Internet-Devianz

KriminalPrävention

KriminalPrävention geht alle an.

geht alle an.

Internet - Devianz

Herausgeber:

Stiftung Deutsches Forum für Kriminalprävention (DFK)
c/o Bundesverwaltungsamt,
Gotlindestraße 91, 10365 Berlin

ISBN-10: 3-00-020166-1
ISBN-13: 978-3-00-020166-0

Vorwort

Das Internet hat sich seit den 90er Jahren des letzten Jahrhunderts sprunghaft vom Kommunikationsmedium elitärer, häufig wissenschaftlicher Kreise zum Massenmedium mit weltweit fast 1 Milliarde Nutzern entwickelt. Es wird gelegentlich als die größte technologische Revolution seit der Erfindung des Telefons beschrieben. Neben der vor allem passiven Informationsabfrage im World Wide Web (WWW) bietet das Internet vielfältigste Möglichkeiten - vom elektronischen Datenaustausch per E-Mail, über Chatrooms bis hin zur Fernsteuerung von Computern. Die wichtigste Veränderung stellt dabei die Befreiung der Sender und Empfänger von geografischen Schranken dar.

Die heutige globalisierte Informationsgesellschaft ist ohne das Internet nicht mehr denkbar. Begriffe wie eBanking, eLearning, eCommerce und eGovernment sind nicht nur Modeworte, sondern stehen beispielhaft für neue, sich ständig fortentwickelnde Formen der Interaktion in den vielfältigsten Lebensbereichen. In vielen Haushalten steht ein Computer mit Internet-Zugang und bereits Grundschulkinder sind mit den Funktionalitäten vertraut und im Internet ‚Zuhause'. Das Internet ist als Kommunikationsmedium sozusagen das Netz der sozialen und wirtschaftlichen Zukunft.

Doch jede nutzbringende Errungenschaft wird über kurz oder lang auch für kriminelle Zwecke missbraucht. So steht mit dem Internet nicht nur die Kommunikation mit allen Teilen der Welt offen, sondern die Nutzer werden auch zunehmend mit kriminellen und risikobehafteten Inhalten und Methoden konfrontiert. Das Spektrum reicht über Betrugsdelikte jeglicher Art bis hin zu verbotenen rechtsextremistischen oder kinderpornografischen Inhalten. Und auch seitens profilierter Anbieter wird Jugendmedienschutzaspekten im Internet nur ungenügend Rechnung getragen.

Der Schwerpunkt der Bekämpfungsansätze bei Internet-Devianz und -Kriminalität liegt bisher im technischen Bereich. Es zeigt sich aber immer wieder, dass Entwicklungen, die heute als Bahn brechend in Sachen Sicherheit im Internet angesehen werden, bereits morgen außer Kraft gesetzt sind. Es besteht ein ständiger Wettlauf zwischen der Sicherheitsindustrie und den zunehmend professionellen Tätern. Effektive technische Schutzvorkehrungen, die sowohl den Schutz der Kinder und Jugendlichen vor illegalen bzw. entwicklungsbeeinträchtigenden Inhalten als auch das Recht auf Meinungsäußerungsfreiheit und den möglichst freien Zugang zu Informationen hinreichend berücksichtigen, gibt es derzeit nicht. Hinzu kommt, dass selbst technisch perfekt abgesicherte Systeme nicht verhindern, dass mittels des Internet Straftaten wie Betrugsdelikte oder Verbreitung illegaler Inhalte begangen werden.

Die Konvergenz der Medien-Inhalte, Medien-Nutzung und Medien-Geräte nimmt zu, insbesondere der Anteil mobiler Geräte und Zugänge steigt. Die von der Anbieterseite gestaltete Entwicklung der Informationsgesellschaft stellt immer höhere Anforderungen an die Nutzer, die einen Großteil der Funktionalitäten moderner Geräte weder nutzen noch verstehen oder beherrschen. Die Komplexität der IT-Systeme überfordert die Anwender in

zunehmendem Maße. Die an sie gerichtete Erwartung, Vertrauen in die Technik zu entwickeln, wird vor dem Hintergrund der in immer kürzer werdenden Abständen auftretenden Sicherheitsprobleme und Gefahren kaum erfüllt werden.

Vor diesem Hintergrund erscheint es wesentlich, angesichts der Entwicklung der IT-Technik und IT-Sicherheitstechnik als geltende Rahmenbedingungen, den Menschen und sein Verhalten als wichtige kriminogene Faktoren im Zusammenhang mit Delinquenz im Internet in den Mittelpunkt der Betrachtung zu stellen. Es gilt sowohl Fragen der Entwicklung von Unrechts- wie Risikobewusstsein in der virtuellen Welt als auch einer effektiven zielgruppenspezifischen Vermittlung von umfassender Medienkompetenz im Umgang mit dem Internet und weiteren Online-Medien zu beleuchten, um auf dieser Grundlage eine zukunftsorientierte, systematische und umfassende Präventionskonzeption erarbeiten zu können. Eine darauf aufbauende Konzentration und Koordination der Präventionsmaßnahmen unterschiedlichster Akteure dürfte die Effektivität und Effizienz der Prävention steigern und zugleich zu einer Akzeptanzsteigerung des Internet beitragen.

Mit dem Ziel, hierzu einen grundlegenden Beitrag zu leisten, veranstaltete die Stiftung Deutsches Forum für Kriminalprävention (DFK) am 14. und 15. Februar 2006 in Bonn einen Workshop zur Konkretisierung des Forschungs- und Handlungsbedarfes zum Thema ‚Prävention von Devianz rund um das Internet', dessen Ergebnisse mit der vorliegenden Publikation unter dem Titel ‚Internet-Devianz' dokumentiert werden. Die Beiträge widmen sich im Schwerpunkt den Themenkomplexen ‚Internet und Gesellschaft', ‚Piraterie- und Betrugsdelikte', ‚Gewalt im Internet', ‚Umgang mit Viren, Würmern und anderen Schadprogrammen' sowie ‚Netzspezifische Medienkompetenz- und Präventionsinitiativen' und geben zum Schluss einen Ausblick auf erkannte Handlungs- und Forschungsfelder.

Der Dank des Deutschen Forums für Kriminalprävention gilt den Teilnehmerinnen und Teilnehmern für ihre Referate und die daraus hervorgegangenen Beiträge sowie dem Bundesministerium der Justiz und dem Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz für ihre logistische und finanzielle Unterstützung. Ein ganz besonderer Dank richtet sich an Frau Dr. Christiane Eichenberg (Universität zu Köln) und Herrn Dr. Werner Rüther (Universität Bonn) für die wissenschaftliche Vorbereitung und Leitung der Veranstaltung.

Joachim Eschemann
Projektleiter
Berlin, im Oktober 2006

Inhaltsverzeichnis

Medienentwicklung und neue Gewaltrisiken in der Informationsgesellschaft

Prof. Dr. Jo Groebel

Mit jedem neuen Medium, ob Schrift, Buch, Film oder Fernsehen und seit kurzem dem Internet ging immer die Befürchtung einher, es könne die Gesellschaft zum Schlechteren bringen, Moral senken, Kriminalität erhöhen. Tatsächlich finden sich jeweils Belege dafür, dass Medien auch negativ benutzt werden können, um gesellschaftlich destruktive Ziele zu erreichen. Dies reicht von ihrem Einsatz zu menschenfeindlicher Propaganda über die Verständigung und Planung bei Gruppendelikten bis hin zur Möglichkeit, in größerem Stil terroristisch aktiv zu sein. Vernachlässigt wird bei diesen Debatten aber häufig, dass Kommunikationsplattformen zunächst neutral sind und vor allem auch Positives bewerkstelligen können: Aufklärung größerer Bevölkerungsgruppen, schnellere Hilfe, Interessensweckung gegenüber friedlichen Problemlösungen. Damit muss man der zu großen Teilen subjektiven Bewertung von Kriminalität neben dem Kulturfaktor auch den Faktor der Medienstrukturabhängigkeit hinzufügen.

Zu den traditionellsten Beziehungshypothesen im Zusammenhang von Medien und Kriminalität gehören Theorien und Studien zu den Wirkungen von Fernsehen und Internet auf Gewalt. Hier hat sich am ehesten ein systemischer Ansatz durchgesetzt. Bereits Gewaltbereite suchen selektiv entsprechende Medieninhalte und werden dann in ihren Tendenzen nochmals verstärkt. Das Medien-Gewalt-Geflecht besteht also aus einer Abfolge aus persönlichen Dispositionen, Medieneigenschaften und kurz- und langfristigen Weiterwirkungen (siehe Tabelle 1).

	PHYSIOLOGISCH	*EMOTIONAL*	*KOGNITIV*	*SOZIAL*
MOTIV	Anregungsbedürfnis	Vorbildsuche	Orientierung	Gehören
MEDIUM	Spannungsdramaturgie	Stories	Infomuster	Soziale Riten
KURZWIRKGUNG	Kick	Identifikation	Faktenwissen	Faszination
LANGWIRKUNG	Gewöhnung	z.B. Abstumpfung	Weltbilder	Gemeinschaft

Tabelle 1: Wirkungsmodell Mediengewalt; aus: Jo Groebel, Media and Human Development. Encyclopedia of the Social Sciences. Elseviers, 2002

Nicht eine einzige Theorie erklärt dabei diese Beziehung, sondern je nach psychologischem oder sozialem Modus treffen unterschiedliche Ansätze zu. Das Anregungsbedürfnis wird vor allem durch die formalen Eigenschaften eines Mediums befriedigt, dies gilt besonders bei actionreichen oder extrem schockierenden Szenen und Filmen, eine wahr-

scheinliche, empirisch belegte Wirkung ist die Gewöhnung nach einiger Zeit, die wiederum zu extremeren Darstellungswünschen führt. Auf das Fernsehen folgte mit extremer Dramaturgie der Bereich Video, auf diesen die noch ausgeprägteren Möglichkeiten im Internet inklusive drastischer Abbildungen, Chatrooms einschlägig Interessierter und die teils sehr brutalen Varianten von elektronischen Spielen. Korrespondierend mit diesen physiologischen Prozessen kann man die emotionalen sehen, bei denen die Erregungsabläufe um inhaltliche Facetten von Vorbildsuche, Geschichten und entsprechender Dramaturgie ergänzt werden. Hier liegt wiederum zusammen mit der Gewöhnung eine ebenfalls belegte Abstumpfung gegenüber Opfern nahe, das heißt, Empathie und Mitleid nehmen systematisch mit der Häufung extremer Angebote ab. Auch hier hat das Internet neue Varianten geschaffen. Viele Geschichten jenseits der institutionalisierten Regulierung sind brutaler geworden, nicht zuletzt im Zusammenhang mit realen, pseudorealen oder realistisch gemachten Angebotsformen. Besonders weitreichend erscheint in der Summe aller einzelnen Medienerfahrungen bei der Kumulation gewalttätiger Szenen die Schaffung von Weltbildern, bei denen vermutet wird, dass Aggression fundamentaler Bestandteil menschlichen Zusammenlebens sei und damit auch zum eigenen Verhaltensrepertoire gehören müsse. Schließlich schaffen Massenmedien, und ganz besonders das Internet, einen Gemeinschaftsraum, in dem Zugehörigkeit gesucht und gefunden wird und symbolisch weiter verstärkt wird. Dies kann genauso aus friedlichen Riten bestehen wie aus gewaltbetonenden. Selbstverständlich ist dabei immer die Aggressionstendenz eine von mehreren Facetten (die besonders männlich geprägt ist); genauso prägen Medien auch friedliche Verhaltensstrategien.

Wie sehr die Tendenz zu eher aggressiven oder nicht-aggressiven Reaktionen von der Kultur abhängt, zeigt eine Studie des Autors (siehe Tabelle 2). Sie belegt den großen Einfluss der allgemeinen in verschiedenen Ländern vorzufindenden Ausprägung sozialer Kontrolle. Länder mit geringer sozialer Kontrolle, also großer Normenunsicherheit und gleichzeitig hoher Mediengewalt weisen die höchste Tendenz zu realem Gewaltverhalten auf, so die Ergebnisse einer 23-Länder-Globalstudie mit 5.500 Zwölfjährigen aus allen Kulturkreisen, Weltregionen und sozialen Schichten. Höhere Mediengewalt allein oder geringere soziale Kontrolle allein korrelierten mit etwas weniger Aggressionstendenzen. Am ‚friedlichsten' in Bezug auf individuelle Gewalt sind offenbar Länder mit einem geringen Vorkommen von Gewaltmodellen und Ächtung von Aggression. Deutschland bewegt sich dabei übrigens auf mittlerem Niveau. Das Internet spielt hier insofern eine besondere Rolle, als es einerseits neue Formen der friedlichen Selbstorganisation und informeller sozialer Kontrolle geschaffen hat (‚Communities'), andererseits aber auch dem, der es sucht, ein viel größeres Spektrum extremer Gewalt anbietet und zugleich auch aggressionstendierende Foren schafft.

KRIMINALITÄT (+/-)	*MEDIENAGGRESSION HOCH*	*MEDIENAGGRESSION NIEDRIG*
SOZIALE KONTROLLE NIEDRIG	Brasilien, Südafrika (++)	Angola (+)
SOZIALE KONTROLLE HOCH	Japan (-)	Indien (-)

Tabelle 2: Graduelle Ausprägung realer Gewaltkriminalität in Korrelation zur Intensität von Mediengewalt und sozialer Kontrolle; Länderbeispiele aus: Jo Groebel, UNESCO Global Study on Media Violence. In: Encyclopaedia of Media and the Youth. Sage Publishers, 2006

Wie relativ die Einschätzung von Schaden auch durch Opfer ist, belegt ein weiteres Ergebnis der Globalstudie. Dass Mord und extremer körperlicher Zwang kulturübergreifend als extreme Gewalt eingestuft werden, liegt nahe. Danach aber beginnt bereits eine Abstufung, die übrigens auch im Zusammenhang mit aktuelleren Konflikten rund um beleidigende Religionsabbildungen interessant ist: Die verbale oder bildliche Schmähung der eigenen Person oder der persönlichen Werte gilt im asiatischen und afrikanischen Raum als größerer Schaden als ein leichter oder selbst mittlerer körperlicher Angriff (siehe Tabelle 3). ‚Das Gesicht zu verlieren' beeinträchtigt in diesen Kulturkreisen die individuelle Integrität offenbar mehr als eine Attacke, bei der man sich ebenfalls körperlich wehren kann. Das Beispiel Zidane im Endspiel der Fußballweltmeisterschaft 2006 illustriert, wie weit die Wirkungsmacht von Worten dabei reichen kann.

SCHADENSBEWERTUNG	*ASIEN/AFRIKA*	*AMERIKA/EUROPA*
PHYSISCH	Niedriger	Höher
PSYCHOLOGISCH	Höher	niedriger

Tabelle 3: Subjektive Bewertung der Schadensintensität im Vergleich zwischen körperlichem Angriff und persönlicher Beleidigung bei 12-Jährigen; aus: Jo Groebel, UNESCO Global Study, 2006

Die unterschiedlichen kulturellen Bewertungen finden sich in Bezug auf Medien selbst innerhalb der westlichen Hemisphäre. Das Internet hatte während seiner Popularisierung lange Zeit die Reputation, vor allem auch ungehemmte Sexualität und Gewalt zu propagieren und zugänglich zu machen. Eine überlieferte amerikanische Studie wird mit dem Resultat zitiert, dass bis zur Mitte der 1990er Jahre die ‚New York Times' internetbezogene Titelüberschriften vor allem im Zusammenhang mit technologischer Neuerung und Wissenschaft gebracht habe, in der zweiten Hälfte der 1990er Jahre vorwiegend risikobezogene Themen zu finden gewesen seien, also Gewalt-Sites und Pornografie, dann erst ökonomische Faktoren dominant geworden seien. In einer eigenen Studie mit u.a. Internetnutzern fanden wir in jedem Fall stark auseinanderdriftende Beurteilungen eines ‚Zuviel' an Sexualität und Gewalt jeweils durch Deutsche und US-Amerikaner (repräsentative Stichproben). Eindeutiges Ergebnis (siehe Tabelle 4): In den USA wird Sexualität noch weitaus kritischer beurteilt als auch extremere Aggression, Deutsche (und andere Europä-

er) dagegen halten Gewaltdarstellungen in Fernsehen und Internet für problematischer als die Gefahr durch Pornografie (ohne Gewaltbezug). Illustriert wird dieses Ergebnis durch die Aufregung, die zum Beispiel beim Superbowl vor einiger Zeit ein entblößter Busen von Janet Jackson in den USA entfachte, während dort auch extremere Gewaltbilder im normalen Fernsehen an der Tagesordnung sind.

SEX & CRIME BEWERTUNG	*USA: TV*	*D: TV*
ZUVIEL SEX	80% (INTERNET 61%)	49% (INTERNET 53%)
ZUVIEL GEWALT	51%	70% (INTERNET 42%)

Tabelle 4: ‚Zuviel'-Bewertung von Sexualität und Gewalt in Medien durch Internet-Nutzer in Deutschland und den USA; aus: Jo Groebel & Gernot Gehrke (Hrsg.). Internet 2002: Deutschland und die digitale Welt. Leske & Budrich, 2003

So wie die Ursachen, die Wahrnehmung und die mediale Einbettung von Gewalt und Kriminalität kulturabhängig zu betrachten sind, so ist auch die Frage nach Prävention und Konfliktlösung in Korrelation mit dem gesellschaftlichen, sozialen und individuellen Umfeld zu sehen (siehe Tabelle 5). Auf der Makroebene, also der Ebene von Gesellschaft und Kultur sind es, wichtiger als die Medien im engeren Sinne, u.a. Normenheterogenität, ökologische Umstände und generell friedliche Traditionen sowie die Belohnung von Deeskalation, die Gewalt mehr oder eben weniger wahrscheinlich sein lassen. Auf der Mesoebene, also der Ebene von größeren Gruppen und Institutionen, ist die Frage entscheidend, wie sehr im direkten Umgang innerhalb der Gemeinschaft miteinander soziale Integration stattfindet bzw. gewaltsame Subgruppentraditionen entstehen. Innerhalb dieser beiden Obersysteme ist schließlich der Zugang zu diesen, aber auch deren Auswirkungen wiederum verknüpft mit individuellen Entwicklungsverläufen, dem Einfluss der Familie (vermutlich inklusive eines gewissen genetischen Anteils) und dem unmittelbaren Miterleben gewaltsamer oder friedlicher Rollenmodelle, bzw. der Ausprägung von Entfaltungsmöglichkeiten oder umgekehrt regelmäßigen Frustrationserlebnissen. Jede neue mediale Umgebung, sei es das Fernsehen, seien es Internet oder elektronische Spiele, ist in Interaktion mit diesen verschiedenen Ebenen zu sehen und prägt natürlich durchaus langfristig (siehe oben) deren eigene Struktur. So hat zweifellos die Fernsehkultur die Gesellschaft bis hin zu den Werten in der Politik verändert, so hat das Internet neue Formen von Gemeinschaft geschaffen, die auch auf die nichtmediale Welt zurückwirken. Eine der vielleicht weitreichendsten Veränderungen durch das Internet ist die Beziehung zwischen Privatheit und Öffentlichkeit (siehe auch: Ralph Weiß & Jo Groebel, Hrsg., Privatheit in der Öffentlichkeit. Leske & Budrich, 2002) sowie der direkte Zugang zu jedweder Art von Lebensform und Normensystem. Dies wirkt sich auch auf Werte- und Identitätsbildung aus, zumindest im Sinne einer größeren Relativierungsmöglichkeit derselben. Attraktive Lebensformen werden dann in ihrem Belohnungswert durchaus auch dort gefunden, wo die traditionelle Umgebung eher sanktioniert hätte bis hin zu ‚kriminellen' Verhaltensweisen unterhalb der universell abgelehnten Ausprägungen wie Mord oder massive Lebensbedrohung.

AGGRESSIONS-KATEGORIE	*MAKRO*	*MESO*	*MIKRO*
KRIMINELLE AGGRESSION	Normenheterogenität	Soziale Ansteckung	Familienkontext
KONFLIKT-LÖSUNG	Belohnung von Deeskalation	Positive Integration	Friedliche Rollenmodelle

Tabelle 5: Beispiele Kategorisierung Kriminalität und Konfliktlösepotenzial in komplexen Zusammenhängen; aus: Jo Groebel & Robert A. Hinde (eds.). Aggression and War. Their Biological and Social Bases. Cambridge University Press, 1991

Während Umstände und Ursachen von Kriminalität und von deren Prävention zunächst eingebettet sind in gesellschaftliche, soziale und individuelle Gegebenheiten ist eine zentrale Frage, davon nicht unabhängig, welche strukturellen Eigenschaften der Medien gar neue oder teil-neue Phänomene von Kriminalität zur Folge haben. Anders als Bildmedien wie Fernsehen oder Film, bei denen sich rechtswidrige Charakteristika zumeist auf die Abbildungen selbst beschränken, zum Beispiel extrem jugendgefährdende Darstellungen, bietet das Internet ein breiteres Spektrum für extremes Verhalten. Die Tatsache anonymer Interaktion, die Möglichkeit zur Gruppenbildung oder auch die Verbreitung von Informationen zur Vorbereitung von Verbrechen bis hin zum terroristischen Anschlag wie dem 11. September 2001 findet so kaum eine Entsprechung in der traditionellen Welt. Und so hat sich eine Infrastruktur entwickelt (siehe Beispiele aus Tabelle 6), die das Internet zwar nicht zu einem automatisch kriminalitätssteigernden System macht, die aber sehr wohl spezifischer Analysen und präventiver Maßnahmen bedarf. Fünf Grundeigenschaften kennzeichnen entsprechend diese Infrastruktur und bieten zugleich den Ansatz für die Vorbeugung von destruktiv abweichendem Verhalten. Die Verbreitung von Online-Information und die Online-Kommunikation lassen sich durch die Kombination der Modi ‚unmittelbar', ‚universal', ‚umfassend', ‚unabhängig von Ort und Zeit' und ‚unterwegs' beschreiben.

RISIKO ALT/NEU	*TRADITIONELLE KRIMINALITÄT*	*MIX KRIMINALITÄT*	*NEUE KRIMINALITÄT*
GRUPPE	Organisierte Kriminalität; Gangs	Pädophilie-Ringe	Cyber-Terrorismus
EINZELNER	Individualangriffe	Kriminelles Internet-Dating	Cracking

Tabelle 6: Alte und neue Delinquenzphänomene in der Informationsgesellschaft; aus: Jo Groebel et al. Cyber Crime. Friedrich-Ebert-Stiftung, 2001

Dass jede kriminalitätsrelevante Information sofort grenzüberschreitend zwischen Sender und Empfänger vermittelt werden kann, ist sowohl relevant für Täter wie für Verfolger. Terroristen wie traditionelle organisierte Kriminalität profitieren davon. Die Verbrechensbekämpfung wird in dem Maße effizienter, in dem entsprechende Kompetenzen, juristische Möglichkeiten und vor allem technische Ausstattungen gegeben sind. Neben die tra-

ditionelle Kontrolle destruktiv abweichenden Verhaltens durch öffentliche Institutionen ist zunehmend eine Selbstregulierung durch die Nutzergemeinschaft selbst getreten. Besonders im Zusammenhang mit Gewaltpornografie und Pädophilie haben sich sowohl Provider wie informelle Jugendschutzgruppen wie spontan aktive Nutzer zu weit reichenden Maßnahmenbündeln wie Hotlines etc. entschieden. Eine neue Generation von potentiell kriminalitätsfördernden wie aber auch präventionssteigernden Möglichkeiten entsteht im Zusammenhang mit dem Sektor der Mobilkommunikation. Der bewegliche Austausch von Informationen war schon seit längerem Bestandteil von Täter- und Verfolgerstrategien. Die mobile Bilderfassung gekoppelt mit sofortiger Verbreitung in informellen Zirkeln wird nun im Rahmen neuer technischer Möglichkeiten zu einem Promotor extremer Gewaltdarstellungen und deren Weitergabe. Das Wissen und die Analyse der sich jeweils weiterentwickelnden technischen Infrastrukturen ist nur ein Teil künftiger Prävention. Auch der seit Jahrzehnten übliche Ruf nach immer mehr Medienkompetenz hat häufig eher beschwörenden denn wirklich hinreichend verhindernden Charakter. Erst die Kombination aus grundlegend gesellschaftspolitischen Maßnahmen und spezifisch technologischen Präventionsanwendungen kann langfristig die Kriminalitätsentwicklung beeinflussen. Die hier berichteten Befunde belegen dabei die Bedeutung des sozialen und familiären Rahmens, in dem sich das Beziehungsgeflecht zwischen Gewalt und neuer Medientechnologie abspielt.

Zur Bedeutung des Internet für jugendliche Lebenswelten - neue Aspekte der Jugendkultur - Ergebnisse der JIM-Studie 2005

Thomas Rathgeb

Die Medienwelt der Jugendlichen in Deutschland hat sich in den vergangenen Jahren verändert. Computer und Internet sind inzwischen alltäglich geworden. Das Angebot an Medien und Mediengeräten ist größer geworden und auch die Medieninhalte haben sich gewandelt. Die Basisuntersuchungen des mpfs ‚JIM - Jugend, Information, (Multi-)Media' und ‚KIM - Kinder und Medien' bieten seit Jahren kontinuierlich repräsentatives Datenmaterial zur Mediennutzung von Kindern und Jugendlichen und erlauben es daher, den Medienumgang von Kindern und Jugendlichen unvoreingenommen abzubilden und Entwicklungen aufzuzeigen. Die nunmehr zum achten Mal in Folge aufgelegte JIM-Studie dokumentiert die Entwicklung der jugendlichen Medienwelt und zeichnet ein aktuelles Bild des Medienalltags 12- bis 19-Jähriger in Deutschland.

Für die Diskussion über Internet Devianz von Jugendlichen können die Studienergebnisse eine wichtige Grundlage bieten. Das Thema Devianz greift die JIM-Studie explizit nicht auf - es handelt sich um eine Medienstudie -, dennoch bietet sie beispielsweise über die Darstellung der Computer- und Internetnutzung wichtige Informationen zu diesem Bereich.

Die Grundgesamtheit der Studie JIM 2005 umfasst die gut sieben Millionen Jugendlichen im Alter von 12 bis 19 Jahren in Telefon-Haushalten der Bundesrepublik Deutschland. Aus dieser Grundgesamtheit wurde eine repräsentative Stichprobe von 1.203 Jugendlichen in der Zeit von Juni bis Juli 2005 telefonisch befragt.

Wie in den vergangenen Jahren hatten sich 2005 als Träger dieser Studie zusammengefunden:

- der Medienpädagogische Forschungsverbund Südwest (mpfs) - eine Forschungskooperation zwischen der Landesanstalt für Kommunikation Baden-Württemberg (LFK) und der Landeszentrale für Medien und Kommunikation Rheinland-Pfalz (LMK)
- die Zeitungs Marketing Gesellschaft (ZMG)

in Zusammenarbeit mit:

- der Bundeszentrale für politische Bildung
- den Landeszentralen für politische Bildung Baden-Württemberg und Rheinland-Pfalz
- der Stiftung Lesen

- der SWR Medienforschung.

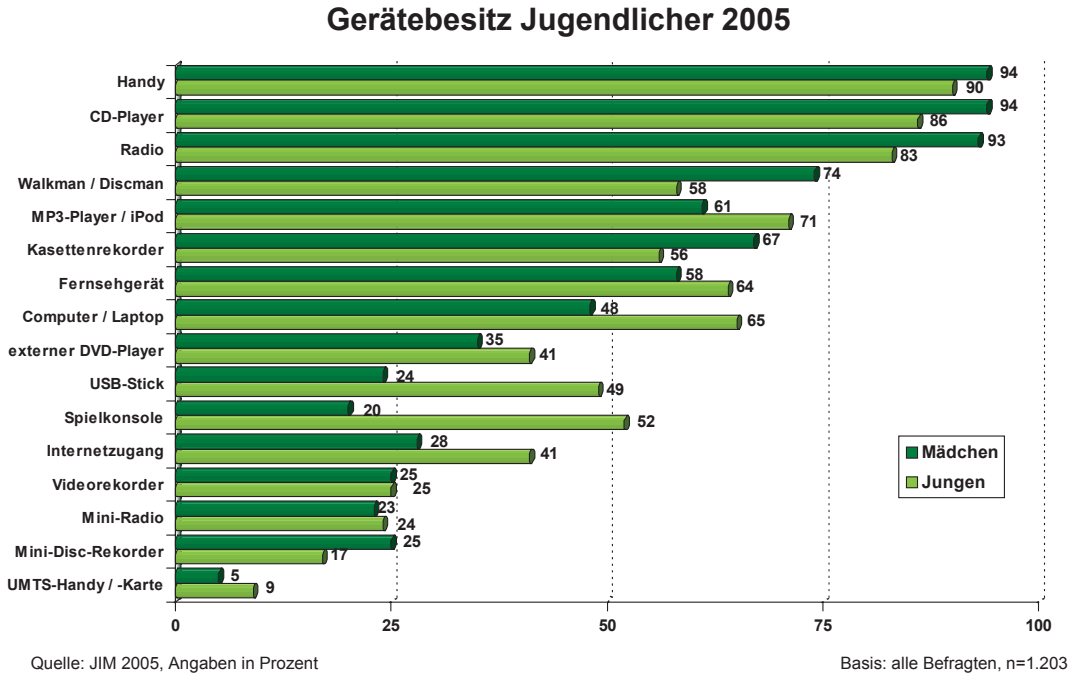
Zentrale Untersuchungsdimensionen waren neben allgemeinen Interessen und Bedürfnissen der Jugendlichen ihr Medienverhalten sowie u.a. Zugangswege zu Informationen. Fragen zum Themenkomplex ‚Computer' wurden nur so genannten Computer-Nutzern gestellt, d.h. denjenigen Jugendlichen, die angeben, **mindestens einmal pro Monat** einen **Computer** in der Freizeit zu nutzen. Ähnlich wurde mit dem Themenbereich ‚Internet' verfahren. Als Internet-Nutzer gelten im Folgenden Jugendliche, die **zumindest selten** von **Internet bzw. Online-Diensten** Gebrauch machen.

Haushaltsausstattung und Medienbesitz

Die immer kürzeren Entwicklungszyklen bei Geräten der Unterhaltungselektronik sorgen auch für eine zunehmende Verfügbarkeit bei Kindern und Jugendlichen. Nahezu jeder Haushalt, in dem 12- bis 19-Jährige heute aufwachsen, verfügt beispielsweise über Fernseher, Mobiltelefon, CD-Player oder Computer. In 89 Prozent der Haushalte ist ein Internetzugang vorhanden (JIM 2004: 85 %), aber auch DVD-Player sind mit einer Ausstattungsrate von 86 Prozent weitgehend etabliert (JIM 2004: 74 %). MP3-Player, vor zwei Jahren gerade mal in jedem vierten Haushalt vorhanden, haben eine überaus starke Verbreitung erfahren und sind nunmehr in 78 Prozent der Haushalte vorhanden (JIM 2004: 41 %).

Betrachtet man die Medien und Geräte, die sich nach Angaben der Jugendlichen in deren Eigenbesitz befinden und somit eine eigenständige Zuwendung erlauben, wird deren Alltäglichkeit besonders deutlich. Mit einer Besitzrate von 92 Prozent führt das Mobiltelefon die Liste der eigenen Geräte an. Es folgt der eigene CD-Player (90 %), das eigene Radio (88 %) und Walk-/Discman bzw. MP3-Player (jeweils 66 %). Kassettenrekorder und Fernseher besitzen jeweils 61 Prozent der Jugendlichen, einen eigenen Computer haben 57 Prozent der 12- bis 19-Jährigen. Es folgen hinsichtlich ihrer Verbreitung (externe) DVD-Player (38 %), Spielkonsole oder USB-Stick zum Transport größerer Datenmengen (jeweils 37 %). Mit 35 Prozent verfügt ein Drittel der Jugendlichen über einen persönlichen Internetzugang.

Im Vergleich zur JIM-Studie 2004 zeigt sich ein Anstieg um 41 Prozentpunkte (!) beim Besitz von MP3-Player, auch DVD-Player haben beim persönlichen Besitz der Jugendlichen um zehn Prozentpunkte zugelegt. Weniger hohe Zuwachsraten auf höherem Ausgangsniveau weist der Besitz eines Computers (plus vier Prozentpunkte) und der persönliche Internetzugang (plus sieben Prozentpunkte) auf. Zuwachsraten beim Handybesitz fallen aufgrund der extrem hohen Verbreitung nur noch sehr gering aus (plus zwei Prozentpunkte).

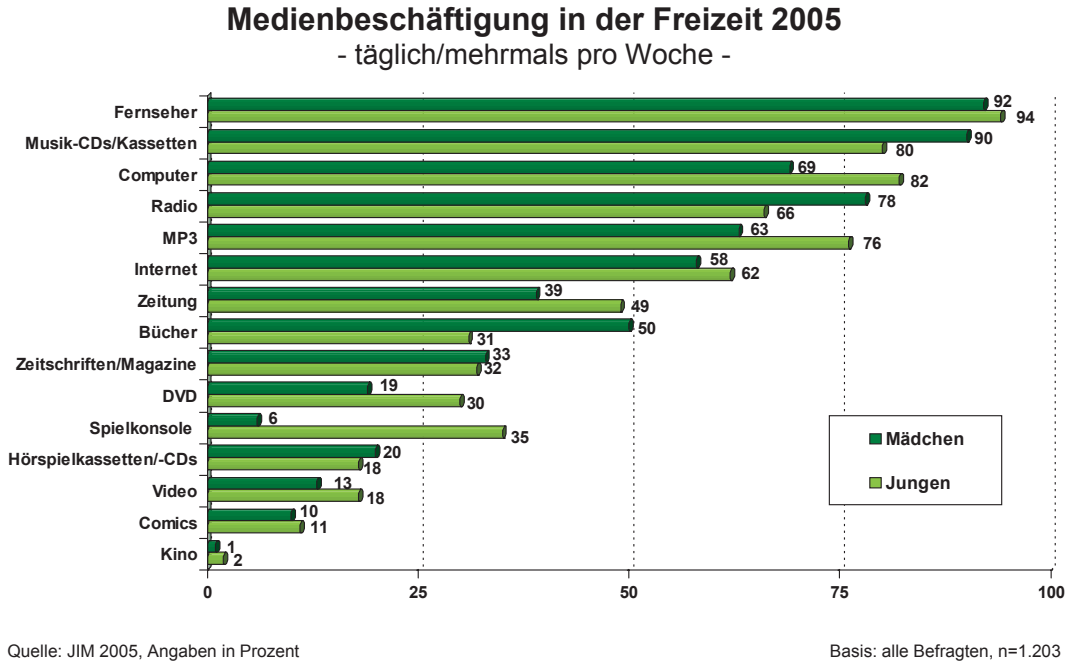


Der persönliche Medienbesitz nimmt insgesamt mit dem Alter der Jugendlichen zu. Ein eigenes Fernsehgerät haben 53 Prozent der 12- bis 13-Jährigen und 62 Prozent der 18- bis 19-Jährigen. Der Besitz eines eigenen Computers ist bei den 16- bis 17-Jährigen am stärksten ausgeprägt (64 %, 12-13 Jahre: 47 %, 14-15 Jahre: 59 %, 18-19 Jahre: 55 %). Deutliche Sprünge gibt es auch beim persönlichen Internetzugang (12-13 Jahre: 19 %, 14-15 Jahre: 33 %, 16-17 Jahre: 42 %, 18-19 Jahre: 42 %). Die bildungsspezifische Betrachtung zeigt die deutlichsten Unterschiede beim Fernseher (Hauptschüler: 68 %, Gymnasiasten: 56 %), beim Computer (Hauptschüler: 43 %, Gymnasiasten: 62 %), beim Internetzugang (Hauptschüler: 22 %, Gymnasiasten: 43 %) und bei Spielkonsolen (Hauptschüler: 45 %, Gymnasiasten: 27 %).

Medien und Freizeit

Medien sind auch in den Alltag junger Menschen fest integriert. Die Liste der Medientätigkeiten (nutze ich mindestens mehrmals pro Woche) wird mit 93 Prozent vom Fernsehen angeführt, die Nutzung von Musik-CDs/-Kassetten kommt mit 85 Prozent auf den zweiten Platz. Die Beschäftigung mit dem Computer rückt vom vierten Platz 2004 auf den dritten Platz 2005 vor, 76 Prozent der Jugendlichen sitzen mindestens mehrmals pro Woche vor dem Bildschirm (plus fünf Prozentpunkte). Das Radio folgt mit 72 Prozent auf dem vierten Rang. Erstmals gesondert abgefragt wurde die Nutzung von MP3-Playern, die mit 70 Prozent nur knapp hinter dem Radio liegt. Einen großen Sprung erlebt auch die Zuwendung zum Internet. So gaben in der JIM-Studie 2004 mit 49 Prozent knapp die Hälfte der 12- bis 19-Jährigen an, mindestens mehrmals pro Woche online zu sein, 2005 ist dieser Anteil auf 60 Prozent angestiegen. Mit leichtem Abstand folgt die Beschäftigung mit Zei-

tungen (44 %) und Büchern (40 %). Zeitschriften und Magazine werden nicht ganz so häufig zur Hand genommen (32 %). Im Vergleich zum Vorjahr um fünf Prozentpunkte angestiegen ist die Nutzung von DVDs (25 %), die Zuwendung zu Spielkonsolen hat sich hingegen nicht verändert (21 %). Hörspielkassetten bzw. -CDs erlebten einen leichten Rückgang auf nunmehr 19 Prozent (minus 5 Prozentpunkte), Video (15 %), Comics (10 %) und das Kino (2 %) bleiben unverändert.



Quelle: JIM 2005, Angaben in Prozent

Basis: alle Befragten, n=1.203

Vergleicht man die Angaben von Jungen und Mädchen, so können das Fernsehen, Zeitschriften/Magazine, Hörspielkassetten/-CDs, Comics, Kino und mittlerweile auch das Internet hinsichtlich ihrer Nutzung als ‚geschlechtsneutral' bezeichnet werden. Jungen und junge Männer sitzen häufiger vor dem Computer und nutzen MP3-Player, Zeitungen, DVDs und Videos stärker. Spielkonsolen sind absolut männlich besetzt, Mädchen und junge Frauen können sich für diese Freizeitbeschäftigung kaum begeistern. Musikkassetten/-CDs, das Radio und vor allem Bücher sind hingegen Medien, die für weibliche Jugendliche eine höhere Attraktivität besitzen als für männliche.

Auch das Alter der Jugendlichen spielt in die Bedeutsamkeit mancher Medien hinein. So geht die Nutzung von Büchern, Comics, Hörspielkassetten/-CDs und Spielkonsolen bereits bei den ab 14-Jährigen deutlich zurück. An Wichtigkeit gewinnen umgekehrt der Computer, MP3s, die Zeitung und vor allem das Internet. Fernseher, Radio, Videos, Tonträger, Zeitschriften und DVDs unterliegen hingegen kaum altersbedingten Schwankungen.

Legt man die Schulbildung der jungen Menschen zugrunde, so zeigen Hauptschüler eine deutlich geringere Zuwendung zu den Printmedien Buch und Zeitung. Zeitschriften, DVDs und Spielkonsolen hingegen werden von Hauptschülern häufiger genutzt als von

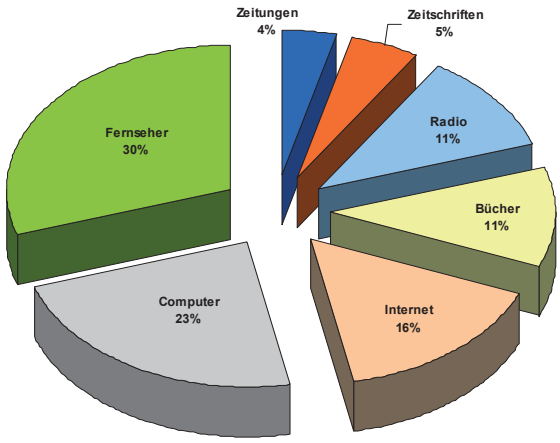
Gymnasiasten. Jugendliche mit höherer Schulbildung beschäftigen sich dagegen häufiger mit Computer und Internet als Hauptschüler.

Die Verbreitung von MP3-Playern ist in den vergangen Jahren sowohl hinsichtlich der Haushaltsausstattung als auch des persönlichen Besitzes der Jugendlichen sprunghaft angestiegen. MP3-Player sind 2005 in 78 Prozent (und damit dreimal so häufig wie noch 2003) der Haushalte, in denen Jugendliche aufwachsen, vorhanden. Der persönliche Besitz bei den 12- bis 19-Jährigen hat sich im selben Zeitraum beinahe verfünffacht.

Medienbindung und Glaubwürdigkeit der Medien

Angesichts des großen Medienangebots und der Verfügbarkeit verschiedener Medien stellt sich die Frage, welche Bindung Jugendliche zu den verschiedenen Medien haben. Hierbei wird gefragt, auf welches Medium sie am wenigsten verzichten können. Zur Auswahl stehen: Fernseher, Zeitungen, Zeitschriften, Radio, Bücher, Computer und Internet. Hierbei entscheiden sich 30 Prozent der Jugendlichen für das Fernsehen, 23 Prozent für den Computer und weitere 16 Prozent für das Internet. Für das Radio würden sich 11 Prozent der Jugendlichen entscheiden, ebenso viele für Bücher. Zeitschriften (5 %) und Zeitungen (4 %) scheinen für Jugendliche die Medien zu sein, auf die am ehesten verzichtet werden könnte.

Bindung an Medien 2005
Am wenigsten verzichten kann ich auf...



Quelle: JIM 2005, Angaben in Prozent

Basis: Gesamt, n=1.203

Allerdings unterscheiden sich die Geschlechter hier deutlich. 31 Prozent der Mädchen und jungen Frauen entscheiden sich für das Fernsehen, mit Ausnahme von Zeitschriften und Zeitungen rangieren aber Computer, Internet, Bücher und das Radio auf vergleichbaren Ebenen. Jungen und junge Männer setzen den Computer auf Platz 1, dicht gefolgt vom Fernsehen. Das Internet kommt auf den dritten Rang, die restlichen Medien sind in dieser subjektiven Einschätzung der Jugendlichen weniger bedeutsam. Auffällig ist die große

Diskrepanz zwischen Jungen und Mädchen beim Computer, während das Internet für beide Geschlechter die gleiche Wichtigkeit hat.

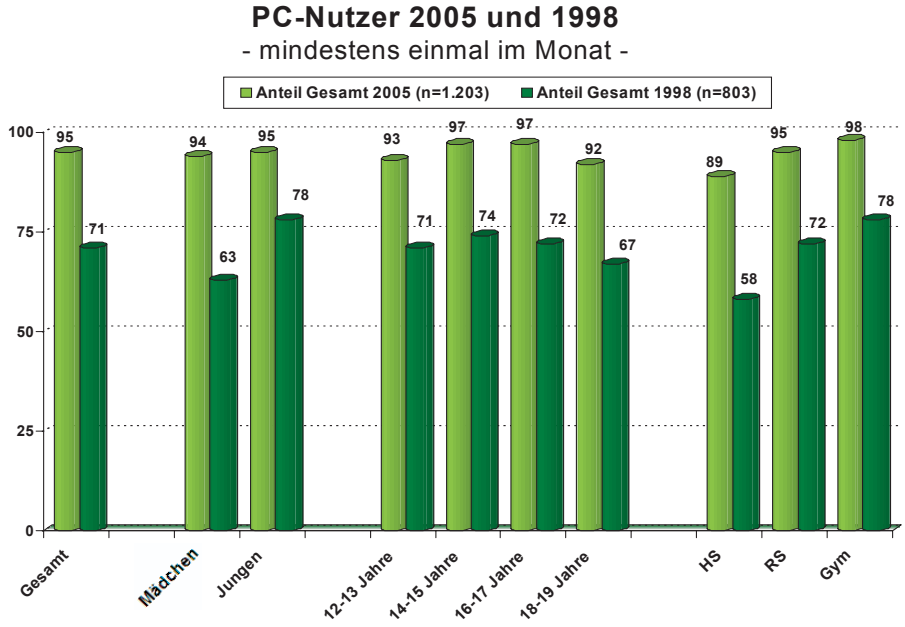
Fragt man die Jugendlichen, welchem Medium sie bei widersprüchlicher Berichterstattung am ehesten glauben würden (hier standen Fernsehen, Radio, Internet und die Tageszeitung zur Auswahl), so entscheiden sich mit 42 Prozent die meisten 12- bis 19-Jährigen für die Tageszeitung, ein gutes Viertel würde am ehesten dem Fernsehen Glauben schenken. Das Internet und auch das Radio werden als weniger glaubwürdig empfunden. Jungen und Mädchen urteilen hier im Großen und Ganzen ähnlich, allerdings genießt das Internet bei Jungen größeres Vertrauen als bei Mädchen.

Die subjektive Glaubwürdigkeit variiert vor dem Bildungshintergrund der Jugendlichen. Für 12- bis 19-Jährige, die die Hauptschule besuchen, liegt das Fernsehen ganz knapp vor der Tageszeitung, aber auch das Internet wird als recht vertrauenswürdig eingestuft. Gymnasiasten hingegen votieren eindeutig für die Tageszeitung, das Fernsehen liegt mit über 20 Prozentpunkten Abstand auf dem zweiten Rang. Mit gleich großem Abstand folgen das Internet und das Radio.

Computer

Die Nutzung eines Computers ist für den überwiegenden Teil der Jugendlichen Selbstverständlichkeit geworden. 95 Prozent der 12- bis 19-Jährigen sitzen mindestens einmal im Monat vor dem Computer, hierbei gibt es kaum Unterschiede zwischen Jungen und Mädchen oder zwischen den Altersstufen. Lediglich bei den Schultypen zeigt sich, dass mit steigendem Bildungsgrad eine häufigere Verwendung von Computern verbunden ist.

Betrachtet man die Ergebnisse der JIM Studie 1998, so zeigt sich, dass die damaligen Un-

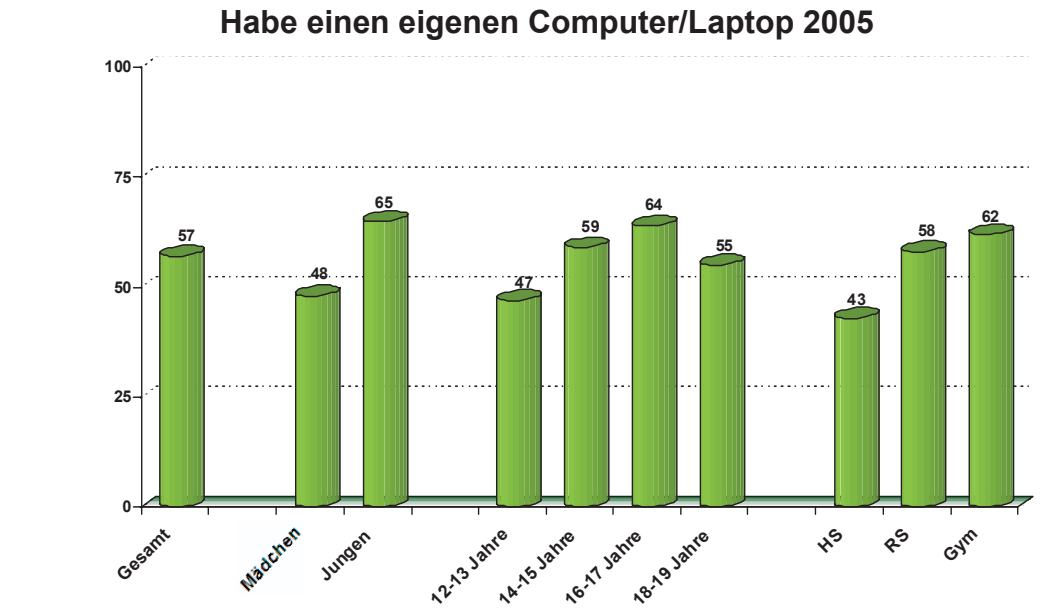


Quelle: JIM 2005; JIM 1998, Angaben in Prozent

terschiede zwischen Jungen und Mädchen sowie das Bildungsgefälle so nicht mehr vorhanden sind. Auch ist der Anteil der Nicht-Nutzer deutlich gesunken. 1998 gaben noch 20 Prozent an, nie einen Computer zu benutzen, seit 2003 liegt dieser Wert unter 5 Prozent (2005: 3 %).

Bei näherer Analyse zeigt sich aber, dass mehr Jungen (82 %) den Computer intensiv (täglich bzw. mehrmals pro Woche) nutzen als Mädchen (69 %). Der Anteil der Intensivnutzer ist mit 80 Prozent unter den Gymnasiasten deutlich höher als bei den Hauptschülern mit 68 Prozent (Realschüler: 76 %). Im Vergleich zum Vorjahr ist der Anteil der Intensivnutzer weiter angestiegen (2004: 71 %, 2005: 76 %).

Die immer häufigere Nutzung des Computers korrespondiert auch mit dem persönlichen Gerätebesitz: 57 Prozent der Jugendlichen verfügen über einen eigenen Computer, wobei die Jungen mit 65 Prozent deutlich besser ausgestattet sind als die Mädchen (48 %). Bei den 12- bis 13-Jährigen hat bereits knapp die Hälfte einen eigenen Computer oder Laptop. Deutliche Unterschiede ergeben sich hinsichtlich der Schulbildung der Jugendlichen - Hauptschüler sind deutlich schlechter mit Computern ausgestattet als Realschüler und Gymnasiasten.



Quelle: JIM 2005, Angaben in Prozent

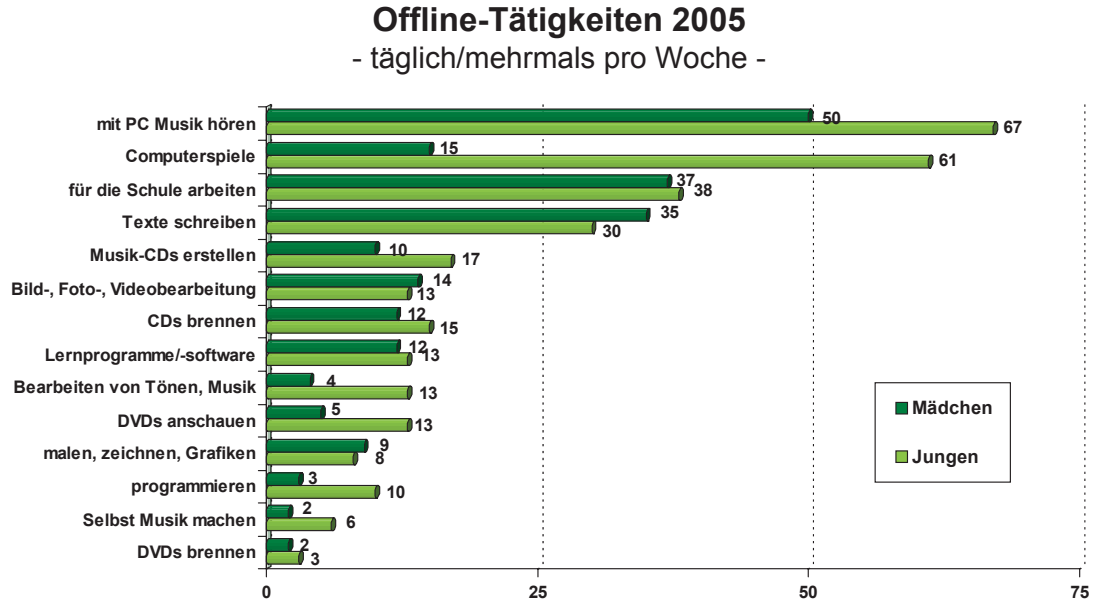
Basis: alle Befragten, n=1.203

Offline-Tätigkeiten am Computer

Die Intensität der Nutzung sagt allerdings noch nichts über die inhaltliche Nutzung aus. Mit einem Computer kann man sowohl für die Schule arbeiten als auch Computerspiele spielen, kreative Betätigungen wie Bildbearbeitung, Videoschnitt oder Zeichnen sind ebenso möglich, wie das Brennen von CDs. Mit der Verbreitung von Multimedia-PCs kann auch Musikhören, CDs-Erstellen und das Anschauen von DVDs am Rechner erfolgen. Die

Möglichkeiten sind also vielfältig. Gefragt nach der Häufigkeit der einzelnen Offline-Tätigkeiten liegt die Musiknutzung (täglich/mehrmals pro Woche) mit 59 Prozent deutlich an der Spitze Mit Abstand an zweiter Stelle folgen Computerspiele (38 %), für die Schule arbeiten (37 %) und Texte schreiben (32 %). Allerdings sind die Interessen der Jungen und Mädchen sehr unterschiedlich: Während zwei Drittel der Jungen den Computer mindestens mehrmals pro Woche als Musikabspielstätte nutzen, tun dies nur die Hälfte der Mädchen. Besonders deutlich ist die unterschiedliche Interessenlage bei den Computerspielen, die für Jungen die zweithäufigste Anwendung darstellen, während Mädchen sich hierfür nur vereinzelt begeistern können.

Vergleicht man diese Ergebnisse mit der JIM-Studie 2004, so ist die Nutzung des Computers als Musikabspielgerät (mindestens mehrmals pro Woche) deutlich gestiegen (von 46 % auf 59 %), dagegen schreiben weniger Jugendliche regelmäßig Texte und auch Computerspiele werden aktuell von einem geringerem Anteil der PC-Nutzer intensiv genutzt (2004: 41 %, 2005: 38 %).



Quelle: JIM 2005, Angaben in Prozent

Basis: PC-Nutzer, n=1.142

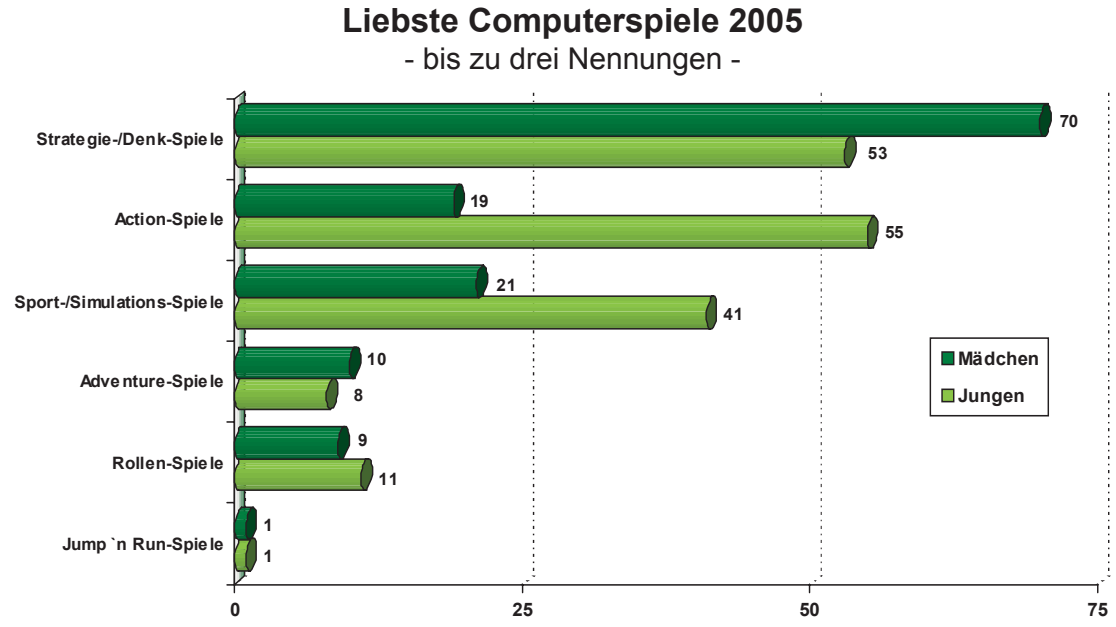
Computerspiele und Jugendmedienschutz

Computer- und Konsolenspiele sind als fester Bestandteil der Jugendkultur weit verbreitet. 61 Prozent der Haushalte mit Jugendlichen haben eine Spielkonsole; bei Computern kann man mit 98 Prozent von einer Vollversorgung ausgehen. Die Jugendlichen selbst verfügen zu 57 Prozent über einen eigenen Computer und zu 37 Prozent über eine eigene Spielkonsole. Als Themenbereich finden zwar insgesamt nur 34 Prozent der Befragten Computerspiele sehr interessant oder interessant, allerdings deutlich mehr Jungen (52 %) als Mädchen (15 %). Dieses geschlechtsspezifische Interesse spiegelt sich auch im Gerätebesitz wider. Jungen zwischen 12 und 19 Jahren besitzen zu 52 Prozent eine eigene Spielkonsole

(Mädchen: 20 %); mit 65 Prozent verfügen auch mehr Jungen über einen Computer als Mädchen (48 %).

Dass Computer- und Konsolenspiele eine Domäne der Jungen sind, zeigt auch die Medienbeschäftigung: 35 Prozent der Jungen nutzen mindestens mehrmals pro Woche Konsolenspiele, Mädchen nur zu sechs Prozent. Dabei spielt der größte Teil der Jugendlichen (46 %) überwiegend alleine, 15 Prozent überwiegend gemeinsam mit anderen und 39 Prozent ‚halbe/halbe'. Der seit Jahren anhaltende Trend, zunehmend alleine zu spielen, wurde 2005 nicht bestätigt, isoliertes Spielen ist zumindest bei den Jungen eher rückläufig (2004: 48 %, 2005: 40 %).

Bei der Frage nach den beliebtesten Computerspielen zeigen sich ebenfalls große geschlechtsspezifische Unterschiede. Strategie- und Denkspiele sind vor allem bei Mädchen beliebt, Spitzenreiter ist hierbei das Spiel ‚Die Sims', bei den Jungen sind eher Action-Spiele angesagt, besonders beliebt ist das Spiel ‚Counterstrike'. Sport- und Simulationsspiele sind ebenfalls eher Themen für Jungen. Beliebtestes Spiel ist hierbei ‚Need for Speed'.

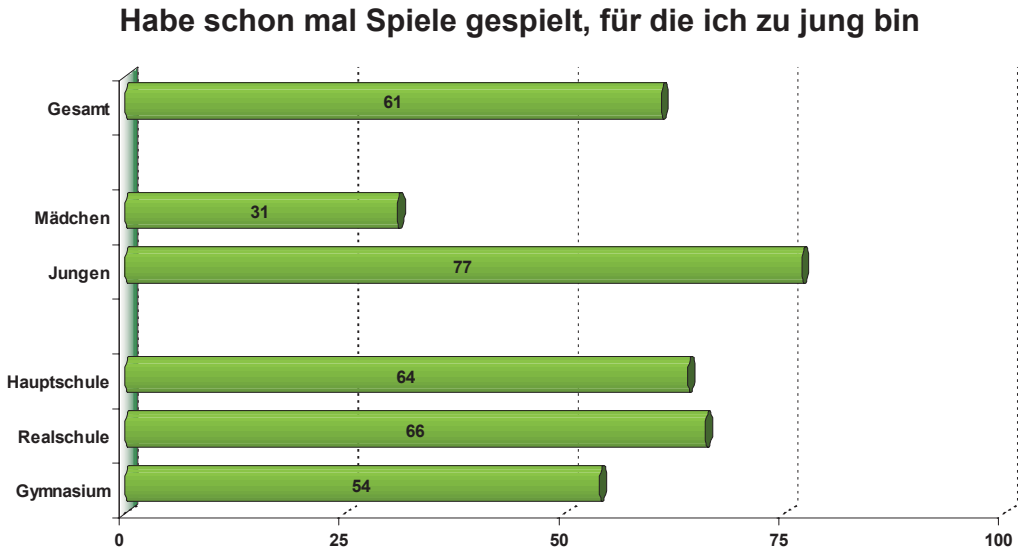


Quelle: JIM 2005, Angaben in Prozent

Basis: Nutzer v. PC-Spielen, n=846

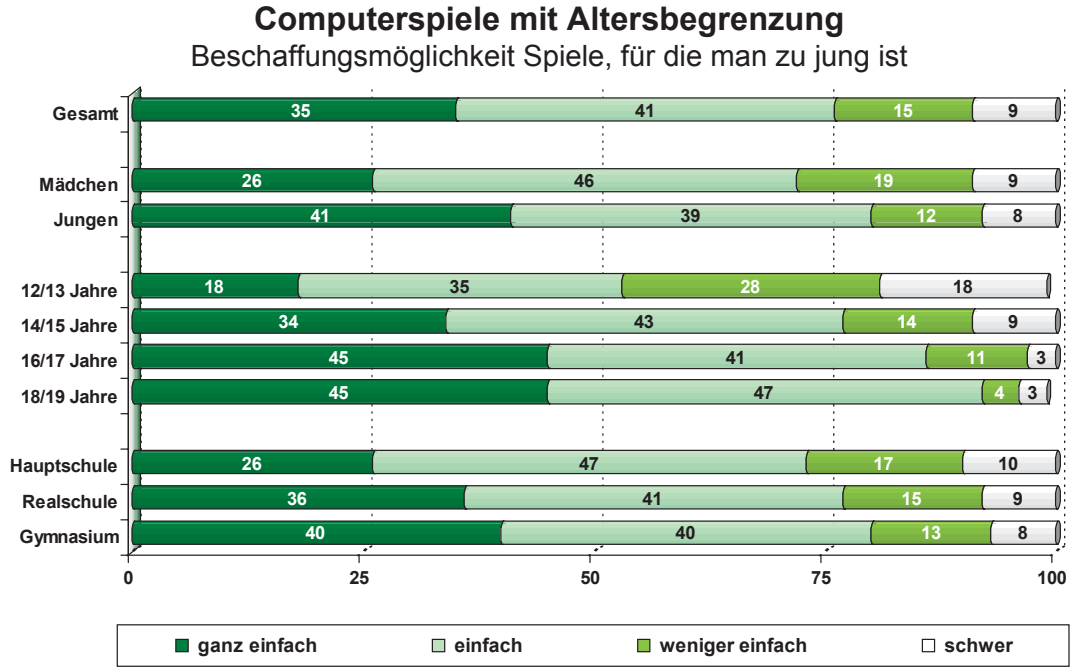
In der JIM-Studie 2004 wurde abgefragt, inwieweit Spiele, die eigentlich für Jugendliche nicht freigegeben (oder gar indiziert) sind, unter den Jugendlichen bekannt sind und auch gespielt werden. Hierbei wurde deutlich, dass die betreffenden Spiele teilweise auch unter jüngeren Spielern weit verbreitet sind. Daher wurden in die JIM-Studie 2005 einige Fragen aufgenommen, die dieses Thema etwas näher beleuchten.

97 Prozent der PC-Spieler wissen, dass es Mindestalterbegrenzungen bei Computerspielen gibt. Von diesen geben 61 Prozent an, schon einmal Spiele gespielt zu haben, für die sie eigentlich zu jung sind, bei den Jungen sind es sogar über drei Viertel (Mädchen: 31 %).

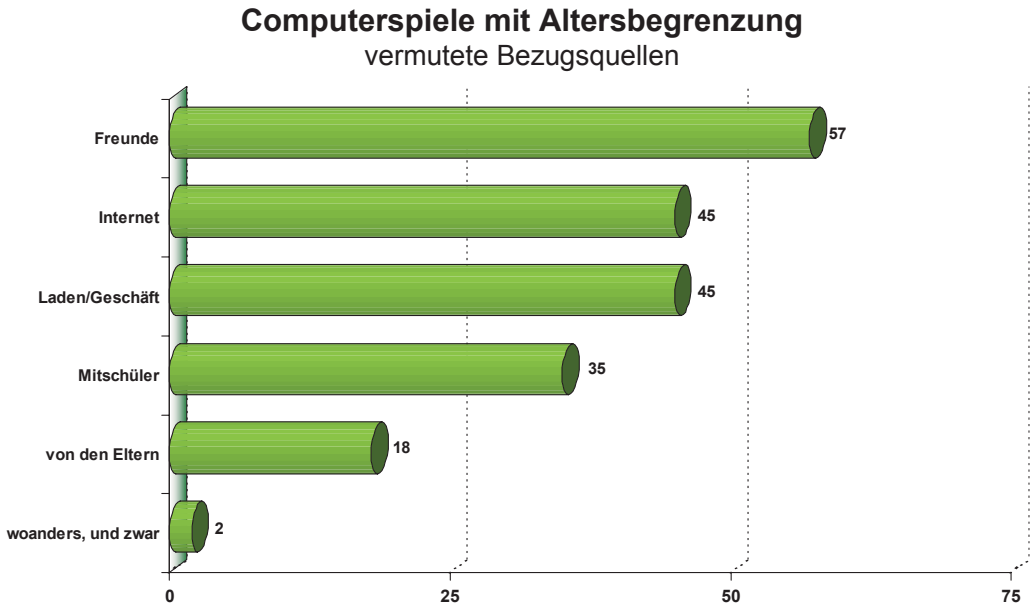


Quelle: JIM 2005, Angaben in Prozent Basis: Nutzer v. PC-Spielen, denen Spiele mit Altersbegrenzung bekannt sind, n=819

Nun sollten Jugendliche eigentlich keinen Zugang zu Spielen haben, die von der USK (Unterhaltungssoftware Selbstkontrolle) für deren jeweilige Altersstufe nicht freigegeben sind. Drei Viertel der Befragten schätzen aber die Möglichkeit, sich solche Spiele zu beschaffen, als einfach oder sehr einfach ein.



Quelle: JIM 2005, Angaben in Prozent Basis: Nutzer v. PC-Spielen, denen Spiele mit Altersbegrenzung bekannt sind, n=819



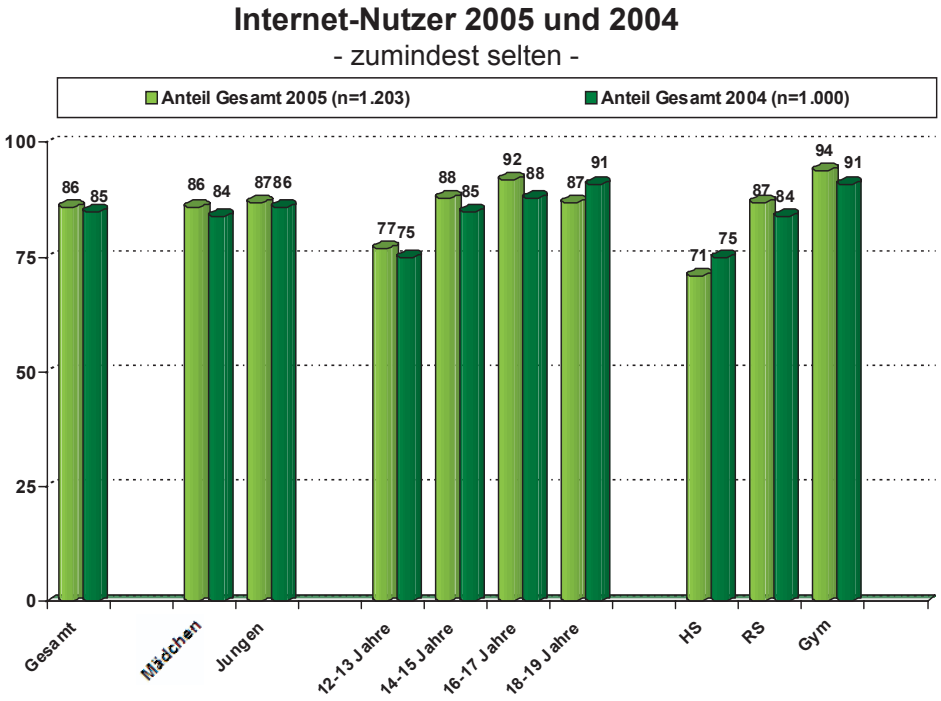
Quelle: JIM 2005, Angaben in Prozent Basis: Nutzer v. PC-Spielen, denen Spiele mit Altersbegrenzung bekannt sind, n=819

Die wichtigsten Befunde der Computernutzung der 12- bis 19-Jährigen

- 95 Prozent nutzen mindestens einmal im Monat einen Computer, 57 Prozent haben einen eigenen PC.
- Über zwei Drittel der Jugendlichen, die einen Computer besitzen, haben diesen ganz für sich alleine.
- Offline sind Computerspielen und Musikhören die häufigsten Tätigkeiten. Computerspielen ist eher rückläufig.
- Ein Drittel der Mädchen und drei Viertel der Jungen, die Altersbegrenzungen kennen, haben bereits Spiele gespielt, für die sei eigentlich zu jung sind.
- Die Beschaffung dieser Spiele scheint relativ einfach zu sein. Die Altersgrenzen bei Computerspielen sind leicht zu umgehen.

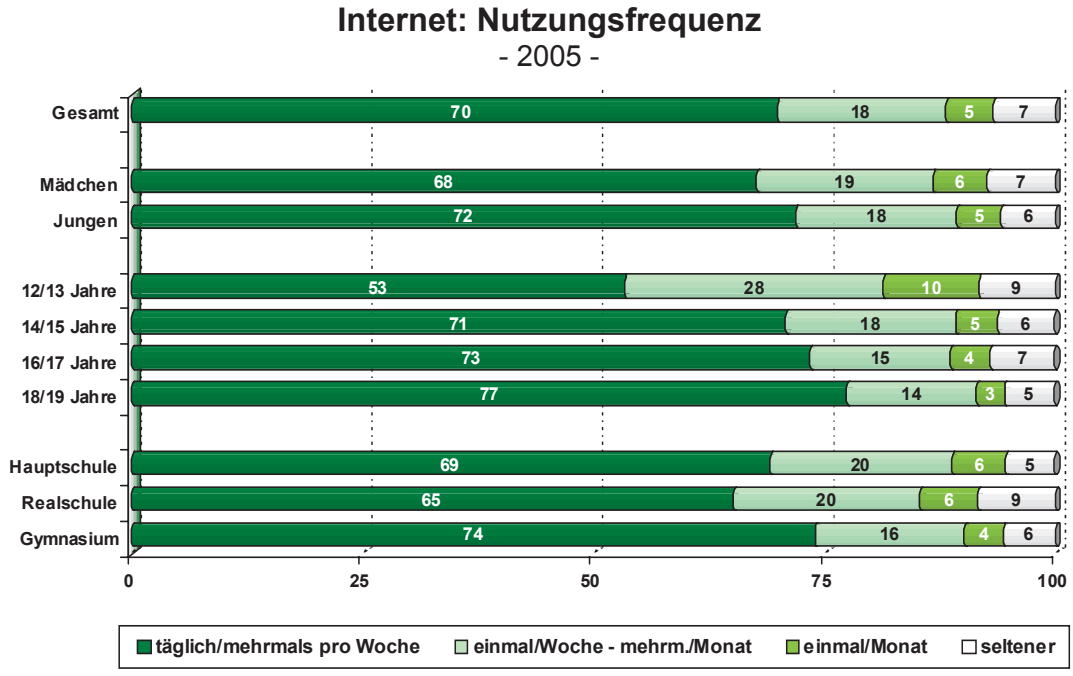
Internet

Der Anteil an Jugendlichen, die über Interneterfahrung verfügen, ist seit einigen Jahren stabil mit leicht steigender Tendenz. Seit dem Jahr 2001 betragen die jährlichen Zuwachsraten gerade mal einen Prozentpunkt, aktuell im Jahr 2005 sind 86 Prozent der 12- bis 19-Jährigen mit dem Onlinemedium vertraut. Dabei bleibt die Kluft zwischen den Bildungsgruppen nicht nur bestehen, sondern vergrößert sich. Denn während sowohl bei den Realschülern als auch bei den Gymnasiasten die Gruppe der Internet-Nutzer um drei Prozentpunkte angestiegen ist, verzeichnet man bei den Hauptschülern einen Rückgang um vier Prozentpunkte.



Quelle: JIM 2005; JIM 2004, Angaben in Prozent

Bei den Jugendlichen handelt es sich zum größten Teil um sehr aktive Internet-Nutzer, aktiver als noch in den Vorjahren. So geben 70 Prozent an, täglich oder mehrmals pro Woche online zu sein (2004: 58 %, 2003: 66 %, 2002: 63 %), weitere 18 Prozent nutzen das Internet etwa einmal pro Woche. Elf Prozent zählen zu den selteneren Nutzern, die



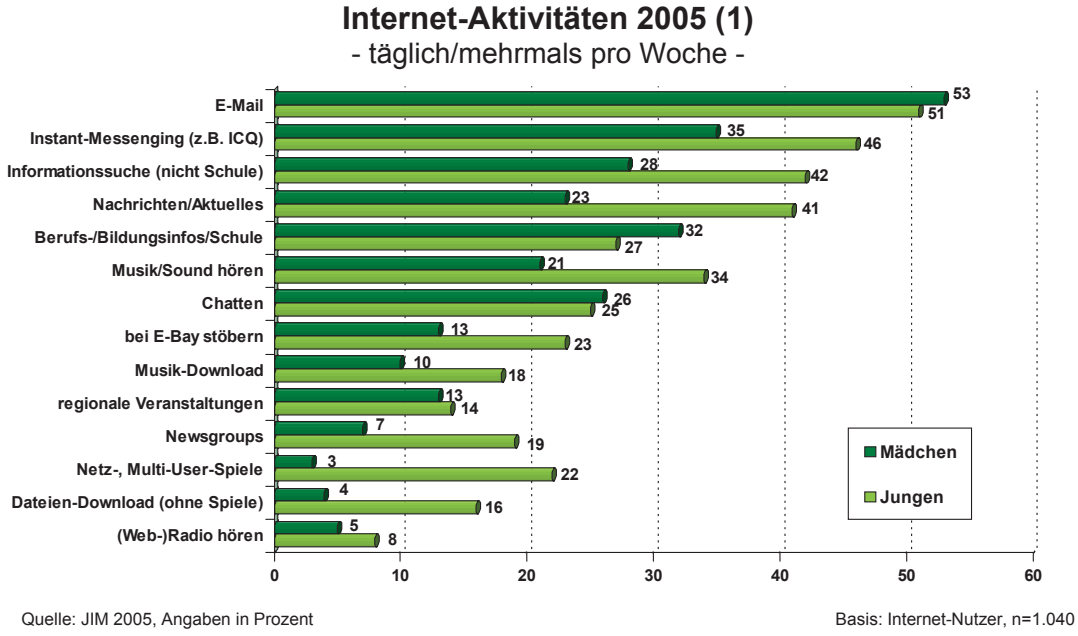
Quelle: JIM 2005, Angaben in Prozent

Basis: Internet-Nutzer, n=1.040

höchstens einmal pro Monat surfen. Hervorstechendes Merkmal dieser Gruppe ist das Alter - es sind eher die Jüngeren - und nicht das Geschlecht oder die Schulbildung. Wenn also Hauptschülerinnen und -schüler erst einmal Zugang zum Internet haben, unterscheiden sie sich hinsichtlich ihrer Nutzungshäufigkeit nicht von Jugendlichen, die die Realschule oder das Gymnasium besuchen bzw. besucht haben.

Das Internet entwickelt sich hinsichtlich seiner Nutzungsmöglichkeiten kontinuierlich weiter – die Bereiche Kommunikation, Information, Spiel und virtuelles Kaufhaus wurden dabei zum Zeitpunkt der Untersuchung um Schlagworte wie Weblog (öffentliches Tagebuch) oder Podcasting ergänzt. Doch wie die Liste unterschiedlichster Nutzungsmöglichkeiten zeigt, ist das Internet für Jugendliche nach wie vor in erster Linie ein Kommunikationsmedium. 52 Prozent der Internet-Nutzer verschicken oder Empfangen mindestens mehrmals pro Woche E-Mails, 41 Prozent nutzen mit dieser Häufigkeit einen Instant-Messenger oder ein Viertel trifft sich regelmäßig zum Plaudern in Chatrooms.

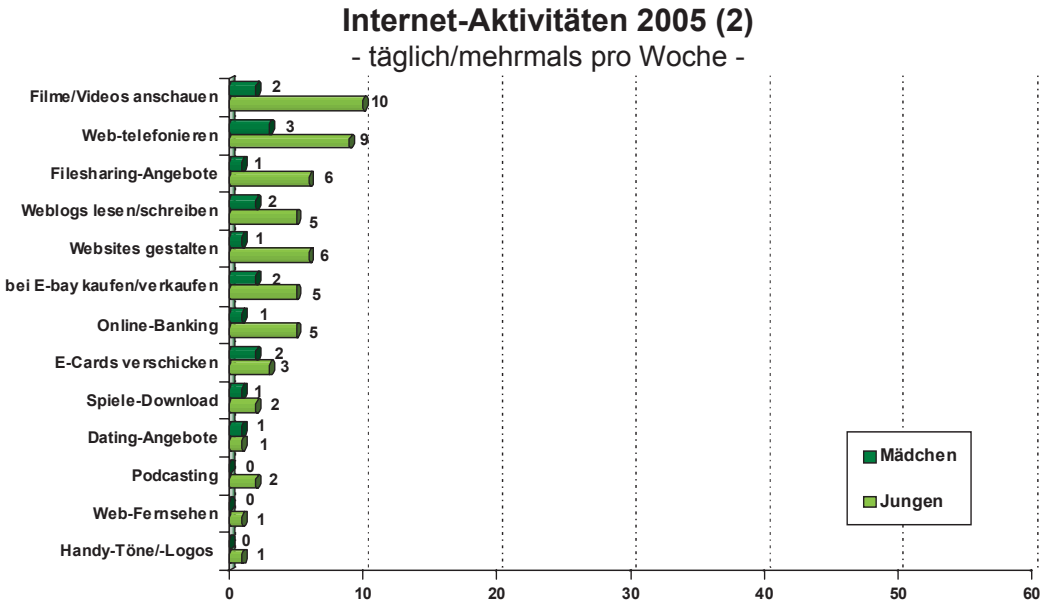
Als Internetauktionäre bei eBay treten die Jugendlichen weniger auf, aber sie stöbern gerne durch das Angebot (18 %). 13 Prozent spielen im Internet alleine oder gemeinsam mit anderen. Das für Jugendliche besonders wichtige Thema Musik wird durch das Internet ebenfalls gut bedient, 28 Prozent hören sich regelmäßig Musikstücke an oder laden diese herunter (14 %).



Quelle: JIM 2005, Angaben in Prozent

Basis: Internet-Nutzer, n=1.040

Mit zunehmendem Alter der Internet-Nutzer weitet sich auch das Anwendungsspektrum aus, was im Allgemeinen sowohl für den Bereich Kommunikation als auch für die Informationssuche gilt. Ausnahme bildet die Nutzung von Chatrooms, die auf Jüngere eine größere Anziehungskraft ausüben als auf Ältere (12-13 Jahre: 32 %, 18-19 Jahre: 19 %). Für alle Altersgruppen gleichermaßen attraktiv sind das Stöbern bei eBay und das Spielen im Netz.

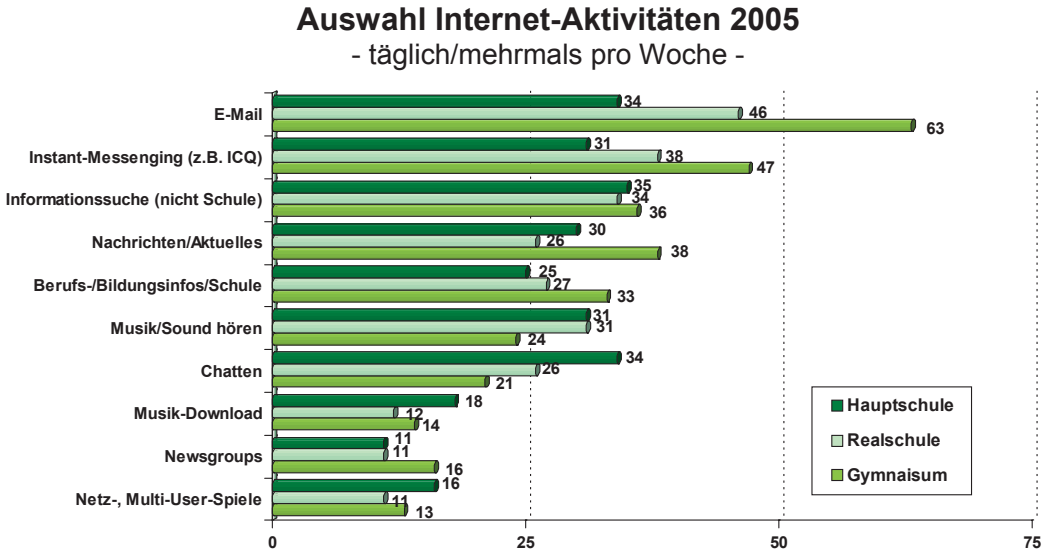


Quelle: JIM 2005, Angaben in Prozent

Basis: Internet-Nutzer, n=1.040

Ließen sich von 2003 auf 2004 für die meisten Anwendungsbereiche eher rückläufige Tendenzen beobachten, so zeigt sich 2005 der umgekehrte Trend. Deutlichste Zuwachsraten liefert die regelmäßige Nutzung von Instant-Messengern (von 25 auf 41 %), und auch die E-Mail-Nutzung ist leicht angestiegen (von 44 auf 52 %).

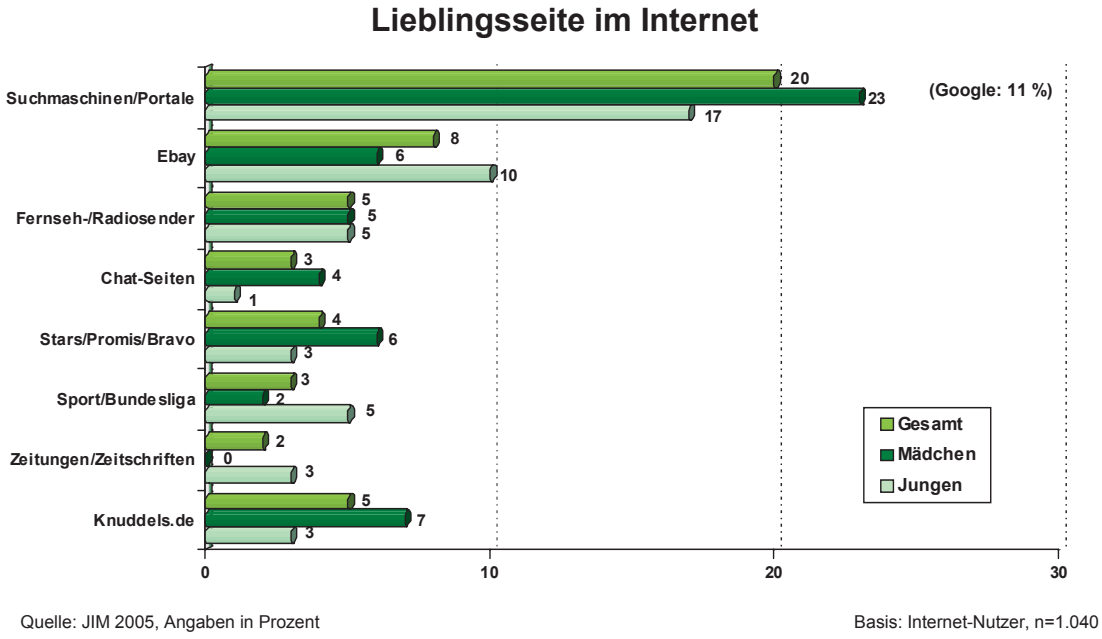
Jugendliche mit geringer formaler Bildung fallen besonders durch eine überdurchschnittliche Nutzung von Chatrooms auf, die anderen Kommunikationsformen werden dagegen unterdurchschnittlich genutzt. Hinsichtlich der Informationssuche zeigen sich kaum noch Unterschiede, aber Hauptschüler setzen das Netz weniger oft für Schule und Beruf ein. Hinsichtlich der anderen Tätigkeiten ergeben sich keine eindeutigen Befunde.



Quelle: JIM 2005, Angaben in Prozent

Basis: Internet-Nutzer, n=1.040

Auf die Frage nach der Lieblingshomepage[1] geben 20 Prozent der jugendlichen Internet-Nutzer eine Suchmaschine an, wobei alleine die Hälfte dieser Nennungen auf Google entfällt. Naturgemäß generiert eine solche Frage eine Vielzahl an Einzelnennungen, trotzdem erreicht eBay als Einzelangebot mit acht Prozent hier eine bemerkenswerte Häufigkeit. Auch das Flirtangebot ‚knuddels.de' ist vor allem bei Mädchen sehr beliebt. Unter anderem stellen Jugendliche hier eigene Fotos (in mehr oder weniger aufreizender Pose) ein und lassen sich von der Community in Form eines Rankings und durch (oft anzügliche) Kommentare bewerten. Internetseiten von Radio- oder Fernsehsendern stellen für fünf Prozent der Internet-Nutzer das beste Angebot im Netz dar.



Quelle: JIM 2005, Angaben in Prozent

Basis: Internet-Nutzer, n=1.040

Gefahren und Probleme bei der Online-Nutzung

Bei allen Chancen und Möglichkeiten, die das Internet bietet – Spaß, Unterhaltung, Spannung und vielfältigste Information – dürfen potentielle Gefahren nicht vergessen werden. Die Stichworte Pornografie und Rechtsextremismus prägen diese Diskussion auf der inhaltlichen Seite, Computerviren oder Dial-Programme stehen für eher technische Gefahren, die durch die Internet-Nutzung entstehen können.

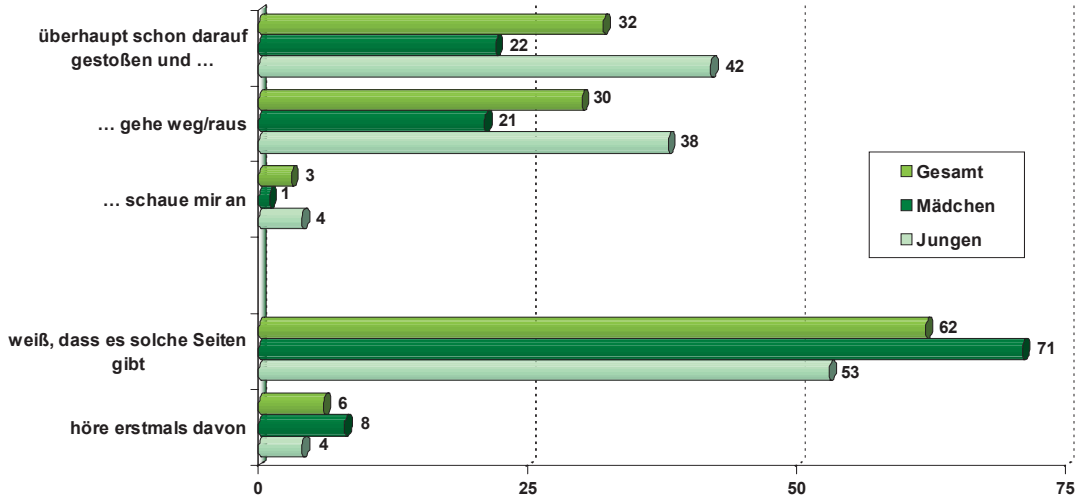
Mit Internetangeboten, die pornografische, rechtsextreme oder stark gewalthaltige Inhalte aufweisen, sind etwa ein Drittel der 12- bis 19-Jährigen Internet-Nutzer schon einmal in

[1] ‚Und welches ist Deine Lieblingsseite bzw. Deine Lieblingshomepage?'

Berührung gekommen – Jungen und junge Männer fast doppelt so häufig wie Mädchen und junge Frauen. Zwar scheinen jüngere Internet-Nutzer vor solchen Inhalten besser geschützt zu sein, aber selbst bei den 12- bis 13-Jährigen sind es bereits 18 Prozent (18-19 Jahre: 48 %). Dabei kann an dieser Stelle aber nicht geklärt werden, ob die Jugendlichen solche Angebote zufällig oder vielleicht auch bewusst genutzt haben.

Als Reaktion geben fast alle Jugendlichen an, diese Seiten sofort wegzuklicken. Ein kleiner Prozentsatz gibt aber zu, sich diese Angebote dann auch näher anzuschauen, sei es nur aus Neugierde. Da hier sicher viele junge Menschen sozial erwünscht antworten, dürfte der Anteil der ‚Nutzer' solcher problematischen Seiten weitaus größer sein.

Pornografische, rechtsradikale oder gewalthaltige Seiten im Internet



Quelle: JIM 2005, Angaben in Prozent

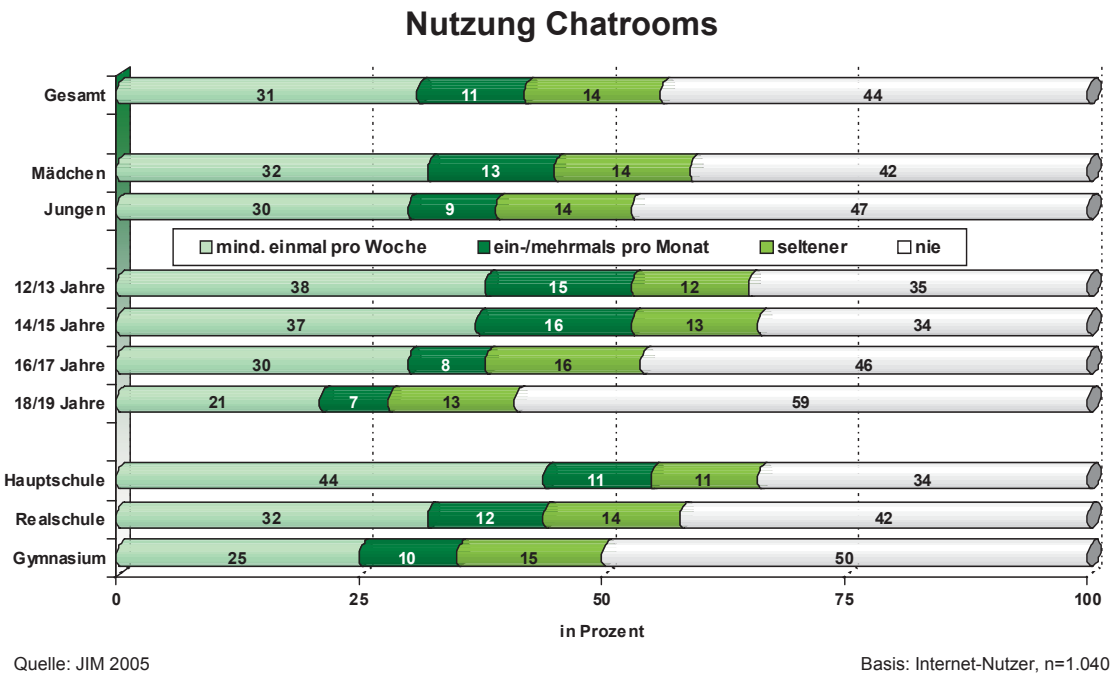
Basis: Internet-Nutzer, n=1.040

Spezielle Filterprogramme, die auf dem Computer installiert werden können, sollen die Nutzer vor solchen Inhalten schützen. Allerdings gibt nur ein Viertel der Internet-Nutzer an, dass auf ihrem Rechner zu Hause eine entsprechende Software installiert sei. Namentlich benennen können die Jugendlichen diese Software aber kaum. Mit 69 Prozent unterliegt aber der weitaus größere Teil der Jugendlichen keinerlei Einschränkungen beim Surfen. Dies gilt verstärkt mit zunehmendem Alter der Internet-Nutzer. So geben bei den 12- bis 13-Jährigen 38 Prozent an, dass sie nicht alle (gewünschten) Seiten anschauen können, bei den Volljährigen beträgt dieser Anteil nur noch 16 Prozent. Auch zeigen sich geschlechtsspezifische Unterschiede. Während ein Drittel der Mädchen über Nutzungseinschränkungen berichtet, trifft dies nur auf jeden fünften Jungen zu.

Online-Kommunikation: Chat

Mit 48 Prozent verfügt im Jahr 2005 knapp die Hälfte aller 12- bis 19-Jährigen über Erfahrungen mit Chatrooms, unter den Internet-Nutzern nehmen 56 Prozent zumindest selten einen derartigen Dienst in Anspruch. Dabei zählt ein knappes Drittel zu denjenigen, die

sehr regelmäßig mindestens einmal pro Woche chatten, elf Prozent kommunizieren gelegentlich (ein- oder mehrmals pro Monat) auf diese Art und Weise. Jungen und Mädchen weisen hier kaum Unterschiede auf, betrachtet man die einzelnen Altersgruppen, so scheint das Chatten für jüngere Onliner eine etwas höhere Attraktivität zu besitzen als für ältere. Unter den Bildungsgruppen fallen vor allem die Hauptschüler durch eine intensivere Nutzung auf.

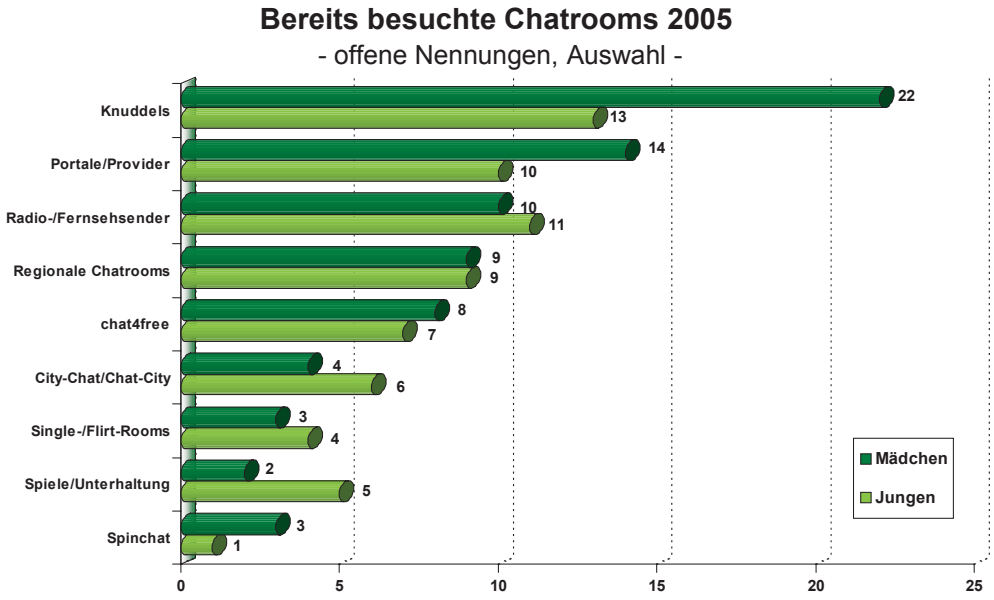


Quelle: JIM 2005

Basis: Internet-Nutzer, n=1.040

Im Vergleich zum Vorjahr ist der Prozentsatz der Chat-Erfahrenen zwar insgesamt etwas rückläufig, die Häufigkeit dieser Kommunikationsform ist aber von 25 Prozent intensiver Nutzung auf 31 Prozent angestiegen. Überdurchschnittlich fiel der Zuwachs bei den 12- bis 13-Jährigen (plus 16 Prozentpunkte) und den Hauptschülern (plus 18 Prozentpunkte) aus.

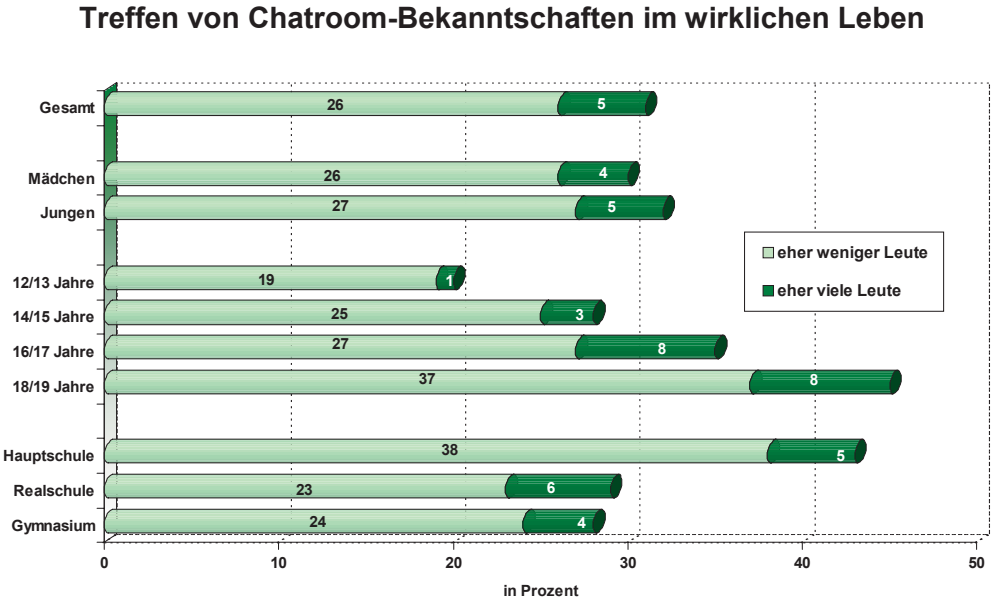
Die Angaben zur Nutzung konkreter Foren fallen genauso zahlreich aus wie die Angebote selbst, trotzdem lassen sich einige Plattformen ausmachen, die bei den Jugendlichen besonders verbreitet sind. Den ersten Platz nimmt sowohl bei den Jungen als auch bei den Mädchen ‚knuddels.de' ein. Communities, die von Providern bzw. größeren Portalen angeboten werden, sind ähnlich beliebt wie die Angebote der Radio- und Fernsehsender oder regionale Chatrooms.



Quelle: JIM 2005, Angaben in Prozent

Basis: Chatroom-Nutzer, n=580

Neue Bekanntschaften, Kontakte oder Flirts sind die wichtigsten Motive für den Besuch eines Chatrooms. Auch wird der Wunsch, sich mit anderen zu unterhalten, generell Gespräche zu führen, von vielen Jugendlichen als Grund genannt. Weitere, wenn auch weniger dominante Motive sind Spaß, Zeitvertreib oder (mehr oder weniger) gezielter Informationsaustausch.



Quelle: JIM 2005

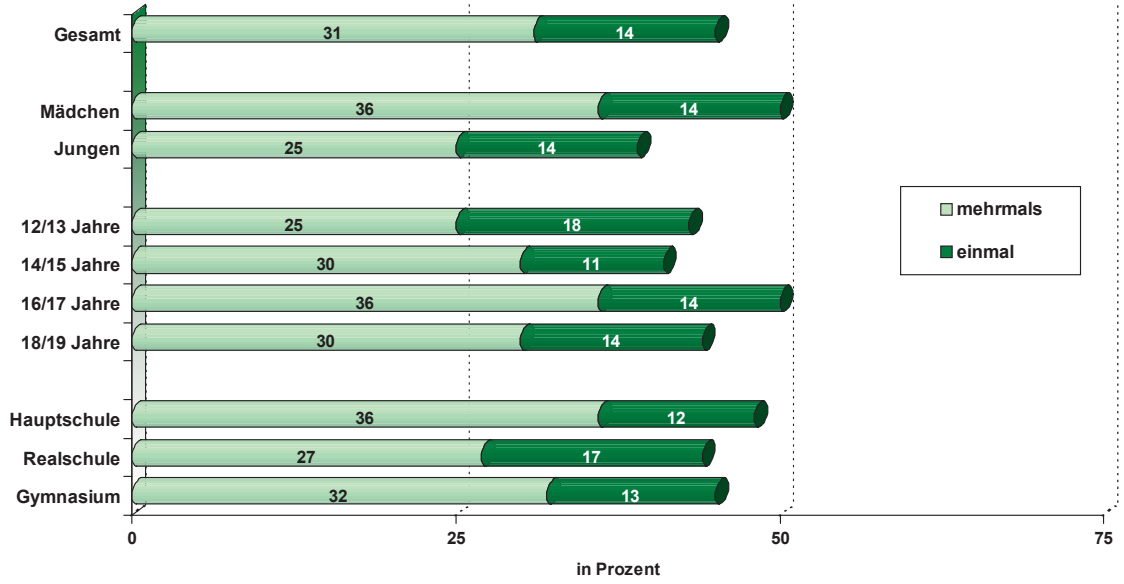
Basis: Chatroom-Nutzer, n=580

Die im Chatroom geknüpften Kontakte führen mit zunehmender Tendenz auch zu realen Begegnungen. 2005 bestätigt ein Drittel dieser Jugendlichen ein solches Treffen, der Vorjahreswert lag mit 24 Prozent darunter. Jungen und Mädchen unterscheiden sich hier nicht, das Treffen von Chat-Bekanntschaften nimmt aber mit dem Alter der Jungendlichen

zu. Bei den 12- bis 13-Jährigen bestätigen bereits 20 Prozent solche Treffen, bei den 18- bis 19-Jährigen mit 45 Prozent mehr als doppelt so viele. Bei den Bildungsgruppen stechen auch hier die Hauptschüler deutlich heraus.

Auf unangenehme Menschen im Chatroom selbst sind ein Drittel der Jugendlichen schon mehrmals, 14 Prozent bisher nur einmal gestoßen. Mädchen fühlen sich häufiger belästigt als Jungen, ansonsten berichten die Jugendlichen unabhängig von Alter oder Bildungshintergrund in vergleichbarem Ausmaß von solchen Begegnungen. Über die Bandbreite solcher Belästigungen (von Kraftausdrücken über Beschimpfungen bis hin zur sexuellen Belästigung) kann dabei nur spekuliert werden. Als Reaktionen geben die Jugendlichen zunächst Ignorieren oder das Verlassen des Chatrooms an, das Sperren von Personen scheint aber ebenfalls an der Tagesordnung zu sein.

Im Chatroom unangenehme Leute getroffen



Quelle: JIM 2005, Angaben in Prozent

Basis: Chatroom-Nutzer, n=580

Die wichtigsten Befunde der Internetnutzung der 12- bis 19-Jährigen

- 86 Prozent der Jugendlichen nutzen das Internet. Für Jugendliche ist das Internet bereits Teil des Alltags.
- 70 Prozent der Internetnutzer sind mehrmals pro Woche im Netz.
- Zunehmend intensive Nutzung von Chatrooms (von 25 % auf 31 %, überdurchschnittlicher Zuwachs bei den jüngsten und bei bildungsfernen Jugendlichen). Kommunikation (Chat, ICQ) gewinnt an Bedeutung.
- Ein Drittel der jugendlichen Chat-Nutzer hat Internetbekanntschaften auch schon im realen Leben getroffen.
- Ein Drittel der Internetnutzer ist bereits auf Seiten gestoßen, die rechtsextreme, stark gewalthaltige oder pornographische Inhalte enthalten.

Exkurs: KIM-Studie 2005 (6 bis 12 Jahre)

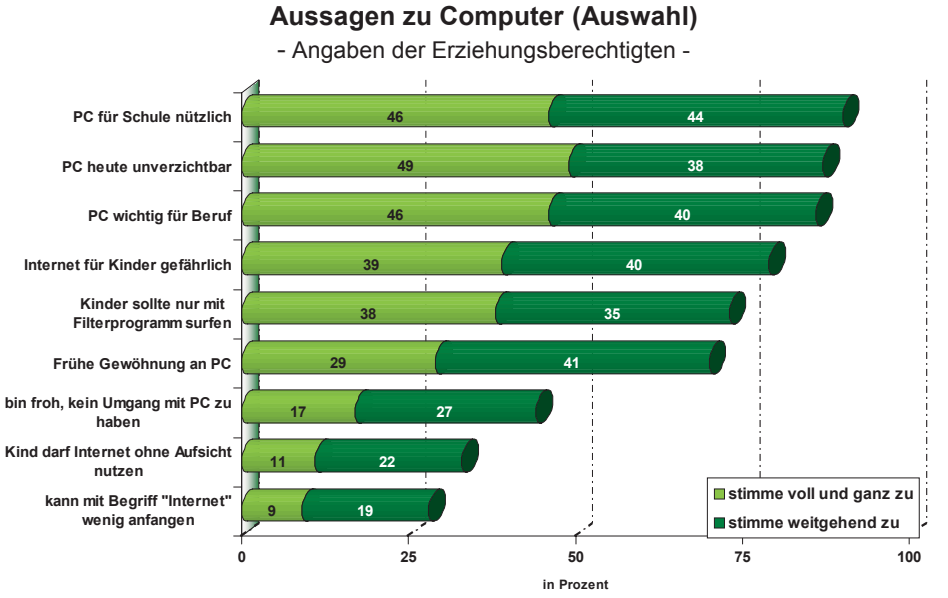
Nach diesem Überblick über die jugendliche Medienwelt zeigt ein kleiner Exkurs zu den Ergebnissen der KIM-Studie, die sich mit dem Medienumgang der 6- bis 13-Jährigen befasst, welchen Stellenwert die Medien bereits bei den Kindern haben.

Der Computer ist bereits Bestandteil der kindlichen Lebenswelt geworden. Kinder haben überwiegend bereits Erfahrungen mit einem Computer gesammelt. Dabei steht bei den 6- bis 13-Jährigen noch der spielerische Umgang im Vordergrund. Jedoch wird der PC bereits für die Schule eingesetzt. Über zwei Drittel der Kinder, die schon Computererfahrung haben, nutzen zumindest selten das Internet.

Ergebnisse der KIM-Studie zum Computerumgang der 6- bis 13-Jährigen

- Drei Viertel der 6- bis 13-Jährigen sind bereits Computernutzer.
- Ein Viertel davon nutzt den Computer jeden Tag.
- Häufigste Tätigkeit ist Computerspielen.
- Jedes zweite Kind nutzt den PC regelmäßig für die Schule.
- Ein Viertel der Kinder darf am Computer machen, was es will.
- Jedes zweite Kind hat bereits Interneterfahrung.

Bei der KIM-Studie wird nicht nur der Medienumgang der Kinder erhoben, auch die Haupterzieher, in der Regel die Mütter, werden zu ihrer Mediennutzung und Einstellung zu Medienfragen befragt. Bei der Frage nach den Einstellungen zum Computer zeigt sich ein ambivalentes Verhältnis der Eltern zum Computer: Einerseits wird der PC als wichtig und unverzichtbar angesehen, andererseits wird das Problempotential des Internet erkannt, dennoch lässt ein Drittel der Eltern die Kinder ohne Aufsicht ins Netz.



Quelle: KIM 2005

Basis: alle Erziehungsberechtigten, n=1.203

Grundlegende Konflikte und Kontroversen beim Umgang mit ‚geistigem Eigentum' in der Wissens- und Informationsgesellschaft

Dr. Andreas Degkwitz

Für die Wissenschaft ist das Internet an vielen Stellen ein riesiger Sprung nach vorne gewesen, sowohl was die Verbreitung von Wissen und natürlich auch was die Produktion von Wissen betrifft. Die vergleichsweise einfachen Möglichkeiten der Produktion von Artikeln und deren schnelle Verbreitung über das Internet haben die Dynamik des Wissens- und Informationstransfer signifikant verändert. In den medizinischen, naturwissenschaftlichen und technologiebezogenen Fachgebieten sind inzwischen fast 90 Prozent der Zeitschriften über das Internet verfügbar. Auch in den juristischen Fachgebieten, die lange Zeit etwas zurückhaltend waren, gibt es inzwischen sehr gute Angebote, die eine Internetnutzung von Fallsammlungen, Paragrafensammlungen, Kommentaren etc. ermöglichen, so dass sich auf einer breiten Strecke - bis hin zu den Geist- und Kulturwissenschaften - von einer starken Internetnutzung auf dem Gebiet der Fachinformation sprechen lässt.

Die Distribution von Fachinformation über das Internet, aber auch die Möglichkeiten, direkt im Internet zu publizieren, stehen in einem gewissen Widerspruch zu der bisherigen Publikationspraxis in der Wissenschaft, die stark an den Verfahren der Produktion und Verbreitung gedruckter Materialien orientiert ist und die Ausgestaltung des Urheberrechts wesentlich geprägt hat. War es bisher so, dass der Produktions- und Verbreitungsprozess von Monographien und Zeitschriften an einen Verleger ‚nach draußen' gegeben wurde, der dann mit Übernahme der Verbreitungsrechte, die ja Bestandteil des Urheberrechtsgesetzes sind, auch das wirtschaftliche Risiko trägt, ist das im Internetzeitalter insofern anders, als der Produktionsanteil des Autors an der Publikation deutlich höher geworden ist und zumindest die technischen Voraussetzungen für die Distribution von Wissensbeiträgen über das Internet gegeben sind. Von daher stellt sich gelegentlich die grundsätzliche Frage, ob der Intermediär ‚Verlag' überhaupt noch erforderlich ist. Verlage haben weiterhin ihre Berechtigung, aber das Verfahren des Publizierens über das Desktop Publishing sowie der Verbreitungs- und Verfügbarkeitsoptionen über das Internet hat die Situation schon verändert.

Hinzu kommt, dass der Wissenschaftsmarkt bzw. der Fachinformationsmarkt im Vergleich zu den Konsumermärkten für Musik und Videos eine Nische darstellt, die sicher kein Massengeschäft garantiert. Zudem konzentriert sich die kommerzielle Publikation wissenschaftlicher Fachinformation für die einzelnen Fachgebiete im Regelfall auf vergleichsweise wenige Anbieter, zu denen es keine echte Marktalternative gibt. Als Beispiel dafür sei für den juristischen Bereich der Beck-Verlag genannt, der ein Quasi-Monopol für seine Publikationsprodukte hat. Es gibt keinen zweiten Beck-Verlag, wo diese Produkte eventuell günstiger zu beziehen sind - das ist für dieses Fachgebiet und gerade in der deut-

schen Gesetzgebung der Beck-Verlag. Für andere Wissenschaftsdisziplinen ist dies - auch auf globaler Ebene - ganz genau so zu sehen.

Natürlich ist die Versuchung groß, aus dieser Monopolstellung heraus nun auch besondere Umsatz- und Gewinnvorteile zu erzielen, die dann dazu führen, dass das Angebot über die Preise stark verknappt wird. Gerade bei den großen, internationalen Verlagskonzernen ist es in den vergangenen Jahren zu überproportionalen Preissteigerungen gekommen. In mancher Hinsicht ist festzustellen, dass es fast kein so sicheres Geschäft wie das dieser Verlagsmonopole gibt - mit kontinuierlichen und nahezu prognostizierbaren Steigerungsraten. Durch das Internet und die Möglichkeiten der Zugriffsbeschränkungen (z.B. Digital-Rights-Managementsysteme) wird diese Entwicklung noch verschärft, so dass die Monopolisierung des Marktes die Informationsfreiheit im konkreten Fall tatsächlich beeinträchtigen kann. Die Informationsfreiheit ist natürlich weiterhin gegeben, aber die hohen Kosten können schon dazu führen, dass der Informations- und Wissensaustausch in Forschung und Lehre erschwert wird. Wer die Budgets deutscher Hochschulen bzw. Hochschulbibliotheken näher betrachtet, wird das schnell nachvollziehen können.

Für den Bereich der akademischen Forschung ist allerdings auch deshalb eine besondere Marktsituation gegeben, weil das Verhältnis zwischen Produzent und Rezipient, zwischen Autor und Leser jedenfalls in den Kernbereichen der Wissenschaft sehr viel dichter beieinander liegt, als das auf den Konsumermärkten der Fall ist. In vielen Fällen sind Autoren und Leser - gerade bei Forschenden und Lehrenden - mehr oder weniger identisch. Auch die Studierenden gehören in dieses Umfeld. Insofern ist festzustellen, dass die Konditionen, die auf den Konsumermärkten existieren, nicht ohne weiteres auf den wissenschaftlichen Fachinformationsmarkt übertragbar sind. Nicht zuletzt ist darauf hinzuweisen, dass die meisten Forschungs- und Lehraktivitäten mit öffentlichen Mitteln finanziert werden und sich insofern auch als eine Art Allgemeingut betrachten lassen. Dadurch, dass auf dem Wege einer Verlagsveröffentlichung die Abtretung der Verbreitungs- bzw. Verwertungsrechte an die Verlage erfolgt und die stattlich finanzierten Institutionen (z.B. Universitäten) dann im Grunde diese Veröffentlichungen zu hohen Preisen wieder zurückkaufen, stellt sich die Frage, ob dieser Kreislauf wirklich so ganz in Ordnung ist. Also erst wird mit öffentlichen Mitteln Forschung und Lehre finanziert und dann werden die publizierten Ergebnisse mit öffentlichen Mitteln wieder zurückgekauft. Es ist allerdings ausdrücklich darauf hinzuweisen, dass sich das Problem dieser Wertschöpfungsform weniger auf die kleinen und mittelständischen Verlage bezieht, die einfach von ihrer Marktposition her darauf angewiesen sind, dass mit dem Preis-Leistungsverhältnis ihrer Produkte eine vernünftige Relation zwischen Kostendeckung auf der Anbieterseite und Finanzierungspotential der (für Fachinformation im Regelfall institutionellen) Käuferseite besteht. Das Problem ist durch die Marktkonzentration großer (shareholder-value-orientierter) Verlagskonzerne insbesondere auf dem Markt der medizinischen, naturwissenschaftlichen und technologieorientierten Fachinformation entstanden – und da geht es schon um Gewinnoptimierung.

Die Urheberrechtsgesetzgebung bietet den rechtlichen Rahmen zur Vermeidung von Missbrauch: Die Interessen von Autoren, Verwertern und derer, die geschützte Materialien nutzen, sollen innerhalb eines rechtlichen Rahmens zu einem Ausgleich gebracht werden. Im Hinblick auf das Internet wird man sicherlich einräumen müssen, dass häufig ein wenig ausgeprägtes Bewusstsein besteht, dass dort verfügbare Materialien (Bilder, Texte, Videos etc.) ebenfalls urheberrechtlich geschützt sind, sodass der Umgang mit Urheber- und Verwertungsrechten in vielen Fällen als eher fahrlässig zu bezeichnen ist. Die Sensibilisierung ist meistens nicht sehr hoch. Von daher kann durchaus passieren, dass beispielsweise im Rahmen von Tele-Teaching und Tele-Learning die Web-basierten E-Learning-Systeme mit (geschützten) Bildern bestückt und öffentlich verfügbar gemacht werden, ohne dass sich jemand darum gekümmert hat, wer die Rechte für diese Bilder besitzt. Das ist bei gedruckten Publikationen eine Aufgabe, die üblicherweise von den Verlagen erledigt wird; dabei wird schon sehr viel eher darauf geachtet, dass dergleichen ordentlich abgewickelt wird.

Insofern ist mit dem Internet der Umgang mit geschützten Materialien freizügiger geworden, ohne dass dies eine rechtliche Grundlage hätte – es wird einfach gemacht, weil es leicht möglich ist und digitale Materialien einfach auffindbar und beliebig reproduzierbar sind. Auf der anderen Seite bestehen mittlerweile auch Ängste, weil es im Kontext von Lehre und Studium schon zu Klagen mit entsprechenden Schadensersatzforderungen kam, sodass Formen des virtuellen Lehrens und Lernens auch deshalb nicht praktiziert werden, weil der Umgang mit geschützten, digitalen Materialien im Schul- und Hochschulbereich nicht oder eben zu wenig bekannt bzw. bewusst ist. Auch ist die Rechtslage nicht an allen Stellen unmittelbar nachvollziehbar und transparent, sodass der Eindruck entsteht, in diesen Kontexten über juristische Spezialkenntnisse verfügen zu müssen.

Die Novellierung des Urheberrechtsgesetzes in Deutschland findet vor dem Hintergrund der europäischen Bemühungen um eine Harmonisierung der Urheberrechtsgesetzgebung in den EU-Partnerländern statt. Dieser Prozess hat 2001 eingesetzt und kommt gegenwärtig in den europäischen Partnerländern zur Umsetzung. In Deutschland hat man den so genannten 1. Korb der Urheberrechtsgesetznovelle im Jahr 2003 verabschiedet. Dabei wurde deutlich, dass die bisher für Bildung und Wissenschaft bestehenden Freiräume (Schranken), die in starkem Maße an der Praxis gedruckter Publikationen orientiert waren, sich nicht ohne weiteres in die elektronische Welt übertragen lassen. Dabei geht es vor allem um folgende Paragraphen, auf die das Aktionsbündnis ‚Urheberrecht für Bildung und Wissenschaft' in seiner Stellungnahme zum Kabinettentwurf zur Urheberrechtsnovelle vom 22. März 2006 eingeht:

- § 52b (Entwurf) zur Wiedergabe von Werken an elektronischen Leseplätzen in Bibliotheken, Archiven und Museen
- § 53a (Entwurf) zum Versand von digitalen Kopien
- § 53 Abs. 2 Nr. 2 UrhG zur Zulässigkeit elektronischer Archive
- § 95b UrhG zur Durchsetzung der Privatkopie bei technischen Schutzmaßnahmen

- § 31a UrhG (Entwurf) zu den unbekannten Nutzungsarten: Archivregelung
- Änderung des § 53 Abs. 5 UrhG zur Erweiterung des Rechts der elektronischen Archivkopie (§ 53 Abs. 2 Nr. 2 UrhG) auf elektronische Datenbankwerke
- § 49 UrhG zu Elektronischen Pressespiegeln
- § 52a UrhG zur Verlängerung der Befristung in § 137k
- § 95b UrhG zur Neubewertung der technischen Schutzmaßnahmen (DRM)

In seiner Stellungnahme hat das Aktionsbündnis auf die folgenden Auswirkungen hingewiesen, die sich aus dem Gesetzgebungsentwurf zu diesen Paragraphen ergeben, und unter *http://www.urheberrechtsbuendnis.de/docs/ABStellungnahmeKorb2.pdf* entsprechende Vorschläge zur Änderung und Verbesserung des Novellierungsentwurfs aufgezeigt (***Zitatanfang***):

§ 52b UrhG (Entwurf): Wiedergabe von Werken an elektronischen Leseplätzen in Bibliotheken, Archiven und Museen (on the spot consultation)

Dass über den neuen § 52b der Zugriff auf elektronische Materialien in Bibliotheken geregelt, also eine positiv einzuschätzende Ausnahmeregelung (eine Ausnahme von dem ansonsten exklusiven Recht der Rechteinhaber, über die Bereitstellung publizierter Materialien zu entscheiden) in das Gesetz aufgenommen werden soll, ist zu begrüßen. Die verschiedenen Einschränkungen dieser Regelung gehen allerdings an Praxis und Bedürfnissen von Bildung und Wissenschaft vorbei. Angesichts der flächendeckend vorhandenen Hochschul- und Universitätsnetze ist absolut unverständlich, dass Wissenschaftler, Dozenten und Studierende ihre gewohnte Umgebung verlassen sollen, um in der Bibliothek an speziellen Leseplätzen elektronische Materialien einzusehen. Befremdlich ist diese Beschränkung auch angesichts der Tatsache, dass selbst in den USA, wo starke Copyright-Regelungen gelten und Studierende selbstverständlich auch von ihrer Wohnung aus auf die Bestände der Bibliothek zugreifen, ein solcher wissenschaftspraxisfremder Vorschlag keine Akzeptanz finden würde. Problematisch ist weiterhin, dass - nicht nur bei diesem Paragraphen, sondern auch bei §§ 52a, 53 und 53a - den Gegebenheiten von Public-Private-Partnership-Projekten, bei denen also auch Partner der Wirtschaft beteiligt sind, nicht Rechnung getragen wird, da auf die Materialien der Bibliotheken nicht mehr zugegriffen werden darf, wenn auch nur indirekt kommerzielle Interessen im Spiel sein könnten.

§ 53a UrhG (Entwurf): Versand von digitalen Kopien

Die vorgesehene Regelung in diesem Paragraphen, durch den der elektronische Kopienversand durch Bibliotheksverbundleistungen (wie bei SUBITO) bildungs- und wissenschaftsfreundlich geregelt werden sollte, ist weitgehend inakzeptabel. Die Beschränkung auf Post und Fax (als erlaubte Versandform) wird der computer- und netzgestützten Wissenschafts- und Ausbildungspraxis nicht gerecht. Was die Beschränkung des Versands elektronischer Materialien auf grafische Dateien betrifft, muss der Gesetzgeber anerkennen, dass dies für die Wissenschaftspraxis keine Lösung ist, wenn z.B. in technischen

Fachgebieten digitale Materialien oder Formeln direkt in eigene Texte übernommen werden wollen (was bei grafischen Dateien nicht geht). Die Medienbrüche bei grafischen Dateien behindern die wissenschaftliche Arbeit. Zudem entsteht durch die Erstellung grafischer Dateien (aus an sich verfügbaren elektronischen Dateien) ein unvertretbarer Mehraufwand für Bibliotheken und Nutzer. Für dieses Problem muss unbedingt ein Kompromiss gefunden werden, der sich mit den Vorgaben der EU-Richtlinie verträgt. Höchst problematisch ist, dass der vorgeschlagene Paragraph den kommerziellen Anbietern quasi ein Monopolrecht auf den elektronischen Versand von Dokumenten einräumt. Dadurch werden zum einen in der Wissenschaft sog. Zwei-Klassen-Gesellschaften entstehen – solche, die Mittel zum Bezahlen der kommerziellen Dienste haben, und solche, die sie nicht haben. Zum andern werden die Studierenden quasi gezwungen, bei Ausbleiben der Informationsversorgung durch die Bibliotheken und bei begrenzten eigenen Mitteln auf das Angebot freier Suchmaschinen (Google, Yahoo etc.) zuzugreifen, was nicht im Interesse eines qualitativ hoch stehenden Hochschulsystems sein kann.

§ 53 Abs. 2 Nr. 2 UrhG: Klarstellung zur Zulässigkeit elektronischer Archive

Die hier einschlägigen Formulierungen in § 53 sind kaum verständlich und werden für Verwirrung in der täglichen Praxis sorgen; z.B. ist nicht eindeutig, ob nun, wie gewünscht, alle Einrichtungen in den Bereichen Bildung und Wissenschaft das Recht auf Anlegen und Nutzen von Archiven zugebilligt wird.

§ 95b UrhG: Durchsetzung der Privatkopie bei technischen Schutzmaßnahmen

Der Gesetzgeber (wie auch die EU-Richtlinie) räumt den technischen Schutzmaßnahmen einen schwer nachvollziehbaren Kredit (auf Zuverlässigkeit und Akzeptanz) ein. Bei einem nachweislich wissenschaftlichen Gebrauch von entsprechend geschützten Werken aus Beständen öffentlich zugänglicher Bibliotheken und vergleichbaren Einrichtungen können die Nutzer die Aufhebung dieser Maßnahmen verlangen, was sich in der Praxis als schwierig erweisen dürfte. ‚Normal'-Bürgern, die ebenfalls zur Absicherung ihrer privaten ‚Geschäfte' auf wissenschaftliche Ergebnisse zurückgreifen wollen und sollen, wird dieses Recht verweigert.

§ 31a UrhG (Entwurf): Unbekannte Nutzungsarten: Archivregelung

Den Wegfall des Absatz 4 von § 31 kritisieren viele Vertreter von Urheberrechtsinteressen. In der Tat ist es kaum zu akzeptieren, dass die Rechte der Autoren zugunsten der Interessen der Verwerter immer weiter geschwächt werden. Allerdings ist es durchaus im Interesse der Autoren in den Bereichen von Bildung und Wissenschaft, wenn Werke so breit wie möglich zugänglich werden, allerdings nicht um den Preis der Aufgabe aller Rechte.

§ 53 Abs. 2 Nr. 2 UrhG: Erweiterung des Rechts der elektronischen Archivkopie auf elektronische Datenbankwerke durch Änderung des § 53 Abs. 5 UrhG

Zu den nach wie vor unzureichend gelösten Problemen der Digitalisierung von Informationsressourcen gehört die Langzeitsicherung dieser Materialien. Das kulturelle Erbe muss in den Bereichen Bildung und Wissenschaft für Zwecke der Forschung und der Lehre gewährleistet sein. Die vorliegenden Formulierungen in § 53 Abs. 2 Nr. 2 UrhG sichern das unverzichtbare Recht auf Archivierung nicht eindeutig zu.

§ 49 UrhG: Elektronischer Pressespiegel

In den Formulierungen von § 49 wird der Wissenschaftspraxis nicht eindeutig das Recht auf Erstellung von Pressespiegeln für den eigenen Gebrauch zugestanden. In manchen Fachgebieten sind diese unverzichtbar. Auf kommerzielle Quellen kann wegen oft fehlender Spezifizierung nicht zurückgegriffen werden.

§ 52a UrhG: Verlängerung der Befristung

Der § 52a, der die öffentliche bzw. teil-öffentliche Bereitstellung von Materialien im Rahmen der sog. Wissenschafts- und Bildungsschranke erlaubt, war im Kontext der ersten Anpassung der Urheberrechtsgesetzgebung (2003) stark umstritten. Vor allem der Börsenverein hatte sich vehement dagegen positioniert. Als Kompromiss hatte man sich auf eine Befristung des § 52a (in seiner jetzigen Form) bis zu Ende 2006 geeinigt. Obgleich § 52a für die Bedürfnisse von Bildung und Wissenschaft sehr restriktiv gefasst ist, würde der vollständige Wegfall zu einer massiven Beeinträchtigung neuer, digitaler Lehr- und Lernformen in Bildung und Wissenschaft führen. Da nicht mehr viel Zeit für eine über eine entsprechende gesetzliche Regelung vorzunehmende Verlängerung dieser Befristung bleibt, besteht hier dringender Handlungsbedarf.

§ 95b UrhG: Neubewertung der technischen Schutzmaßnahmen (DRM)

Die Regelungen in § 95b könnten im Prinzip positiv gesehen werden, weil hierdurch den Nutzern von Werken, die mit technischen Schutzmaßnahmen versehen sind, das Recht eingeräumt wird, ihren Rechtsanspruch auf Zugriff auch auf solche Werke ggf. einklagen zu dürfen. Die Praxis der Durchsetzung eines solchen Anspruchs ist aber in § 95b nicht realistisch geregelt. Eine Klage wird bei in der Regel aktuell zu befriedigenden Informationsbedürfnissen (z.B. bei der Einsicht für einen gerade anstehenden Kurs) zu nicht hinnehmbaren Verzögerungen führen. Die bisherigen Ausnahmeregelungen, die für den Wissenschaftsbereich bestanden, die so genannten Schrankenregelungen, sind de facto aufgehoben. Der Referentenentwurf, der jetzt Anfang des Jahres den 2. Korb noch einmal aufleben ließ, hat zwar an einigen Stellen die bisherigen Vorschläge revidiert, aber signifikant hat sich nichts geändert (***Zitatende***).

Wenn der vorliegende Entwurf Gesetz wird, führt dies dazu, dass sich das Urheberrecht eher als ein Handels- und Verwertungsrecht erweist und nicht so sehr als eine Gesetzge-

bung versteht, die den Interessen von Autoren und Rezipienten (Leser) im Bildungs- und Wissenschaftsbereich Rechnung trägt. Damit wird ausdrücklich nicht behauptet, dass eine Urheberrechtsgesetzgebung gar nicht gebraucht wird - die braucht man natürlich; denn die Wissenschaftler wollen als Autoren und Rezipienten in diesem Kontext geschützt sein. Diesen Schutz brauchen sie nicht zuletzt gegenüber den Verlagen.

Nun lässt sich einwenden, warum in der Gesetzgebung für den Bildungs- und Wissenschaftsbereich eine Ausnahme geschaffen werden soll - ist doch der Wissenschaftsmarkt im Grundsatz genau so ein Markt wie alle anderen Märkte auch. Dann muss man sich allerdings der Tatsache bewusst sein, dass dies zu signifikant höheren Kosten auf dem Fachinformationsmarkt führen wird, die sich primär auf zusätzliche Lizenzierungskosten und in der weiteren Folge auf die versteckten Kosten für das gesamte Handling im Umgang mit digitalen Informationen beziehen, das sich aus dieser Gesetzgebung ergibt. Denn wenn Heerscharen von Bibliothekaren oder Mitarbeitern von Medienzentren dafür eingesetzt werden müssen, um z.B. für Forschende und Lehrende Lizenzverhandlungen zu führen, kann das eigentlich nicht als ein Fortschritt auf dem Weg in die Informationsgesellschaft betrachtet werden. Die Forschungs- und Studienbedingungen an deutschen Hochschulen werden sich dadurch verschlechtern.

Deswegen brauchen wir faire Bedingungen, die in diesem Segment die multilateralen Interessen berücksichtigen, und dafür setzt sich das Aktionsbündnis ‚Urheberrecht für Bildung und Wissenschaft' ein. In diesem Zusammenhang werden Vergütungsregelungen eine wichtige Rolle spielen, wie sie für gedruckte Publikationen schon seit längerem existieren (z.B. über die VG Wort). Darüber hinaus sollte man sich im Rahmen des weiteren Gesetzgebungsprozesses stärker an Beispielen des angloamerikanischen Auslandes orientieren, wo für den Bereich von Bildung und Wissenschaft Fair-use-Regelungen existieren, die den bisher in der deutschen Urheberrechtsgesetzgebung bestehenden Schrankenregelungen (Freiräume) in etwa entsprechen.

Das Aktionsbündnis ‚Urheberrecht für Bildung und Wissenschaft' wurde 2004 im Zusammenhang mit der Novellierung der Urheberrechtsgesetzgebung in Deutschland gegründet. Das Aktionsbündnis setzt sich für ein ausgewogenes Urheberrecht ein und fordert für alle, die zum Zweck von Bildung und Wissenschaft im öffentlichen Raum tätig sind, den freien Zugang zur weltweiten Information zu jeder Zeit von jedem Ort. Grundlage des Aktionsbündnisses ist die Göttinger Erklärung zum Urheberrecht für Bildung und Wissenschaft vom 5. Juli 2004. Diese Erklärung wurde unterzeichnet von der Allianz der Wissenschaftsorganisationen (Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., Helmholtz-Gemeinschaft Deutscher Forschungszentren e.V., Hochschulrektorenkonferenz, Max-Planck-Gesellschaft, Wissenschaftsgemeinschaft Gottfried Wilhelm Leibniz e.V. und Wissenschaftsrat), von 260 wissenschaftlichen Fachgesellschaften, Informationseinrichtungen und Verbänden sowie von mehr als 3.700 Einzelpersönlichkeiten (Stand 2006).

Literatur:

Beger, Gabriele: Urheberrecht und elektronische Bibliotheksangebote. Ein Interessenkonflikt. Erschienen in der Reihe Berliner Arbeiten zur Bibliothekswissenschaft. Band 8. – hrsg. v. Institut für Bibliothekswissenschaft der Humboldt-Universität Berlin, Logos Verlag Berlin 2002

Degkwitz, Andreas: ‚Berliner, Göttinger und Wiener Erklärung: Empfiehlt sich für die Universität Hannover eine Unterschrift?' – Zugang: *http://www.iri.uni-hannover.de/de/start/veranstaltungen/urheberrechts-tagung.html* (2006)

Göttinger Erklärung des Aktionsbündnisses ‚Urheberrecht für Bildung Wissenschaft' - Zugang: *http://www.urheberrechtsbuendnis.de* (2004)

Hoeren, Thomas: Urheberrecht und Verbraucherschutz. Überlegungen zum Gesetz über Urheberrecht in der Informationsgesellschaft. Gutachten im Auftrag von Verbraucherzentrale Bundesverband e.V. in Berlin. - Zugang: *http://www.vzbv.de/mediapics/1043159929Gutachten_Urheberrecht_Hoeren_2003.pdf (*2003)

Kuhlen, Rainer: Wissen als Eigentum. Wie kann der freie Zugang zu den Ressourcen des Wissens in globalen Informationsräumen gesichert werden? Zugang: *http://www.Wissensgesellschaft.org/themen/publicdomain/wisseneigentum.pdf* (2003)

Meier, Michael: Returning Science to the Scientists. Der Umbruch im STM-Zeitschriftenmarkt unter Einfluss des Electronic Publishing. – München, Peniope, 2002

National Research Council: The Digital Dilemma. Intellectual Property in the Information Age. Zugang: *http://www.nap.edu/html/digital_dilemma/notice.html* (2003)

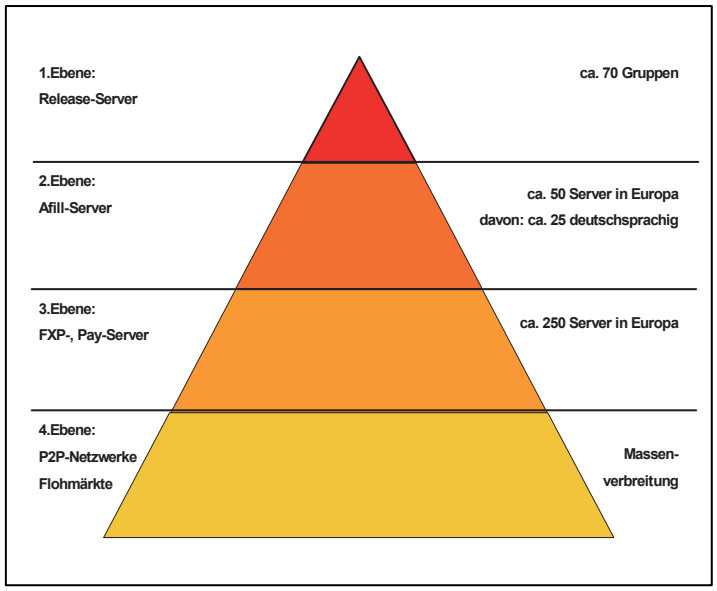
Sieber, Ulrich; Hoeren, Thomas: Urheberrecht für Bildung und Wissenschaft – Anforderungen an das Zweite Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft. Beiträge zur Hochschulpolitik 2. - Hochschulrektorenkonferenz, Bonn 2005

Stellungnahme des Aktionsbündnisses ‚Urheberrecht für Bildung und Wissenschaft' zum Kabinettentwurf zur Urheberrechtsnovelle vom 22. März 2006. Zugang: *http://www.urheberrechtsbuendnis.de/docs/ABStellungnahmeKorb2.pdf* (2006)

Prävention und Verfolgung von ‚digitalen Pirateriedelikten' aus der Sicht der gewerblichen Urheber und Marktanbieter

Jan D. Scharringhausen

Etwa seit Ende des Jahres 2000 ist die Filmbranche in all ihren Auswertungsstufen Opfer der digitalen Piraterie und dabei insbesondere der durch das Internet beförderten in Sekundenbruchteilen vor sich gehenden illegalen Verbreitung von neuesten Kinofilmen. Die hier gezeigte Grafik gibt einen schematischen Überblick über die Verteilung von Raubkopien aktueller Kinofilme. Ausgangspunkte der Kinofilm-Raubkopien sind in den allermeisten Fällen die so genannten Releasegroups, die illegale Kopien der Filme beschaffen, diese digitalisieren und für das Internet aufbereiten. Zu der Releasegroup-Szene ist auch die Ebene der sog. Affil-Server zu rechnen, Server im Internet, auf denen die Gruppen sich untereinander ihre Releases präsentieren. Aus der Releasegroup-Szene gelangen die Filmdateien in die FTP/FXP-Szene. Die ftp-Server der Zwischenszene sind dann die Quelle für all die Dateien, die in den Peer-to-Peer-Netzen auftauchen oder als gebrannte DVD- oder CD-Kopien auf Flohmärkten verkauft werden. Und selbst die professionellen Piraten auf den Grenzmärkten in Polen bzw. in Tschechien benutzen die von den Releasegroups stammenden Dateien als Master für die Produktion ihrer massenhaft vertriebenen, professionell aufgemachten Produkte.



Die aufgezeigte Struktur macht schon deutlich, dass das Phänomen der Releasegroups nicht plötzlich aufgetaucht ist, sondern seit langen Jahren existiert. Die ersten Gruppen stammen aus einer Zeit, als das Internet noch kein Massenmedium war und sich lediglich Spezialisten an den Universitäten mit dem Internet beschäftigten. In diesen Kreisen von Administratoren von Universitätsservern oder großen Firmenservern, die damit begannen, untereinander Programme auszutauschen und sich später ein Hobby daraus machten, wer am schnellsten den Kopierschutz eines Computerprogramms oder -spiels knacken konnte, entstand diese Szene. Es bildeten sich Gruppen, die untereinander einen Wettbewerb führten, wer kann als erster der Szene ein Softwareprogramm liefern, wer sind die fähigsten Cracker. Bald wurde der Wettbewerb auch auf Musik- und dann Filmdateien ausgedehnt. Diese Community existiert noch heute und bezeichnet sich selbst als so genannte ‚Old-

Schooler'. Sie verfolgen das Motto, alles aus der Szene für die Szene. Das Motiv für ihr Tun ist das Streben nach Anerkennung ihrer Fähigkeiten innerhalb ihrer Peer Group.

Innerhalb der Gruppen gibt es eine festlegte Struktur und Aufgabenteilung - so gibt es Spezialisten für die Bildbeschaffung, die Tonbeschaffung und das Muxen, das ‚Synchronisieren' von Bild und Ton. Über 80 Prozent dieser ersten Kopien sind Abfilmungen von der Kinoleinwand mit Digitalkameras, entsprechend unterschiedlich sind die Qualitäten dieser Raubkopien. Nach unserer Erfahrung gelingt es jedoch den Gruppen relativ schnell, qualitativ zufrieden stellende Raubkopien herzustellen. Die Releasegroups in Deutschland unterhalten mehr oder weniger ausgeprägte Beziehungen zu Gruppen in den USA, Russland und Fernost. Aufgrund dieser Kontakte erhält eine deutsche Release Gruppe die Genehmigung der US-Gruppe, deren illegales Bildmaterial für deutschsprachige Releases zu verwenden und die hiesige Gruppe muss sich nur noch den Synchronton beschaffen.

Alle Releasegruppen veröffentlichen zu ihren Releases so genannte nfo-Dateien. Dort werden neben Informationen zu Darstellern und Handlung des Films auch Angaben zur Qualität der Bild- und Tonquellen gemacht. Für die illegale Szene sind die nfo-Dateien besonders wichtig, denn aus Ihnen gehen die ‚Urheber' dieser illegalen Version hervor. Je häufiger ein Name dort auftaucht, desto mehr Anerkennung findet die Releasegroup und die daran beteiligten Personen in ihrer Peer Group.

Das Ziel jeder Releasegruppe ist es zunächst, bei der Veröffentlichung eines Release schneller zu sein als die Konkurrenzgruppen. Je öfter dies einer Gruppe gelingt, desto höher steht sie in der Hierarchieordnung der Szene. Es existiert so ein erheblicher Wettbewerb zwischen den Gruppen, der aber durch so genannte ‚Rules' (Regeln) geregelt ist. Sobald ein neuer Film im Kino läuft, beginnt eine Art Wettrennen, bei den Gruppen selbst als ‚Race' klassifiziert, welche Gruppe den Film als erste in bester Qualität illegal veröffentlicht. Wenn eine Gruppe nun als Erste eine bestimmte Qualität veröffentlicht hat, darf keine andere Gruppe ihr Produkt in derselben Qualität veröffentlichen. Tut sie es doch, wird ihr ‚Produkt' von den Admins der illegalen Server gelöscht (genuked), was eine erhebliche Schädigung des Ansehens der Gruppe in der Szene bedeutet.

Es ist für das Funktionieren der Szene und deren nationalem und internationalem Zusammenspiel sehr wichtig, dass neben der Affilserverszene, auf denen die Releasegroups ihre Releases der Szene präsentieren können, auch ein Informationssystem besteht, aus dem sie entnehmen können, ob bereits ein Release eines Kinofilmes von einer anderen Gruppe vorliegt. Zu diesem Zweck werden von den Gruppen bzw. verschiedenen Administratoren im Netz Internetseiten unterhalten, so genannte ‚Dupechecks', auf denen die illegalen ‚Veröffentlichungen' der Gruppen und deren nfo-Dateien laufend gelistet werden.

Mit dem rasanten Anstieg der Verfügbarkeit schneller leistungsstarker Internetverbindungen in den letzten drei bis vier Jahren drängen mit neuen Gruppen Personen in diese Releasegroup-Szene, die zwar auch der sportliche Ergeiz treibt, die aber eben auch finanzielle Interessen haben, so genannte ‚New-Schooler'. Der von den ‚Old-Schooler' Szenemit-

gliedern noch oft vertretene Szene-Grundsatz ‚Alles von der Szene, alles für die Szene!!' ist bei genauer Betrachtung nur noch die Beschreibung eines Wunschzustandes. Tatsächlich erscheint jedes Release einer Releasegruppe heute in enger zeitlicher Nähe zu seiner illegalen Veröffentlichung auf Servern im Internet. New-Schooler arbeiten in den Releasegroups unerkannt mit, geben aber dann das Material aus der Releasegroup-Szene weiter an Betreiber von ftp-Servern, so genannten Pay-Servern, die dann weiteren Personen Zugänge auf diese Server verkaufen. Ein solcher Pay-Server war beispielsweise die unter dem Namen ftp-welt bekannt gewordene Servergruppe. Über eine Homepage, die auf den British Virgin Islands registriert war, konnte man einen Zugang auf den ftp-Server kaufen, und von dort aktuelles Material wie Filme und Spiele herunterladen. Betrieben wurde dieser Server, wie sich später im Rahmen eines Strafverfahrens herausstellte, von zwei computertechnisch versierten 18 und 21 Jahre alten Brüdern, die nach Feststellungen der Polizei in ca. eineinhalb Jahren über eine Halbe Million Euro mit den Servern verdient haben sollen.

Wenn die illegalen Dateien aber auf den genannten Pay-Servern aufgetaucht sind, dauert es nur wenige Stunden, bis diese auch in den Peer-to-Peer-Netzen wie eDonkey oder BitTorrent zu finden sind. In diesen Netzen werden bekanntermaßen die Dateien kostenlos getauscht, und man fragt sich, wer verdient eigentlich Geld in diesen Systemen mit den Piraterieprodukten. Hier hat sich ein interessantes Phänomen entwickelt, die so genannten Hashlingsseiten bzw. Portalseiten.

Im Peer-to-Peer-System kursieren, wenn ein neuer Film in die Kinos kommt, oft viele verschiedene Dateien, die den Filmtitel in ihrem Dateinamen verwenden. Neben den Raubkopien des Films, die schon von sehr unterschiedlicher Qualität sein können, sind dies auch Fakes, Spiele oder auch Dateien mit pornografischem Inhalt. Es ist daher in der Regel sehr mühselig und zeitaufwendig, die wirklich guten Dateien eines gesuchten Films zu finden. Genau in diesem Bereich setzen die Portalseiten mit ihrem Service an. Die Betreiber dieser Seiten treffen eine Vorauswahl nach Funktionalität und guter Qualität und nach bestimmten Formaten. Nach Auswahl des gewünschten Films gelangt der Nutzer durch Anklicken eines Links direkt in das File-Sharing-System und kann die von ihm gesuchte Datei dann herunterladen. Aufgebaut werden diese Portalseiten, wie unsere Verfahren gezeigt haben, von Technik affinen Heranwachsenden, die stark in die Peer-to-Peer- und der FTP/FXP-Szene involviert sind. Finanziert werden diese Seiten durch Banner und Klick-Werbung. Wie lukrativ das sein kann, zeigte ein Verfahren aus dem Raum Münster, in dem einem Betreiber einer Portalseite nachgewiesen werden konnte, dass er innerhalb von vier Monaten durch Werbung ca. 18.000 Euro eingenommen hatte. Da wundert es wenig, dass inzwischen den eher amateurhaft arbeitenden Freaks Domainnamen wie ‚Saugstube' oder ‚Goldesel' von professionell arbeitenden Tätergruppen abgekauft wurden.

Wie ist nun die Strategie der Filmindustrie gegen das Problem der Piraterie? Schwerpunkt aller Aktivitäten ist derzeit insbesondere die Bekämpfung der aktuellen Filmpiraterie. Die Ergebnisse der Brennerstudie 2005 der FFA[1] (Filmförderungsanstalt, Berlin) zeigen den Umfang der Problematik:

- 1,7 Mio. Deutsche laden illegal Filme aus dem Internet und
- haben im ersten Halbjahr 2005 11,9 Mio. Filme herunter geladen.
- Nur 23 Prozent der Personen geben an, einen Download eines Films erst nach der Veröffentlichung der legalen DVD des Films getan zu haben.

Die Strategie der Filmindustrie steht derzeit auf drei Säulen:

1. Die Kampagne der ZKM ‚Raubkopierer sind Verbrecher', die die Aufmerksamkeit der Bevölkerung auf das Problem der Piraterie, insbesondere der Film-Piraterie lenken soll.
2. Ein Informationsangebot über Piraterie und deren Folgen auf der Internetseite *www.respectcopyrights.de*, auf der neben Informationen auch Unterrichtsmaterialien für Lehrer kostenlos angeboten werden.
3. und - das ist hier mein Schwerpunkt: Die aktive Bekämpfung der Piraterie durch die GVU – Gesellschaft zur Verfolgung von Urheberrechtsverletzungen e.V..

Bei der Bekämpfung konzentriert sich die GVU auf den Einsatz von strafrechtlichen Mitteln, da diese eine hohe spezial und generalpräventive Wirkung haben. Dies bedingt eine enge Zusammenarbeit mit den Strafverfolgungsbehörden. Die GVU ist bundesweit tätig und unterstützt die Behörden in allen produktbezogenen und rechtlichen Fragen der Filmpiraterie. Insofern wirkt die GVU als Puffer zwischen den Rechteinhabern und den Strafverfolgungsbehörden und versucht, das berechtigte Interesse der Mitglieder am Schutz der Filme und dem Strafverfolgungsinteresse der Behörden, welches Produkt unabhängig ist und die Straftat an sich zum Gegenstand hat, in Einklang zu bringen. Uns ist durchaus bewusst, dass die Zusammenarbeit zwischen Strafverfolgungsbehörden und einer Privatorganisation, die die Interessen von Verletzten wahrnimmt, eine sensible Nahtstelle darstellt. Aus diesem Grund verzichtet die GVU bewusst auf ein Mandat, zivilrechtliche Ansprüche gegen überführte Piraten geltend zu machen. Es gehört eben nicht zu unseren Aufgaben, für die einzelnen Rechteinhaber umfangreiche Schadenersatzansprüche zu generieren. Es ist schon außergewöhnlich, dass eine ganze Branche – weit über 80 Prozent aller relevanten Kinofilme werden von unseren Mitgliedern herausgebracht – sich zusam-

[1] Die Studie kann unter *http://www.filmfoerderungsanstalt.de/downloads/publikationen/brenner_studie4.pdf* angesehen werden.

menschließt, um unabhängig vom Einzelinteresse gemeinsam gegen das Pirateriephänomen vorzugehen.

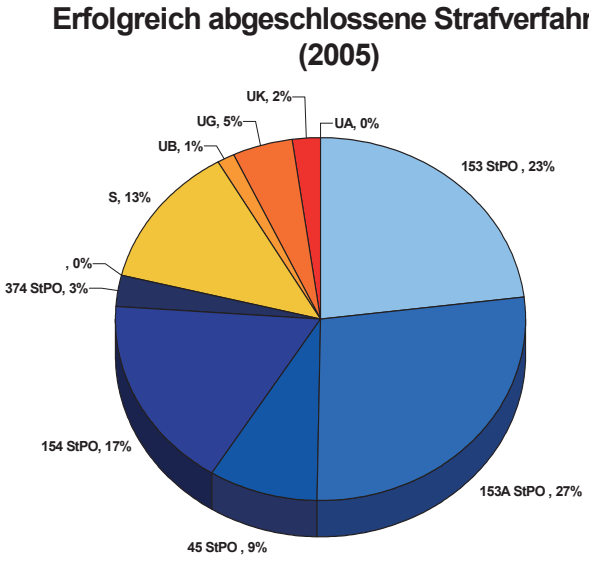
Die anfangs vorgestellte Pirateriepyramide macht deutlich, dass eine wirksame Bekämpfung der Piraterie durch die GVU an der Quelle des Übels, den Releasegroups, und den direkt nachgeordneten Verteilern ansetzen muss. Wenn wir verhindern können, dass aktuelle Filme später bzw. überhaupt ins Internet gelangen, dann bricht die gesamte Pirateriepyramide – jedenfalls was die Raubkopien von aktuellen Kinofilmen betrifft – zusammen. Diese Ermittlungen gestalten sich jedoch schwierig, da es sich - wie zuvor geschildert - um eine geschlossene, sehr spezielle Szene handelt, in die ein Eindringen ohne szenezugehörigen Informanten kaum möglich ist. Insbesondere greifen übliche Ermittlungsansätze bei Wirtschaftskriminalität, wie z.B. die Verfolgung von Finanzbewegungen, nicht, da diese Gruppen überwiegend nicht aus finanziellen Motiven handeln. Zudem sind die Ermittlungsmöglichkeiten einer privaten Organisation sehr begrenzt und enden mangels eines zivilrechtlichen Auskunftsanspruchs gegen Zugangsprovider schon bei dem Versuch, den Nutzer einer dynamischen IP-Adresse zu identifizieren. Wir sind daher auf die enge Kooperation mit den Strafverfolgungsbehörden angewiesen, die allein substanzielle Ermittlungen mit den von der StPO gewährten Mitteln durchführen können. Wir unterstützen die Ermittlungen, indem wir die Aktivitäten der einzelnen Releasegroups dokumentieren und versuchen, Informanten aus der Szene zu gewinnen. Weiterhin werten wir Filmdownloads nach Ton- und Bildkodierungen aus, um so gezielte Quellenermittlung zu ermöglichen, und bringen sich überschneidende Ermittlungen verschiedener Dienstellen zusammen bzw. sorgen für einen notwendigen Informationsaustausch (deshalb scherzhaft genannt das BKA der Filmpiraterie). Wir übernehmen die oft sehr arbeitsintensive Auswertung sichergestellter Asservate und sorgen für die notwendigen Strafanträge der verletzten Rechteinhaber. Gerade die Dienststellen, die im Internet sachgerechte Ermittlungen durchführen können, aber oft mit Verfahren wegen Kinderpornografie und ähnlichen Delikten stark belastet sind, stehen unserer Tätigkeit positiv gegenüber, auch, weil wir sie gerade nicht mit Mengen von ungefilterten Hinweisen oder mit automatisiert generierten Massenverfahren überschütten.

Ein weiter Schwerpunkt unserer Tätigkeit ist das Vorgehen gegen die professionellen Verteiler, die eigentlichen Wirtschaftskriminellen, die entweder Unterstützungsleistungen, wie Portalseiten ins Web bringen oder gewerbsmäßig Vervielfältigungen anfertigen und auf Flohmärkten oder auf den Grenzmärkten in Polen und Tschechien verkaufen. Gerade bei dieser Aufgabe bewährt es sich, dass die GVU in das internationale Netzwerk von Antipirateriеorganisationen eingebunden ist. Allein im EMEA-Raum haben wir 38 Partnerorganisationen, und diese Kontakte sind gerade bei grenzüberschreitender Piraterie von unschätzbarem Wert.

Im Bereich der so genannten Massenpiraterie oder Enduserpiraterie entfaltet die GVU dagegen keine Ermittlungstätigkeit. Grundsätzlich sind hierfür die anderen Säulen der Antipirateriеaktivitäten der Filmindustrie zuständig. Trotzdem gilt für uns das so genannte

Zero-Toleranz-Prinzip. Dies bedeutet, dass wir in jedem Fall, in dem die Strafverfolgungsbehörden ein Verfahren wegen Urheberrechtsverletzungen eingeleitet haben, diese bei der Bearbeitung des Falles unterstützen.

Wir stellen grundsätzlich, auch in kleinen Fällen einfacher Delinquenz, Strafanträge, weil wir es für wichtig erachten, dass jedem erwischten Täter deutlich gemacht wird, dass er etwas Unrechtes getan hat und die Verletzung geistigen Eigentums kein Kavaliersdelikt ist. Dieses konsequente Handeln ist erforderlich, um ein Unrechtsbewusstsein nicht nur beim Täter, sondern auch in seinem Umfeld zu erreichen. Um es an einem einfachen Beispiel deutlich zu machen: Wenn ein Jugendlicher, der von der Polizei beim Downloaden oder beim Tauschen von Filmdateien erwischt wurde, in die Schule zurückkommt und sagt: ‚Die Staatsanwaltschaft hat das Verfahren zwar eingestellt, aber wenn ich das nächste Mal erwischt werden, bekomme ich eine Strafe', wird dies auf ihn und sein Umfeld mehr Wirkung erzielen, als wenn er sagen kann: ‚war alles halb so schlimm, ich hab alles wiederbekommen, für die Sache hat sich keiner interessiert'. Daher auch unser Appell an die Bundesregierung, auf die Einführung einer Bagatellklausel zu verzichten. Diese führt lediglich dazu, die Grenzen zwischen legalem und illegalem Handeln noch weiter zu verwischen, als es durch die unnötig komplizierten Regelungen zum privaten Gebrauch bereits jetzt der Fall ist. Schon heute sind nur Handlungen strafrechtlich relevant, die aus dem Anwendungsbereich Privatkopierschranke des § 53 Abs. 1 UrhG herausfallen, d.h. nur der Nutzer, für den offensichtlich ist, dass er aus einer rechtswidrigen Quelle kopiert, macht sich nach § 106 UrhG strafbar. Hier ist überhaupt kein Raum, diesen Bereich – auch wenn es sich nur um einfache Kriminalität handelt - noch weiter zu entkriminalisieren. Und ob es in diesen einfachen Fällen überhaupt zu einer strafrechtlichen Verurteilung kommt, ist ohnehin eine andere Frage. Gerade für diese kleineren Fälle bietet die StPO mit den §§ 153 ff. und das JGG in § 45 den Strafverfolgungsbehörden einen ausreichenden Ermessensspielraum, Strafverfahren wegen geringer Schuld oder Geringfügigkeit einzustellen. Dass die Behörden hiervon auch regen Gebrauch machen, spiegelt sich in der Statistik der Abschlüsse der Strafverfahren, an denen die GVU beteiligt war, wider. Wie aus der Grafik zu ersehen, werden die meisten Verfahren -



und dies gilt insbesondere für Verfahren gegen Ersttäter - von den Staatsanwaltschaften mit Auflagen, Bußen und Einziehung der Raubkopien eingestellt. Gegen Wiederholungstäter, Portalseitenbetreiber und Täter, denen eine Mitgliedschaft in einer Releasegroup nachgewiesen werden konnte, werden dagegen zunehmend deutlich höhere Strafen verhängt.

Digitale Mentalität

Hergen Wöbken & Manuel Dolderer

1 Einleitung – Raubkopieren und Digitale Mentalität

Das Kopieren und Verbreiten von digitalen Inhalten aller Art ist durch das Internet zu einem Teil unseres Alltags geworden. Das betrifft auch das nicht lizenzierte Kopieren von digitalen Inhalten, das unter dem Stichwort ‚Raubkopieren' zu einem weltweiten Phänomen geworden ist. In der öffentlichen Meinungsbildung scheint die Tatsache keine große Rolle zu spielen, dass das unerlaubte Kopieren und Nutzen urheberrechtlich geschützter Inhalte, beispielsweise der Einsatz von nicht ordnungsgemäß lizenzierter Software, eine Ordnungswidrigkeit ist – im schlimmsten Fall sogar eine Straftat, wie es durch die nicht ganz treffende Bezeichnung Raubkopieren[1] unterstrichen wird. Wir befinden uns in einer Situation, in der sich ein erheblicher Teil unserer Gesellschaft wissentlich oder unwissentlich über geltendes Recht hinwegsetzt, ohne dass sich dieses Verhalten auf bestimmte Gruppen innerhalb der Gesellschaft einschränken ließe. Gleichzeitig entsteht dabei nach Aussage verschiedener Studien Jahr für Jahr ein beträchtlicher wirtschaftlicher Schaden.

Auch die Softwareindustrie sieht sich herausgefordert, in der Öffentlichkeit ein Bewusstsein für diesen Schaden, der durch das Phänomen ‚Raubkopieren' entsteht, zu schaffen. Soll die momentane Raubkopierrate verringert werden, kommen neben dem Rückgriff auf drastische Drohgebärden, wie sie zurzeit von der Film- und Musikindustrie in Stellung gebracht werden[2], auch noch Alternativen in Frage. Ein erster Schritt auf dem Weg zu diesen Alternativen ist eine grundlegende Beschreibung des Phänomens und seiner konkreten Erscheinungsformen. Auf dieser Grundlage können weitere Überlegungen hinsichtlich eines konstruktiven Umgangs mit dem Phänomen ‚Raubkopieren' aufgebaut werden. In einer Studie (Institut für Strategieentwicklung 2004) haben wir Computernutzer im Hinblick auf den Einsatz von nicht ordnungsgemäß lizenzierter Software im privaten oder gewerblichen Bereich untersucht. Der gewerbliche Vertrieb von Raubkopien – eine Erscheinungsform organisierter Kriminalität – wurde dabei ausgeklammert.

Das Phänomen ‚Raubkopieren', verstanden als Verstoß gegen geltendes Recht, müsste eigentlich die Ausnahme und dürfte nicht die Regel sein, wie wir sie erleben. Tatsächlich aber können wir beobachten, dass Raubkopieren für viele Menschen zum alltäglichen Le-

[1] Die Silbe ‚Raub' wird gewöhnlich verwendet, wenn Gewalt eine Rolle spielt, wie etwa bei einem ‚Raubüberfall'

[2] Siehe nur die Kampagne ‚Hart aber gerecht': *www.hartabergerecht.de*

ben gehört. Mit der Studie lässt sich das Phänomen des Raubkopierens im Hinblick auf die Mentalität beschreiben, die damit verbunden ist. Mentalität meint dabei die Denkmuster innerhalb einer Gruppe von Menschen, die das Verhältnis zur Wirklichkeit und das kollektive Verhalten bestimmen.

2 Executive Summary

Die Befunde der Studie sind das Ergebnis einer theoretischen Analyse[3], die empirische Daten aus Recherchen, Experteninterviews und einer Online-Umfrage einbezogen hat. Die wichtigsten Ergebnisse und Zusammenhänge werden im Folgenden dargestellt.

Das Handeln folgt nicht dem Bewusstsein

Es gibt ein verbreitetes Wissen um die Tatsache, dass Raubkopieren eine Straftat ist, die wirtschaftlichen Schaden verursacht. Dieses Wissen hat jedoch nur geringen Einfluss auf das tatsächliche Raubkopierverhalten. Im Falle der Urheberrechtsverletzung, die durch digitale Vervielfältigung begangen wird, bleibt ein intuitives Verständnis für das damit verbundene Unrecht aus, weil das Tatbestandsmerkmal der Wegnahme fehlt, das unseren historisch gewachsenen Vorstellungen von Diebstahl zugrunde liegt.

Das Bindeglied zwischen einem vorhandenen Wissen um die Unrechtmäßigkeit einer Verhaltensweise und dem tatsächlichen Verhalten des Verbrauchers ist eine Nachvollziehbarkeit im Sinne eines intuitiven Rechtsverständnisses. Erst wenn sich eine rechtliche Regelung dem intuitiven Rechtsverständnis des Einzelnen erschließt und damit für ihn nachvollziehbar wird, richtet er auch sein Handeln danach. Fehlt diese Nachvollziehbarkeit, bleibt nur noch die glaubwürdige Androhung von Sanktionen, um das gewünschte Verhalten zu erzielen.

Raubkopierer lassen sich unterscheiden

Da sich die Gesamtheit der Raubkopierer nicht auf einen Nenner bringen lässt, erlaubt die Aufteilung in Gruppen eine Beschreibung spezifischer Verhaltensweisen und Denkmuster. Die Gruppe der ‚PC-Freaks' zeichnet sich durch eine hohe Computer-Expertise sowie durch eine hohe Raubkopierintensität aus. Die ‚Hobby-User' zeichnen sich durch eine weniger leidenschaftliche Beziehung zu ihrem PC aus, ähneln allerdings im Raubkopierverhalten den PC-Freaks. Die ‚Pragmatiker' setzen den Computer schlicht als Arbeitsgerät ein, Raubkopien werden in vergleichsweise geringem Maße eingesetzt. Die ‚PC-Profis'

[3] Im Sinne von Gerhard Schulze, Die Erlebnis-Gesellschaft: Kultursoziologie der Gegenwart, 8. Auflage Frankfurt am Main 2000, S. 25 ff.

stellen die vierte Gruppe der identifizierten digitalen Typen dar. Sie nutzen ihren PC in einem professionellen Zusammenhang und setzen dabei legal erworbene Software ein.

In der Online-Umfrage konnte ein bedeutender Unterschied festgestellt werden, wenn es darum ging, Raubkopieren als Straftat einzuschätzen. Die Nutzung von Raubkopien im privaten Umfeld wird zwar als Straftat erkannt, allerdings distanziert sich die Mehrheit der Umfrageteilnehmer in ihrer subjektiven Einschätzung von dieser juristischen Bewertung. Im Gegensatz dazu wird die Nutzung von Raubkopien in Unternehmen von der Mehrheit der Befragten nicht nur als Straftat erkannt, sondern auch – in Übereinstimmung mit der juristischen Bewertung – aus der persönlichen Einschätzung heraus als solche bewertet.

Die Zahl der ideologisch motivierten Raubkopierer, die Raubkopieren bspw. als wirtschaftlichen Boykott der Preispolitik von Softwaremonopolisten legitimieren, ist denkbar gering und reicht nicht aus, um als abgrenzbare Gruppe innerhalb der Masse der Raubkopierer erfasst zu werden.

Allgemeine Forderung nach Investitionsschutz

Als gemeinsamer Nenner der verschiedenen Positionen lässt sich festhalten, dass zumindest eine grundlegende Form von Investitionsschutz als notwendig erachtet wird, die sicherstellt, dass Investitionen in die Entwicklung von Software auch weiterhin von kommerziellen Unternehmen getätigt werden. Dazu bedarf es einer realistischen Möglichkeit, angemessene finanzielle Rückflüsse zu erzielen.

Durchsetzung und Sicherung von Verfügungsrechten

Es ist ein fehlender Zusammenhang zwischen Raubkopierverhalten und Rechtsbewusstsein zu beobachten, der für die folgenden Ausführungen eine große Rolle spielen wird. Diesen fehlenden Zusammenhang in Rechnung gestellt, ist Raubkopieren aus unternehmerischer Perspektive nur vordergründig ein Urheberrechtsproblem. Ein Diskurs über die Rechtslage verschiebt das Problem zu neuen Fragestellungen, löst es aber nicht. In Bezug auf die Softwareindustrie handelt es sich tatsächlich um das Problem der Durchsetzung und Sicherung von Verfügungsrechten. Gelingt diese Durchsetzung trotz der entsprechenden Rechtslage nicht, kann es aus Sicht der Softwareindustrie dennoch keine Verhaltensoption sein, Raubkopieren als unangenehmes Phänomen zu dulden.

Digitales Selbstverständnis muss wachsen

Vielmehr sollte die Softwareindustrie im Unterschied zur Filmindustrie ihren Umgang mit dem Problem und ihre Positionierung dazu im Rahmen einer Digital Honesty aktiv gestalten und Raubkopierer als potenzielle Kundengruppe wahrnehmen. Hierfür gilt es, eine differenzierte Kommunikation zu entwickeln, die sich an der Unterteilung der vorher anonymen Masse der Raubkopierer in die Gruppen der ‚PC-Freaks', der ‚Hobby-User', der ‚Pragmatiker' und der ‚PC-Profis' orientiert und auf den jeweiligen Verhaltensweisen und Denkmustern der einzelnen Gruppen aufbaut.

3 Die rechtliche, technische und wirtschaftliche Dimension

3.1 Das Urheberrecht

Durch das Urheberrecht erhält ein Urheber das Recht, über die Nutzung seines Werks zu verfügen. Das heißt, er kann bestimmen, ob und in welcher Form sein Werk vervielfältigt, veröffentlicht oder verbreitet wird und ggf. die jeweiligen vertraglichen Bedingungen hierfür in weitem Umfang festlegen.

Entstehung des Urheberrechts

Bis zum Mittelalter kannte man ein Recht am geistigen Werk als solches noch nicht. Erst im Zeitalter der Aufklärung setzte sich ein Menschenbild durch, das sich durch Individualität und damit einzelne unveräußerliche Persönlichkeitsrechte auszeichnete. Zu diesen Persönlichkeitsrechten zählte auch der Schutz eigener Schöpfungen. Bereits 1857 wurde in Preußen ein allgemeiner Urheberrechtsschutz eingeführt. Um urheberrechtlichen Schutz über den Hoheitsbereich eines einzelnen Staates hinaus zu gewährleisten, wurden in der Folgezeit auch internationale Vereinbarungen getroffen.

Im Jahr 1967 wurden alle bis dahin existierenden Übereinkommen unter dem Dach der Vereinten Nationen (UNO) in die Weltorganisation für geistiges Eigentum (World Intellectual Property Organization, WIPO) eingebracht. Heute haben einzelne Staaten nur noch geringe Spielräume in der Ausgestaltung des Urheberrechts. Den größten Spielraum haben unter den gegebenen Verhältnissen die USA, die mit dem Digital Millennium Copyright Act (DMCA) die Grundrichtung hin zu strengerem Urheberrechtsschutz vorgegeben haben. In Europa setzen EU-Richtlinien den Rahmen, der durch nationales Recht ausgefüllt werden kann.

3.2 Technische Entwicklung – Digitale Kopien

Spätestens mit der Verbreitung des Kassettenrekorders in den 60er und 70er Jahren des 20. Jahrhunderts erschloss der technische Fortschritt dem Einzelnen Möglichkeiten, analoge Kopien von urheberrechtlich geschützten Inhalten anzufertigen. Damals weigerte sich die Politik, den Grundsatz von der Unverletzlichkeit der Wohnung zugunsten einer effektiven Verfolgung der damit möglich gewordenen Urheberrechtsverletzungen preiszugeben. Stattdessen wurde auf die technischen Geräte und Leermedien, die diese Form der Urheberrechtsverletzung ermöglichten, eine Abgabe erhoben, die über Verwertungsgesellschaften den potenziell geschädigten Urhebern zufloss.

Eine analoge Kopie führt zu einem zumindest geringen Qualitätsverlust, wodurch die Reproduzierbarkeit von Analogkopien ihre natürlichen Grenzen hat – im Unterschied zu einer digitalen Kopie, die ein exaktes Abbild des Originals ist und beliebig ohne Qualitätsverlust vervielfältigt werden kann.

Das Computerzeitalter

Der Computer lieferte die technischen Möglichkeiten, verlustfreie Digitalkopien von urheberrechtlich geschützten Originalen herzustellen, und jede Digitalkopie konnte ihrerseits wieder als Vorlage für eine weitere verlustfreie Kopie dienen. Am Prinzip der Abgabe auf die entsprechenden technischen Geräte und der Verteilung der Gelder an potentiell geschädigte Urheber änderte sich jedoch nichts – was gleichbedeutend war mit der fortgesetzten Duldung der Privatkopie, also der Kopie urheberrechtlich geschützter Inhalte für den privaten Gebrauch.

Mit dem Einzug des Computers in Büros und Haushalte verbreiteten sich auch die verschiedensten Arten von Software und wurden ein begehrtes Ziel von Raubkopierern. Allerdings gab es – im Unterschied zu Musik, Film und anderen urheberrechtlich geschützten Inhalten – bei Software keine der ‚Privatkopie' vergleichbare Regelung. Von Anfang an gab es nur das Recht des Käufers, eine Sicherheitskopie des erworbenen Datenträgers anzufertigen. Keinesfalls durften mehrere Kopien im Familien- und Freundeskreis verteilt werden. Diese Differenzierung ist für manche Verbraucher schwer nachzuvollziehen, da sie, etwa beim Kauf eines CD-Brenners, eine Abgabe bezahlen, die sie mit Einschränkung zur Erstellung von Kopien für den privaten Gebrauch berechtigt. Der für die Rechtmäßigkeit dieser Kopien fundamentale Unterschied zwischen einer Musik- und einer Software-CD, nämlich das im Fall der Software nicht vorhandene Zugeständnis der Privatkopie, wird dabei oftmals vernachlässigt.

Das Internetzeitalter

Um eine weitere Dimension ergänzt wurden die technischen Möglichkeiten des Computers durch das Internet. Damit war ein Medium geschaffen, das quer durch alle gesellschaftlichen Schichten eine neue Kommunikationsform etablierte. Plötzlich standen urheberrechtlich geschützte Inhalte überall auf der Welt und rund um die Uhr zum Kopieren zur Verfügung.

Wichtiger Bestandteil dieser Entwicklung war eine reizvolle Kombination aus Gemeinschaft und Anonymität. Diese Anonymität, verbunden mit der Möglichkeit, verlustfrei Kopien von jeder Form digitaler Inhalte zu machen, schuf die Grundlage dafür, dass wir das Phänomen Raubkopieren in seiner heutigen Dimension beobachten können.

3.3 Die wirtschaftlichen Folgen

Der wirtschaftliche Schaden, entstanden allein durch den Einsatz unlizenzierter Software in Unternehmen, belief sich nach einer Studie des Marktforschungsinstituts International Data Corporation (IDC) im Auftrag der Business Software Alliance (BSA) im Jahr 2005

in Deutschland auf 1,54 Milliarden Euro an Umsatzeinbußen[4]. Tatsächlich ist es verwunderlich, dass diese enormen wirtschaftlichen Verluste einer ganzen Branche in der Wahrnehmung des Verbrauchers eine untergeordnete Rolle zu spielen scheinen.

Zwar sind die Kosten der digitalen Vervielfältigung und Distribution von Software im Vergleich zu herkömmlichen Industrien verschwindend gering, dafür fallen bei der Produktion von Software sehr hohe fixe Kosten für Forschung, Entwicklung und Programmierung an. Aus Sicht eines Softwareunternehmens kann es daher keine Verhaltensoption sein, Raubkopieren als unangenehmes, aber ökonomisch nicht weiter relevantes Phänomen zu dulden. Die Softwareindustrie ist darauf angewiesen, ihre hohen Investitionskosten durch hohe Verkaufsvolumina zu refinanzieren. Jeder scheinbar noch so marginale Einbruch gefährdet das zugrunde liegende Geschäftsmodell und damit längerfristig auch die Geschäftsgrundlage, wenn auch nicht unbedingt die kurzfristige Gewinnlage.

Digitale Mauern

Dabei geht es in diesem Zusammenhang neben der gesellschaftlichen Akzeptanz von Urheberrechten vor allem um den Schutz von Eigentum. Eigentum setzt die Möglichkeit voraus, andere wirkungsvoll vom Zugang dazu auszuschließen. Zu diesem Zweck werden in der nicht-digitalen Welt Zäune gezogen, Mauern gebaut, Tresore aufgestellt und Alarmanlagen installiert. Dort, wo die Softwareindustrie nicht mehr in der Lage ist, diesen Zugang zu limitieren und nur gegen Zahlung zu gestatten, versagt das Geschäftsmodell. Um dieser prinzipiellen Gefährdung des Geschäftsmodells zu begegnen, können im Softwarebereich zwar keine Mauern gebaut, aber ähnlich wirkungsvolle Schutzmechanismen in Form eines Digital Rights Managements etabliert werden.

Bei vielen Softwareprodukten hat sich die Produktaktivierung bewährt, nicht, weil damit kein Missbrauch mehr möglich wäre, sondern weil das Prinzip der Limitierung des Zugangs erfolgreich etabliert wird. Dadurch wird auch das Geschäftsmodell gesichert. Dass auch mit solchen technischen Schutzmaßnahmen nicht jede Form von Raubkopieren verhindert werden kann, wird in den nun folgenden Betrachtungen zu den verschiedenen Gruppen von Raubkopierern und ihren Motiven deutlich.

4 Analyse – Die Raubkopierer und ihre Motive

Der allgemeine Begriff Raubkopierer steht für verschiedene, höchst unterschiedliche Gruppen von raubkopierenden Computernutzern. Die Unterscheidung dieser Typen von Raubkopierern erfolgt nach den Motiven für ihr Verhalten. Dabei wurde die Motivation

[4] *http://www.bsa.org/germany/presse/newsreleases/upload/IDC-Pirateriestudie-2005.pdf*

für professionelle und gewerbliche Vervielfältigung oder Manipulation (gewerbliche Softwarepiraterie) nicht untersucht.

Um festzustellen, welche Gruppen sich anhand welcher Merkmale tatsächlich stichhaltig definieren lassen, welches die grundlegenden Motive für das Raubkopierverhalten der einzelnen Gruppen sind, wie groß die Gruppen sind und wie sie untereinander zusammenhängen, haben wir mit Hilfe eines detaillierten Fragebogens eine Online-Umfrage durchgeführt, deren Details im Folgenden erläutert werden.

Ergebnisse der Online-Umfrage

Die Ergebnisse der Online-Umfrage zum Thema ‚Digitale Mentalität' basieren auf 126 ausgewerteten Fragebögen von Computernutzern mit Internetzugang (32 Prozent Frauen, 68 Prozent Männer). Die Einladungen zur Umfrage erfolgten per E-Mail an Personen innerhalb Deutschlands. Die Umfrage fand zwischen dem 12. und 25. April 2004 statt.

Die Befragten waren zum Zeitpunkt der Umfrage zwischen 18 und 70 Jahre alt (arithmetisches Mittel = 31,03, Standardabweichung = 9,92). Die Mehrheit besitzt Abitur oder Fachhochschulreife (insgesamt 91 Prozent). Die zwei am stärksten vertretenen Berufsgruppen sind Studierende (34 Prozent) und Angestellte (35 Prozent). Über die Hälfte der Umfrageteilnehmer sind in Unternehmen beschäftigt (62 Prozent). Der in Unternehmen beschäftigte Teil arbeitet überwiegend in Unternehmen mit bis zu 2.000 Mitarbeitern (85 Prozent). Von den Befragten nutzt eine Mehrheit von 84 Prozent Microsoft Windows als einziges Betriebssystem auf dem privaten Computer. MacOS von Apple nutzt eine Minderheit (10 Prozent). Die verbleibenden 6 Prozent betreiben Microsoft Windows parallel zu Linux (4 Prozent) oder Apple MacOS (2 Prozent).

Zum Vergleich[5]: Im Jahr 2005 waren 75 Prozent der Bevölkerung zwischen 14 und 49 Jahren in Deutschland online. Die Frage, wer derzeit das Internet in Deutschland nutzt, ist eng mit den soziodemographischen Faktoren wie Alter, Bildung und Einkommen verknüpft. Durchweg sind Internetnutzer eher jünger, haben einen höheren Bildungsabschluss und leben in Haushalten mit vergleichsweise hohem Einkommen.

Die Ergebnisse der Online-Befragung zeichnen sich sowohl durch eine hohe Übereinstimmungs- und Vorhersagevalidität als auch eine hohe Reliabilität (Split-half-Reliabilität) aus.

[5] (N)Onliner Atlas 2005, TNS Infratest

Die Strafwürdigkeit von kommerzieller und privater Nutzung von Raubkopien

Eine Mehrheit von 86 Prozent der Befragten stimmte zu, dass der Verkauf von Raubkopien bestraft werden sollte. Die Nutzung nicht lizenzierter Software in Unternehmen wurde ebenfalls als Straftat gesehen: 95 Prozent der Befragten sprachen sich für eine Bestrafung der kommerziellen Nutzung von Raubkopien aus. Im Gegensatz dazu befürworteten bei der privaten Nutzung von Raubkopien nur 22 Prozent der Teilnehmer eine Bestrafung, wohingegen 78 Prozent einer Bestrafung der privaten Nutzung ablehnend gegenüberstanden (siehe auch folgende Abbildungen).

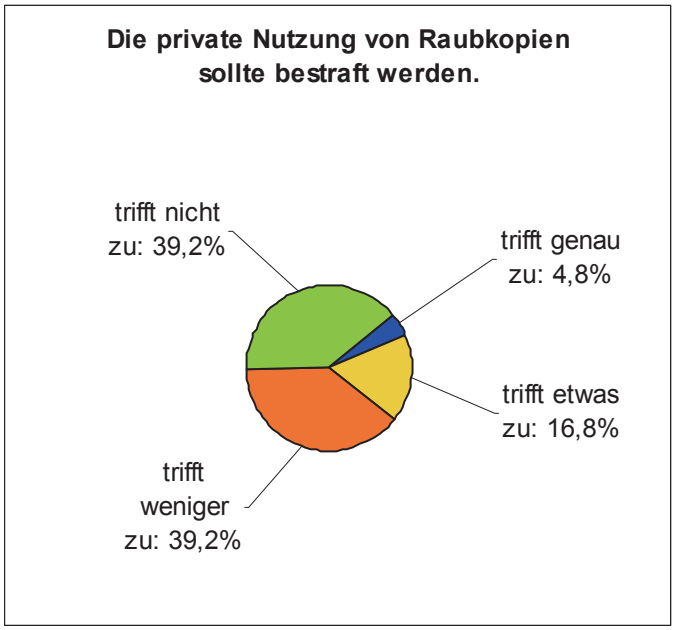


Abb. Institut für Strategieentwicklung: Online-Umfrage – Die private Nutzung von Raubkopien sollte bestraft werden

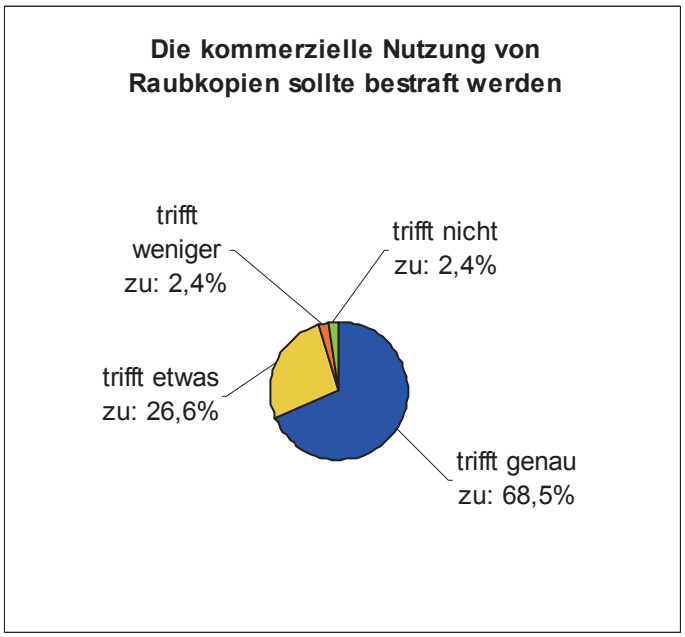


Abb. Institut für Strategieentwicklung: Online-Umfrage – Die kommerzielle Nutzung von Raubkopien sollte bestraft werden

Aus diesen Ergebnissen lässt sich schließen, dass das Rechtsempfinden bei Softwarenutzern bezüglich des Einsatzes von Raubkopien im kommerziellen Bereich mit geltendem Recht weitgehend übereinstimmt. Setzt man dagegen privates Raubkopieren in Bezug zu anderen illegalen Handlungen, ergibt sich ein differenzierteres Bild.

Einschätzung des Raubkopierens im Vergleich zu anderen Straftaten

Privates Raubkopieren wurde von 66 Prozent der Teilnehmer als weniger gravierend als Ladendiebstahl empfunden. Immerhin 30 Prozent beurteilten es als ebenso gravierend und etwa 3 Prozent stuften Raubkopien als gravierender als Ladendiebstahl ein. Gründe für diese Einschätzung wurden in qualitativen Interviews geäußert: Sie liegen vor allem in der Anonymität des Raubkopierens sowie in der Tatsache, dass beim Raubkopieren der Geschädigte nicht ins Bewusstsein tritt. Die Umfrage unterstützt auch die Vermutung, dass beim privaten Einsatz von Raubkopien – anders als beim Ladendiebstahl – keine Strafverfolgung befürchtet wird. 60 Prozent der Nutzer von Raubkopien hatten keine Sorge, erwischt zu werden.

Im Vergleich zu anderen Straftaten wird das Raubkopieren von Software am ehesten in die Nähe von illegalen Downloads von MP3-Dateien und dem Kopieren von Film-DVDs gestellt. Jeweils 64 resp. 52 Prozent stuften diese Straftaten als ebenso gravierend ein wie Raubkopieren. 15 resp. 18 Prozent hielten Raubkopieren für gravierender und 15 Prozent der Befragten hielten Raubkopieren für weniger gravierend, als MP3-Dateien aus dem Internet herunter zu laden oder Film-DVDs illegal zu kopieren.

Deutlich anders wurden Software-Raubkopien in Bezug zum Kopieren von Musik-CDs für Freunde gesetzt. 24 Prozent hielten das Kopieren von Software für gravierender als das Kopieren von Musik-CDs für Freunde. Für 42 Prozent war es ebenso schwerwiegend und 19 Prozent hielten Raubkopieren für weniger gravierend.

Eine Mehrheit von 74 Prozent der Teilnehmer stimmte der Annahme zu, dass jede Raubkopie den Softwarehersteller finanziell schädigt. 60 Prozent waren sich darüber im Klaren, dass mit Raubkopien Schäden verursacht werden, auch wenn keine physische Enteignung des Rechteeigentümers der Software vorliegt.

Zusammenfassung der Ergebnisse

Fasst man diese Ergebnisse zusammen, so lässt sich in der untersuchten Gruppe ein sowohl stark ausgeprägtes als auch differenziertes Rechtsempfinden in Bezug auf das Raubkopieren festhalten. Eine erkennbare Anzahl ideologisch motivierter Raubkopierer, die Raubkopieren beispielsweise als wirtschaftlichen Boykott der Preispolitik von Softwaremonopolisten betrachten, ist nicht auszumachen. Dies spiegelt sich auch in der Tatsache wider, dass weniger als 2 Prozent der befragten Teilnehmer der Ansicht waren, Software sei ebenso wie Information ein freies Gut, über das niemand eigentumsrechtlich verfügen können sollte. Stattdessen stimmten 45 Prozent der Teilnehmer zu, dass dem Software-

entwickler sämtliche Rechte an der Software zustehen sollten. 53 Prozent waren der Auffassung, Softwareentwickler sollten im Rahmen einer zeitlichen Befristung angemessen für ihre Arbeit entlohnt werden.

Unabhängig von dem differenzierten Rechtsbewusstsein lässt sich ein weit reichender Einsatz von Raubkopien feststellen. Bei 29 Prozent der Befragten bestand ein Großteil oder sogar der Gesamtbestand der genutzten Software aus Raubkopien, und 37 Prozent hatten zumindest einen kleinen Teil Raubkopien im Einsatz. 25 Prozent der Befragten sagten aus, dass sie keine Raubkopien nutzten. Immerhin 10 Prozent der Befragten wussten selbst nicht, ob sie Raubkopien auf ihrem Computer haben. Das bedeutet, dass zwei Drittel aller Umfrageteilnehmer in bedeutsamem Maße Raubkopien einsetzen, obwohl sie in anderen Punkten der Umfrage unmissverständlich deutlich gemacht haben, dass ihnen die Illegalität ihres Verhaltens bewusst ist.

Zur Methodik der Identifizierung digitaler Typen

Zur Untersuchung der unterschiedlichen Ausprägungen einer Digitalen Mentalität bei verschiedenen Software-Nutzergruppen mussten diese Nutzergruppen zunächst einmal voneinander unterschieden werden. Als Unterscheidungskriterien boten sich zwei Größen an: zum einen die Beurteilungen der individuellen Computer-Expertise, die Kenntnisse, Auseinandersetzungen und Begeisterung für das Medium Computer beschreibt, und zum anderen die Raubkopierintensität im Privatbereich, die Besitz und Verbreitung von Raubkopien zusammenfasst. Diese beiden voneinander unabhängigen Größen ergaben – in Kombination miteinander – geeignete Schnitte durch die Stichprobe. Generiert wurden beide Dimensionen aus einer Verdichtung von ausgewählten Variablen des Fragebogens, die untereinander eine hohe Korrelation aufwiesen und als stark prägend für die entsprechende Dimension identifiziert werden konnten.

Bildet man die beiden Dimensionen auf einer Matrix ab, lassen sich überschneidungsfrei vier unterschiedliche digitale Typen identifizieren.

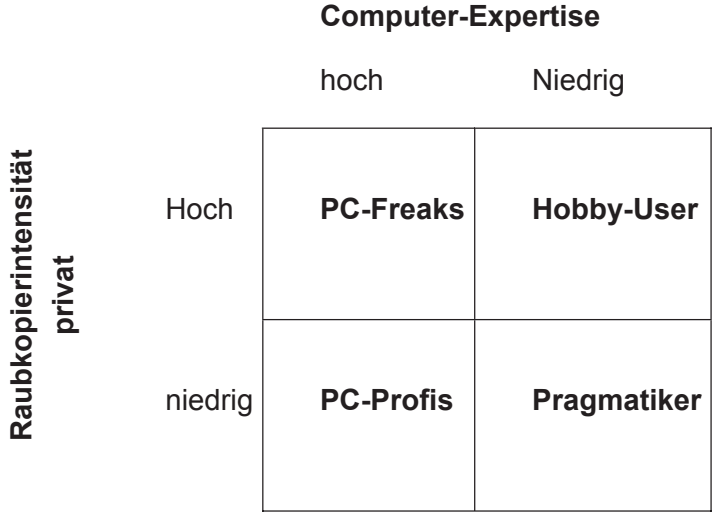


Abb. Institut für Strategieentwicklung:
Vier-Felder-Matrix der digitalen Typen

Im Folgenden sollen diese vier Software-Nutzergruppen kurz charakterisiert werden.

PC-Freaks zeichnen sich durch eine hohe Computer-Expertise sowie durch eine hohe Raubkopierintensität aus. PC-Freaks sind leidenschaftliche Computernutzer, die einen Großteil ihrer Freizeit mit Computern verbringen. Über die Jahre haben sie sich ein großes Computerwissen angeeignet und nutzen dieses, um ihr System stets in optimalem Zustand zu halten. In Bezug auf das Raubkopierverhalten können die PC-Freaks als echte ‚Jäger und Sammler' gelten, die sich sämtliche Software besorgen, die sie irgendwann einmal gebrauchen könnten. Aus diesem Grund fungieren sie als bedeutende Knoten im Tauschnetzwerk für Raubkopien. Familienmitglieder, Freunde und Bekannte werden von ihnen mit Software-Raubkopien versorgt. Der typische PC-Freak ist männlich, unter 25 Jahre alt und beschreibt sich selbst als äußerst technikbegeistert.

Hobby-User sind in gewisser Weise die kleinen Geschwister der PC-Freaks. Auch wenn sie altersmäßig über den Freaks (um die 29 Jahre) liegen, ist doch ihr Computerwissen deutlich weniger ausgeprägt. Bei Problemen mit Software greifen sie eher auf externe Hilfe zurück, da sie letztendlich doch nicht die Muße aufbringen, sich in alle notwendigen vertrackten Details eines Computers einzuarbeiten. Was das Raubkopieren angeht, stehen sie allerdings ihren großen Brüdern in nichts nach: Kopiert wird alles, was interessant erscheint – ob eine tatsächliche Verwendungsmöglichkeit besteht, ist zunächst einmal zweitrangig. Der Hobby-User ist jedoch darauf angewiesen, dass ihm der PC-Freak den Weg bahnt, ihm also die Tools zur Verfügung stellt, die zum Cracken der digitalen Zugangsbarrieren (Kopierschutz, Zwangsregistrierung, Softwareaktivierung etc.) notwendig sind.

Die Pragmatiker wiederum gehören zu einer Nutzergruppe, die den Computer schlicht als Arbeitsgerät einsetzt. Die Begeisterung für die technischen Möglichkeiten eines Computers hält sich in Grenzen, und dementsprechend gering sind auch die weitergehenden Computerkenntnisse. Raubkopien sind vergleichsweise nur in geringem Maße vorhanden, und dann auch nur so weit, wie sie auch tatsächlich genutzt werden. Die Gruppe der Pragmatiker ist innerhalb der Umfrage am stärksten ausgeprägt – knapp 50 Prozent aller Teilnehmer gehören ihr an. Der Altersdurchschnitt liegt bei 34 Jahren.

PC-Profis stellen die letzte Gruppe der identifizierten digitalen Typen. Sie lassen sich als eher gesetzte Computernutzer beschreiben, die ihren Rechner bestens beherrschen, aber im Unterschied zu den PC-Freaks kaum auf Raubkopien zurückgreifen. Der Altersdurchschnitt dieser Gruppe liegt mit 38 Jahren deutlich am höchsten, und die Personen dieser Gruppe haben es beruflich bereits zu etwas gebracht – viele leitende Angestellte und Geschäftsführer finden sich hier. Sie nutzen ihren PC in einer professionellen Weise und setzen dabei legal erworbene Software ein.

Die Teilnehmer der Online-Umfrage verteilen sich wie folgt auf die vier digitalen Typen (siehe Abbildung):

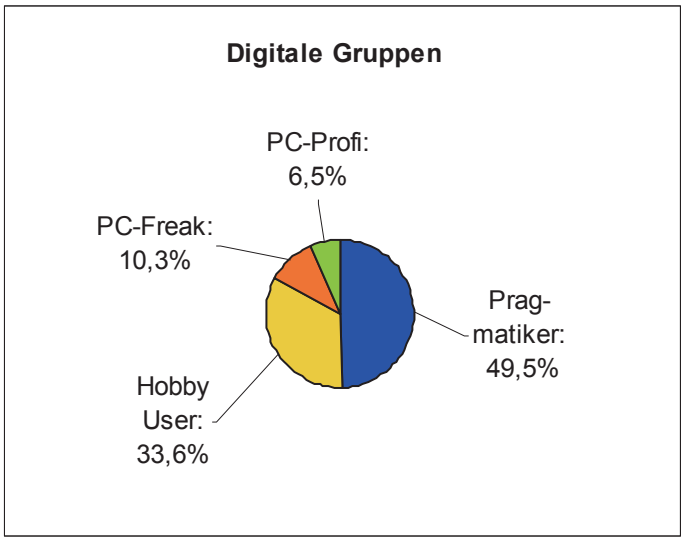


Abb. Institut für Strategieentwicklung: Verteilung digitaler Typen

Diese vier Nutzergruppen dienen als Einheiten der weiteren Analyse. Um die vielen, auf die Erforschung der Digitalen Mentalität abzielenden Items des Fragebogens auswertbar zu machen, wurden sie zu übergeordneten Größen zusammengefasst – ähnlich wie bei der Entwicklung der digitalen Typen. Es konnten zwei unterschiedliche Größen gewonnen werden, mit denen sich die Einstellung der Softwarenutzer zu Raubkopien prägnant beschreiben lässt. Diese Größen sind die Raubkopiermentalität und das Rechtsbewusstsein.

Digitale Typen und Raubkopiermentalität

Die Raubkopiermentalität misst, in welchem Maß das Raubkopieren von Software eine Sonderrolle im Vergleich zum Kopieren von CDs, MP3-Dateien oder DVDs einnimmt. Eine stark ausgeprägte Raubkopiermentalität bedeutet zum Beispiel, dass Software-Raubkopien im Vergleich als gravierender eingestuft werden.

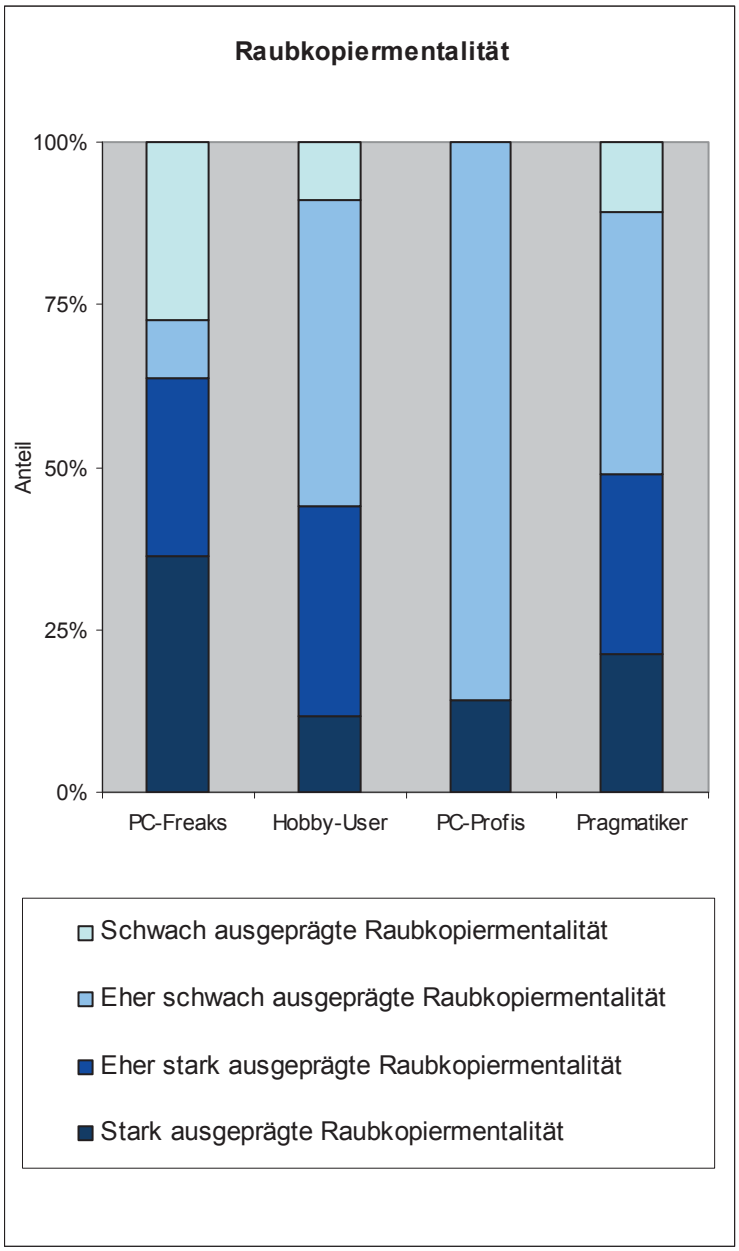


Abb. Institut für Strategieentwicklung: Ausprägungen der Raubkopiermentalität

Herausragende Werte der Ausprägung der Raubkopiermentalität finden sich bei der Gruppe der PC-Freaks. Knapp 65 Prozent dieser Gruppe lassen sich einer stark bis eher stark ausgeprägten Raubkopiermentalität zuordnen. Diese starke Ausprägung bei den PC-Freaks kann im ersten Moment überraschen, da sie aussagt, dass Software-Raubkopien im Vergleich zu anderen Copyright-Verletzungen als gravierender eingestuft werden. Hier scheint sich ein Widerspruch anzudeuten, wenn gerade die Gruppe der Vielkopierer das Raubkopieren als besonders gravierend einstuft. Die Gruppe der PC-Freaks hat trotzdem oder gerade deshalb Anreize für das Raubkopieren. Die mögliche Selbstwahrnehmung als Gesetzesbrecher und Bezwinger der Kopierschutzmechanismen motiviert vermutlich einen Teil dieser Gruppe, sich ständig aufs Neue den Herausforderungen des Raubkopierens zu stellen.

Digitale Typen und Rechtsbewusstsein

Das Rechtsbewusstsein zeigt, inwieweit sich das klassische Rechtsempfinden auf die digitale Welt überträgt. Mit dem Maß des Rechtsbewusstseins lässt sich feststellen, inwieweit Verletzungen von Urheberrechten wie eine physische Eigentumsverletzung wahrgenommen werden. Außerdem benennt das Rechtsbewusstsein das Ausmaß an Ehrlichkeit und drückt den gewissenhaften Zahlungswillen für in Anspruch genommene Leistungen aus.

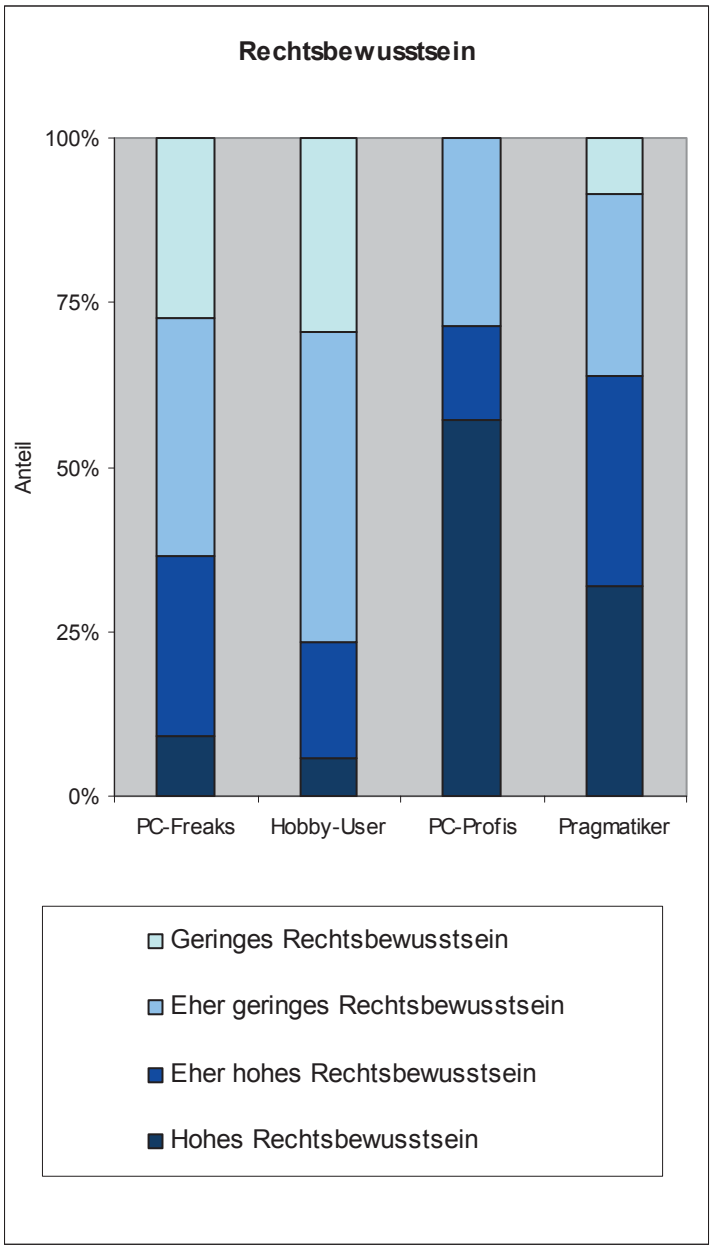


Abb. Institut für Strategieentwicklung: Ausprägungen des Rechtsbewusstseins

In dieser Aufschlüsselung zeigt sich, welchen Einfluss ein entsprechend ausgeprägtes Rechtsempfinden auf das Raubkopierverhalten hat – das Ausmaß des Rechtsbewusstseins der Vielkopierer (PC-Freaks, Hobby-User) bleibt deutlich hinter dem der Wenigkopierer zurück. In der Gruppe der PC-Profis deutet der Anteil von 75 Prozent an eher hohem bis hohem Rechtsbewusstsein darauf hin, dass diese Gruppe ganz bewusst auf Raubkopien

verzichtet, um sich gesetzeskonform zu verhalten. Ähnliches lässt sich auch über die Gruppe der Pragmatiker sagen, die zwar in der Ausprägung des Merkmals ‚Rechtsbewusstsein' hinter den PC-Profis zurückbleibt, aber dennoch deutlich die 50-Prozent-Marke überschreitet.

Datenschutz und Privatsphäre

Bei allen Schlussfolgerungen aus dieser Analyse darf ein Aspekt nicht unberücksichtigt bleiben, der besonders bei der Akzeptanz technischer Innovationen wie dem Trusted Computing oder neuen Formen des Digital Rights Managements eine wesentliche Rolle spielen wird: Allgemein werden in Deutschland in Bezug auf das Internet erhebliche Gefährdungen der Privatsphäre, des Datenschutzes und der Datensicherheit gesehen. Das Vertrauen in Wirtschaftsunternehmen und staatliche Institutionen hinsichtlich der Einhaltung des Datenschutzes ist gering. Diese Ängste wurden in anderen industrialisierten Ländern bestätigt, so dass man nicht nur von einer deutschen, sondern auch von einer international verbreiteten Einstellung ausgehen kann.[6] Daher spielt auch bei der Etablierung neuer Sicherheitssysteme für den heimischen Computer die im weiteren Verlauf der Studie beschriebene Digital Honesty eine große Rolle, weil es mit ihrer Hilfe gelingt, dem Verbraucher die Vorteile technischer Innovationen nahe zu bringen, ohne dass der Verbraucher im Gegenzug den Softwareherstellern unlautere Absichten mit persönlichen Daten unterstellt.

5 Schlussfolgerungen – Digital Honesty

Gelten unsere bisherigen Werte bezüglich Recht und Unrecht, Eigentum und Diebstahl auch noch im digitalen Medium? Lässt sich ein neues Bewusstsein, eine neue Sensibilität für die Notwendigkeit schaffen, diese grundlegenden Werte unserer Gesellschaft auch im digitalen Medium zu wahren und zu leben?

Die Antwort auf diese beiden zentralen Fragen hängt von einer dritten Frage ab: Wird das tatsächliche Handeln – in der digitalen wie in der nicht-digitalen Welt – vom vorherrschenden Unrechtsbewusstsein bestimmt oder von den zu erwartenden Sanktionen? Genügt es, klar herauszustellen, wo die Grenze zwischen Recht und Unrecht verläuft, oder muss dafür gesorgt werden, dass die Angst vor den Konsequenzen illegalen Handelns ausreichend groß ist?

---

[6] Groebel, J., Gehrke G. (Hrsg.), Internet 2002: Deutschland und die digitale Welt. Internetnutzung und Medieneinschätzung in Deutschland und Nordrhein-Westfalen im internationalen Vergleich, Opladen 2003

Wir konnten feststellen, dass in der Frage nach dem Rechts- und Unrechtsbewusstsein im digitalen Medium eine weit verbreitete Klarheit herrscht. Es fällt der überwiegenden Mehrheit der Verbraucher nicht schwer, ihr eigenes Handeln im Bezug auf Raubkopien als Unrecht zu klassifizieren.

Rechtsbewusstsein und tatsächliches Verhalten

Faktum ist jedoch, dass dieses Rechtsbewusstsein nur einen geringen Einfluss auf das tatsächliche Raubkopierverhalten hat. Beobachten lässt sich beispielsweise, dass besonders der Anreiz, Freunde und Familie mit Raubkopien zu versorgen, eine Eigendynamik entwickelt. Im Sinne eines Gebens und Nehmens sind die Mitglieder einer solchen Gruppe darauf angewiesen, selbst nicht nur als Empfänger, sondern auch als Verteiler agieren zu können, um sich erkenntlich zu zeigen. Dazu erschließen sie sich weitere Quellen außerhalb des engeren Familien- und Freundeskreises.

Die Kräfte und die Eigendynamik dieses Kopierens im Freundeskreis überwiegen den möglichen Einfluss einer rechtlichen Regelung bei weitem. Hieran zeigt sich, dass die Frage nach der Nachvollziehbarkeit der Unterscheidung von Recht und Unrecht aus der Sicht des Verbrauchers viel entscheidender für sein tatsächliches Verhalten ist. Denn erst im Nachvollziehen – im Sinne von Akzeptanz – gewinnt die rechtliche Regelung einen verbindlichen Charakter, da sich der Einzelne aufgrund seiner persönlichen Überzeugungen nun an die rechtliche Regelung gebunden fühlt.

Nachvollziehbarkeit als entscheidende Größe

Wie wichtig diese Nachvollziehbarkeit ist, zeigt sich auch an der folgenden Betrachtung, die anhand theoretischer Überlegungen erörtert, welche prinzipiellen Bedingungen erfüllt sein müssen, damit Menschen sich an geltendes Recht halten.

Idealerweise stimmt ein Gesetz oder eine Verordnung mit dem intuitiven Rechtsempfinden des Einzelnen überein. In diesem Fall entspricht das rechtskonforme Verhalten der Verhaltensweise, die diese Person auch ohne die entsprechende gesetzliche Regelung gezeigt hätte.

Wo diese Übereinstimmung von intuitivem Rechtsempfinden und geltendem Recht nicht gegeben ist, braucht es Aufklärung. Die gesetzlichen Regelungen müssen so dargelegt und begründet werden, dass es dem Einzelnen möglich ist, sie zu kennen und nachzuvollziehen. Sobald beides – Kenntnis und Nachvollziehbarkeit – vorhanden ist, verhält sich der Einzelne im Idealfall kraft seiner eigenen Einsicht in die Sinnhaftigkeit der rechtlichen Regelung gesetzeskonform.

Wird aber trotz umfassender Aufklärungsarbeit die rechtliche Regelung nur zur Kenntnis genommen, ohne dass beim Einzelnen eine Einsicht in ihre Sinnhaftigkeit entsteht, ist nicht zu erwarten, dass er sein Verhalten nach der rechtlichen Regelung richtet. Um an diesem Punkt eine Verhaltensänderung zu bewirken, ohne die Sinnhaftigkeit der gesetzli-

chen Regelungen in Frage zu stellen, bleibt nur die Sanktionierung gesetzwidrigen Verhaltens. Dabei müssen zwei Bedingungen erfüllt sein. Zum einen muss das Sanktionierungspotenzial, also die Höhe der angedrohten Strafe, ausreichend sein, um die geforderte Verhaltensänderung zu rechtfertigen, und zum zweiten muss die Wahrscheinlichkeit, dass gesetzwidriges Verhalten im Einzelfall auch tatsächlich sanktioniert wird, hinreichend hoch sein.

Das Beispiel Filmindustrie

Dass jeder Rückgriff auf die Androhung von Sanktionen auch als Ausdruck von Ratlosigkeit interpretiert werden kann, lässt sich am Beispiel der Filmwirtschaft beobachten.

Die Filmwirtschaft sieht sich zurzeit, ähnlich wie die Softwarebranche, mit dem Phänomen konfrontiert, dass eine nicht unerhebliche Anzahl von Menschen trotz ausreichender Kenntnis der Rechtslage Urheberrechtsverletzungen begeht. Dieser mangelnden Übereinstimmung zwischen intuitivem Rechtsempfinden des Einzelnen und geltendem Recht begegnet die Filmwirtschaft nicht, indem sie glaubhaft für die Sinnhaftigkeit und Nachvollziehbarkeit der gesetzlichen Regelungen wirbt, sondern – das zeigt die momentan in den deutschen Kinos präsente Kampagne ‚Raubkopierer sind Verbrecher' deutlich – indem sie auf die abschreckende Wirkung der drohenden Strafe setzt und damit Millionen von privaten Raubkopierern kriminalisiert.

Gleichzeitig wird mit exemplarischen Klagen gegen Nutzer von Internet-Tauschbörsen versucht, auch auf diesem Weg allen anderen Nutzern die drohenden Sanktionen so deutlich vor Augen zu führen, dass sie ihr urheberrechtverletzendes Verhalten einstellen.

Das Prinzip Abschreckung läuft ins Leere

Die abschreckende Wirkung solcher exemplarischen Strafaktionen konnte bisher nicht bewiesen werden. Das lässt sich dadurch erklären, dass durch die große Anzahl der Nutzer in einer Tauschgemeinschaft das Risiko für den Einzelnen sehr gering ist. Inzwischen vertreten auch andere Studien die Position, dass die von der Musikindustrie formulierten Drohungen zu keiner bemerkenswerten Verhaltensänderung bei den Nutzern von Tauschbörsen geführt haben.

Die Strategie der Musik- und Filmindustrie wäre für die Softwarebranche keine Erfolg versprechende Option. Die Unternehmen der Softwareindustrie würden ihren Ruf und das Vertrauen ihrer bisherigen Kunden aufs Spiel setzen – ganz zu schweigen von der Beziehung zu den potenziellen Kunden unter den Raubkopierern.

Diese Unterscheidung ist bei der Betrachtung der verschiedenen Typen von Raubkopierern im Bereich Software von entscheidender Bedeutung. Hier muss es der Softwareindustrie gelingen, aus einem Großteil bisheriger Raubkopierer mit entsprechenden Argumenten oder Angeboten Kunden zu machen. Diese Überlegungen legen einen taktvolleren

und sensibleren Umgang mit dem Phänomen Raubkopieren nahe, als ihn die Filmwirtschaft zurzeit pflegt.

Eine Möglichkeit des nachhaltigeren Umgangs mit dem Phänomen Raubkopieren ist es, in unserer Gesellschaft eine Kultur des Umgangs mit geistigem Eigentum in der digitalen Welt zu entwickeln und zu etablieren.

Digital Honesty – eine gesellschaftliche Herausforderung

Immer mehr Aspekte unseres Lebens spielen sich in der digitalen Welt ab, werden von ihr berührt oder verlagern sich komplett in diese Welt. Der Erfolg dieser Entwicklung wird direkt von der Frage abhängen, welchen Stellenwert diese digitale Welt in unserer Gesellschaft hat und haben wird. Ebenso wie es für den Erhalt und den Erfolg unserer Gesellschaft wichtig ist, dass sich ihre Mitglieder an grundlegende, festgeschriebene oder unausgesprochene Regeln des Miteinander halten, ist es für die Zukunft unserer Gesellschaft auch wichtig, dass es gelingt, entsprechende Regeln in der digitalen Welt zu etablieren, um auch dort ein fruchtbares Miteinander zu gewährleisten.

Um die Wichtigkeit einer solchen Kultur des Umgangs mit geistigem Eigentum in der digitalen Welt zu vermitteln, ist es notwendig darauf hinzuweisen, dass Eigentum kein Privileg der Reichen ist, sondern eine hochgradig – nämlich zeitlich, sachlich und ökologisch – konditionierte Konzession der Gesellschaft, die Eigentümern Verfügungsrechte einräumt, die den Ausschluss aller anderen von diesen Verfügungsrechten implizieren und nur unter diesen Bedingungen den Handel – als Transfer von Verfügungsrechten – mit Eigentum ökonomisch möglich und lohnend machen.

Auf einer solchen Definition von Verfügungsrechten auch im Umgang mit digitalisierten Inhalten beruht die Ausarbeitung von Geschäftsmodellen, die Formierung eines Produktionsmarktes und auf dieser Grundlage die Markierung von Innovationsgelegenheiten und Innovationschancen.

6 Ausblick

Die Differenz zwischen vorhandenem Rechtsbewusstsein und fehlender Konsequenz im tatsächlichen Handeln kann nachhaltig nur durch eine vorgelebte und transportierte Digital Honesty aufgehoben werden. Eine Arbeit aller Beteiligten an dieser Digital Honesty wird sich auf Dauer im Bewusstsein der Konsumenten verankern – denn entgegen zeitweiliger Eindrücke durch die öffentliche Berichterstattung ist der Anteil der extremen Befürworter des Raubkopierens in der Bevölkerung sehr gering.

Um eine Digital Honesty zu etablieren, bleibt der Softwarebranche keine andere Möglichkeit, als in Vorleistung zu gehen. Das bedeutet konkret: Die Wahrnehmung der Softwarebranche und ihres Verhaltens durch den Verbraucher spielt eine wesentliche Rolle für die erfolgreiche Etablierung einer solchen Kultur des Umgangs mit geistigem Eigentum.

Nur eine Softwarebranche, die ihre Ansprüche und Ziele klar kommuniziert und eine Digital Honesty in den Augen des Verbrauchers glaubhaft lebt, schafft die Grundlage für ein Verständnis des Verbrauchers für die rechtlichen Regelungen zum Umgang mit geistigem Eigentum in der digitalen Welt. Und erst das Verständnis sorgt für eine umfassende Ausrichtung des Verhaltens an den rechtlichen Gegebenheiten.

Alles in allem wird jeder Ansatz seine Zeit benötigen – ein digitales Selbstverständnis muss kulturell wachsen. Dabei sollten die genannten möglichen Ansätze genutzt werden, um dieses Wachstum zu unterstützen.

Betrugsdelikte im Internet

Zum aktuellen Stand des empirischen Wissens aus kriminologischer Sicht

Dr. Werner Rüther

In den ersten Jahren des neuen Jahrtausends kann man in allen gesellschaftlichen Bereichen eine zunehmende Verbreitung der modernen, digitalen Informations- und Kommunikationstechnologien beobachten. Besonders auffallend ist dabei, dass die Bürgerinnen und Bürger des Landes auch immer häufiger und zahlreicher das weltweite Daten- und Kommunikationsnetz des Internet nutzen.[1] Nach den neuesten Zahlen der so genannten (N)Onliner-Studie 2006[2] von TNS-Infratest im Auftrag der Initiative D21 hat sich die Nutzerquote in den letzten fünf Jahren von 37,0 Prozent im Jahre 2001 auf 58,2 Prozent im Jahre 2006 um mehr als 20 Prozent gesteigert. Nach zahlreichen anderen vergleichbaren Untersuchungen kann man in der Bundesrepublik Deutschland derzeit in etwa von einer Zwei-Drittel-Netzgesellschaft ausgehen; das heißt: zwei von drei Personen nutzen mehr oder weniger intensiv das Internet, wobei die höchste Nutzerquote eindeutig bei den jüngeren und mittleren Jahrgängen liegt.[3]

1 Einführung in die Fragestellung: Was wissen wir über ‚E-Devianz' und speziell über Betrugsdelikte im Internet?

Bedenkt man in diesem Zusammenhang, dass das Internet für den Normalbürger noch vor gut eineinhalb Jahrzehnten vollkommen unbekannt war und überhaupt noch nicht genutzt wurde, so kann man mit Recht von einer mehr oder weniger revolutionären Entwicklung im gesellschaftlichen Kommunikationsverhalten seit Anfang der 90er Jahre sprechen. Dabei ist es eine Selbstverständlichkeit, dass sich mit den Veränderungen im ‚normalen' Kommunikationsverhalten auch Veränderungen im so genannten abweichenden (Kommu-

[1] Die Internetnutzung in der Bevölkerung wird in der Regel durch repräsentative Befragungen gemessen, von denen mittlerweile nicht wenige in regelmäßigen Abständen durchgeführt und auch publiziert werden. Einen umfassenden Überblick und guten Zugang zu diesen Nutzungsstudien findet man im Netz unter *http://www.digitale-chancen.de/content/stories/index.cfm/key.399/secid.16/secid2.49*

[2] Diese Studie ist seit Anfang August 2006 im Internet zugänglich unter der Adresse: *http://www.nonliner-atlas.de/index.asp*

[3] Alle Studien belegen übereinstimmend, dass speziell die älteren Jahrgänge derzeit (noch) den geringsten Zugang zum Netz haben, obwohl auch hier ansteigende Tendenzen erkennbar sind. Siehe z.B. (statt vieler) die Ergebnisse der Forschungsgruppe Wahlen unter *http://www.fgw-online.de/Ergebnisse/Internet-Strukturdaten/web_II_06.pdf*

nikations-)Verhalten ergeben haben. Bei zahlreichen, sich entwickelnden Abweichungsphänomenen im elektronischen, digitalen Zeitalter wird das Internet entweder als Handlungsziel oder als Handlungsmittel genutzt. In Anlehnung an die klassische sozialwissenschaftliche Devianzforschung lassen sich diese (derzeit gesellschaftlich vielfach noch offenen und unstrukturierten) Phänomene auch mit dem Begriff der ‚elektronischen Devianz' oder kurz und prägnant auch mit dem modernen Begriff der ‚E-Devianz' fassen. Fragt man in der Bevölkerung oder in speziellen Bevölkerungsgruppen, wie wir es bei Studierenden an der Universität Bonn ansatzweise getan haben, welche einzelnen Phänomene mit den Begriffen ‚E-Devianz' oder ‚Internetdelinquenz' in Zusammenhang gebracht werden, so werden relativ häufig verschiedene Betrugsdelikte genannt, welche im Rahmen und mittels des Internet begangen werden. Verschiedene weitere kriminologisch relevante Indikatoren deuten darauf hin, dass die Betrugsphänomene im Internet auch rein zahlenmäßig eine nicht unbedeutende Rolle spielen. Was wissen wir jedoch Genaueres über diese neuen digitalen Betrugsphänomene im Internet? In jüngster Zeit, so verbreiten sich die Eindrücke, wird das anfänglich vorhandene, relativ große ‚Nichtwissen' durch erste systematische Wissensbestände abgelöst, die es zu sichten, ansatzweise darzustellen und zu interpretieren gilt.

Im folgenden Beitrag soll versucht werden, zunächst einmal eine vorwiegend beschreibende Annäherung an die verschiedenen Betrugsphänomene im Internet zu erreichen, um erste deutlichere Konturen und Anhaltspunkte für spätere kriminologische Diskussionen und speziell auch mögliche präventive Maßnahmen zur Verfügung zu haben. Dabei sollen sowohl offizielle Daten der Behörden (z.B. PKS) als auch Daten aus empirischen Dunkelfeldstudien herangezogen werden.

2 Zur Entwicklung der Betrugsdelikte in der Polizeilichen Kriminalstatistik (Hellfeld)

Während sich die Gesamtzahlen der Polizeilichen Kriminalstatistik (PKS) schon seit langem, etwa seit Mitte der 90er Jahre auf einem relativ konstanten Niveau um die 6,5 Millionen registrierte Fälle herum bewegen (mit zuletzt sogar leicht sinkender Tendenz), kann man speziell bei einzelnen Deliktsbereichen durchaus unterschiedliche Entwicklungen und auch kontinuierliche Anstiege feststellen.

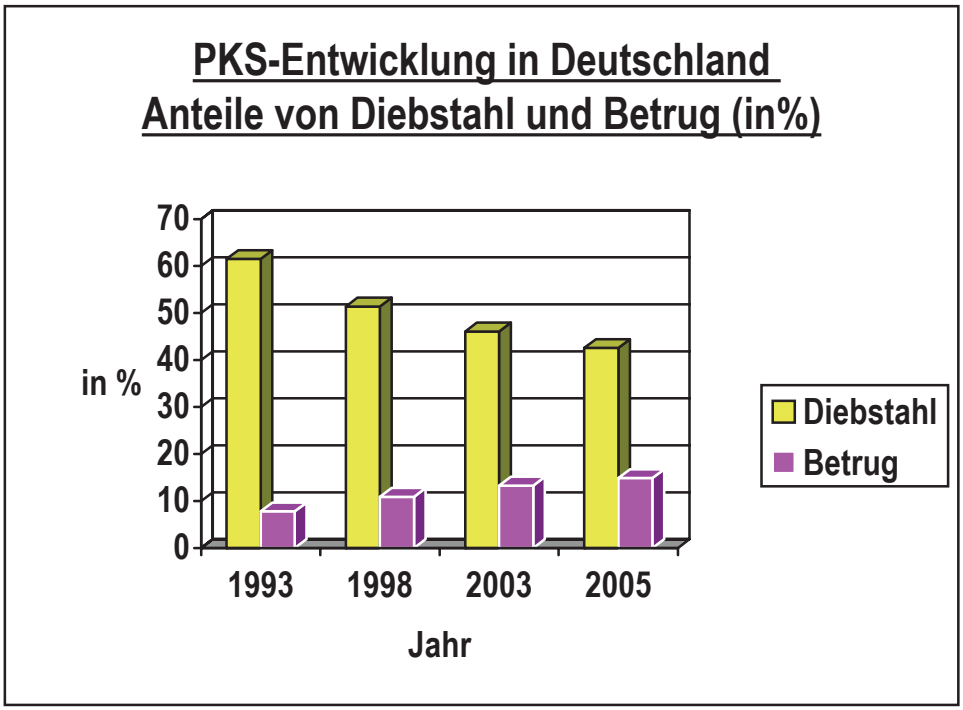
2.1 Betrugsdelikte allgemein

Zu den auffallenden Deliktsbereichen mit eindeutig ansteigender Tendenz zählen seit ca. 12 Jahren in der Polizeilichen Kriminalstatistik die Betrugsdelikte mit der Schlüsselkenn-

zahl 5100. Sie haben sich von 1993 bis zum Jahre 2005 von gut einer halben Million Fälle (528.410) auf knapp eine Million Fälle (949.921) nahezu verdoppelt.[4]

Auf der anderen Seite haben die Diebstahlsdelikte, die in den zurückliegenden Jahren und Jahrzehnten (mit über 60%) stets den bei weitem größten Anteil ausmachten, kontinuierlich und deutlich abgenommen. Während 1993 im gesamten Bundesgebiet noch deutlich über 4 Millionen Diebstahlsdelikte polizeilich registriert wurden (n = 4.151.087), waren es im Jahre 2005 deutlich weniger als 3 Millionen (n = 2.727.048).

Dies hat zur Folge, dass der Prozentanteil des Diebstahls insgesamt in der PKS mittlerweile klar unter 50 Prozent gesunken ist, während der Anteil des Betrugs sich insgesamt von 7,8 Prozent (im Jahr 1993) auf 14,9 Prozent (im Jahr 2005) nahezu verdoppelt hat.



Es ist durchaus nahe liegend, dass man diesen deutlich erkennbaren Trend auch für die folgenden Jahre weiter in die Zukunft hinein extrapolieren kann und somit eine weitere Annäherung der prozentualen Anteile von Diebstahls- und Betrugsdelikten in der PKS für die kommenden Jahre prognostizieren kann. Denn dieser Trend in der Verschiebung der Deliktstruktur geschieht nicht rein zufällig, sondern er basiert auf deutlichen Veränderun-

[4] Dieser deutliche Anstieg der Betrugsdelikte ist dabei nicht nur auf die PKS beschränkt, sondern er spiegelt sich in ähnlicher Form auch in den Zahlen der Strafverfolgungsstatistik wider. Danach sind die Verurteilungen bei den Betrugsdelikten in den Jahren 1993 bis 2003 von 75.708 auf 105.843 Fälle angestiegen. (Quelle: Statistisches Bundesamt, Hrsg., Arbeitsunterlage Strafverfolgung – Fachserie 10 Reihe 3)

gen in den gesellschaftlichen Entwicklungen und Strukturen, besonders im Bereich des Kommunikationsverhaltens. Dieses hat sich durch die modernen Medien und Telekommunikationstechniken in den letzten Jahren nahezu revolutionär verändert. Die so genannte ‚digitale Revolution', in deren Zusammenhang auch das rasant wachsende Internet zu sehen ist, hat einerseits neue Möglichkeiten und Chancen für das weltweite System der menschlichen Kommunikation eröffnet, andererseits jedoch auch neue Risiken und Gefahren mit sich gebracht, welche sich auch hinsichtlich der Begehungsformen von Delikten bemerkbar machen.

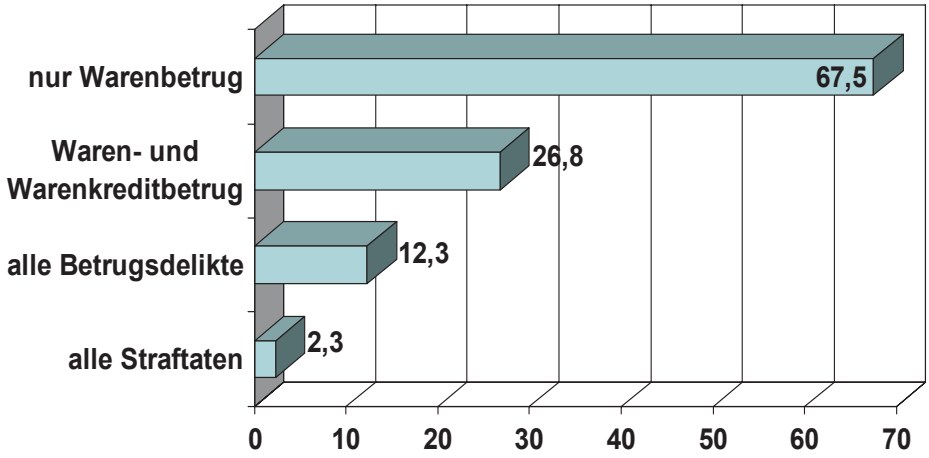
Die im direkten Vergleich zu den klassischen ‚Face-to-Face'-Kommunikationen relativ abstrakt und anonym ablaufenden Tele-Kommunikationen im Internet bieten speziell für die zentralen Täuschungshandlungen der verschiedenen Betrugsphänomene neue und gute Rahmenbedingungen und somit relativ günstige Gelegenheitsstrukturen zur Tatbegehung.

2.2 Betrugsdelikte im Zusammenhang mit dem ‚Tatmittel Internet'

Um auch zahlenmäßig nachvollziehen zu können, in welchem Ausmaß und Umfang die Anzahl der einzelnen Delikte und speziell der Betrugsdelikte auf diesen Hintergrund zurückzuführen ist, wurde mit Beginn des Jahres 2004 in der Polizeilichen Kriminalstatistik eine Sonderkennung ‚Tatmittel Internet' eingeführt, welche bei allen Deliktsfällen immer dann anzukreuzen ist, wenn man davon ausgehen kann, dass das Delikt im Wege der Internet-Kommunikation begangen worden ist. Wie bei vielen Neuregelungen in der Statistik üblich, bedurfte auch diese neuartige Registrierung zunächst einer gewissen Anlaufzeit, welche die diesbezüglichen PKS-Zahlen für das Jahr 2004 (noch) nicht allgemein und problemlos verwerten lassen. Selbst im Jahr 2005 haben sich noch nicht alle Bundesländer dieser Neuregelung anschließen können[5], sodass auch diese Zahlen nur mit Einschränkung und als ein erster Anhaltspunkt zu sehen sind.

[5] Nach der PKS 2005 fehlen bei der einschlägigen Tabelle (T240, S.247) immer noch die beiden Bundesländer Bayern und Niedersachsen.

Anteil „Tatmittel Internet“ (in %)
bei PKS-Straftaten 2005 (BRD)
- speziell bei Betrugsdelikten -



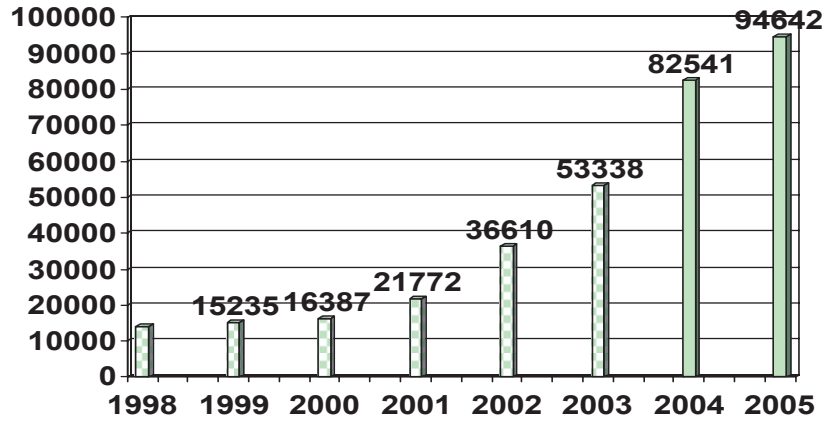
Quelle: BKA, Polizeiliche Kriminalstatistik 2005, T240, S.247

Während das ‚Tatmittel Internet’ bezüglich der Gesamtheit aller polizeilich registrierten Straftaten mit 2,7 Prozent (bisher) doch nur eine sehr bescheidene und untergeordnete Rolle spielt, sieht die Situation hinsichtlich der Betrugsdelikte (Schlüsselzahl 5100) und dabei speziell bei den Waren- und Warenkreditbetrugsdelikten (Schlüsselzahl 5110) doch schon ein wenig anders aus. Konzentriert man sich nun noch auf die spezielle Unterkategorie ‚Warenbetrug’ (Schlüsselzahl 5113), so muss man feststellen, dass hier der Anteil der Fälle mit ‚Tatmittel Internet’ bereits mehr als zwei Drittel (67,5%) ausmacht. Dies ist insoweit nicht besonders verwunderlich, wenn man bedenkt, dass hierunter vor allem jene Strafanzeigen registriert werden, die im Zusammenhang mit den rasant zunehmenden Online-Auktionsgeschäften (speziell bei eBay)[6] ihren Ausgangspunkt haben. Bei den Online-Auktionshäusern ist es üblich, dass die Person, die ein Objekt ersteigert hat, zunächst in Vorkasse tritt und den erforderlichen Geldbetrag an den Versteigerer (bzw. Verkäufer) überweist; danach wird in der Regel erst die ersteigerte Ware geliefert. Geschieht dies in einzelnen Fällen nun nicht bzw. unvollständig oder mangelhaft, so liegt hier häufig ein Ansatzpunkt für (zunächst) zivilrechtlich zu lösende Konflikte, welche von den Geschädigten und Betroffenen offensichtlich verstärkt auch auf den strafrechtlichen Weg ge-

[6] Nähere Angaben hierzu finden sich in dem Beitrag: Rüther, Werner, Neue Medien, neue Formen der Massendelinquenz und neue Herausforderungen für die Prävention. In: forum kriminalprävention, 2/2005, S.3-5

schickt werden[7] und dort von der Polizei unter der Schlüsselnummer 5113 (Warenbetrug) eingeordnet werden.

Entwicklung der polizeilich registrierten Warenbetrugsdelikte in der BRD (1998-2005)



Quelle: BKA, Polizeiliche Kriminalstatistik, 1993-2005, T166; Schlüsselzahl: 5113

Hier zeigt die registrierte Entwicklung in der PKS, dass sich die Warenbetrugsdelikte seit Beginn dieses Jahrtausends und damit seit Beginn der rasanten Entwicklung im Bereich der Online-Auktionen weit mehr als verfünffacht haben, von 16.387 Fällen im Jahre 2000 auf 96.642 Fälle im Jahr 2005. Gerade diese Zahlen geben jedoch Anlass zu der Vermutung, dass hiermit weniger das reale Geschehen im tatsächlichen Vorkommen der Delikte abgebildet wird, sondern dass hiermit vor allem Aussagen über das veränderte Anzeigeverhalten und die dahinter liegenden subjektiven Einschätzungen und Bewertungen der Betroffenen gemacht werden können.

[7] Interessant ist in diesem Zusammenhang, welche Rolle dabei die verschiedenen Möglichkeiten zur Erstellung von Online-Anzeigen spielen, die in jüngster Zeit in zahlreichen Bundesländern durch spezielle Online-Portale eröffnet werden. Speziell zu den Mechanismen der Online-Anzeige in NRW führt unser Institut derzeit ein gesondertes Forschungsprojekt durch. Siehe hierzu: Rüther, Werner, Die Online-Strafanzeige als neues Instrument der strafrechtlichen Sozialkontrolle. Erste empirische Erkenntnisse und geplante Projekte in einem bisher weitgehend unerforschten Gebiet. In: BKA, Hrsg., Forum KI 1 – 2005, S. 1 - 20

3 Neuere Erkenntnisse über die Phänomenologie von Betrugsdelikten im Internet anhand weiterer Indikatoren (Dunkelfeld)

Die in der kriminologischen Forschung allseits bekannte, begrenzte und selektive Aussagekraft von offiziellen statistischen Daten führt auch hier konsequenter Weise zur Suche nach weiteren Indikatoren und Daten, welche vor allem auch über das so genannte Dunkelfeld nähere Angaben machen können.

3.1 Erkenntnisse aus wissenschaftlichen Studien

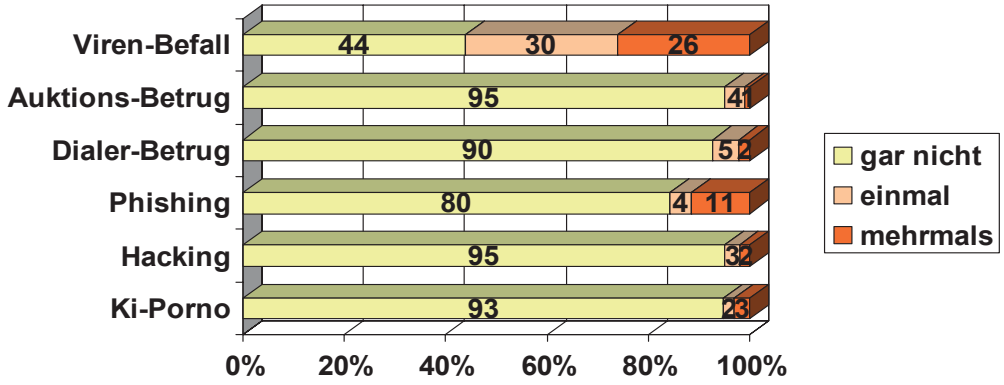
Da die Internetdelinquenz als relativ neues Phänomen in der kriminologischen Forschung der etablierten Institute bisher noch weitgehend ausgeblendet ist, sind wissenschaftliche Erkenntnisse und aktuelle Ergebnisse von speziellen Untersuchungen zu dieser Thematik bisher noch Mangelware. Anstelle eines Überblicks über die vorhandene kriminologische Forschung zu diesem Deliktsbereich bietet sich zum jetzigen Zeitpunkt zunächst ein kurzer Blick auf diesbezügliche empirische Erkenntnisse aus eigener Forschungsarbeit an (3.1.1), um anschließend dann noch kurz und konzentriert auf internationale Forschungsergebnisse einzugehen, die interessanter Weise vom aktuellen ‚British Crime Survey' (BCS) berichtet werden (3.1.2).

3.1.1 Eigene Online-Befragungen an der Universität Bonn

Am Kriminologischen Seminar der Universität Bonn sind in den letzten Jahren mehrere kleinere Untersuchungen zum Thema ‚Sicherheit und Delinquenz im Internet' (SUDI) durchgeführt worden. Dabei ist in erster Linie eine studentische Population im Wege von Online-Studien zu aktuellen Themen im Zusammenhang mit neuen Phänomenen der Internetdelinquenz befragt worden. Neben unterschiedlichen Einstellungsfragen vor allem zum Sicherheitsgefühl im Netz und in der Wohngegend ging es dabei auch um Dunkelfeldfragen und spezielle Betroffenheiten von Internetdelinquenz sowohl als Täter als auch als Opfer.

Die aktuellste Untersuchung ist im Sommersemester dieses Jahres (2006) durchgeführt worden und sie richtete sich im Wesentlichen an Studierende der Rechtswissenschaften und der Kriminologie. Studierende sind speziell für Online-Befragungen eine sehr geeignete Population, da sie als eine der wenigen gesellschaftlichen Gruppen bereits schon jetzt fast zu 100 Prozent im Internet unterwegs und somit nahezu vollständig und ausnahmslos erreichbar sind. Von ursprünglich 300 einbezogenen Befragten haben ca. zwei Drittel den Fragebogen auch vollständig ausgefüllt.

Auf die Frage ‚Wie häufig sind Sie innerhalb der letzten 12 Monate von folgenden Einzeldelikten betroffen bzw. geschädigt worden?' ergab sich folgende Antwortverteilung:



n = 187

Dabei fällt auf, dass die Haupt-Betroffenheit von mehr als 50 Prozent eindeutig beim ‚Viren-Befall' liegt. Bei allen anderen angegebenen Internetdelikten hält sich die studentische Betroffenheit in den letzten 12 Monaten doch sehr in Grenzen.[8] Von den Betrugsdelikten weist das so genannte ‚Phishing' mit insgesamt 15 Prozent Betroffenheit noch den größten Prozentsatz auf. Der Auktions-Betrug liegt zwar prozentual mit 5 Prozent klar an hinterer Stelle, auf die Gesamtheit aller Studierenden hochgerechnet[9] dürften sich jedoch auch hier absolute Zahlen ergeben, die sich im fünfstelligen Bereich bewegen.

Bei einer angenommenen Zahl von 1 Million Studierenden sind danach etwa zwischen 40.000 und 60.000 Personen vom Auktions-Betrug im Netz innerhalb eines Jahres betroffen. Geht man nun mit den aktuellsten Daten der repräsentativen Internetnutzungsforschung[10] zumindest von ca. 40 Millionen aktiven Netzbürgerinnen und Netzbürgern in der Bundesrepublik Deutschland aus[11], so muss man diese Zahl entsprechend vervielfachen bzw. maximal vervierzigfachen; man nähert sich nach dieser Dunkelfeldschätzung somit einer maximalen Fallzahl an Online-Auktionsbetrugsdelikten von deutlich über einer Millionen. Bei knapp 100.000 offiziell registrierten Warenbetrugsdelikten im Hellfeld (s.o.)

[8] Im Vergleich dazu lag die Opferbetroffenheit beim klassischen Delikt ‚Fahrraddiebstahl' immerhin bei 11,9% und beim sonstigen Diebstahl sogar bei 20,5%.

[9] Dabei ist es selbstverständlich klar, dass derartige Hochrechnungen bei der vorhandenen geringen und nicht repräsentativen Stichprobe allenfalls erste Annäherungsversuche und mehr oder weniger gewagte Schätzungen darstellen können, welche mangels vorhandener repräsentativer Daten nur hilfsweise vorgenommen werden.

[10] So z.B. TNS Infratest, Initiative D21, (N)Onliner-Atlas 2006, publiziert am 1.8.2006 im Netz unter *http://www.nonliner-atlas.de/pdf/dl_NONLINER-Atlas2006.pdf*

[11] Danach sind 58,2% der Bevölkerung über 14 Jahren in der BRD ‚online'. Bei einer absoluten Zahl von ca. 71 Millionen Bundesbürgern über 14 Jahren (siehe die entsprechenden Statistik des Statistischen Bundesamtes) ergeben sich danach in etwa 40 Millionen ‚Onliner'.

beträgt die Hellfeld-Dunkelfeld-Relation danach zumindest 1:10, was im Vergleich zu anderen Bagatelldelikten nicht einmal besonders hoch erscheint.[12]

3.1.2 Ergebnisse des British Crime Survey (BCS) 2003/04 und des Offending, Crime and Justice Survey (OCJS) 2004

Da in der Bundesrepublik Deutschland repräsentative Befragungen, welche die Täter- und Opferbetroffenheiten der Bürgerinnen und Bürger systematisch und kontinuierlich erfassen könnten und somit auch Aussagen über die Betroffenheiten von modernen Delikten mit Internetbezug machen könnten, leider immer noch vergeblich gesucht werden und derartige Dunkelfelduntersuchungen trotz deutlicher Forderungen speziell auch aus dem Bereich der kriminologischen Wissenschaft[13] immer noch nicht institutionalisiert sind, gilt es hier hilfsweise einen Blick über den nationalen Grenzzaun nach Großbritannien zu werfen. Anders als in Deutschland werden dort schon seit vielen Jahren repräsentative und regelmäßige so genannte ‚British Crime Surveys' durchgeführt, welche im Wesentlichen die Opferbetroffenheiten von zahlreichen unterschiedlichen Delikten zum Gegenstand haben. Seit einigen Jahren wird zudem auch eine spezielle Befragung durchgeführt, welche sich den Täter-Betroffenheiten innerhalb der Bevölkerung zuwendet und hierbei auch die modernen Intenetdelikte zumindest ansatzweise mit einbezieht.

Die neuesten Ergebnisse des British Crime Survey (BCS) 2003/04 und des Offending Crime and Justice Survey (OCJS) 2004 zu den hier interessierenden Phänomenen ‚Fraud and technology crimes' sind Anfang September 2006 vom Britischen ‚Home Office' im Netz zugänglich gemacht worden.[14] Danach bezieht sich die häufigste Opferbetroffenheit bei Internetdelikten auch (ähnlich wie in der Bonner Umfrage) auf das Phänomen des ‚Viren-Befalls'. Mehr als jeder vierte, genau 27 Prozent der Befragten zeigen sich innerhalb der letzten 12 Monate hiervon als Opfer betroffen. Die Zahlen zur Betrugsbetroffenheit lassen leider keine speziellen Aussagen zum uns hier besonders interessierenden Aukti-

---

[12] Dass die Dunkelziffer in diesem Bereich relativ gering und die Anzeigequote relativ hoch ist, könnte nach neueren Erkenntnissen im Zusammenhang mit spieltheoretischen Experimenten (siehe den Spieltheoretiker und Wirtschaftswissenschaftler Ockenfels; siehe zudem eigene Experimente im Rahmen der Vorlesung ‚Internetdelinquenz') auch auf den so genannten ‚Fluch des Gewinnens' zurückzuführen sein. Je größer die Beteiligung an Online-Auktionen ist, desto höher ist nach dem ‚Gesetz der großen Zahl' letztendlich der Betrag, den der Gewinner zu zahlen hat. Er liegt dabei häufig mehr oder weniger deutlich über dem eigentlichen Wert des Gegenstandes. Der Auktionsgewinner wird somit zum eigentlichen Verlierer und kann sich eher als ‚Betrogener' fühlen mit entsprechenden Konsequenzen für eine erhöhte Beschwerde- und Anzeigebereitschaft.

[13] Siehe hier statt vieler: Heinz, Wolfgang, Jugendkriminalität zwischen Verharmlosung und Dramatisierung. In: DVJJ-Journal, Jg. 8, Nr. 3, Seite 270 - 293

[14] Siehe: Wilson, Debbie, u.a., Fraud and technology crimes. Findings from the 2003/04 British Crime Survey, the 2004 Offending, Crime and Justice Survey and administrative source. Unter: *http://www.homeoffice.gov.uk/rds/pdfs06/rdsolr0906.pdf*

onsbetrug zu, sondern sie machen nur Angaben zum so genannten Betrug mit Debit- und Kreditkarten; die Opfer-Betroffenheit liegt hier über die Jahre relativ konstant bei nur 3 – 4 Prozent.

Auch hinsichtlich der im Rahmen des Offending, Crime and Justice Survey (OCJS) erhobenen Täter-Betroffenheiten sind bisher leider keine speziellen Fragen zum Online-Auktionsbetrug gestellt worden, so dass auch hier zunächst auf mögliche Ergänzungen und Erweiterungen des Deliktskatalogs im Rahmen zukünftiger Befragungen gewartet werden muss.[15]

3.2 Auswertung des Anzeigeverhaltens (bei internetspezifischen Melde-Portalen)

Eine weitere interessante Alternative zur Systematisierung und Verbreiterung des empirischen Wissens im Bezug auf die modernen Internetdelikte stellen die verschiedenen Melde-Portale dar, bei denen man eigene Deliktsbetroffenheiten relativ schnell und unkompliziert ‚online' melden und anzeigen kann.

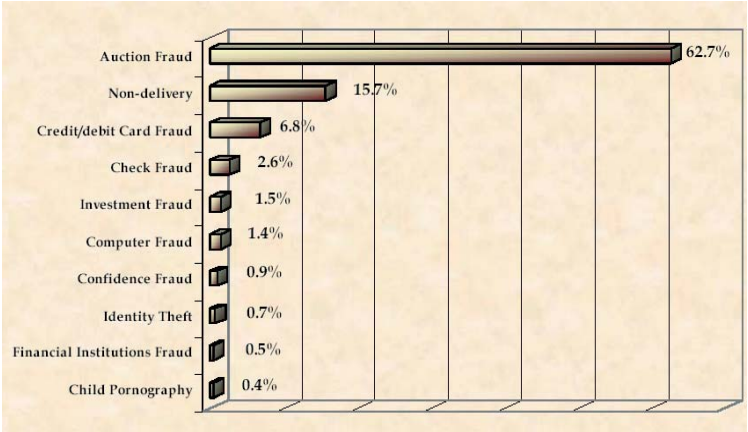
3.2.1 Daten des Internet Crime Complaint Center (IC3) aus den USA

In den Vereinigten Staaten von Amerika wurde zu Beginn des Jahrtausends unter der Federführung des FBI das so genannte ‚Internet Fraud Complaint Center' (IFCC) eingerichtet, auf dessen Internetseite man vorwiegend solche Betrugsdelikte melden sollte, die im weitesten Sinne einen Zusammenhang mit dem Internet aufweisen können. Im Jahre 2003 wurde die Zuständigkeit auf möglichst alle netz-bezogenen Delikte ausgeweitet und der Institutsname entsprechend in ‚Internet Crime Complaint Center' (IC3) geändert.

Während zu Beginn im Jahr 2000 deutlich weniger als 50.000 Delikte gemeldet wurden, waren es im Jahr 2005 bereits insgesamt 231.493, welche im neuesten Jahresbericht auch in ihrer Deliktsstruktur veröffentlicht worden sind. Danach bezieht sich der Löwenanteil von 62,7 Prozent der Fälle (= 145.146) auf den so genannten Auktionsbetrug. Der durchschnittlich gemeldete Schaden in diesem Bereich beträgt 385,00 $. Alle anderen Betrugsdeliktsarten sind demgegenüber prozentual deutlich geringer vertreten. Dies mag u.a. auch daran liegen, dass das größte Online-Auktionshaus eBay seit einiger Zeit einen direkten Link zur Homepage von IC3 geschaltet hat, was die Anzeigewahrscheinlichkeit und letztendlich auch die realisierte Anzeigehäufigkeit durchaus erhöht.

[15] Es erscheint interessant, zu erwähnen, dass ca. 10% der befragten 18-25-jährigen Personen des OCJS 2004 immerhin einen Versicherungsbetrug zugegeben haben. Das am meisten begangene Delikt in dieser Personengruppe ist mit (nur ?) 26% das illegale Herunterladen von Software, Musik und Filmen.

Internet Fraud Crime Report 2005
Die 10 häufigsten beim IC3 gemeldeten Delikte



Quelle: http://www.ic3.gov/media/annualreport/2005_IC3Report.pdf

3.2.2 Daten der nationalen US-Verbraucherschutz-Organisation NCL (Internet Fraud Watch)

Unter der Internetadresse *www.fraud.org* hat die National Consumers League (NCL) in den USA bereits seit dem Jahre 1997 eine weitere Plattform geschaffen, um speziell Betrugsdelikte im Zusammenhang mit dem Internet anzuzeigen. Auch hier machen die Auktionsbetrugsdelikte seit Jahren den größten Anteil aus. Die aktuellsten im Netz veröffentlichten Zahlen des Jahres 2005 haben einen Gesamtumfang von (nur) 12.315 und sind somit deutlich geringer als die oben dargestellten Zahlen von IC3. Auch der Anteil der Auktionsdelikte liegt hier (wenn auch wiederum an der Spitze) so doch ‚nur' bei 42 Prozent und somit klar unter 50 Prozent. Dies lässt sich in erster Linie damit erklären, dass das Auktionshaus eBay (aus welchen Gründen auch immer) im Frühjahr 2003 seinen bis dahin bestehenden Link zur Website der NCL gelöscht hat. Nach Angaben der NCL im entsprechenden Trendbericht 2005 ist daraufhin die Anzahl der Auktionsbetrugsmeldungen auf ca. 1/6 des früheren Niveaus zurückgegangen. *‚Based on statistics prior to eBay's action, NCL estimates that there would have been 30.720 auction complaints in 2005, representing 71 percent of complaints overall.'* Dies zeigt, wie sehr derartige Zahlen über das Anzeigeverhalten von den jeweiligen institutionellen Rahmenbedingungen abhängig sind. Insoweit dürfen derartige Daten nicht als 1:1-Abbildungen der zugrunde liegenden, realen Deliktsvorkommen interpretiert werden, sondern sie müssen in erster Linie als Konsequenz der vorhandenen Melde- und Kontrollstrukturen und somit als soziales Konstrukt gesehen werden.[16]

[16] Diese Erkenntnis bezieht sich grunds. auch auf alle anderen datenmäßigen u. statistischen Erfassungen von Deliktsphänomenen; sie ist ein wichtiger und unverzichtbarer Bestandteil der kriminol. Forschung seit der Diskussion um den so genannten Definitionsansatz zu Beginn der 70-er Jahre des vorigen Jahrhunderts.

4 Fazit und Ausblick

Bei aller Berücksichtigung der sozialen Konstruiertheit, Vorläufigkeit und Vagheit des vorhandenen empirischen Wissens zur Verbreitung und Häufigkeit der Betrugsdelikte im Zusammenhang mit dem Internet[17] kann man unter dem Strich dennoch zu einigen übereinstimmenden Erkenntnissen gelangen, welche in der Regel nicht grundsätzlich zu hinterfragen sind und welche zumindest deutliche Tendenzen erkennen lassen.[18] Es gibt einerseits vor dem Hintergrund der gesellschaftlichen Veränderungsprozesse der ‚digitalen Revolution' deutliche Anzeichen für eine mehr oder weniger selbstverständliche Zunahme von Betrugsdelikten im Zusammenhang mit den immer wichtiger werdenden neuen Telekommunikationsformen speziell auch im Internet. Es gibt andererseits nach allen Indikatoren, die uns zur Verfügung stehen, jedoch auch keinen erkennbaren Anlass dazu, die spezielle Deliktslage zu dramatisieren und zu überzeichnen. Wie in vielen anderen Bereichen auch, ist für den angemessenen und wirksamen Umgang mit den neuen Phänomenen der ‚E-Devianz' zunächst einmal eine auf möglichst differenzierten Daten beruhende kritisch-rationale Analyse der Befundlage erforderlich. Gerade bei der jetzt schon erkennbaren breiten Ausdehnung dieser digitalen Delikte in den Bereich der bagatellartigen Massendelinquenz erscheint auch eine durchaus kritische Reflektion und Analyse der möglichen präventiven Rolle des Strafrechts und der Strafverfolgungsbehörden angezeigt.

Die Strafverfolgungsbehörden und in erster Linie die Polizei stehen angesichts der rasant zunehmenden Internetkommunikation vor der Aufgabe der Bewältigung eines neuen und zunehmenden Massendeliktsbereichs, welcher sich ja nicht nur auf die Online-Betrugsdelikte bezieht, sondern welcher speziell in Hinsicht auf die zahlreichen Jedermann-Delikte im Rahmen der Musik-, Video- und Softwarepiraterie die begrenzten Kapazitäten und Ressourcen der Polizei sehr stark herausfordern kann.[19]

Nicht nur angesichts der bekannten knappen finanziellen öffentlichen Mittel ist es dringend anzuraten, dass man sowohl auf der Ebene der strafrechtlichen Normsetzung (z.B. beim 2. Korb der Urheberrechtsreform und der dort anstehenden Formulierung von Bagatellklauseln bei Privatkopien) als auch auf der Ebene der polizeilichen Organisation und Aufgabenbewältigung eine gewisse Spezialisierung und Konzentration auf die besonders

---

[17] Siehe hierzu auch den Beitrag des australischen Kriminologen: Smith, Russel G., Internet-Related Fraud: Crisis or Beat-Up? Canberra 2001. (Conference-Paper, Australian Institute of Criminology) unter: *http://www.aic.gov.au/conferences/outlook4/SmithIRF.pdf*

[18] Siehe hierzu auch die aktuellen Ergebnisse des CSI/FBI Computer Crime and Security Survey 2006.

[19] Neben dem gesamten Bereich der Urheberrechtsdelikte (Texte-, Film-, Musik-Piraterie), von dem speziell die jugendlichen und jungen Internetnutzer betroffen sind, ist hier auch an die rasant wachsende Zahl der so genannten Spam-Mails zu denken, von denen mehr oder weniger jeder Netzteilnehmer betroffen ist und welche sich zu einer Art Massenplage ausweiten. Hier zur Regelung das Strafrecht heranzuziehen, erscheint aus mehreren Gründen genauso verfehlt wie wirkungslos.

komplexen und schädlichen ‚Cyber-Crimes' (gewerbsmäßig und organisiert betrieben, wie z.B. Identitäts-Diebstahl oder Geldwäsche über das Internet) anzielt und die Kontrolle der bagatellartigen Massendelikte eher anderen präventiven und technischen Regelungsmechanismen überlässt, für die in erster Linie die beteiligten und betroffenen gesellschaftlichen Gruppen, wie z.B. die einschlägige Wirtschaft, die Musik- und Filmindustrie und der Online- und Auktionshandel selbst zuständig sind.[20]

Das Kommunikationssystem des Internet ist zudem ein System, welches vor allem auf technologischen Entwicklungen und Strukturen basiert und welches sich keinen nationalen Grenzen unterwirft, sondern mehr oder weniger grenzenlos funktioniert. Allein schon diese beiden Systemeigenschaften machen plausibel, dass das Strafrecht als rein rechtliches und vorwiegend nationales Regelungssystem hier an seine eigenen Grenzen stößt und eher unpassend und systemfremd wirkt, was nicht heißen muss, das es vollkommen verzichtbar ist. Die Regelungsprioritäten liegen beim Internet-System jedoch noch klarer als im klassischen gesellschaftlichen Kommunikationssystem bei der Prävention, bei technischen Schutzmaßnahmen[21] und bei der gezielten und bewussten Aufklärung hierüber.[22]

Literatur

Eichenberg, Christiane/ Rüther, Werner. Prävention von Devianz rund um das Internet. Ein Ausblick auf Handlungs- und Forschungsfelder. (in diesem Band)

Gordon, Lawrence A., u.a.. CSI/FBI Computer Crime and Security Survey 2006. Online-Präsentation vom September 2006. unter *http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf*

Heinz, Wolfgang. Jugendkriminalität zwischen Verharmlosung und Dramatisierung oder: (Jugend-)Kriminalpolitik auf lückenhafter und unzulänglicher Tatsachengrundlage. In: DVJJ-Journal, Jg. 8, Nr. 3, Seite 270 - 293

Internet Crime Complaint Center (IC3). Internet Fraud Crime Report 2005. unter *http://www.ic3.gov/media/annualreport/2005_IC3Report.pdf*

Lessig, Lawrence. Der Code und andere Gesetze des Cyberspace. Berlin 2001

[20] Siehe hierzu auch die in diesem Band thematisierten Selbstregelungsmechanismen und vertrauensbildenden Effekte im Zusammenhang mit Online-Auktionen. (speziell der Beitrag von: Wehrli, Stefan, Betrugsprävention durch Reputationssysteme)

[21] Siehe in diesem Zusammenhang das sehr interessante und anregende Buch des us-amerikanischen Rechtsprofessors Lawrence Lessig, Der Code und andere Gesetze des Cyberspace. Berlin 2001

[22] Siehe hierzu vor allem auch den zusammenfassenden Beitrag am Schluss dieses Bandes: Eichenberg, Christiane/ Rüther, Werner, Prävention von Devianz rund um das Internet. Ein Ausblick auf Handlungs- und Forschungsfelder.

National Consumers League/ National Fraud Information Center (USA). Internet Scams. Fraud Trends January-December 2005. unter *http://www.fraud.org/2005_Internet_Fraud_Report.pdf*

Rüther, Werner. Neue Medien, neue Formen der Massendelinquenz und neue Herausforderungen für die Prävention. In: forum kriminalprävention, 2/2005, S.3-5

Rüther, Werner. Die Online-Strafanzeige als neues Instrument der strafrechtlichen Sozialkontrolle. Erste empirische Erkenntnisse und geplante Projekte in einem bisher weitgehend unerforschten Gebiet. In: BKA, Hrsg., Forum KI 1 – 2005, S. 1 – 20 unter *http://www.bka.de/kriminalwissenschaften/kiforum/kiforum2005_dr_ruether.pdf*

Smith, Russel G.. Internet-Related Fraud: Crisis or Beat-Up? Canberra 2001. (Conference-Paper, Australian Institute of Criminology) unter *http://www.aic.gov.au/conferences/outlook4/SmithIRF.pdf*

Wehrli, Stefan. Betrugsprävention durch Reputationssysteme. (in diesem Band)

Wilson, Debbie u.a.. Fraud and technology crimes. Findings from the 2003/04 British Crime Survey, the 2004 Offending, Crime and Justice Survey and administrative sources. Home Office, Online Report 09/2006 unter *http://www.homeoffice.gov.uk/rds/pdfs06/rdsolr0906.pdf*

Zu den Grenzen der Technik bei der Entwicklung von Konzepten zur Online-Betrugs-Prävention

Ivan Martinovic & Jens Schmitt

Obwohl das Internet zwar als unsicher gilt und manchmal sogar als gefährlich bezeichnet wird, gibt es immer mehr Menschen, die privat oder beruflich auf das Internet nicht mehr verzichten können und wollen. Aspekte der Sicherheit werden somit immer wichtiger. Leider will der typische Internetnutzer möglichst wenig bis gar nicht mit den entsprechenden Verfahren konfrontiert werden, sondern will einfach seine Arbeit erledigen.

Die bereits heute zur Verfügung stehenden Sicherheitstechnologien bieten eine Vielzahl von Methoden, welche bestimmte Angriffsszenarien unmöglich machen. Diese Mechanismen sind von einem technischen Standpunkt aus gesehen sehr effektiv, durch die soziotechnische Interaktion mit dem typischen Internetnutzer ergeben sich aber weitere Sicherheitsproblematiken.

In diesem Beitrag beschreiben wir das wachsende Problem der sicheren Kommunikation im Internet. Kapitel 1 gibt eine kurze Übersicht über die Geschichte der technischen Sicherheit und die wichtigsten Sicherheitsmaßnahmen, die uns die heutige Internettechnologie bietet. Warum das noch immer nicht ausreicht, um den Internetbenutzer effektiv zu schützen, wird in Kapitel 2 diskutiert. In Kapitel 3 wir dann das so genannte *Social Engineering* als wohl erfolgreichstes Paradigma aktueller Angriffe diskutiert. Eine Zusammenfassung und Diskussion der identifizierten Herausforderungen wird in Kapitel 4 gegeben.

1 Eine kurze Geschichte der Sicherheit

Die Sicherheitsziele bei der Kommunikation im Internet spiegeln die Sicherheitsanforderungen, wie wir sie aus der realen Welt kennen, wider. Die Informationen, die wir bekommen, sollen einen vertrauensvollen Ursprung haben, sie sollen nicht unterwegs verändert werden können, der Zugang zu Informationen darf nur autorisierten Personen gestattet werden und Ursprung oder Änderung von Informationen soll rückverfolgbar sein.

Um diese Sicherheitsziele zu gewährleisten, wurde eine Vielzahl an Methoden und Protokollen entwickelt (für eine detaillierte technische Darstellung empfiehlt sich [3], [4]). Eine grobe Kategorisierung von Sicherheitsverfahren ist anhand grundlegender Konzepte aus der Kryptographie möglich [2]. Es wird hauptsächlich zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren unterschieden.

Symmetrische Verfahren basieren auf dem gleichen Schlüssel für Ver- und Entschlüsselung. Die Idee zu symmetrischen Verfahren war schon in der Antike bekannt, so z.B. das nach Julius Cäsar benannte *Cäsar-Chiffre,* bei dem man jeden Buchstaben mit dem um drei Positionen entfernten Buchstaben ersetzt (z.B. wird A zu D, B zu E und X zu A). Der

Schlüssel für Ver- und Entschlüsselung ist dann gerade das Wissen über die Verschiebung der Buchstaben um drei Positionen im Alphabet (reihum). Der Vorteil, dass der gleiche Schlüssel für Verschlüsselung und Entschlüsselung genutzt wird, wird aber gerade in der heutigen Zeit zu einem großen Nachteil. Da es nur einen Schlüssel gibt, stellt sich die Frage des sicheren Schlüsselaustauschs zwischen den beiden Kommunikationspartnern. Dies ist insbesondere in der digitalen Welt, wo sich beide Teilnehmer an verschiedenen Orten der Welt befinden können und sich vielleicht noch nie persönlich kennen gelernt haben, ein schwieriges Problem, da der Schlüsselaustausch über einen sicheren Kanal (zum Beispiel ein persönliches Treffen) stattfinden muss, was hier jedoch schwierig zu erreichen ist. Obwohl der Schlüsselaustausch bei symmetrischen Verfahren ein großes Hindernis darstellt, sollen die Vorteile von symmetrischen Verfahren nicht verschwiegen werden. Symmetrische Verfahren sind sehr schnell ausführbar und lassen sich effizient in Hardware implementieren, zudem sind sie aufgrund ihrer langen Historie sehr gut erforscht. Darum werden auch heute noch symmetrische Verschlüsselungsverfahren in vielen Bereichen eingesetzt, insbesondere in Netzwerkprotokollen und verschiedenen Chipkarten (Smartcards). Zu den bekanntesten Verschlüsselungsverfahren, welche auf symmetrischer Kryptographie basieren, zählen u.a. DES (Data Encrypton Standard), das 1976 zum Standard erklärt wurde, heute aber nicht mehr als sicher gilt und AES (Advanced Encryption Standard), der DES-Nachfolger, welcher 2001 zum Standard erklärt wurde.

Eine Revolution der Kryptographie fand Anfang 1970 durch die Erfindung der asymmetrischen Kryptographie von Whitfield Diffie, Martin Hellman und Ralph Merkle statt. Eines der ersten und bekanntesten Verfahren, die auf asymmetrischen Konzepten beruhen, ist das von Ronald L. Rivest, Adi Shamir und Leonard M. Adleman entwickelte RSA-Verfahren. Durch asymmetrische Kryptographie ist es möglich geworden, zwei verschiedene Schlüssel zu erzeugen, so dass ein Schlüssel der Verschlüsselung (*öffentlicher Schlüssel*) und der andere der Entschlüsselung (*privater Schlüssel*) dient. Das Herleiten eines der beiden Schlüssel aus dem anderem gilt als praktisch unmöglich und bietet dadurch die Möglichkeit zu einer neuen Art der Schlüsselverteilung. Die Idee ist, dass der öffentliche Schlüssel jedem zugänglich ist (jeder sollte eine Nachricht verschlüsseln können), und der für die Entschlüsselung benutzte private Schlüssel nur seinem Besitzer bekannt bleibt (nur der Besitzer soll die verschlüsselten Nachrichten lesen). Dadurch wird ein Austausch der geheimen Schlüssel vollständig vermieden.

Die asymmetrische Kryptographie, auch *Public-Key* Kryptographie genannt, realisiert noch weitere Verfahren, welche versuchen Sicherheitsmechanismen, wie wir sie aus der realen Welt kennen, in das digitale zu übertragen. So werden durch Public-Key Kryptographie auch digitale Signaturen (manchmal elektronische Unterschriften genannt) und digitale Zertifikate realisiert. Digitale Signaturen bestätigen die Authentizität und Integrität von Nachrichten (analog zu menschlichen Unterschriften). Bei jeder signierten Nachricht, kann die Authentizität der Nachricht eindeutig bestimmt und jede Veränderung erkannt werden. Obwohl die Public-Key Kryptographie den Austausch von geheimen Schlüsseln unnötig macht, besteht noch immer die Gefahr, dass der öffentliche Schlüssel,

welcher jetzt über einen unsicheren Kommunikationskanal verteilt werden kann (z.B. kann man ihn per E-Mail senden oder auf der eigenen Webseite veröffentlichen) nicht dem wahren Besitzer gehört. Ein Angriff, der auf der Vortäuschung der Zugehörigkeit eines öffentlichen Schlüssels zu einem bestimmten Benutzer basiert, ist ein sog. Man-In-The-Middle Angriff (MITM). MITM ist eines der erfolgreichsten Angriffsparadigmen überhaupt (das bekannte Phishing ist auch eine Art des MITM Angriffes, bei dem man das Vertrauen in eine E-Mail durch die Fälschung der Absenderadresse ausnutzt).

Um die Zugehörigkeit des öffentlichen Schlüssels zu schützen und prüfbar zu machen, wurden *digitale Zertifikate* entwickelt. Diese sind vergleichbar mit einem Personalausweis, in dem der öffentliche Schlüssel an die Identität einer Person oder Institution gebunden wird. Digitale Zertifikate werden von Zertifizierungsstellen (auch Trusted Third Parties genannt) ausgegeben und beinhalten die Identität des Benutzers, seinen öffentlichen Schlüssel und weitere Daten wie E-Mail-Adresse, Gültigkeitsdauer sowie die digitale Signatur der Zertifizierungsstelle.

In der folgenden Tabelle, sind die wichtigsten Begriffe der Public-Key Kryptographie kurz zusammengefasst und aufgelistet.

Name	**Bedeutung**
Öffentlicher Schlüssel	Dient der Verschlüsselung der Nachrichten und ist öffentlich bekannt.
Privater Schlüssel	Dient der Entschlüsselung der Nachrichten und darf nur seinem Besitzer bekannt sein.
Digitale Signatur	Gewährleistet die Authentizität und Integrität der Nachricht.
Digitales Zertifikat	Bindet den öffentlichen Schlüssel an die Identität des wahren Benutzers (und schützt damit die Zugehörigkeit des öffentlichen Schlüssels).
Zertifizierungsstelle	Herausgeber eines digitalen Zertifikates und muss eine vertrauenswürdige Institution sein.

Tabelle: Public-Key Sicherheitsmaßnahmen

Als technischer Nachteil der Public-Key Kryptographie ist hauptsächlich die geringe Ausführungsgeschwindigkeit der entsprechenden Verfahren zu nennen, so dass in der Praxis oft eine Mischung aus symmetrischen und asymmetrischen Verfahren vorzufinden ist. Dabei wir der problematische Schlüsselaustausch am Anfang einer Kommunikation durch Public-Key Kryptographie übernommen, mit deren Hilfe sich die beiden Kommunikationspartner auf einen gemeinsamen und geheimen Sitzungsschlüssel einigen. Der Sitzungsschlüssel wird dann weiter für die symmetrische Datenver- und -entschlüsselung benutzt. Ein solches ‚gemischtes' Verfahren wird auch als *hybrid* bezeichnet und ist heute der de-facto Standard jeder sicheren Kommunikationsverbindung.

Als ein weiterer Nachteil der Public-Key Kryptographie wird oft die Annahme einer vertrauensvollen Zertifizierungsstelle genannt. Das Problem dabei soll hier vereinfacht darge-

stellt werden: Wenn Alice eine vertrauliche Nachricht an Bob senden möchte, muss sie den richtigen öffentlichen Schlüssel von Bob haben und fragt dafür die Zertifizierungsstelle, die Bobs öffentlichen Schlüssel zertifiziert hat. Dabei wird jedoch angenommen, dass Alice und Bob immer eine gemeinsame vertrauenswürdige Zertifizierungsstelle haben. Ob das immer realistisch ist, wird oft als Nachteil angeführt, wobei die Diskussion darüber gelegentlich philosophische Züge annimmt, auf die wir hier jedoch nicht weiter eingehen möchten. Wichtig ist festzuhalten, dass keine dieser Nachteile oder streitbaren Annahmen bei den heutigen Angriffen, die im Internet stattfinden, eine wirklich signifikante Rolle spielen. Das einzige was aktuelle Angriffe ausnutzen, ist das beim heutzutage typischen Internetbenutzer geringe Wissen über Sicherheitsverfahren. Und das leider mit großem Erfolg.

2 Sicheres Surfen – von Theorie zur Praxis

Wie im vorangehenden Kapitel beschrieben, bietet auch die heutige Internettechnologie bereits eine Vielzahl an Sicherheitsmethoden. Obwohl diese Methoden aus technischer Sicht jeden heutigen Angriff (wie z.B. Phishing) abwehren können, ist die Anzahl erfolgreicher Angriffe stark gestiegen. Laut [5] wurden zwischen Mai 2005 und Mai 2006 die bislang höchste Zahl von über 20.000 unterschiedlichen (und einzigartigen) Phishing-Angriffen gemeldet sowie über 11.000 Webserver entdeckt, welche eine gefälschte Webseite anbieten. Im März 2006 zählten Banken zu den meist angegriffenen Institutionen. Dies bekräftigt auch die Vermutung, dass die gestohlenen Kundeninformationen (Login, Password, PIN und TANs) ‚erfolgreich' wirtschaftlich ausgenutzt werden. Die Gründe für einen solchen Erfolg der Phishing-Angriffe werden im Folgenden kurz anhand von zwei Szenarien beschrieben.

Szenario 1

Alice möchte Ihre Rechnungen über das Onlineportal Ihrer Bank zahlen. Sie ruft mit Ihrem Browser die Webseite der Bank auf. Der Browser übernimmt die Authentifizierung und sorgt für eine sichere Verbindung zwischen der Bank und Alices Browser. Im Falle, dass der Browser das Zertifikat der Bank nicht als vertrauenswürdig einstuft (d.h. die Zertifizierungsstelle ist dem Browser nicht bekannt), muss Alice entscheiden, ob das Zertifikat akzeptiert wird oder nicht. Sie prüft das digitale Zertifikat des Onlineportals auf Vertrauenswürdigkeit (ist das Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle ausgegeben und ist es gültig) sowie, ob das Zertifikat wirklich das Onlineportal der Bank authentifiziert. Dadurch kann Alice sicher sein, dass sie mit dem Portal ihrer Bank verbunden ist.

Szenario 2

Alice bekommt eine E-Mail, die sehr überzeugend von ihrer Bank zu sein scheint und sie auffordert wegen Systemreorganisationen ihr Login, PIN und zehn gültige TANs anzugeben. Sie prüft die Vertrauenswürdigkeit der digitalen Signatur der E-Mail ihrer Bank

und stellt fest, dass sie falsch ist oder die E-Mail gar nicht signiert wurde und dadurch nicht authentisch ist. Es ist einfach für Alice, die E-Mail als einen Phishing-Versuch zu erkennen und ihre TANs für sich zu behalten.

Für beide Szenarien gilt, dass Alice in der Lage ist, digitale Zertifikate und digitale Signaturen zu verstehen und zu prüfen, ob sie wirklich von einer akkreditierten und vertrauenswürdigen Zertifizierungsstelle stammen. Diese Voraussetzung ist das mindeste an Wissen, was die technische Sicherheit heute von einem Internetbenutzer erwartet, und wenn das tatsächlich erfüllt wird, ist es sehr unwahrscheinlich, dass ein erfolgreicher Angriff stattfinden kann.

Leider aber sieht die Realität ganz anders aus:

1. Alice kennt keine Public-Key Kryptographie, sie möchte einfach ihre Rechnungen zahlen und nutzt das Internet, um das Warten in der Bankfiliale zu vermeiden.

2. Die Bank benutzt standardmäßig keine signierten E-Mails (dadurch wird Alice auch nicht motiviert, die Sicherheitsmaßnahmen kennen zu lernen), sodass Alice bei gefälschten (Phishing) E-Mails, welche durchaus sehr überzeugend sein können, das Risiko und die Gegenmaßnahmen überhaupt nicht richtig wahrnimmt.

Auf diesen Tatsachen basieren heute die meisten Angriffe im Internet. Warum sollte man komplexe kryptographische Protokolle angreifen, wenn ein System genauso sicher ist wie sein schwächstes Glied, und das ist nun mal der Benutzer? Die Benutzer haben eine subjektive Wahrnehmung und Risikoabschätzung, die hauptsächlich auf ihrem persönlichen Wissen basiert. Die Möglichkeiten von Angriffen, die Naivität und Gutgläubigkeit von Benutzern ausnutzen, sind groß und werden häufig unter dem Begriff *Social Engineering* zusammengefasst. Beim Social Engineering versucht man, durch plausible und anscheinend bekannte Informationen das Vertrauen des Benutzers zu erschleichen, um ihm persönliche und wichtige Benutzerdaten zu entlocken.

3 Der Erfolg des Social Engineering

Der Erfolg des Social Engineering ist gewaltig und die Ursachen dafür liegen auf beiden Seiten – komplexe Technologie und unvorbereitete Internetbenutzer.

Das Profil und die Anzahl der Internetbenutzer haben sich mit der Zeit sehr stark verändert. Das Internet und Internettechnologien wie z.B. World Wide Web, E-Mail und Voice-over-IP (VoIP) haben Interesse bei vielen Menschen geweckt und die Anzahl der Internetbenutzer ist dementsprechend stark gestiegen (im Jahr 2006 gibt es mehr als eine Milliarde Internetbenutzer [6]). Der typische Internetbenutzer ist nicht mehr der gleiche wie vor zehn Jahren, als schon ein Zugang zum Internet ein gewisses technisches Wissen (und entsprechenden Enthusiasmus) an Betriebssystem-, Modem- und Verbindungseinrichtung zur Voraussetzung hatte.

Heute sind die Internetbenutzer Leute, die Technik und IT-Welt nicht als oberste Priorität ihrer Beschäftigung sehen, sondern das Internet nur als Werkzeug zur Unterstützung ihrer Arbeit verwenden. Ein bekannter Sicherheitsexperte beschrieb dies folgendermaßen:

> *‚People don't understand computers. Computers are magical boxes that do things. People believe what computers tell them. People just want to get their job done.' [1].*

Auf der anderen Seite muss man auch feststellen, dass die Technologie äußerst komplex geworden ist und dass bei Konzipierung der Sicherheitslösungen die veränderten Charakteristika von Internetbenutzern nicht berücksichtigt wurden. Wie realistisch ist es, zu erwarten, dass jeder Internetbenutzer die im ersten Kapitel beschriebenen Sicherheitsmechanismen gut versteht und richtig bedient? Als Beispiel soll hier die Realisierung einer sicheren Verbindung dienen:

Beim Aufbau einer sicheren Verbindung zwischen einem Browser und einer Website wird bei jedem Zertifikat, das der Browser noch nicht kennt, der Benutzer gefragt, ob er es akzeptieren möchte. Zur Auswahl stehen typischerweise folgende Optionen:

- ‚Dieses Zertifikat immer akzeptieren',
- ‚Dieses Zertifikat temporär (für diese Sitzung) akzeptieren',
- ‚Dieses Zertifikat nicht akzeptieren und nicht mit dieser Website verbinden'.

Die von dem Browser vorgegebene Antwort ist *‚Dieses Zertifikat temporär (für diese Sitzung) akzeptieren'*. Dadurch wird diesem Zertifikat nur einmalig vertraut und bei der nächsten Sitzung wird der Benutzer wieder mit der gleichen Frage konfrontiert. Ohne in eine psychologische Analyse zu verfallen, wie oft haben Sie ‚Dieses Zertifikat permanent akzeptieren' gewählt?

Auch wenn Sie Zertifikate richtig prüfen können, das ‚permanente' Akzeptieren wird nicht von dem Browser standardmäßig vorgeschlagen, und dies verunsichert einen typischen Benutzer. Er wird daher lieber der vorgeschlagenen Antwort des Browsers folgen und das Zertifikat nur temporär akzeptieren, was dann bei jeder weiteren Sitzung den Benutzer wieder vor die gleiche Wahl stellt. Mit der Zeit gewöhnt sich der Benutzer daran, schnell auf den Vorschlag des Browsers zu hören, um sich zügig weiter seiner eigentlichen Aufgabe widmen zu können. Obwohl in den meisten Fällen dieser Automatismus keine weiteren Folgen hat, kann es in Ausnahmen passieren, dass ein gefälschtes Zertifikat angeboten wird, um einen Man-In-The-Middle Angriff zu starten.

4 Diskussion

Das Paradoxon der Sicherheit – *‚Jeder will sie haben, aber keiner will sie sehen'*[1].

In diesem Kapitel stellen wir ein paar Diskussionspunkte vor, die uns helfen sollen, die Sicherheitsproblematik des heutigen Internet besser zu verstehen und den Internetbenutzer besser zu schützen.

Sicherheitsmaßnahmen standardmäßig benutzen

Die erfolgreiche Abwehr von Angriffen im Internet wird durch verschiedene Faktoren beeinflusst. Auf der einen Seite ist der Internetnutzer gefordert, sich mit dem Thema Sicherheit im Internet aktiv zu beschäftigen, auf der anderen Seite sollte die Technologie auch dem durchschnittlichen Internetbenutzer ‚näher' kommen. Bisher wurde E-Mail als Medium zwischen Dienstanbieter und Kunde hauptsächlich für den Austausch von unpersönlichen und nicht vertrauenswürdigen Daten benutzt. Dadurch waren ausgefeilte Sicherheitsmechanismen nicht notwendig. Dienstanbieter hatten möglicherweise auch nie vorgesehen, E-Mail aktiv für den Austausch von persönlichen Informationen zu nutzen, aber der Kunde wusste das leider nicht. Als die erste Welle mit Phishing E-Mails auftrat, waren beide Parteien unvorbereitet. Um Sicherheitsmaßnahmen und Risiken dem Benutzer näher zu bringen, sollten Dienstanbieter aktiv Sicherheitsmaßnahmen standardmäßig benutzen – wie z.B. E-Mails mit digitalen Signaturen und Zertifikaten. Dadurch wird auch der Benutzer gefördert, sich damit aktiv zu beschäftigen.

Informierte Kunden

Eine der wichtigsten Maßnahmen gegen Angriffe, die auf dem Social Engineering basieren, ist der informierte Kunde. Dadurch, dass Phishing Angriffe eine epidemische Natur haben und für den Erfolg stark verbreitet werden müssen, können sie nicht lange unentdeckt bleiben. Die Informationen über Sicherheitsmaßnahmen und aktuelle Angriffe müssen Thema der Kommunikation zwischen Kunde und Dienstanbieter sein. Die Entscheidung des Dienstanbieters das Internet als einen weiteren Vertriebskanal zu verwenden, bedeutet auch dafür zu sorgen, dass der Kunde geschützt und informiert bleibt.

Angepasste Technologie

Wenn Sicherheitsmechanismen zu viel Zeit in Anspruch nehmen und die eigentliche Aufgabe des Benutzers unterbrechen, werden sie nicht beachtet und sehr oft ausgeschaltet. Dadurch werden gerade Social Engineering Angriffe noch effizienter und einfacher zu gestalten. Wie bereits angedeutet, haben sich die Anzahl und das Profil des Internetbenutzers in den letzten Jahren stark verändert. Bei der Konzipierung von Sicherheitsmechanismen muss von einem realistischen Benutzerprofil ausgegangen werden. Dazu gehört auch die Annahme über das technische Wissen des Benutzers und seine Risikowahrnehmung. Gerade die Social Engineering Angriffe basieren auf der Tatsache, dass ein Benut-

zer in eine Ausnahmesituation versetzt wird und dadurch ein übereiltes Handeln erzwungen wird. Die Frage, die sich hier stellt, ist: Wer ist hier der Experte, der Benutzer oder der Rechner (ergo der Systemadministrator) und wer soll die Entscheidung treffen?

Zusammenfassend ist zu sagen, dass auf dem Weg zu einer sicheren Kommunikation im Internet zwei Entwicklungswege beschritten werden sollten. Einerseits sollte die Sicherheitsforschung verstärkt auf die Eigenschaften des typischen Internetnutzers fokussieren (wie es das Social Engineering auch macht), andererseits ist es von zentraler Bedeutung, dass die Dienstanbieter im Internet ihre Kunden bezüglich der Sicherheitsproblematiken aufklären.

5 Referenzen

[1] B. Schneier, Secrets and Lies: Digital Security in a Networked World, John Wiley & Sons, 1 Edition, 2001.

[2] G. Schäfer, Netzsicherheit – Algorithmische Grundlagen und Protokolle, dpunkt.verlag, 2003.

[3] C. Eckert, IT-Sicherheit. Konzepte – Verfahren – Protokolle, Oldenbourg Verlag, 2006.

[4] J. Buchmann, Einführung in die Kryptographie, Springer Verlag, 2003.

[5] APWG: Anti-Phishing Working Group, *http://www.antiphishing.org*, (zugegriffen Juni 2006).

[6] Internet World Stats – Usage and Population, *http://www.internetworldstats.com*, (zugegriffen Juni 2006).

Betrugsprävention durch Reputationssysteme

Stefan Wehrli

1 Das Vertrauensproblem im Online-Handel

Tauschhandlungen auf Internet-Marktplätzen – insbesondere Online-Auktionen als deren häufigste Transaktionsart – sind nach wie vor mit einem Risiko verbunden, das aus der zeitlichen und räumlichen Trennung der Tauschpartner entsteht. Wird der Verkäufer liefern, nachdem der Käufer die Ware bezahlt hat? Entspricht der Paketinhalt der deklarierten Qualität? Dies sind Fragen, die sich ein Nutzer angesichts der ungünstigen Ausgangslage zu Recht stellt. Da Verkäufer bei Auktionen ihre Bieter nicht aussuchen können, verlangen sie in der Regel eine Vorauszahlung und sichern sich den Vorteil des ‚Second-Movers' (Diekmann und Wyder 2001). Der Käufer hat sprichwörtlich die Wahl, gegen Vorauskasse von einem Unbekannten eine ‚Katze im Sack' zu erwerben. Aufgrund der Größe dieser Marktplätze muss er weiter davon ausgehen, dass er seinen Interaktionspartner nicht wieder antreffen wird. In den Sozialwissenschaften wird dies als nicht wiederholtes Vertrauensspiel mit unvollständiger Information beschrieben (Ockenfels 2003, Akerlof 1970), eine Situation mit minimaler zeitlicher und sozialer Einbettung. Aus theoretischer Sicht wird man erwarten, dass ein Verkäufer das Vertrauen immer missbraucht und deshalb ein Käufer solche Angebote nie berücksichtigt. Tagtäglich findet aber eine große Zahl eben solcher Interaktionen statt. Ermöglicht wird dies durch ein Set von internen und externen Maßnahmen, die es im zweiten Teil zu diskutieren gilt.

Trotz der großen Zahl an Transaktionen, die scheinbar problemlos über Online-Marktplätze abgewickelt werden, bietet das Marktumfeld einen fruchtbaren Boden oder zumindest Nischen für opportunistisches und betrügerisches Verhalten. Tatsächlich gehört der Warenbetrug zu einer der am schnellsten wachsenden Deliktformen in der Bundesrepublik Deutschland. Betrug ist zugleich die häufigste Form von Internet-Delinquenz. Der polizeilichen Kriminalstatistik (2006:8) ist zu entnehmen: ‚Bei etwa vier Fünftel der Fälle mit Internet als Tatmittel handelt es sich um Betrugsdelikte (79,5 Prozent)'.

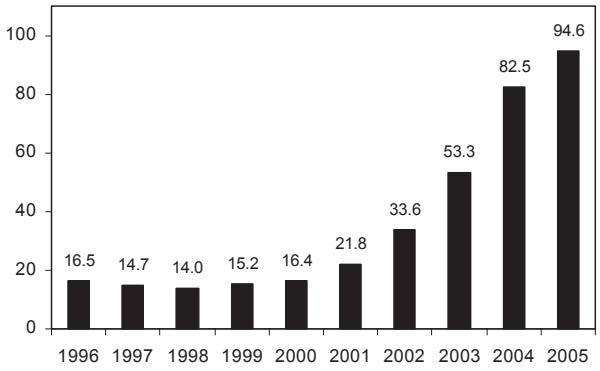


Abb. 1: Entwicklung des Warenbetrugs in der BRD 1996-2005 (in 1000).
Quelle: BMI, Polizeiliche Kriminalstatistik, Schlüssel 5113

Die Kennung ‚Tatmittel Internet' hat erst kürzlich eine Berücksichtigung in den öffentlichen Statistiken erhalten; den Zahlen wird man deshalb noch mit Vorsicht begegnen wollen. Der Kategorie Warenbetrug in Abbildung 1 kann man jedoch die besorgniserregende Dynamik entnehmen. Die Fallzahl hat sich seit 2000 etwa verfünffacht und steigt jedes Jahr weiter, wenn auch im letzten Jahr deutlich schwächer. Die Fallzahl gehört aber auch ins Verhältnis gesetzt. Im gleichen Zeitraum entwickelte sich der Handel im Internet mit weitaus höherer Wachstumsrate. Die Mitgliederzahl von eBay ist in diesem Zeitraum rasant auf ca. 20 Millionen Nutzer in der Bundesrepublik Deutschland gewachsen. Es war zu erwarten, dass mit zunehmender Transaktionszahl auch die Zahl devianter Fälle zunimmt. Und man darf hoffen, dass sich die Entwicklung des Warenbetrugs mit zunehmender Sättigung der Online-Märkte auf hohem Niveau stabilisieren wird.

Neben krimineller Energie und eigentlichen Betrugsfällen muss man in diesem Feld aber hauptsächlich mit Opportunismus und Übervorteilungen rechnen, die auf der Ebene der Produktqualität anzusiedeln sind. Um Käufer vor solchen Formen der Ausbeutung zu schützen, haben die großen Auktionsplattformen fast ausnahmslos Systeme eingeführt, die es den Beteiligten erlaubt, eine Qualitätsbewertung zu veröffentlichen. Diese Form der digitalisierten Mund-zu-Mund-Propaganda eröffnet vertrauenswürdigen Akteuren die Möglichkeit eine Reputation aufzubauen (Dellarocas 2003). Das einmalig gespielte Vertrauensspiel wird zeitlich eingebettet, indem man den Teilnehmern Sanktionschancen über das Bewertungsforum eröffnet. Dieser simple Mechanismus der Kooperationsförderung hat die wissenschaftliche Neugier geweckt. Zur Wirkungsweise solcher Reputationssysteme existiert mittlerweile eine große Zahl an wissenschaftlichen Studien.[1] Einige der zentralen Hypothesen sollen im dritten Teil an neuen Daten von ebay.de demonstriert werden.

2 Interne und externe Lösungen des Vertrauensproblems

In der Literatur werden Lösungen auf das oben skizzierte Kooperationsproblem oft in interne und externe Ansätze unterschieden. Wesentliches Abgrenzungskriterium ist dabei der Träger der Intervention. Externe Anreiz- und Sanktionssysteme werden von außen stehenden Dritten eingesetzt. Es wird dabei versucht, das Kräftegleichgewicht zugunsten der benachteiligten Partei anzupassen, indem die Interaktions- oder Auszahlungsstruktur verändert wird. Typischer Akteur ist in diesem Kontext jeweils der Rechtsstaat oder die Plattformbetreiberin. Auf einer ersten Ebene wird präventiv versucht, die ungünstigen

[1] Überblicke bieten Bajari und Hortaçsu (2004), sowie Resnick et al. (2003) für Studien über ebay.com für den U.S.-amerikanischen Markt. Diekmann und Wyder (2002), Snijders und Zijdeman (2004) und Berger und Schmitt (2005) zeigen neuere empirische Ergebnisse aus dem mitteleuropäischen Raum.

Rahmenbedingungen des Online-Handels durch bessere Information und Aufklärung über potentielle Risiken zu entschärfen. Es werden Identitätsprüfungen beim Eintritt ins System durchgeführt (z.T. kostenpflichtig). Mit technischen Hilfsmitteln wird versucht, die Kommunikationshürden zwischen den Handelspartnern zu entschärfen, um mit Text, Ton- und Bildübertragung an die klassischen Vorzüge eines Marktplatzes anzuschließen. Oder es werden Treffpunkte im öffentlichen Raum geschaffen, wo die Handelspartner die Transaktion gleich von Angesicht zu Angesicht abwickeln können.

Eine weitere Möglichkeit besteht darin, den Ablauf einer Transaktion zu modifizieren. Durch die Einführung von Rückgaberechten wird der Vorteil des ersten Spielzuges seitens des Verkäufers hinfällig. Produktgarantien verfolgen einen identischen Zweck. Private Anbieter schließen in der Regel aber beides aus, sodass Rückgaberechte nur eine Teillösung des Problems darstellen. Das Ausmaß an Online-Handel erlaubt mittlerweile auch, dass Plattformbetreiber ihre Kunden gegenüber unerwünschten Transaktionsergebnissen versichern können. All dies hat zur Folge, dass die ungünstige Interaktionsstruktur in eine Vielzahl von externen Maßnahmen eingebettet wird und der Online-Handel so an Sicherheit gewinnt. Derselbe technische Fortschritt, der den Online-Handel hervorgebracht hat, gibt den Plattformbetreibern und Strafverfolgungsbehörden auch neue Mittel zur Früherkennung und Überwachung. Benutzer von Online-Plattformen glauben sich zwar am heimischen PC in Sicherheit. Bei der Nutzung des Internet resultieren jedoch Spuren, die es den Behörden je länger je mehr ermöglichen, abweichendes Verhalten erfolgreich zu identifizieren und zu verfolgen. Im letzten Jahr wurden mehr als 90 Prozent der Fälle von Betrug im Internet aufgedeckt (BMI 2006: 55).

Aufgrund der rasanten Entwicklung des Online-Handels, insbesondere der großen Teilnehmerzahl, wurden die rechtsstaatlichen Institutionen jedoch überrascht und gelangten zugleich an die Grenzen ihrer Möglichkeiten. Dies führte dazu, dass sich die Rolle legaler Maßnahmen auf den subsidiären Einsatz im Sinne einer Ultima Ratio beschränkte. Erstens fehlten in den vergangen Jahren oft noch die gesetzlichen Rahmenbedingen, um des Problemfeldes des Online-Betrugs habhaft zu werden; insbesondere dann, wenn es sich um transnationale Transaktionen handelte. Die Lebensdauer von Online-Unternehmungen ist bisweilen so kurz, dass diese zum Zeitpunkt einer Strafverfolgung teilweise gar nicht mehr existieren. Zweitens hat die Anonymität und mangelnde Identifizierbarkeit der Beteiligten die polizeiliche Arbeit nicht erleichtert. Mit billigen Pseudonymen und kostenlosen E-Mail-Konten lassen sich die Spuren nach erfolgter Tat vergleichsweise einfach verwischen. Und nicht zuletzt stehen im Online-Handel die Kosten für eine rechtliche Durchsetzung oft in einem ungünstigen Verhältnis zum Streitwert. Gerade wenn es sich um kleine Transaktionsvolumina handelt, werden geprellte Käufer oder Verkäufer auf legale Sanktionen verzichten.

Neben den oben skizzierten externen Lösungsansätzen haben sich im Online-Handel mittlerweile weitere interne, von den Nutzern selbst organisierte Mechanismen etabliert, die mittels Vertrauens- und Reputationsbildung das Opportunismusproblem zu entschärfen

versprechen. Erstens handelt es sich dabei um Reputationssysteme (Bewertungsforen), die den Beteiligten nach Transaktionsabschluss ermöglichen, sich gegenseitig zu bewerten und falls notwendig zu sanktionieren. Zweitens erlauben einige Plattformanbieter den Benutzern, mittels glaubwürdigen Signalen (Hinweis einer geprüften Identität) als sicher und vertrauenswürdig aufzutreten. Ein Grenzfall zwischen internem und externem Mechanismus besteht in der Zuhilfenahme eines vertrauenswürdigen Dritten. Beim Treuhandservice werden Zahlung und Ware geparkt, sobald beide beim Treuhänder eingetroffen sind, werden sie an die Handelspartner weitergeleitet. Das Vertrauensproblem wird durch die gemeinsame Wahl eines Intermediärs umgangen, der im Schadensfall haftet, sich dafür jedoch entgelten lässt. Die Risikoprämie geht an den Treuhänder. Berger und Schmitt (2005) zeigen, dass zwischen Reputation und dem Treuhandangebot des Verkäufers ein klarer substitutiver Zusammenhang besteht. Wer erst eine bescheidene Reputation vorweisen kann, bietet mit höherer Wahrscheinlichkeit die Option der Treuhandlösung an. Käufer werden dadurch aber erst recht auf die fehlende Reputation aufmerksam und scheinen Angebote mit Treuhandservice zu meiden. Berger und Schmitt (2005) folgern: ‚Dies ist auch ein Hinweis darauf, dass von den Käufern Kooperation des Verkäufers offenbar als erwarteter Normalfall eingestuft wird, der nicht mit übertriebenen Maßnahmen garantiert werden muss.' Eine alternative Erklärung besteht darin, dass die Reputationsprämie an den Verkäufer in der Regel deutlich geringer ausfällt als die Kosten für einen Treuhänder. Die Zahlungsbereitschaft für Sicherheit in Online-Märkten ist offenbar sehr gering. Für das tiefe Risikosegment scheinen die Reputationslösung und die Versicherungen zu genügen. Die Treuhandlösung erscheint deshalb hauptsächlich als Option für besonders risikoreiche Transaktionen.

Sobald technische Systeme den Aufgabenbereich von Strafverfolgungsbehörden ergänzen oder gar ersetzen, desto wichtiger wird es für alle Beteiligten, ob solche Reputationssysteme auch in gewünschter Weise ihre Wirkung entfalten. Die Wirkungsweise des Reputationssystems von ebay.de soll in den folgenden zwei Abschnitten ausführlich diskutiert werden.

3 Das Reputationssystem von eBay

Einige Autoren gehen davon aus, dass es für das Funktionieren eines Reputationssystems genügt, wenn nur alle Beteiligten an dessen Wirkung glauben. Resnick und Zeckhauser (2001) bemerken: 'In a nutshell, it's not how the system works, but that its participants believe it works – even if they don't know why.' Sobald sich aber ein System mit Trial and Error ausbeuten lässt, wird ein solches nicht lange Bestand haben. Wesentliche Bedingungen für die Stabilität und Glaubwürdigkeit des Systems sind erstens ein hinreichend großer Beteiligungsgrad am Feedbackforum und zweitens die wahrheitsgetreue Berichterstattung nach erfolgter Transaktion. Resnick und Zeckhauser (2001) haben für ebay.com eine Beteiligungsquote von 50-60 Prozent geschätzt. Meine Analysen zeigen, dass sich deut-

sche eBay-Nutzer mit einer Rücklaufquote von gegen 80 Prozent wesentlich häufiger am Bewertungsforum beteiligen.

Die dritte und vermutlich zentrale Bedingung eines Reputationssystems ist jedoch die Anwesenheit einer Reputationsprämie. Ein guter Ruf muss sich lohnen, ansonsten werden rationale Akteure nicht in den Aufbau einer Reputation investieren. Reputationseffekte sollten sich bei eBay deshalb auf verschiedenen Ebenen des Transaktionsablaufes feststellen lassen. Erstens müssten Verkäufer mit hoher Reputation eher in der Lage sein, ihre Produkte abzusetzen, d.h. die Wahrscheinlichkeit eines Verkaufes sollte mit zunehmend positiver Reputation steigen. Zweitens sollten Verkäufer mit gutem Ruf mehr Gebote und damit einen höheren Endpreis erzielen können. Eine makellose Reputation sollte hier also explizit ein Rendite, ein ‚return on investment' auf das gesparte Vertrauenskapital in Form einer Prämie erwirtschaften. Auf eBay entsteht Reputation durch positive, neutrale und negative Bewertungen der Transaktionspartner. Wir können daher eine positive und negative Dimension von Reputation unterscheiden. Positive Reputation entspricht dabei einer einfachen Funktion der Anzahl positiv bewertender Handelspartner, negative Reputation analog. Für eine Diskussion weiterführender Konzeptionen von Reputation siehe Brinkmann und Seifert (2001).

Sobald abweichende Marktteilnehmer mit schlechteren Verkaufschancen konfrontiert werden, zahlt sich betrügerisches Verhalten langfristig nicht aus. Es lässt sich zeigen, dass bereits wenige negative Bewertungen genügen, um die Verkaufschancen markant zu senken. In Anwesenheit einer Reputationsprämie sollten deshalb auch rationale Egoisten kooperative Verhaltensstrategien bevorzugen.[2] Neben den direkten Reputationseffekten an Verkaufserfolg und Endpreis lassen sich bei eBay auch Effekte zweiter Ordnung aufzeigen. Statushierarchien und Reputationsrangfolgen haben die Eigenart, dass sich Matthäus-Effekte im Sinne von Multiplikatoren beim Erwerb des generativen Merkmals einstellen. Personen mit hoher positiver Reputation werden dabei als überproportional vertrauenswürdig betrachtet. Sie erhalten mehr Aufmerksamkeit, werden wahrscheinlicher positiv bewertet und können wirksame Hemmschwellen für negative Bewertungen etablieren. Personen mit ungünstigem Leistungsnachweis verfügen dagegen oft nur über geringe Chancen, ihre Fehler auszubügeln. Im Extremfall werden sie im Sinne einer Steinigung kontinuierlich benachteiligt und längerfristig aus dem System entfernt. Steine werfen sich einfacher, wenn das Gegenüber bereits stigmatisiert ist. Reputationseffekte zweiter Ord-

[2] Trotz günstiger Anreizstruktur kann man nicht ausschließen, dass opportunistische Akteure sich eine Reputation kaufen. Die Verhaltensstrategie des Hochstaplers bleibt weitgehend intakt. Ein Marktteilnehmer kann sich mit kleineren Transaktionen eine Reputation aufbauen, um dann in einem hochkarätigen Geschäft einmal zuzuschlagen und seine Reputation gegen den Warenwert zu tauschen. Der Aufbau einer neuen Identität und Reputation ist jedoch ein mühseliges Geschäft, das sich nur in Anwesenheit von sehr hohen Reputationsprämien lohnen würde.

nung sind für die Präventionspraxis deshalb von Bedeutung, weil sie eine beschleunigende Wirkung auf das primäre Belohnungs- und Sanktionsregime ausüben. Insbesondere für die sozialwissenschaftliche Theoriebildung ergeben sich wertvolle Einsichten. Bereits aus einfachsten Bewertungsmechanismen entsteht eine Sozial- und Statusordnung, die für die Akteure Handlungsrelevanz besitzt. Sie investieren Zeit und Mühe um günstige Positionen einzunehmen und verteidigen diese bereits mit legalen Mitteln.

4 Daten und Analysen

Mit Hilfe einer automatisierten Internetbeobachtung habe ich zwischen November 2004 und Januar 2005 öffentlich zugängliche Prozessdaten von 1.084.882 Auktionen aus 177 Produktmärkten auf ebay.de beobachtet. Bereinigte Ausschnitte dieser Daten liegen den folgenden Analysen zugrunde. Der Auktionshandel von eBay und insbesondere der deutsche Ländermarkt ist ein besonders günstiges Studienobjekt. eBay ist in Deutschland unangefochtener Marktführer mit einer großen Benutzerzahl. Es resultierten daraus wenig selektive und nicht reaktive Verhaltensbeobachtungen einer großen Zahl von Akteuren in einem realen Marktkontext. Bemerkenswert ist dabei, dass der Forschende die (fast) identische Informationsgrundlage beobachten kann, die auch den Akteuren für ihre Entscheidungsfindung dient. Der Auktionsprozess wurde vollständig beobachtet vom Einstellzeitpunkt über den Bieterprozess bis zum Verkauf. Daneben wurden auch alle Akteursattribute zum Verkaufszeitpunkt erhoben, im Falle des Verkaufserfolgs von Verkäufer und Käufer. In einer zweiten Erhebung wurde nach 90 Tagen für jede Auktion festgestellt, wann und ob eine Bewertung eingetroffen ist.

In Tabelle 1 sind Schätzungen für die primären Reputationseffekte eines Ausschnitts des Mobiltelefonmarktes von eBay dargestellt. Modell 1 zeigt mit einer logistischen Regression, dass die positive Reputation eines Verkäufers die Wahrscheinlichkeit, das Produkt zu verkaufen, signifikant zu steigern vermag. Negative Bewertungen senken hingegen die Wahrscheinlichkeit eines erfolgreichen Transaktionsabschluss. Die negative Reputation hinterlässt dabei erwartungsgemäß einen wesentlich stärkeren Einfluss auf den Verkaufserfolg als positive Reputation.[3] Als Bieter ist man bei zwei identischen Produkten nicht bereit, einem Verkäufer mit schlechter Reputation denselben Preis zu entrichten. Oder umgekehrt sind Käufer gewillt, eine hohe positive Reputation mit einem Aufpreis zu vergüten. Modell 2 belegt mit einem linearen Regressionsmodell die Anwesenheit von Reputationsprämien auf den Endpreis.

[3] Messbare Effekte auf den Verkaufserfolg erstaunen aufgrund der geringen Varianz, da nur 5 Prozent der Produkte nicht verkauft werden. Es wird also auch bei Verkäufern mit geringem Reputationsnachweis geboten. In einem perfekten Markt mit vollständiger Markträumung werden Reputationseffekte nur beim Verkaufspreis ersichtlich. Der auffälligste Effekt für den Verkaufserfolg ist zweifelsfrei der Startpreis.

Tabelle 1: Reputationseffekte auf Verkaufserfolg und Verkaufspreis (Mobiltelefone)

	Model 1: Verkaufserfolg		Model 2: Verkaufspreis	
	Hypothese	Effekt	Hypothese	Effekt
Positive Reputation (log)	+	0.142*	+	1.069***
Negative Reputation (log)	-	-0.353*	-	-1.995***
Startpreis	-	-0.032***	+	0.034***
Anzahl Bieter			+	0.573***
Anbieterkonkurrenz (pro Tag)	-	-0.008*	-	-0.070***
Auktionsdauer	+	0.017	+	0.050
Kalenderzeit (zentriert)	-	-0.011	-	-0.312***
Beschreibungslänge (log)	+	-0.018	+	1.001***
Produktbild	+	0.134	+	3.736**
[…]				
McFadden R^2 / Korr. R^2		0.644		0.842
N		5’338		5’096

Anmerkung: Modell 1 zeigt Schätzungen einer logistischen Regression auf die binäre abhängige Variable ‚Verkaufserfolg’, 95 Prozent der Mobiltelefone wurden verkauft. Modell 2 zeigt die Schätzungen einer OLS Regression auf den Verkaufspreis in Euro. Schätzungen basieren auf sieben intern homogenen Kategorien, bestehend aus neuen und originalverpackten Mobiltelefonen mit einem Durchschnittspreis von 220 Euro. Robuste Standardfehler mit Clustering bei den Verkäufern. Signifikant für $p < 0.05$(*), $p < 0.01$ (**) und $p < 0.001$ (***) bei zweiseitigem Test. Positive Reputation = ln(Anzahl positive Bewertungen + 1), negative Reputation analog. Folgende Kontrollvariablen sind hier nicht ausgewiesen: Konstante, Sonntagsverkauf, Galeriebild, Fettschrift, Käuferreputation, Zahlungsvorteil, Produkte-Dummies. Vgl. Wehrli (2005) für eine ausführlichere Diskussion der Modelle.

Tabelle 2: Reputationseffekte auf die Rate positiver Bewertungen (DVD-Markt)

	Hypothese	Model 3: Bewertungen von Verkäufern	Model 4: Bewertungen von Käufern
Partner bewertet zuerst (tvc)	+	2.351***	0.986***
Partner positive Reputation (log)	+	0.089***	0.073***
Partner negative Reputation (log)	-	-0.174***	-0.063***
Positive Reputation selbst (log)	+	0.046**	0.144***
Negative Reputation selbst (log)	-	-0.176***	-0.259***
Partner zuerst X pos. Partnerreputation (ie)	-	-0.094***	-0.031***
Partner zuerst X neg. Partnerreputation (ie)	+	0.205***	-0.051***
Wiederholte Interaktion (0/1)	-	-0.296***	-0.497***
[…]			
Anzahl Fälle (Auktionen)		157’377	157’377
Anzahl Ereignisse (Bewertungen)		133’277	133’125

Anmerkung: Proportional Hazards Modelle mit der abhängigen Variable Zeitdauer bis positives Feedback (in Minuten). Maximum Likelihood-Schätzungen der Effekte auf die Hazardrate. Robuste Standardfehler, korrigiert für Clustering bei Verkäufern bzw. Käufern in Model 4. Positive Reputation = ln(Anzahl positive Bewertungen + 1), negative Reputation analog. [TVC] entspricht einer zeitvariablen Kovariate, die die Partnerbewertung zeitgenau im Bewertungsprozess des fokalen Akteurs modelliert. [IE] steht für Interaktionseffekte zwischen Partnerbewertung und Partnerreputation. Die Daten stammen aus einem Teil-Sample von DVD-Auktionen, Fälle sind Auktionen, Ereignisse die eintreffenden Bewertungen. Signifikanz für $p < 0.01$ (**) und $p < 0.001$ (***) bei zweiseitigem Test. Vgl. Wehrli (2005) für deskriptive Statistiken und Diagnostik.

Aus einer Verdoppelung der positiven Bewertungen resultiert eine Prämie von ca. 75 Cents. Eine Verdoppelung der negativen Bewertungen führt zu einem Preisabschlag von ca. 1,40 Euro.[4] Eine Produktabbildung und ausführliche Beschreibung helfen weiter, das Informationsproblem des Käufers zu entschärfen und werden entsprechend abgegolten. Die restlichen Kontrollvariablen bestätigen weitgehend die Hypothesen der Auktionstheorie (Startpreis, Anbieterkonkurrenz). Für eine ausführliche Diskussion der Modelle insbesondere der hier nicht ausgewiesenen Kontrollvariablen siehe Wehrli (2005).

Die Reputationseffekte zweiter Ordnung sind in der Tabelle 2 nachgewiesen. Hier interessieren wir uns für die Frage, wie die Bewertung in der strategischen Interdependenz zwischen Käufer und Verkäufer entsteht. Der auffälligste Einfluss ist zuerst ein direkter Reziprozitätseffekt (Partner bewertet zuerst). Wenn das Gegenüber bereits vorher bewertet hat, dann steigt die Wahrscheinlichkeit, dass der fokale Akteur auch eine Bewertung schreibt, markant. Die Modelle 3 und 4 zeigen nur die Determinanten einer positiven Bewertung. Für die negativen Bewertungen ist der direkte Reziprozitätseffekt noch deutlich stärker ausgeprägt (hier nicht ausgewiesen, vgl. Wehrli 2005). Die Verkäufer warten in der Regel auf die Käuferbewertung. Falls die Bewertung des Käufers nicht eintrifft, erspart man sich den Zeitaufwand. Als Second-Mover erhält sich der Verkäufer den strategischen Vorteil eines Vergeltungspotentials. Tatsächlich muss der Käufer beim Schreiben einer negativen Bewertung mit angrenzender Sicherheit mit einem ungünstigen Echo rechnen. Dies führt unter Umständen dazu, dass Käufer mit Statusambitionen oder Verkaufsabsichten auf negative Bewertungen verzichten. Hinweise aus der Neuroökonomik legen jedoch nahe, dass Personen auch unter Kosten und Risiko bereit sind, deviante Marktteilnehmer zu bestrafen (vgl. ‚altruistic punishment', Fehr und Gächter 2000).

[4] Die Interpretation der Prämien ist aufgrund der semi-logarithmischen Modellierung leicht umständlich. Eine Verdoppelung der positiven Bewertungen entspricht einem ln(2) *1.069 = 0,74 Euro höheren Endpreis. Ein Verkäufer an der unteren Quartilsgrenze der Reputationsverteilung hat im vorliegenden Sample 14 positive Bewertungen. Im Vergleich dazu kann ein Verkäufer aus dem Mittelfeld (Median=45) einen um ln(45/14)*1.069 = 1,25 höheren Endpreis realisieren. Meine Schätzungen fallen deutlich tiefer aus im Vergleich zu den bisherigen Studien und bewegen sich mit einem prozentualen Einfluss auf den Endpreis von 0,7-1.4% an der unteren Grenze ökonomischer Relevanz. Experimentelle Befunde (Resnick und Slawson) und andere empirische Belege (Diekmann und Wyder 2001) haben weit stärkere Reputationseffekte ausgewiesen.

Tabelle 3: Verteilung der realisierten Bewertungen nach Markt

	Mobiltelefone		DVDs	
	Verkäufer	Käufer	Verkäufer	Käufer
Positive Bewertungen	97,46%	95,78%	99,49%	99,12%
Neutrale Bewertungen	0,53%	1,48%	0,13%	0,46%
Negative Bewertungen	2,10%	2,74%	0,38%	0,42%
Anzahl Bewertungen	10'109	9'744	134'390	134'374
% von Total	75,44%	72,71%	84,55%	84,54%
Total Auktionen	13'400	13'400	158'941	158'941

Interpretation: Bei 13.400 Auktionen von Mobiltelefonen haben 75,4 Prozent der Verkäufer und 72,7 Prozent der Käufer eine Bewertung abgegeben. Von den eingereichten Verkäuferbewertungen waren 97,5 Prozent positiver Natur und 2,1 Prozent waren negative Bewertungen.

Ein Indiz für diesen Verdrängungsprozess aufgrund des gegenseitigen Feedbacks lässt sich aus der Bewertungsrate herleiten. In Tabelle 3 sind die Bewertungsquoten für zwei unterschiedliche Märkte dargestellt. Wenn man davon ausgeht, dass Transaktionen mit Mobiltelefonen problemanfälliger und riskanter sind, dann korrespondiert solches gut mit den beobachteten Häufigkeiten. Bei den Mobiltelefonen liegt der Anteil nicht-positiver Bewertungen bei 2-3 Prozent, bei den DVDs unter 1 Prozent. Bei den Handys erfolgt bei 72-75 Prozent der Fälle eine Bewertung, bei den DVDs ist der Anteil gleich 10 Prozent höher. Wie groß der Anteil der Personen ist, die ein Schweigen bevorzugen, lässt sich mit Beobachtungen nicht klären (vgl. ‚reporting bias', Dellarocas und Wood 2005). Eines gilt es hier aber festzuhalten. Die Bewertungsquote liegt über alle beobachteten Märkte zwischen 70-85 Prozent. Dies ist im Vergleich zu den Schätzungen zum US-amerikanischen Markt (50-65 Prozent) ein erfreuliches und zugleich erstaunlich hohes Niveau (vgl. Resnick und Zeckhauser 2001). Mit einer Theorie rationaler Akteure würde man erwarten, dass bei einmaligen, nicht eingebetteten Interaktionen, der Second-Mover nach Erhalt der Partner-Bewertung keinen Anreiz mehr hat, eine Bewertung zu schreiben. Und weil dies sein Gegenüber antizipiert, letztlich im Gleichgewicht niemand bewerten würde. Die Bereitstellung des öffentlichen Informationsgutes scheint bei eBay weitgehend intakt und das Trittbrettfahren auf dem Informationsangebot anderer nur gering.

Für Sozialwissenschaftler sind auch die kumulativen Vor- und Nachteile des Reputationssystems interessant. Tabelle 2 zeigt, dass Personen mit positiver Reputation überproportional häufig positiv bewertet werden. Negative Bewertungen bremsen hingegen den Aufbau einer positiven Reputation (Partnerreputation). Dies führt zu einer Beschleunigung des Selektionseffekts im ‚Ökosystem eBay' und einer impliziten Benachteiligung abweichenden Verhaltens. Ungünstig erscheint mir, dass sich wiederholte Interaktionen und der Aufbau von stabilen Käufer-Verkäuferbeziehungen nicht lohnen. Mitglieder können sich

nur einmal bewerten, dies aus Gründen der Fälschungssicherheit. Sofern sich zwei Handelspartner erneut antreffen, ist die Wahrscheinlichkeit, dass sie sich erneut bewerten, signifikant tiefer. Ein klares Indiz dafür, dass viele Benutzer das System gut durchschaut haben und sich strategisch darauf einstellen.

5 Schlussfolgerungen

Die Analysen zeigen, dass das Reputationssystem von eBay tatsächlich die intendierten Effekte induziert. Personen mit einem guten Leistungsausweis werden belohnt, wogegen eine negative Reputation zu geringeren Verkaufswahrscheinlichkeiten, tieferen Preisen und einer bescheideneren Bewertungsrate führt. Den Daten kann man auch entnehmen, dass ungünstige Transaktionen auftreten. Ein Reputationssystem kann abweichendes Verhalten nicht verhindern, sondern höchstens hemmen, verzögern und damit präventiv einwirken. Manchmal entspricht die Ware nicht den erwarteten Qualitätsvorstellungen, in seltenen Fällen wird man sogar betrogen. Der Pessimist könnte unter Berücksichtigung der Bewertungsquote befürchten, dass auf dem Mobiltelefonmarkt bis zu 25 Prozent der Beteiligten unzufrieden sind. Der Optimist wird entgegnen, dass bei mehr als 95 Prozent der Mobiltelefon-Auktionen und bei 99 Prozent der DVDs positive Rückmeldungen zu beobachten sind. Er wird zugleich rhetorisch anfügen, ob ein für ihn unbekanntes Geschäft in der Innenstadt die gleiche Quote verspricht.

Zweifelsfrei bestehen für Reputationssysteme Verbesserungsvorschläge. Man könnte das Regime gegenseitiger Bewertungen überdenken, Interaktionen fördern die wiederholten und langfristigen Charakter haben. Man könnte in Verkäufer- und Käuferreputation unterscheiden, allenfalls die Transaktionen mit dem Verkaufspreis gewichten. Ein Anteil von 95 Prozent positiver Bewertungen eines Verkäufers hat nicht in jedem Markt die gleiche Bedeutung. Populationsmittelwerte nach Märkten wären für Käufer sehr informativ. Nicht zuletzt müsste man den Benutzern auch die Möglichkeit einräumen, nach Reputationsbedürfnissen zu suchen und Schwellenwerte zu definieren, um abweichendes Verhalten aktiv zu diskriminieren. Für Reputationssysteme besteht jedoch immer ein Trade off zwischen Usability und Wirkungsgrad – d.h. der Schlichtheit und Zugänglichkeit im Gebrauch vs. perfektionierter Anreizkompatibilität. Nicht selten sind es die Nutzer, die an einem einfachen und ‚bewährten' System festhalten möchten. Dies auch aus der Unsicherheit eines Regimewechsels, der allenfalls erreichte Positionen im Reputationssystem verändert.

Inwiefern Reputationssysteme genügen, um der zunehmenden Zahl von Betrugsfällen und Übervorteilungen zu begegnen, lässt sich mit dieser Analyse nicht beantworten. Es ist auch unklar, wie stark die präventive Wirkung im Vergleich zu anderen internen und externen Maßnahmen ausfällt. Der vorliegende Fall zeigt jedoch, dass das Reputationssystem von eBay die gewünschten und erwarteten Effekte hervorrufen kann. Es hilft den Beteiligten, Unsicherheit in ein berechenbares Risiko zu überführen, und bietet eine brauchbare Informationsgrundlage für den aufgeklärten Benutzer. Ein Rechtsstaat sollte die präventive Wirkung solch selbst organisierter Systeme der Kooperationsförderung begrüßen,

auch wenn diese nicht vollständig ‚wasserdicht' sind. Er schont dabei seine Ressourcen für gravierende Vorkommnisse. Vielleicht sind es gerade diese Reste von Unsicherheit, die Personen veranlassen, über das Internet einzukaufen. Vertrauen beschleunigt, verbilligt, aber induziert ein Risiko. Offensichtlich sind viele bereit, dieses ‚Wagnis' einzugehen und erwarten nicht den Ausnahmefall. Die Erwartungen werden auch mit sehr hohem Anteil bestätigt. Mit Hilfe der diskutierten präventiven Mechanismen ist es möglich, auch unter den ungünstigsten Umständen eines asymmetrisch informierten Tauschs mit einem Unbekannten ein Geschäft abzuschließen. Dabei erneuern solche Interaktionen genau das, was zu ihrer Entstehung erforderlich ist: Vertrauen.

6 Literatur

Akerlof, G.A. (1970): The Markets for Lemons: Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics* 84(3): 488-500.

Bajari, P. und A. Hortaçsu (2004): Economic Insights from Online Auctions. *Journal of Economic Literature* 42(2): 457-486.

Berger, R. und K. Schmitt (2005): Vertrauen bei Internetauktionen und die Rolle von Reputation, Informationen, Treuhandangebot und Preisniveau. *Kölner Zeitschrift für Soziologie* 57: 86-111.

Bundesministerium des Innern (2006): Die Kriminalität in der Bundesrepublik Deutschland. Polizeiliche Kriminalstatistik 2005. *http://www.bmi.bund.de*.

Brinkmann, U. und M. Seifert (2001): ‚Face to Interface': Zum Problem der Vertrauenskonstitution im Internet am Beispiel von elektronischen Auktionen. *Zeitschrift für Soziologie* 30: 23-47.

Dellarocas, C. (2003): The Digitization of Word of Mouth: Promise and Challenges of Online Feedback Mechanisms. Management Science 49(10): 1407-24.

Dellarocas, C. und C. Wood (2005): The Sound of Silence in Online Feedback: Estimating Trading Risks in the Presence of Reporting Bias. Working Paper, University of Maryland.

Diekmann, A. und D. Wyder (2002): Vertrauen und Reputationseffekte bei Internetauktionen. *Kölner Zeitschrift für Soziologie und Sozialpsychologie* 54: 647-93.

Fehr, E. und S. Gächter (2000): Cooperation and Punishment in Public Good Experiments. *American Economic Review* 90: 980-994.

Ockenfels, A (2003): Reputationsmechanismen auf Internet-Marktplattformen. Theorie und Empirie. Zeitschrift für Betriebswissenschaft 73(3): 295-315.

Resnick, P. und R. Zeckhauser (2001): Trust among Strangers in Internet Transactions: Empirical Analysis of eBay's Reputation System. *The Economics of the Internet and E-Commerce* 11: 127-57.

Snijders, C. und R. Zijdeman (2004): Reputation and Internet Auctions: eBay and Beyond. *Analyse & Kritik* 26: 158-84.

Wehrli, S. (2005): ‚Alles bestens, gerne wieder.' Reputation und Reziprozität in Online Auktionen. Unveröffentlichte Lizentiatsarbeit. Institut für Soziologie der Universität Bern.

Cyberstalking[1]

Dr. Jens Hoffmann

Auf den ersten Blick mag Cyberstalking wie ein Modeschlagwort wirken, welches vor allem dem Boom der virtuellen Welten Tribut zollt, aber letztlich inhaltlich ohne eigentliche Substanz bleibt. Tatsächlich gilt der Begriff auch in der wissenschaftlichen Gemeinschaft mittlerweile als fest etabliert – nicht zuletzt, da die Erfahrungen in der realen Welt zeigen, dass es sich hier um ein ernstzunehmendes Problem im Kontext von Stalking handelt.

Cyberstalking bezeichnet zunächst Stalking-Verhalten, welches sich eines vernetzten Computers bedient. Stärker definitorisch ausgedrückt handelt es sich um die obsessive Verfolgung oder Belästigung einer anderen Person unter Nutzung des Internet, von E-Mails, eines Intranet oder verwandter elektronischer Medien. Cyberstalking kann zum einen völlig eigenständig auftreten, aber auch Teil eines Stalking-Vorfalles sein, bei dem zusätzlich herkömmliche Stalking-Verhaltensweisen wie Telefonanrufe oder physische Annäherungen zu beobachten sind. Es ist anzunehmen, dass Cyberstalking mit der Verbreitung und Selbstverständlichkeit der Nutzung dieser Technologien weiter ansteigen wird.

Obgleich zunächst nur anekdotische Hinweise und Erfahrungswerte von Experten über Cyberstalking bestanden, nahm sich die US-amerikanische Regierung der Fragestellung schon vor einigen Jahren auf höchster Ebene an. Im Februar 1999 gab der damalige Vizepräsident Al Gore dem Justizministerium den Auftrag, einen Bericht über das Ausmaß des Problems zu erstellen, der bereits ein halbes Jahr später fertig gestellt wurde (U.S. Department of Justice, 1999a). Etwa zu diesem Zeitraum fing man auch in Australien an, sich mit diesem Thema zu beschäftigen. Das Australian Institute of Criminology hatte zuvor bereits andere Bereiche von Cyber-Kriminalität bearbeitet und widmete sich nun auch dem Cyberstalking. Man begann mit einer beschreibenden Erfassung und theoretischen Einordnung des Phänomens ohne eigene quantitative Studien durchzuführen (Ogilvie 2000, 2001).

---

[1] Gekürzte Fassung aus Jens Hoffmann: Stalking. Springer, Heidelberg 2006. Abdruck mit freundlicher Genehmigung des Springer-Verlages.

1 Empirische Befunde zum Cyberstalking

Empirisch-wissenschaftliche Untersuchungen, die speziell Cyberstalking zum Gegenstand haben, sind erst nach der Jahrtausendwende durchgeführt worden. Zunächst wurden im Rahmen anderer Studien und durch die Befragung offizieller Stellen Anhaltspunkte dafür gesucht, wie häufig Stalker E-Mails und das Internet einsetzen (U.S. Department of Justice, 1999a). So ergab eine Umfrage unter US-amerikanischen College-Studentinnen in den späten 90er Jahren, dass bei einem Viertel der siebenhundert dort gemeldeten Stalking-Vorfälle auch Cyberstalking-Aktivitäten auftraten. Für die gleiche Zeitperiode nannten die Staatsanwaltschaften in Manhattan und Los Angeles ähnliche Zahlen. Ihren Schätzungen zufolge war bei etwa zwanzig Prozent der von ihnen behandelten Stalking-Fälle auch Cyberstalking zu beobachten.

Eine spezielle Polizeieinheit für Computerkriminalität in New York meldete, dass in gut vierzig Prozent ihrer Ermittlungen auch elektronische Bedrohungen und Belästigungen zu verzeichnen waren. Eine an dieser Stelle durchgeführte Aktenstudie (D'Ovidio & Doyle, 2003) ergab, dass die Täter in knapp achtzig Prozent der Fälle männlich waren und der Altersdurchschnitt bei 24 Jahren lag, wobei es sich bei einem guten Viertel der obsessiven Belästiger um Jugendliche handelte. Überraschenderweise wurde in aller Regel pro Stalking-Fall nur ein einziges Kontaktmedium der Cyberwelt verwendet, wie beispielsweise E-Mail oder Chatroom, und nicht mehrere. Zielobjekte des virtuellen Stalking waren in gut der Hälfte der Vorfälle Frauen, in 35 Prozent Männer und in dem restlichen Teil Institutionen oder Unternehmen.

Weitere Zahlen lieferte die Internet Community WHOA (Working to Halt Online Abuse, 2003), die es sich zum Ziel gesetzt hat, gegen (online-)Belästigungen im Netz vorzugehen. Die Organisation erfasste demografische Daten von insgesamt 609 Fällen, die in den Jahren 2000 und 2001 an sie herangetragen wurden. Die Geschlechterverteilung der Opfer entsprach dabei im Unterschied zu der eben erwähnten Untersuchung in New York mit rund 15 Prozent männlichen und 85 Prozent weiblichen Betroffenen in etwa denjenigen Studien, die die traditionellen Formen des Stalking untersucht hatten. Bei der Frage nach dem Geschlecht der Stalker hingegen fiel das Ergebnis nicht mehr ganz so stark mit einem männlichen Übergewicht aus: hier waren etwa ein Drittel Frauen und zwei Drittel Männer zu verzeichnen. Beunruhigend war, dass sich in mehr als einem Viertel aller Fälle neben der virtuellen Form auch ein Verhaltensmuster von Stalking in der realen Welt herausbildete.

Wie oft treten obsessive Belästigungen überhaupt online auf? Spitzberg und Hoobler (2002) untersuchten dies anhand einer Gruppe von vergleichsweise jungen Menschen, nämlich Studenten. Es ist zu erwarten, dass diese Population aufgrund ihrer selbstverständlichen und häufigen Nutzung des Internet derartige Erfahrungen häufiger als viele andere machen. Tatsächlich waren die Zahlen bemerkenswert: ein knappes Drittel der 235 befragten Studenten berichtete, unerwünschten und obsessiven Kommunikationen ausgesetzt gewesen zu sein, die über das Internet oder andere elektronische Medien übertragen

wurden. Dabei waren übertriebene Äußerungen von Zuneigung am verbreitetesten. Immerhin jeder Fünfte gab aber auch an, sexuell belästigt worden zu sein, und jeder Zehnte erhielt explizite Drohungen über das Internet.

2 Besondere Qualitäten des Cyberstalking

Trotz vieler struktureller Ähnlichkeiten existieren doch spezifische Unterschiede zwischen der virtuellen und der ‚offline' Form wiederholter Verfolgung und Belästigung (McGrath & Casey, 2002; U.S. Department of Justice, 1999a). Wenngleich beim ‚klassischen' Stalking auch Medien wie Telefon, Faxe oder Briefe grundsätzlich die Überwindung einer größeren geografischen Distanz zwischen Verfolgern und Verfolgten ermöglichen, ist dies mit den Mitteln elektronischer Kommunikation deutlich einfacher zu bewerkstelligen. Zu jedem Zeitpunkt kann eine Nachricht ohne nennenswerten Aufwand von zu Hause aus auf den Weg gebracht werden - und dies über eine beliebige Entfernung. So existieren mittlerweile sogar Fälle von kontinentübergreifendem Stalking. (....)

Ein weiteres besonderes Merkmal der virtuellen Belästigung liegt darin, dass der Stalker über das Internet auch eine Öffentlichkeit schaffen kann und so dritte Personen ermutigt, sich an einer Kampagne gegen das Opfer zu beteiligen. Dies kann geschehen, indem er etwa auf so genannten bulletin boards, Homepages oder in chatrooms entsprechende Nachrichten lanciert. (....)

Als ein weiteres Charakteristika des Cyberstalking ist zu bemerken, dass die Hemmschwellen vergleichsweise niedrig angesiedelt sind. Es ist nicht nötig, dem Opfer persönlich aufzulauern, noch müssen Schreiben zum Briefkasten gebracht oder es muss darauf gewartet werden, dass die Zielperson eines Anrufs am anderen Ende der Leitung abhebt. Diese Möglichkeit des Zugangs stellt gerade für Prominenten-Stalker oft den einzigen Weg oder die Hoffnung dar, mit ihrem Anliegen zu dem abgeschirmten Star vorzudringen. Zudem ist es beim Cyberstalking relativ einfach möglich, in völliger Anonymität zu agieren. (....)

Es erscheint zudem plausibel, dass die wahrgenommene Anonymität am Computerschirm sowie die dort bestehende sensorische Reizarmut bestimmte psychische bzw. psychodynamische Prozesse begünstigen (Meloy, 1998a). Beim Cyberstalking sieht, hört, riecht und berührt man keine andere Person, noch erspürt man sie im direkten Gegenüber. Der in der Unerkanntheit vorherrschende Mangel an sozialer Kontrolle kann etwa bewirken, dass bestimmte Emotionen wie Wut, Eifersucht und ein Bedürfnis nach Macht nicht unterdrückt werden und aggressives Stalking somit erleichtert wird. Dabei spielt auch das Nichtvorhandensein von nonverbalen Rückmeldungen eines direkten Interaktionspartners, die in der Kommunikation sozial regulierend wirken, eine Rolle (Ellison, 1999). Signale, wie etwa Gesichtsausdruck, Körperhaltung oder Tonfall der Stimme haben oftmals einen eindämmenden Effekt auf auftauchende Aggressivität und Feindseligkeit.

Der Mangel an sensorischen Eindrücken und die Zurückgezogenheit an der Pforte zum Internet vermögen auch die Fantasietätigkeit des Stalkers zu erhöhen. Er ist in der Lage, elektronisch in jede beliebige Identität zu schlüpfen und beispielsweise sein Opfer in seiner Fantasie allmächtig zu kontrollieren oder es durch die Selbstzuschreibung ihm attraktiv erscheinender Attribute zu beeindrucken zu versuchen. So wird aus Sicht des Stalkers eine befriedigende Beziehung virtuell konstruiert und er erlebt sich selbst in einer Annäherung an eine narzisstische Perfektion, welche als Verstärker für eine Fortsetzung seines Stalking-Verhaltens wirken kann. Dabei kann es auch zu einem Verschwimmen der Grenzen zwischen Realität und Fantasie kommen sowie zu einer für den Stalker immer wichtiger werdenden Pseudo-Intimität mit dem Opfer. (....)

3 Ausdrucksformen des Cyberstalking

Oberflächlich scheint es, dass Cyberstalking seinem Wesen nach nur über eine überschaubare Anzahl von Verhaltensfacetten verfügen kann. Die Erfahrung hat jedoch genau das Gegenteil gezeigt. Die technischen Möglichkeiten des Internet erlauben eine Vielzahl von Formen obsessiver Belästigung oder Bedrohung. Die folgende Aufzählung (angelehnt an Spitzberg & Cupbach, 2001), die nicht vollständig sein kann, liefert einen kurzen Überblick über die Komplexität der Handlungsmuster beim Cyberstalking:

- Wiederholtes und unangemessenes Zusenden von Gefühlsäußerungen oder Drohungen über E-Mails, elektronische Postkarten etc.
- Weitergabe von privaten Informationen des Opfers an andere über Chat-Räume, Massen-E-Mails, Internetseiten etc.
- Versenden von Grafiken oder Fotomontagen, in denen das Opfer in aggressiver, sexuell beleidigender oder anderer verunglimpfender Art dargestellt ist
- Verbreitung von Gerüchten und übler Nachrede über das Opfer
- Rauben der Identität des Opfers und Aufnahme schädigender Kontakte unter dessen Namen
- Kontaktaufnahme mit dem Opfer unter einem elektronischen alias, also mit vorgetäuschter Identität
- Systematisches Verfolgen der Internet-Aktivitäten des Opfers
- Abfangen von elektronischen Kommunikationen des Opfers, z.B. E-Mails
- Versuche, den Computer des Opfers auszuspionieren, etwa durch Trojanische Pferde
- Versuche, den Computer des Opfers zu schädigen, beispielsweise durch Viren
- Manipulation der elektronischen Identität des Opfers, etwa durch Veränderung seiner Signatur oder privaten Homepage
- Systematische Internet-Recherche über private Informationen des Opfers

Cyberstalking lässt sich unter verschiedenen Gesichtspunkten noch einmal in mehrere Untergruppen aufteilen. Kategorien, die bisher erstellt wurden, betrafen beispielsweise die Motive der Stalker (Burgess & Baker, 2002) sowie die verschiedenen Rahmenbedingungen, unter denen das Internet von Stalkern genutzt wurde (Ogilvie, 2000; McGrath & Casey, 2002). Als einfache und funktionale Möglichkeit erwies es sich, eine Differenzierung zu treffen, welche Bereiche und Funktionsmöglichkeiten der virtuellen Welt von dem Stalker genutzt werden. Hierbei kann grob zwischen den drei Gruppen E-Mail-, Internet- und Computerstalking unterschieden werden (Ogilvie, 2001).

E-Mail-Stalking

Obsessive Kontaktversuche mittels E-Mails stellen vermutlich die am häufigsten auftretende Variante des Cyberstalking dar. Auf der Verhaltensebene besteht hier zudem die größte strukturelle Ähnlichkeit mit den ‚klassischen' Handlungsmustern von Stalking, die etwa wiederholte Telefonate und Briefkontakt beinhalten. Und tatsächlich lässt sich E-Mail-Stalking vielfach als durch technologischen Fortschritt bedingte Erweiterung eines bereits vorhandenen Verhaltensrepertoires begreifen.

Dem wird in mehreren US-Staaten auch juristisch explizit Rechnung getragen. So erweiterte beispielsweise Kalifornien sein Anti-Stalking-Gesetz um einen speziellen Cyberstalking-Passus. Dort heißt es, dass Stalking auch anzunehmen ist bei der ‚...Benutzung eines elektronischen Kommunikationsmediums oder bei einer Bedrohung durch ein Verhaltensmuster oder einer Kombination aus verbalen, geschriebenen oder elektronisch übermittelten Mitteilungen.' (U.S. Department of Justice, 2002, S. 5). In Folge der gesetzlichen Maßnahmen wurden mehrfach Personen wegen Cyberstalking verurteilt, auch in Fällen der obsessiven Belästigung von bekannten Persönlichkeiten. (....)

Obgleich E-Mails eine distanzierte Form der Kommunikation darstellen, vermögen sie doch die Privatsphäre der Opfer zu verletzen und nicht zuletzt dadurch psychische Belastungen zu verursachen. Gerade die exzessive Wiederholung, mit der die elektronischen Nachrichten von Stalkern im virtuellen Briefkasten vorgefunden werden, kann Gefühle der Verunsicherung, Ohnmacht und Wut hervorrufen. Für viele Menschen ist das Versenden von E-Mails inzwischen ein ebenso gebräuchliches Medium der Kommunikation wie das Telefon und spielt damit im sozialen Leben eine bedeutsame Rolle, so dass hier eine spezifische Verwundbarkeit auf einer sehr persönlichen Ebene gegeben ist. (....)

Internet-Stalking

Das Medium Internet hat in der Informationsrecherche völlige neue Dimensionen eröffnet. Dabei lassen sich nicht nur allgemeine, sondern häufig auch private Daten ermitteln. Es ist wenig überraschend, dass sich in zahlreichen Fällen auch Stalker diese ‚Goldmine von online zugänglichen persönlichen Informationen' (Lloyd-Goldstein, 1998, S. 209) zu Nutze machen und Hinweise auf ihre Zielpersonen aus dem Internet ziehen.

Tatsächlich existieren sogar kommerzielle Angebote im Netz, die damit werben, innerhalb weniger Minuten unter anderem die Adresse einer bestimmten Person und deren Telefonnummer herauszufinden, selbst wenn diese nicht in öffentlichen Verzeichnissen aufgelistet ist. Zwar gibt ein Unternehmen wie beispielsweise ‚Net Detective' an, dass den Kunden nur Positives ermöglicht werden soll, wie beispielsweise alte Klassenkameraden und verlorene Lieben wieder zu entdecken. Doch sind das Missbrauchspotenzial und die verlockende Möglichkeit, sensible, sonst nur schwer zugängliche private Informationen zu erhalten, natürlich für jeden Besucher der Site offensichtlich. Ähnliche virtuelle Quellen existieren auch für Personen, die vornehmlich an Prominenten interessiert sind. So gibt es etwa Internetseiten, auf denen Adressen und gegenwärtige Aufenthaltsorte von Stars der Unterhaltungsbranche zum Teil täglich aktualisiert werden.

Verblüffenderweise soll vor einigen Jahren sogar eine Homepage speziell für Personen eingerichtet worden sein, die sich als Stalker versuchen möchten (Mullen et al., 2000). Nachdem das gewünschte Geschlecht und der Wohnort eingegeben wurden, erschien auf der Internet-Site eine Liste mit potenziellen Opfern und deren Adressen und Telefonnummern. Glücklicherweise verschwand dieser mehr als fragwürdige Service wieder aus dem Internet.

Ein Faktor, welcher das Internet-Stalking begünstigt, besteht darin, dass viele Surfer im World Wide Web ihre Anonymität massiv überschätzen (Ellison & Akdeniz, 1998). Tatsächlich hinterlässt jede Aktivität im Netz individuelle Spuren, die von dritter Seite unerkannt beobachtet werden können. So lassen sich beispielsweise unter anderem Informationen über die Seiten, welche eine Person im Internet besucht hat oder Details über den von ihr genutzten Computer relativ leicht erfassen. Es gibt sogar kommerzielle Anbieter, die diese virtuellen Spuren systematisch auswerten und individuelle Profile erstellen, die sie dann etwa für Marketing-Zwecke gemeinsam mit der E-Mail-Adresse des Users verkaufen. Obwohl regelmäßig Berichte über derartige Praktiken auch in den Massenmedien erscheinen, ist für viele Menschen, wenn sie alleine am Computer im Internet surfen, die Illusion von Privatheit und Unerkanntheit so mächtig, dass aufkommende Bedenken leicht weg geschoben werden.

Eine weitere Sorglosigkeit, welche das Internet-Stalking erleichtert, ist die weit verbreitete Angewohnheit, private Homepages ins Netz zu stellen, die mit einer Fülle ebenso sensibler wie persönlicher Angaben versehen sind. Stolz werden Anschriften, Festnetz- und Handy-Nummern präsentiert, aber auch private Fotografien, die geeignet sind, bei manchem Betrachter Fantasien einer intimen Nähe auszulösen. Mehr als einmal nahm eine lange Periode von Stalking durch eine fremde Person ihren Anfang beim zufälligen Anklicken einer privaten Homepage.

Eine besondere Gefährdung besteht für Personen, die aufgrund ihrer Profession bereits ein erhöhtes Risiko besitzen, Opfer von Stalking zu werden. Hierzu zählen beispielsweise Ärzte, Therapeuten, Politiker, aber natürlich auch Prominente. Gerade diese Berufsgruppen sollten ihre Internet-Präsenz wohlüberlegt gestalten. (....)

In einem anderen Teilgebiet des Internet-Stalking setzt der Stalker bewusst auf die Öffentlichkeitswirksamkeit des elektronischen Mediums, ein deutlicher Unterschied zur intimeren, weil nur zweiseitigen Form der Kommunikation beim E-Mail-Stalking. Wie bereits aufgeführt kann dies Diffamierungen beinhalten, etwa durch die Veröffentlichung kompromittierender Informationen und Bilder, bis hin zu Aufforderungen an andere Internet-Nutzer, das Opfer ebenfalls zu belästigen. Im Bereich prominenter Betroffener ist zudem zu beobachten, dass manche Stalker ihrer Obsession für den Star auf den Seiten des World Wide Web Ausdruck verleihen, wobei die inhaltliche Spannbreite groß ist und sich zwischen aggressiven Wahnvorstellungen und anrührenden Liebesbekundungen bewegen kann.

Als ein weiterer, für Stalking relevanter Bereich des Internet sind Chatrooms zu nennen. Hier findet sich ein Delikts- und Tätertypus mit einer geradezu prototypischen Verlaufsform: ‚Typischerweise ‚trifft' der zumeist männliche Cyberstalker das Opfer in einem Chatroom und entwickelt dort seine Obsession. Sodann versucht er, in eine enge Beziehung mit seinem nichts ahnenden Opfer zu treten. Falls er zurückgewiesen wird, reagiert er mit einer regelrechten Kampagne von Cyberspace-Belästigungen, die von der virtuellen in die reale Welt übergehen können, falls die entsprechenden persönlichen Angaben des Opfers dem Stalker zugänglich sind.' (Pathè, 2002, S. 72).

Ein weiteres, von Stalkern genutztes Internet-Instrumentarium stellen Instant Messenger dar. Mit Hilfe dieser Software lassen sich, wenn beide Parteien zeitgleich online sind, Text-, Audio- oder Videonachrichten austauschen. Kennt der Stalker die nötigen Zugangsdaten der Gegenseite, kann er seine Belästigungen in Echtzeit auf dem Bildschirm des Opfers erscheinen lassen.

Tabelle 5: Häufigkeit eingesetzter Medien in Fällen von Cyberstalking; (n = 201)

Eingesetzte Medien in Fällen von Cyberstalking	**Prozent (%)**
E-Mails	79 %
Instant Messenger	13 %
Chat Room	8 %
Message Board	4 %
Internet Site	2 %
Usegroup	1 %
Falsches User-Profil	1 %

Anmerkung: Quelle: D'Ovidio & Doyle, 2003

Computer-Stalking

Bei dieser Form des Cyberstalking greift der Täter online direkt auf den Computer des Betroffenen zu. Dies kann etwa das Löschen oder Verändern von Daten bedeuten, das

gezielte Herunterladen von persönlichen Dateien, wie etwa Text-Dokumenten oder das ‚Abhören' des Opfers, beispielsweise mit wem es E-Mails austauscht.

Das Eindringen in den Computer stellt die mit Abstand seltenste Form der virtuellen Belästigung und Verfolgung dar. Zugleich kann dies, etwa wenn der Stalker für das Opfer unmittelbar erkennbar die Herrschaft über den Rechner übernimmt, zu einem besonders ausgeprägten Gefühl des Kontrollverlustes führen (Ogilvie, 2001). (....)

Bei dieser Form des Cyberstalking können auf dem Rechner des Opfers auch spezielle Programme installiert werden (z.B. Trojanische Pferde), die dem Stalker, für das Opfer unerkannt, Informationen aus dem Computer zukommen lassen.

4 Prävention von Cyberstalking

Tatsächlich ist Cyberstalking ein Bereich, in dem man präventiv vergleichsweise gut tätig werden kann. In mehreren Anti-Stalking-Ratgebern sind sogar spezielle Maßnahmenkataloge zum Schutz vor Online-Belästigungen aufgeführt (z.B. Brown, 2000; Pathé, 2002).

Als ein erster wichtiger Punkt ist ein vorsichtiger und bewusster Umgang mit der Veröffentlichung persönlicher Informationen im Internet zu nennen, beispielsweise über private Homepages. Der Sicherheitsexperte de Becker (2000) drückt dies in plakativer Anschaulichkeit aus, wenn er warnt, nichts auf einer Web-Seite zu platzieren, was man nicht auch an jedem schwarzen Brett im ganzen Land angeschlagen sehen möchte. Es kann sich lohnen, über Suchmaschinen den eigenen Namen einzugeben, um zu sehen, ob nicht andere Personen sensible Informationen über einen selbst in das Netz eingestellt haben. Dies geschieht oft ohne schlechte Absicht. Die schlichte Bitte, die persönlichen Angaben wieder zu löschen, hat sich vielfach als ein ebenso einfacher wie effektiver Weg bewährt.

Eine weitere Empfehlung betrifft die Eigendarstellung im Internet. Ein eher geschlechtsneutrales Synonym als E-Mail-Adresse oder in Chatrooms verringert die Wahrscheinlichkeit, Zielobjekt einer potenziell unangenehmen Kontaktaufnahme zu werden, als im Gegensatz dazu beispielsweise aufreizende oder sexuell eingefärbte Namensgebungen zu wählen. Auch sollte kein einfacher Rückschluss von dem virtuellen auf den realen Namen möglich sein, um ein Übergreifen von Online-Belästigungen in die physische Welt zu erschweren.

Vorsicht ist bei im Internet geknüpften Kontakten geboten, sich auch persönlich zu treffen. Was man über die andere Person weiß, ist nicht sehr sicher, kann sie doch in der elektronischen Kommunikation ihre Motive, ja sogar das Geschlecht oder ihr Alter verfälscht haben. Deswegen sollte ein derartiges Zusammenkommen in einem öffentlichen Raum in der Anwesenheit anderer Menschen stattfinden, wenn möglich zur Tagzeit. Zudem ist es vorteilhaft, im Vorfeld Freunden oder der Familie von dem Treffen zu erzählen und auch den Ort bekannt zu geben.

Allgemein gilt, dass unangemessene oder belästigende Online-Kommunikation sofort abgebrochen werden sollte, Chatrooms in denen derartiges passiert, sollten verlassen werden. Ist man dennoch zum Opfer eines Cyberstalkers geworden, gilt es wie bei anderen Formen obsessiver Belästigung auch, das gesamte Stalking-Verhalten zu dokumentieren, um eventuelle spätere juristische, polizeiliche oder sicherheitspsychologische Schritte zu erleichtern. (....)

Pornographie im Internet – Ersatz oder Anreiz für sexuelle Gewalt?[1]

Dr. Andreas Hill, Peer Briken, Wolfgang Berner

Zusammenfassung:

Die Frage, ob Pornographie im Internet sexuelle Gewalt fördert oder eher als Sicherheitsventil dient, ist ein gesundheits-, medien- und kriminalpolitisch wichtiges Thema. Studien zur Wirkung von Pornographie generell zeigen, dass Softcore-Pornographie und gewaltfreie Pornographie als ‚harmlos' gelten, während gewaltfreie Hardcore- und Gewalt-Pornographie Aggressivität steigern können. Personen mit hohem Risiko für sexuelle Gewalt haben mehr Interesse an gewalttätiger Pornographie und werden durch diese stärker negativ beeinflusst. Die besonderen Merkmale von Internet-Pornographie und ‚Cybersex' sind: leichter Zugang von zu Hause, Anonymität, niedrige Kosten, Mannigfaltigkeit und Devianz des Materials, grenzenloser Markt, Auflösung der Grenzen zwischen Konsument und Produzent, interaktive Kommunikation, Experimentierraum zwischen Fantasie und ‚real life'-Verhalten, virtuelle Identitäten, leichte Kontaktaufnahme zwischen Täter und Opfer bzw. verschiedenen Tätern, sowie niedriges Entdeckungsrisiko. Dem Phänomen ‚sexueller Sucht' (oder Paraphilie-verwandte Störung) kommt beim problematischen Umgang mit Internet-Pornographie eine besondere Bedeutung zu. Neben präventiven Maßnahmen zum Schutze potentieller Opfer werden für die Täterseite Behandlungsstrategien vorgestellt, die außer einer Beschränkung des Zugangs zu Internet-Sexualität die Therapie komorbider psychischer Störungen und Probleme (soziale Isolation, Trauerprozesse, Stress- und Wut-Management, Schuld und Scham, Kindheitstraumata, kognitive Verzerrungen, Opfer-Empathie), evtl. auch medikamentöse Behandlung und die Förderung einer integrativeren und beziehungsreicheren Sexualität umfassen.

1 Einleitung

Pornographie im Internet ist zunächst einmal Pornographie – und sie ist nur eine von vielen Ausdrucksformen von Sexualität in diesem nicht mehr ganz neuen Medium. Das Wort Pornographie stammt aus dem Griechischen und bedeutet ursprünglich ‚über Huren schreiben'. Unter Pornographie wird heute die sprachliche oder bildliche ‚Darstellung

[1] Der Beitrag basiert auf einem Aufsatz, der zu einem Schwerpunktheft des Bundesgesundheitsblattes zum Thema ‚Sexualmedizin' verfasst wurde. Abdruck mit freundlicher Genehmigung des Springer-Verlages.

geschlechtlicher Vorgänge unter einseitiger Betonung des genitalen Bereichs und unter Ausklammerung der psychischen und partnerschaftlichen Aspekte der Sexualität' verstanden [1]. Dass jedoch die Zuordnung zu dem Begriff Pornographie sehr von dem Kontext abhängig ist, wird in der Definition im *Psychrembel Wörterbuch Sexualität* deutlich: ‚Darstellung von Sachverhalten mit sexuellem Inhalt, die nach den jeweils (individuell oder sozial) zugrunde gelegten Normen als Obszönität gelten, indem sie Tabus brechen oder aus anderen Gründen als sozial nicht akzeptabel erscheinen' [2].

Pornographie ist immer wieder mit sexueller Gewalt in Verbindung gebracht worden. Dazu gibt es vier kontroverse Grundpositionen:

Position 1: Pornographie ist ein **Sicherheitsventil**. Risikopersonen können sich mit Hilfe von Pornographie davor schützen, deviante Fantasien und Impulse in der Realität in selbst- oder fremdschädigendes Verhalten umzusetzen. So könne z.B. der Konsum von Kinderpornographie als Ersatz für reale sexuelle Kontakte mit Kindern dienen.

Position 2: Pornographie ist die direkte oder indirekte **Ursache** von sexueller Gewalt. Aus der feministischen Kritik an Pornographie stammt das Motto: ‚Pornographie ist die Theorie, Vergewaltigung die Praxis'. Besonders bei Risikopersonen fungiert Pornographie als Verstärker oder Auslöser sexuell aggressiver Fantasien und Impulse.

Position 3: Der Konsum von Pornographie ist lediglich **Folge bzw. Ausdruck** einer bestehenden Neigung zu sexueller Aggressivität.

Position 4: Es gibt **keinen ursächlichen Zusammenhang** zwischen Pornographie und sexueller Gewalt.

Bevor diese Positionen erörtert werden, soll zunächst die Bedeutung des Internet für Sexualität insgesamt kurz dargestellt werden.

2 Sexualität und Internet

Das Internet hat sich in den letzten 20 Jahren zu dem wahrscheinlich wichtigsten Kommunikationsmedium in der industrialisierten Welt entwickelt. Dabei spielt Sexualität weiterhin eine herausragende Rolle: Bei der Internet-Suchmaschine Google finden sich aktuell unter dem Stichwort ‚Sex' 719.000.000 Links, unter ‚Pornography' 35.400.000 (28. Juli 2006). Um die Jahrtausendwende waren ca. 20 Prozent aller Internetnutzer in irgendeiner Form im Netz sexuell aktiv [3]. Die Zahl von Besuchern auf Sex-Websites stieg in der Zeit von Dezember 1999 bis Februar 2001 um 27 Prozent von 22 Mio. auf 28 Mio. [4]. Laut einer Untersuchung der Firma NetValue konsumierten im Jahr 2001 33 Prozent der deutschen Internetnutzer häufig Cybersex, davon waren 82 Prozent Männer und 18 Prozent Frauen [5]. Mit dem Internet – so Cooper und Griffin-Shelley [6] – sei eine ‚neue sexuelle Revolution' angebrochen, vergleichbar mit dem Einfluss der Antibaby-Pille. Mit dem Internet gehe das mechanische Zeitalter zu Ende, das virtuelle Zeitalter entfalte sich [7].

Sexualität findet im Internet mannigfaltige Ausdrucksformen: Fotos, Filme, Texte, Kurzbotschaften (Instant-Message-Systeme), Chats, Multi-User Domains (MUD), direkte akustische (Telefon) und visuelle (Webcam) Kommunikation (für einen detaillierte Übersicht über die aktuellen Möglichkeiten s. [8]). Unter ‚Cybersex' im engeren Sinne (auch ‚Cybering', ‚Online-Sex', ‚virtueller Sex' u. ä. genannt) versteht man ‚computervermittelte zwischenmenschliche Interaktionen, bei denen die beteiligten Personen offen sexuell motiviert sind, also sexuelle Erregung und Befriedigung suchen, während sie einander digitale Botschaften übermitteln' [5, 6]. Cybersex ist also keine Mensch-Maschine-Interaktion und als soziales Geschehen auch kein Solosex. Beim videobasierten Cybersex treten die Teilnehmer per Online-Videokontakt oder -konferenz miteinander in Verbindung, bei Bedarf ergänzt durch Audio- und Textdialog. Derzeit dominiert aber der textbasierte, maschinenschriftliche Cybersex, sei es zeitgleich und zeitversetzt. Die Inhalte variieren zwischen kurzen, erotischen Textbotschaften und ausgefeilten Szenarien. Im Gegensatz zu Face-to-Face-Begegnungen erfordert diese Art des Cybersex ein schriftliches Verbalisieren des Begehrens, ohne dabei körperlos zu sein [5]. Gerade in der Schriftsprache entfaltet sich ein besonderer Raum für individuelle Fantasien. Cybersex ist ‚kondomlos und zeitnah', und in Zeiten der HIV-Prävention mit einem ‚geradezu verschwenderischen Umgang mit Körperflüssigkeiten' [9]. Cybersex kann sowohl eine prostitutive Dienstleistung sein (vorwiegend videobasiert, vergleichbar mit Peep- und Sexshows), als auch privaten, nichtkommerziellen Zwecken dienen, die sich mal in flüchtigen Begegnungen erschöpfen, mal in dauerhaftere, verbindlichere soziale Beziehungen münden [5, 10]; er kann auf Kontakte per Internet beschränkt bleiben, aber auch ‚reale' Kontakte (‚in real life', IRL) anbahnen. Das Internet ist über seine Bedeutung für rein sexuelle Kontakte hinaus mittlerweile zum Hauptmedium bei der Partnerschaftssuche avanciert; es trägt zur Globalisierung von Sexualität als Ware und Dienstleistung bei; wie bei eBay wird ein lokaler, sexueller Markt durch einen weltweiten ersetzt bzw. ergänzt, wobei die lokaleren Netzwerke weiterhin eine Bedeutung für die Anbahnung von In-real-life-Kontakten haben [11].

Die Unterscheidung von ‚real' und ‚virtuell' erweist sich im Internet jedoch auf den zweiten Blick durchaus als schwierig. Die mittels Internet entwickelten Fantasie-Welten und sexuellen Betätigungen haben durchaus eine eigene, nicht nur gedankliche Realität. Unter Hinweis auf die Interdependenz von realen und virtuellen Räumen schlug Dekker vor, den mit dem Internet verbundenen Computer als ‚eine Art elektronischen Spiegel zu begreifen, der die Utopie des virtuellen Raums ... mit dem realen Raum verbindet' [12]. Bauman [13] stellte die provokante Frage, was realer sei, Cybersex oder In-Real-Life-Sex. Betrachtet man das Gehirn als das wichtigste menschliche Sexualorgan, verwischen sich auch die Grenzen zwischen ‚real' und ‚virtuell'.

Was sind spezifische Charakteristika der Internet-vermittelten Sexualität, z.B. im Vergleich zum Telefonsex, der trotz noch größerer Verbreitung des Telefons, nie die Ausmaße angenommen hat wie Internet-Sex? Das Internet bedient sich gerade im sexuellen Bereich weiterhin stark einer Text-Kommunikation, die für die Entwicklung von ‚romantischen' Beziehungen schon immer von besonderer Bedeutung war [14]. Dies erlaubt den

individuell angemessenen Grad an Nähe bzw. Distanz, sowohl räumlich als auch zeitlich, und ermöglicht damit auch eine optimale Abstimmung von Begehren und Fantasien zwischen den Beteiligten [11]. Gerade dieser individuell sehr variable Abstand zwischen den kommunizierenden Partnern ermöglicht es, sich in der Anonymität des Netzes von sozialen Attributen zu befreien – das gesprochene Wort verrät häufig nicht nur Geschlecht, Alter, Nationalität – und die Worte sorgfältiger abzuwägen. Je nach Geschmack und Notwendigkeit kann in Sekundenschnelle oder verzögert, mit Pausen kommuniziert werden, quasi in einer variablen Kombination von Telefon- und Briefqualitäten. Das Internet expandiert den Zwischenraum zwischen privater Fantasie und realem Verhalten, zwischen Denken, Tun und Sein. Es erlaubt das sexuelle Experimentieren auch mit ungewöhnlichen, möglicherweise ‚gefährlichen' Fantasien aus der Sicherheit der Anonymität und gleichzeitig der Geborgenheit des eigenen Zuhauses. Im Internet lassen sich besonders leicht interaktionell Erzählungen entwickeln, häufig in einer offensichtlich attraktiven Mischung aus romantischer Erzählung und Pornographie [11]. Das Netz bietet sich besonders an für die wechselseitige Konstruktion sexueller Skripte, wo die Partner sowohl Drehbuchautoren als auch Schauspieler sind [15, 16].

Fast jedes neue Medium – sei es Buchdruck, Fotografie, Telefon oder Fernsehen - stand anfänglich unter dem Verdacht, es werde die Sexualität korrumpieren und zum Sittenverfall beitragen. Bei solchem Technik- und Kulturpessimismus ist Vorsicht geboten. Das Internet birgt für die Sexualität sowohl Chancen als auch Risiken (Tab. 1), beide sind häufig nicht voneinander zu trennen und sollten nicht einseitig gegeneinander ausgespielt werden [5, 17, 18].

Tab. 1: Chancen und Risiken des Internet in der Sexualität

Chancen:

- Erleichterung sozialer Kontakte, besonders für Menschen mit geringen sozialen Fähigkeiten (schüchterne, selbstunsichere), Behinderungen oder körperlichen ‚Nachteilen'
- Entwicklung (virtueller) Gemeinschaften und Subkulturen mit gemeinsamen sexuellen Interessen, besonders für sexuelle Minderheiten (Schwule, Lesben, Bisexuelle, Transgender- und Intersex-Personen, Menschen mit ausgefallenen sexuellen Praktiken); leichteres Coming-Out; Internet als ‚extended family' [18]
- Ermöglichung sexueller Kontakte (besonders für sexuelle Minderheiten) in abgelegenen, ländlichen Regionen
- Große Partnerauswahl; bessere Abstimmung (matching) von sexuellen und anderen Präferenzen und Persönlichkeitsmerkmalen
- Abbau von Vorurteilen und Stereotypen
- Erweiterung des Spektrums sexueller Fantasien und sexuellen Verhaltens, Experimentieren in einem sicheren Raum, evtl. auch für Partnerbeziehungen
- Bei reinem Cybersex kein Risiko bzgl. sexuell übertragbarer Erkrankungen (z.B. HIV)

- Verbreitung von Informationen, sexuelle Aufklärung und Erziehung, besonders für Kinder und Jugendliche (z.B. über Schwangerschaftsverhütung, sexuell übertragbare Krankheiten und Safer Sex, sexuelle Störungen)
- Beratung, Selbsthilfe und Behandlung sexueller Probleme via Internet
- Ersatz für reale sexuelle Übergriffe
- Freiheit: Von Dritten nur schwer kontrollierbares Medium

Risiken:

- Vermeidung von ‚realen' - sexuellen und nicht-sexuellen - zwischenmenschlichen Kontakten, Isolation, Vereinsamung
- Unzufriedenheit mit ‚Real-life'-Sexualität und -Beziehungen, die mit den ausgefeilten sexuellen Fantasien und Bildern aus der virtuellen Internetwelt nicht ‚mithalten' können
- Belastung von Partnerschaften
- Flucht in eine virtuelle Welt
- Normalisierung des Ungewöhnlichen
- Süchtige Entwicklungen (unbegrenzte, leichte Verfügbarkeit von Pornographie und Cybersex)
- Senkung von Hemmschwellen: wiederholte, evtl. selbst- und/oder fremdschädigende Fantasien werden leichter ‚in real life' umgesetzt
- Steigerung sexuell aggressiver Impulse
- Missbrauch von im Netz aufgebauten Vertrauensverhältnissen
- Von Dritten nur schwer kontrollierbares Medium

3 Pornographie und sexuelle Gewalt

3.1 Erklärungsmodelle

Laut dem *Erregungs-Transfer-Modell* führt Pornographie zu einer unspezifischen physiologischen Erregung, die nach Provokation in Wut überführt wird. Das *Modell des Sozialen Lernens* postuliert, dass Pornographie die Degradierung von Frauen, Gewaltanwendung oder die sexuelle Ausbeutung von Kindern legitimiert; der explizit sexuelle Inhalt von Pornographie wird dabei als sekundär angesehen. Der Konsument identifiziert sich mit dem ‚Täter' bzw. dem dominanten Partner in der pornographischen Darstellung, ahmt diesen nach. Nach der *Desensitivierungstheorie* gewöhnt sich der Konsument an die Verknüpfung von Sexualität und Gewalt, wie sie häufig in der Pornographie dargestellt wird. Auch kann es durch häufigen Pornographiekonsum zu einer Abstumpfung und Langeweile bei ‚normaler' Pornographie kommen und ein Verlangen nach einem stärkeren Reiz, d.h. devianteren, evtl. gewalttätigeren Stimuli wachsen (für einen Überblick zu den theoretischen Modellen vgl. [19, 20]). Nach *psychodynamischen Theorien* kann Pornographie-

konsum als narzisstische Plombe zur Kompensation von Minderwertigkeits- und Ohnmachtsgefühlen, zur Selbsttröstung und zur Angstabwehr dienen und stellt in seinen devianteren Formen eine ‚erotische Form von Feindseligkeit' dar. Wichtig ist dabei die der Pornographie innewohnende ‚Fetischisierung' des Objekts [21, 22].

3.2 Empirische Untersuchungen

Will man die Auswirkungen von Pornographie untersuchen, ist es notwendig das Ausmaß der Gewaltdarstellung zu berücksichtigen und zwischen Softcore, Hardcore, Gewalt- und Vergewaltigungspornographie zu unterscheiden [23, 24].

Tab. 2 Pornographie-Typen nach Ausmaß der Gewalt (nach Boering 1994 [24])

Softcore-Pornographie:	Nacktdarstellungen (z.B. in Playboy, Praline)
Hardcore-Pornographie:	Darstellung gewaltfreier sexueller Handlungen (i.d.R. mit einem oder mehreren Partnern)
Gewaltpornographie:	Darstellung von Fesseln, Schlagen, aber offensichtlich noch konsensuell
Vergewaltigungspornographie:	Darstellung von Gewaltanwendung, aber sichtbar nicht mehr konsensuell

Zur Klärung des Zusammenhangs zwischen Pornographie und Gewalt werden (a) experimentelle Studien, häufig mit unauffälligen Studentenpopulationen, (b) eher korrelative Untersuchungen bei Sexualstraftätern und (c) epidemiologische Studien an großen Bevölkerungsgruppen herangezogen [20]. In einer Meta-Analyse von 33 **experimentellen Studien** mit insgesamt 2.040 Probanden konnte gezeigt werden, dass Softcore-Pornographie (einfache Nacktdarstellungen) die Aggressivität senkt (Effektstärke r= -.14), während gewaltfreie Hardcore-Pornographie (r=.17) und Gewalt-Pornographie (r=.22) diese steigern [25], allerdings nur bei den Probanden, die zuvor provoziert und in einen gereizten Zustand versetzt (‚angered') worden waren. Diese unspezifische gereizte Ausgangsstimmung ist offensichtlich eine wichtige Vorraussetzung für die negative Wirkung von Pornographie. Oddone-Paolucci und Mitarbeiter [26] fanden in einer weiteren Meta-Analyse von 46 experimentellen Studien mit insgesamt 12.323 Probanden Korrelationen von Pornographie mit devianter Sexualität (Effektstärke r=.31), sexueller Gewalt (r=.22), negativen Einstellung über Intimbeziehungen (r=.20) und Vergewaltigungs-Mythen (r=.31).

Daraus kann geschlossen werden, dass Pornographie nur einer von vielen Einflussfaktoren auf die Entwicklung sexueller Gewalt ist [23]. Als moderierende Einflussfaktoren auf die Wirkung von Pornographie kommen neben der *Art der Pornographie* (Gewaltlevel) und dem *aktuellen emotionalen Zustand* des Konsumenten (Wut, Ärger, Traurigkeit) auch das *kulturelle* (z.B. Geschlechter-Gleichheit, Permissivität für Gewaltanwendung) und *familiäre Milieu* (z.B. Umgang mit Sexualität, Traumatisierungen), *Persönlichkeitsfaktoren* (z.B. Bindungsstil, Feindseligkeit, Impulsivität, Intelligenz, sexuelle Präferenzen etc.) und der Einfluss *psychotroper Substanzen* (Alkohol, Drogen) in Frage. Daher ist es wichtig, bzgl. der Wirkung von Pornographie zwischen verschiedenen Risikogruppen zu unter-

scheiden. In einer experimentellen Studie mit 1.713 College-Studenten fand sich zwar in allen Risiko-Gruppen (eingeteilt anhand der Merkmale feindselige Männlichkeit und Promiskuität) ein Zusammenhang zwischen Häufigkeit des Pornographiekonsums und sexueller Aggression [27]. Dieser Effekt war aber am ausgeprägtesten in der Höchst-Risiko-Gruppe (13 Prozent der Stichprobe): diejenigen mit dem häufigsten Pornographiekonsum zeigten siebenmal so häufig sexuelle Aggressionen als diejenigen, die nie Pornographie konsumierten. Ein kausaler Zusammenhang ist in zwei Richtungen denkbar:

(a) Personen mit einer besonderen Bereitschaft für sexuelle Aggression konsumieren häufiger Pornographie.

(b) Pornographiekonsum fördert die sexuelle Aggressivität.

Meistens handelt es sich wahrscheinlich um eine Wechselwirkung zwischen dem Konsumenten und dem pornographischen Material.

In einer Meta-Analyse von 13 Studien zum Einfluss von Pornographie auf **Sexualstraftäter** (Gesamt-N = 2.542) fand sich zwar kein Unterschied zwischen Sexualstraftätern und Kontrollgruppen bzgl. der Häufigkeit und dem Alter beim ersten Pornographiekonsum, aber Sexualstraftäter waren nach Pornographiekonsum häufiger sexuell aktiv, sei es in Form von Selbstbefriedigung, konsensuellen oder erzwungenen sexuellen Kontakten (r=.23), und sie wurden durch Pornographiekonsum stärker sexuell erregt (r=.15), besonders durch Gewalt-Pornographie (r=.39). Interessanterweise wurden die Sexualstraftäter durch konsensuelle Pornographie weniger erregt als die Kontrollprobanden (r= -.26) [28].

Im direkten Kontext von Sexualstraftaten kann Pornographie zu unterschiedlichen Zwecken dienen:

(a) zur Eigenstimulationen des Täters vor der Tat,

(b) zur Verführung des Opfers, bes. von Kindern und Jugendlichen, die häufig eine besondere Neugierde für solches, für sie ansonsten nicht leicht zugängliches Material haben,

(c) zur späteren Selbststimulation nach einer Tat,

(d) zu kommerziellen Zwecken (z.B. Verkauf von Kinderpornographie).

Selbststimulation vor der Sexualstraftat kommt relativ selten bei Inzesttätern (13%) vor, aber immerhin zu gut einem Drittel bei hetero- wie homosexuellen, extrafamiliären Missbrauchstätern (36% bzw. 38%) und Vergewaltigern (35%) [29]. In zwei Befragungen von Sexualstraftätern gaben 16 Prozent bzw. 27 Prozent an, dass Pornographiekonsum zu ihrem devianten Sexualverhalten beitrug [30, 31]. Laut einer neueren Untersuchung von Langevin und Cornoe [32] nutzen 13 Prozent der untersuchten Sexualstraftäter Pornographie zur Selbststimulation vor der Tat, die Hälfte (55%) zeigten dem Opfer bei der Tat

pornographisches Material (meistens zur Verführung, manchmal auch zur Einschüchterung) und ein Drittel (37%) machten Aufnahmen von ihrem Opfer.

Es gibt kaum prospektive Untersuchungen zum Einfluss von Pornographie auf sexuelle Gewalttätigkeit. Von besonderer Bedeutung ist die Frage, ob und in welchem Ausmaß der Konsum von Kinderpornographie als Vorläufer – sei es als Ursache oder nur als Prädiktor - von realen sexuellen Missbrauchsdelikten an Kindern zu sehen ist. Seto und Eke [33] untersuchten 201 Täter, die wegen des Besitzes oder Handels mit Kinderpornographie aufgefallen waren. Etwa ein Viertel dieser Täter (24%) hatten zuvor schon sog. Hands-on Sexualdelikte verübt und 15 Prozent waren schon früher mit Kinderpornographie straffällig geworden. Innerhalb des Nachuntersuchungszeitraums – durchschnittlich 2,5 Jahre in Freiheit (sog. time at risk) – hatten insgesamt nur wenige Täter ein Hands-on Sexualdelikt begangen: 1,3 Prozent derjenigen, die bis dahin nur mit Kinderpornographie aufgefallen waren, aber signifikant mehr (9,2%, $p<.05$) von denen mit einem früheren Hands-on Delikt. Nach dieser Studie scheint es eher die Ausnahme als die Regel, dass Personen, die mit Kinderpornographie aufgefallen sind, später auch schwerwiegendere, ‚reale' Missbrauchsdelikte begehen.

Aus **epidemiologischen Studien** ergibt sich ein eher widersprüchliches Bild zur Bedeutung von Pornographie und sexueller Gewalt. In Dänemark sank parallel zur Legalisierung und Zunahme des Pornographiekonsums seit den 1960er Jahren die Häufigkeit von Sexualstraftaten, v.a. von sexuellem Missbrauch von Kindern, voyeuristischen und exhibitionistischen Delikten; ähnliche Entwicklungen konnten für West-Deutschland und Schweden gezeigt werden [34]. Gerade die Abnahme der Hands-Off-Delikte könnte allerdings auch durch eine insgesamt liberalere, gelassenere Haltung solchen Taten gegenüber erklärt werden. In den USA hingegen stieg mit höherem Pornographie-Konsum die Rate von Vergewaltigungen, wobei dieser Anstieg wahrscheinlich auf andere Einflüsse zurückzuführen ist, v.a. eine erhöhte Anzeigebereitschaft; und Faktoren, die für die parallele Steigerung von nicht-sexueller Gewaltdelinquenz verantwortlich sind [34]. In Japan ging die Verbreitung von Pornographie zwischen 1972 und 1995 sogar mit einem Rückgang der Sexualstraftaten einher [35]. Kausale oder auch nur korrelative Zusammenhänge aus solchen epidemiologischen Studien zu ziehen, ist jedoch höchst problematisch, da es eine Vielzahl von bekannten und unbekannten zusätzlichen Einflussfaktoren gibt (z.B. Bevölkerungsdichte, sozialer Status u.a.). Soweit möglich sollte man bei solchen Untersuchungen ebenfalls zwischen Soft- und Hardcore-Pornographie unterscheiden.

Fasst man die empirischen Befunde zusammen, so ist von einer Wechselwirkung auszugehen: Menschen (i.d.R. Männer) mit hohem Risiko für sexuelle Gewalt haben mehr Interesse an gewalttätiger Pornographie und werden durch diese stärker negativ beeinflusst. Softcore-Pornographie und gewaltfreie Pornographie kann im Allgemeinen als ‚harmlos' gelten. Gewaltfreie Hardcore- und Gewalt-Pornographie steigern Aggressivität. Pornographiekonsum fördert wahrscheinlich die Fixierung sexueller Devianz (z.B. bei Pädophilie, Sadomasochismus) und kann der Vorbereitung von Sexualstraftaten dienen. Bezogen auf

die o.g. Grundpositionen bedeutet dies, dass zumindest Hardcore- und gewalttätige Pornographie bei Risikopersonen eher als Stimulus für sexuelle Gewalt und nicht als ein Sicherheitsventil anzusehen ist.

4 Internet, Pornographie und sexuelle Gewalt

Das Internet kann von – potentiellen – Sexualstraftätern zu unterschiedlichen Zwecken genutzt werden [36-38]: um Fantasien zu entwickeln, Hemmungen zu überwinden, Opfer zu beobachten und zu kontaktieren, Entdeckung zu vermeiden oder mit anderen Tätern zu kommunizieren. Dazu gibt es jedoch bisher nur wenige empirische Studien.

In Deutschland ist laut der Polizeilichen Kriminalstatistik in den letzten Jahren ein deutlicher Anstieg von Besitz und Beschaffung von Kinderpornographie (§ 184c StGB) zu verzeichnen - alleine von 2003 auf 2004 eine Steigerung um 68 Prozent auf 4.819 erfasste Fälle (4.365 Tatverdächtige, mit einem nur geringen Ausländeranteil von 4 Prozent). Bei der Verbreitung pornographischer Erzeugnisse an Personen unter 18 Jahren (§ 184 StGB) wurde sogar eine Verdoppelung auf 1.089 Fälle mit 685 Tatverdächtigen (2004) registriert. Diese Steigerungen werden v. a. auf eine verstärkte Sachaufklärung durch die Polizei und ein verbessertes Anzeigeverhalten durch die Bevölkerung zurückgeführt [39]. Von der Gesamtzahl der Fälle von Verbreitung pornographischer Schriften (§§ 184, 184a, 184b, 184c StGB) – insgesamt 5.555 – wurden 52 Prozent (2.908 Fälle, 2.301 Tatverdächtige) mit Hilfe des Internet verübt, mit einer Aufklärungsquote von 79 Prozent [40].

In einer repräsentativen Befragung von Kindern und Jugendlichen (n=1.501, Alter 10-17 Jahre, MW 14 Jahre), die regelmäßig das Internet nutzen, fanden Mitchell, Finkelhor und Wolak [41], dass 19 Prozent der Befragten innerhalb eines Jahres unerwünschte sexuelle Kontaktversuche erlebt hatten, immerhin 3 Prozent berichteten von aggressiver sexueller Belästigung. Nur 25 Prozent derjenigen mit unerwünschten Kontaktversuchen fühlten sich dadurch sehr verstört oder verängstigt, besonders waren dies die Jüngeren (10-13 Jahre). 10 Prozent der Kinder und Jugendlichen, die sexuelle Kontaktversuche erlebt hatten, wendeten sich deswegen an eine offizielle Stelle (z.B. Internet-Provider, Polizei). Keiner der Befragten hatte infolge des Internet-Kontakts einen ‚realen' sexuellen Übergriff erlebt. Ein höheres Risiko für unerwünschte Kontaktversuche hatten Mädchen, ältere Jugendliche (14-17 Jährige), solche aus schwierigen psychosozialen Verhältnissen (z.B. Nutzer mit depressiven Symptomen), häufige Internetnutzer, Teilnehmer von Chat-Rooms und diejenigen, die ein risikoreiches Internetverhalten zeigten, mit fremden Personen online kommunizierten oder das Internet nicht in der elterlichen Wohnung nutzten. Interessanterweise hatte elterliches Kontrollverhalten (Internetbenutzung nur nach elterlicher Erlaubnis; Regeln über die Dauer und Art der Internetnutzung; Filter- oder Sperrtechniken; Kontrolle von Bildschirm, Datenverlauf oder Datenspeichern) keinen Einfluss auf das Risiko, unerwünschte sexuelle Kontaktversuche zu erleben.

Laut der *National Juvenile Online Victimization Study* [42], einer Befragung von 2.574 staatlichen und privaten Institutionen in den USA, die sich mit Übergriffen auf Minderjährige befassen, wurden im Jahr 2001/2002 insgesamt 129 Internet-bezogene Sexualstraftaten gegen Minderjährige bekannt. Immerhin 18 Prozent dieser Delikte wurden durch Familienangehörige oder Bekannte verübt. In 5 Prozent der Fälle wurde Gewalt angewendet. Die Opfer waren zum größten Teil (75%) 13-15jährige Mädchen, die erwachsene Täter (76% >25 J.) in Chat-Rooms kennen lernten. Interessanterweise täuschten die Täter die Opfer i.d.R. nicht über ihr Alter und ihre sexuellen Absichten. Die meisten Opfer trafen sich mehrmals mit dem Täter, 50 Prozent waren in den Täter verliebt oder zeigten eine enge emotionale Beziehung zu ihm. In einer darauf aufbauenden Untersuchung, mit einer kleineren Stichprobe (n=77) zeigten Walsh und Wolak [43], dass die Täter in fast allen Fällen (91%) verurteilt wurden, selbst wenn das Opfer freiwillig an den sexuellen Handlungen teilnahm und bei der strafrechtlichen Verurteilung nicht kooperierte.

In einer Schweizer Studie wurde der Zusammenhang von Internet-Kinderpornographie und Kontakt-Delikten an 33 Konsumenten von Kinderpornographie untersucht, die im Rahmen einer größeren polizeilichen Ermittlung aufgedeckt worden waren [44]. Dabei handelte es sich um eine sozial gut integrierte Gruppe (72% Akademiker und Angestellte, 12% Arbeiter, 12% Selbständige, 3% Arbeitslose), die Hälfte war verheiratet oder lebte in einer Partnerschaft, 40 Prozent hatten Kinder. Immerhin ein Drittel hatte jedoch noch nie eine Partnerschaft erlebt. Obgleich mehr als die Hälfte der Betreffenden (58%) neben Kinderpornographie auch sadomasochistische, Tier- oder koprophile Pornographie konsumierten, war nur ein einziger Täter zuvor wegen eines Sexualdelikts und vier (12%) wegen illegalem Pornographiebesitz oder –handel aufgefallen. Die Autoren schlossen daraus, dass auch der Konsum besonders devianten, (kinder-)pornographischen Materials kein spezifischer Risikofaktor für sexuelle Kontakt-Delikte sei.

In einer Untersuchung von 39 ‚Internet Outpatients' (darunter eine Frau), die am *National Institute for the Study, Prevention and Treatment of Sexual Trauma* (Baltimore, USA) wegen Internet-bezogenen sexuellen Problemen Hilfe suchten, wurde bei 82 Prozent eine Paraphilie diagnostiziert, v .a. eine nicht näher bezeichnete Paraphilie (49%) oder Pädophilie (23%); die Hälfte der Patienten litt unter einer Depression und 13 Prozent unter einem Alkoholmissbrauch [45]. Die Hälfte der Patienten hatte sich Kinderpornographie aus dem Internet herunter geladen, ein Viertel hatte einem Kind Pornographie zugemailt und ein Drittel hatte versucht, ein Kind für einen Sexualkontakt ‚in real life' zu treffen. In der Vorgeschichte waren jeweils ein Patient zuvor mit exhibitionistischen Handlungen, sexueller Belästigung und sexueller Gewalt aufgefallen, zwei Patienten mit sexuellen Kontakten zu Minderjährigen.

5 Sexuelle Süchtigkeit

Ein hoher Pornographiekonsum kann – gerade in ‚Risikogruppen' [27] – auch ein Symptom einer zwanghaften bzw. suchtartigen Sexualität sein. Eine solche suchtartige Ent-

wicklung kann einerseits Merkmal einer progredienten Entwicklung bei einer Störung der Sexualpräferenz (ICD-10) bzw. Paraphilie (DSM-IV) sein, oder aber Symptom einer eigenständigen Störung, bei der aber nicht das ‚Sexualobjekt' bzw. die Art der sexuellen Praktik deviant ist. Die diagnostische Einordnung und Terminologie (sexuelle Sucht, obsessiv-zwanghafte Sexualität, gesteigertes sexuelles Verlangen, Paraphilie-verwandte Störung, Impulskontrollstörung) wird kontrovers diskutiert [46-49]. Als typisch für ‚sexuelle Sucht' gelten sexuelle Gedanken und Handlungen, die als nicht kontrollierbar, als nicht unbedingt lustvoll und als nicht oder nur kurzzeitig befriedigend erlebt werden. Zudem bestehen eine Steigerungstendenz und Angst- oder Leeregefühle bei Verzicht auf die sexuellen Aktivitäten. Diese können soweit gehen, dass für andere Aktivitäten kaum mehr Interesse besteht und soziale Folgen nicht ausreichend berücksichtigt werden (z.B. Beziehungs-, Arbeits- und finanzielle Probleme) [2]. Aus unserer Arbeitsgruppe wurde eine Operationalisierung vorgeschlagen, die sich an der Struktur des DSM-IV orientiert [48].

Tab. 3: Diagnostische Kriterien für Paraphilie-verwandte Störung/'sexuelle Sucht' (modifiziert nach Briken, Hill u. Berner 2005 [48])

- Über einen Zeitraum von mindestens 6 Monaten wiederkehrende Schwierigkeiten , sexuelle Phantasien oder Verhaltensweisen zu kontrollieren
- Die sexuellen Phantasien und Verhaltensweisen beinhalten *nicht*-paraphile Symptome wie exzessive Masturbation, Pornographie-, Telefon- oder Cybersex, protrahierte Promiskuität.
- Die sexuellen Phantasien und Verhaltensweisen verursachen klinisch relevante Schwierigkeiten oder Einschränkungen in sozialen, beruflichen oder anderen funktionell wichtigen Bereichen.
- Die Störung wird nicht durch eine andere psychische Störung besser erklärt und ist nicht Folge einer körperlichen Erkrankung.

Die spezifischen Qualitäten des Internet bergen im Vergleich zu anderen Medien (z.B. Zeitschriften, Büchern, Videos) wahrscheinlich ein höheres ‚Suchtpotential' (für Übersichten s. [50-52]). In Untersuchungen mit Internet-Nutzern erfüllten 4-10 Prozent die Kriterien für eine ‚Internet-Sucht' [53]. Laut einer aktuellen deutschen Untersuchung verbringen Personen mit einer Internet-Sucht wöchentlich etwa 32 Stunden im Internet, meist entwickelte sich die Störung auf dem Boden eines psychischen Grundleidens, v. a. Angststörungen und posttraumatische Belastungsstörungen, Depressionen und Substanzabhängigkeiten [52].

Die Rolle von Internet- und Cybersex für die Entwicklung einer sexuell süchtigen Symptomatik ist vielfach untersucht worden [3, 54-63]. ‚Cybersex-süchtiges' Verhalten kann als eine Kombination von Internet- und sexueller Sucht verstanden werden. Das besondere Suchtpotential liegt wahrscheinlich in der wechselseitigen Potenzierung eines suchtgefährdenden Mediums und einer Lust erzeugenden Aktivität. In einer Online-Untersuchung von 9.265 Internetnutzern diagnostizierten Cooper und Mitarbeiter [3] bei ca. 1 Prozent eine zwanghaft-süchtige Internet-Sexualität. Die Gruppe mit den meisten sexuell-

zwanghaft/süchtigen Symptomen verbrachten durchschnittlich 11 Stunden pro Woche mit Internet-Sexualität zu. Unter den Cybersex-Nutzern wurde zwischen einem stressreaktivem, einem depressiven und einem Phantasie-Typus unterschieden [64, 65]. Für die Diagnose einer behandlungsbedürftigen Cybersex-süchtigen Problematik genügt nicht die Anwendung eines oder mehrerer Screening-Instrumente [60, 66, 67], die Diagnose sollte von einem erfahrenen Kliniker anhand operationalisierter Kriterien gestellt werden, ggf. mit Informationen von Angehörigen, Partnern, Freunden, Arbeitskollegen oder Vorgesetzten. Besonders anfällig für einen süchtigen Konsum von Internet-Sexualität sind Menschen mit Depressionen, Angststörungen (z.B. sozialen Phobien), Zwangsstörungen, Suchterkrankungen, Paraphilien (Störungen der Sexualpräferenz), Impulskontroll- und Persönlichkeitsstörungen, z.B. Borderline-Persönlichkeitsstörungen [48, 63]. Bei besonders prädisponierten Personen – z.B. Sexualstraftätern – geht eine sexuelle Süchtigkeit mit einem höheren Risiko für Sexualdelikte einher [68].

6 Spezifische Merkmale von Internet-Pornographie

Wiederholt ist das Internet als ‚triple A-engine' bezeichnet worden, wegen der Spezifika *Zugänglichkeit* (accessibility), *niedrige Kosten* (affordability) und *Anonymität* (anonymity) [6]. Das Internet ist bequem vom heimischen Computer, Palm oder Mobiltelefon aus, mittlerweile drahtlos und jederzeit, d.h. an 365 Tagen im Jahr rund um die Uhr zugänglich. Die Kosten sind im Vergleich zu anderer Pornographie extrem niedrig, viele auch explizit sexuelle bzw. pornographische Angebote sind kostenfrei zugänglich, bei monatlichen Kosten für eine Flatrate von unter 10,- €.

Tab. 4: Merkmale von Internetpornographie

1)	*Niedrige Zugangsschwelle*: leicht zugänglich (zu Hause, jederzeit), kostengünstig, anonym
2)	*Mannigfaltigkeit* des pornographischen Materials: Fotos, Filme, Texte, Message-Systeme, Chats (zu zweit oder mit mehreren Personen), audiovisuelle Kommunikation (Mikrofon, Webcams), in Zukunft evtl. auch Übertragung anderer Sinnesqualitäten
3)	*Grenzenloser Markt*: ständig neues Material
4)	*Verschwimmen der Grenzen zwischen Konsument, Produzent und Anbieter*
5)	*Deviantere, gewalttätigere Pornographie*
6)	*Interaktive* Kommunikation mit gegenseitiger Beeinflussung von Fantasien bzw. realem Verhalten, zeitversetzt und synchron
7)	*Raum zum Experimentieren* zwischen Fantasie und ‚real life'-Verhalten
8)	*Virtuelle Identitäten*
9)	ermöglicht konkretes ‚*Selbstvertauschungsagieren'*
10)	erleichtert *suchtartigen Konsum und Produktion*

11) Leichte, unbegrenzte *Vernetzung*: anonyme Kontaktanbahnung zwischen ‚Täter' und ‚Opfer' bzw. verschiedenen ‚Tätern'

12) *Niedriges Risiko* bzgl. Entdeckung illegaler Aktivitäten

Das Internet bietet als Multimedia-Platform ein sehr *mannigfaltiges Angebot* von pornographischem Material und Aktivitäten. Darüber hinaus ist der Pornographie-Markt im Internet nahezu *grenzenlos*. Material aus der ganzen Welt ist unmittelbar verfügbar und dieser Markt verändert sich kontinuierlich. In einer Stunde sind schon wieder andere, neue Bilder, Filme, Texte und besonders Nutzer im Netz. Zudem findet ein Demokratisierungsprozess statt, quasi eine postkommunistische Enteignung der Produktionsmittel: jeder Mann, jede Frau kann mit relativ einfachen technischen Mitteln (einem Computer mit Mikrofon und Webcam) Texte, Bilder, Videos ins Netz stellen und somit weltweit verbreiten. Die Grenzen zwischen Konsument, Produzent und Anbieter verwischen sich im Netz.

Die im Internet zugängliche Pornographie ist nach einer empirischen Untersuchung von Barron und Kimmel [69] insgesamt *gewalttätiger* als Print- oder Video-Pornographie und stellt häufiger non-konsensuelle sexuelle Kontakte und Männer als Täter dar. Sie bietet mehr Freiräume für *ungewöhnliche, deviante Praktiken*. Dies beinhaltet das für Pornographie-Konsum insgesamt belegte Risiko, dass das ‚Ungewöhnliche' mit der Zeit ‚normal' wird, eine Gewöhnung eintritt, das Normale schnell langweilig erscheint [70, 71]. So soll das Internet die späte (‚late onset') Entwicklung von fetischistischen Präferenzen und die Verbreitung von riskanten Sexualpraktiken wie Asphyxie (als sog. ‚breath control') fördern [71]. Wenn man sich im Internet umschaut, scheint es fast zum guten, aufgeklärten Ton zu gehören, wenigstens *einen* Fetisch zu haben: So bietet z.B. das schwule, nichtkommerzielle Internetforum ‚Gayromeo' (*www.gayromeo.de*) mit immerhin 236.000 ‚Usern' (Stand 1.8.2006) alleine in Deutschland für jeden Nutzer ein Profil an, in dem neben 13 verschiedenen Fetischen (von Leder bis Anzug) weitere spezielle sexuelle Präferenzen angekreuzt werden können.

Die *interaktive* Kommunikation stimuliert das wechselseitige Ausgestalten von Fantasien und *virtuellem Experimentieren* mit sexuellen Praktiken und Szenarien. Der Fall des Armin Meiwes, des ‚Kannibalen aus Rotenburg', ist dafür ein gutes, wenngleich extremes Beispiel: Mit ca. 30 Personen tauschte er regelmäßig über mehrere Jahre seine Schlachtungsphantasien im Netz aus, schaltete Online-Kontaktanzeigen und fand schließlich unter 204 Freiwilligen aus mehreren Ländern sein Opfer, mit dem er über längere Zeit intensiven Internet-Kontakt unterhielt [5, 72].

Eine Besonderheit der Cybersexualität und –pornographie ist die Möglichkeit, in Schrift und Bild, evtl. auch im Ton (Sprachmodifikationstechniken) *virtuelle Identitäten* anzunehmen. Erwachsene können sich als Kinder und Jugendliche, Männer als Frauen ausgeben. Auch narzisstischen Größenphantasien bietet sich ein unbegrenzter Gestaltungsraum, nicht nur in Textform. Im Netz kann man sich Material für die eigene ‚Identitätsbildung' aneignen; mittels ‚Fotoshop' und anderer Bildbearbeitungsprogrammen lassen sich Ge-

schlechtsmerkmale beliebig vergrößern, verkleinern oder den eigenen Fantasien anpassen. Ein besonderer Fall einer virtuellen Identität ist das Hineinschlüpfen eines pädophilen Erwachsenen in eine kindliche Identität, das häufig auf einer narzisstischen Problematik beruht. In pädosexuellen Fantasien und Handlungen identifiziert sich der Erwachsene oft oszillierend sowohl mit dem eigenen Kindsein, als auch mit der früheren Elternfigur: er/sie tut an dem Kind das, was er/sie sich früher von den Eltern gewünscht hätte (Zuwendung, Zärtlichkeit), bei gleichzeitiger Identifikation mit der versagenden oder aggressiven Elternfigur (Manipulation, Übergriff). Dieser Mechanismus wurde in Anlehnung an A. E. Meyer [73] als ‚Selbstvertauschungsagieren' bei Pädophilen bezeichnet [74, 75]. Im Internet lässt sich dieses Selbstvertauschungsagieren in einer sehr konkretistischen Art und Weise ‚realisieren', wobei virtuelle Täter und Opfer als Alias-Figuren von der gleichen Person erschaffen und ausgestaltet werden können.

Die genannten Merkmale fördern die Entwicklung von *suchtartigem Konsum* und *Produktion* von Internet-Pornographie und Cybersex (s. o.).

Das Internet ermöglicht potentiellen *Sexualstraftätern* nicht nur einen leichten, anonymen *Kontakt zu potentiellen Opfern*, z.B. Kindern und Jugendlichen [76], sondern auch eine *Vernetzung untereinander* [37]. Im Internet wird Intimität (d.h. Offenbarung von persönlichen Emotionen, Präferenzen und Handlungen, die normalerweise einer breiteren Öffentlichkeit vorenthalten werden) und Vertrauen wahrscheinlich sehr viel schneller entwickelt als bei Face-to-Face-Kontakten [11]. Die Vernetzung von potentiellen Tätern betrifft v. a. Menschen mit devianten sexuellen, z.B. pädosexuellen Präferenzen, die zunehmend das Internet zum Austausch von Informationen, Kinderpornographie und Vorbereitung von sexuellen Übergriffen auf Kinder nutzen [8, 77]. Das *Risiko einer Entdeckung* erscheint vielen dieser Täter offensichtlich eher *gering*. Zwar ist das Internet für den technisch versierten Fachmann längst nicht mehr anonym; der Polizei gelingt es z.B. immer wieder, Internet-Konsumenten bzw. –Händler von Kinderpornographie zu ermitteln und deren Computer und Speichermedien zu beschlagnahmen (für eine umfassende Beschreibung des derzeitigen Stands solcher Ermittlungstechniken s. [8]). Allerdings ist davon auszugehen, dass dabei oft nur die Spitze eines Eisbergs aufgedeckt wird. Die Flüchtigkeit, Flexibilität und Grenzenlosigkeit des Internet schützt vor Entdeckung und effektiver Strafverfolgung (zu den Versuchen Internet-Pornographie zu kontrollieren s. [8, 78, 79]). Zudem dauert die Auswertung der beschlagnahmten Computer und Datenträger aufgrund eingeschränkter personeller Ressourcen bei Polizei und Staatsanwaltschaft häufig sehr lange, im Falle eines Patienten unserer Poliklinik mehrere Jahre.

7 Prävention und Therapie

Wie können die aufgezeigten Risiken des Internet für die Sexualität, insbesondere Produktion und Verbreitung illegaler Pornographie, sexuelle Belästigungen, Anbahnung von Hands-on-Sexualdelikten, aber auch die Entwicklung von sexsüchtigen Verhaltensweisen reduziert werden? Auf Seiten potentieller ‚Opfer' wird häufig auf die Stärkung der Me-

dienkompetenz, v. a. von Kindern und Jugendlichen hingewiesen. Diese sollte auch in der Schule vermittelt werden, da gerade besonders gefährdete Personen häufig aus ungünstigen psychosozialen Familien stammen, die oft dazu nicht in der Lage sind. Empfehlungen für Eltern und andere Erziehungspersonen wurden dazu z.B. von Longo und Mitarbeitern [80] gegeben (Tab. 5). Einschränkend sei daran erinnert, dass in der o.g. Studie von Mitchell und Mitarbeiter [41] keine Schutz vor sexuellen Belästigungen im Internet durch kontrollierende Maßnahmen (Regeln über die Dauer und Art der Internetnutzung, Filter- oder Sperrtechniken, Kontrolle von Bildschirm, Datenverlauf oder Datenspeichern) nachgewiesen werden konnte. Es sollte darüber aufgeklärt werden, dass schon durch die Preisgabe einer E-Mail-Anschrift ein etwas versierter Täter binnen 45 Minuten die Wohnanschrift, Telefonnummer und Schule eines Kindes ausfindig machen kann [80]. In der Primärprävention von sexueller Gewalt kommt generell der Gewährleistung einer allgemeinen, hinreichend guten Sozialisation ohne Traumatisierungen und der Förderung von Selbstsicherheit und allgemeinen sozialen Fähigkeiten eine große Bedeutung zu. Eine gezielte Aufklärung über den möglichst sicheren Umgang mit dem Internet sollte sich daher im Sinne einer Sekundärprävention v. a. an besonders gefährdete, randständige, psychosozial vernachlässigte Kinder und Jugendliche, aber auch Erwachsene richten.

Tab. 5: Empfehlungen für Erziehungspersonen zur Internet-Nutzung von Kindern und Jugendlichen (nach Longo et al. 2002 [80])

- Sexuelle Aufklärung vor der Adoleszenz
- Kein Computer mit Internetzugang im Kinderzimmer
- Installierung von Sicherheitssoftware (u.a. zur Spurenverfolgung des Benutzers)
- Hilfe für Kinder und Jugendliche bei der Erkundung des Cyberspace
- Kinder/Jugendliche lehren, ihre Identität (inkl. e-Mail-Adresse) nicht preiszugeben
- Kinder/Jugendliche lehren, nie auf feindselige, belästigende, inadäquate oder unangenehme Kontakte zu antworten
- Online-Freunde des Kindes kennen lernen
- Kinder aus Chat-Rooms heraushalten oder dabei kontrollieren
- Begrenzung der Zeit am Computer / im Internet

Für die potentiellen ‚Täter' sind die genannten primärpräventiven Maßnahmen ebenfalls gültig. Aus einer randständigen, ungünstigen Sozialisation gehen sowohl Opfer wie Täter hervor, häufig sind spätere Täter früher selbst Opfer in verschiedener Hinsicht gewesen. Darüber hinaus sollte weiterhin der Konsum und die Verbreitung illegaler Pornographie sozial geächtet werden. Die Stärkung der Medienkompetenz und Aufklärung, Supervision und ggf. niedrigschwellige Therapie bei problematischer, sexuell süchtiger Nutzung des Internet sollte sich ebenfalls gezielt an Risikogruppen, z.B. Menschen mit devianter Sexu-

alität bzw. Paraphilien (Störungen der Sexualpräferenz), Persönlichkeitsstörungen (z.B. Borderline- oder dissoziale) oder Suchterkrankungen, richten.

Für die Behandlung problematischer bzw. süchtiger Internet- bzw. Cybersexualität sind mehr oder weniger spezifische Behandlungsprogramme entwickelt worden, die sich z.T. an die Therapie der Spielsucht bzw. sexueller Süchtigkeit anlehnen [46, 48, 63]. Es mangelt bisher aber an evidenz-basierten, d.h. auf kontrollierten Studien fußenden Behandlungsleitlinien. Delmonico et al. [63] unterscheiden dabei zwischen therapeutischen Zielen erster und zweiter Ordnung (Tab. 6): Während die Veränderungen erster Ordnung im Sinne einer Krisenintervention darauf abzielen, durch konkrete Handlungen rasch das Problem zu begrenzen und Folgeschäden zu vermeiden, sollen durch die Veränderungen zweiter Ordnung die tiefer liegenden Ursachen bearbeitet und länger anhaltende Therapieerfolge erzielt werden.

Tab. 6: Behandlungsstrategien bei Cybersex-Süchtigkeit
(modizifiert nach Delmonico et al. 2002 [63])

Therapieziele 1. Ordnung

- Reduzierung der Verfügbarkeit von Internet-Sexualität
- Förderung des Problembewusstseins

Therapieziele 2. Ordnung

- Verringerung der Attraktivität der Internet-Sexualität
- Psychiatrisch-psychologische Diagnostik und Behandlung komorbider Störungen
- Bearbeitung assoziierter Probleme: z.B. Trauerprozesse, Stress- und Wut-Management, Schuld und Scham, Kindheitstraumata, kognitive Verzerrungen, Opfer-Empathie
- Abbau der sozialen Isolation
- Förderung einer integrativeren und beziehungsreicheren Sexualität
- Einbeziehung von Partnern, Kindern, Angehörigen, Freunden oder Arbeitskollegen

Im ersten Schritt soll im Sinne einer Stimuluskontrolle bzw. -Abstinenz der Zugang zu Internet-Sexualität beendet werden. Oft ist es anfangs notwendig, dass der Betreffende seinen Internetzugang abmeldet oder nur am Arbeitsplatz nutzt. Es kann aber auch ausreichen, den Computer in einem anderen, besser kontrollierbaren Raum zu installieren; Kontroll-Software zu installieren (z.B. CyberPatrol, NetNanny, SafeSurf, SurfWatch); einen Internet-Anbieter zu wählen, der die zugänglichen Inhalte filtert; oder die Zeit im Internet zu begrenzen. Parallel dazu soll das Bewusstsein für die mit dem Internet-Konsum verbundenen Probleme gefördert, Bagatellisierungstendenzen abgebaut und eine Änderungsmotivation erreicht werden [81].

In dem zweiten Schritt soll versucht werden, die weiter bestehende Attraktivität des Internet für den Patienten zu reduzieren, Alternativen zu entwickeln und damit den häufig ritualisierten Konsum von Cybersex zu verändern. Ein besonderes Augenmerk sollte auf eine umfassende psychiatrisch-psychologische Diagnostik und Behandlung komorbider Störungen gelegt werden, v. a. Angst- und Zwangsstörungen, Depressionen, Suchterkrankungen, Paraphilien und Persönlichkeitsstörungen. Je nach Symptomatik ist auch eine medikamentöse Behandlung, z.B. mit einem Selektiven Serotonin-Wiederaufnahme-Hemmer (SSRI) zu erwägen. SSRIs, die sich in Behandlung von Depressionen, Angst- und Zwangserkrankungen bewährt haben, werden seit Anfang der 1990er Jahre auch erfolgreich in der Behandlung sexueller süchtiger, zwanghafter und impulsiver Symptome eingesetzt, wobei bisher keine doppelblinden, placebokontrollierten Studien vorliegen [48, 82, 83]. Neben der Behandlung manifester psychischer Störungen sollen weitere, mit der Cybersex-Süchtigkeit direkt oder indirekt verbundene psychische Probleme bearbeitet werden, v. a. Trauerprozesse, Stress- und Wut-Management, Schuld- und Schamgefühle, Kindheitstraumata.

Zu bearbeiten sind zudem die kognitiven Verzerrungen (Bagatellisierungen und Verleugnungen), derer sich die Täter z.B. beim Konsum von Kinderpornographie häufig bedienen (z.B. ‚ein Nacktfoto schadet keinem Kind', ‚solche Fotos sind sowieso im Netz'). Eng verknüpft damit ist die Verbesserung von Opfer-Empathie, d.h. die Täter sollen lernen, sich besser einzufühlen in die möglichen Folgen z.B. der Herstellung von Kinderpornographie für die betreffenden Kinder, sowohl die kurzfristigen (z.B. Misstrauen und Enttäuschung durch Ausnutzen eines Vertrauensverhältnis, Scham, Angst, Ekel), als auch die langfristigen Folgen (z.B. Gefühl, keine Kontrolle über die Verbreitung und Nutzung der im Internet kursierenden Bilder zu haben, starke Sexualisierung oder Vermeidung von Sexualität, psychische Störungen wie Depressionen, Persönlichkeitsstörungen). Letztlich sollte die Gesamtbehandlung von Sexualstraftätern, die das Internet nutzen, dem entsprechen, was für die Behandlung von Sexualstraftätern im Allgemeinen gilt, und kann im Einzelfall auch eine medikamentöse Behandlung beinhalten [82-84].

Für viele Patienten stellt die der Cybersex-Süchtigkeit zugrunde liegende und durch sie verstärkte soziale Isolierung und Vereinsamung ein besonderes Problem dar. Es ist oft ein schwieriges, langwieriges Unterfangen, nicht vorhandene oder lange Zeit vernachlässigte ‚real-life' Kontakte neu aufzubauen. Eng verbunden mit dem Abbau sozialer Isolation ist die Entwicklung einer befriedigenderen, integrativeren und beziehungsreicheren Sexualität, die neben Selbstbefriedigung auch ‚face-to-face' und körperliche zwischenmenschliche Kontakte umfasst. Es wird vor der Gefahr eines Rückzugs in totale sexuelle Abstinenz gewarnt [63]. Nicht nur bei diesem Therapieziel wird eine generelle Gefahr offensichtlich, die das Konstrukt sexueller Süchtigkeit und dessen Behandlung in sich birgt: leicht schleichen sich mehr oder weniger explizit normative Vorstellung über ‚gesunde', ‚nichtdeviante', ‚normale' Sexualität ein, die z.T. einen moralisierenden, auch religiösen Hintergrund haben. Dies spiegelt sich z.B. in den, nicht nur in den USA verbreiteten Selbsthilfegruppen für Sexsüchtige wider, die in Anlehnung an das 12-Schritte-Programm der A-

nonymen Alkoholiker konzipiert sind [48], als auch einem von Delmonico und Mitarbeitern [63] angeführten Therapieziel zweiter Ordnung, der Förderung von Spiritualität, das hier bewusst nicht in die Therapiestrategien (Tab. 6) aufgenommen wurde.

Um die genannten Ziele zu erreichen, kann es hilfreich sein, Partner, Kinder, Angehörige, Freunde oder Arbeitskollegen in die Diagnostik oder Behandlung mit einzubeziehen. Dies kann z.B. die Offenlegung der sexuellen Problematik beinhalten, selbstverständlich immer nur in Absprache und mit dem Einverständnis des Patienten, aber auch die Förderung protektiver Faktoren. Delmonico und Mitarbeiter [63] warnen jedoch davor, zu frühzeitig und unreflektiert Paartherapien durchzuführen. Ebenso wenig sollten Partner und Angehörige mit Kontroll- und Überwachungsaufgaben betraut und überfordert werden. Selbsthilfegruppen können in der Behandlung hilfreich sein, auch dazu liegen jedoch keine empirischen Daten vor.

8 Ausblick

Die rasante technische Entwicklung des Internet und anderer Medien wird weiterhin die Sexualität und zwischenmenschlichen Beziehungen maßgeblich verändern und beeinflussen. In Zukunft werden wahrscheinlich alle Sinnesqualitäten – audiovisuell, taktil und olfaktorisch - mittels Ganzkörper-Datenanzug, Datenhelm und -handschuh per Internet kommuniziert bzw. simuliert werden (‚Virtual Reality Cybersex', ‚Teledildonics', vgl. [18, 85, 86]). Dabei sind nicht nur die hier fokussierten Risiken, sondern auch die Chancen zu würdigen. So favorisiert Döring (2004) aus feministischer Perspektive ein sog. sexuelles Empowerment. Dies könnte die bereichernde Exploration von Bedürfnissen einerseits, und das Aushandeln von Grenzen andererseits ermöglichen - und die ideologischen Spaltungen in Internet-feindliche Kulturpessimisten und unkritische, neoliberale Konsumfetischisten überwinden. Frühzeitiges Aufklären und Lernen über den geeigneten, sicheren Umgang mit dem Internet, z.B. in der Schule, sollte ausgebaut und evaluiert werden. Trotz aller primär- und sekundärpräventiver Bemühungen ist allerdings weiterhin mit problematischen Entwicklungen für bestimmte Personengruppen zu rechnen. Es gilt, dafür genauere diagnostische Kriterien zu etablieren und empirisch zu überprüfen, die Ursachen für pathologische Entwicklungen zu ergründen (z.B. Wechselwirkungen zwischen dem Nutzer und dem Medium, Bindungsverhalten und neurobiologische Prozesse), valide Erhebungsinstrumente zu entwickeln und mehr oder weniger spezifische Beratungs- und Behandlungsmaßnahmen – psycho- und soziotherapeutische wie medikamentöse - in kontrollierten Studien auf ihre Wirksamkeit hin zu überprüfen. Auch die technischen Möglichkeiten von Regulierung sollten diesbezüglich weiterentwickelt werden.

Literatur

[1] Dudenredaktion (Hrsg) (2001) Duden – Fremdwörterbuch. Dudenverlag, Mannheim

[2] Dressler S, Zink C (2003) Pschyrembel Wörterbuch Sexualität. De Gruyter, New York.

[3] Cooper A, Delmonico DL, Burg R (2000) Cybersex Users and Abusers: New Findings and Implications. J Treat Prev 1-2: 5-30.

[4] Schwartz J (2001) New Economy: The Steamy Side of the Internet, Pervasive and Resilient to Recession, is the Underpinning of a New Online Cash Venture. New York Times, S 4.

[5] Döring N (2004) Cybersex – Formen und Bedeutungen computervermittelter sexueller Interaktionen. In: Richter-Appelt H, Hill A (Hrsg) Geschlecht zwischen Spiel und Zwang. Psychosozial-Verlag, Gießen, S 177-207.

[6] Cooper A, Griffin-Shelley E (2002) Introduction. The Internet: The Next Sexual Revolution. In: Cooper A (Hrsg) Sex and the Internet. Brunner-Routlege, New York, S 1-15.

[7] Stone AR (1995) The War of Desire and Technology at the Close of the Mechanical Age. MIT Press, Cambridge, MA.

[8] Ferraro MM, Casey E (2005) Investigating Child Exploitation and Pornography. Elsevier Acad Press, Burlington, USA, S 21-40.

[9] Dannecker M (2000) Wider die Verleugnung sexueller Wünsche. In: Aids Infothek 1, S 4-10.

[10] Dekker A (2004) Körper und Geschlechter in virtuellen Räumen. In: Richter-Appelt H, Hill A (Hrsg) Geschlecht zwischen Spiel und Zwang. Psychosozial-Verlag, Gießen, S 209-224.

[11] Ross MW (2005) Typing, Doing, and Being: Sexuality and the Internet. J Sex Res 42: 342-352.

[12] Dekker A (2004) Cybersex und Online-Beziehungen. In: Hornung R, Buddeberg C, Bucher T (Hrsg) Sexualität im Wandel. vdf, Hochsch.-Verlag, Zürich, S 159-179.

[13] Bauman Z (2003) Liquid Love. Polity Press, Cambridge, MA.

[14] Giddens A (1992) The Transformation of Intimacy: Sexuality, Love and Eroticism in Modern Societies. Stanford University Press, Oxford.

[15] Gagnon J, Simon W (1973) Sexual Conduct: The Social Sources of Human Sexuality. Hutchinson London.

[16] Simon W (1996) Postmodern Sexualities. Routledge, London.

[17] Barak A, King SA (2000) The Two Faces of the Internet: Introduction to a Special Issue on the Internet and Sexuality. Cyberpsychol Behav 3: 517-520.

[18] Weise ER (1996) A Thousand Aunts with a Modem. In: Cherny L, Weise ER (Hrsg) Wired Women: Gender and New Realities in Cyberspace. Seal Press, Seattle, WA.

[19] Seto MC, Maric A, Barbaree HE (2001) The Role of Pornography in the Etiology of Sexual Aggression. Aggr & Viol Beh 6: 35-53.

[20] Barwick, Helena (2003) A Guide to the Research into the Effects of Sexually Explicit Films and Videos. Office of Film& Literature Classification, Wellington, Australia.

[21] Stoller RJ (1975/1998) Perversion - Die erotische Form von Hass. Psychosozial-Verlag, Gießen.

[22] Stoller RJ (1991) Porn - Myths for the Twentieth Century. Yale University, Yale.

[23] Berner W, Hill A (2004) Gewalt, Missbrauch, Pornografie. In: Hornung R, Buddeberg C, Bucher T (Hrsg) Sexualität im Wandel. vdf, Hochsch.-Verlag, Zürich, S 141-157.

[24] Boeringer SB (1994) Pornography and Sexual Aggression: Associations of Violent and Nonviolent Depictions with Rape and Rape Proclivity. Deviant Behavior: an Interdisciplinary Journal 15: 289-304.

[25] Allen M, D'Alessio D, Brezgel K (1995) A Meta-Analysis Summarizing the Effects of Pornography II, Hum Comm Res 22: 258-283.

[26] Oddone-Paolucci E, Genius M, Violato C (2000) A Meta-Analysis of the Published Research on the Effects of Pornography. In: Violato C, Oddone-Paolucci E, Genius M (Hrsg) The Changing Family and Child Development. Ashgate, Aldershot , UK, S 48-59.

[27] Malamuth NM, Addison T, Koss M (2000) Pornography and Sexual Aggression: Are There Reliable Effects and Can We Understand Them? Ann Rev Sex Res 6: 26-91.

[28] Allen M, D'Alessio D, Emmers-Sommer TM (2000) Reactions of Criminal Sexual Offenders to Pornography: A Meta-Analytic Summary. In: Roloff M (Hrsg) Communication Yearbook 22. Sage, Thousand Oaks, CA, S 139-169.

[29] Marshall WL (1988) The Use of Sexually Explicit Stimuli by Rapicts, Child Molesters and Nonoffenders, J Sex Res 25: 267-288.

[30] Kearns CM, Nutter DE (1988) A Preliminary Examination of the Pornography Experience of Sex offenders, Paraphiliacs, Sexual Dysfunction Patients, and Controls based on Meese Commission Recommendations. J Sex Marit Ther 14: 285-298.

[31] Nutter DE, Kearns ME (1993) Patterns of Exposure to Sexually Explicit Material Among Sex Offenders, Child Molesters and Controls. J Sex Marit Ther 19: 77-85.

[32] Langevin R, Curnoe S (2004) The Use of Pornography During the Commission of Sexual Offences. Int J Offender Ther Comp Criminol 48: 572-86.

[33] Seto MC, Eke AW (2005) The Criminal Histories and later Offending of Child Pornography Offenders. Sex Abuse: J Res Treat 17: 201-10.

[34] Kutchinsky B (1999) Law, Pornography and Crime. The Scandinavian Res Council Criminol 16: 11-347.

[35] Diamond M, Uchiyama A (1999) Pornography, Rape, and Sex Crimes in Japan. Int J Law Psychiatry 22: 1-22.

[36] McGrath MG, Casey E (2002) Forensic Psychiatry and the Internet: Practical Perspectives on Sexual Predators and Obsessional Harassers in Cyberspace. J Am Acad Psychiatry Law 30: 81-94.

[37] McGrath M (2005) Cyber Offenders. In: Ferraro MM, Casey E (Hrsg) Investigating Child Exploitation and Pornography: The Internet, the Law and Forensic Science. Elsevier Academic Press, USA, S 51-78.

[38] Hughes DM (2004) The Use of New Communications and Information Technologies for Sexual Exploitation of Women and Children. In: Waskul DD (Ed) net.seXXX – Reading on Sex, Pornography, and the Internet. Peter Lang, New York, S 105-107.

[39] Bundeskriminalamt (Hrsg) (2005) Polizeiliche Kriminalstatistik 2004 - Bundesrepublik Deutschland. Bundeskriminalamt, Wiesbaden.

[40] *www.bka.de/pks/pks2004*

[41] Mitchel KJ, Finkelhor D, Wolak J (2001) Risk Factors for and Impact of Online Sexual Solicitation of Youth. JAMA 285: 3011-3014.

[42] Wolak J, Finkelhor D, Mitchel KJ (2004) Internet-Initiated Sex Crimes against Minors: Implications for Prevention Based on Findings from a National Study. J Adolesc Health 35: 424.e11-20.

[43] Walsh WA, Wolak J (2005) Nonforcible Internet-related Sex Crimes with Adolescent Victims: Prosecution Issues and Outcomes. Child Maltreat 10: 260-71.

[44] Frei A, Ereney N, Dittmann V, Graf M (2005) Paedophilia on the Internet. A Study of 33 Convicted Offenders in the Canton of Lucerne. Swiss Med Wkly 135: 488-494.

[45] Galbreath NW, Berlin FS, Sawyer D (2002) Paraphilias and the Internet. In: Cooper A (Hrsg) Sex and the Internet, Brunner-Routlege, New York, S 187-205.

[46] Goodman A (1998) Sexual Addiction: An Integrated Approach. Int. Universities Press Madison. Conn.

[47] Kafka MP, Hennen J (1999) The Paraphilia-Related Disorders: An Empirical Investigation of Nonparaphilic Hypersexuality Disorders in Outpatient Males. J Sex Mar Ther 25: 305-319.

[48] Briken P, Hill A, Berner W (2005) Sexuelle Sucht: Diagnostik, Ätiologie, Behandlung. Z Sexualforsch 18: 185-196.

[49] Bancroft J, Vukadinovic Z (2004) Sexual Addiction, Sexual Impulsivity, or What? Toward a Theoretical Model. J Sex Res 41: 225-234.

[50] Goldsmith TD, Shapira NA (2006) Problematic Internet Use. In: Hollander E, Stein DJ (Eds) Clinical Manual of Impulse-Control-Disorders. Am Psychiatric Publ, Washington DC, US, S 291-308.

[51] Young KS (2004) Internet Addiction: A New Clinical Phenomenon and Its Consequences. Am Behav Sci 48: 402-415.

[52] Kratzer S (2006) Pathologische Internetnutzung. Pabst Science Publishers, Lengerich.

[53] Taintor MD (2005) Telemedicine, Telepsychiatry, and Online Therapy. In: Sadock BJ, Sadock VA (Hrsg) Kaplan & Sadock's Comprehensive Textbook of Psychiatry, 8.Aufl. Lippincott Williams & Wilkins, Baltimore, S 955-963.

[54] Cooper A, Scherer CR, Boies SC, Gordon BL (1999) Sexuality on the Internet: From Sexual Exploration to Pathological Expression. Prof Psych: Research and Practice 230: 154-164.

[55] Griffith M (2000) Excessive Internet Use: Implications for Sexual Behavior, Cyberpsychol Behav 3: 537-553.

[56] Greenfield DN (1999) Virtual Addiction, New Harbinger Publications, Oakland, CA.

[57] Putnam DE (2000) Initiation and Maintenance of Online Sexual Compulsivity: Implications for Assessment and Treatment. Cyberpsychol Behav 3: 553-564.

[58] Putnam DE, Maheu MM (2000) Online Sexual Addiction and Compulsivity: Integrating Web Resources and Behavioral Telehealth in Treatment. Sexual Addiction and Compulsivity 7: 91-112.

[59] Schwartz MF, Southern F (2000) Compulsive Cybersex: The New Tea Room. Sexual Addiction and Compulsivity 7: 127-144.

[60] Young K (1998) Cybersexual Addiction Quiz. *http://www.netaddiction.com/resources/cybersexual_addiction_quiz.htm*

[61] Stein DJ, Black DW, Shapira, NA, Spitzer R (2001) Hypersexual Disorder and Preoccupation with Internet Pornography. Am J Psychiatry 158: 1590-1594.

[62] Griffiths MD (2001) Sex on the Internet: Observations and Implications for Internet Sex Addiction. J Sex Res 38: 333-342.

[63] Delmonico DL, Griffin E, Carnes PJ (2002) Treating Online Compulsive Sexual Behavior: When Cybersex Is the Drug of Choice. In: Cooper A (Hrsg) Sex and the Internet. Brunner-Routlege, New York, S 147-167.

[64] Cooper A, Putnam DE, Planchon LA, Boies SC (1999) Online Sexual Compulsivity: Getting Tangled in the Net. J Treat Prev 6: 79-104.

[65] Cooper A, Griffin-Shelley E, Delmonico DL, Mathy R (2001) Online Sexual Problems: Assessment and Predictive Variables. J Treat Prev 8: 267-285.

[66] Delmonico DL (1999) Internet Sex Screening Test. *http://www.sexhelp.com/internet_screening_test.cfm*

[67] Putnam DE (1997) Online Sex Addiction Questionnaire. *http://onlinesexaddict.com/osaq.html*

[68] Briken P, Habermann N, Kafka MP, Berner W, Hill A (2006) The Paraphilia-Related Disorders: An Investigation of the Relevance of the Concept in Sexual Murderers. J Forensic Sci 51: 683-688.

[69] Barron M, Kimmel M (2000) Sexual Violence in Three Pornographic Media: Toward a Sociological Explanation. J Sex Res 37: 161-168.

[70] Koop CE (1987) Report of the Surgeon Gerneral's Workshop on Pornography and Public Health. Am Psycholist 42: 944-945.

[71] Bancroft J (2002) Preface. In: Sex and the Internet- A Guidebook for Clinicians, Brunner-Routlege, New York, ix-xiii.

[72] Egg R (2005) Armin M – A German Cannibal. Vortrag auf First International Conference of Sexual Offences, São Paulo, Brasilien.

[73] Meyer AE (1976) Zur Psychoanalyse der Perversionen. Sexualmedizin 5: 169-176.

[74] Berner W (1985) Das Selbstvertauschungsagieren Pädophiler. Psychother Psychosom med Psychol 35: 1-40.

[75] Pfäfflin F (2004) Sexualstraftaten. In: Foerster K, Venzlaff U (Hrsg) Psychiatrische Begutachtung. Urban & Fischer Verlag, München, S 275-302.

[76] McGrath M (2005) Cyber Victims. In: Ferraro MM, Casey E (Hrsg) Investigating Child Exploitation and Pornography: The Internet, the Law and Forensic Science. Elsevier Academic Press, USA, S 41-49.

[77] Alexy EM, Burgess AW, Baker T (2005) Internet Offenders - Traders, Travelers, and Combination Trader-Travelers. J Interpers Viol 20: 804-812.

[78] Roberds SC (2004) Technology, Obscenity, and the Law: A History of Rescent Efforts to Regulate Pornography on the Internet. In: Waskul DD (Ed) net.seXXX – Reading on Sex, Pornography, and the Internet. Peter Lang, New York, S 295-315.

[79] Mitchel KJ, Finkelhor D, Wolak J (2005) The Internet and Family and Acquaintance Sexual Abuse. Child Maltreat 10: 49-60.

[80] Longo RE, Brown SM, Orcutt DP (2002) Effects on Internet Sexuality on Children and Adolescents. In: Cooper A (Hrsg) Sex and the Internet. Brunner-Routledge, New York, S 87-104.

[81] Miller WR, Rollnick S (1991) Motivational Interviewing. Guilford, New York.

[82] Hill A, Briken P, Kraus C, Strohm K, Berner W (2005) Medikamentöse Therapie von Sexualstraftätern. In: Wischka B, Rehder U, Specht F, Foppe E, Berner W (Hrsg) Sozialtherapie im Justizvollzug. Kriminalpädagogischer Verlag, Lingen, S 344-359.

[83] Berner W, Hill A, Briken P (2006) (in press) Sexualstraftäter behandeln mit Psychotherapie und Medikamenten. Eine Anleitung. Dt Ärzteverlag, Köln.

[84] Marshall WL, Anderson D, Fernandez Y (1999) Cognitive Behavioural Treatment of Sexual Offenders. Wiley, Chichester.

[85] Rheingold H (2004) Teledildonics: Reach Out and Touch Someone. In: Waskul DD (Ed) net.seXXX – Reading on Sex, Pornography, and the Internet. Peter Lang, New York, S 319-322.

[86] Barber T (2004) A Pleasure Prophecy: Predictions for the Sex Tourist of the Future. In: Waskul DD (Ed) net.seXXX – Reading on Sex, Pornography, and the Internet, Peter Lang, New York, S 323-336.

Suizidforen im Internet: Gefahr oder präventiver Nutzen?

Dr. Christiane Eichenberg

1 Einleitung

Es gibt eine Reihe von Schnittstellen zwischen dem Internet und der Klinischen Psychologie als theoretische und angewandte Teildisziplin der Psychologie (zur Übersicht siehe [1]). Während man sich in der Forschung wie Praxis zunächst mit den Möglichkeiten des Internet zur Intervention beschäftigte, wurden später zunehmend auch die klinisch relevanten Effekte der Internetnutzung diskutiert, und hier vorwiegend dramatischere Problembereiche. Am häufigsten wurde dabei der Themenkomplex des pathologischen Internetgebrauchs problematisiert (zur Übersicht siehe z.B. [2] [3)], gefolgt von dem Internet-Sex-Diskurs, der sowohl die klinisch relevanten Ausprägungen der verschiedenen Arten von Online-Sexualität als auch die Auswirkungen sexueller Inhalte und Nutzungsweisen von Kindern, Jugendlichen und jungen Erwachsenen fokussierte (zur Übersicht siehe [4]). Spätestens nach dem ersten via Internet verabredeten Selbsttötungs-Rendezvous im Jahr 2000 zwischen dem 24jährigen Norweger Daniel V. und der Österreicherin Eva D., 17, das mit einem Aufruf zu einem gemeinschaftlichen Suizid in der Newsgroup <alt.suicide.holiday> begann (s. Abb. 1) und mit einem gemeinsamen Sprung von einer Felsenklippe endete, wird das Internet in einem weiteren Zusammenhang sowohl in Fachkreisen als auch der Öffentlichkeit diskutiert.

Datum: 02.09.2000

Hello a.s.h. readers,

This is my first posting to this newsgroup, so if this message is inappropriate for this group, please accept my apologies. Also, this message is only for people determined to kill themselves, so if this is not your desire, you can stop reading now.

I am planning on committing suicide, and I've been thinking about this for quite some time (years), it's not some impulse decision.

But, and this may sound a bit bizarre to some I guess, I would like to do this together with someone else. So, if someone else has similar wishes, please get in touch with me. I live in Norway, so it would be best if you live somewhere near (by this I mean Northern Europe, I am willing to do some traveling / alternatively pay for your ticket to get here, if funds are tight)

Any serious replies are welcome, send me a mail and we can arrange it. Do-gooders and trolls, save yourself the trouble and go on to the next posting.

Yours, Dan

Abb. 1: Posting in der Newsgroup <alt.suicide.holiday>

Angesprochen ist damit die Existenz so genannter ‚Suizidforen', d.h. virtuelle Diskussionsplattformen, in denen sich vorrangig Menschen mit Suizidgedanken austauschen. Im deutschsprachigen Raum existieren ca. 30 solcher Foren, international tausende.

Werden das generelle Potenzial des Internet zur Selbsthilfe bei verschiedenen Störungen und Problembereichen[5] sowie die Chancen zur Suizidprävention[6 7] mittels dieses Mediums insgesamt positiv eingeschätzt, so ist die Beurteilung bezüglich der Gefahren bzw. des Nutzens dieser Suizid-Selbsthilfeforen sehr heterogen (s. Tabelle 1), wobei alarmierende Stimmen deutlich überwiegen. Dabei beruhen die Beurteilungen fast ausschließlich auf theoretischen Überlegungen bzw. anekdotischen Berichten.

Tab. 1: Potenzielle Risiken und Chancen von Suizid-Selbsthilfeforen

Gefährdende Effekte	**Suizidpräventive Effekte**
Weitere Labilisierung insbesondere bei jungen[8] u. psychisch kranken Menschen[9]	Enttabuisierung eines in der Gesellschaft stark stigmatisierten Themas[13]
Verbreitung von Suizidmethoden[10]	Abbau suizidalen Handlungsdrucks durch Diskussionen über Suizidmethoden[14]
Ansteckung und Imitation (‚Werther-Effekt')[11]	Anonymer und unzensierter Austausch mit anderen Betroffenen mit dem Effekt der sozialen Unterstützung[15]
Schwellenerniedrigung i. S. des Abbaus von Ambivalenzen durch Prozesse des Gruppendrucks[12]	Kontaktaufnahme zu suizidalen Menschen von Seiten Professioneller, die auf andere Weise nicht erreicht würden[16]
Veränderung der Einstellungen zum Suizid[9]	Erleichterter Zugang zu professionellen Krisenangeboten[17]
Conclusion: Staatliche Maßnahmen zur Zensur entsprechender Internet-Inhalte und zur Foren-Schließung	Conclusion: Selbsthilfeaktivität suizidaler Internetnutzer fördern

Beide Positionen sind spekulativ, denn sowohl einseitige Schädlichkeitszuschreibungen, die - gespeist durch spektakuläre Medienberichte - sich insbesondere auf die Ansteckungs- und Aufschaukelungseffekte beziehen, als auch beschwichtigende Haltungen beruhen auf ungeprüften Annahmen. Die empirische Forschungslage zu den Inhalten, Funktionen und Effekten dieser Foren ist nicht nur ergänzungs-, sondern grundsätzlich klärungsbedürftig. Bisher liegt nichtmals eine Hand voll *systematischer* Studien vor, die sich empirisch mit der Thematik befassen. Z.B. stellte Fekete[18] mittels einer inhaltsanalytischen Untersuchung divergierende Kommunikationsmuster in unterschiedlich ausgerichteten Foren (Depression, Angst, Suizidalität) fest. Miller und Gerge[19] analysierten in einem Zeitraum von 11 Monaten alle Postings des ‚AOL suicide bulletin boards' und kamen zu dem Schluss, dass die meisten Beiträge positive und empathisch-unterstützende Inhalte hatten. Schmidtke, Schaller und Kruse[11] gingen der Frage nach, ob sich in solchen Foren Häufungen bei Suiziden oder Suizidversuchen in bestimmten Zeiträumen nachweisen lassen. Ihre Hypothese ist, dass eine episodische überzufällige Häufung von Verabredungen zu suizidalem Verhalten Imitationseffekte nahe legt. Zwar weisen ihre Ergebnisse in diese Richtung - Postings mit der Suche nach Suizidpartnern traten in bestimmten Zeiträumen gehäuft auf – jedoch ist damit noch kein Imitationsverhalten innerhalb eines Forums bewie-

sen, da auch andere Ursachen (saisonale Effekte, Berichte in anderen Medien) diese erhöhte Häufigkeit bedingt haben könnten. Winkel[13] konnte mit einer multimethodalen Studie zeigen, dass User solcher Foren viel soziale Unterstützung und nur in geringem Ausmaß soziale Belastung erfahren.

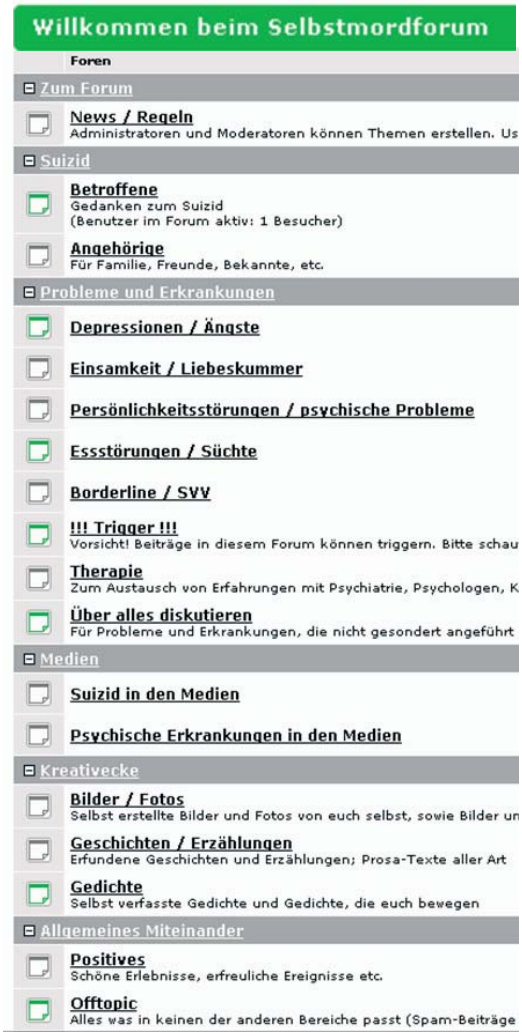
2 Fragestellung

In der vorliegenden Studie sollen spekulativen Annahmen über destruktive vs. konstruktive Funktionen von ‚Suizidforen' empirische Ergebnisse gegenübergestellt werden. Ungeklärte Forschungsfragen betreffen insbesondere Charakteristika der Nutzerklientel und werden daher aufgegriffen: Welche soziodemografischen Merkmale besitzen die Teilnehmer von ‚Suizidforen'? Welche ‚suizidale Geschichte' haben sie? Welche Motive sind ausschlaggebend für die Partizipation an solchen virtuellen Plattformen? Lassen sich verschiedene Nutzertypen identifizieren? Welche Inhalte dominieren die Forendiskussion? Welche Effekte sind zu erwarten?

3 Methode

Um die aufgeführten Forschungsfragen zu klären, wurde in dem meistfrequentierten Forum im deutschsprachigen Internet (*www.selbstmordforum.de*) eine Online-Befragungsstudie durchgeführt.

Diese Datenerhebungsmethode war der niederschwelligste Zugang zu der Stichprobe. Da sich bei webbasierten Umfragen gegenüber traditionellen schriftlichen Befragungen besondere Probleme ergeben, wurde eine professionelle Befragungssoftware[1] genutzt, die eine Reihe von datenqualitätssteigernde Features bietet (z.B. Filterführung, Plausibilitätscheck, Vollständigkeitskontrolle, Kontrolle von MehrfachausfüllerInnen) und die in der einschlägigen Literatur zur Online-Forschung (z.B. [20]) empirisch abgesicherten Empfehlungen zu Aufbau



[1] *http://www.globalpark.de*

und Gestaltung von webbasierten Fragebögen berücksichtigt.

In der vorliegenden Studie kam ein Fragebogen mit 29 Items zum Einsatz. Darin wurden u.a. folgende Angaben der Nutzer erhoben: Soziodemografische Daten, Angaben zur suizidalen Geschichte und der Ausprägung suizidaler Gedanken, Nutzungsgewohnheiten und Motive zur Teilnahme am selbstmordforum.de, Inhalt der eigenen Postings, Selbsteinschätzung der Veränderung der suizidalen Problematik durch die Teilnahme am selbstmordforum.de. Der Aufruf zur Studie wurde auf der Startseite des Portals platziert und die Teilnahme durch eine Befürwortung des Webmasters motiviert. Der Erhebungszeitraum betrug vier Wochen (März / April 2003) und führte zu 164 komplett ausgefüllten Fragebögen.

4 Ergebnisse

4.1 Soziodemografie und Suizidalität

Die Gesamtstichprobe setzt sich aus 164 Personen (je 50 % männlich bzw. weiblich) zusammen. Die Probanden wiesen eine überwiegend adoleszente Altersstruktur auf (59 % < 21 Jahre; 88 % ≤ 30 Jahre). Der größte Teil der Befragungsteilnehmer lebte als Single (80 %).

Bezüglich der suizidalen Geschichte zeigte sich, dass die Gruppe derer mit einer kurzen Vergangenheit (< 1 Jahr) hinsichtlich des Erlebens suizidaler Gedanken relativ gering war (14,0 % der Gesamtstichprobe); demgegenüber bestanden bei 28,6 Prozent suizidale Tendenzen zwischen 1-3 Jahre und 34,1 Prozent der befragten Forumsnutzer hatten die Suizidgedanken schon länger als fünf Jahre. Bei denjenigen, die angaben, noch nie suizidale Gedanken gehabt zu haben (11,6 %), wurden die weiteren Items zur Erhebung der suizidalen Erfahrungen ausgeschlossen.

Von den Befragungspersonen mit erlebten Suizidgedanken (N = 145) hatten über die Hälfte mindestens einen Suizidversuch unternommen (55 %); 19 Prozent gaben an, zwei bis drei mal versucht zu haben, sich das Leben zu nehmen. Noch häufigere Suizidversuche wurden selten berichtet. Unterschiede zwischen den Geschlechtern ergaben, dass die befragten Frauen signifikant häufiger Suizidversuche unternommen haben ($Z = 2116$; $p < .05$) und ihre suizidalen Gedanken länger bestehen ($Z = 2763{,}5$; $p < .05$).

4.2 Nutzung des Forums

Ingesamt nutzten 78 Prozent der Befragungsteilnehmer ausschließlich das selbstmordforum.de, nur 22 Prozent gaben an, noch weitere ‚Suizidforen' im Internet zu frequentieren. Obwohl die Anzahl derjenigen, deren suizidale Problematik sich erst in jüngerer Zeit entwickelt hatte, gering war, fand sich eine deutliche Gruppe von Personen, die das Forum erst vor kurzem das erste mal aufgesucht hatten: 29 Prozent nutzten es seit weniger als einem Monat, 22 Prozent seit weniger als sechs und 15 Prozent seit weniger als 12 Mona-

ten. Demgegenüber waren jedoch auch 34 Prozent mit dem Forum schon länger als ein Jahr verbunden.

Die Nutzungsintensität des untersuchten Forums war hoch: Knapp die Hälfte der Stichprobe (45 %) besuchte es im Durchschnitt mindestens täglich, wobei Gelegenheitsbesucher (seltener als einmal im Monat) aber auch deutlich vertreten waren (17 %).

Motive das Forum zu besuchen

Zur Erfassung der Motive der User zur Teilnahme am Forum wurden mögliche Gründe vorgegeben, die die Befragungspersonen auf einer 5-stufigen Ratingskala nach dem Grad des Zutreffens für sich einschätzten (0 = *trifft gar nicht zu* bis 4 = *trifft vollkommen zu*) (s. Tab. 2).

Tab. 2: Motive zur Forumsteilnahme auf einer 5-stufigen Ratingskala (0 = *trifft gar nicht zu* bis 4 = *trifft vollkommen zu*) (Mittelwerte und Standardabweichungen) (N = 164)

Motive	***M***	***SD***
um Menschen mit ähnlichen Problemen/Gedanken kennen zu lernen	2.5	1.3
um meine Probleme, die hinter meinen Selbstmordgedanken stehen, mitteilen zu können	2,0	1.5
um in einer akuten suizidalen Krise AnsprechpartnerInnen zu finden	1.7	1.5
Neugier	1.7	1.5
um anderen zu helfen	1.7	1.3
um meine Selbstmordgedanken loszuwerden	1.4	1.3
um mit Menschen mit ähnlichen Problemen die Krise zu überwinden	1.4	1.2
um Hinweise zu effektiven Selbstmordmethoden zu bekommen	1.3	1.6
um Informationen über professionelle Hilfe zu bekommen	0.8	1.1
um jemanden zu finden, der sich mit mir zusammen umbringt	0.6	1.2
um Informationen zu bekommen, wie Menschen mit Selbstmordgedanken am besten zu begegnen ist	0.5	1.2

So nannten beispielsweise 81 Prozent der Befragten als zutreffendsten Grund für ihre Partizipation, dass sie im Forum Menschen mit ähnlichen Problemen kennen lernen wollten. Daneben spielte das Motiv, die eigenen Probleme mitteilen zu können für 62 Prozent der Besucher eine entscheidende Rolle. Demgegenüber waren hingegen die Motive, Informationen zu professioneller Hilfe zu erhalten oder jemanden zu finden, mit dem man sich gemeinsam umbringen könne, wenig relevant. Für 77 Prozent bzw. 81 Prozent der Befragten traf dieser Grund wenig oder gar nicht zu.

Mit einer Faktorenanalyse (Hauptkomponentenanalyse) über die Motive zur Forumsteilnahme ließen sich drei orthogonale Faktoren extrahieren, die 58,32 Prozent der Gesamtvarianz aufklärten (vgl. Tab. 3).

Tab. 3: Faktorenmatrix der Motive zur Forumsteilnahme (N = 164)

	Motive		
	konstruktiv	destruktiv	unspezifisch
um meine Probleme, die hinter meinen Selbstmordgedanken stehen, mitteilen zu können	**.76**	-.15	-.21
um in einer akuten suizidalen Krise AnsprechpartnerInnen zu finden	**.75**	-.02	-.19
um mit Menschen mit ähnlichen Problemen und Gedanken die Krise zu überwinden, weil es gemeinsam leichter geht	**.74**	-.20	.24
um Menschen mit ähnlichen Problemen und Gedanken kennen zu lernen	**.68**	-.20	-.01
um meine Selbstmordgedanken loszuwerden	**.66**	-.11	-.13
um Informationen zu bekommen, wie ich professionelle Hilfe finde	**.62**	.03	.14
um anderen zu helfen	.53	.11	.52
um Hinweise zu effektiven Selbstmordmethoden zu bekommen	.22	**.81**	-.32
um jemanden zu finden, der sich mit mir zusammen umbringt	.33	**.78**	-.23
um Informationen zu bekommen, wie anderen Menschen mit Selbstmordgedanken am besten zu begegnen ist	.13	.29	**.75**
Neugier	-.20	.34	.43
Summen von quadrierten Faktorladungen für Extraktion	3.47	1.59	1.34
% der Varianz	31.58	14.47	12.26

Extraktionsmethode: Hauptkomponentenanalyse. 3 Komponenten extrahiert

Es zeigte sich, dass die eher konstruktiven Motive das Forum zu besuchen (Faktor 1), die im Wesentlichen hilfesuchender Natur sind, unabhängig von den destruktiven Motiven (Faktor 2) sind, wie beispielsweise einen Partner oder neue Methoden für den Suizid zu finden.

Inhalte der Beiträge im Forum

Grundsätzlich ist möglich, aktiver oder passiver (ausschließliches Mitlesen der Beiträge anderer) Teilnehmer zu sein. Gut ein Drittel (34 %) der Befragungsteilnehmer gab an, rein passiver Nutzer zu sein. Die meisten User schrieben direkt beim ersten Besuch (22 %) bzw. ein paar Tage später (29 %) einen eigenen Beitrag, nur wenige warteten 1-4 Wochen (12 %) oder noch länger (3 %) ab, um sich im Forum einzubringen.

Die Inhalte der eigenen Postings im Forum wurden auf einer Skala von 0 (*trifft gar nicht zu*) bis 4 (*trifft vollkommen zu*) erhoben. Die Inhalte der Beiträge der Studienteilnehmer weisen ebenfalls eine bemerkenswerte Struktur auf. Hier ließen sich zwei Faktoren extrahieren, die 59,8 Prozent der Gesamtvarianz aufklären. Es sind zum einen eher eigenzentrierte (z.B. ‚Ich äußere meine Selbstmordgedanken'), zum anderen eher fremdzentrierte Inhalte (z.B. ‚Ich gehe auf die Selbstmordgedanken anderer ein') (vgl. Tab. 4).

Tab. 4: Rotierte Faktorenmatrix der Inhalte der eigenen Postings (N = 108)

	Inhalte der Beiträge	
Item	**fremdzentriert**	**eigenzentriert**
Ich versuche, andere von ihren Selbstmordgedanken abzubringen.	**.89**	-.05
Ich versuche, die Probleme der anderen zu lösen, die zu den Selbstmordgedanken führten.	**.88**	.05
Ich gehe auf die Selbstmordgedanken anderer ein.	**.80**	.13
Ich teile meine Erfahrungen mit, wie ich meine Suizidgedanken überwunden habe.	**.66**	.19
Ich unterhalte mich einfach mit anderen Teilnehmer/innen, das Thema ‚Selbstmord' spielt dabei keine Rolle.	.37	-.31
Ich äußere meine Selbstmordgedanken.	-.11	**.83**
Ich beschreibe die Probleme, die zu meinen Selbstmordgedanken führten.	.09	**.78**
Ich bitte um Hilfe.	.28	**.67**
Rotierte Summe der quadrierten Ladungen	2,88	1,89
% der Varianz	36,06	23,73

Extraktionsmethode: Hauptkomponentenanalyse. Rotationsmethode: Varimax mit Kaiser-Normalisierung. Die Rotation ist in 3 Iterationen konvergiert.

Nutzertypen

Über die Motive, das Forum zu besuchen, wurde mit 164 Fällen eine Clusterzentrenanalyse mit 10 Iterationen gerechnet. Hierbei ergab sich eine akzeptable Unterteilung in drei Typen. Im ersten Cluster (Typ 1) waren 35, im zweiten Cluster (Typ 2) 51 und im dritten Cluster (Typ 3) 78 Fälle. In einer ANOVA über die gemittelten Items, die jeweils auf den betreffenden Faktor hoch laden (vgl. Tab. 4), unterschieden sich die drei Typen sowohl hinsichtlich der konstruktiven Motive (F (2, 161) = 120,23; $p < .01$) als auch bezüglich der destruktiven Motive (F (2, 161) = 235,49; $p < .01$) überzufällig (siehe Abb. 2). Auch in Bezug auf eigenzentrierte (F (2, 105) = 23,28; $p < .01$) bzw. fremdzentrierte (F (2, 105) = 7,42; $p < .01$) Inhalte der eigenen Beiträge (N = 108) fanden sich bedeutsame Unterschiede (siehe Abb. 3).

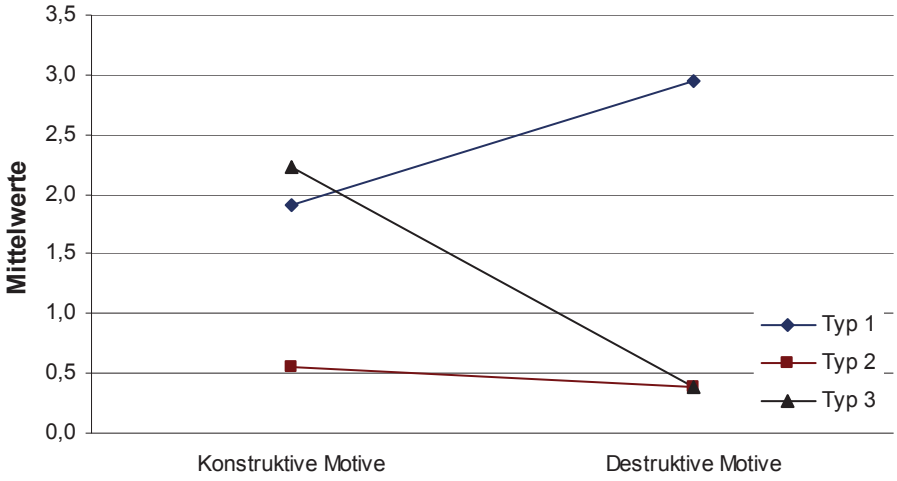


Abb. 2: Unterschiede der Nutzertypen in den Motiven ihrer Teilnahme am Forum (Mittelwerte; *N* = 164)

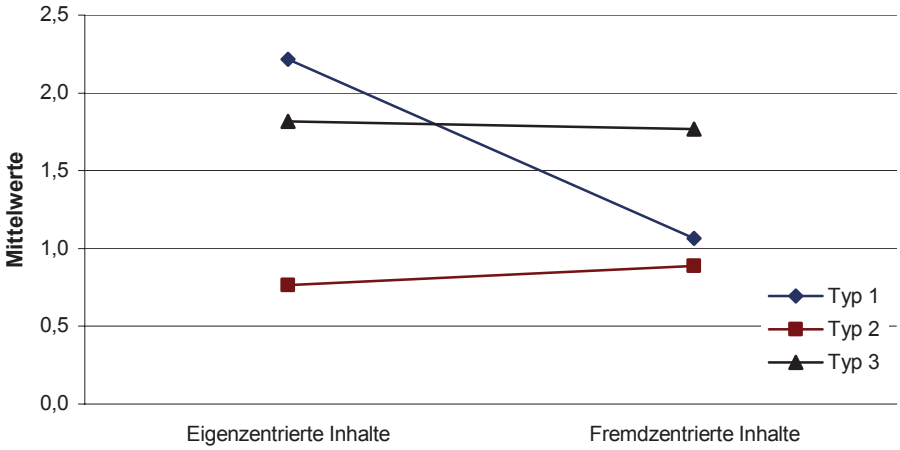


Abb. 3: Unterschiede der Nutzertypen in den Inhalten der eigenen Beiträge (Mittelwerte; N = 108)

In Tabelle 5 sind die post-hoc-Ergebnisse (Scheffé) bezüglich der Unterschiede zwischen den einzelnen Usertypen angegeben. Es zeigte sich, dass die gefundenen signifikanten Ergebnisse teilweise mit außerordentlich hohen Effektstärken einhergehen.

Tab. 5: Mehrfachvergleiche zwischen den Nutzertypen (Scheffé)

Abhängige Variable	(I) Cluster-Nr. des Falls	(J) Cluster-Nr. des Falls	Mittlere Differenz (I-J)	*p*	*d*
Konstruktive Motive	1	2	1.35	< .001	1.79
		3	-0.32	< .05	-0.44
	3	2	1.67	< .001	3.34
Destruktive Motive	1	2	2.55	< .001	3.61
		3	2.57	< .001	3.91
	3	2	0.01	n.s.	
Eigenzentrierte Inhalte	1	2	1.45	< .001	1.77
		3	0.40	n.s.	
	3	2	1.05	< .001	1.43
Fremdzentrierte Inhalte	1	2	0.18	n.s.	
		3	-0.70	< .05	-0.61
	3	2	0.88	< .01	0.85

Typ 1 (21 % der Nutzer) erscheint als der eigentlich problematische User, da hier mit Abstand am stärksten (auch) aus destruktiven Motiven das Forum aufgesucht wird. Allerdings weist dieser Nutzertyp ebenso eine starke Tendenz auf, sich aus konstruktiven Motiven am Forum zu beteiligen. Diesen Nutzertypen könnte man als den ‚ambivalent Hilfesuchenden' bezeichnen. Hinsichtlich der Beiträge im Forum fällt auf, dass Typ 1 stärker eigen- aber kaum fremdzentrierte Inhalte veröffentlicht. 66 Prozent der Nutzer dieses Typs sind im Forum auch aktiv.

Typ 2 (31 % der Nutzer) fällt durch eine signifikant niedrigere Ausprägung in fast allen Motiven des Forumsbesuchs auf. Er hat also weder stark ausgeprägte konstruktive noch destruktive Motive und frequentiert das Forum vermutlich also weder, um sich von einem Leidensdruck zu entlasten oder um gegenseitige Hilfe zu erfahren, noch um Unterstützung zum Vollziehen des eigenen Suizids zu erhalten. Diesen Typen nennen wir im Folgenden den ‚unspezifisch Motivierten'. Obwohl 53 Prozent dieses Typs Beiträge veröffentlicht haben, weisen die Postings weder stark eigen- noch fremdzentrierte Inhalte bezüglich einer suizidalen Problematik auf.

Typ 3 (48 % der Nutzer) kann als Person mit den am stärksten ausgeprägten konstruktiven Motiven im Sinne des Problemaustausches und der Kommunikation mit Menschen, die ähnliche Gedanken und Gefühle haben, beschrieben werden. Demgegenüber spielen die destruktiven Motive wie bei Typ 1 fast keine Rolle. Aufgrund dieser Motivlage bezeichnen wir diesen Nutzertyp im Folgenden als den ‚konstruktiv Hilfesuchenden'. Bezüglich der Inhalte der eigenen Beiträge weist Typ 3 gleichermaßen ausgeprägte Tendenzen zu eigen- und fremdzentrierten Inhalten auf. Typ 3 scheint auch am aktivsten im Forum zu sein. 74 Prozent dieser User beteiligen sich durch eigene Beiträge.

4.3 Effekte der Nutzung des Suizidselbsthilfe-Forums

Die Befragungsteilnehmer wurden gebeten, das Ausmaß ihrer Suizidgedanken unmittelbar vor dem ersten Besuch des Forums und zum Erhebungszeitpunkt auf einer 7-stufigen Ratingskala einzuschätzen (0 = *gar keine Suizidgedanken* bis 6 = *sehr starke Suizidgedanken*). Es zeigte sich eine signifikante Reduktion des Ausmaßes der Suizidgedanken von 4,32 (*SD* = 1,55) vom Zeitpunkt ‚vor der Nutzung' des Forums auf 3,08 (*SD* = 1,90) zum Zeitpunkt der Erhebung mit einer Effektstärke von $d = 0{,}72$ (t (144) = 9,2; $p < .01$). Natürlich kann vom Rückgang der Suizidgedanken nicht auf eine Wirkung der Teilnahme am Suizid-Selbsthilfeforum geschlossen werden. Die Befundlage legt aber eine Überprüfung einer solchen Vermutung nahe.

Vergleicht man die drei identifizierten Nutzertypen hinsichtlich der Selbsteinschätzung des Ausmaßes der suizidalen Gedanken *vor dem ersten Besuch des Forums* (F (2, 142) = 14,59; $p < .01$) und *im Moment* (F (2, 142) = 26,85; $p < .01$), so fällt auf, dass der ‚ambivalent Hilfesuchende' (Typ 2) post hoc (Scheffé) sowohl hinsichtlich der suizidalen ‚Ausgangslage' *vor dem Besuch des Forums* (Mittlere Differenz zu Typ 2 = 1,85; $p < .01$; Mittlere Differenz zu Typ 3 = 1,13; $p < .01$) als auch *im Moment* des Erhebungszeitpunkts (Mittlere Differenz zu Typ 2 = 2,08; $p < .01$; Mittlere Differenz zu Typ 3 = 2,45; $p < .01$) das höchste Ausmaß an Suizidalität aufweist. Die stark ausgeprägten Motive, im Forum ebenso Hinweise auf Suizidmethoden und Kontakte zum gemeinschaftlichen Suizid zu finden, könnten sich vielleicht aus einem besonders hohen Leidensdruck dieses Nutzertypen erklären. Gleichzeitig teilen diese Motive nur ein geringer Anteil der Forumsteilnehmer insgesamt (21 %), so dass die Kommunikation von aggressiven Aspekten (z.B. über die Diskussion von effizienten Suizidmethoden) vermutlich auf wenig Resonanz stößt oder sogar durch forumsimmanente Überzeugungen negativ sanktioniert wird und somit keine Entlastung schafft.

Bei dem ‚konstruktiv Hilfesuchenden' gab es im Vergleichszeitraum den stärksten Rückgang im Ausmaß der Suizidgedanken, was eventuell dadurch erklärt ist, dass Personen mit vorwiegend konstruktiven Hilfegesuchen von der Teilnahme an solchen Foren stärker profitieren als Menschen, deren konkrete Motivlage eher unspezifisch ist (Typ 2) (vgl. Abb. 4).

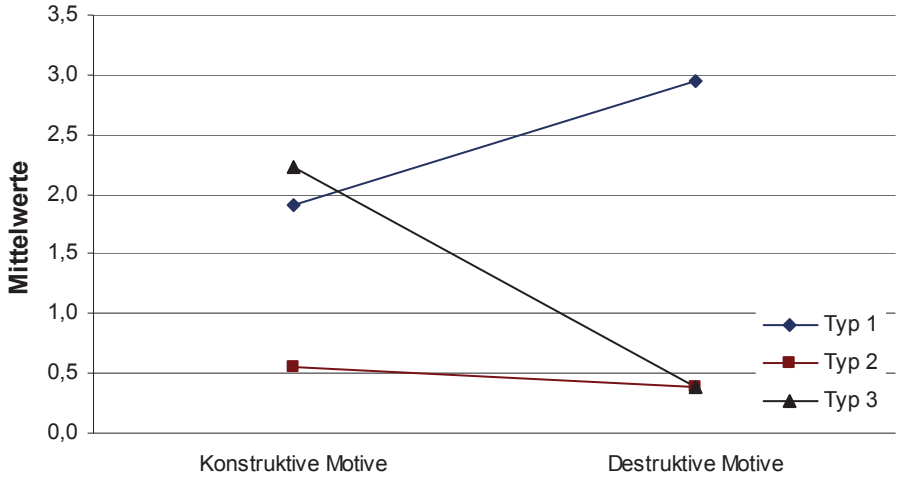


Abb. 4: Unterschiede der Nutzertypen im Ausmaß der Suizidgedanken vor dem ersten Forumsbesuch und zum Erhebungszeitpunkt auf einer 7-stufigen Ratingskala (0 = *gar keine Suizidgedanken* bis 6 = *sehr starke Suizidgedanken*) (Mittelwerte; $N = 145$)

Um Schlussfolgerungen auf mögliche Imitationseffekte ziehen zu können, wurden die Befragungsteilnehmer um ihre Erfahrungen mit der Suizidierung von Forumsteilnehmern gebeten: der größte Teil (72 %) hatte in der gesamten Zeit der Nutzung von Suizidforen nicht erlebt, dass sich ein Teilnehmer suizidiert hat. Von denjenigen mit solchen Erfahrungen (28 %) gaben 34 Personen an, dass sie im Mittel von 2,1 Personen ($SD = 2,0$) wussten, die sie aus dem ‚selbstmordforum.de' kannten, und sich das Leben genommen hatten. 15 User berichteten von durchschnittlich 1,8 suizidierten Personen ($SD = 1,3$), die sie aus einem anderen ‚Suizidforum' kannten.

Ob das untersuchte Forum ein geschlossener virtueller Lebensraum ist, sollte durch Fragen nach der Ausweitung auf andere Kommunikationsmodi geklärt werden. Offensichtlich wird privaterer Kontakt, wie ein Rückzug aus dem öffentlichen Forum und der Wechsel auf die Ebene persönlicher E-Mails oder Treffen, wenig präferiert: Lediglich gut ein Drittel (36 %) gab an, mit durchschnittlich 3,5 Usern ($SD = 2,8$) in regelmäßigem E-Mail-Kontakt zu stehen. Andere Personen aus dem ‚selbstmordforum.de' bereits persönlich getroffen zu haben, gaben jedoch immerhin 16 Prozent an; diese hatten durchschnittlich 4,4 Nutzer ($SD = 3,8$) persönlich kennen gelernt.

5 Diskussion

Auch wenn die vorgestellten Daten aufgrund methodischer Einschränkungen (z.B. wurden die Befragungsteilnehmer aus einem einzigen ‚Suizidforum' rekrutiert; zum Problem von Selbstselektionsprozessen bei WWW-Umfragen und damit einhergehenden Stichprobenverzerrungen vgl. [21]) keinen repräsentativen Schluss auf die gesamte Kultur der ‚suizidalen Szene' im Internet zulassen, so können sie jedoch einige in der Öffentlichkeit und z.T. auch in Fachkreisen (vgl. Tab. 1) vorherrschende Gefahrenzuschreibungen entdramatisie-

ren. Anhand der in dieser Studie identifizierten Nutzertypen sind Annahmen, die besagen, dass die stärksten Motive zum Aufsuchen von ‚Suizidforen' in dem Wunsch bestünden, Hilfe und Unterstützung bei der Umsetzung des Suizides zu bekommen, was sich in dominierenden Diskussionen über Suizidmethoden und der gegenseitigen Animation zum ‚Mitsterben' manifestieren solle, zu relativieren. Die größte Gruppe der User des untersuchten Forums scheint demgegenüber konstruktive Hilfe in einer als ausweglos empfundenen Situation durch Kommunikation mit Menschen, von denen man sich verstanden fühlt, zu suchen und zu finden. Zwar ließ sich eine Subgruppe von Nutzern identifizieren, die eine hohe Motivation hat, Methoden und Partner zum Vollzug des Suizids zu finden, und sich in der Forumsdiskussion kaum mit fremdzentrierten Inhalten im Sinne des Eingehens auf andere beteiligt. Dieser Nutzertyp ist jedoch anteilig sehr gering. Er zeigt ein vergleichsweise erhöhtes Ausmaß an Suizidalität, was die Intensität des oberflächlich betrachtet ‚destruktiven' Kommunikationsanliegens erklären könnte. Im Übrigen können Diskussionen über Suizidmethoden nicht pauschal als dysfunktional bezeichnet werden, da sie auch die Funktion haben können, den suizidalen Handlungsdruck abzubauen[14].

Ob das Anliegen dieser stark belasteten Gruppe negative Effekte auf andere Nutzertypen hat, bleibt empirisch zu klären. Damit einher geht die generelle Frage nach Ansteckungseffekten. Die Behauptung, dass vormals nicht suizidale Personen, insbesondere Jugendliche und junge Erwachsene, durch die Teilnahme an ‚Suizidforen' ‚suizidal gemacht' würden[8], wird durch die Ergebnisse dieser Studie stark in Frage gezogen: In der (überwiegend adoleszenten) Stichprobe ist zum einen die Gruppe ohne ‚suizidale Vorgeschichte' äußerst gering, zum anderen zeigte sich eine signifikante Reduktion des Ausmaßes der Suizidgedanken vom Zeitpunkt ‚vor der Nutzung' des Forums bis zum Zeitpunkt der Erhebung (‚momentan'). Diese Reduktion kann zwar vorerst nicht ursächlich auf die Forumspartizipation zurückgeführt werden, spricht aber gegen den Trend von ‚Werther-Effekten'.

Ingesamt stützen die vorliegenden Ergebnisse eine Haltung, ‚Suizidforen' im Internet nicht pauschal zu skandalisieren. Die bestehenden Foren unterscheiden sich in ihrer Ausrichtung untereinander[22 23]. Von daher würde eine globale Negativeinschätzung den differenzierten Blick auf das tatsächliche, unter Umständen forumsspezifische Geschehen, gerade verhindern. Eine Dämonisierung dieser Kommunikationsplattformen entbehrt angesichts der vorliegenden Ergebnisse der empirischen Grundlage. Sie könnte jedoch zu bedenklichen Maßnahmen führen, die in jedem Falle auch die konstruktiven, suizidpräventiven und möglicherweise sogar kurativen Funktionen der Foren, wie sie in dieser Untersuchung beobachtet wurden, eliminieren würden. Für Deutschland bieten auch epidemiologische Daten derzeit keinen Anhaltspunkt für die Vermutung, dass durch Verbreitung und Nutzung des Internet ein Anstieg der Suizidrate zu verzeichnen wäre. Unsere Aufmerksamkeit sollte sich in dieser Situation vor allem auf Möglichkeiten richten, die Selbsthilfeaktivität suizidaler Internetnutzer mit suffizienter professioneller Online- und Offline-Hilfe zu vernetzen, um die beobachteten suizidpräventiven Möglichkeiten des Mediums möglichst effektiv auszuschöpfen. Ebenso sollte eine Medienerziehung etabliert werden, die von Schule und Elternhaus wahrgenommen wird, und den Umgang mit problematisie-

renden Netzinhalten mit einschließt. Letztlich wird Suizidalität insbesondere von Kindern und Jugendlichen nur von den engsten Bezugspersonen erkannt werden; die Entdeckung entsprechender ‚Internetaktivitäten' kann und muss damit nur als Anlass zur Fürsorge und des gemeinsamen Gesprächs werden.

Literatur

1. Ott, R. & Eichenberg, C. (Hrsg.) (2003). Klinische Psychologie und Internet. Potenziale für klinische Praxis, Intervention, Psychotherapie und Forschung. Göttingen: Hogrefe.

2. Beard, KW. Internet addiction: A review of current assessment techniques and potential assessment questions. CyberPsychology & Behavior 2005; 8: 7-14.

3. Morahan-Martin, J. Internet abuse: Addiction? Disorder? Symptom? Alternative Explanations? Social Science Computer Review 2005, 23: 39-48.

4. Cooper, A (ed.) (2002). Sex and the Internet: A Guidebook for Clinicians. Philadelphia, PA: Brunner-Routledge.

5. Döring, N. (2000). Selbsthilfe, Beratung und Therapie im Internet. In B. Batinic (Hrsg.), Internet für Psychologen (2., überarb. u. erw. Aufl.) (S. 509-548). Göttingen: Hogrefe.

6. Eichenberg, C. & Pennauer, J. (2003). Krisenintervention im und via Internet: Angebote und Möglichkeiten. Psychotherapie im Dialog, 4, 411-415.

7. Stoney, G. (1998). Suicide prevention on the Internet. In R.J. Kosky & H.S. Eshkevari (Ed.), Suicide prevention: The global context (pp. 237-244) New-York: Plenum Press.

8. Prass, S. (2002). Suizid-Foren im World Wide Web. Eine neue Kulturgefahr. Jena: IKS Garamond.

9. Sher, L. (2000). The Internet, suicide, and human mental functions. Canadian Journal of Psychiatry, 45, 297.

10. Alao AO, Yolles JC, Armenta, WR. (1999). Cybersuicide: The Internet and suicide. American Journal of Psychiatry 1999; 156: 1836-7.

11. Schmidtke, A., Schaller, S. & Kruse, A. (2003). Ansteckungsphänomene bei den neuen Medien – Fördert das Internet Doppelsuizide und Suizidcluster? In E. Etzersdorfer, G. Fiedler & M. Witte (Hrsg.), Neue Medien und Suizidalität. Gefahren und Interventionsmöglichkeiten (S. 150-166). Göttingen: Vandenhoeck & Ruprecht.

12. Baume, P, Cantor, CH, Rolfe, A. Cybersuicide: The role of interactive suicide notes on the Internet. Crisis 1997; 18: 73-7.

13. Winkel, S., Groen, G. & Petermann, F. (2003). Suizidalität von Jugendlichen und jungen Erwachsenen: Nutzung von Selbsthilfeforen im Internet. Zeitschrift für Klinische Psychologie, Psychiatrie & Psychotherapie, 51, 158-175.

14. Fiedler, G. (2003). Suicidality and new media: Dangers and possibilities. In: Etzersdorfer, E, Fiedler, G, Witte, M (eds.). New media and suicide - Dangers and possible interventions. Göttingen: Vandenhoeck & Ruprecht, pp. 19-55.

15. Mehlum, L (2000). The Internet, suicide, and suicide prevention. Crisis 2000; 21: 186-8.

16. Richard, J, Werth, JL, Rogers, JR. Rational and assisted suicidal communication on the Internet. A case example and discussion of ethical and practice issues. Ethics and Behavior 2000; 10: 215-238.

17. Janson, MP, Alessandrini, ES, Strunjas, SS, Shahab, H, El-Mallakh, R, Lippmann, SB. Internet-observed suicide attempts. Journal-of-Clinical-Psychiatry 2001; 62 (6): 478.

18. Fekete, S. The Internet – A New Source of Data on Suicide, Depression an Anxiety: A Preliminary Study. Archives of Suicide Research 2002; 6: 351-61.

19. Miller, JK & Gergen, KJ. Life on the line: the therapeutic potentials of computer-mediated conversation. Journal of Marital and Family Therapie 1998; 24 (2): 189-202

20. Batinic, B, Reips U.-D., Bosnjak, M (eds.) (2002). Online Social Sciences. Seattle, WA: Hogrefe & Huber.

21. Bandilla, W (2002). Web Surveys – An Appropriate Mode of Data Collection for the Social Sciences? In: Batinic B, Reips, U.-D., Bosnjak, M (eds.). Online Social Sciences. Seattle, WA: Hogrefe & Huber, pp. 1-6.

22. Becker, K, Mayer, M, Nagenborg, M, EL-Faddagh, M, Schmidt, MH. Parasuicide online: Can suicide websites trigger suicidal behaviour in predisposed adolescents? Nordic Journal of Psychiatry 2004; 58: 111-4.

23. Eichenberg, C. (2002). Suizidalität im Internet. *TELEPOLIS*, 03.11.2002.

Ansätze zur Förderung des Risikobewusstseins bei den Netzbürgern im Umgang mit ‚Viren, Würmern, Trojanern, Hoaxes etc.'

Frank W. Felzmann

Es fehlt noch eine empirische Untersuchung unter Computer-Nutzern zum Thema ‚Wann haben Sie zum ersten Mal Mordgedanken entwickelt? Erstens: nach Einspielen eines Windows-Update? Zweitens: nach dem Versuch, eine Internet-Verbindung aufzubauen? Oder drittens, nachdem Sie sich einen Computer-Virus eingefangen haben?'

Schadprogramme - Definitionen

Beginnen wir mit den Computer-Viren, die zu den Programmen mit Schadensfunktion oder kurz Schadprogrammen gehören. Darunter fallen auch die Trojanischen Pferde und Würmer. Damit eine einheitliche Grundlage entsteht, ist es notwendig, die einzelnen Typen dieser Schadprogramme zu definieren.

Als erstes den **Computer-Virus**: ‚Ein Computer-Virus ist eine nicht selbständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. Zusätzlich können programmierte Schadensfunktionen vorhanden sein.'

Die Eigenschaft der Selbstreproduktion ist der Grund dafür, dass - in Analogie zum biologischen Virus - dieses Schadprogramm eben Computer-Virus genannt wurde. Es muss neben der Verbreitung nicht unbedingt auch eine zusätzliche programmierte Schadensfunktion vorhanden sein. Ein Großteil der Computer-Viren, die in der letzten Zeit aufgetreten sind, hat als einzigen ‚Schaden' nur sich selbst verbreitet. Es genügte den unbekannten Autoren meist auch als ‚Erfolg', wenn in den Medien ‚ihr' Virus eine besondere Aufmerksamkeit erreichte, ohne dass explizit ein Schaden auf den infizierten Rechnern entstand. Aber diese ‚Schadensfreiheit' ist leider nicht die Regel. Es gibt auch einige Viren-Autoren, die bösartige Viren in Umlauf bringen, welche bestimmte Typen von Dateien auf den befallenen Rechnern löschen, wodurch sogar der Rechner unbrauchbar wird, wenn darunter wichtige Betriebssystem-Dateien sind.

Wichtig bei der Definition eines Computer-Virus ist der Passus: ‚vom Anwender nicht kontrollierbare Manipulationen'. Damit ist nämlich ganz klar: Es gibt keine nützlichen oder ‚guten' Computer-Viren. Hin und wieder ist die Idee aufgetaucht, man könnte ja einen nützlichen Virus schreiben. Zum Beispiel einen Virus, der andere Viren von der Festplatte löscht. Es gab sogar einmal eine Art Viren-Krieg zwischen zwei Viren-Autorengruppen, in dem die eine Gruppe versucht hat, Rechner zu infizieren und diese dann zu durchsuchen, ob vielleicht ein Virus der anderen Gruppe bereits vorhanden war.

Der wurde gegebenenfalls entfernt und durch den eigenen Virus ersetzt. Worauf die erste Gruppe sich revanchiert hat, und nun ihrerseits auf die Jagd gegangen ist. Aber das Hauptproblem beim Schreiben von Viren ist, dass die Autoren meist nicht wissen können, wie sich das Betriebssystem verhält, und ob sie auch die richtigen Dateien ‚erwischen'. Das führt in der Regel dazu, dass auch angeblich nützliche Computer-Viren aufgrund der nicht kontrollierbaren Manipulationen eben doch großen Schaden anrichten, wenn auch unbeabsichtigt. Also nochmals zur Klarstellung: Jeder Computer-Virus ist eine Gefahr, ist schädlich, ist nicht nützlich.

Nun zum nächsten Schadprogramm, dem **Trojanischen Pferd**. ‚Ein Trojanisches Pferd ist ein selbständiges Programm mit einer versteckten Zusatzfunktion, ohne Selbstreproduktion.' Man beachte hier den Passus ‚ohne Selbstreproduktion', denn dies ist der entscheidende Unterschied zum Computer-Virus.

Das Trojanische Pferd als Schadprogramm hat seinen Namen aus der klassischen griechischen Sage. Die Griechen konnten nach zehn Jahren fortgesetzter Belagerung die Stadt Troja noch immer nicht erobern. Odysseus kam schließlich auf die Idee, den Trojanern als vermeintliches Abschiedsgeschenk ein riesiges hölzernes Pferd zu hinterlassen. Die Trojaner schleppten das Holzpferd in ihre Stadtmauern, jedoch waren in seinem Inneren 40 Krieger versteckt, die nachts hinausschlüpften, ihrer heimlich angerückten Armee die Tore öffneten - und das war das Ende von Troja. Und genau wie bei dem mythischen Pferd lauern im Inneren des Computer-Pferdes versteckte Programmbefehle, die sich irgendwann aktivieren und ihre Funktionen ausführen – meist zu Lasten des ahnungslosen Computer-Nutzers. Mittlerweile wird statt von ‚Trojanischen Pferden' umgangssprachlich nur noch von ‚Trojanern' gesprochen, womit die armen Trojaner unverdientermaßen von Opfern zu Tätern gemacht werden.

Neben dem Hauptunterschied hinsichtlich der Reproduktion ist auch von Interesse, was die Vor- und Nachteile sind hinsichtlich der Verbreitung und Entdeckung von Computer-Virus und Trojanischem Pferd - aus Sicht des jeweiligen Schadprogramms. Der Computer-Virus hat den großen Vorteil, dass er sich sehr gut und rasch verbreiten kann. Der Nachteil ist, dass er durch die Verbreitung auch relativ gut entdeckt werden kann, da er zwangsläufig Veränderungen im Computer vornimmt. Beim Trojanischen Pferd ist es umgekehrt: Es hat zwar sehr beschränkte Möglichkeiten zur Verbreitung, da es nach der Installation auf einem Rechner auch auf diesem verbleibt. Aber dadurch ist die Gefahr der Entdeckung auch relativ gering. Und wenn es sich um ein speziell für einen bestimmten Rechner geschriebenes Trojanisches Pferd handelt, dann ist die Entdeckung äußerst schwierig. Denn der Anwender weiß ja nicht, dass das Schadprogramm sich eingenistet hat. Die Schadensfunktion, die eventuell in ihm steckt, kann zu einem bestimmten Zeitpunkt, zum Beispiel nach einem halben Jahr einsetzen, indem beispielsweise die ganze Festplatte gelöscht wird. Das Trojanische Pferd vernichtet sich auf diese Weise allerdings auch selbst und hinterlässt damit auch keine Hinweise auf seine Existenz.

Der letzte Schädling aus dieser Gruppe ist der **Computer-Wurm**: ‚Ein Computer-Wurm ist ein selbständiges Programm, das sich über Computer-Netze weiter verbreitet (z.B. durch Versenden infizierter E-Mails über Mail-Programme oder eigene SMTP-Maschine).' Für die Definition ausschlaggebend ist hier der Begriff ‚Computer-Netze'. Aber auch viele Computer-Viren und Trojanische Pferde bringen mittlerweile ihr eigenes Mail-Programm mit, ihre eigene SMTP-Maschine. Die Grenze zwischen Virus und Wurm ist sozusagen fließend geworden, die Begriffe werden gelegentlich auch verwechselt. Für den Benutzer ist es im Endeffekt gleich, wer den Schaden auf seinem Rechner angerichtet hat. Für den Anwender ist die genaue Klassifikation daher mehr akademischer Art.

Abschließend sei hier noch der **Hoax** erwähnt: ‚Hoax (engl. Jux, Scherz, Schabernack) bezeichnet eine Falschmeldung, die sich vorwiegend per E-Mail verbreitet, von vielen für wahr gehalten und daher an viele andere weitergeleitet wird. Meist sind es Warnungen über einen angeblichen Computer-Virus.'

In der Regel behaupten solche Falschmeldungen: ‚Hier ist ein völlig neuer Virus aufgetaucht. Kein einziges Viren-Schutzprogramm kann ihn entdecken, er richtet furchtbaren Schaden an, sofort die Nachricht an alle bekannten Freunde weiterleiten!' Aber diese Verbreitung ist gerade die Schadensfunktion. Der bekannteste Hoax dürfte die Warnung 1994 vor dem ‚Good Times Virus' gewesen sein. Die gute Nachricht: Diese ‚elektronischen Enten' sind kaum mehr verbreitet. In 2005 gab es nur noch zwei, drei kleinere Vorfälle; in früheren Jahren traten Hoaxes wesentlich massiver auf und stellten eine ziemliche Belastung für den E-Mail-Verkehr dar.

Schadprogramme – Verbreitung

Wie verbreiten sich Schadprogramme? In erster Linie durch unaufmerksame, unerfahrene Benutzer, die auf alles klicken, was per E-Mail versendet wird. Kommt eine E-Mail mit irgendeinem Attachment an, wird der Text kurz durchgelesen und auf den Anhang geklickt - und das war es dann auch schon: der Rechner ist infiziert.

Neben den Benutzern gibt es aber noch eine weitere große Gruppe, die Schadprogramme bei ihrer Verbreitung unbeabsichtigt unterstützt. Es sind dies die Administratoren, deren Aufgabe es ist, die Betriebssysteme zu warten und zu pflegen. Die Betriebssysteme, insbesondere Microsoft Windows, aber auch Linux und andere Systeme, sowie Anwendungsprogramme enthalten aufgrund von Programmierfehlern gefährliche Sicherheitslücken. Werden diese entdeckt, gibt der Hersteller des Systems oder des Programms ein Sicherheits-Update – oder auch Sicherheits-Patch genannt – heraus. Die Administratoren sollten idealerweise diese Updates zeitnah einspielen, damit die Rechner gegen Angriffe von außen gewappnet sind. Aber leider werden diese Korrekturen von den Administratoren eben nicht immer sofort eingespielt, wodurch die Rechner verwundbar bleiben und von Schadprogrammen befallen werden können. Diese Fahrlässigkeit ist auch ein Grund, warum in letzter Zeit so viele Viren-Epidemien aufgetreten sind.

Die Verbreitungswege der Schadprogramme sind - über die Jahre gesehen - sehr interessant. Es gibt eine Studie der amerikanischen ICSA, der International Customer Service Association, die seit 1996 jährlich durchgeführt wird. In dieser Studie, die auf Umfragen unter vielen Firmen beruht, wird unter anderem auch nach dem Auftreten von Schadprogrammen und deren Verbreitungsweg gefragt (siehe Abbildung 1). Dabei ist klar zu erkennen, dass früher – 1996 bis 1998 oder auch 1999 – das hauptsächliche Verbreitungsmedium die Diskette war, mit einem Anteil von bis zu 85 Prozent. Aber mittlerweile ist die Diskette als Datenträger nahezu abgelöst und damit praktisch auch kein nennenswertes Verbreitungsmedium mehr. Die meisten neuen Rechner haben mittlerweile überhaupt kein Diskettenlaufwerk mehr. Das hängt auch damit zusammen, dass die Programme so groß geworden sind, dass die Daten nicht mehr auf eine Diskette passen, die nur eine Kapazität von 1,2 Megabyte hat. Zudem sind die CD-ROM preislich so günstig geworden, dass diese nunmehr als Datenträger benutzt werden.

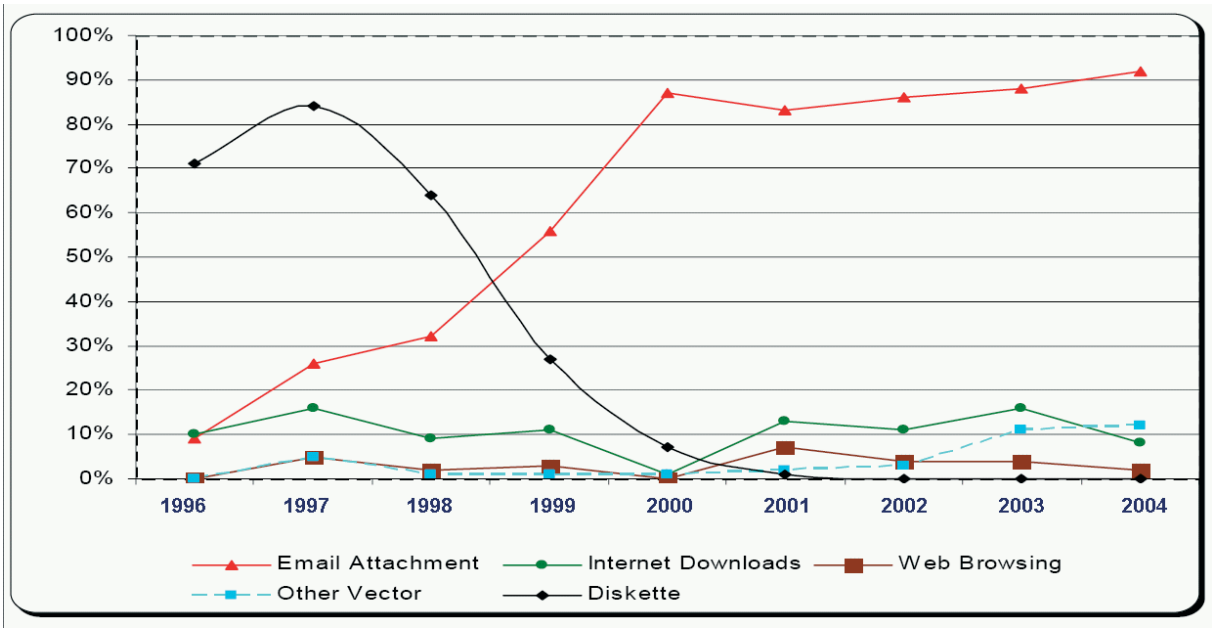


Abb. 1: Verbreitungswege von Schadprogrammen © ICSA (International Customer Service Association)

Sehr stark zugenommen hat die Verbreitung von Schadprogrammen über Datei-Anhänge in E-Mails, den E-Mail-Attachments. Daten per E-Mail lassen sich blitzschnell elektronisch von einem Ort der Erde an einen anderen versenden. Im Gegensatz zum Attachment ist die Diskette ein physikalisches Medium, das erst von einer Stelle zu einer anderen transportiert werden muss, meist auf dem Postweg. Die E-Mail dagegen ist schnell geschrieben und genauso schnell kann sie weltweit (z.B. von Deutschland in die USA oder von Brasilien nach Österreich) innerhalb kürzester Zeit versendet werden. Man kann sagen, die angefügten Dateien einer E-Mail sind praktisch eine Art ‚elektronischer Diskette'.

Ein weiterer Weg, den Schadprogramme zur Verbreitung nutzen, ist das Internet. Zum einen verstecken sich diese Schädlinge in Dateien, die zum Download angeboten werden, zum anderen auf Web-Seiten in so genannten Aktiven Inhalten, wie JavaScript und ActiveX. Geht ein ahnungsloser Benutzer auf eine solche Webseite und hat er die Ausführung

von Aktiven Inhalten erlaubt, kann er sich ganz schnell den eigenen Rechner infizieren. Dazu kommt noch, dass sich im Internet auf Web-Seiten sehr viele Trojanische Pferde verstecken, die über Sicherheitslücken im Betriebssystem oder auch im Browser den Rechner übernehmen. Die Trojanischen Pferde kontrollieren die Eingaben der Benutzer, und wenn sie dabei entdecken, dass eine Verbindung beim Online-Banking aufgebaut wird, werden alle wichtigen Daten – wie Name, Konto-Nummer, PIN und TAN – umgehend an andere Rechner übertragen. Damit ist es Gaunern möglich, Konten von ahnungslosen Anwendern zu plündern.

Aufklärung der Netzbürger

Aufgrund dieser mannigfaltigen Bedrohungen im Internet ist eine entsprechende Aufklärung der Netzbürger zwingend erforderlich. Immer mehr Leute tummeln sich im Internet, ohne die Bedrohungen durch Schadprogramme zu kennen.

Bereits 1991 sagte der damalige Innenminister Otto Schily, dass selbstverständlich auch jeder einzelne Bürger Anspruch darauf habe, vor Straftätern im Internet geschützt zu werden; allerdings hätten die Internet-Nutzer auch hier eine gewisse Mitverantwortung. ‚Zu bedauern ist', erklärte Schily in Anbetracht der jüngsten Virus-Epidemien, ‚dass häufig einfachste und längst bekannte Sicherheitsvorkehrungen nicht beachtet werden'.

Betrachten wir einmal beispielsweise die Sicherheitsvorkehrungen bei E-Mails, dem Hauptverbreitungsmedium von Schadprogrammen. Wenn E-Mails ankommen, sollte man nicht sinnvolle E-Mails von Unbekannten einfach löschen. Aber auch wenn man glaubt, den Absender vermeintlich zu kennen, sollte man prüfen, ob die E-Mail auch zum Absender passt. Ist die E-Mail von einem deutschen Kollegen, aber mit englischem Text, ist dies schon sehr verdächtig. Auch sollte man die Formulierungen des Textes dahingehend überprüfen, ob der Absender sich tatsächlich so ausdrücken würde. Es ist leider so, dass man davon ausgehen muss, dass in der Regel die Absenderangaben gefälscht sind. Das Wichtigste bleibt jedoch: Nicht auf jede angefügte Datei einfach klicken zum Öffnen oder sogar Ausführen, ganz gleich, was einem versprochen wird, was für tolle Bilder oder Informationen angeblich enthalten sein sollen. Nicht nur in der Werbung gilt ‚Sex sells!', sondern auch für die Verbreitung von Computer-Viren. Und wenn man sich nicht sicher ist, sollte man im Zweifelsfall eben doch mal eine Rückfrage bei dem angeblichen Absender tätigen, ob das Attachment mit dem Inhalt tatsächlich von ihm kommt.

Um den eigenen Rechner vor Computer-Viren oder sonstigen Schadprogrammen zu schützen und Angriffe aus dem Internet abzuwehren, sollten folgende drei Dinge beachtet werden:

Erstens, unbedingt ein Viren-Schutzprogramm einsetzen mit aktuellen Signaturen zur Erkennung von neuen Computer-Viren. Die Aktualisierung ist dabei äußerst wichtig. Ein Viren-Schutzprogramm, dessen Erkennungs-Signaturen ein halbes Jahr alt sind, kann man getrost löschen, denn es nutzt nicht mehr viel und man hat wenigstens mehr Speicherplatz.

Zweitens sollten Sicherheits-Updates, die Sicherheitslücken schließen, sowohl für das Betriebssystem, als auch für Anwendungsprogramme, insbesondere den Browser, schnellstmöglich eingespielt werden. Dadurch schützt man sich nicht nur selbst, sondern auch andere vor der Infektion und möglicher Verbreitung von Schadprogrammen.

Drittens sollte eventuell noch eine Firewall eingesetzt werden. Man darf allerdings nicht verschweigen, dass sehr viele PC-Nutzer mit dem Einsatz einer Firewall schlicht überfordert sind. Entweder ist die Firewall zu stark eingestellt, so dass andauernd Meldungen hochpoppen. Dann wird jedes Mal der Einfachheit halber mit ‚Ja' bestätigt, auch wenn gelegentlich ein ‚Nein' angebracht wäre. Wenn dieser Ablauf irgendwann zu sehr nervt, wird die Firewall durch Regeln auch schon mal etwas günstiger gestaltet. Im Extremfall lautet die erste Regel der Firewall dann ‚Alles darf rein, alles darf raus!'. Dann ist zwar unten im Fenster auf dem PC noch das Symbol für eine aktive Firewall zu besichtigen, aber die Firewall selbst ist eben total offen. Das heißt, die ‚Brandmauer' ist völlig zusammengebrochen, und das merkt der Nutzer nicht so ohne weiteres. Eine Firewall sollte man deshalb nur einsetzen, wenn man sich auch informiert hat, was sie genau tut.

Förderung des Risikobewusstseins

Die Förderung des Risikobewusstseins ist sehr schwierig. Das ist vor allem darauf zurückzuführen, dass die Hersteller hinsichtlich der Bedienbarkeit von Personal Computern den Kunden mit dem folgenden Slogan ködern: ‚Plug and Play!', auf Deutsch ‚Anschließen und Loslegen'. Und wie sieht die Realität aus? Passender wäre da wohl: ‚Plug and Pray!', also ‚Anschließen und Beten'. Beten, dass alles gut geht. In vielen Fällen geht es aber eben nicht gut, was auch damit zusammenhängt, welchen Stellenwert die IT-Sicherheit hat. Die Hersteller schreiben leider meist Funktionalität riesengroß und Sicherheit sehr, sehr klein.

Die Anwender sind indes nicht viel besser. Bei ihnen kommt an erster Stelle die Bequemlichkeit, dann irgendwo unter ‚ferner liefen' die Sicherheit. Das ist eigentlich erstaunlich, wenn man die übliche Autobahn mit der Daten-Autobahn, dem Internet, vergleicht. Wenn Bürger eine Autobahn benutzen wollen, ist ein Führerschein notwendig und ein amtlich zugelassenes Fahrzeug. Und dann gilt die alte Regel: ‚Erst gurten, dann starten!' Wie sieht es auf der Daten-Autobahn aus? Es gibt keinen PC-Führerschein, es gibt keine zugelassenen Fahrzeuge, die Sicherheitseinstellungen, das Analogon zum Sicherheitsgurt, werden nicht gemacht. Und dann wundern sich die Netzbürger, dass sie mit DSL-Höchstgeschwindigkeit ‚aus der Kurve fliegen', d.h., mit dem ‚nicht zugelassenen' Rechner ihre Daten verlieren und sich Schadprogramme einfangen. Reagiert wird erst, wenn auch ein Schaden entstanden ist, entweder, dass wertvolle Daten unwiederbringlich verloren sind, oder der Anwender sogar finanzielle Einbußen erlitten hat, weil sein Online-Bankkonto mit ergaunerten Zugangs-Daten geplündert wurde. Zu oft gilt eben leider: ‚Nur durch Schaden wird man klug!' Das ist aber der mühsamste Weg, zu lernen, was Sicherheit bedeutet.

Der bessere Weg ist hingegen: Aufklärungsarbeit und Informationsvermittlung. Das Wichtigste ist dabei, die Informationen an die Netzbürger zu bringen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) leistet dies durch eine Reihe von verschiedenen Maßnahmen.

Die erste und wichtigste ist sicher dabei die Bereitstellung von Informationen im Internet. Dazu gibt es zwei verschiedene Webseiten: Zuerst einmal *www.bsi.bund.de*, die Version für die erfahreneren Nutzer oder Profis. Außerdem *www.bsi-fuer-buerger.de* (siehe Abbildung 2), ein Informationsangebot mehr für Computer-Laien gedacht; hier werden die Sachverhalte einfacher und weniger technisch dargestellt.

Abb. 2: Startseite von *www.bsi-fuer-buerger.de*

Außerdem gibt es Mailing-Listen des BSI, auf denen man sich eintragen kann, um Informationen per E-Mail zu erhalten. Eine Liste informiert über aktuelle, besonders stark verbreitete Viren, eine weitere über Sicherheitsvorfälle. Wenn ein Vorfall besonders brisant ist, gibt es noch ad-hoc Warnungen über die Medien. Erwähnt seien hier nur der Sasser-Wurm, die Varianten des Sober-Virus oder die Warnung vor dem E-Mail-Wurm Nyxem alias MyWwife alias Blackmal (es gab ungefähr acht verschiedene Namen), der tatsächlich darauf programmiert war, Dateien zu löschen.

Zusätzlich hat das BSI noch eine Viren-Hotline eingerichtet. Wenn ein Nutzer Probleme mit einem Computer-Virus hat, kann er zwischen 9:00 und 16:00 Uhr die folgende Nummer anrufen: 0228/9582-444. Bürger können natürlich auch ihre Anfragen per E-Mail an spezielle Mail-Adressen senden: Für Anfragen, wenn es um Computer-Viren geht, ist dies *antivir@bsi.bund.de*, und wenn es um Dialer geht, *dialer@bsi.bund.de*. Auf der BSI-Seite gibt es unter ‚Kontakte' noch eine ganze Reihe von anderen speziellen Mail-Adressen zu besonderen Sachverhalten. Diese sollte man statt einer allgemeinen Adresse – wie *bsi@bsi.bund.de* – verwenden, damit die Abfrage gezielt bei der zuständigen Stelle landet und nicht erst weitergeleitet werden muss, da es ansonsten zu Verzögerungen bei der Antwort kommen kann.

Ergänzt werden diese Aufklärungsaktivitäten durch Veröffentlichungen in Fachzeitschriften und Auftritte des BSI auf Fachmessen, wie CeBit, Systems und Security. Auch auf sonstigen Messen und Kongressen halten BSI-Mitarbeiter immer wieder Fachvorträge. Erwähnenswert sind zudem Interviews zu aktuellen Themen in Radio, Fernsehen und Zeitungen.

Ebenfalls wichtig, um das Risikobewusstsein zu fördern, sind Schutzprogramme für den Anwender: Unter *www.bsi-fuer-buerger.de* ist eine Sammlung von Software (Toolbox) zu finden, in der Programme zum Download angeboten werden. Die vom BSI ausgewählten Tools müssen für die private Nutzung kostenlos sein (Freeware), sowie in deutscher Sprache zu installieren und zu benutzen sein. Gewisse funktionale und ergonomische Kriterien müssen erfüllt sein, das heißt, sie sind auch einfach in der Handhabung.

Die angebotenen Programme schützen vor Computer-Viren, Dialern, Spyware und bieten Möglichkeiten für Backup und Verschlüsselung. Zudem werden noch eine Firewall sowie ein Programm angeboten, das sicherstellt, dass Kinder gefahrlos im Internet surfen können, ohne auf jugendgefährdende Seiten zu gelangen.

Es gibt auch viele sonstige kostenlose Programme, um den Rechner vor Angriffen aus dem Internet zu schützen; sie sind aber oft in englischer Sprache abgefasst. Zwar haben die meisten Netzbürger in der Schule auch Englisch gelernt, haben jedoch häufig Probleme mit englischen Fachbegriffen.

Natürlich gibt es auch noch kostenpflichtige Sicherheitspakete. Sehr viele Internet Service Provider - wie T-Online, GMX, Web.de - bieten mittlerweile, neben der normalen Monatsgebühr für die Internet-Nutzung zusätzlich noch Sicherheitspakete an. Hierbei liegen

die Zusatzkosten bei 5 bis 10 oder 20 Euro, je nachdem, wie umfassend der Schutz sein soll. Und nach neuesten Pressemitteilungen plant auch Microsoft für das Windows Betriebssystem ein Sicherheitspaket namens ‚Windows One Care Live'. Dieses Paket soll etwa 50 Dollar im Jahr kosten. Zwar gibt es hierzu schon Kritik aus Fachkreisen mit dem Tenor: ‚Microsoft bringt Betriebssysteme und Anwendungspakete mit Fehlern heraus, die armen Kunden haben Probleme damit, und dann sollen sie auch noch für die Beseitigung der Fehler 50 Dollar zahlen'. Immerhin aber ist es schon mal ein Anfang. Es ist auch noch nicht genau bekannt, was dieses Angebot alles umfasst.

Problemgruppen

Wie durchdacht und sinnvoll Informationsangebote auch sein mögen, es verbleiben stets einige Problemgruppen, welche die vorhandenen Angebote nicht nutzen wollen. Hierzu gehören vor allem die Anwender, die sagen: ‚Wir wollen überhaupt nicht lesen. Wir wollen die Kiste anschließen und loslegen und surfen!' Vielleicht ein verständlicher Standpunkt, dass man beim Freizeitspaß ‚Surfen im Internet' kein Interesse an langwieriger Informationsbeschaffung hat. Aber dann darf man sich natürlich auch nicht beschweren, wenn wertvolle Daten auf dem Rechner verschwinden oder durch Gauner finanzieller Schaden entsteht.

Eine weitere Gruppe von Anwendern beherzigt voll das Motto ‚Geiz ist geil!'. Der Rechner samt Peripherie und Programmen war schon teuer genug, also muss alles andere kostenlos sein. Und das gilt natürlich dann auch für die Kosten von Sicherheitspaketen. Ein Schadensfall, der ohne ‚Sicherheitsnetz' evtl. eintritt, kann allerdings dann viel teurer werden.

Die Vertreter der letzten Gruppe sind der Auffassung, dass alles bequem sein muss, es darf keine Einschränkungen geben. Sicherheit ist immer ein bisschen lästig, also verzichten sie lieber darauf. Und wenn sie tatsächlich einen Virus auf ihren Rechnern haben, der keinen Schaden anrichtet und sich ‚nur' verbreitet, was soll's? Wenn andere ihn nicht bekommen wollen, sollen sie halt eben aufpassen.

Verbleibende Aufklärungsarbeit

Die verbleibende notwendige Aufklärungsarbeit besteht darin, allen Netzbürgern klar zu machen, dass es Sicherheit nur durch Wissen gibt - und nicht zum Nulltarif. Außerdem verlangt Sicherheit immer gewisse Einschränkungen, so wie der Sicherheitsgurt im Auto. Es ist zwar lästig, wenn man den Gurt anlegen muss, aber er hilft, Leben zu retten. Bei der Nutzung des Computers geht es bei den Netzbürgern sicher nur in äußerst seltenen Fällen um den Schutz von Leben, aber sehr häufig um den Schutz von Daten. Daher sind alle aufgefordert, sich zu informieren, gelegentlich auch etwas Geld in die IT-Sicherheit zu investieren und vor allem elementare Sicherheitseinstellungen zu beachten, auch wenn sie mit Einschränkungen verbunden sein sollten. Denn auf der Daten-Autobahn gefährdet

man nicht nur sich selber, sondern auch andere, wenn der eigene Rechner plötzlich Computer-Viren verteilt oder durch ein Trojanisches Pferd Teil eines riesigen Netzes geworden ist, über das dann andere Rechner angegriffen werden – womöglich mit unabsehbaren Folgen. Wie mit allen anderen technischen Errungenschaften sollte man eben auch mit dem Computer verantwortungsbewusst umgehen.

Ein sicheres Internet für alle? Netzspezifische Medienkompetenz- und Präventionsinitiativen in Europa

Dr. Gernot Gehrke

In nahezu allen europäischen Ländern haben sich im Zuge der Implementierung von Regierungsprogrammen auf nationaler und internationaler Ebene, die in Deutschland inzwischen auch von privaten Initiativen großer Konzerne begleitet werden, Aktionsprogramme und Projektzusammenschlüsse zur Förderung eines sicheren Internet etabliert. Die Übersicht zeigt, in welchen Ländern inzwischen nationale Knotenpunkte allein im Rahmen des Safer Internet Programms der Europäischen Union eingerichtet wurden (23 Knotenpunkte in 21 Ländern) - und verweist außerdem auf weitere Sicherheitsinitiativen in Nordamerika, Asien und Australien.

Übersicht zu den europäischen Sicherheitsinitiativen

Screenshot aus der Website *www.saferinternet.org* (zuletzt erreicht am 29. Juni 2006)

Die Frage, wie die Sicherheit von Internetnutzung gewährleistet werden kann, ist eine der zentralen Fragen für die weitere Entwicklung der Informationsgesellschaft in Deutschland, Europa und der Welt. Sicherheitsfragen sind keine Problemstellungen, die in lokalen, regionalen oder nationalen Kontexten befriedigend beantwortet werden können. Sie können hier *auch* beantwortet werden, keineswegs aber vollständig. Das Internet ist ein entgrenzendes Medium. Deshalb sind Fragen nach Sicherheit im Internet von internationaler Bedeutung und können nur in einem internationalen Kontext sinnvoll beantwortet werden. Die Qualität der Antworten darauf, wie ein sicheres Internet zu gewährleisten ist, oder – realistischer betrachtet – es sicherer gemacht werden kann für jene, die es nutzen, wird entscheidend dafür sein, ob und in welcher Form das Internet und seine Anwendungspotenziale künftig genutzt werden und die sich neu konstituierenden Kommunikationsräume entwickeln (können).

1 Zum Hintergrund der EU-Initiative für mehr Sicherheit im Internet

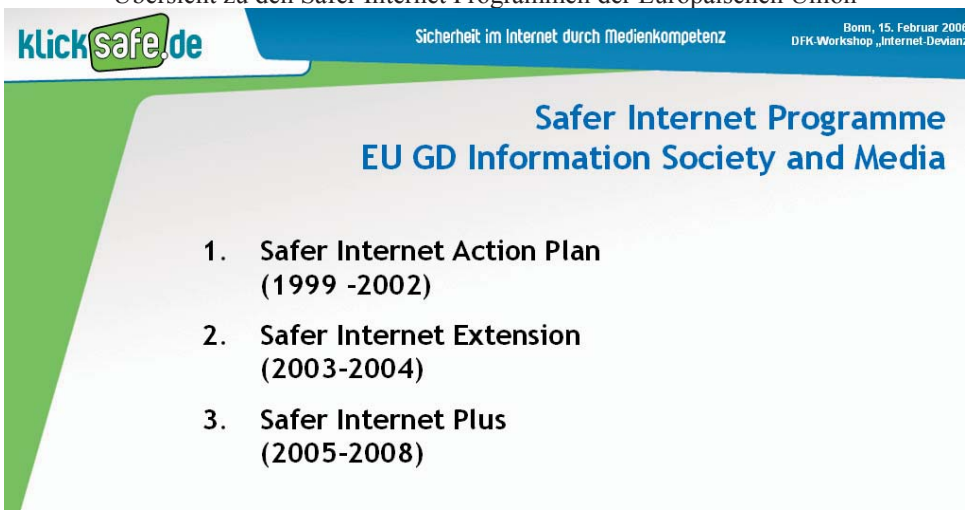
Die Ausgangsvoraussetzungen für die Implementierung von Initiativen, die ein sicheres Internet propagieren, sind denkbar unterschiedlich. So liegt die Nutzung des Internet in den einzelnen Staaten etwa der EU-15 trotz intensiver Bemühungen der Europäischen Union und ihrer Mitgliedstaaten noch immer auf sehr verschiedenen Niveaus. Diese beobachtbaren Unterschiede, die häufig unter dem Stichwort Digitale Teilung als geographische Spaltung beschrieben werden, sind noch größer, wenn die EU-24 als Referenzpunkt gewählt wird. Gleiches gilt natürlich für die wirtschaftlichen Ausgangsbedingungen oder für die rechtlichen Rahmenbedingungen, die in den jeweiligen Ländern wirksam sind und Anwendung finden. Entsprechend dieser disparaten Ausgangslage sind die verschiedenen Regierungsprogramme, die sich dem Internet und seiner Entwicklung im jeweiligen Land widmen, von sehr unterschiedlichem Charakter. Während in den Ländern Südeuropas Regierungsprogramme häufig vor allem noch darauf zielen, den generellen Umgang mit und die Anwendung der neuen Möglichkeiten zu propagieren, sind beispielsweise die Länder Nordeuropas, insbesondere Skandinaviens, auf einem anderen Niveau von Sensibilisierung und politischen Strategien angelangt. Hier liegt die generelle Nutzung des Internet inzwischen bereits über 70 Prozent. Das Internet ist hier auf dem Weg zu einem weit verbreiteten und gesellschaftlich verankerten Massenmedium, das nahezu gleichberechtigt neben Zeitung, Hörfunk und Fernsehen steht und diesen etablierten Medien teilweise schon den Rang als wichtigstes Medium abläuft. Das Verständnis für besondere Problematiken, wie zum Beispiel riskante Inhalte (Rechtsradikalismus, Pornographie, Pädophilie, Gewalt) im Internet, ist hier sehr viel stärker ausgeprägt als in jenen Ländern, in denen die Nutzung des Internet noch Wenigen vorbehalten ist und breite Bevölkerungsschichten noch nicht erreicht hat. Gleiches gilt für die Bereitschaft, entsprechende Initiativen anzustoßen und dauerhaft zu unterstützen. Wo die Nutzung noch nicht besonders verbreitet ist, kann Internetsucht von Jugendlichen kein Thema sein; wer noch keinen Einkauf für das Internet abgewickelt hat, für den spielen die mit dem Bezahlvorgang verbundenen Risiken keine Rolle; wenn Kinder keinen Zugang zu PC und Internet haben, stellt sich das Prob-

lem von gewalttätigen oder Gewalt verherrlichenden und die Entwicklung beeinträchtigenden Inhalten nicht.

Die EU hat in den vergangenen Jahren erhebliche Anstrengungen unternommen, das Internet und die über das Internet angebotenen Dienste und Anwendungspotenziale sicherer zu machen. Im Zentrum stand dabei in erster Linie die Bekämpfung illegaler, unerwünschter und schädlicher Inhalte durch die Förderung eines sicheren Umfeldes. Die Aufklärung über die Risiken soll nach den Vorstellungen der EU immer mit einer gleichzeitigen Betonung der Chancen des Internet erfolgen. Weitere Maßnahmen waren und sind die Förderung praktischer Maßnahmen zur Verbreitung vorbildlicher Projekte und die Vernetzung unterschiedlicher so genannter ‚stakeholder', also das Zusammenbringen jener Akteure, denen eine besondere Wirkungskraft im öffentlichen ebenso wie im privaten Raum zugebilligt wird.

In der Entscheidung des Europäischen Rates und des europäischen Parlaments vom Januar 1999 über die ‚Annahme eines mehrjährigen Aktionsplans der Gemeinschaft zur Förderung der sicheren Nutzung des Internet durch die Bekämpfung illegaler und schädlicher Inhalte in globalen Netzen' wird die Geschichte und die Grundlage der Safer Internet Programme beschrieben. Schon 1996 hat die Kommission dem Europäischen Parlament, dem Rat, dem Wirtschafts- und Sozialausschuss und dem Ausschuss der Region eine Mitteilung zu illegalen und schädlichen Inhalten im Internet ebenso zukommen lassen wie ein Grünbuch über den Jugendschutz und den Schutz der Menschenwürde in den audiovisuellen und den Informationsdiensten. Danach schließen sich dann eine Reihe Entscheidungen an, in den verschiedenen Organgremien, die immer wieder neu die besondere Bedeutung von Initiativen für Sicherheit im Internet betonen und schließlich in die Safer Internet Programme münden.

Übersicht zu den Safer Internet Programmen der Europäischen Union



Inzwischen ist bereits die nächste Stufe der Safer Internet Programme geplant. Von 2009 bis 2013 könnten insgesamt bis zu 70 Millionen Euro für die Weiterführung des Programms zur Verfügung gestellt werden.

Innerhalb dieser Programme existieren zentrale Zielvorstellungen, die immer wieder neu formuliert und mit Vorschlägen für konkretes Handeln versehen werden. Sie unterstreichen die besondere Bedeutung, die dieser Aktionslinie von der Europäischen Kommission beigemessen wird. Zu nennen sind hier beispielsweise

- das Zusammenspiel von Regulierung einerseits und Selbstkontrolle andererseits,
- der wirksame Verbraucherschutz,
- die Entwicklung von Filtersystemen,
- die Sensibilisierung und Bewusstseinsschaffung bei Verbraucherinnen und Verbrauchern.

Die Entwicklung von Filtersystemen wird inzwischen nicht mehr vorangetrieben; der Erfolg der bisherigen Aktivitäten war und ist noch immer begrenzt. Derzeit wird unter dem Titel SIP-Bench eine Evaluation der bisherigen EU-Anstrengungen zum Thema Filtersoftware durchgeführt. Weiteres Geld für konkrete Entwicklungen von Systemen wird derzeit nicht zur Verfügung gestellt. Erste Resultate der Bewertung sollen bereits Ende 2006 zur Verfügung stehen. Einen sehr starken Schwerpunkt setzt die EU nach wie vor auf das Element der Co- und Selbstregulierung als Element der Gestaltung eines sicheren Internet. So finden derzeit (Juli 2006) beispielsweise Konsultationen der Generaldirektion Medien und Informationsgesellschaft mit den europäischen Mobilfunkbetreibern mit dem Ziel statt, Bewusstsein für Sicherheitsaspekte zu schaffen. Diese Einbeziehung jener Akteure, deren Arbeitsfeld Gegenstand von Regulierungsbemühungen wird, ist angesichts der besonderen Charakteristika des Regelungsgegenstandes alternativlos – wie am Beispiel Internet leicht gezeigt werden kann. Regelnde Sicherheitsinitiativen können hier immer nur ein Tropfen auf dem heißen Stein sein; sie müssen angesichts der Menge von Milliarden verfügbarer Websites, den oft nur schwer identifizierbaren Akteuren und der schnell wachsenden Zahl an Anbietern, der raschen Aktualisierung der Angebote und den immer neuen und veränderten Verbreitungswegen, die ein ständiges Kompetenzdefizit auf Seiten der Regelnden und der Nutzenden hinterlassen, um Initiativen zur Selbstregulierung der Anbietenden und Kompetenzentwicklung der Nutzenden ergänzt werden.

Von Anfang war die Förderung von Sensibilisierung und ist es noch heute deshalb ein zentraler Bestandteil europäischer Politik. Die Aktionslinie Sensibilisierung ist eine von vier Aktionslinien im aktuellen Safer Internet Programm. Die weiteren sind:

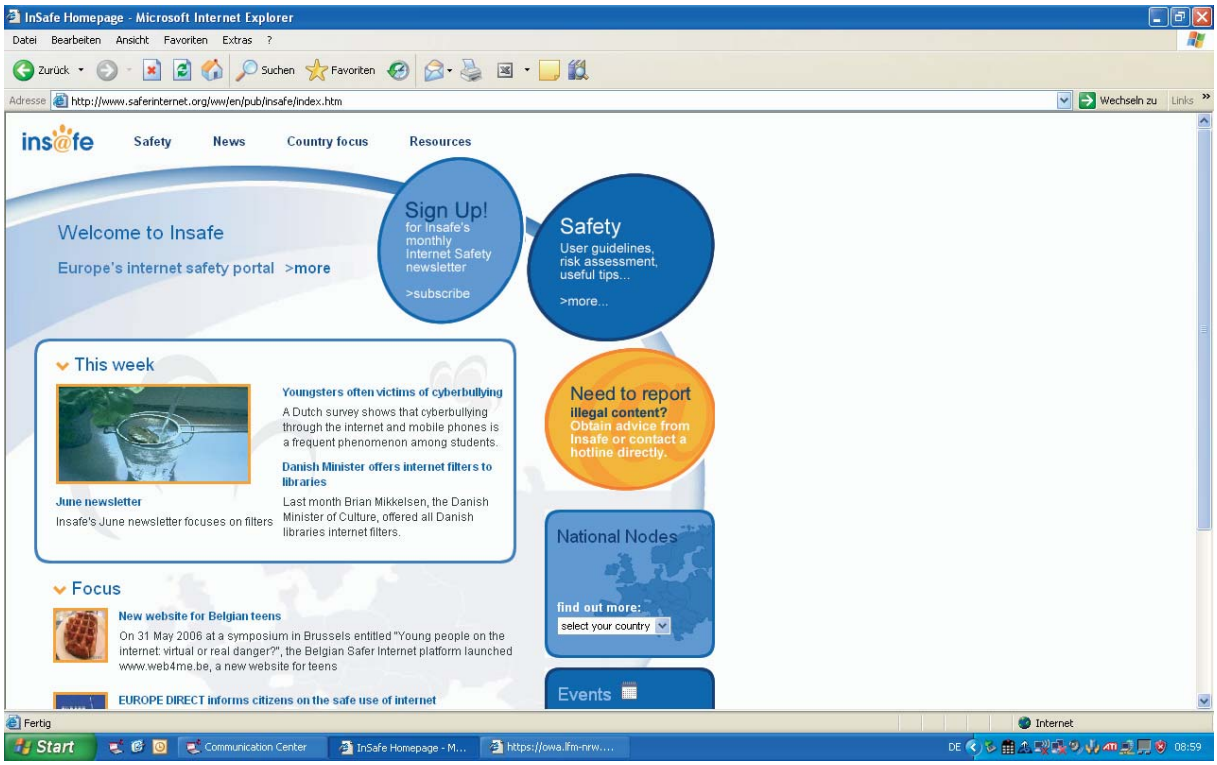
- Kampf gegen illegale Inhalte,
- Bekämpfung unerwünschter und schädlicher Inhalte und
- Förderung eines sicheren Umfeldes.

Zu den Aufgaben in dem Bereich Awareness / Sensibilisierung zählt es, nationale Knotenpunkte einzurichten – so genannte National Nodes. Sie alle haben in den Ländern die Auf-

gabe, ein Netzwerk der ‚stakeholder' aufzubauen – und damit auf nationaler Ebene ebenso wirksam zu werden, wie auf europäischer Ebene an der Durchführung von Sensibilisierungskampagnen mitzuwirken. Im gesamten Safer Internet Programm stehen 50 Prozent der Mittel für Sensibilisierung zur Verfügung. Das zeigt, wie stark der Schwerpunkt im aktuellen EU-Programm auf diese Aktionslinie gesetzt wird und wie groß die Hoffnung auf Erfolg durch eine eher weiche Regulierung ist.

Die nationalen Knotenpunkte sind im Verbund ‚Insafe' zusammengeschlossen. Hier arbeiten die National Nodes zusammen, tauschen sich über Maßnahmen und best practices aus und versuchen, kennen zu lernen, wie andere Länder ihre Kampagnen ausgestalten und in welcher Form sie Inhalte an die Zielgruppen herantragen, die als besonders unterrichtenswert eingeschätzt werden. Der europäische Verbund ist sehr stark mit paneuropäischen Aktionen in Erscheinung getreten, wie z. B. einem Storytelling Contest, der 2005 durchgeführt wurde, oder in einem weltweiten so genannten ‚Blogathon' zum Safer Internet Day 2006. Auch für 2007 ist ein Safer Internet Day geplant, an dem in allen Ländern der EU gleichzeitig das Thema Internet und Sicherheit in Aktionen und Veranstaltungen aufgegriffen wird.

Verbund der Awareness Nodes (Insafe)



Screenshot der Website *http://www.saferinternet.org/ww/en/pub/insafe/index.htm*
(zuletzt erreicht am 29. Juni 2006)

2 Beispiele für europäische Sensibilisierungskampagnen

Die einzelnen Kampagnen in den europäischen Ländern werden sehr unterschiedlich ausgestaltet und sind dabei natürlich einerseits Ergebnis der insgesamt zur Verfügung stehenden finanziellen Mittel für die Kampagne, andererseits aber auch der bereits angesprochenen unterschiedlichen Ausgangsvoraussetzungen, die in den verschiedenen Ländern vorzufinden sind. So zeigt etwa der Vergleich der Bevölkerungszahlen in Island und Deutschland schnell, das Kampagnen hier und dort einen sehr unterschiedlichen Charakter entwickeln müssen, um erfolgreich zu sein. Island kann die Bevölkerung von 300.000 Einwohnern anders ansprechen und erreichen als dies in Deutschland mit einer Bevölkerung von rund 80 Millionen möglich ist. In allen europäischen Ländern werden zum Teil sehr spezielle Schwerpunkte gesetzt, die sich auf die Situation im Land beziehen und nicht selten auch eine Spiegelung dessen sind, was insgesamt an Aktionen im Themenbereich durchgeführt wird, weil unterdessen ja auch eine Reihe von Aktivitäten entwickelt wurde, die jenseits der Programme der Europäischen Kommission durchgeführt werden. Die Beschäftigung mit riskanten Inhalten wie Pädophilie, Rechtsradikalismus, Gewalt(-verherrlichung) und Pornographie spielt dabei in allen Ländern eine herausgehobene Rolle. Die folgende Auswahl zeigt einige Beispiele für nationale Kampagnen. Sie sind hier nur kurz beschrieben. Ausführliche Informationen stehen über die jeweiligen Websites zur Verfügung.

Awareness Node Großbritannien (Internet Safety Zone)

Screenshot von *http://www.internetsafetyzone.co.uk/root/* (zuletzt erreicht am 29. Juni 2006)

In Großbritannien wird der National Node von der so genannten ‚Public Awareness Sub group' der ‚Internet Task Force on Child Protection' des Innenministeriums betreut. Namhafte Unternehmen und Einrichtungen unterstützen diese Initiative. Zu ihnen gehören neben dem Innenministerium und dem ‚National Criminal Intelligence Service' auch Unternehmen wie AOL, Vodafone, Fiscali, Orange, O2 und Microsoft. Beteiligt sind ebenso OFCOM, die britische Regulierungsbehörde für Medien und Telekommunikation, die ‚British Educational Communications and Technology Agency (BECTa)', die BBC, British Telecom oder CEOP, das neu gegründete ‚Child Exploitation and Online Protection Centre'. Über die Website verfolgt die ‚Internet Safety Zone' einen ganzheitlichen Ansatz und möchte Informationen zur sicheren Nutzung des Internet ebenso an Erwachsene wie an Kinder und Jugendliche weitergeben. Erwachsene werden dabei in ihren unterschiedlichen Rollen als Eltern, Betreuende, Großeltern, Lehrende, Beratende, Sozialarbeitende etc. adressiert, um es ihnen so zu erleichtern, junge Menschen über das Thema Sicherheit im Internet zu informieren.

Spanischer Awareness Node (Protegeles)

Screenshot von *http://www.protegeles.com/* (zuletzt erreicht am 29. Juni 2006)

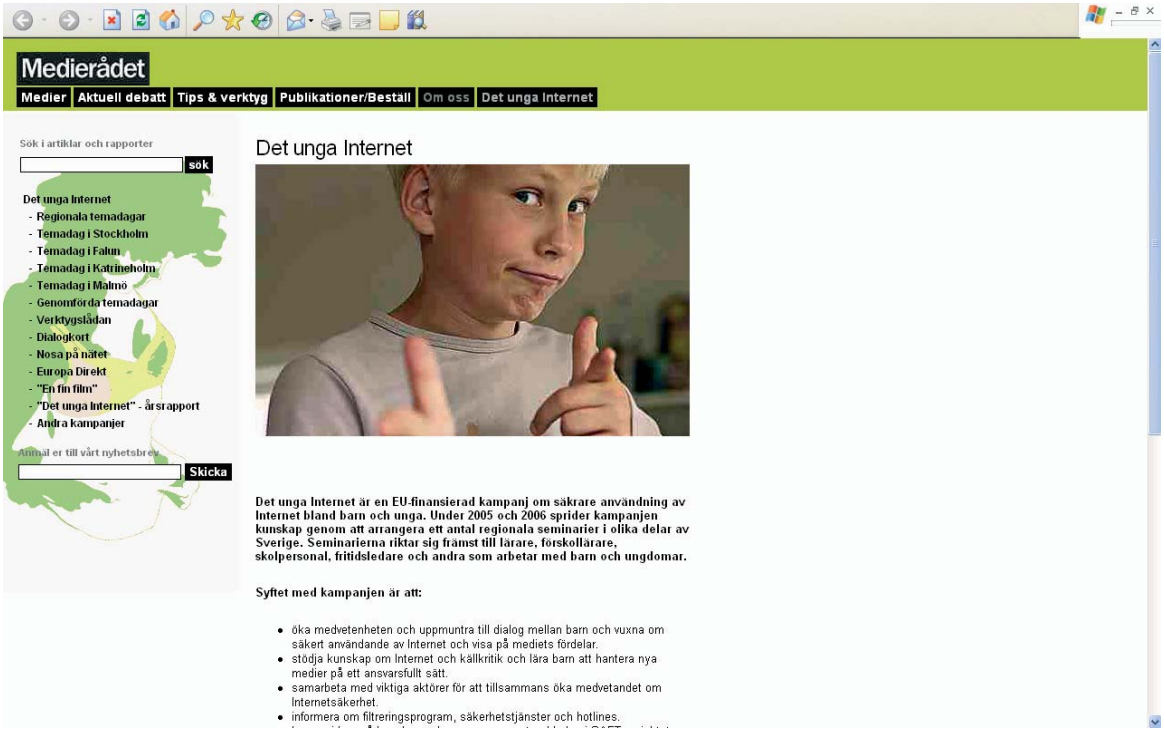
Der spanische Awareness Node mit dem Titel SAFENET wird gemeinsam von Protégeles und Terra Networks getragen. Protégeles wurde vom spanischen Unternehmen Optenet (früher Red Educativa) und der Nicht-Regierungsorganisation ACPI (Acción Contra la Pornografía Infantil) gegründet, um den Anforderungen der EU-Kommission für eine Unterstützung des Awareness Nodes zu entsprechen. Terra Networks ist ein global operierendes Internetunternehmen mit Standorten in 40 Ländern. Über die Website stellt Protégeles in erster Linie seine Aktivitäten beim Betreiben einer Hotline gegen Kinderpornographie in den Mittelpunkt.

Awareness Node Tschechien

Screenshot von *http://www.safer-internet.cz/home.asp?idk=1* (zuletzt erreicht am 29. Juni 2006)

Der tschechische Awareness Node richtet sich in erster Linie an Kinder, Lehrer und Eltern. Ziel ist es, eine Diskussion darüber zu entfalten, welche Inhalte warum schädlich sind und wie ihnen entgegengewirkt werden kann. Veranstaltungen, die diese Thematik aufgreifen, spielen dabei eine zentrale Rolle.

Awareness Node Schweden (Det unga internet)



Screenshot von *http://www.medieradet.se/templates/Page____496.aspx* (zuletzt erreicht am 29. Juni 2006)

Der schwedische Awareness Node wird von zwei Partnern getragen – dem schwedischen Medienrat (dem schwedischen Bildungsministerium unterstellt) und der nationalen Agentur für die Verbesserung des Schulwesens. Die Kampagne ‚Det unga Internet' (Das junge Internet) konzentriert sich auf die Entwicklung von konkreten Hilfsmitteln (‚Werkzeugkasten') zur Vermittlung des Themas Internetsicherheit in der Schule und die Durchführung von Konferenzen in unterschiedlichen Regionen von Schweden. Der Werkzeugkasten fasst dabei bereits existierende Materialien zusammen und ergänzt sie um neue Entwicklungen. Gleichzeitig produziert der Awareness Node auch Materialien für die Zielgruppe der 4 – 8-Jährigen. In den Veranstaltungen werden vor allem Lehrende und jene, die sich professionell mit Kindern und Jugendlichen beschäftigen, qualifiziert und geschult.

3 Klicksafe.de – die deutsche Kampagne

Klicksafe.de ist der deutsche Knotenpunkt im europäischen Netzwerk. In Deutschland hat die Europäische Kommission das Konsortium aus

- Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz
- Landesanstalt für Medien Nordrhein-Westfalen (LfM)
- Europäisches Zentrum für Medienkompetenz (ecmc)

beauftragt, als awareness campaign ‚klicksafe.de' das Safer Internet Programm umzusetzen und einen nationalen Knotenpunkt in Deutschland aufzubauen. Die entscheidenden Aufgaben liegen darin, Kinder und Jugendliche, Eltern und Pädagogen aufzuklären und Kompetenzen zu vermitteln. Parallel werden auch den Anbietern von Internetseiten Möglichkeiten aufgezeigt, zu höherer Sicherheit im Internet beizutragen. Der Autor dieses Beitrages ist Geschäftsführer des Europäischen Zentrums für Medienkompetenz. Die folgenden Informationen wurden im Projektbüro des Projektes erarbeitet.

Der Awareness Node Deutschland arbeitet seit 1. November 2004. Ziel eines Sensibilisierungs-Netzes in Deutschland für mehr Sicherheit im Internet ist der Aufbau eines organisatorischen und kommunikativen Knotenpunktes. Zielgruppen der Aktivitäten von klicksafe.de sind Kinder und Jugendliche, die über Eltern, Pädagogen und andere Multiplikatoren erreicht werden sollen. Klicksafe.de will die Entwicklung von Maßnahmen zielorientiert vorantreiben und sie zugleich in einen europäischen Kontext stellen. Vier Säulen konstituieren das Projekt.

Die Klicksafe-Kampagne:

- klicksafe.de führt eine bundesweite Sensibilisierungsaktion für Internetsicherheit durch, unter Einbezug unterschiedlicher Medien,
- spricht alle Zielgruppen an und
- organisiert themenbezogene Veranstaltungen.

Das Klicksafe-Netzwerk:

- klicksafe.de knüpft ein Netzwerk mit Anbietern und Akteuren, die über Sicherheit im Internet aufklären und Medienkompetenz fördern,
- nutzt die Expertise des Klicksafe-Beirats und
- fördert die Diskussion zwischen Verantwortlichen aus Bildung, Wirtschaft und Technik.

Die Klicksafe-Website:

- klicksafe.de arbeitet als nationale Plattform und unabhängiges Informationsportal,
- bündelt Informationen über Sicherheit im Internet,
- stellt empfehlenswerte Initiativen und Projekte vor,
- informiert aktuell über Entwicklungen, Chancen und Risiken,
- bindet Informationen aus anderen europäischen Staaten ein,
- informiert über Internetbeschwerdestellen (Hotlines) und
- bietet Netzregeln für Inhalte-Anbieter, um ihnen Möglichkeiten aufzuzeigen, wie sie selbst zur Sicherheit im Internet beitragen können.

Die Klicksafe-Qualifizierung:

- klicksafe.de entwickelt Konzepte für bundesweite Schulungen mit Lehrern, Eltern und Pädagogen,
- unterstützt Schulungen für Kinder, Jugendliche, Eltern, Pädagogen und Multiplikatoren zu Chancen und Risiken des Internet.

Awareness Node Deutschland (klicksafe.de)

Screenshot von *http://www.klicksafe.de/#realContent* (zuletzt ereicht am 29. Juni 2006)

Von besonderer Bedeutung innerhalb des Projektes klicksafe.de war die Produktion und Ausstrahlung eines TV-Spots zum Thema Internetsicherheit. Die Botschaft des Klicksafe TV-Spots, welcher erstmals am 20. Oktober 2005 ausgestrahlt wurde, lautet: ‚Im wirklichen Leben würden Sie ihre Kinder schützen, dann machen Sie es doch auch im Internet'. Der von Ogilvy & Mather, Frankfurt, für das Projekt klicksafe.de kostenfrei entwickelte Spot greift vier Problembereiche des Internet auf und stellt diese real in den familiären Kontext. An der Haustür einer jungen Familie klingeln nacheinander verschiedene Personengruppen, die zum Sohn ‚Klaus' der Familie wollen. Eine Gruppe Rechtsradikaler, eine Gruppe Prostituierter, ein Kämpfer aus einem Computerspiel (der in der Wohnung rumballert) und zum Schluss ein netter Herr, der die fünfjährige Tochter der Familie wegführt, um ihr einen ‚richtigen' Hasen zu zeigen. Der Spot provoziert und schockiert, vor allem durch den subtilen Einsatz des älteren Herrn, der einen Pädophilen verkörpern soll und die naive Haltung der Mutter. Der Spot wirkt sehr stark emotional. Die Zugriffszahlen auf die Klicksafe-Website sind nach der Ausstrahlung des Spots um das Dreifache gestiegen, viele Anfragen erreichen das Projektbüro mit der Bitte um konkrete Hilfestellungen. Deutlich

wird, dass die Wirkung des TV-Spots sein Hauptziele erreicht: Aufmerksamkeit für das Thema ‚Internetsicherheit' und das Portal klicksafe.de.

Ein wichtiger Pfeiler der klicksafe.de-Kampagne ist die klicksafe.de-Website, welche die Nutzer über die relevanten Sicherheitsthemen im Internet informiert, best-practice-Materialien versammelt und als Portal zu empfehlenswerten Seiten führt. Ebenso finden sich hier die Hintergrundinformationen zum Projekt, wie auch zu den nationalen, wie auch internationalen Partnern. Die Website ‚klicksafe.de' bietet strukturierte und übersichtliche Informationen zu den wichtigen Sicherheitsthemen an und stellt dabei präventive bzw. pädagogische Jugendschutzmaßnahmen in den Vordergrund. In Deutschland etabliert sich die Website als unabhängiges Portal für die Förderung von Sicherheit im Internet durch Medienkompetenz. Rückmeldungen der Nutzer (E-Mails an das klicksafe.de-Büro) und Expertenbefragungen (des Beirats) zur Website bestätigen, dass das Angebot in seiner dargestellten Struktur angenommen wird.

Klicksafe.de hat es sich zur Aufgabe gemacht, kontinuierlich bestehende empfehlenswerte Informationen und Materialien auszuwählen und auf der Website kostenlos zum Downloaden bereitzustellen. Darüber hinaus werden von klicksafe.de erarbeitete konkrete umsetzbare Hilfestellungen auf der Website angeboten. Dazu gehört eine Vielzahl an praktischen Maßnahmen (z.B. Klicksafe.de-Tipps im Bereich ‚Problematisches im Netz'), wie das Surfen, Chatten und Mailen für Kinder und Jugendliche sicherer gestaltet werden kann. Auf der Grundlage von aktuellen Entwicklungen und basierend auf den Ergebnissen von Studien werden die Themen kontinuierlich angepasst und überarbeitet bzw. erweitert. So wurden beispielsweise die Themen des ausgestrahlten TV-Spots - Rechtsradikalismus, Pornografie, Gewaltdarstellungen und Pädosexualität im Internet - für Eltern inhaltlich aufbereitet. Die Themen werden aus der Sicht des gesetzlichen Jugendmedienschutzes erläutert. Außerdem werden pädagogische Jugendschutzmaßnahmen aufgezeigt, welche ersten Schritte Eltern zum Schutz ihrer Kinder unternehmen können und bei welchen Hotlines/Institutionen problematische Inhalte gemeldet werden können.

Für die Zielgruppen der klicksafe.de-Website, vor allem Erwachsene, wie Eltern und Pädagogen ohne größere technische und inhaltliche Vorkenntnisse, werden die Informationen verständlich in Form von Fragen präsentiert. Dies geschieht vor allem vor dem Hintergrund, dass Studien immer wieder belegen, dass nur wenige Eltern und Pädagogen wissen, was ihre oder die ihnen anvertrauten Kinder im Internet machen oder wie sie sie vor schädlichen Inhalten im Internet schützen können. Die Website verfolgt deshalb zu allererst das Ziel, die Aufklärung und Sensibilisierung der Eltern und Pädagogen voranzutreiben, um über diesen Weg den Kinder- und Jugendschutz zu verbessern. Aber nicht allein die Eltern und Pädagogen sind dafür verantwortlich, dass Heranwachsende einen verantwortlichen Umgang im Internet erlernen, sondern auch den Anbietern von Internetseiten sollen auf der Website die Möglichkeiten aufgezeigt werden, zu mehr Jugendschutz im Internet beizutragen. Gemeinsam mit der Partnerorganisation jugendschutz.net wird auf der Website von klicksafe.de dieses Ziel verfolgt. Die Zugriffsstatistiken zeigen eindeutig,

dass das Ziel der Marketingmaßnahme mit dem TV-Spot für mehr Sicherheit im Internet zu sensibilisieren und die Aufmerksamkeit der breiten Öffentlichkeit auf *www.klicksafe.de* zu lenken, erreicht wurde. Bei der Auflistung der URLs, die zuerst angesteuert werden, liegt die Seite mit dem TV-Spot an erster Stelle. Jedoch werden auch vor allem die Themenbereiche ‚technische Filter', ‚Sicher surfen' und ‚Problematisches im Netz' hoch frequentiert. Die Idee des Spots, dass Kinder im Internet wie im realen Leben geschützt werden müssen, hat demzufolge die Zuschauer erreicht.

Neben der Bereitstellung von Informationsmaterialien sieht klicksafe.de auch einen Aufgabenbereich in der Entwicklung von Fortbildungsmaßnahmen für Multiplikatoren. Gemeinsam mit dem Verein Schulen ans Netz e.V. arbeitet klicksafe.de an der Entwicklung und Durchführung eines ‚Internetsicherheitsmoduls' für Pädagogen und hat inzwischen Schulungen aufgenommen. Da eine grundlegende Schulung von Pädagogen im Bereich Internetsicherheit in Deutschland notwendig ist und keine erprobten Module vorliegen, haben klicksafe.de und WebLOTSEN (Projekt von Schulen-ans-Netz) gemeinsam ein Internetsicherheitsmodul aufgebaut. In einer ersten Pilotphase von April bis Sommer 2006 wurden drei Veranstaltungen in ganz Deutschland durchgeführt. Nach der Pilotphase wird das Internetsicherheitsmodul evaluiert und modifiziert, um eine Optimierung des Schulungskonzeptes und der dazugehörigen Handreichungen zu erreichen. Das modifizierte Modul wird in der 2. Projektphase, ab Herbst 2006, auf breiter Ebene in Fortbildungsinstitutionen implementiert, damit eine große Anzahl an Pädagogen geschult wird. Klicksafe.de plant, in dieser Weise auch Konzepte für die Elternbildung, wie auch für die außerschulische Jugendarbeit zu entwickeln.

Um breit adressieren zu können, ist klicksafe.de dabei auf eine Partnerstruktur angewiesen, die letztlich die Erwartungen einlösen kann, die ein Fernsehspot weckt. Dazu gehören Organisationen wie der Medienpädagogische Forschungsverbund Süd-West oder Projekte wie Internet-ABC und mekonet – das Medienkompetenznetzwerk NRW. Die folgende Übersicht zeigt, welche Institutionen und Einrichtungen mit welchen Projekten, Internetangeboten und Materialien klicksafe.de unterstützen. Eine aktuellere Übersicht liefert jeweils die Website unter *www.klicksafe.de*.

Portale und Suchmaschinen für Kinder und Jugendliche in Deutschland

- *www.internet-abc.de* Informationsportal für Kinder und Eltern
- *www.internauten.de* Kinder-Portal zur Aufklärung über Gefahren des Internet
- *www.netzcheckers.de* Jugendportal des Projektbüros ‚Jugend ans Netz'
- *www.seitenstark.de* Arbeitsgemeinschaft vernetzter Kinderseiten, gemeinsam gegründet von ‚Milkmoon', ‚Blinde-Kuh' und ‚Kidsville'
- *www.blinde-kuh.de* Umfangreiche Suchmaschine für Kinder; kommentierte Links sowie Verknüpfung zu Kinderseiten im Internet

- *www.kidsville.de* Interaktive ‚Mitmachstadt' im WWW für Kinder
- *www.milkmoon.de* Suchmaschine für Kinder
- *www.kindersache.de* Kinderportal des Deutschen Kinderhilfswerks

Webseiten zur Förderung von Sensibilisierung und Awareness

- *www.sicher-im-netz.de* Bundesweite Allianz namhafter Partner aus Politik, Wirtschaft und Gesellschaft mit dem Ziel, das Internet speziell für deutsche Nutzer sicherer zu machen
- *www.mekonet.de* Medienkompetenz-Netzwerk in Nordrhein-Westfalen
- *www.fairlink.de* Jugendinitiative gegen rechtsextreme Webseiten und zur Förderung von Toleranz
- *www.kidcarenet.de* KidCareNet richtet sich gegen Kindesmissbrauch, Gewalt gegen Kinder im allgemeinen sowie gegen Kinderpornografie im Internet
- *www.bundespruefstelle.de* Informationen für Eltern zur Orientierung im Medienalltag

Kampagnen

- ‚Schau Hin!' Kampagne des Bundesministeriums für Familie, Senioren, Frauen und Jugend zur Information von Eltern (*www.schau-hin.org*)
- ‚Sicherheits-Truck-Tour' Aktionstage zur Information von Familien über Sicherheitsanforderungen im Internet (*www.sicher-im-netz.de*)

Broschüren

- ‚Ein Netz für Kinder – Surfen ohne Risiko?' Leitfaden für Eltern und Pädagogen im Auftrag des Bundesministeriums für Familie, Senioren, Frauen und Jugend (*www.bmfsfj.de/Kategorien/Publikationen/Publikationen,did=4712.html*)
- ‚Chatten ohne Risiko?' Sicherheitshinweise, Bewertungen und Empfehlungen für Kinder, Eltern und Anbieter (*www.jugendschutz.net/materialien/chatten_ohne_risiko.html*)
- ‚Kindersache – der Internetguide für Kids' Broschüre des Deutschen Kinderhilfswerks für Kinder (*www.kindersache.de/interakt/sicherheit/Internet-Guide2.pdf*)
- Unterrichtsreihe ‚Echt cool und fast umsonst - Kinder als Konsumenten in den Neuen Medien' Broschüre des Deutschen Kinderhilfswerks und der FSM für Kinder und Lehrer

- Der ‚FSM Internetguide für Eltern' (*www.fsm.de/?s=FSM+Internet+Guide+f%FCr+Eltern*)

Kindersoftware

- ‚Kinderbrauser' Lernsoftware des Instituts für Film und Bild (*www.kinderbrauser.de*)
- Überblick über 80 geprüfte Spiel- & Lernprogramme (Broschüre, Band 14) des Bundesministeriums für Familie, Senioren, Frauen und Jugend (*www.bmfsfj.de/Kategorien/publikationen,did=22916.html*)

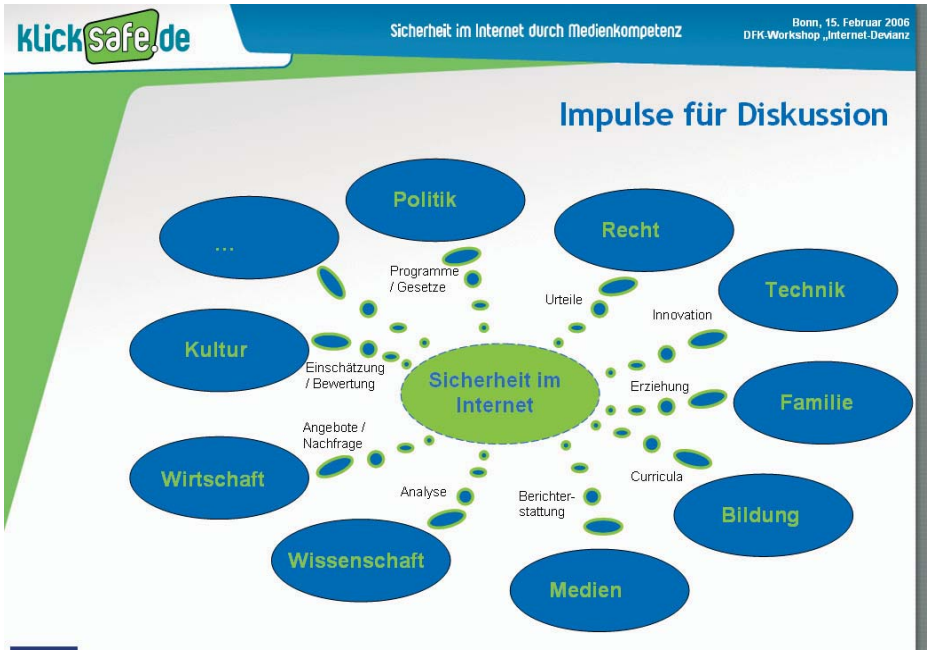
Projekte

- *www.jugend.info* Die Bundesinitiative ‚Jugend ans Netz' des Bundesministeriums für Familie, Senioren, Frauen und Jugend unterstützt junge Menschen beim außerschulischen Wissenserwerb über das Medium Internet (*www.bmfsfj.de/RedaktionBMFSFJ/Broschuerenstelle/Pdf-Anlagen/Flyer-Jugend-ans-Netz,property=pdf.pdf*)
- *www.erfurter-netcode.de* Qualitätsinitiative zur Verleihung von Gütesiegeln für Kinderangebote
- ‚Rechtsextremismus im Internet' CD-ROM für Eltern und Schüler der Entimon-Projektgruppe (*www.bpb.de/publikationen/08103406325021770341392050832337,,0,Rechtsextremismus_im_Internet.html*)

4 Ausblick

Die Diskussion um Sicherheit im Internet leidet häufig darunter, dass einzelne Aspekte des Themenbereichs sehr exklusiv diskutiert werden und nicht hinreichend in einen geeigneten Kontext eingebettet werden. Beispiele dafür sind die Diskurse um rechtliche Rahmenbedingungen, technische Fortentwicklungen von Nutzungstechniken oder Filtersystemen sowie Nutzungssituationen von Kindern und Jugendlichen in Schule oder Familie. Ein systemisch angeleiteter Ordnungsversuch lohnt deshalb und macht zunächst die Größe des Themenfeldes und einige der wichtigsten bedingenden Faktoren sichtbar.

Sicherheit im Internet – Gesellschaftlicher Kontext



Trotzdem werden Diskussionen häufig zu eng geführt: Wie kann also eine rechtliche Regelung wahlweise ent- oder verschärft werden, um damit das Problem lösen? Was können wir in der Schule tun, um das Problem einer Lösung näher zu bringen? Wie können Eltern in die Lage versetzt werden, besser die Internetnutzungsgewohnheiten ihrer Kinder mit zu gestalten? Jedes dieser genannten Beispiele ist ein wichtiges Element im komplexen Prozess, Sensibilität für das Thema ‚Sicherheit im Internet' zu schaffen. Es scheint jedoch von besonderer Bedeutung zu sein, gerade die Komplexität und Vielschichtigkeit des Gegenstandsbereichs zum Ausgangspunkt von Überlegungen zu machen. Der verständlichen Versuchung, ein sehr komplexes Problem analytisch quasi so zu reduzieren, dass die Komplexität bearbeitbar wird, sollte nicht zu Lösungen führen, die der Realität dann nicht angemessen sind. Für alle Lösungsversuche und jeden Schritt zur Antwort auf die Frage, wie denn Internetsicherheit zu gewährleisten sei und wie das Niveau von Sensibilisierung erhöht werden könnte, sollte das Wissen um die Komplexität des Themenfeldes leitend sein. Es stellen sich große Aufgaben in der Schule, wo Curricula nicht in Ansätzen darauf reagieren, was sich an Herausforderungen stellt. Das gesamte technische Feld wird selbst für Experten schwierig zu überblicken. Und wie die Situation in Familien verbessert werden kann, wenn es um Kinderbetreuung und Kindererziehung gilt, wird nicht zuerst unter Mediennutzungsaspekten diskutiert, sondern ist ein gesellschaftliches Megathema. Zu schweigen davon, dass die Diskussion, wie weiter oben erwähnt, im Grunde international zu führen ist, weil nationale Lösungen kaum noch greifen. Schon deshalb brauchen regelnde und sensibilisierende Eingriffe immer auch die Mitwirkung breiter gesellschaftlicher Kreise und der Anbieter selbst im Sinne von regulierter Selbstregulierung und Entwicklung wie Förderung von Medienkompetenz aller Beteiligten. Die Initiativen im Rahmen der europäischen Safer Internet Programme liefern dafür eine viel versprechende und sehr geeignete Ausgangsbasis.

Prävention von Devianz rund um das Internet
Ein Ausblick auf Handlungs- und Forschungsfelder

Dr. Christiane Eichenberg & Dr. Werner Rüther

Die rasanten Entwicklungen auf dem Gebiet der digitalen Technologien und die damit einhergehende Ausbreitung des Internet auf eine ständig zunehmende Zahl von Menschen auf dem gesamten Erdball haben die gesellschaftlichen Informations- und Kommunikationsstrukturen in den letzten 10-15 Jahren nahezu revolutioniert.

Dabei haben sich in vielen Bereichen vor allem ganz neue Möglichkeiten und Chancen für die teilnehmenden Netzbürgerinnen und Netzbürger aufgetan, welche auf der anderen Seite wie selbstverständlich auch von gewissen Risiken und Gefahren begleitet sind. Zu diesen Risiken zählen ganz unterschiedliche Formen von abweichenden, problematischen, in irgendeiner Form schädlichen Verhaltensweisen, welche durch das Internet erst ermöglicht oder gegebenenfalls auch gefördert werden. Es entwickelt sich insofern ein neuer Bereich von zum Teil noch nicht (straf-)rechtlich eindeutig und klar definierten Phänomenen, die man insgesamt unter dem Begriff der ‚Devianz rund um das Internet' oder auch kürzer und griffiger unter dem Begriff der ‚E-Devianz' zusammenfassen kann.

Die zahlreichen und unterschiedlichen Phänomene der E-Devianz sind logischer Weise erst durch das Internet und die dahinter stehenden technologischen Neuerungen der ‚digitalen Revolution' entstanden. Sie sind Ausdruck von radikal veränderten Gelegenheitsstrukturen zur weltweiten Kommunikation in den letzten 10-15 Jahren. Ihre einzelnen Erscheinungsformen und ihre quantitativen Größenordnungen sind zum gegenwärtigen Zeitpunkt der dynamischen Entwicklung vielfach noch gar nicht klar feststellbar, und sie werden von unterschiedlichen gesellschaftlichen Akteuren mit unterschiedlichen Interessenstandpunkten und mit unterschiedlichen professionellen Blickwinkeln auch unterschiedlich beschrieben und bewertet (vgl. Rüther, 2006).

Dass die Themen zur ‚Devianz rund um das Internet' und besonders auch die Aspekte der ‚Prävention von E-Devianz' von großer Wichtigkeit sind und auch in Zukunft nicht an Bedeutung verlieren werden, ist unter Expertinnen und Experten aus unterschiedlichen Disziplinen, die in den verschiedensten Zusammenhängen mit der Thematik konfrontiert sind, allerdings weitgehend konsensuell.

Auch wenn Pädagogen, Psychologen, Soziologen, Kriminologen, Juristen, Informatiker, Betriebswirte etc. jeweils unterschiedliche Aspekte fokussieren, wenn sie sich mit devianten Verhaltenweisen im Netz und ihren Auswirkungen befassen, so verfolgen alle Berufsgruppen ein gemeinsames Ziel:

Welche Präventionsstrategien sind zielführend, um deviantes Verhalten im Zusammenhang mit der Internetnutzung zu minimieren? Welcher Handlungs- oder Forschungsbedarf besteht zum aktuellen Zeitpunkt, um den Devianz-Phänomenen im Internet zu begegnen?

Da diese Phänomene ein breites Spektrum an Delikten abdecken (von Piraterie- und Betrugsdelikte über Interaktions- und Gewaltdelikte bis hin zu Sachbeschädigungen im Internet, vgl. die Einzelbeiträge in diesem Band), stellt sich die Frage, ob und in welcher Form Präventionsmaßnahmen möglich sind, die phänomenübergreifend wirksam sein können.

I Zum Präventionsbegriff

Prävention (spätlat. preventio: das Zuvorkommen) bezeichnet alle Bemühungen, pathologische Abläufe zu verhindern bzw. in ihrem Verlauf abzumildern. Dabei fokussiert Prävention hauptsächlich die Beeinflussung und Vermeidung delinquenten Verhaltens, die Vorbeugung von Krankheiten und Verhaltensstörungen sowie die Verhinderung bzw. Abmilderung belastender Lebensereignisse.

Bei der Klassifikation von Prävention hat sich die Einteilung nach dem zeitlichen Aspekt (Caplan, 1964) durchgesetzt. Die *primäre Prävention* umfasst dabei alle Maßnahme zur Senkung der Auftretenswahrscheinlichkeit bestimmter Ereignisse, die *sekundäre Prävention* Maßnahmen der Früherkennung und Frühbehandlung mit dem Ziel der Abmilderung von Folgen eines schon eingetretenen Ereignisses und die *tertiäre Prävention* intendiert die Vermeidung von Folgeschäden bei einer bereits eingetretenen Schädigung.

Während auch die sekundären und die tertiären Präventionsstrategien im Umgang mit den Devianz-Phänomenen im Internet zum gegenwärtigen Zeitpunkt als wenig entwickelt anzusehen sind, gilt dies im besonderen Maße und erst recht für die primären Präventionsansätze.

Bei vielen Problemen im Zusammenhang mit kriminellen Inhalten und Taten im Internet wurde zunächst versucht, ihnen mit *technischen Maßnahmen* zu begegnen. Dass technologische Maßnahmen zwar sinnvoll sein können, aber als einziges Mittel nicht weitreichend genug sind, um Netznutzer vor bestimmten gefährdenden Internetinhalten zu schützen, kann folgendes Beispiel illustrieren. Um Kinder und Jugendliche von beispielsweise rechtsextremistischem oder pornografischem Material fernzuhalten, wurde spezielle Filter-Software (z.B. CYBERsitter, *www.cybersitter.com)* entwickelt, die in Schulen oder am heimischen PC installiert werden kann. Doch leicht lässt sich einsehen, dass solche Maßnahmen nur ein vermeintlicher Schutz sind, da Kinder und Jugendliche häufig über mehr Interneterfahrung verfügen als die Elterngeneration und das Knowhow haben, Zugriffssperren zu umgehen. Zudem kann man sich die Frage stellen, ob diese nicht die Antithese zu Vertrauen und vernünftigem Diskurs zwischen Erwachsenen und Kindern bilden. Wichtiger als technische Abhilfe ist in jedem Fall die Überlegung, wie man die Diskussion mit Kindern und Jugendlichen anregen kann über das, was sie im Internet zu sehen bekommen, anstatt ihnen dieses Material durch Vorzensursysteme vorzuenthalten, was durch diese Tabuisierung erst recht neugierig macht.

Vor diesem Hintergrund erscheint es wesentlich, angesichts der Entwicklung der IT-Technik und IT-Sicherheitstechnik als geltende Rahmenbedingungen, den Menschen und sein Verhalten als wichtige kriminogene Faktoren im Zusammenhang mit Delinquenz im Internet in den Mittelpunkt der Betrachtung zu stellen. Damit angesprochen ist die *soziale Ebene* von Prävention im Zusammenhang mit deviantem Internetnutzungsverhalten von Seiten der Täter und den Effekten auf Opferseite.

II Handlungsbedarf

Initiativen, die sich mit der Prävention von E-Devianz befassen, müssen insgesamt zwei Zielgruppen berücksichtigen: Um das Auftreten von deviantem Verhalten zu vermeiden, muss einerseits das *Unrechtsbewusstsein* von potenziellen Tätern, andererseits das *Risikobewusstsein* bei potenziellen Opfern fokussiert werden. Die am im diesem Band dokumentierten Workshop teilnehmenden Expertinnen und Experten extrahierten die in Tabelle 1 zusammengefassten Strategien zur Umsetzung dieser Ziele.

Einzelne Handlungsfelder	
Förderung der Medien- und Informationskompetenz bei Kindern und Jugendlichen	▪ Implementation als fester Baustein der Bildung in Kindergarten und Schule ▪ Stärkere und gezielte Nutzung der vorhandenen Ausstattung in Schulen
Explizieren von Regeln bzgl. der Ge- und Verbote bei der Internetnutzung	
Ìnstitutionalisierung regelmäßiger Kampagnen zur Aufklärung, Sensibilisierung und Förderung des Risikobewusstseins	▪ z.B. Patch-Day von Microsoft mit regelmäßigerer Häufigkeit und stärkerer Medienaufmerksamkeit
Bündelung der Strafverfolgung	▪ Schwerpunktstaatsanwaltschaft für Internetkriminalität
Breiterer Einsatz von Reputationssystemen	▪ Baustein zur Selbstregulation von sozialverträglicher Kommunikation im Internet
Forderungen an Hersteller von PC-Produkten	▪ Verbesserung der Benutzerfreundlichkeit vorhandener technischer Lösungen ▪ Vermarktung zertifizierter Produkte
Meta-Bedarf **→ Bündelung der bereits vorliegenden Materialien, Hinweise, Hilfestellungen und Handreichungen von unterschiedlichen Institutionen**	

Tab. 1: Primärer Handlungsbedarf zur Prävention von Devianz im Internet

Als basalste Maßnahme wurde eine effektive zielgruppenspezifische Vermittlung von umfassender *Medienkompetenz* im Umgang mit dem Internet gesehen. Zum aktuellen Zeitpunkt ist die Medienerziehung als pädagogischer Baustein in Bildungseinrichtungen wie Kindergarten und Schulen noch nicht flächendeckend in die Lehrpläne implementiert. Wünschenswert wären feste didaktische Einheiten, die im größeren Ausmaß als bisher regelhaft in Bildungscurricula eingebunden werden. Dafür ist Voraussetzung, dass Erzieher/-innen und Lehrer/-innen selbst qualifiziert und fortlaufend fortgebildet werden, um mit den sozio-technischen Entwicklungen im Bereich der neuen Medien Schritt halten zu können. Die Vermittlung von Medienkompetenz ermöglicht, zugleich das Unrechts- sowie das Risikobewusstsein bezüglich devianten Nutzungsverhaltens zu vermitteln und zu schärfen.

Damit hängt zusammen, dass in der Gemeinde der Internetnutzer unzureichend Wissen darüber herrscht, dass bestimmtes Verhalten verboten bzw. einen strafrechtlich relevanten Tatbestand darstellt. Während beispielsweise früh moralische Werte bezüglich des Eigentums anderer vermittelt und internalisiert wurden (z.B. ‚Du darfst im Geschäft nichts mitnehmen, ohne zu bezahlen.'), scheinen diese tradierten Normen nicht automatisch auf das Agieren in der Netzwelt übertragen zu werden. Ob so digitale Pirateriedelikte wie Raubkopien oder Diebstahl des geistigen Eigentums (z.B. das Kopieren ganzer Texte bzw. Textbausteine, die von Studierenden innerhalb von Haus- oder Diplomarbeiten unzitiert verwendet werden, vgl. Himmelrath, 2005) zustande kommen aus Unkenntnis (im Internet stehen ja alle Produkte frei verfügbar zum Download bereit), aus fehlender Angst vor Konsequenzen (Glaube an die vermeintliche Anonymität im Internet) oder einer impliziten Etikette im Internet, die andere Normen und Werte beinhaltet (Kultur des freien Nehmens und Gebens, vgl. die Ursprünge des Internet, Helmers, Hoffmann & Hofmann, 1996), ist noch klärungsbedürftig. Das *Explizieren von Ge- und Verboten bei der Internetnutzung* stellt demnach auch einen wesentlichen Bestandteil beim gesellschaftlichen Umgang mit abweichendem und speziell kriminellem Verhalten dar.

Für strafrechtlich relevante Nutzungsweisen und das Risiko, mit solchen im Netz konfrontiert werden zu können, zu sensibilisieren, kann sowohl netzextern (als Bestandteil der Medienerziehung, über Berichte und Sendungen in anderen Medien) als auch netzintern realisiert werden. So existiert im Internet die so genannte Netiquette (Kunstwort aus engl. *net* – Netz und *etiquette* – Etikette), die ursprünglich Verhaltensempfehlungen im Usenet zusammenfasste, aber mittlerweile für alle Bereiche in Datennetzen verwendet wird, in denen Menschen miteinander kommunizieren. Obwohl sie von vielen Netzteilnehmern als sinnvoll anerkannt wird, werden Teilaspekte häufig kontrovers diskutiert. Zudem gibt keinen einheitlichen Netiquettetext, sondern eine Vielzahl von Dokumenten, die sich inhaltlich jedoch überschneiden. Sie um rechtlich relevante Aspekte zu vervollständigen, die juristische Verbindlichkeit besitzen, wäre eine von vielen Möglichkeiten, das Unrechtsbewusstsein von Netznutzern zu schärfen.

Im Falle von kriminellem Internetnutzungsverhalten sind die *Möglichkeiten der Strafverfolgung* ebenso verbesserungsbedürftig. Angesprochen ist damit der Aspekt der sekundären Prävention. Aufgrund der föderalistischen Struktur werden in Deutschland rechtliche Vergehen auf Landesebene verfolgt. So werden viele Anzeigen, z.B. wegen betrügerischen Dialern, die sich automatisch und unbemerkt auf den Computern ahnungsloser Nutzer installieren und in der Folge Kosten für bestimmte Dienste abrechnen, die unwissentlich genutzt wurden, wegen Geringfügigkeit eingestellt. Eine Bildung von Schwerpunktstaatsanwaltschaften würde andere Möglichkeiten schaffen, Internetkriminalität konsequenter strafrechtlich zu sanktionieren, was im günstigsten Fall einen Abschreckungseffekt haben könnte.

Externe Präventionsansätze können durch den *Ausbau von selbstregulativen Systemen* im Internet selbst ergänzt werden. So haben sich beispielsweise Reputationssysteme bei Online-Auktionen als effektiv erwiesen, um eine sozialverträgliche Kommunikation zu fördern und Betrugsphänomene zu minimieren (vgl. den Beitrag von S. Wehrli in diesem Band). Eine breitere Etablierung mediumimmanenter Kontrollsysteme, die die Nutzer selbst erhalten, könnten auch in anderen Nutzungszusammenhängen fruchtbare Instrumente sein. Einen Gegenpol dazu stellen Software-Produkte der Industrie dar, um Netznutzer vor kriminellen Tatbeständen (z.B. Phishing) zu schützen. Eine Reihe von *technologischen Schutzsystemen* stehen auf dem Markt zur Verfügung, doch wäre hier wünschenswert, dass die Benutzerfreundlichkeit dieser Anwendungen von Seiten der Hersteller verbessert werden bzw. nur solche Produkte auf den Markt kommen, die gewissen Qualitätskriterien entsprechen.

Insgesamt schließt der Handlungsbedarf, um zum jetzigen Zeitpunkt möglichst effektiv deviantem Verhalten im Internet zu begegnen, verschiedene Ebenen ein. Primärpräventive Maßnahmen, die netzextern (z.B. Medienerziehung), netzintern (z.B. Ausbau von selbstregulativen Systemen) oder technologisch (z.B. Verbesserung von IT-Sicherheitssoftware) orientiert sind, stehen dabei ihrerseits in einem Ergänzungsverhältnis zu sekundärpräventiven Strategien (z.B. Verbesserung der Strafverfolgung). Aktuell zielführend ist, bereits vorliegende Materialien (Curricula zur Vermittlung von Medienkompetenz), Hinweise (Netiquette) und Hilfestellungen (z.B. das Internetportal *www.klicksafe.de*) zu bündeln, um Synergieeffekte der Aktivitäten aller Institutionen, die sich im weitesten Sinne mit ‚Sicherheit im Internet' befassen, erreichen zu können. Eine Vielzahl von Initiativen und Handreichungen existieren bereits, die jedoch zum einen unverbunden, zum anderen wenig bekannt nebeneinander stehen.

III Forschungsbedarf

Ausgehend vom aktuellen Stand der wissenschaftlichen Diskussion und Forschung kann man im Bereich der sich weitgehend neu bildenden Phänomene der E-Devianz und ihrer gesellschaftlichen Genese, Definition und Prävention sehr große Forschungslücken und damit einen überdurchschnittlich großen Forschungsbedarf konstatieren.

Einzelne empirische Fragestellungen	
Grundlegende Exploration der Phänomene	▪ In welchem Ausmaß, in welchen Kontexten, aufgrund welcher Motive kommt es zu den verschiedenen Varianten devianten Verhaltens im Internet?
Exploration weniger bekannter Phänomene mit extremen psychosozialen Auswirkungen	▪ z.B. Pädophilie, Suizidforen etc.
Vergleich von virtuellem vs. realem Verhalten	▪ Wann ist das Internet Katalysator von Phänomenen, die wir kennen, oder wann ist es Generator, d.h. wann generiert es eigene strafbare Zustände? ▪ Welche Mechanismen existieren in der ‚realen Welt', die Vergehen vermeiden, und können diese auf das Internet übertragen werden? Funktionieren sie im Internet? Wenn nicht, warum nicht? ▪ Welche Unterschiede bestehen zwischen dem Interaktionsverhalten im Internet vs. dem ‚real life'? (z.B. bei sexuellen Übergriffen)
Wie kann positives Verhalten im Internet gefördert werden?	▪ Welche Möglichkeiten bestehen, z.B. prosoziales, gesundheitsförderndes Verhalten zu unterstützen?
Welche Formen von Prävention korrespondieren mit dem selbst organisierenden Charakter des Internet?	▪ z.B. freie Initiativen ▪ Belohungssysteme ▪ Reputationssysteme: In welchen Aspekten können die gängigen Reputationssysteme verbessert werden?
Sicherheit im Internet	▪ Welche Methoden zur Steigerung des Interesses der Nutzer/-innen am Thema ‚Sicherheit im Internet' sind zielführend?
Informatisierung der Netznutzer	▪ Wie erreicht man interessierte aber auch uninteressierte Netznutzer, um über Gefahren im Internet zu sensibilisieren, das Risikobewusstsein zu schärfen?
Evaluation der bereits implementierten Curricula zur Medienerziehung in der Schule	▪ Wie effektiv ist die Vermittlung von Medienkompetenz?

Metastudien
→ **Bündelung vorliegender Befunde zur Effektivität vorhandener Programme**
→ **Breitere Evaluation vorhandener Projekte, Maßnamen und Materialien**

Tab. 2: Primärer Forschungsbedarf zur Prävention von Devianz im Internet

Dieser Forschungsbedarf lässt sich zum einen aus den Vorträgen und Diskussionsbeiträgen, welche im Rahmen des internationalen DFK-Workshops am 14. und 15. Februar 2006 in Bonn präsentiert worden sind, ableiten. Man kann jedoch davon ausgehen, dass hier allenfalls ein erster Zugang zu den einschlägigen Forschungserfordernissen und Fragestellungen gesucht und gefunden worden ist, welcher sich durch weitere Forschungsfragen ergänzen lässt. Die folgenden Ausführungen wollen diese Ergänzungen aus eigener Perspektive ansatzweise versuchen und mit einbinden.

Insoweit werden zunächst einzelne Forschungsbereiche benannt, in denen besondere Forschungsdefizite verortet werden können. (A) Dabei scheint ein besonderer Schwerpunkt bei der umfassenden Prävention von E-Devianz in der durchaus nachhaltigen Entwicklung von Internet-Kompetenz für nahezu alle Netzbürgerinnen und Netzbürger zu liegen. (B) Hierbei geht es neben der Entwicklung von Inhalten vor allem auch um die Entwicklung von geeigneten Methoden, mit denen man die Inhalte möglichst frühzeitig, möglichst umfassend und möglichst nachhaltig an die Menschen heranbringen kann.[1] In einem weiteren Punkt (C) werden dann einzelne methodische Zugangswege aufgezeigt, auf denen man die vorher benannten Forschungsdefizite jeweils angehen kann.

A) Die Forschungsdefizite konzentrieren sich auf folgende Bereiche:

1. Grundlagenforschung über das Verhalten von Menschen in virtuellen Umgebungen (mit speziellem Bezug zu deviantem Verhalten und entsprechenden Deutungshintergründen). In einem besonderen Fokus sollte dabei das Verhalten von Kindern hinsichtlich der zahlreichen neuartigen Angebote und Erlebniswelten des Internet stehen.

2. Empirische Forschungen über die quantitativen Dimensionen der unterschiedlichen Phänomene der E-Devianz auf der zunächst rein deskriptiven Ebene.

[1] Dabei erscheint es lohnenswert, ein differenziertes Konzept zur gesellschaftlichen Aneignung von Internet-Kompetenz der britischen Medienwissenschaftlerin Sonia Livingstone näher in die Betrachtungen einzubeziehen.

3. Empirische Forschungen zu den unterschiedlichen (psychologischen und soziologischen) Einflussfaktoren auf die Entwicklung von abweichenden Verhaltensweisen im Netz.

4. Forschung zur Entwicklung, Vermittlung und Evaluation von ganzheitlichen, nachhaltig wirkenden Präventionskonzepten zum adäquaten Umgang mit dem Internet und anderen modernen Informations- und Kommunikationstechnologien.

5. Forschung zur Entwicklung, Vermittlung und Evaluation von speziellen Konzepten zur Medien-/Internetkompetenz als einer elementaren Fähigkeit für alle Mitglieder in der modernen Informationsgesellschaft, speziell im Bereich der Kindergärten und Schulen. Dabei beinhaltet der Begriff der ‚Medien- und Internetkompetenz' nicht nur die Fähigkeit, die einzelnen Computer und speziell die Internet-Technologie richtig handhaben zu können, sondern vor allem auch die Fähigkeit, sinnvoll mit den Inhalten des Netzes umgehen zu können.

B) Es geht bei der Schaffung und nachhaltigen Entwicklung von Internetkompetenz für möglichst alle (Netz-)Bürgerinnen und (Netz-)Bürger um folgende inhaltliche Punkte:

1. um eine möglichst realistische Einschätzung der Risiken im Internet, wobei die Risiken nicht nur die technischen, sondern vor allem auch die kommerziellen und die sozialen Risiken (problematische Kontakte und problematische Inhalte) umfassen.

2. um eine möglichst realistische Einschätzung und konsequente Nutzung der Chancen im Internet, welche man sowohl mit den Instrumenten und Mechanismen des ‚User Empowerment' als auch mit der Vermittlung von entsprechenden internetspezifischen Fähigkeiten (‚Internet Literacy') fördern und unterstützen kann.

3. um eine möglichst ausgewogene Balance zwischen ‚Gefahrenschutz und Förderung/Ausbildung' und zwischen ‚Sicherheitsgewährung und Chanceneröffnung'. Zur Erreichung dieser Balance ist die Entwicklung eines Curriculums zur grundlegenden Bildung und Förderung von ‚Internet-Kompetenz' zentral wichtig (siehe: S. Livingstone u.a.).

C) Zur Erreichung der Forschungsziele und zur Abdeckung des Forschungsbedarfs bieten sich verschiedene methodische Zugangswege an:

1 Zur Grundlagenforschung

- Hier sind vorwiegend explorative Forschungsansätze und qualitative Forschungsmethoden in dem bisher weitgehend unerforschten Bereich des devianten Kommunikationsverhaltens in virtuellen Umgebungen vorwiegend aus sozialpsychologischer Perspektive angezeigt.

- Speziell der Zugang zu den empirisch bisher überwiegend verschlossenen Bereichen der kindlichen und jugendlichen Netzkulturen und des entsprechenden Verhaltens bedarf des Einsatzes von eher qualitativen und geradezu ethnomethodologisch ausgerichteten Forschungsdesigns.

- Die vor allem in den USA, aber zunehmend auch in Europa angewandten quantitativen Erhebungen zum kindlichen und jugendlichen Internetnutzungsverhalten sind zu ergänzen durch vertiefende qualitative Studien, aber auch durch metaanalytisch und international vergleichend angelegte Forschungsprojekte.

2 Zur phänomenologischen Beschreibung und quantitativen Erfassung der verschiedenen Deliktsbereiche der E-Devianz.

- Für die meisten Phänomene der Internetdelinquenz, welche sich alle in einem hoch interessanten gesellschaftlichen Geneseprozess und zudem in einem stetigen dynamischen Entwicklungsprozess befinden, gibt es aus wissenschaftlicher Sicht bisher nur ganz wenige fundierte und umfassende empirische Untersuchungen. Dem klassischen Methodengerüst der kriminologischen Dunkelfeldforschung folgend sind hier in erster Linie möglichst repräsentative Befragungen bei der Grundgesamtheit aller Netzbürgerinnen und Netzbürger anzuzielen. Diese können sowohl als Opfer- und Täterbefragungen, als auch als Informantenbefragungen angelegt sein. Nicht nur kostenmäßig sehr reizvoll, sondern auch inhaltlich sehr adäquat und sinnvoll erscheint dabei der Einsatz internetbasierter Datenerhebungstechniken (z.B. Online-Surveys).

- Neben einer empirischen Beschreibung des zugrunde liegenden Delinquenzverhaltens interessieren den wissenschaftlichen und speziell den kriminologischen Betrachter vor allem auch jene gesellschaftlichen Reaktionen, welche das auffällige Verhalten in die Nähe oder in den Bereich des strafrechtlichen Kontrollprozesses bringen. Hierzu ist zunächst das private Anzeigeverhalten von besonderem Interesse. Speziell im Internet gibt es jedoch eine Vielzahl von behördlichen, halboffiziellen und privaten Anzeige- und Meldeportalen, deren Input bisher weitgehend wissenschaftlich noch vollkommen unerforscht ist. Insgesamt dürfte das dort vorhandene Datenmaterial (z.B. bei jugendschutz.net, Eco/Inhope u.a.) eine Fundgrube für in erster Linie quantitativen Auswertungen und Analysen darstellen.

- Weitgehend unberührt stellt sich derzeit auch (noch) die Forschungslandschaft im Bereich der einzelnen Kontrollinstanzen dar. Anders als bei den klassischen Delikten gibt es hinsichtlich der Erforschung der Kontroll- und Erledigungspraxis der einschlägigen Instanzen noch so gut wie kein systematisches empirisches Wissen. Weder im Bereich der Polizei noch im Bereich der Justiz (Staatsanwaltschaft und Gerichte) sind bisher größere empirische Untersuchungen zum Kontroll- und Erledigungsverhalten der modernen Internetdelinquenz bekannt geworden. Dabei drängen sich mittlerweile (nicht nur aus quantitativen Überlegungen) verschiedene

äußerst kontrovers und konflikthaft gehandelte digitale Massendelikte (z.B. Pirateriedelikte) für eine nähere kriminologische Analyse geradezu auf.

3 Zur empirischen Überprüfung von unterschiedlichen (externen und internen) Steuerungskonzepten in einzelnen konkreten Deliktsbereichen mit massenhaftem Vorkommen, wie z.B. bei den Piraterie-Delikten und bei den Delikten im Zusammenhang mit Online-Auktionen:

a) Piraterie-Delikte

Hier ist einerseits zu untersuchen, ob das tradierte Moralverständnis von Eigentum auf das Internet anzuwenden ist, und andererseits zu überlegen, inwieweit eine gezielte Überprüfung von konkreten Hypothesen (wie z.B. jene, die in der Theorie von Opp/Diekmann zur ‚Befolgung von Gesetzen' enthalten sind) auf den Bereich des Urheberrechts zu übertragen ist. Dabei ließen sich dann auch mögliche Einflüsse der klassischen kriminalpolitischen Ansätze der positiven und der negativen Generalprävention (also von Unrechtsbewusstseinsbildung und von Abschreckung/ Strafandrohung) und auch von alternativen (Verkaufs- und Konsum-)Angeboten näher analysieren.

b) Online-Auktions-Delikte

Hier ist zu untersuchen, welche Formen von Prävention mit dem selbst organisierenden Charakter des Internet besser korrespondieren. Dabei kann an der bereits praktizierten Forschung zur Wirkung von bestehenden Reputationssystemen angeknüpft werden und es können mögliche Verbesserungsmaßnahmen implementiert und empirisch überprüft werden. Auch die Wirkung von verschiedenen freien Initiativen und von Belohnungssystemen gilt es näher zu untersuchen. Hier scheint auch ein besonderes Anwendungsgebiet von experimentellen Studien zu liegen. Zudem erscheint es für den Empiriker sehr verlockend, in diesem Bereich offensichtlich auf eine Vielzahl von relativ komfortabel analysierbaren Daten in digitalisierter Form zugreifen zu können.

4 Zur empirischen Überprüfung von (a) unterschiedlichen Präventionskonzepten und von (b) unterschiedlichen Angeboten zur Vermittlung von Internetkompetenz.

- (a) In der aktuellen Diskussion lassen sich vor allem zwei unterschiedliche Präventionskonzepte ausfindig machen, die auf zwei unterschiedliche Erklärungsansätze von E-Devianz zurückzuführen sind. Im ersten Fall stehen die vorwiegend technologisch zu sehenden Gelegenheitsstrukturen im Mittelpunkt, an denen es anzusetzen gilt. Im zweiten Fall steht vor allem der Mensch und sein Verhalten im Zentrum der Erklärung und des präventiven Vorgehens. Es gilt empirisch zu untersuchen, welcher Hebel in welcher Situation und gegebenenfalls in welcher Mischung bessere Präventionswirkungen entfalten kann. Das könnte beispielhaft im Vergleich zu Präventionsansätzen im Bereich des Autoverkehrs geschehen (Autoverkehr – Datenverkehr).

- (b) Ausgehend von der These, dass bestehende Angebote zur Vermittlung von Internetkompetenz nicht die Nutzungspräferenzen der unterschiedlichen Bevölkerungsgruppen berücksichtigen, sondern vielfach aus der Sicht der Anbieter und deren Vorstellungen über das Nutzungsverhalten gestaltet werden, gilt es in erster Linie, alternative, eher an den Nutzern orientierte Konzepte zu entwickeln und diese auf ihre Wirksamkeit und Effizienz hin empirisch zu überprüfen.

5 Zur Evaluation von bereits implementierten Curricula zur Medienerziehung in der Schule.

Hier gilt es zu untersuchen, wie effektiv die bereits praktizierte Vermittlung von Medienkompetenz speziell in der Schule ist, welche unterschiedlichen Ansätze und Probleme hier vorhanden sind und welche Alternativen sich anbieten. Dabei ist neben den Inhalten vor allem auch auf die möglichst umfängliche und vollständige Erreichbarkeit der Adressaten zu achten. Das beste Konzept bewirkt wenig, wenn es seine Adressaten nicht erreicht. Hier ist notwendiger Weise auch die Ausbildung der Ausbilder in die Planungen einzubeziehen.

IV Ausblick

Angesichts der beschriebenen Handlungs- und Forschungsdefizite erscheint es an der Zeit, dass sich die Gesellschaft und ihre einschlägigen (Forschungs-)Instanzen dieser immer dringlicher werdenden Thematik verstärkt annehmen. Das Internet und die dort stattfindende Kommunikation werden zu einem immer bedeutenderen und umfassenderen Bestandteil unserer modernen Gesellschaft. Alle Verantwortlichen werden sich von daher in Zukunft noch intensiver um einen möglichst engagierten Umgang mit den riesigen Chancen, aber auch um einen möglichst reflektierten Umgang mit den bestehenden Risiken der modernen Internetkommunikation zu befassen haben.

Literatur

Caplan, G., Principles of preventive psychiatry. New York 1964 (Basic Books)

Diekmann, A., Die Befolgung von Gesetzen. Empirische Untersuchungen zu einer rechtssoziologischen Theorie. Berlin 1980

Helmers, S., Hoffmann, U. & Hofmann, J. Netzkultur und Netzwerkorganisation. Das Projekt ‚Interaktionsraum Internet'. Discussion Paper FS II 96-103. Wissenschaftszentrum Berlin. 1996 [Online Dokument]. URL *http://duplox.wz-berlin.de/texte/dp103/* [29.04.2006]

Himmelrath, A., Pfusch bei Hausarbeiten. Uni droht mit 50.000 Euro Strafe. Spiegel Online vom 06.10.2005. [Online Dokument]. URL *www.spiegel.de/unispiegel/studium/0,1518,378304,00.html* [29.04.2006]

Livingstone, S., User empowerment and media competence: Combining protection and education. In: European Forum on Harmful and Illegal Cyber Content: Self-Regulation, User Protection and Media Competence. Council of Europe, Strasbourg 2001

Livingstone, S., Children´s use of the internet: reflections on the emerging research agenda. In: new media & society, Heft 2/2003, S. 147-166

Livingstone, S., Media Literacy and the Challenge of New Information and Communication Technologies. In: Communication Review 7, 1/2004, S. 3-14. URL *www.lse.ac.uk/collections/media@lse/whosWho/soniaLivingstone.htm*

Rüther, W., Delinquenz-Phänomene im Internet. Kriminologische Ansätze zu ihrer Definition und zu ihrer quantitativen Erfassung. In: Cimichella, Sandro u.a., Hrsg., Neue Technologien und Kriminalität: Neue Kriminologie? Zürich 2006 (Ruegger-Verlag