich die Grundprozesse der »Digitalisierung« und der »Globalisierung«. Beide Prozesse erschweren es in erheblichem Maße, sowohl die Einhaltung der existierenden Regelungen zu kontrollieren als auch diese durchzusetzen, weil sie gewaltige Transaktionsströme mit sich bringen, die in kürzester Zeit den im wahrsten Sinne des Wortes »grenzenlosen« Raum des Internets durchqueren können. Zudem besteht zwischen dieser »Grenzenlosigkeit« und den zumeist national gebundenen Rechts- und Strafverfolgungssystemen ein grundlegendes Spannungsverhältnis.

Internetkriminalität tritt in zahlreichen Erscheinungsformen auf. Sie kann sich als herkömmliche Kriminalität »im Gewand« moderner Technik (z.B. bei Betrug und Urheberrechtsverletzungen) manifestieren, als unmittelbar technikbezogene »Internetkriminalität im engeren Sinne« (wie bei »Spam« oder »Viren«), als inhaltsbezogene Rechtsverletzung (terroristische Propaganda oder [Kinder-] Pornographie) oder in Form des »Cyberterrorismus«. Die vorliegenden empirischen Daten lassen dabei sowohl eine kriminelle Intensität als auch Entwicklungstrends erkennen, die als besorgniserregend bezeichnet werden müssen.

Gleichwohl bieten sich zahlreiche Reaktionsmöglichkeiten, die hier unter den Stichwörtern »Integration«, »Kooperation«, »Adaption« und »Innovation« zusammengefasst worden sind. Weder die internationale Gemeinschaft noch die Bundesrepublik sind auf diesen Gebieten untätig geblieben. Es gibt erfolgversprechende Ansätze der internationalen Integration und Kooperation. Auch im Bereich der Regelungsanpassung wurde in Deutschland schon einiges auf den Weg gebracht, und überdies wurden dabei durchaus innovative Implementationsformen entwickelt. Trotzdem verweisen die Trends der Internetkriminalität darauf, dass weiterhin dringender Handlungsbedarf besteht. Die folgenden Maßnahmen sollten dabei im Mittelpunkt stehen:

- Es gilt, die internationale Harmonisierung möglichst vieler internetrelevanter Regelungsbereiche weiter voranzutreiben. Das Gebot der Rechtsanpassung betrifft fast alle Varianten der Internetkriminalität, vor allem aber die neuen Betrugsformen und die Internetkriminalität im engeren Sinne. Besonders hier müsste der Dynamik neuer Bedrohungen eine Dynamik der Regelungsharmonisierung entsprechen. Aber auch im Bereich der Kinderpornographie, des Jugendschutzes und der rassistischen und xenophoben Kommunikationsinhalte sind selbst die Industrieländer von wirklich einheitlichen Standards noch weit entfernt.
- Bei diesen Harmonisierungsbemühungen ist es erforderlich, dass die Länder mit einem hohen absoluten Anteil der Internetnutzer voranschreiten. Dass der Europarat bisher eine so wichtige Rolle gespielt hat, ist zwar erfreulich, aber auch bezeichnend für die mangelnden Aktivitäten anderer Organisationen und Foren. Die G8 könnten als Vorreiter wesentlich mehr leisten als bisher, denn allein in den acht Staaten der Gruppe sind fast 75 Prozent aller Internethosts angesiedelt. Die G8 haben sich in der Vergangenheit vor allem mit der Bedrohung des Cyberterrorismus auseinandergesetzt. Doch sie könnten als Gruppe entscheidend dazu beitragen, das Thema Internetkriminalität in seiner ganzen Breite auf die internationale Tagesordnung zu setzen. Als Institution, in deren Rahmen dann die konkreten Harmonisierungs- und Kooperationsschritte weiter ausgearbeitet und koordiniert werden könnten, bietet sich die OECD an, denn in ihr sind nahezu alle Staaten mit dichter Internetstruktur organisiert. OECD-Leitlinien zu den oben genannten Themenbereichen kämen damit quasi einer »globalen Regelung« gleich und wären entsprechend effektiv.
- Gleichzeitig sollten die bereits vorhandenen Harmonisierungen auf eine möglichst große Zahl von Staaten ausgedehnt werden, um die Effektivität der Regelungen zu steigern und eine möglichst große Signalwirkung zu erzielen. Dies gilt für alle Regelungsbereiche der Budapester Konvention, ins-

besondere für die Internetkriminalität im engeren Sinne und für Kinderpornographie. Auch wenn sich die USA nicht anschließen werden, wäre es sinnvoll, möglichst viele Staaten auch für das Zusatzprotokoll der Konvention über rassistische und xenophobe Kommunikationsinhalte zu gewinnen. Derartige Maßnahmen sind allerdings nur dann zweckmäßig, wenn in den potentiellen Partnerländern auch die reale Möglichkeit existiert, gegen entsprechende Kriminalitätsformen vorzugehen. Sinnvollerweise muss die Ausdehnung der Rechtsharmonisierung daher – insbesondere für Staaten jenseits des OECD-Raumes – mit Maßnahmen des »Capacity-Building« einhergehen.

- Für Deutschland ist zu empfehlen, beim Kampf gegen die Internetkriminalität erstens die föderale Kompetenzverteilung zugunsten des Bundes zu zentralisieren und zweitens den gesamten Kriminalitätsbereich als Querschnittsthema aufzufassen und gemeinsame Einrichtungen zu schaffen, in denen verschiedene staatliche Behörden zusammenarbeiten. Das 2007 gegründete Gemeinsame Internetzentrum (GIZ) ist ein erster richtiger Schritt auf diesem Weg. Es bedarf aber im gesamten Spektrum der Internetkriminalitätsbekämpfung mehr solcher Zentren auf Bundesebene. So erfolgreich die Arbeit der LKAs im Einzelfall sein mag: Zentrale Institutionen sind gegenüber einer so globalisierten Struktur wie dem Internet effizienter; sie erleichtern die zwischenstaatliche Kooperation, und es ist deutlich einfacher, sie technisch auf dem neuesten Stand zu halten. Aus denselben Gründen sollte eine innovative Institution wie das Bundesamt für Sicherheit in der Informationstechnik als zentrale Einrichtung gestärkt werden – vor allem mit Blick auf die Internetkriminalität im engeren Sinne.
- Insbesondere in der Bekämpfung der »traditionellen Kriminalität« und der inhaltlichen Regelverletzungen sind zahlreiche nichtstaatliche Initiativen aktiv. Auch hier wäre es vorteilhaft, wenn sich die entsprechenden Einrichtungen – möglicherweise unter der »Schirmherrschaft« einer staatlichen Institution – bündeln würden. Für den Nutzer sollte ein einziger Ansprechpartner erkennbar sein, an den er sich mit allen Problemen der Internetkriminalität wenden kann und der gleichzeitig als Informationsquelle dient und sicherheitsrelevante Informationen zügig und zuverlässig verbreitet.
- Das Bestreben, die nationalen Gesetze und Regelungen an die durch das Internet veränderte Lage anzupassen, sollte sich mit Blick auf die internationale Rechtsharmonisierung daran orientieren, ob die jeweiligen Bestimmungen überhaupt durchsetzbar sind. Das gilt insbesondere für den Bereich der politisch motivierten Äußerungsdelikte und das Urheberrecht. Es ist fraglich, ob den zugrundeliegenden Rechtsgütern, aber auch dem Rechtsstaat ein Gefallen getan wird, wenn man an Regelungen festhält, deren Einhaltung sich im Zeitalter des Internets nicht mehr effektiv erzwingen lässt. Es geht nicht darum, dem Internet quasi »nachzugeben« und gesetzliche Bestimmungen »aufzugeben«, sondern darum, sich auf die eigentlichen Rechtsgüter (Ächtung des politischen Extremismus, angemessener Schutz der Urheberrechte) zu fokussieren. Eine einfache Fortschreibung des Rechts mit Blick auf das Internet unter Inkaufnahme einer Fülle von unverfolgten und unverfolgbaren bagatellartigen Massendelikten ist nicht zielführend.
- Die Prozesse der Digitalisierung und Globalisierung schaffen nicht nur Probleme für die Rechtsdurchsetzung; sie machen auch neue polizeiliche Ermittlungstechniken möglich. Bei deren Einführung muss allerdings sehr sorgfältig auf das Kosten-Nutzen-Verhältnis geachtet werden. Dabei sind unter »Kosten« vor allem Einschränkungen von Grundfreiheiten und Grundrechten zu verstehen. Es ist insbesondere zu berücksichtigen, dass dem Datenschutz und dem Recht auf informationelle Selbstbestimmung in Zeiten eines ubiquitären digitalen Mediums ein entscheidender Wert zukommt. Kriminalprävention und Strafverfolgung dürfen nicht mit signifikanten Einschnitten in einen Grundrechtsbereich erkauft werden, dessen Bedeutung nicht zuletzt aufgrund des Internets immer größer wird.
- Der Bereich der Internetkriminalität muss dringend weiter erforscht werden, insbesondere unter den Aspekten der globalen und nationalen Schadenswirkung, der Rechtsharmonisierung und der Regelungsinnovation. Auch hier ist eine Querschnittsbetrachtung gefordert, die der Komplexität des Themas gerecht wird. So unterschiedlich die jeweiligen Kriminalitätsformen sein mögen – das Internet mit seiner digitalen und globalisierten Struktur schafft spezifische Probleme, die unterschiedlichste Regelungsbereiche auf eine ähnliche Art und Weise empfindlich treffen.

Abkürzungen

ARPA	Advanced Research Projects Agency
BGH	Bundesgerichtshof
BKA	Bundeskriminalamt
BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz
BPjM	Bundesprüfstelle für jugendgefährdende Medien
BSA	Business Software Alliance
BSI	Bundesamt für Sicherheit in der Informationstechnik
CERN	Conseil Européen pour la Recherche Nucléaire
DoD	(U.S.) Department of Defense
DNS	Domain Name System
DoS	Denial of Service Attack
FBI	Federal Bureau of Investigation
FSM	Freiwillige Selbstkontrolle Multimedia-Diensteanbieter
FTC	Federal Trade Commission
G8	Gruppe der Acht (die sieben führenden westlichen Industriestaaten + Russland)
GIZ	Gemeinsames Internetzentrum
HTML	Hypertext Markup Language
IC3	Internet Crime Complaint Center
ICANN	Internet Corporation for Assigned Names and Numbers
IFPI	International Federation of the Phonographic Industry
INHOPE	International Association of Internet Hotlines
ISP	Internet Service Provider
IuKDG	Informations- und Kommunikationsdienste-Gesetz
LKA	Landeskriminalamt
MPA	Motion Picture Association
NCL	National Consumer League
NFIC/IFW	National Fraud Information Center/ Internet Fraud Watch
NSF	National Science Foundation
NW3C	National White Collar Crime Center
PCCIP	President's Commission on Critical Infrastructure Protection
PICS	Platform for Internet Content Selection
PIN	Personal Identification Number
PPP	Public Private Partnership
SRI	Stanford Research Institute
TAN	Transaktionsnummer
TCP/IP	Transfer Control Protocol/Internet Protocol
TDG	Teledienstegesetz
TRIPS	Trade Related Aspects of Intellectual Property Rights
WCT	WIPO Copyright Treaty
WIPO	World Intellectual Property Organization
W3C	World Wide Web Consortium
WTO	World Trade Organization
WWW	World Wide Web
ZaRD	Zentralstelle für anlassunabhängige Recherche in Datennetzen
ZfCh	Zentralstelle für das Chiffrierwesen