Zeitschrift: Reihe Kriminologie / Schweizerische Arbeitsgruppe für Kriminologie = Collection criminologie / Groupe suisse de travail de criminologie

Herausgeber: Schweizerische Arbeitsgruppe für Kriminologie

Band: 24 (2006)

Artikel: Phänomene der Internetdelinquenz : Ansätze, Probleme und Erkenntnisse zu ihrer gesellschaftlichen Definition und zu ihrer quantitativen Erfassung

Autor: Rüther, Werner

DOI: https://doi.org/10.5169/seals-1051074

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 17.07.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

WERNER RÜTHER

PHÄNOMENE DER INTERNETDELINQUENZ – ANSÄTZE, PROBLEME UND ERKENNTNISSE ZU IHRER GESELLSCHAFTLICHEN DEFINITION UND ZU IHRER QUANTITATIVEN ERFASSUNG[1]

«Das Netz ist wie ein Blatt Papier. Es ist nichts als ein weiteres Werkzeug für die Kommunikation und kann als solches genutzt und auch missbraucht werden.»
VINT CERF, Miterfinder der grundlegenden Netzwerkprotokolle TCP/IP und Vorsitzender der globalen Internet-Verwaltung ICANN

Zusammenfassung
Phänomene der Internetdelinquenz 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. Die neuen digitalen gesellschaftlichen Strukturen liefern ihre Abweichungsphänomene sozusagen automatisch mit. Abweichung und Delinquenz in der globalen Internetgesellschaft sind von daher als gesellschaftliche Phänomene genauso normal wie Abweichung und Delinquenz in jedem anderen gesellschaftlichen System. Interessant erscheinen in diesem Zusammenhang Parallelen zum automobilen Verkehrssystem, welches im letzten Jahrhundert die Gesellschaft(en) verändert hat und ebenfalls durch neuartige technologische Entwicklungen hervorgerufen worden ist. Der Autoverkehr hat allerdings deutlich höhere Risiken für Leib und Leben mit sich gebracht als das aktuell der wachsende Datenverkehr des Internet erkennen lässt. Die alltäglichen Risiken des Internet beziehen sich in erster Linie auf materielle Eigentums- und Vermögensschädigungen.
Ihre einzelnen Ausprägungen und ihre quantitativen Grössenordnungen sind hingegen für den gewohnten kriminologischen Betrachter aus verschiedenen Gründen noch komplexer, unklarer, undefinierter und unzugänglicher als dies schon bei Abweichungsphänomenen in «realen» Gesellschaften der Fall ist. Die vielfach vorhandenen Ansätze zur phänomenologischen Beschreibung und Quantifizierung sind besonders zum gegenwärtigen, relativ frühen Zeitpunkt des globalen Geneseprozesses als ein durch vielfältige und unterschiedliche Interessen bestimmtes Kon-

1 Überarbeitete Fassung meines Vortrags auf der Tagung der Schweizerischen Arbeitsgruppe für Kriminologie (SAK) «Neue Technologien und Kriminalität: Neue Kriminologie?» vom 8.–10. März 2006 in Interlaken.

strukt zu sehen. Insoweit lassen sich diese Prozesse durchaus angemessen aus der auch kriminologisch etablierten Perspektive des sozialen Konstruktivismus analysieren. Es bedarf also keiner grundsätzlich neuen Kriminologie, sondern eher einer Erweiterung ihrer Methoden und einer Globalisierung ihrer Perspektiven. Um in Zukunft einen möglichst rationalen und reflektierten Umgang mit der Thematik der Internetdelinquenz erreichen zu können, sind zunächst einmal einige moderne, für die digitale und globale Phänomenologie passende methodische Zugänge zu suchen und zu etablieren.Besonders vielversprechend erscheint mittelfristig ein «Global Online Survey».

Résumé

Le phénomène de la délinquance liée à Internet – provenance et problèmes de définition et de relevé quantitatif

Le phénomène de la délinquance liée à Internet est logiquement né d'Internet et des nouveautés technologiques sous-jacentes à la «révolution digitale». Il est l'expression du changement radical, intervenu ces dix à quinze dernières années, passant de structures occasionnelles à une communication universelle. Les nouvelles structures digitales de la société créent ainsi leur propre déviance. Dans la société globale d'Internet, la déviance et la délinquance sont des phénomènes de société aussi normaux que la déviance et la délinquance dans n'importe quel autre système social. Dans ce contexte, un parallèle avec le trafic automobile semble intéressant; ce dernier, né au travers des développements des nouvelles technologies, a en effet modifié la (les) société(s) au cours du siècle passé. Le trafic automobile a toutefois créé des risques sensiblement plus importants pour l'intégrité corporelle que la croissance du trafic de données sur Internet. Les risques quotidiens engendrés par Internet consistent en premier lieu en des dommages matériels à la propriété et en des dommages patrimoniaux.

En revanche, leur dénombrement est encore plus complexe, moins clair, moins bien défini et moins accessible pour les criminologues avertis que ce n'est le cas pour les phénomènes de déviance dans la société «réelle». La multitude d'approches tendant à la description et à la quantification de ces phénomènes doit être perçue, en cette période relativement proche de la genèse du processus global, comme un modèle déterminé par des intérêts multiples et différents. Sur ce point, ce processus s'analyse au regard des perspectives criminologiques du constructivisme social. Cela ne nécessite donc pas une criminologie fondamentalement nouvelle, mais plutôt un élargissement de ses méthodes et une globalisation de ses perspectives. Pour parvenir, dans l'avenir, à une mise en oeuvre la plus rationnelle et réfléchie possible du thème de la délinquance liée à Internet, il est nécessaire de chercher et d'établir en premier lieu certains accès méthodologiques modernes adaptés à une phénoménologie digitale et globale. A moyen terme, un «Global Online Survey» semble particulièrement prometteur.

1 Kriminologische Einführung unter konstruktivistischer Perspektive

Die Aufgabe, einen kriminologischen Vortrag zu halten, welcher die Fragestellung nach Umfang und Entwicklung der modernen «Kriminalität begangen mittels neuer Technologien»[2] behandeln soll, gleicht in vielerlei Hinsicht dem Ansinnen, eine Vielzahl von sich ständig bewegenden Bällen und mehr oder weniger aufgeblasenen Ballons in einem riesigen Gefäss festhalten und (be)greifen zu wollen.[3] Um im Bild zu bleiben: diese Ballons sind angesichts der vorhandenen technologischen Dynamik und der mannigfachen gesellschaftlichen Interessen, welche sie in Bewegung halten und mit unterschiedlicher Luft versorgen, nicht ganz so einfach und problemlos zu fixieren und zu begreifen.

Dabei fallen zunächst einmal jene relativ dicken und knalligen Ballons ins Auge, die alle von einem sehr steilen und rasanten Anstieg jener neuen Formen von Kriminalität künden, welche mit dem Internet zusammenhängen. So positiv und dynamisch sich das Internet einerseits entwickelt, so dynamisch entwickeln sich auf der anderen Seite auch die zahlreichen Meldungen und Berichte über immer wieder neue Phänomene und über ständig steigende Zahlen der «Internetdelinquenz» (bzw. der «Internet-Kriminalität» oder auch der «Cybercrimes»). An einzelnen quantifizierenden Beschreibungsansätzen besteht jedenfalls in der aktuellen Situation kein Mangel. Allerdings stammen diese weniger aus den Reihen der Wissenschaft und ganz selten aus den Reihen der Kriminologie, sondern vor allem aus den Reihen ganz unterschiedlich betroffener und beteiligter Organisationen, Gruppen und Unternehmen. Ihre mehr oder weni-

2 So die Formulierung in der ersten schriftlichen Anfrage und Einladung zu einem Vortrag durch MARCEL ALEXANDER NIGGLI vom Sommer vergangenen Jahres 2005.

3 In Anlehnung an den Satz von STEVEN FURNELL im Vorwort seines Buches *Cybercrime. Vandalizing the Information Society.* Boston 2002, S.IX: «It must be observed that trying to write a book about cybercrime is very much like trying to hit a moving target.»

ger differenzierten Datensammlungen sind häufig auch im Internet in vielfältigen Variationen zugänglich.[4]

Ich sehe meine jetzige Aufgabe als wissenschaftlicher Betrachter nun in erster Linie nicht darin, diesen Variationen eine weitere hinzuzufügen, sondern die bisherigen zu sichten und kritisch auf ihren gesellschaftlichen Herstellungsprozess hin zu hinterfragen. Dabei ist ein solches Unterfangen für die neuere Kriminologie seit der Entdeckung des sogenannten Definitionsansatzes vor nun schon über 30 Jahren eigentlich nichts Besonderes, sondern mehr oder weniger eine Selbstverständlichkeit.[5] Die Perspektive des sozialen Konstruktivismus[6] erscheint speziell bei sich ganz neu entwickelnden gesellschaftlichen Abweichungs- und Kriminalitätsphänomenen wie der hier zu analysierenden «Internetdelinquenz» als eine besonders angemessene Perspektive. Es handelt sich somit um einen aktuellen Anwendungsfall für den relativ neuen, aber nun schon weitgehend etablierten Definitionsansatz in der Kriminologie. Es bedarf vor diesem Hintergrund keiner grundsätzlich «neuen Kriminologie», wie sie in der Fragestellung zum Gesamtthema dieser Tagung anklingt, sondern eher einer Erweiterung ihrer Methoden und einer Globalisierung ihrer Perspektiven.

2 Die Auswirkungen der «Digitalen Revolution» auf die gesellschaftliche Kommunikation und das entsprechende Delinquenz-Verhalten.

Während der kriminologische Definitionsansatz und die Schlachten, welche speziell in der Bundesrepublik Deutschland um ihn geschla-

4 Hilfestellungen bei der einschlägigen Informationssuche sind zu finden unter: http://www.cyber-crime.info.

5 Es ist in dieser frühen Genesephase eines neuartigen Phänomens, welches durch zahlreiche mehr oder weniger aufgeblasene Ballons abgebildet wird, zunächst einmal wichtiger zu analysieren, wer, wie und warum die Ballons aufbläst, als die präsentierte Grösse und Beschaffenheit der Ballons unhinterfragt zum alleinigen Gegenstand der wiss. Analyse zu machen.

6 Siehe hierzu: HESS, HENNER / SCHEERER, SEBASTIAN, Was ist Kriminalität? Skizze einer konstruktivistischen Kriminalitätstheorie. In: *Kriminologisches Journal,* Jg. 29, Nr. 2/1997, S. 83–155.

gen worden sind,[7] eher schon etwas Historisches an sich haben, sind die Phänomene der Internetdelinquenz, welche es hier und heute anhand dieses Definitionsansatzes zu analysieren gilt, noch relativ jung an Jahren. Sie befinden sich allenfalls im zarten Alter von «Teenagern». Diese jungen gesellschaftlichen Phänomene sind nur vor dem Hintergrund jener äusserst dynamischen, technologischen Entwicklungen zu verstehen, welche man auch mit dem Begriff der «digitalen Revolution» kennzeichnet. Deren historische Wurzeln sind mit der Entdeckung des auf digitale Technologie basierenden Computers in der Mitte des vorigen Jahrhunderts anzusiedeln. Die besonders merklichen Veränderungen in den Vernetzungsmöglichkeiten der einzelnen Computer untereinander und die Auswirkungen dieser speziellen Technologien auf die gesamte gesellschaftliche Kommunikation liegen im Jahr 2006 jedoch erst gut 12 Jahre zurück.

2.1 Die Entwicklung des Internets zu einem interaktiven Massenmedium und die Entstehung einer neuen globalen Gesellschaft

Mit den bahnbrechenden Erfindungen des «WorldWideWeb» (WWW und der grundlegenden Hypertext-Sprache HTML) durch TIM BERNERS-LEE (am CERN in Genf) und der so genannten Browser-Technologie (MOSAIC und NETSCAPE) durch MARC ANDREESEN (vom NCSA der University of Illinois) zu Beginn der 90er-Jahre stand auf einmal eine anwenderfreundliche Technik zur Verfügung, welche nun die breite Nutzung der global vernetzten Internet-Kommunikation ermöglichte.[8] Das Internet wandelte sich von einer elitären Kommunikationsplattform zu einem interaktiven Massenmedium. Anders als die klassischen Massenmedien zeichnet sich das

7 Zusammenfassend hierzu: RÜTHER, WERNER, *Abweichendes Verhalten und labeling approach,* Köln u.a. 1975.

8 Der Webbrowser wird deswegen auch als «Killerapplikation» des Internet bezeichnet. Als «Killerapplikation» gilt eine konkrete Anwendung, die einer neuen Technologie zum Durchbruch verhilft. Siehe unter: http://de.wikipedia.org/wiki/Killerapplikation.

Internet dadurch besonders aus, dass es neben Millionen von Empfängern auch Millionen von mehr oder weniger aktiven Sendern gibt. Dies macht seine *besondere Interaktivität als Massenmedium* aus. Soziologisch betrachtet[9] konstituiert sich jede Gesellschaft durch Kommunikation und Interaktion. Man kann so die Konstituierung und Etablierung einer vollkommen neuartigen, globalen Gesellschaft nachvollziehen, in welcher neue Qualitäten und besonders auch neue Quantitäten von menschlichen Verhaltensweisen und sozialen Interaktionen möglich und real geworden sind. In den ersten beiden Jahren nach Einführung der Internet-Browser-Technologie stieg die Zahl der Internetnutzer in aller Welt von bis dato wenigen Tausend rasant an und sie erreichte allein in Deutschland schon sehr bald die Millionengrenze.[10] Im Jahr 1995 wurden weltweit bereits 25 Millionen Internetnutzer gezählt.

Drei Jahre später (1998) wurde die 100-Millionen-Grenze durchbrochen; die halbe Milliarde ist im Jahr 2001 erreicht worden und zu Beginn dieses Jahres 2006 wurde eine Meldung verbreitet, dass im Laufe des Jahres 2005 die globale Schar aller Internetnutzer auf über 1 000 000 000 Menschen angestiegen ist.[11] Das sind nun bereits mehr als 15% aller Erdbewohner, welche durch das Internet direkt miteinander verbunden sind und somit eine neue Form von Weltgesellschaft (in einer Art globalem Dorf) mit weiter zunehmender Grösse bilden.[12] Auf dem 2. UN-Weltgipfel zur Informationsgesellschaft (WSIS) in Tunis im November 2005 ist u. a. beschlossen worden,[13] dass in Zukunft ein Kern von IT-Nutzungsdaten regelmässig und zentral für alle UN-Mitgliedsstaaten erhoben und zusammenge-

9 So z.B. Niklas Luhmann, *Die Gesellschaft der Gesellschaft,* Frankfurt 1997.

10 Aus kriminologischer Sicht besitzt das Internet nicht nur Millionen von potentiellen Opfern, sondern gleichzeitig auch Millionen von potentiellen Tätern.

11 «The number of Internet users surpassed 1 billion in 2005 … The 2 billion Internet users milestone is expected in 2011.» Quelle: http://www.etforecasts.com/pr/pr1o6.htm (vom 3.1.2006).

12 Ein weiterer Indikator für die rasante Entwicklung des Internet wird vom Internet Systems Consortium (ISC) veröffentlicht. Hier wird im Rahmen des ISC-Domain-Survey die Anzahl aller Rechner (Hosts) im weltweiten Netz gemessen. Nach 200 Rechnern im Jahr 1981 über 6,6 Mio im Jahr 1995 wurden danach im Jahr 2005 insgesamt bereits 318 Mio Rechner gezählt. Siehe hierzu: http://www.isc.org/index.pl?/ops/ds/host-count-history.php.

13 Quelle: http://www.itu.int/wsis/docs2/pc2/plenary (vom 15.1.2006).

stellt werden soll, sodass man dann ein relativ umfassendes Bild über die quantitative Nutzungstruktur des gesamten Internet auf Dauer zur Verfügung haben wird.[14] Dabei werden speziell die besonderen Fragen und Probleme der ungleichen Zugangschancen zum Netz (Problematik des «Digital Divide») eine besondere Rolle spielen.

2.2 Zur «Normalität» der Entwicklung von Delinquenz-Phänomenen im Internet.

Die Schaffung und Entwicklung des Netzes ist nach einem seiner Entdecker und Entwickler VINT CERF[15] nichts anderes als die Schaffung und Entwicklung eines weiteren Werkzeugs zur Kommunikation wie es auch ein Stück Papier darstellt; genauso wie ein solches Stück Papier kann man auch dieses Kommunikations-Werkzeug entweder positiv nutzen oder auch für abweichende, kriminelle Zwecke missbrauchen.[16]

Insoweit sind Abweichungs-Phänomene im Internet, wie man sie auch immer bezeichnen mag, zunächst einmal vollkommen selbstverständlich und «normal». Der Kriminalsoziologe HANS HAFER-

14 Derzeit kann man hinsichtlich der Internetnutzungsdaten auch schon auf ein relativ breites Angebot von jeweils nationalen Daten in zahlreichen Länder (so auch in der BRD) zurückgreifen. Nach den neuesten Zahlen der Forschungsgruppe Wahlen, welche vierteljährlich eine repräsentative telefonische Umfrage bei der deutschen Bevölkerung (ab 18 Jahren) zur Ermittlung von Internet-Strukturdaten durchführt, verfügten im 4.Quartal 2005 bereits nahezu zwei Drittel (65%) aller deutschen Erwachsenen über einen Internetzugang. Bei der ersten derartigen Erhebung im 4.Quartal 1999 waren kaum mehr als ein Zehntel (ca. 12%) an das Internet angeschlossen. In dieser kurzen Zeit von sechs Jahren sind die Internetnutzer in unserer Gesellschaft von einer kleinen Minderheit zu einer eindrucksvollen Zwei-Drittel-Mehrheit herangewachsen. Dabei sind die Nutzerquoten höchst unterschiedlich bei den einzelnen gesellschaftlichen Gruppen, was auch unter dem Aspekt des «digital divide» problematisert wird. Die höchsten Quoten von über 80% befinden sich bei den jungen Leuten (unter 30 Jahren) und bei denen mit Hochschulabschluss. Die älteren Jahrgänge (ab 60) sind erst zu 30% an das Internet angeschlossen; bei den Hauptschülern (ohne Lehre) liegt die Quote nur bei 17%. Weitere Ergebnisse finden sich unter: http://www.forschungsgruppe.de.

15 Siehe das Zitat des «Internet-Gurus» VINT CERF auf der Titelseite dieses Beitrages.

16 Als eine weitere Grundform schädigender, delinquenter Handlungen im Internet gilt es solche Aktivitäten abzuschichten, bei denen das Kommunikations-Werkzeug Internet selbst zum Ziel der Handlungen wird.

KAMP[17] hat in den 70er-Jahren des vorigen Jahrhunderts (in Bezug auf den französischen Soziologie-Klassiker EMILE DURKHEIM) die hier und da als verwunderlich aufgenommene, aber eigentlich selbstverständliche Botschaft nochmals hervorgehoben: «Kriminalität ist normal». Es bedeutet ja nichts anderes als zu sagen, dass jede Gesellschaft, welche durch soziale Normen und Regeln gekennzeichnet ist, automatisch auch die Abweichung von diesen Regeln und Normen mitliefert. Abweichung ist die folgerichtige und logische Konsequenz jeder Norm; Kriminalität ist die logische Konsequenz jeder Strafrechtsnorm. Das Internet kann zwar als ein neuartiger Kommunikationsraum angesehen werden, in dem sich u.a. auch neue Normen und Regeln bilden. Es kann aber nicht als vollkommen normenloser und rechtsfreier Raum begriffen werden,[18] in dem sozusagen anarchische Zustände herrschen und mehr oder weniger alles möglich ist und ohne jede rechtliche Konsequenzen bleibt. Die bestehenden, zum Teil übernommenen und die zum Teil sich entwickelnden (Rechts-)Normen konstituieren wie selbstverständlich Normabweichungen im Internet und somit das Phänomen der «Internet-Abweichungen».

Interessant erscheinen in diesem Zusammenhang Parallelen zur Entwicklung des Autoverkehrs, welcher im letzten Jahrhundert die Gesellschaft(en) massiv verändert hat und ebenfalls durch neuartige technologische Entwicklungen hervorgerufen worden ist.[19] Der Autoverkehr hat allerdings deutlich höhere Risiken für Leib und Leben mit sich gebracht als das aktuell der wachsende Datenverkehr des Internet erkennen lässt. Die alltäglichen Risiken des Inter-

17 HAFERKAMP, HANS, *Kriminalität ist normal. Zur gesellschaftlichen Produktion abweichenden Verhaltens.* Stuttgart 1972.

18 Siehe hierzu auch: NIGGLI, MARCEL ALEXANDER / SCHWARZENEGGER, CHRISTIAN, *Internet – ein rechtsfreier Raum?* in: CASSANI, URSULA, u.a., Hrsg., *Medien, Kriminalität und Justiz*. Reihe Kriminologie, Band 19, 2001, S. 303–329.

19 Die Genese neuer Delinquenzphänomene und Kriminalitätstrends lässt sich nach KILLIAS in der Regel durch das Auftreten so genannter «Brüche» (breaches) erklären; das sind relativ plötzlich auftauchende neue Gelegenheitsstrukturen in Folge von technologischen Entwicklungen. Siehe hierzu: KILLIAS, MARTIN, The Opening and Closing of Breaches. A Theory on Crime Waves, Law Creation and Crime Prevention. In: *European Journal of Criminology,* Heft 1/2006, S. 11–31.

net beziehen sich in erster Linie auf materielle Eigentums- und Vermögensschädigungen. Diese unterliegen hinsichtlich ihrer sozialen und welt-gesellschaftlichen normativen Abgrenzungen und Definitionen einer besonders ausgeprägten Variabilität. Da das Internet weltweit und sozusagen grenzenlos funktioniert, die rechtlichen und vor allem die strafrechtlichen Normen traditionell noch überwiegend auf die nationalen Räume bezogen und somit relativ begrenzt sind, ergeben sich besondere Definitions-, Abgrenzungs- und Verfolgungsprobleme.[20] Der sich entwickelnde Prozess der (welt-)gesellschaftlichen Definition von Internet-Kriminalität ist und bleibt ein besonders interessanter Gegenstand für kriminologische Fragestellungen und Analysen in der Tradition des «labeling approach» oder des sozialen Konstruktivismus.

Angesichts der rasanten Zunahme der Internetnutzung ist ein zu erwartender und sehr wahrscheinlicher Anstieg der Internetdelinquenz nicht *per se* als problematisch anzusehen, sondern vor allem ein solcher Anstieg, welcher im direkten quantitativen Vergleich zum Anstieg der Internutzung deutlich erhöht wäre. Da das empirisch gesicherte Wissen von Seiten der Wissenschaften über die Quantitäten des delinquenten Verhaltens im Internet derzeit als äusserst spärlich, selektiv und defizitär anzusehen ist,[21] bestehen durchaus gewisse Risiken von Überzeichnungstendenzen, die durch spezielle gesellschaftliche Interessen gefördert werden.

2.3 Zur Dramatisierungsgefahr von Delinquenz-Phänomenen im Internet

Sowohl in der Weltgesellschaft in Form der globalen Internet-Community, wie sie sich z.B. auf dem «World Summit on Information

20 Weil weltweit (noch) kein einheitlicher strafrechtlicher Definitionsrahmen zur Verfügung steht, bietet es sich an, in der global (noch) relativ offenen Definitionslage nicht von «globaler Internet-Kriminalität», sondern besser von «globaler Internetdelinquenz» zu sprechen.

21 Siehe dazu u.a.: MOITRA, SOUMYIO D., *Analysis and Modelling of Cybercrime: Prospects and Potential.* MPI-Veröffentlicheung, Freiburg 2003, http://www.iuscrim.mpg.de/verlag/Forschaktuell/FA-Moitra 03. pdf.

Society» (WSIS) zu artikulieren versucht hat,[22] als auch und besonders in zahlreichen einzelnen nationalen Gesellschaften (wie z. B. in der Bundesrepublik Deutschland, der Schweiz oder auch in Übersee) sind eher Überzeichnungs- als Unterbelichtungstendenzen erkennbar. Die dahinter stehenden (der oben beschriebenen «Normalität» nicht angemessenen) Dramatisierungs-Initiativen sind wiederum ein durchaus bekanntes Phänomen bei sich neu bildenden gesellschaftlichen Problemen. Hierzu gibt es aus der Soziologie sozialer Probleme und speziell auch aus der kriminalsoziologischen Forschung der letzten Jahre und Jahrzehnte genügend interessante und gut belegte Beispiele.[23]

2.3.1 Wirtschaftliche Interessengruppen

Bei neu auftauchenden gesellschaftlichen Problemen, wie sie jetzt die Phänomene der Internetdelinquenz darstellen, machen sich stets auch verschiedene gesellschaftliche Interessengruppen bemerkbar,[24] welche weniger an einer möglichst sachlichen Beschreibung der Lage, sondern viel mehr an einer Überzeichnung und Dramatisierung interessiert sind. Angesichts der modernen Errungenschaften der digitalen Computer-Technologie sind quantitative Daten über alle möglichen Delinquenz-Ereignisse relativ schnell, einfach und kostengünstig durch interessierte Firmen und Betriebe zu erheben. Dies sind zum einen spezielle, globale Anbieter von Sicherheitssoftware wie *Symantec, McAfee, Websense Security Labs und Kaspersky Lab* und zum anderen grosse, weltweit operierende Wirtschaftsberatungsunternehmen wie KMPG und PWC.

---

22 Die Probleme der abweichenden, delinquenten und kriminellen Nutzungsmöglichkeiten des Internet sind auf beiden bisherigen UN-Gipfeln zwar ebenfalls Thema der Verhandlungen gewesen, aber selbst von ersten ansatzweisen quantitativen Beschreibungen der Phänomene, die man supranational gern mit dem Begriff «cybercrimes» erfasst, ist man derzeit auf UN-Ebene noch meilenweit entfernt.

23 Z.B. bei: ALBRECHT, GÜNTER, Konstruktion von Realität und Realität von Konstruktionen. In: *Soziale Probleme*, Jg. 12/2001, Nr. 1/2, S. 116–145.

24 Aus Australien gibt es hierzu einen interessanten kriminologischen Beitrag von: SMITH, RUSSEL G., *Internet-Related Fraud: Crisis or Beat-Up?* Paper presented at the 4. National Outlook Symposium on Crime in Australia, Canberra 2001.

Dabei gehen die grössten Aktivitäten von jenen Unternehmen aus, welche im besonderen Masse verschiedene Produkte aus dem Bereich der Sicherheitstechnologien (speziell Virenschutz-Software, Firewalls etc.) anbieten und verkaufen wollen. Sie haben wie selbstverständlich ein besonderes Interesse an einer möglichst deutlichen Akzentuierung und Hervorhebung der verschiedenen Gefahrenlagen im Netz. So wird über die drohenden Schädigungen und Delikte in der Internet-Kommunikation in Form von so genannten Bedrohungs-Reports (z.B. «Internet-Security-Threat-Report») regelmässig und ausführlich berichtet. Das Bedürfnis und die Nachfrage bei den Netzbürgern nach den angebotenen Sicherheitsprodukten soll dadurch geweckt und gesteigert werden.

Beispielhaft hervorgehoben seien hier nur die Studien und die Berichte des globalen Sicherheitsanbieters Kaspersky Labs. Der auch als «russischer Antiviren-Guru» bezeichnete EUGENE KASPERSKY, Chef der Firma Kaspersky Labs, wendet sich stets vehement gegen Meldungen und Behauptungen, welche sinkende Schadenssummen bei der Internetdelinquenz angeben. Er ist sich sicher, dass die wirtschaftlichen Schäden durch «cybercrimes» real immer weiter zunehmen. Die Schadensdelikte würden möglicher Weise in Zukunft indirekter und unsichtbarer, sie seien deshalb aber nicht weniger gefährlich;[25] im Gegenteil: die Lage erfordere immer mehr Sicherheitstechnik und Sicherheitskompetenz, die nur solche Sicherheitsfirmen wie die seine bieten und vermitteln können.

Eine nicht ganz so offensichtliche Interessen-Orientierung wie bei den Software-Anbietern für Sicherheitstechnologie ist auf den ersten Blick bei den globalen Wirtschaftsberatungs-Unternehmen wie *KPMG und PWC* vorhanden. Diese führen regelmässig weltweite Befragungen bei grösseren und kleineren Wirtschaftsunternehmen durch, um deren Betroffenheiten von potentiellen Schädigungen in der Internet-Kommunikation zu beschreiben und um diese Kunden

25 Quelle: http://silicon.de/cpo/_cfg/print.php?nr=26248.

verstärkt über die Sicherheitsproblematik und die Sicherheitsanforderungen im Internet zu sensibilisieren und zu informieren. Digitale Sicherheitsdienstleistungen und das Erstellen von entsprechenden Sicherheitsprofilen sind offensichtlich ein wesentlicher Bestandteil der modernen Aufgaben und Anforderungen in der Unternehmensberatung des digitalen Zeitalters.

Eine ganz besondere Interessenlage zeichnet sich bei der «Business Software Alliance» (BSA) ab, welche alljährlich den globalen «Software-Piraterie-Report» veröffentlicht , um speziell die besonders hohen Schadenssummen der angeschlossenen Software-Unternehmen demonstrieren zu können. Ein zentrales unternehmerisches Ziel dabei ist sicherlich, der Öffentlichkeit vor Augen zu führen, wie wichtig im Interesse einer gesunden, prosperierenden Wirtschaft und damit auch im Interesse der Allgemeinheit weitere gezielte und globale Massnahmen zur Einschränkung der Software-Piraterie sind.

2.3.2 Skandalisierungsinteressen einzelner Medien

Eine weitere Interessengruppe an möglichst aufrüttelnden und skandalisierenden Darstellungen von Delinquenz- und Kriminalitätsfällen findet sich traditionell in den Reihen der klassischen *Medien*. Aus der bisherigen kriminologischen Forschung zu den objektiven und subjektiven Sicherheitslagen in der Bevölkerung, speziell auch in der Kommune, gibt es einen bekannten und viel diskutierten Zusammenhang zwischen der vorwiegend auf Dramatisierung ausgerichteten Kriminalberichterstattung der Massenmedien und einem relativ grossen Unsicherheitsgefühl zahlreicher Bürgerinnen und Bürger.[27] Eine derartige Berichterstattung tendiert dazu, eine mög-

26 Die Ermittlung der quantitativen Daten geschieht dabei in erster Linie über einen rein rechnerischen Vergleich der Summen der verkauften Hardware mit den Summen der verkauften Software. Überproportionale Differenzen werden auf Piraterie-Aktivitäten zurückgeführt.

27 Siehe hierzu u.a.: RÜTHER, WERNER, *Kommunale Kriminalitätsanalyse. Auswertung offizieller Kriminalitätsdaten und einer Bürgerbefragung zum Sicherheitsgefühl in der Kommune.* Kassel 2005.

lichst rationale Kriminal- und Sicherheitspolitik in vielen Bereichen der Gesellschaft eher zu behindern als zu fördern.[28] Der Motor und die innere Logik dieser auf Skandalisierung und Emotionalisierung angelegten Berichterstattung findet sich in der starken Abhängigkeit der klassischen Medien (vor allem der Boulevard-Presse und der privaten TV-Anstalten) von den jeweiligen Verkaufszahlen und den entsprechenden Einschaltquoten.

Zahlreiche Akteure aus dem Bereich der *modernen Online-Medien* und speziellen Online-Plattformen (wie z.B. Telepolis) sind derzeit offensichtlich (noch) ökonomisch unabhängiger strukturiert und im Sinne der Nutzer eher aktivierend orientiert. Sie sehen sich als Mitglieder einer (netz)bürgerfreundlichen, partizipatorischen und weitgehend selbstbestimmten Netzkultur. Sie sind von daher systematisch eher in der Lage, möglichst rational, hintergründig und differenziert auch über Sicherheitsprobleme und Delinquenzphänomene im Netz zu berichten.

Dies mag beispielhaft an eigenen Erfahrungen demonstriert werden, welche ich selbst im Zusammenhang mit einem Online-Forschungsprojekt zur «Sicherheit und Delinquenz im Internet» vor einiger Zeit machen konnte. Dabei handelte es sich um eine Online-Befragung[29] einer überwiegend studentischen Population (n = 1419) aus dem Köln-Bonner Raum. Zentrale Fragen dieser Studie bezogen sich auf die im letzten Jahr gemachten Täter- und Opfererfahrungen in der eigenen Internet-Kommunikation. Eine weitere Fragestellung betraf das persönliche Sicherheitsgefühl im Netz und zwar im direkten Vergleich zum traditionell erfragten «Standard-Sicherheitsgefühl auf der Strasse». Die Ergebnisse dieser pilot-artigen, auch aus methodischen Gründen durchgeführten Studie waren eigentlich wenig

28 Siehe hierzu relativ aktuell und eindrucksvoll: PFEIFFER, CHRISTIAN, u.a., Die Medien, das Böse und wir. Zu den Auswirkungen der Mediennutzung auf Kriminalitätswahrnehmung, Strafbedürfnisse und Kriminalpolitik. In: *MSchrKrim,* 6/2004, S. 415-435

29 Zusammengefasste Ergebnisse hierzu unter: http://www.jura.uni-bonn.de/institute/krimsem/Online-Publikationen/Sudi03/8Zusammenfassung.PDF.

spektakulär. Entsprechend knapp und weitgehend sachlich ist auch unsere damalige Pressemitteilung ausgefallen. Das bekannte Online-Magazin «Telepolis» nahm diese Mitteilung zum Anlass, um bei uns weiter nachzufragen und ein fachlich durchaus kompetentes Online-Interview anzuhängen, welches dann auch im Internet unter dem Titel «Sicherer als auf der Strasse» publiziert wurde.[30]

Auf der anderen Seite liess es sich die aktuelle Nachrichten-Redaktion eines privaten Fernsehsenders (es war wohl «Pro 7») trotz deutlicher Gegenwehr meinerseits nicht nehmen, ihre abendliche Nachrichten-Show um 20 Uhr mit einer Meldung zur angeblich «deutlich steigenden Internet-Kriminalität» aufzumachen, welche dann noch durch einen entsprechenden filmischen Beitrag unterlegt wurde. Insoweit ist es nicht verwunderlich, wenn in den Köpfen der Bevölkerung zunehmend der Eindruck entsteht, dass die wachsende Internet-Kriminalität eine riesige Bedrohung unserer globalen Gesellschaft und unserer täglichen Kommunikation im Netz darstellt.

Bei aller Anerkennung der (wie oben beschrieben) zwangsläufig und absolut zunehmenden Delinquenzfälle im Internet, stellt sich aus wissenschaftlicher Sicht jedoch die berechtigte Frage, welche Erkenntnisse es gibt, um diesen Anstieg im Vergleich zum deutlichen Anstieg der generellen Internetnutzung einigermassen adäquat beurteilen und bewerten zu können. Das eigentliche Ziel sollte weder Dramatisierung noch Verharmlosung, sondern eine möglichst objektive und sachliche Beurteilung der Lage sein.

3 Bisherige Ansätze zur quantitativen Beschreibung der Internetdelinquenz und ihre Defizite

Hierzu will ich im folgenden die in der kriminologischen Fachwelt bekannten Datenquellen heranziehen, um einerseits das derzeit vor-

30 Im Netz derzeit immer noch zugänglich unter: http://www.heise.de/tp/r4/artikel/14/14806/1.html.

handene Wissen aufzuzeigen und um andererseits die vorhandenen Wissensdefizite deutlich zu machen und Wege zu ihrer zukünftigen Überwindung anzuregen und zur Diskussion zu stellen.

3.1 Besonderheiten der Internetdelinquenz und Dunkelzifferproblematik

Neben der rein quantitativen Beschreibung ist zunächst einmal eine eher *qualitative, kategoriale Beschreibung und Differenzierung* (oder kurz auch Kategorisierung) der unterschiedlichen Delinquenzphänomene im Internet vorzunehmen. Dazu gibt es bei den Behörden und in der Literatur zahlreiche Kategorisierungsangebote[31], welche sich im Kern fast alle auf eine grundlegende Zweiteilung[32] reduzieren lassen:

1. *Internetdelikte im engeren Sinne,* bei denen das Internet und die einzelnen angeschlossenen Computer als Tatziel dienen (z.B. Hacking, Viruses) und
2. *Internetdelikte im weiteren Sinne,* bei denen das Internet und die einzelnen angeschlossenen Computer als Tatmittel (auch für klassische Eigentumsdelikte wie z.B. Betrugsdelikte) dienen.

Hinsichtlich der *quantitativen Beschreibung* der Internetdelinquenz gilt es sozusagen vor der Klammer einige Besonderheiten zu erwähnen, welche eine zuverlässige Erfassung erschweren können. Neben der oben bereits genannten *Globalität und Transnationalität* sind dies vor allem auch die besondere *Virtualität und Anonymität* der Interaktionen im Netz. Diese Spezialitäten behindern einen umfassenden definitorischen und deskriptiven Zugang und fördern *besondere Selektivitäten und Dunkelzifferproblematiken.* Zahlreiche ab-

31 Die von mir ausgearbeiteten tabellarischen Übersichten hierzu können beim Autor bezogen werden (wruether@jura.uni.bonn.de).

32 Auf eine solche Zweiteilung bezieht sich u.a. auch: YAR, MAJID, The Novelty of «Cybercrime». In: *European Journal of Criminology,* Heft 4/2005, S. 407–427. DAVID WALL (*Crime and the Internet,* London 2001, S. 3–7) kommt letztendlich zu vier unterschiedlichen Arten von Cybercrimes: 1.Cyber-trespass, 2.Cyber-thefts,-fraud and -piracy; 3.Cyber-pornography; 4.Cyber-violence (hate speech, stalking).

weichende und delinquente Verhaltensweisen im Netz werden auf der ersten Selektionsstufe wahrscheinlich überhaupt nicht bemerkt. Falls sie bemerkt werden, müssen sie auf einer weiteren Selektionsstufe nicht unbedingt als strafrechtlich relevant definiert werden. Selbst wenn sie als strafrechtlich relevant angesehen werden, werden sie in einem weiteren Selektionsschritt vielfach nicht als solche bei den Strafverfolgungsbehörden angezeigt. Hierfür gibt es spezielle Gründe, wovon an erster Stelle (speziell bei betroffenen Unternehmen) immer wieder ein befürchteter Image-Schaden genannt wird, den man möglichst verhindern möchte.[33] Selbst wenn sie letztendlich dort als potentielle Straftaten ankommen, findet auf dieser Ebene ein weiterer Ausfilterungsprozess statt. Dieser hat viel damit zu tun, dass die erforderlichen Ressourcen und Kompetenzen für eine sachgerechte Bearbeitung und Erledigung der «modernen, digitalen Delinquenz» bei den Strafverfolgungsbehörden (noch) nicht in ausreichendem Masse zur Verfügung stehen.

3.2 Erfassungen auf nationaler Ebene: Daten der Strafverfolgungsbehörden

3.2.1 Polizeiliche Daten

Die polizeilichen Daten hinsichtlich der Internetdelinquenz liegen in der BRD zwar in drei unterschiedlichen, voneinander unabhängigen Varianten (PKS; IuK-Meldedienst; ZaRD-Statistik) vor, sie weisen dennoch alle drei die gleichen und die aus der kriminologischen Forschung hinlänglich bekannten Selektionsprobleme auf. Je intensiver zum Beispiel beim BKA zentral und anlassunabhängig nach überwiegend kinderpornografischen Inhalten im Netz gefahndet wird, desto mehr Delinquenz wird auch gefunden. Im Endeffekt sa-

33 Weitere bekannte Gründe für die Vermeidung von Strafanzeigen sind: 1. Mangelndes Zutrauen in die Arbeit der Behörden. 2. Mangelnde Informationen über die Zuständigkeiten. 3. Bewusstes Setzen auf alternative Konfliktlösungen. 4. Bagatellartige Einordnung des delinquenten Geschehens. 5. Besondere Beweis- und Nachweis-Problematik.

gen alle dort erstellten Zahlen mehr über die Aktivitäten der jeweils tätigen Behördenvertreter aus als über die realen Verhältnisse und Entwicklungen der zugrundeliegenden Delinquenz. Das gilt in besonderer Weise auch für die registrierten Fälle, welche durch den speziell eingerichteten polizeilichen IuK-Meldedienst anfallen.

Die einschlägigen Daten der PKS in der BRD besitzen zudem noch eine historisch zu interpretierende Selektivität und Beschränkung auf einzelne Delikte der klassischen «Computerkriminalität», deren Geburtsstunde in den 80er-Jahren gelegen hat. Damals hatte die Computertechnologie in Wissenschaft und Wirtschaft zwar schon ihre ersten markanten Spuren hinterlassen, das Internet als breites gesellschaftliches Kommunikationssystem hatte jedoch noch keinerlei Relevanz.[34]

Unter dem Summenschlüssel «Computerkriminalität» hat man insgesamt acht unterschiedliche Einzeldelikte zusammengefasst, die eigentlich relativ wenig Bezug zum Internet aufweisen. Zu Beginn der polizeilichen Registrierung im Jahr 1987 sind in dieser neuen Kategorie weniger als 5 000 Fälle von «Computerkriminalität» gezählt worden. Im Jahre 2004 waren es immerhin schon mehr als das zehnfache, nämlich 66 973 Fälle. Dennoch muss man relativierend berücksichtigen, dass dies im Endeffekt nur gut 1% von insgesamt über 6 Millionen polizeilich registrierten Straftaten in der BRD sind. Die grösste Einzelgruppe (mit 36 088 Fällen) bilden die «Betrugsdelikte mittels rechtswidrig erlangter Debitkarten mit PIN». Dahinter verbergen sich die bekannten Betrügereien mit elektronischen Bankkarten, welche überwiegend in Folge von klassischen Dieb-

34 Hier kann man sehr schön sehen, dass polizeiliche Erfassungsstrukturen sehr viel schwerfälliger und schwieriger zu ändern sind, als es die dynamischen gesellschaftlichen und technologischen Entwicklungen eigentlich erforderten. Die hier interessierenden, sich global im gesamten Netz verbreitenden Abweichungsphänomene sind mit dem Begriff Computerkriminalität keineswegs mehr adäquat zu erfassen. Hinsichtlich der besonderen Charakteristika, welche sich auf die gesamte vernetzte Kommunikation im Rahmen des Internet beziehen, ist der Begriff Internet-Kriminalität sehr viel adäquater. Bezogen auf die vielen eigentlich noch nicht weltweit und einheitlich als kriminell definierten Phänomene erscheint der Begriff Internetdelinquenz oder -devianz noch angemessener und er soll deshalb auch in diesem Text vorrangig verwandt werden.

stahlsdelikten stattfinden und relativ wenig mit dem Internet zu tun haben.

Abbildung 1 PKS-Computerkriminalität (BRD) nach Deliktsgruppen

Schlüssel	Straftaten(gruppen)	erfasste Fälle 2004	erfasste Fälle 2003
8970	***Computerkriminalität***	***66973***	***59691***
	davon:		
5163	Betrug mittels rechtswidrig erlangter Debitkarten mit PIN	36088	35954
5175	Computerbetrug (§ 263a StGB)	14186	11388
5179	Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	7357	7003
5430	Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung (§§ 269, 270 StGB)	570	237
6742	Datenveränderung, Computersabotage (§§ 303a, 303b StGB)	3130	1705
6780	Ausspähen von Daten	1743	781
7151	Softwarepiraterie (private Anwendung, z.B. Computerspiele)	2782	2053
7152	Softwarepiraterie in Form gewerbsmässigen Handelns	1117	570

Quelle: Bundeskriminalamt, Polizeiliche Kriminalstatistik 2004, Wiesbaden 2005

Seit dem Jahr 2004 sollen nun in der PKS auch all jene klassischen Delikte, welche mit dem «Tatmittel Internet» begangen worden sind, durch eine *entsprechende Sonderkennung* besonders gekennzeichnet werden, um so auch quantitative Anhaltspunkte über die «IuK-Kriminalität im weiteren Sinne» zu erhalten. Im ersten Jahr wurden auf diese Weise allerdings bundesweit «nur» 55 000 Internet-Straftaten (= 1,5% aller internet-relevanten Delikte überhaupt) gezählt, da die neue Erfassungspraxis noch nicht in allen Bundesländern angewandt wurde.[35] Es ist zu erwarten, dass nach breiterer Beteiligung der Län-

35 In diesem Jahr 2004 haben nur 10 von 16 Bundesländern diese neue Erfassungsmodalität praktiziert und das in vielen Behörden wegen der üblichen Anfangsprobleme noch zusätzlich selektiv und defizitär. Dabei wurden vor allem «Waren-Betrugsdelikte» im Zusammenhang mit Online-Auktionen registriert: Obwohl der Ersteigerer (in Vorkasse) gezahlt hat, wird keine (oder mangelhafte) Ware geliefert. Es bleibt hier die Frage, inwieweit hier überhaupt strafrechtliche oder eher «nur» zivilrechtliche Relevanz vorliegt.

der und der Behörden an dieser Erfassungspraxis im Jahre 2005 der Anstieg der entsprechenden Delinquenz (begangen mit dem «Tatmittel Internet») deutlicher ausfallen wird, aber selbstverständlich auch nicht überinterpretiert werden darf.[36]

3.2.2 Justiz-Daten

Dies trifft in ähnlicher Weise auch für die offiziellen Daten aus dem Justizbereich zu, welche aufgrund des bekannten Selektionsprozesses der strafrechtlichen Sozialkontrolle besonders auf der fortgeschrittenen Selektionsstufe der gerichtlichen Verurteilungen noch deutlich geringer und dürftiger ausfallen. Dies kann man beispielhaft an der Deliktskategorie der «Datenveränderung und Computersabotage» (§§ 303a, 303b StGB) demonstrieren. Während hierzu in der PKS immerhin noch deutlich mehr als 1000 Fälle gezählt werden, benötigt man zur Zählung der diesbezüglichen strafrechtlichen Verurteilungen nur noch einige wenige Hände: im Jahr 2001 sind für dieses zentrale IT-Delikt in allen Ländern der alten Bundesrepublik zusammen nur 24 Verurteilungen[37] ausgesprochen worden.[38]

---

36 Wie aus früheren Untersuchungen zum Anstieg der Umweltkriminalität (RÜTHER, 1986) bekannt ist, werden gerade bei neueren Delinquenzphänomenen die registrierten PKS-Zahlen durch spezielle Organisations- und Selektionsstrategien bei der Polizei zusätzlich gesteigert, was in erster Linie als eine verstärkte Ausschöpfung des Dunkelfeldes und weniger als ein realer Anstieg der Delikte zu interpretieren ist.

37 Statistisches Bundesamt, Arbeitsunterlage Strafverfolgung 2001, Tab. 2.1, S. 32f. / zum Vergleich: alle wegen Straftaten Verurteilten 2001: 517 118 + 201 584 (Straft. im Strassenverkehr) = 718 702, Stat. Bundesamt, a.a.O., S.18f.

38 Ohne jetzt im Detail auf weitere dieser spärlichen absoluten Zahlen eingehen zu wollen, lässt sich hinsichtlich der allgemeinen Deliktsstruktur (im Verhältnis Diebstahl zu Betrug) im Zeitablauf der letzten 10 Jahre immerhin eine interessante Entwicklung feststellen, die auch schon bei den polizeilich erfassten Straftaten auffällig geworden ist. Siehe Näheres hierzu bei: RÜTHER, WERNER, Zum Einfluss des Internets auf die Kriminalitätsstruktur und die Kriminalitätskontrolle. In: *Kriminalistik,* Heft 11/2004, S. 698–701. Diese Zahlen (siehe Abbildung 1) können in ihrer unterschiedlichen Entwicklung recht eindrucksvoll belegen, dass sich die offiziell registrierten und verurteilten Straftaten in ihrer gesamten Struktur weg von den bisher deutlich in der Überzahl befindlichen Diebstahlsdelikten und hin zu den Betrugsdelikten entwickeln. Es ist zu vermuten, dass dabei die massiven gesellschaftlichen Strukturveränderungen eine Rolle spielen, wozu auch die Entwicklungen und «Brüche» im Zusammenhang mit der oben beschriebenen «digitalen Revolution» gehören dürften. Im Sinne von KILLIAS (a.a.O., EuJCrim, 1/2006, S. 11–31) kann man dies als Folge eines technologisch induzierten «Bruches» in den Gelegenheitsstrukturen interpretieren.

Auf einer anderen justiziellen Ebene, nämlich auf der Ebene der Staatsanwaltschaften, wird man hingegen speziell im Jahr 2005 wahrscheinlich von einem riesigen Anstieg der staatsanwaltschaftlichen Ermittlungsverfahren in Bezug auf Verletzungen des Urheberrechts durch private Tauschbörsen-Nutzer erfahren. Hier wird nämlich speziell die Staatsanwaltschaft Karlsruhe seit dem letzten Jahr durch eine so genannte *Strafanzeigen-Maschinerie* des Schweizer Unternehmens Logistep in Zusammenarbeit mit einer Karlsruher Rechtsanwaltskanzlei mit entsprechenden Strafanzeigen überflutet.

Von der Karlsruher Generalstaatsanwaltschaft ist berichtet worden, dass innerhalb eines halben Jahres «rund 40 000 (!!) Strafanzeigen wegen illegaler Kopien von Musik, Software und Computerspielen» eingegangen seien. Die maschinelle Anzeigen-Produktion funktioniert dabei in folgender Weise: die Schweizer Firma ist darauf spezialisiert, für Rechteinhaber bestimmte Dateien in P2P-Netzwerken durch eine spezielle Technik aufzuspüren und die IP-Adressen der Dateianbieter zu protokollieren. In Zusammenarbeit mit der Karlsruher RA-Kanzlei werden sodann massenhaft Strafanzeigen gegen unbekannt gestellt. Die Staatsanwaltschaft ermittelt anschliessend im Rahmen eines eingeleiteten Strafverfahrens die zu den IP-Adressen passenden Personaldaten der Anschlussinhaber, welche dann auch durch Akteneinsichtnahme den Rechtsanwälten zugänglich und bekannt werden. Diese können nun gezielt für ihre Mandanten weiter tätig werden, während die Staatsanwaltschaft mit ihrem begrenzten Personal allein schon in den massenhaften formalen Registrierungsarbeiten zu ertrinken droht und um Abhilfe ringt.

Derzeit sieht die praktische Lösung so aus, dass man sich mit einer behörden-internen Bagatellregelung zu retten sucht, nach der alle Fälle eingestellt werden sollen, in denen die P2P-Nutzer nicht mehr als 100 verschiedene geschützte Werke zum Tausch angeboten haben. Als Konsequenz werden sowohl die staatsanwaltschaftlichen Ermittlungsfälle zu den Delikten der Internet-Piraterie rasant ansteigen, aber auch die entsprechenden Einstellungsquoten. Da diese

Verfahren in der Regel (an der Polizei vorbei) direkt zur Staatsanwaltschaft laufen, wird die Polizeiliche Kriminalstatistik hiervon kaum betroffen sein. Neben der Problematik einer Instrumentalisierung der Strafverfolgungsbehörden für sachfremde zivilrechtliche Zwecke und einer damit zusammenhängenden möglichen Überkriminalisierung von privaten Internetnutzern werden hier auch typische Probleme und Selektivitäten der statistischen Zählung von sich gesellschaftlich erst entwickelnden Internetdelikten offen gelegt.

3.3 Erfassungen auf internationaler Ebene: Befragungen und Meldestatistiken

Bei einem Blick über den nationalen Tellerrand hinaus zeigen sich aus kriminologischer Sicht weitere interessante Erfassungsansätze und Daten zur quantitativen Beschreibung der Phänomene der Internetdelinquenz. Dies sind zunächst Daten, welche aus klassischen Dunkelfeldbefragungen (3.3.1) gewonnen werden und zudem Daten, welche auf spezielle Meldestellen für Internetdelinquenz (3.3.2) zurückgehen.

3.3.1 Daten aus einzelnen Dunkelfeldbefragungen

Die Befragungsdaten lassen sich wiederum unterteilen in solche, welche (1.) durch repräsentative Bevölkerungsstichproben gewonnen werden und in solche, wo dies (2.) durch gezielte Befragungen von Behörden und Unternehmen geschieht.

1. Daten aus repräsentativen Bevölkerungsstichproben
Während das «normale» Internet-Verhalten in seiner gesellschaftlichen Struktur und Entwicklung durch repräsentative Bevölkerungsbefragungen relativ zuverlässig und gut abgebildet und beschrieben

wird,[39] kann man dies für das hier besonders interessierende «abweichende» Internet-Verhalten leider nicht behaupten. In der Bundesrepublik Deutschland sind entsprechende repräsentative Dunkelfeldbefragungen allenfalls in der Planung.[40]

In Grossbritannien hingegen besteht unter der Regie des «Home Office» zum einen bereits eine gewisse Tradition für die Durchführung von repräsentativen Dunkelfeldbefragungen speziell für die klassischen Delikte; aber neuerdings sind auch die modernen Internetdelikte («fraud and technology crimes») in die Erhebungen des «British Crime Survey 2002/03»[41] und des «Offending, Crime and Justice Survey 2003»[42] einbezogen worden. Dies erlaubt erste quantitative Aussagen zu einzelnen Aspekten der Internetdelinquenz und des vermuteten Dunkelfeldes aus kriminologischer Sicht.[43]

Danach liegt die Täter-Prävalenzrate bei den dort erfassten Internetdelikten zwar insgesamt bei immerhin 8,8% (gegenüber nur 3,9% bei den klassischen Diebstahlsdelikten); diese ist jedoch fast ausschliesslich auf die hohe Quote (8,7%) beim «illegalen Herunterladen von Software und Musik» zurückzuführen. Demgegenüber bewegen sich die beiden anderen abgefragten Delikte «Hacking» (0,4%) und «Sending viruses» (0,3%) nahezu an der Null-Linie. Hervorzuheben bleibt hierbei noch, dass die Internet-Täter überproportional häufig (etwa dreimal soviel) unter den befragten Männern (13,0%) als unter den befragten Frauen (4,7%) zu finden sind; dies gilt auch für al-

39 Siehe hierzu: CHRISTU, JEANETTE / KAISER, MARGIT, *Überblick über die wichtigsten Studien zur Internetnutzung in Deutschland und Europa*. Unter: http://www.digitale-chancen.de/content.

40 So z.B. das geplante DFG-Projekt des MPI in Freiburg (von T. KÖLLISCH), welches allerdings einigen Einschränkungen unterliegt (keine Online-Befragungen, keine Wiederholungs-Befragungen vorgesehen).

41 Der British Crime Survey (BCS), der bereits im Jahr 1982 zum ersten Mal durchgeführt worden ist, ist in erster Linie eine Opferbefragung von Bürgern (ab 16 Jahren) aus England und Wales. Näheres unter: http://www.homeoffice.gov.uk/rds/bcs1.html.

42 Der «Offending, Crime and Justice Survey» (OCJS) ist ein relativ neues Instrument, welches vor allem als Täterbefragung («self-reported offending and drug use») bei einer Population (von 10–65 Jahren) eingesetzt wird. Näheres unter: http://www.homeoffice.gov.uk/rds/offending_survey.html.

43 WILSON, DEBBIE, Hrsg., *Fraud and technology Crimes: findings from the 2002/03 British Crime Survey and 2003 Offending,* Crime and Justice Survey, Home Offfice Online Report 34/05 unter: http://www.homeoffice.gov.uk/rds/pdfs05/rdsolr3405.pdf.

le einzelnen Internetdelikte, besonders deutlich beim «Hacking» (0,6 zu 0,1%).

Abbildung 2 Täter-Prävalenz bei 18–65-Jährigen (letzte 12 Monate; nach Geschlecht)

Percentages ...	... in last 12 months		
	Males 18–65s	**Females 18–65s**	**All 18–65s**
Any theft offence	5.6	2.3	3.9
Any criminal damage offence	0.7	0.4	0.6
Any violent offence	4.1	2.5	3.3
Any drug offence	1.4	0.6	1.0
Any 'mainstream' offence	9.3	4.8	7.5
Unweighted base	*3,342*	*3,815*	*7,157*
Any fraud offence	**7.3**	**4.1**	**5.7**
Technology crime	**13.0**	**4.7**	**8.8**
Hacking	0.6	0.1	0.4
Sending viruses	0.4	0.1	0.3
Illegally downloading software/music	12.8	4.6	8.7

Quelle: British Offender Crime and Justice Survey (OCJS) 2003, S. 36
http://www.homeoffice.gov.uk/rds/pdfs05/rdsolr3405.pdf

Hinsichtlich der Opferbetroffenheiten von Internetdelinquenz lassen sich noch folgende Befunde herausstellen:

- 2,8% aller Befragten (bzw. 3,6% der befragten E-Karten-Inhaber) sind *Opfer eines elektronischen Karten-Betrugs* geworden; das wären hochgerechnet auf die Bevölkerung des Landes ca. 1,2 Millionen Personen.
- 6 % aller Befragten (bzw. 18,3% der befragten häuslichen Internetnutzer) haben angegeben, in den letzten 12 Monaten *durch einen Virus geschädigt* worden zu sein. Gut ein Drittel (36%) haben diesen Vorfall (zumeist an den Internet Service Provider) gemeldet; nur ganze 1% an die Polizei.[44]

44 Zur empirischen Aufhellung der Vorgänge und Hintergründe bei der Online-Strafanzeige siehe das aktuelle Forschungsprojekt des Kriminologischen Seminars der Universität Bonn: RÜTHER, WERNER, *Die Online-Strafanzeige als neues Instrument der strafrechtlichen Sozialkontrolle,* unter: http://www.bka.de/kriminalwissenschaften/kiforum/kiforum2005_dr_ruether.pdf.

- 1% aller Haushalte (bzw. 2,2% aller Haushalte mit Internetanschluss) sind nach dieser Befragung im letzten Jahr *Opfer von Hacking-Attacken* auf ihrem häuslichen PC geworden. Die diesbezüglichen Opferquoten liegen allerdings bei speziellen Opferbefragungen von wirtschaftlichen Unternehmen und Behörden durchaus höher.

2 *Daten aus speziellen Befragungen von Behörden und Unternehmen*

Die US-amerikanische Behörde/Strafverfolgungsbehörde CSI/FBI führt seit einigen Jahren eine umfangreiche Befragung zur IT-Sicherheit und zur Betroffenheit von «Computer-Crimes» bei einer Stichprobe von ca. 24 000 Wirtschaftsunternehmen mit mehr als einer Million US-Dollar Jahresumsatz und mindestens 5 Beschäftigten durch.[45] Insgesamt gibt es in den USA ca. 14 Millionen derartiger Unternehmen. Als Betroffenheitsquote wird im neuesten (10.) Bericht des Jahres 2005 eine Zahl von 87% genannt. Der Grossteil der Befragten (83,7%) sei in den letzten 12 Monaten von Viren, Würmern und Trojanern betroffen worden. Die nationale Gesamtschadenssumme durch IT-Delinquenz wird relativ freischaffend und ungezügelt auf 67 Milliarden US-Dollar hochgerechnet.[46]

Dabei ist jedoch zu bedenken, dass die Antwortquote bei dieser Befragung deutlich unter 10% gelegen hat; nur 2.066 der 24.000 angeschriebenen Unternehmen haben überhaupt geantwortet. Man darf korrekter Weise davon ausgehen, dass hier (wie bei derartigen Befragungen üblich) eine gezielte Selektion und Verzerrung stattgefunden hat. Es beteiligen sich besonders solche Unternehmen an

45 Die Ergebnisse werden jeweils in dem «Computer-Crime and Security Survey» veröffentlicht: http://www.crime-research.org/news/11.06.2004/423/.

46 Das US Treasury Department kommt in seinen Schätzungen sogar auf eine Summe von 105 Milliarden US-Dollar, welche durch die unterschiedlichsten kriminellen Handlungen per Internet im Jahr 2005 in dunkle Kanäle geflossen seien. Der Anbieter von Sicherheits-Software J. OBERMANN schreibt im Online-Sicherheitsmagazin *ITSecCity,* dass damit «Cybercrime profitabler sei als die Arzneimittelindustrie.» (!?!) http://www.itseccity.de/?url=/content/markt/kommentare/060126_mar_kom_mirapoint.html (26.1.06).

derartigen Befragungen, die überproportional betroffen und geschädigt sind. Gemessen an der angeschriebenen Grundpopulation liegt die IT-Betroffenheitsquote (von Viren, Würmern etc.) demnach eher nur bei 7% als bei 20%; letzteres wird in einem kühnen und kaum rational nachvollziehbaren Schritt jedoch von Seiten des FBI geschätzt und angenommen. Bei einem ermittelten durchschnittlichen Schaden von 24 000 US-Dollar und im wahrsten und doppelten Sinne des Wortes hochgerechneten 2,8 Millionen betroffenen Firmen (20% von 14 Millionen) summiert sich die insgesamt errechnete Schadenssumme auf stolze 67 Milliarden US-Dollar pro Jahr. Berücksichtigt man nun noch, dass in die Schadensberechnungen der gesamten Internetdelinquenz des Landes auch noch solche fragwürdigen Vorkommnisse im Zusammenhang mit Pornografie am Arbeitsplatz (22,4%) und eher als reine Bagatellen anzusehende Port-Scans (32,9%) einbezogen werden, dann darf man hier berechtigter Weise wohl eher von dramatisierenden Luftnummern sprechen als von seriösen Berechnungsgrundlagen.

Als Hintergrund dieser nationalen Schadens-Hochrechnungen (durch IT-Delinquenz) in den oberen zweistelligen «Milliarden- oder Phantastilliarden-Bereich», darf man handfeste fiskalische Interessen vermuten. Das FBI, welches die Bekämpfung der Internet-Kriminalität inzwischen angeblich auf Platz drei seiner Prioritätenliste gesetzt hat,[47] kämpft derzeit folgerichtig um eine entsprechende Erhöhung der finanziellen und personellen Ressourcen-Ausstattung für die kommenden Jahre. Auch im allgemeinen Kampf gegen den Terror kann eine stärkere Kontrolle der angeblich so schädlichen und gefährlichen Internet-Delinquenz und damit zwangsläufig auch eine intensivere Überwachung der generellen Internet-Kommunikation aus FBI-Sicht nicht schaden.

47 Siehe hierzu eine Heise-Meldung vom 20.1.2006: http://www.heise.de/newsticker/meldung/68593.

3.3.2 Daten von (Online-)Meldestellen

Ein weiterer Datenzugang zu den Phänomenen der Internetdelinquenz eröffnet sich durch spezielle Online-Angebote von privaten und staatlichen Organisationen, bei denen alle betroffenen Delinquenzopfer sozusagen per Mausklick eine Meldung oder Anzeige über das erlebte Delinquenzgeschehen erstatten können. Die wohl bekannteste und am meisten frequentierte Einrichtung dieser Art ist unter dam Namen «Internet Crime Complaint Center» (IC3) als eine offizielle Anlaufstelle der Regierung in den USA angesiedelt.[48]

Das IC3 veröffentlicht jedes Jahr einen Bericht, in dem sämtliche Online-Anzeigen zu den einzelnen Delinquenzfällen in einer Übersicht zusammengefasst und kommentiert werden. So ist die Gesamtzahl der Meldungen im Jahr 2004 (n = 207 449) gegenüber dem Jahr 2003 (n = 124 509) um über 66% angestiegen. Zu Beginn der statistischen Erfassungen im Jahre 2000 waren es weniger als 20 000 Meldungen pro Jahr. Das Anzeigenaufkommen hat sich somit innerhalb von vier Jahren mehr als verzehnfacht.

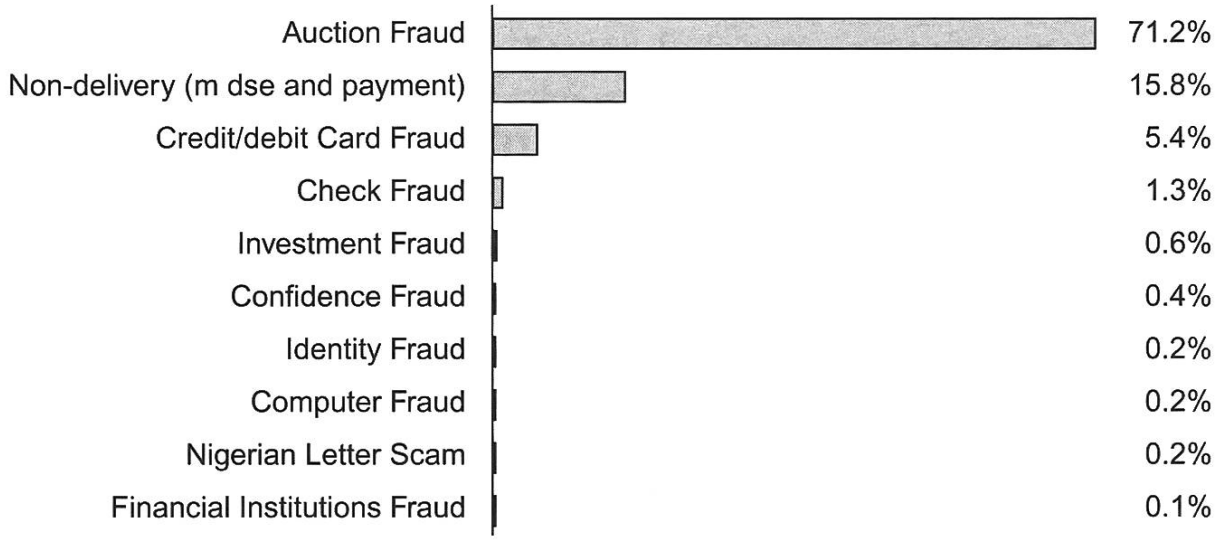
Dabei gilt es zu berücksichtigen, dass diese Zahlen nicht nur auf einen Anstieg des realen Delinquenzaufkommens hindeuten, sondern dass sie wahrscheinlich auch eine deutliche Veränderung und Zunahme des privaten Anzeigeverhaltens reflektieren. Dies ist u.a. dadurch gesteigert worden, dass die grossen Online-Auktionshäuser (wie z.B. ebay) einen direkten Link für betroffene Kunden zur IC3-Seite geschaltet haben.

Ein Blick auf die prozentuale Verteilung der Anzeigen hinsichtlich der einzelnen Deliktsarten zeigt denn auch ein deutliches Übergewicht des «Online-Auktionsbetrugs». Nahezu 3 von 4 Anzeigen (71,2%)

48 Sie wurde zu Beginn dieses Jahrhunderts zunächst unter dem Namen «Internet Fraud Complaint Center» (IFCC) eingerichtet. Zunächst hatte man eine Spezialisierung auf die Online-Betrugsdelikte angezielt; seit Ende des Jahres 2003 hat man das Spektrum jedoch erweitert auf «such criminal matters having a cyber (Internet) nexus.»

beziehen sich allein auf dieses Phänomen. Mit 15,8% folgen solche Online-Betrugsdelikte, bei denen im Bereich des sonstigen Online-Handels entweder kein Geld oder keine Ware geliefert worden ist. Alle anderen Deliktsphänomene machen in dieser Anzeigen-Statistik nur einen nahezu verschwindend geringen Anteil aus. Dies mag u.a. daran liegen, dass sie von den Betroffenen entweder gar nicht erkannt werden oder aber auch daran, dass sie nicht als melderelevant eingeschätzt werden. Insoweit darf man mit einiger Berechtigung vermuten, dass diese Daten der Online-Meldestellen, die es auch in vielen anderen Ländern gibt,[49] mehr über die Organisation, Bekanntheit und Attraktivität dieser Meldestellen aussagen als über die Quantitäten und Verteilungen der zugrunde liegenden Delinquenzphänomene.

Abbildung 3 Beim US-IC3 gemeldete Internetdelinquenz (2004) Verteilung auf die einzelnen Deliktsarten (in %)



Quelle: Jahresbericht 2005 des IC3, http://www.ic3.gov/media/annualreport/2004_IC3Report.pdf

49 Als ein weiteres Beispiel sei hier für die Schweiz die «Koordinationsstelle zur Bekämpfung der Internet-Kriminalität» (KOBIK) hervorgehoben. http://www.cybercrime.admin.ch/ Dort werden pro Jahr ca. 6000 Online-Meldungen registriert, welche allerdings auch solche Phänomene wie Spam (fast 30% der Anzeigen) und allgemeine Pornografie (14%) einbeziehen. Zur Verteilung auf die einzelnen Delikte siehe die Grafiken unter: http://www.cybercrime.admin.ch/d/rech/Rechenschaftsbericht_2004_d.pdf.

Aus einer übergeordneten kriminologischen Sicht ist ein weiterer gravierender Mangel der Datenbestände der verschiedenen Online-Meldestellen[50] darin zu sehen, dass sie untereinander so gut wie gar nicht zu vergleichen, geschweige denn in irgendeiner Form zusammenzufassen sind. Hier ist Abhilfe in Form von möglichst weitgehender Abstimmung auf supranationaler Ebene angezeigt.[51]

4 Zukünftige Erfassungsansätze auf supranationaler Ebene

Internetdelinquenz ist wie das Internet selbst ein supranationales, globales Phänomen, welches einigermassen sinnvoll und adäquat auch nur supranational und global beschrieben und erfasst werden kann. Hierzu ist zunächst einmal eine einheitlich und weltweit abgestimmte Kategorisierung (Taxonomie) aller einzelnen Phänomene erforderlich. Derzeit gibt es dazu eine Vielzahl von mehr oder weniger unterschiedlichen Ansätzen.[52]

4.1 Offizielle globale Meldesysteme (UN / WSIS)

Nachdem man sich auf eine einigermassen solide Basis der Kategorisierung (mit in der Natur der Sache liegender Dynamisierungs-Komponente) geeinigt hat, könnte man darauf aufbauend eine supranational operierende Sammelstelle für Internetdelinquenz-Daten anzielen. Diese wäre am besten im Rahmen der bereits laufenden und in Zukunft weiter geplanten WSIS-Aktivitäten aufgehoben. Auf dem letzten UN-Treffen in Tunis hat der «World Summit of Internet

50 So veröffentlicht auch die US-amerikanische Handels- und Verbraucherschutzbehörde FTC (Federal Trade Commission) regelmässig einen Bericht über die dort eingegangenen Bürgerbeschwerden und Anzeigen wegen unterschiedlicher, persönlich erlebter Betrugsfälle. Etwa die Hälfte der dort gemeldeten Fälle beziehen sich auf das Internet. Quelle: http://www.consumer.gov/sentinel/pubs/Top10Fraud 2005.pdf.

51 Dafür plädiert ebenfalls: MOITRA, SOUMYO D., *Analysis and Modelling of Cybercrime: Prospects and Potential.* Freiburg 2003 (MPI).

52 Siehe hierzu die tabellarischen Übersichten (beim Autor erhältlich: wruether@jura.uni-bonn.de).

Society» ja bereits eine zukünftige UN-Clearing-Zentrale für weltweite Internet-Nutzungsdaten beschlossen, welche sich sinnvoller Weise durch eine entsprechende Erfassung von weltweiten Internet-Delinquenzdaten ergänzen liesse.

4.2 Supranationale Dunkelfeldbefragungen

Eine relativ kurzfristig realisierbare und durchaus praktikable Möglichkeit in Richtung einer weltweiten, supranationalen Erfassung von Daten zur Internetdelinquenz scheint mir in einer entsprechenden Ergänzung und Erweiterung der bereits bestehenden Instrumente der supranationalen Dunkelfeldbefragungen zu liegen. So könnten in den Fragenkatalog des «International Crime and Victim Surveys» (ICVS) auch einzelne spezielle Fragen zur Betroffenheit von zentralen und bedeutenden Phänomenen der Internetdelinquenz aufgenommen werden. Dabei erscheint eine Orientierung an den diesbezüglichen einschlägigen Erfahrungen mit dem «British Crime Survey» (BCS) als durchaus sinnvoll.

Desweiteren bietet es sich gerade bei der Thematik der Internetdelinquenz in besonderer Weise an, auch das Internet selbst als methodisches Instrument und als Plattform für Befragungen zu nutzen und zumindest mittel- und langfristig auch «globale Online-Surveys» (GOLS) in das Standardrepertoire von weltweit konzipierten Dunkelfelderhebungen aufzunehmen. Je grösser in Zukunft die Anschlussquote der Bevölkerung an das Internet sein wird, desto besser werden auch die Möglichkeiten sein, möglichst repräsentative Stichproben der gesamten Bevölkerung auch in Online-Befragungen zu realisieren. Unter Berücksichtigung der Tatsache, dass man von Internetdelinquenz eigentlich auch nur im Internet als sogenannter Netzbürger (mit einem entsprechenden Netzzugang) betroffen werden kann, liessen sich sinnvoller Weise jeweils repräsentative Stichproben von der speziellen Grundgesamtheit der vorhandenen Netzbürger anzielen, welche dann auch online befragt werden könnten.

Methodisch wäre dies ein nicht nur kostensparendes, sondern ein in vielfacher Hinsicht reizvolles Unternehmen, was zudem noch der speziellen inhaltlichen Thematik (Internet) vollkommen angemessen wäre.

4.3 Neue technologische Wege in der Dunkelfeldforschung?

In dieser Richtung lassen sich noch einige weitere interessante methodische Zugänge zur Aufhellung des vermutlich sehr grossen Dunkelfeldes ins Auge fassen, welche bisher und traditionell (noch) gar nicht möglich waren und welche speziell durch die moderne Internet-Technologie erst ermöglicht werden. Ohne hierauf näher eingehen zu können, sei hier nur eine spezielle Art von *Online-Beobachtungen* (sog. «defacement mirrors») oder die Durchführung von besonderen *Online-Experimenten* (sog. «honeypots») erwähnt.[53] Es handelt sich hierbei um neuartige Instrumente des digitalen Zeitalters. Sie machen den Empiriker einerseits neugierig. Sie beinhalten andererseits wiederum ihre eigenen, nicht nur datenschutzrechtlichen Problematiken. Insofern werden sie die klassischen Instrumente nicht vollständig ersetzen, sondern allenfalls in gewissen Bereichen erkenntnisfördernd ergänzen können.

5 Fazit und Ausblick

Die Phänomene der Internetdelinquenz sind logischer Weise erst durch das Internet und die dahinter stehenden technologischen Veränderungen der «digitalen Revolution» entstanden. Sie sind Ausdruck von radikal veränderten Gelegenheitsstrukturen zur weltweiten Kommunikation. Die neuen digitalen gesellschaftlichen Struktu-

53 Näheres zu diesen neuartigen Methoden bei: DORNSEIF, MAXIMILLIAN, *Neue Wege in der kriminologischen Dunkelfeldforschung und Prävention? Vorgehensweisen, Erkenntnisse und Probleme beim Einsatz von elektronischen Ködern (honeypots).* In: DFK-Workshop, Prävention von Devianz rund um das Internet. Bonn, 14.–15.2.2006.

ren liefern ihre Abweichungsphänomene sozusagen automatisch mit. Abweichung und Delinquenz in der globalen Internetgesellschaft sind von daher als gesellschaftliche Phänomene genauso normal wie Abweichung und Delinquenz in jeder klassischen, «realen» Gesellschaft. Ihre einzelnen Ausprägungen und ihre quantitativen Grössenordnungen sind hingegen aus verschiedenen Gründen noch komplexer, unklarer, undefinierter und unzugänglicher als dies schon bei Abweichungsphänomenen in der klassischen Gesellschaft der Fall ist. Die vielfach vorhandenen Ansätze zur phänomenologischen Beschreibung und Quantifizierung sind besonders zum gegenwärtigen, relativ frühen Zeitpunkt des globalen Geneseprozesses als ein durch vielfältige und unterschiedliche Interessen bestimmtes Konstrukt zu interpretieren. Insoweit lassen sich diese Prozesse durchaus angemessen aus der auch kriminologisch etablierten Perspektive des sozialen Konstruktivismus analysieren. Es bedarf also keiner grundsätzlich neuen Kriminologie, sondern eher einer Erweiterung ihrer Methoden und einer Globalisierung ihrer Perspektiven. Die derzeitige Datenlage über die neuen Phänomene der Internetdelinquenz ist äusserst defizitär und widersprüchlich. Sie lässt sich als Spielball in alle möglichen Richtungen hin aufblasen und instrumentalisieren. Hierzu sind in diesem Vortrag mehrere Beispiele benannt und beschrieben worden.

Um in Zukunft einen möglichst rationalen und reflektierten Umgang mit der Thematik der Internetdelinquenz erreichen zu können, sind zunächst einmal die vorhandenen Wissensdefizite möglichst weit abzubauen und einige moderne, für die digitale und globale Phänomenologie passende methodische Zugänge zu suchen und zu etablieren. Dabei gibt es gute Gründe für eine zumindest mittelfristig zu realisierende Forderung nach einer weltweiten, netz-basierten und auf Dauer gestellten Online-Befragung und -Beobachtung durch eine weitgehend unabhängige, globale Institution.

Literaturverzeichnis

ALBRECHT, GÜNTER, Konstruktion von Realität und Realität von Konstruktionen. In: *Soziale Probleme,* Jg. 12/2001, Nr. 1/2, S. 116–145.

DORNSEIF, MAXIMILLIAN, *Neue Wege in der kriminologischen Dunkelfeldforschung und Prävention? Vorgehensweisen, Erkenntnisse und Probleme beim Einsatz von elektronischen Ködern (honeypots).* In: *DFK-Workshop, Prävention von Devianz rund um das Internet.* Bonn, 14.–15.2.2006.

FURNELL, STEVEN, *Cybercrime. Vandalizing the Information Society.* Boston 2002.

HAFERKAMP, HANS, *Kriminalität ist normal. Zur gesellschaftlichen Produktion abweichenden Verhaltens.* Stuttgart 1972.

HESS, HENNER / SCHEERER, SEBASTIAN, Was ist Kriminalität? Skizze einer konstruktivistischen Kriminalitätstheorie. In: *Kriminologisches Journal*, Jg. 29, Nr. 2/1997, S. 83–155.

KILLIAS, MARTIN, The Opening and Closing of Breaches. A Theory on Crime Waves, Law Creation and Crime Prevention. In: *European Journal of Criminology,* Heft 1/2006, S. 11–31.

LUHMANN, NIKLAS, *Die Gesellschaft der Gesellschaft,* Frankfurt 1997.

MOITRA, SOUMYIO D., *Analysis and Modelling of Cybercrime: Prospects and Potential.* MPI-Veröffentlichung, Freiburg 2003.

NIGGLI, MARCEL ALEXANDER / SCHWARZENEGGER, CHRISTIAN, *Internet – ein rechtsfreier Raum?* in: CASSANI, URSULA, u.a., Hrsg., *Medien, Kriminalität und Justiz.* Reihe Kriminologie, Band 19, Chur/Zürich 2001, S.303–329.

PFEIFFER, CHRISTIAN, u.a., Die Medien, das Böse und wir. Zu den Auswirkungen der Mediennutzung auf Kriminalitätswahrnehmung, Strafbedürfnisse und Kriminalpolitik. In: *MSchrKrim,* 6/2004, S. 415–435.

RÜTHER, WERNER, *Abweichendes Verhalten und labeling approach,* Köln u.a. 1975.

RÜTHER, WERNER, Zum Einfluss des Internets auf die Kriminalitätsstruktur und die Kriminalitätskontrolle. In: *Kriminalistik,* Heft 11/2004, S. 698–701.

RÜTHER, WERNER, *Kommunale Kriminalitätsanalyse. Auswertung offizieller Kriminalitätsdaten und einer Bürgerbefragung zum Sicherheitsgefühl in der Kommune.* Kassel 2005.

SMITH, RUSSEL G., *Internet-Related Fraud: Crisis or Beat-Up?* Paper presented at the 4. National Outlook Symposium on Crime in Australia, Canberra 2001.

WALL, DAVID, *Crime and the Internet,* London 2001, S. 3–7.

YAR, MAJID, The Novelty of «Cybercrime». In: *European Journal of Criminology,* Heft 4/2005, S. 407–427.